Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TOWARDS AN EFFICIENT IOT SYSTEM BY INTEGRATING BLOCKCHAIN IN IOT

RAJAT VERMA[1, *], NAMRATA DHANDA[1], VISHAL NAGAR[2], MUDRIKA DHANDA[3]

[1, *]Department of CSE, ASET, Amity University, Lucknow, Uttar Pradesh, India.

[2]Department of CSE, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India.

[3]Senior Product Analyst, Anaplan, United Kingdom.

E-mail: [1, *]rajatverma310795@gmail.com, [1]ndhanda@lko.amity.edu , [2]nagarvishal8212@gmail.com,

[3]mdrkdhanda@gmail.com

ABSTRACT

The extension of the Internet of Things (IoT) started with the invention of the Electromagnetic Telegraph in 1832. Since then, IoT has never looked back and continues to grow rapidly. Today, IoT is capable enough of interacting with billions of users together, generating a voluminous amount of data by performing different operations on IoT devices by the users. Data and Operations are precious assets of an organization that must be kept secure. It should have Confidentiality, Integrity and Availability, which denotes the normal CIA triad in cyber-security. With this, the 3 A's (i.e., Authentication, Authorization and Auditing) should also be followed for keeping the facts and figures secured. Alternatively, the negative side of the development in the technological field is also evolving i.e., cyber-attacks. Today with the development, cyberattacks are much stronger, so conventional security must be upgraded with some SMART solutions. The reason is that the old solutions are somehow responsible for the bugs and concerns it generates in the IoT systems. Here, Blockchain comes into the picture, which is a network technology, which follows immutability, transparency and decentralization. Blockchain emerged as the next big thing when it was used with Bitcoin as a security measure. This Paper illustrates the integration of Blockchain in IoT for enhancing the security aspects of IoT systems. Moreover, this paper also analyses the efficiency of Blockchain transactions in IoT, making a normal IoT device into a Blockchain-secured IoT device (IoT-B). A variety of use cases are available, but the authors have considered a General-Purpose Input Output (GPIO) emulator as an IoT device for examining the efficiency of blockchain transactions.

Keywords: *Blockchain, IoT, IoT-B, Privacy, Security.*

1. INTRODUCTION

The Internet of Things (IoT) is a renowned technology, whose popularity needs no introduction. It can communicate with devices and sensors with or without the intervention of human beings. IoT is a multidimensional field that involves various aspects such as communication technology, information technology, actuator technology, etc. According to research by 2025, the number of connected devices in the IoT spectrum will be around 75 billion [1]. The data volume & IoT data (worldwide) will have limitless figures by 2025 [1][2][3], which must be kept secured as attackers are everywhere to harm the integrity of the data and operations. Along with Integrity, Confidentiality and Availability are also required to follow the CIA triad of cyber-security. If any of the aspects is disturbed, then it can create a loss in the reputation of the organization and may harm its economy. Cyberattacks are also upgrading and enhancing day by day and the conventional measures to stop the security attacks are not well enough now. Therefore, there is a requirement for a modern and SMART solution. SMART stands for Specific, Measurable, Achievable, Realistic and Timely, with all these characteristics Blockchain comes into the picture which is a network technology that involves decentralization, immutability and transparency that can eliminate the central failure point and minimize data breaches and inconsistency. The initial blockchain concept was developed by the American Scientist David Chaum in 1982 [4][5]. Then around 9 years later, i.e., in 1991, W. Scott Stornetta and Stuart Haber incorporated Merkle Root [6]. Slowly and gradually, in 2008, the initial release of

Blockchain came with bitcoin [7][8]. Blockchain is an arrangement of blocks that are amalgamated using hash values, if tampering is attempted then all the hash values should be altered in the chain. If the attacker has all the resources for tampering with a single chain, then also it is somehow impossible to alter the chains present in the entire decentralized network [9]. Blockchain has evolved four times starting from Blockchain 1.0 and going to 4.0. The initial Blockchain 1.0 was considered Bitcoin Emergence and ran from 2008 to 2013. Blockchain 2.0 was known as Ethereum Development and ran from 2013 to 2015. Blockchain 3.0 was known as the Applications Phase and ran from 2015 to 2021. Blockchain 4.0 is currently in the developing phase that deals with the combined phase of Blockchain and Artificial Intelligence [9][10]. Blockchain follows a high-end security mechanism that follows Secure Hashing Algorithms (SHA-256), the combined approach of Digital Signatures and Elliptic Curves (ECDSA). Secure Hashing Algorithms provide a fixed output of 64 hexadecimal characters [11]. The ECC has an identical security level to RSA, but with a lesser number of keys [12]. The comparison of the keys (nature-approximate) of RSA and ECC is shown below in Figure 1 [22] [23] [24].

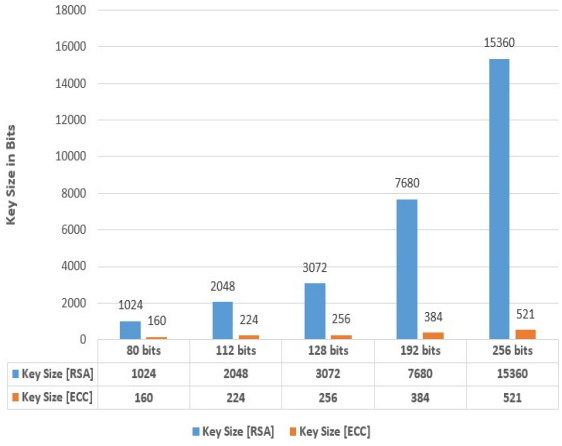

Figure 1: Key Size Comparison (RSA & ECC) [22-24]

Figure 1 shows the key comparison between the RSA & ECC algorithms while providing the same amount of security. Thus, ECC is far better than RSA. The purpose of the manuscript and the implementation is to analyze the efficiency of blockchain transactions on an IoT device. Here the General-Purpose Input Output (GPIO) emulator is acting as an IoT device (as an illustration) that will be evaluated on different seconds of operations (1, 2, 3…) and the blockchain transactions will be observed. Securing the status of pins (ON & OFF) present on the GPIO emulator using Blockchain technology is also an objective of the implementation.

The Next Section illustrates the layout of the Block & Blockchain.

2. BLOCK & BLOCKCHAIN

The Block's structure of a Blockchain is unique as it has two segments. The upper segment is known as the Header that contains 5 elements, such as Block's Sequence Number, Current Block Hash, Previous Block Hash, Nonce, and Creation-Time Stamp. The lower segment considers the Body Data. The Blocks are connected to form a Blockchain. The layout of a block is shown in Figure 2.

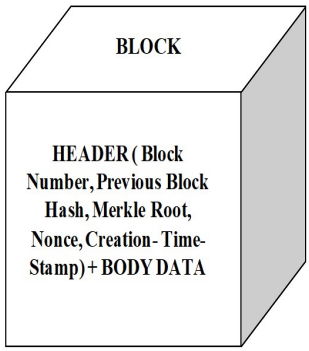

Figure 2: The layout of a Block in a Blockchain

Figure 2 illustrates the constituent of a blockchain. The initial entity of the header indicates the location of a node in the blockchain where the block lies in the sequence. The previous hash digest is the hash of the succeeding node about the present block. The Hash Digest of the present block is referred to digest of the current block. The nonce is the identity concerning the number that will be used only once and acts as a security measure. Lastly, the time of node creation. The First node is known as the Genesis Block, highlighted as A in figure 3 [13][14][15].

Blockchain follows the principle of the longest chain. If the nodes belong to the longest chain, they are valid blocks and if not, they will be known as Orphan Blocks [16]. Figure 3 shows the concept of Blockchain with orphan blocks.

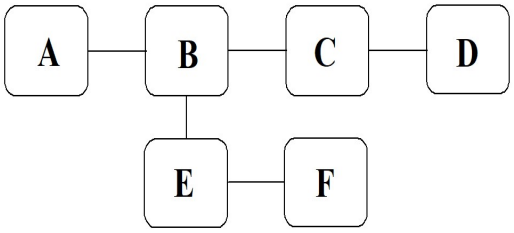

Figure 3: A Simple Blockchain

Figure 3 shows the structure of a Blockchain that has two chains, one from A to D (considering A as the starting point) and the other from B to F (as an example and considering B as the starting point). The first chain i.e., from A to D is the main chain and the sub-chain from B to F where E and F are orphan blocks that do not belong to the main chain. Here, blocks A, B, C, and D are valid blocks [17].

3. IOT ISSUES AND ITS BLOCKCHAIN SOLUTIONS

The Development of IoT with conventional security techniques lead to diverse consequences that are shown below in Table 1. Issues in any industry must be cleared and corrected as ignoring the issues can lead to serious challenges and may harm the reputation of the organization.

Table 1 also highlights the attributes of Blockchain and the corresponding comments concerning IoT issues. Majorly the issues focus on illegitimate device access, bugs, intrusion, rules and regulations, standard configurations, transparency and enforcement, risks, minimal encryption, etc.

Table 1: Issues of the Internet of Things & its Blockchain Solutions

Issues	Comments	Blockchain Attributes
Erroneous & Illegitimate Device Access	The accepted mechanism of IoT can have maximal confidence in the nodes present in a LAN. Further certification is not possible because of the trust that is already developed.	SHA- 256 & Immutability permits the concerned issue of IoT to be tackled.
Insufficiency in Encryption	The accepted mechanism of IoT is vulnerable to attacks. The reason is the frail encryption.	SHA-256 & ECDSA permit the concerned issue of IoT to be tackled.
Buggy software susceptibility & deficiency of a trusted environment for the implementation	The accepted mechanism of IoT admits that logic bombs and other relatable attacks can be activated and triggered by bugs.	Agreement-based mechanisms permit the concerned issue of IoT to be tackled.
Idleness with Intrusion	The accepted mechanism of IoT admits that they function normally if any intrusion is detected that attempts for tampering.	Complete change of hash values when tampering is attempted permits the concerned issue of IoT to be tackled.
Control, Authentication, Confidentiality	The accepted mechanism of IoT devices admits that there is a lack of optimality in operations (controlling) to secure devices from attacks.	Confidentiality is achievable with suitable configurations. Cryptography involves authentication and control.
Rules & Laws	The accepted mechanism of IoT admits that IoT devices and software are being developed without properly following the laws of security leading to data which misleads in various aspects.	Ensures security and other relatable parameters. Minimal chances of misleading data.
Security with shared collaborations	The accepted mechanism of IoT is also not sure whether can with shared collaborations, IoT Security could be enhanced or not?	Consensus Mechanisms, Decentralization, Immutability, and Transparency ensure the same.
Fairness regarding the collection and use of facts and figures	The accepted mechanism of IoT admits that there is an unavailability of standard and rigid regulations against the	The concerned issue of IoT is achievable with blockchain attributes.

	collection and use of facts.	
Transparency & Enforcement	The accepted mechanism of IoT admits that there is an unavailability of configurations and models that can tackle the concerned issue.	The concerned issue of IoT is achievable with blockchain attributes.
Risks	The accepted mechanism of IoT admits that there is negligible awareness of risk protocols.	Technical risks, Inconsistency and Breaches in facts and figures are minimized. The reason is immutability.
Standard Configurations	The accepted mechanism of IoT admits that there is an unavailability of standard configuration which can deal with scalability factor.	Standard configurations and lightweight blockchain (future scope) can enhance scalability.

4. THE IMPLEMENTATION OF AN IOT SYSTEM SECURED BY BLOCKCHAIN

The Implementation over here is the development of an IoT system that is secured by Blockchain. Here, a General-Purpose Input Output Emulator (GPIO) is considered that is acting as an IoT Device involving sensors and circuits. This means that the GPIO emulator is acting here as a use case. GPIO is a digital pin on an Integrated Circuit (IC) or a circuit board (electronic) that can be operated by software and can function as input or output or both. This IoT system with Blockchain is a general approach to increase the security spectrum of IoT devices. For the efficient integration of python programming, the emulator is being used rather than hardware [18]. This implementation is required because it will revolutionize the traditional scenario of security that was based on a centralized architecture and will work in a much more secure and efficient manner by eliminating the conventional security and privacy issues of IoT.

Figure 4 shows the GPIO emulator with default values i.e., the values are not altered and are represented by green colour.

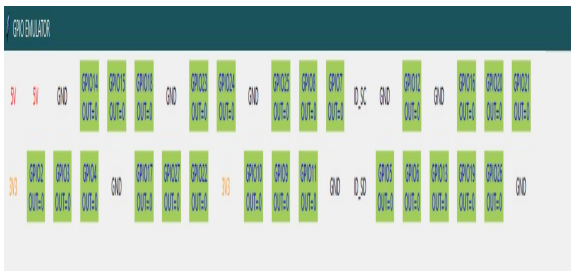

Figure 4: GPIO Emulator with Default values (Green Color)

The emulator is downloaded [18] from the python website and the last version was released in 2022, Feb [18]. Now, this IoT System should belong to the domain of distributed and decentralized applications (DApps) and the third version of Blockchain i.e., the Application's Phase [2015-2021) is responsible for this IoT system. The reason for making it a decentralized application is that the traditional architecture of IoT follows a centralized architecture which means a single point of failure will exist and a decentralized application is a part of Blockchain 3.0. This Applications Phase has a suite known as the Truffle suite. This suite has three major sub-categories, such as Ganache, Truffle and Drizzle [19]. Ganache helps in testing smart contracts. Truffle permits the client to make applications (decentralized) via Ethereum Virtual Machine (EVM). Drizzle can make the front end of applications (decentralized) informative. So, Blockchain 3.0. can eliminate the single point of failure as it has the decentralized attribute.

To secure the status of the pins of the emulator shown in Figure 4, and to operate it, a Web-App is required. This web app shown in figure 6 is made using a flask in python.

Here, in this case, the web app is running on the local host, port number 9000. For making a decentralized application, the author has made eight machines on 8 different ports ranging from 9000 to 9007. The reason for considering these large port numbers is that they are not reserved and can be used on a free-to-use basis. Port number 9000 shows the mechanism to connect all the isolated systems from 9001 to 9007.

Figure 5 shows the blockchain running on different systems ranging from 9001 to 9007 ports on the postman platform. It has four major components highlighted in bold and named from 1 to 4.

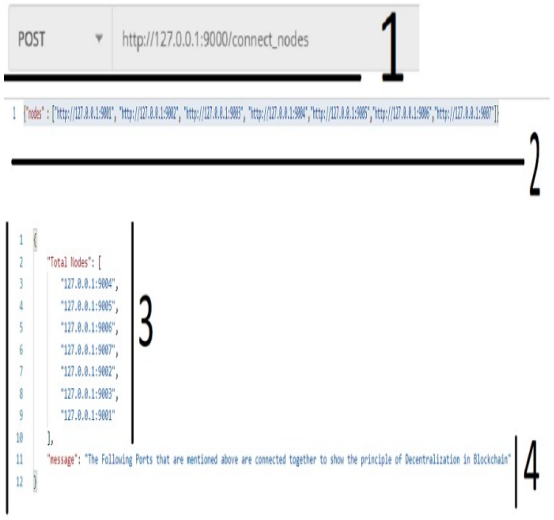

Figure 5: Blockchain running on different isolated systems.

Figure 5 has four points to answer. 1 denotes the address of the isolated system with the POST method. Number 2 denotes the nodes that are required to be coordinated and connected to be part of the blockchain. Number 3 illustrates the nodes that are connected in the Blockchain environment, ranging from 9001 to 9007. The last number i.e., Number 4 denotes the message that is showing the principle of decentralization in Blockchain. With this, the initial phase of IoT and Blockchain is completed.

The next phase considers the Web-Application of IoT concerning the GPIO Emulator Pins. Figure 6 shows the web application of the GPIO emulator running on port number 9001.

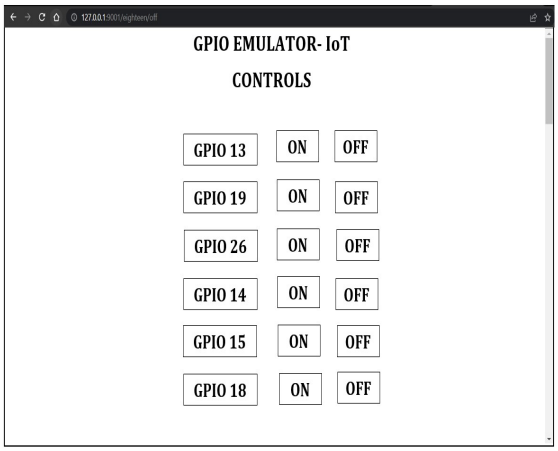

Figure 6: Web-Application running on Local Host

Figure 6 shows the web application of the GPIO emulator, which is showing PIN on the left side, then the two operations ON & OFF on the centre and right side, respectively. Now the overall objective is to secure the status of the pins. If the status is ON, then it should be OFF only when the correct private key is encountered. Now since this is SHA-256, the private key is 64 hexadecimal characters. Figure 7 shows the flow chart, illustrating the flow of sequence concerning the implementation of GPIO and Blockchain 3.0. features.

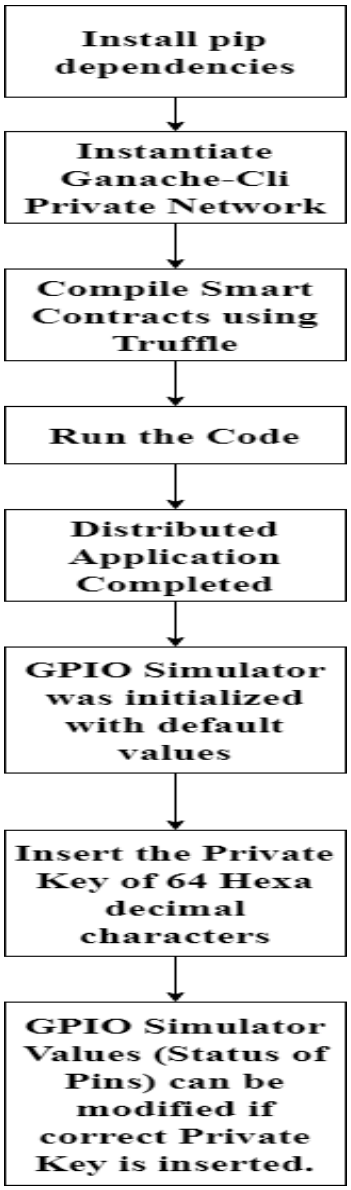

Figure 7: Flow Chart of Enhancing Security of GPIO Emulator Pins using Blockchain Technology

Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 7 shows the complete flowchart depicting the entire process. Now the next step is to instantiate the Ganache-Private Network. For installing and instantiating the network, the following codes highlighted as Eq. 1 and Eq. 2 can be used. The Ganache Private Network is highlighted in Figure 8.

npm install -g ganache-cli (1)

ganache-cli (2)

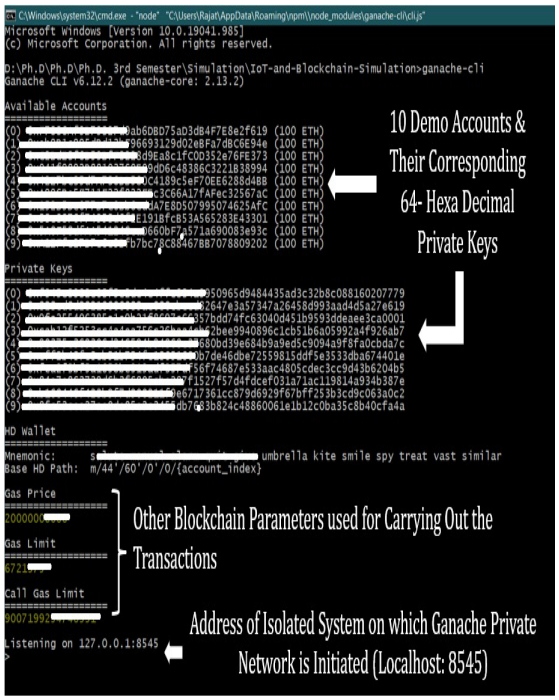

Figure 8: Ganache Private Network

Figure 8 illustrates the Ganache private network, which is the first step in integrating Blockchain with IoT. In the private network, there are 10 available accounts and their corresponding private keys. White strikethrough is done for the security and privacy aspects. The author does not wish to show the information about the available accounts and private keys. After this, the smart contracts will be compiled with truffle, which is written in solidity language whose extension is .sol [20][21]. The command for compiling the smart contracts is shown below:

truffle compile (3)

Now, as a button (ON or OFF) is clicked on the emulator (shown in Figure 6), a transaction will initiate that will ask for the required private key to enter. If any wrong private key of 64 hexadecimal characters is entered, then it will show the dialogue box, that tampering is attempted. And if the correct private key is encountered, then it will show the status of the pins of the GPIO emulator to be changed from green colour (shown in Figure 4) to orange. The changed coloured pins of the GPIO are shown below in Figure 9.

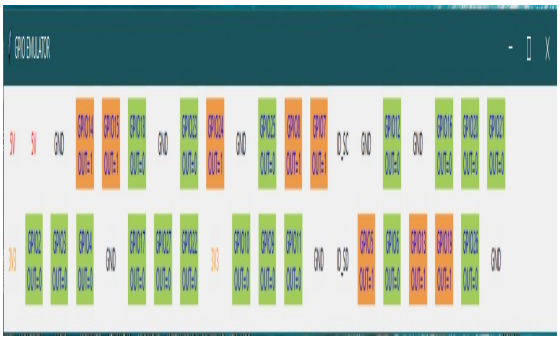

Figure 9: GPIO Emulator with Changed Values (Orange Colour)

Figure 9 shows the correct implementation of Blockchain in an IoT system that illustrates the status of pins to be protected by Blockchain. When the status of the pins was changed from green to orange, transactions used to happen, and the block is mined that involves the entities of Blockchain to participate. Table 2 shows the sample of Blockchain transactions for the IoT system when a button is clicked on the emulator and the blocks are mined.

In Table 2, the default time (second column in table 2) that is considered is of 10 seconds starting from 09:00:00 to 09:01:30 for the implementation of the emulator highlighted in figure 6. But it can be configured for any time gap for example 1 second, 2 seconds, 3 seconds and so on.

The first column of the table shows the sequence of blocks in the chain with the amount of gas it has consumed which is shown in column 3. Gas is a unit to calculate the effort (computational) to perform and complete operations on the network of blockchain. That blockchain can be ethereum or any other type of blockchain network.

The fourth column of the table highlights the contracts created that have 40 hexadecimal characters and the last column contains the data about the transactions that have 64 hexadecimal characters.

In the form of bits (normal) 40 hexadecimal characters will go to 160 bits (approx.) and 64 hexadecimal characters will go to a total of 256 bits (approximately).

Table 2: Sample of Blockchain Transactions for IoT Operations

Block Number	Creation Timestamp (Mining)	Gas Usage	Contract Created (40-Hexa Decimal Characters)	Transaction (64-Hexa Decimal Characters)
1	09:00:00	158049	0x90777275c99edd60fe59261f6c1e9c6f8faf79xx	0x132decf54199086c94c1d71a19d67c9d57c7faf45ca17c9e2e9c24a8417661xx
2	09:00:10	42569		0xc52b6c531994bc003b727cd793547475bffed1899b0d9ed5b1372f6864c758xx
3	09:00:20	42569		0xfeb274f301de675c58cef231377e77c60447b00f1cf91b35233e1b4f5d463dxx
4	09:00:30	23369		0x66991a4009861665d271a393cf1737c125b4963b867a811bb3f9ca59e2cab5xx
5	09:00:40	23369		0x576D5A7134743777217A25432A46294A404E635266556A586E327235753878xx
6	09:00:50	42569		0x655368566D597133743677397A244326462948404D635166546A576E5A7234xx
7	09:01:00	42569		0x4B6150645367566B597033733676397924242264529482B4D6251655468576Dxx
8	09:01:10	42569		0x2A462D4A614E645267556B58703273357638792F423F4528472B4B62506553xx
9	09:01:20	42569		0x7A25432646294A404E635266556A586E3272357538782F413F4428472D4B61xx
10	09:01:30	42569		0x3677397A244326452948404D635166546A576E5A72347537782141254 42A47xx

Table 2 shows the Blockchain transactions for IoT systems. Here, a sample of 10 IoT operations is highlighted that is happening at a time gap of 10 seconds and is customizable. Here, 10 blocks are mined that is having their Transaction ID (64 hexadecimal characters) and a Contract (40 hexadecimal characters). The Last two digits of the Contract ID and Transaction ID are kept secret for security and privacy aspects. This was the last phase of the implementation (general).

5. ANALYSIS OF INTEGRATED IOT-BLOCKCHAIN SYSTEM (IOT-B)

This modified IoT system ran in 6 phases. Each phase was operating in different timeslots, the first phase considered 200 transactions, and each operation was happening at 10 seconds. Phase 2 considered 1000 transactions in which every Blockchain transaction for IoT happened at 3 seconds, Phase 3 considered 2000 transactions, considering every transaction at 4 seconds, Phase 4 considered 5000 transactions considering every operation of IoT at 5 seconds, and Phase 5 considered 8727 transactions each working at 6 seconds, The last phase i.e., Phase 6, considered 11075 transactions happening at 6 seconds. The detailed analysis of The IoT operations with Blockchain security (phase-wise) is highlighted in Table 3.

Table 3 contains the number of transactions, time for IoT operations, total time taken, blocks that failed during mining and lastly the machine on status.

Table 3. Analysis of Blockchain Transactions on IoT Devices

Number of Transactions	Time for IoT Operation	Total Time Taken	Blocks Failed during Mining	Machine on Status
200	10 sec	2000 sec	None	0.56 Hrs
1000	3 sec	3000 sec	1	0.833 Hrs
2000	4 sec	8000 sec	1	2.22 Hrs
5000	5 sec	25000 sec	1	6.9 Hrs
8727	6 sec	52362 sec	None	14.545 Hrs
11075	6 sec	66450 sec	None	18.458 Hrs

6. RESULTS & DISCUSSION

From the above textual matter, it should be observed that Blockchain is an optimal solution for enhancing the security and privacy of IoT systems. Table 2 illustrates the sample of 10 Blockchain transactions in IoT systems. This was in the first phase. When the machine ran in 6 phases then there was a total of 28002 transactions out of which 27999 transactions were properly working that was providing the entire efficiency of 99.98%. The phase-wise details were discussed in Table 3. The graphical illustration of Table 3 is shown below in figures 10 & 11.

The Major findings obtained are shown below:

1. Total number of transactions: 28002

2. Total time taken in performing 28002 transactions: 158771.34 Seconds [For simplified analysis, considered 1 operation = 5.67]

3. Total Blocks Formed= 27999

4. Any Block Failed= 3

5. Efficiency= 99.98%

6. Machine on Status= 43.511 Hrs

With the implementation of blockchain transactions for IoT systems, a few more observations were carried out, which are shown in Table 4.

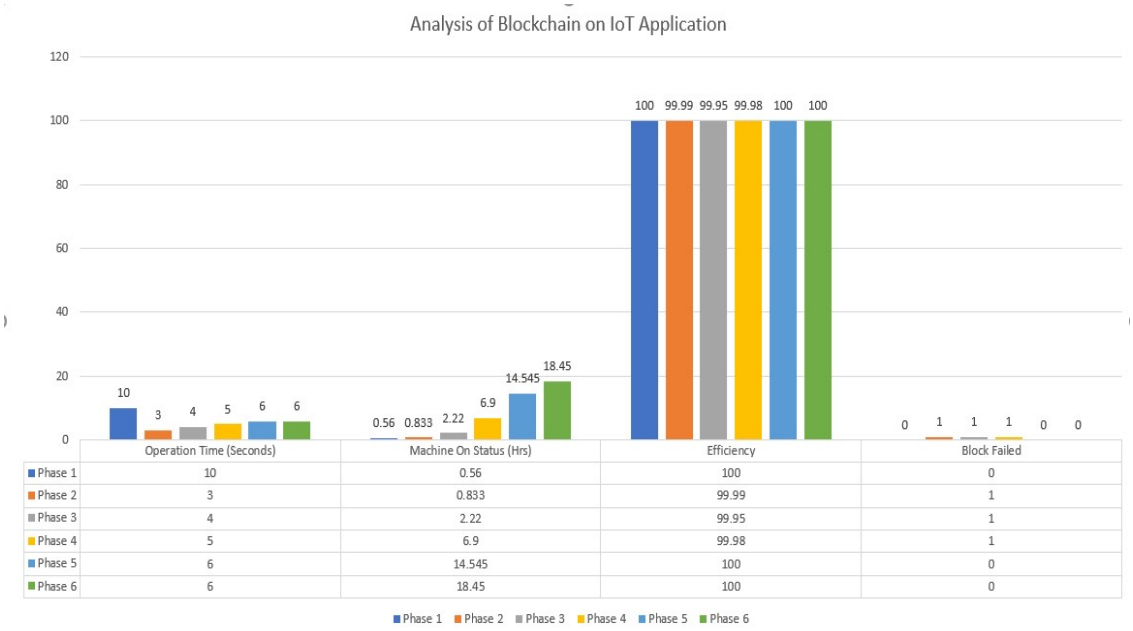

Figure 10: Analysis of Blockchain in IoT Systems

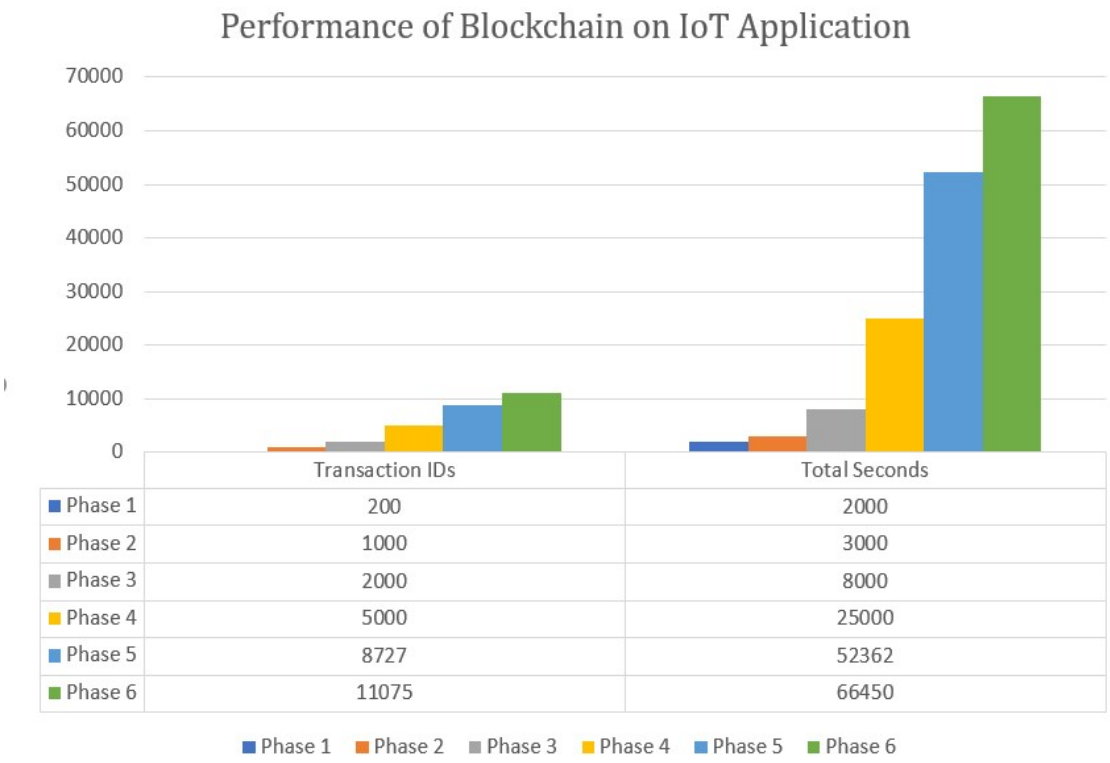

Figure 11: Analysis of the Time Taken by Blockchain in IoT for Verification & Validation

Table 4. Additional Findings of the Implementation

Issue of IoT	Blockchain Illustration & Parameter Justified
Tampering/Fabricated Data by entering a different private key	Secured in blockchain [Error displayed when tampering was attempted] [Pin colour will not change from green to orange] & Yes [Immutability]
Centralization	Secured in blockchain [The same machine could run on different isolated systems (Here, from 9001….9007)] & Yes [Decentralization]
Security	Secured in blockchain [The status of the pins remains the same]
Data Breach	Data Breach has minimized in Blockchain [Error displayed (via developer mode) when the data breach was attempted] [Pin Color will not change from green to orange] & Yes [Immutability]
Data Inconsistency	Blockchain provides consistent & consensus mechanisms and thus, data inconsistency is minimized in the blockchain. & Yes [CIA triad, Immutability]

7. CONCLUSION AND FUTURE SCOPE

The technological ecosystem has witnessed the contribution of IoT in developing the lives of human beings. The overall development of IoT started in 1832. Since then, IoT has never disappointed. However, with the positive side, the negative side has also developed that corresponds to cyber-attacks. With the evolved cyberattacks, IoT cannot depend on the traditional methods of security and requires SMART solutions such as Blockchain. The introduction of IoT and Blockchain with its structure is shown here. The integration of Blockchain & IoT with a measure to increase the security spectrum of IoT is depicted here. The analysis of Blockchain transactions (6

phases) when an operation is performed in an IoT device is also shown in this paper. The overall efficiency of the system was noted to be 99.98% when 28002 transactions were performed out of which 27999 transactions successfully took place. The 3 blocks failed due to network fluctuation. The diverse IoT issues and their Blockchain solutions are depicted here. This implementation is an approach towards an efficient IoT system by integrating blockchain into it. The characteristics provided by blockchain and the efficient results that were obtained from the integrated implementation of IoT & Blockchain allow the author to conclude. This examination is significant because this allows any IoT device to be blockchain secured. With Blockchain traditional security issues and concerns can be eliminated and future research could be done to optimize it and launch this on a commercial aspect. The implementation of a lightweight blockchain is also a future scope.

REFERENCES:

[1] Bera A 2021. (80) Insightful Internet of things statistics (Infographic). White Paper 2021. Retrieved from https://safeatlast.co/blog/iot-statistics/#gref

[2] Data volume of internet of things (IoT) connections worldwide in 2019 and 2025(in zettabytes). Retrieved from https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size/#:~:text=Data%20volume%20of%20IoT%20connected%20devices%20worldwide%202019%20and%202025&text=The%20statistic%20shows%20the%20overall,reach%2079.4%20zettabytes%20(ZBs)

[3] Manyika J, Chui M, Bisson P, Woetzel J, Dobbs R, Bughin J, Aharon D. Unlocking the Potential of the Internet of Things. McKinsey Global Institute. 2015 Jun 19;1.

[4] Blakely GR, Chaum D, editors. Advances in Cryptology: Proceedings of Crypto'84. Springer; 2003 May 16.

[5] Chaum D, Evertse JH. Cryptanalysis of DES with a reduced number of rounds. InConference on the Theory and Application of Cryptographic Techniques 1986 (pp. 192-211). Springer, Berlin, Heidelberg.

[6] Narayanan A, Clark J. Bitcoin's academic pedigree. Communications of the ACM. 2017 Nov 27;60(12):36-45.

[7] Verma R, Dhanda N, Nagar V. Security Concerns in IoT Systems and Its Blockchain Solutions. InCyber Intelligence and Information Retrieval 2022 (pp. 485-495). Springer, Singapore.

[8] Dhanda N, Garg A. Revolutionizing the Stock Market With Blockchain. InRevolutionary Applications of Blockchain-Enabled Privacy and Access Control 2021 (pp. 119-133). IGI Global.

[9] Sharda Tiwari D, Dhanda N, Dev H, Pandey D. A Hybrid Framework based on IoT and Blockchain Network to Store the Patient Health Data. Mathematical Statistician and Engineering Applications. 2022 Apr 25;71(2):330-9.

[10] Bodkhe U, Tanwar S, Parekh K, Khanpara P, Tyagi S, Kumar N, Alazab M. Blockchain for industry 4.0: A comprehensive review. IEEE Access. 2020 Apr 17;8:79764-800.

[11] Verma R, Dhanda N, Nagar V. Enhancing Security with In-Depth Analysis of Brute-Force Attack on Secure Hashing Algorithms. InProceedings of Trends in Electronics and Health Informatics 2022 (pp. 513-522). Springer, Singapore.

[12] Mahto D, Yadav DK. RSA and ECC: a comparative analysis. International journal of applied engineering research. 2017 Oct;12(19):9053-61.

[13] Bhadoria RS, Arora Y, Gautam K. Blockchain hands on for developing genesis block. InAdvanced applications of blockchain technology 2020 (pp. 269-278). Springer, Singapore.

[14] Busygin A, Konoplev A, Kalinin M, Zegzhda D. Floating genesis block enhancement for blockchain based routing between connected vehicles and software-defined VANET security services. InProceedings of the 11th International Conference on Security of Information and Networks 2018 Sep 10 (pp. 1-2).

[15] Rajat Verma, Dr. Namrata Dhanda, Dr. Vishal Nagar. Addressing the Issues & Challenges of Internet of Things Using Blockchain Technology. IJAST [Internet]. 2020May30, 29(05):10074 -1082.

[16] Göbel J, Keeler HP, Krzesinski AE, Taylor PG. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Performance Evaluation. 2016 Oct 1;104:23-41.

[17] Vokerla RR, Shanmugam B, Azam S, Karim A, De Boer F, Jonkman M, Faisal F. An overview of blockchain applications and attacks. In2019 international conference on

vision towards emerging trends in communication and networking (ViTECoN) 2019 Mar 30 (pp. 1-6). IEEE.

[18] Retrieved from https://pypi.org/project/RPi.GPIO/

[19] Shawn LW, Murali Mohan P, Loh Kok Keong P, Balachandran V. Blockchain-based Proof of Existence (PoE) Framework using Ethereum Smart Contracts. InProceedings of the Eleventh ACM Conference on Data and Application Security and Privacy 2021 Apr 26 (pp. 301-303).

[20] Verma R, Dhanda N, Nagar V. Application of Truffle Suite in a Blockchain Environment. InProceedings of Third International Conference on Computing, Communications, and Cyber-Security 2023 (pp. 693-702). Springer, Singapore.

[21] Verma R, Dhanda N, Nagar V. Towards a Secured IoT Communication: A Blockchain Implementation Through APIs. InProceedings of Third International Conference on Computing, Communications, and Cyber-Security 2023 (pp. 681-692). Springer, Singapore.

[22] Verma R, Dhanda N, Nagar V. Enhancing & Optimizing Security of IoT Systems using Different Components of Industry 4.0. International Journal of Engineering Trends and Technology, vol. 70, no. 7, pp. 147-157, 2022. Crossref, https://doi.org/10.14445/22315381/IJETT-V70I7P216

[23] Verma R, Nagar V, Mahapatra S. Introduction to supervised learning. Data Analytics in Bioinformatics: A Machine Learning Perspective. 2021 Feb 1:1-34.

[24] Verma, R. ., Dhanda, N. ., & Nagar, V. . (2023). Analysing the Security Aspects of IoT using Blockchain and Cryptographic Algorithms. International Journal on Recent and Innovation Trends in Computing and Communication, 11(1s), 13–22. https://doi.org/10.17762/ijritcc.v11i1s.5990