Blockchain Frontier Technology (B-Front)
Vol. 2 No. 1 July 2022

P-ISSN: 2808-0831
E-ISSN: 2808-0009

Blockchain for IoT Security Issues

Agung[1], Erick Febriyanto[2], Nur Iskandar[3], Rizki Alpian Sah[4], Yoke Suhendra[5], Nadila Andini[6]
Manajemen Retail, University of Raharja[1]
Multimedia Audio Visual and Broadcasting, University of Raharja[2,3,4,5,6]
Modern, Jl. Jenderal Sudirman No.40, RT.002/RW.006, Cikokol, Kec. Tangerang,
Kota Tangerang, Banten 15117
Indonesia
e-mail: agung.agung@raharja.info, erick@raharja.info, nur.iskandar@raharja.info, rizki.alpian@raharja.info, yoke.suhendra@raharja.info, nadila@raharja.info

Author Notification
01 July 2022
Final Revised
05 July 2022
Published
07 July 2022

Agung, Febriyanto, E., Iskandar, N., Alpian Sah, R., Suhendra, Y., & Andini, N. (2022). Blockchain for IoT Security Issues. Blockchain Frontier Technology, 2(1), 36–43.
DOI: https://doi.org/10.34306/bfront.v2i1.104

Abstract

In the past couple of years block chain has acquired a parcel of prominence in light of the fact that blockchain is the center innovation of bitcoin. Its use cases are filling in a number of fields like security of Internet of Things (IoT), banking area, enterprises and clinical focuses. Also, IoT has extended its acknowledgment as a result of its organization in brilliant homes and city improvements around the world. Sadly, IoT network gadgets work on restricted registering power with low capacity limit and organization transfer speed. In this manner, there are additional near assaults than other endpoint gadgets, for example, mobile phones, tablets, or PCs. This paper centers around tending to critical security issues of IoT and maps IoT security issues in logical inconsistency of existing arrangements tracked down in the writing. Besides, gifts that are not tackled after execution of blockchain are featured.

Keywords: *IoT, Blockchain, Organization, Security, Public*

1. Introduction

In the present period, advances have upset the expectation for everyday comforts of our general public. This is frequently a direct result of development in correspondence and semiconductor innovations, which grant gadgets to be associated over an organization and modify the method of network among machines and people. Such a pattern is generally noted as Internet-of-Things (IoT) [1].

With the quick ascent of splendid gadgets and fast organizations, the IoT has acquired wide acknowledgment and notoriety since it utilizes the standard called low-power lossy networks (LLNs) [2]. These LLNs can possibly utilize the restricted asset by consuming exceptionally low power. The gadgets in IoT might be controlled from a distance to carry out the predetermined role. The information dividing between the gadgets happens through the organization that utilizes the standard conventions of correspondence. The very much associated gadgets or "things" differ from simple wearable assistants to immense machines which contain locator (Sensor) chips [3].

Be that as it may, as it becomes well known the network between gadgets is expanding, and furthermore the processing foundation can turn out to be also muddled. This difficulty can give an ascent to weaknesses for the digital assaults [4]. In IoT, the actual gadgets are set in unstable conditions which could be exposed from programmers accordingly

offering them the chance to adjust the data that communicates over the organization. Consequently, gadget approvals and data root would be an indispensable issue [5].

In the most recent couple of years blockchain has started as the innovation that has numerous qualities to tackle various issues looked by IoT network gadgets. Blockchain keeps a disseminated data set of records [6]. In which confirmation of work between the organization hubs is totally denied of an outsider. This will help in taking care of the issue of weak links. Network exchange records are unchanging and can be established by means of the historical backdrop of the IoT network which at long last assists with getting the fascination by trust of the public in the IoT organization. This Public trust plays an essential part for the public monetary exchanges, early on for another universe of circulating economy in the Internet of Things space [7].

The blockchain is groupings of blocks that hold all exchange records occuring in a blockchain network. As depicted in figure.1 each block contains a block header and block body/exchange counter. Block header contains the accompanying;

1. Block adaptation which demonstrates the product rendition also, approval rules.
2. Merkle Tree root hash addresses the hash worth of the exchange and synopsis of all exchanges.
3. Timestamp comprises current all inclusive time since January 1970.
4. N-Bits characterize the quantity of pieces expected for exchange check.
5. Nonce is any 4-byte number that begins from 0 and increments for each hash of the exchange.
6. Parent block hash holds the hash esteem which shows the past block.

Exchange counter is equipped for covering all the exchanges and a most extreme number of the exchange relies on the block size. Blockchain innovation alluded as a public record what not finished exchanges are kept in a rundown of blocks. This chain of blocks develops as new blocks are added to the chain constantly [8]. Public key cryptography and conveyed agreement calculations carried out for client security. The blockchain innovation has key attributes of decentralization, persistence, secrecy, and auditability. With these qualities, blockchain can save the expense and expands the viability [9].

This paper is requested as follows. Segment 2 covers the Blockchain properties whereas segment 3 features its qualities. Different security necessities and issues are shrouded in segment 4 and segment 5 gives the arrangement of safety issues utilizing blockchain. Area 6 depicts the issues that are not tackled by blockchain. At last in Section 7 end and future work is introduced[10] .

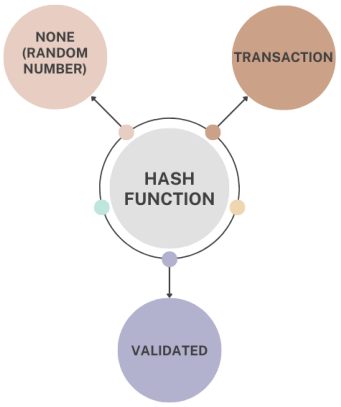

Figure 1. Proof of Work.

2. Research Method

2.1. Blockchain Working Steps

Hubs speak with the blockchain network through a mix of private and public keys. The User Uses Its Own confidential key to carefully sign its own exchanges and afterward can This paper is requested as follows. Area 2 covers the Blockchain properties whereas segment 3 features its attributes. Different security necessities and issues are access to the organization through the public key. Each marked exchange is communicated by a hub that makes the exchange.

The exchange is then checked by all hubs inside the blockchain network aside from the hub that makes the exchange. During this step, any invalid exchanges are disposed of. It's known as confirmation.

Mining is the third move toward which each real exchange is gathered by the organization hubs during a proper time into a block and carries out a proof-of-work to track down a nonce for its block. When a hub finds a nonce, it communicates the block to every participating hub.

Each hub gathers a recently created block and affirms whether the block contains (a) lawful exchanges and (b) pronounces the precision of the parent block by using the hash esteem. After the culmination of affirmation, hubs will add the block to the blockchain and apply the exchanges to bring the blockchain modern. On the off chance that, on the off chance that the block isn't affirmed, the projected block is dismissed. This closures the current mining round.

2.2. Check

Blockchain innovation guarantees the end of the duplication issues by taking help from unbalanced cryptography which contains a public and a confidential key. The confidential key is hidden from different hubs though the public key is divided between any remaining hubs. Besides, the exchange (stage 1) is carefully endorsed by a hub that makes the exchange which is communicated to the whole blockchain network. All getting hubs will confirm the exchanges by decoding the mark with a public key of the introducing hub. The exchange is confirmed by the check of mark which shows the introducing hub isn't altered.

2.3. Verification of-Work (POW)

The verification-of-work (figure 2) contains the most common way of finding a worth that is hashed with Secure Hash Algorithm 256. The common work required is outstanding inside the range of zero pieces required and affirmed by running the hash calculation. In Figure 2. Verification of Work.

3. Attributes OF BLOCKCHAIN

3.1. Decentralization
In a concentrated exchange handling climate, every exchange should be approved through the brought together confided in party (e.g., banking framework), that outcome into significant expense and low execution at the essential issue. Regarding the unified IoT model, the outsider is not generally required in the blockchain. Agreement calculations in blockchain are utilized to keep up with information trustworthiness and consistency.

3.2. Persistency
When an exchange record is approved by an excavator hub (unique hubs that approve the exchange) in a blockchain network its duplicate is communicated to the whole organization and that record isn't erased or rolled back from the whole blockchain.

3.3. Secrecy
In Blockchain, hubs collaborate with the organization utilizing a public key that tends to the hub on the whole blockchain network by keeping the genuine personalities of the client as confidential.

3.4. Security
Blockchain utilizes the unbalanced cryptographic strategy to get the whole organization. Topsy-turvy or public key cryptography contains 2 keys, one public key and second private key.

3.5. Adaptability or More Addressing Space
AS adaptability is concerned blockchain contains 160-piece address space when contrasted with 128 bit in IPv6. These 160-pieces are created by ECDSA (Elliptic Curve Digital Signature Algorithm). Blockchain has 4.3 billion additional Addresses over IPv6.

3.6. Versatile Backend
Each circulated hub inside the blockchain IoT network keeps an imitation of the entire record. This aids in protecting the organization from any possible disappointments and assaults.

3.7. High Efficiency
Since the exchange eliminates the contribution of the outsider and may continue in low-trust condition, the time spent to confirm an exchange will be diminished though the proficiency will be expanded.

3.8. Straightforwardness
Changes made to the public blockchain network are freely distinguishable by all members in the organization. Additionally, all exchanges are permanent, meaning they can't be changed or erased.

3.9. Shrewd Contract
The shrewd agreement is one of the most proficient parts of Ethereum presented by Nick Szabo in 1994. Utilizing brilliant agreement programs are written in which access freedoms

and various approaches are characterized. Many programming dialects are upheld by Ethereum to compose brilliant agreements like Solidity.

4. SECURITY NECESSITIES FOR IoT OR ISSUES

4.1. Information Privacy

Due to a differentiated joining of administrations and organization, the information recorded on a gadget is defenseless against assault by compromising hubs existing in partner IoT organizations. Besides, an assailant can get the information without the proprietor 's consent.

4.2. Information Integrity

In a unified client-server model, the aggressor might acquire unapproved admittance to the organization and change the first information or data and forward it. For instance, X sends information to Y, Z the center person could get information first and forward the information after alteration.

4.3. Outsider

Information gathered in a unified climate is put away and constrained by a third concentrated substance that might miss utilize this information or give it to another person.

4.4. Confided in Data Origin

In the IoT climate, it is hard to know the beginning of information and information may be modified during the transmission by anybody.

4.5. Access Control

Access control is one of the main pressing concerns in the IoT organization. It is hard to characterize in an IoT network which hub has the option to get to and carry out an alternate role with information.

4.6. Weak links

Constant development of unified networks for the IoT based framework could uncover weak links. As everything information of the whole organization is put away and checked by a focal expert for the situation, in the event that the essential issue falls flat or goes down the entire organization is upset.

4.7. Versatility

IoT interfaces an enormous number of sensors and different gadgets for data sharing and countless applications by means of the web. It challenges the construction and the fast development of the framework to meet adaptability.

4.8 Illegal utilization of Personal Data.

IoT gadgets are essentially sensors and embedded chips that assemble individual, significant data and pass it on through the web. The accumulated data is put away in a focal data set of any firm. This information uncovered the individual execution of clients; classification of clients is in danger as firms would utilize the information illicitly. An illustration of such secrecy abuse is the PRISM Surveillance program.

4.9 IoT Network Information Sharing.

The data accumulated by IoT network gadgets are recorded particularly with the end goal of investigation. Data sets might contain IoT gadgets, network information load or their working logs. To affirm the effectiveness of instruments and tests, open availability of data assumes a fundamental part. Thus, every time these data sets are transparently shared their

trustworthiness is critical.

5. BLOCKCHAIN SOLUTIONS FOR IoT

5.1. Information Integrity

The blockchain is a distributed organization where all hubs have similar duplicates of records. At the point when an exchange is started, the initiator hub signs the exchange with its confidential key and sends it to different hubs for approval. Any remaining digger hubs partake in the nullification cycle and attempt to track down nonce. The hub which finds the nonce initially has the option to approve and get a prize. Additionally, the recently made block will be communicated to any remaining hubs of the whole organization. When the record is stacked in the blockchain it can't be changed or erased.

Figure 3. Consortium Blockchain Network.

5.2. Information Privacy

Consortium blockchain used to give information security in a blockchain network. As in figure.3,nodes utilized for a specific object are consolidated together to frame a confidential organization/sidechain. Each sidechain is liable for dealing with its own IoT information. Hubs that are partaking in one sidechain are not permitted to participate in the approval cycle of opposite side chains. To get to the information of the consortium blockchain network the hub first necessitates to enlist and turn out to be important for that sidechain network. Consortium blockchain approaches control and forestalls unapproved access.

5.3. Tending to Space

Blockchain contains 160-piece address space when contrasted with 128 digits in IPv6. These 160-pieces are produced by ECDSA (Elliptic Curve Digital Signature Algorithm). Blockchain has 4.3 billion additional addresses than IPv6 along these lines giving more tending to separating than IPV6 addresses.

5.4. Confided in Accountability.

Each activity record should be transferred to the blockchain network. This gives each activity a character and every activity is detectable. At the point when an unusual way of behaving is recognized in an element, blockchain will be utilized for an extra examination.

5.5. Adaptation to internal failure

Decentralized gadgets are more averse to flop coincidentally on the grounds that they depend on many separate parts. The blockchain is a highlight point decentralizing organization; in it, each gadget has a similar duplicate of a record. That is the reason the disappointment of a solitary hub affects the organization. In this way, blockchain forestalls a weak link.

5.6. Confided in Data Origin

To follow information in the blockchain network, an extraordinary id is relegated to each IoT gadget. Information gathered from a gadget is related with its id and subsequent to working out a hash on information, the information is submitted to the whole organization. This turns into the reason for confiding in information beginning.

5.7. Eliminating Third-Party Risks

Blockchain innovation makes the gadgets fit for performing tasks without the delegate or outsider, hence making it risk-liberated from an outsider.

5.8. Access Control

By utilizing brilliant agreements, programs for blockchain can be created in which access

privileges and various arrangements are characterized. Model a standard is set when the meter scopes to 135 KW, gadgets will enter in energy saving mode.

5.9 Illegal Use of Personal Data.
Unlawful utilization of individual information can be disallowed with the utilization of blockchain. As Blockchain Peer to Peer (P2P) , putting away frameworks can confirm and record all activities achieved on IoT network information. The point is to convey decentralized capacity any place administrators can have control over their information as an option in contrast to any unified mediator authority. So the security is more extended to various levels [6] where 'Consortium blockchain' for IoTs is proposed.

5.10 IoT Network Information Sharing.
As the size of IoT network data sharing is expanding, in this manner the key stockpiling cost will likewise increment. So data sets are kept in far off beginnings and a concentrated server is protected which will desolate hold the references to these starting points. Besides, Blockchain is utilized to keep the RIM (Reference Integrity Matrix) of the data set. As the Blockchains have an Immutability element, and availability of the RIM with all IoT network gadgets in Blockchain, guarantees the Integrity of RIM. Each time a compulsory Information Set is taken from the beginning, its Integrity can be affirmed by contrasting its RIM being kept up with on Blockchain.
In Table 1 attributes of blockchain are featured through which issues of IoT can be handled.

6. BLOCKCHAIN IMPLEMENTATION PROBLEMS.

Obscurity
Blockchain is a dispersed organization; obscurity is influential for safeguard protection. Properly, blockchain gives pseudonymity meaning the clients don't have a genuine ID. The clients have a Public key which is utilized to accomplish exchanges on this disseminated network. Utilizing this ID a client can be found by means of a blend of these Ids and IP tends to connect with them. Additionally, when a client utilizes beyond what one Public key it very well may be followed by checking whether the various addresses have a place with a similar client. Answer for the Anonymity is a future work.

7. Conclusion

This paper means to introduce the writing audit on Blockchain and Internet of Things and underscored issues connected to an IoT air. IoT is the following arising innovation with the ascent of rapid organization and clever organization gadgets. Tragically, IoT gadgets are more inclined to assaults and incapable of safeguarding themselves. In this paper, the various properties and attributes of the blockchain network are featured to eliminate the issues in IoT. Additionally, issues that are not settled after execution of blockchain are featured.

7.1 Future Work
We further expect to basically execute blockchain properties on the web of things for checking, mistake revelation, and programmed issue revision in high basic IoT frameworks. Additionally, reproduction based execution evaluation can be led to exhibit the adaptability and viability of the blockchain-based arrangements.
Moreover, as IoT gadgets are in straightforwardly reachable regions and very under the control of a rival, a blockchain based arrangement can be executed that will guarantee the security and classification of the data kept in the gadgets. This will likewise address diminishing the choice of the equipment and programming of an IoT gadget from being compromised assuming the gadget is open to everybody.

References

[1] R. Widayanti, U. Rahardja, F. P. Oganda, M. Hardini, and V. T. Devana, "Students Formative Assessment Framework (Faus) Using the Blockchain," in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2021, pp. 1–6.

[2] M. Saraswati, N. Lutfiani, and T. Ramadhan, "Kolaborasi Integrasi Inkubator Bersama Perguruan Tinggi Sebagai Bentuk Pengabdian Terhadap Masyarakat Dalam Perkembangan Iptek," *ADI Pengabdi. Kpd. Masy.*, vol. 1, no. 2, pp. 23–31, 2021.

[3] N. Sari, W. A. Gunawan, P. K. Sari, I. Zikri, and A. Syahputra, "Analisis Algoritma Bubble Sort Secara Ascending Dan Descending Serta Implementasinya Dengan Menggunakan Bahasa Pemrograman Java," *ADI Bisnis Digit. Interdisiplin J.*, vol. 3, no. 1, pp. 16–23, 2022.

[4] U. Rahardja, T. Hariguna, and W. M. Baihaqi, "Opinion mining on e-commerce data using sentiment analysis and k-medoid clustering," *Proc. - 2019 12th Int. Conf. Ubi-Media Comput. Ubi-Media 2019*, pp. 168–170, 2019, doi: 10.1109/Ubi-Media.2019.00040.

[5] I. Handayani, U. Rahardja, E. Febriyanto, H. Yulius, and Q. Aini, "Longer Time Frame Concept for Foreign Exchange Trading Indicator using Matrix Correlation Technique," *Proc. 2019 4th Int. Conf. Informatics Comput. ICIC 2019*, 2019, doi: 10.1109/ICIC47613.2019.8985709.

[6] R. Aulia, A. Sururi, and S. Sukendar, "Effectiveness Of Featured Product Of Rural Areas Program (Prukades) In Improving The Economy Of Teluk Village Community Pandeglang Regency," *ADI J. Recent Innov.*, vol. 2, no. 1 Sept, pp. 204–211, 2020.

[7] E. Retnaningtyas, E. Kartikawati, and D. Nilawati, "erma UPAYA PENINGKATAN PENGETAHUAN IBU HAMIL MELALUI EDUKASI MENGENAI KEBUTUHAN NUTRISI IBU HAMIL," *ADI Pengabdi. Kpd. Masy.*, vol. 2, no. 2, pp. 19–24, 2022.

[8] F. P. Oganda, M. Hardini, and T. Ramadhan, "Pengaruh Penggunaan kontrak cerdas pada Cyberpreneurship Sebagai Media Pemasaran dalam Dunia Bisnis," *ADI Bisnis Digit. Interdisiplin J.*, vol. 2, no. 1, pp. 55–64, 2021.

[9] U. Rahardja, Q. Aini, F. P. Oganda, and V. T. Devana, "Secure Framework Based on Blockchain for E-Learning During COVID-19," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–7.

[10] T. Alam, "Cloud Computing and its role in the Information Technology," *IAIC Trans. Sustain. Digit. Innov.*, vol. 1, no. 2, pp. 108–115, 2020.