Internet of Things Based Blockchain Technology for Gas Station

Samaher A.Yousiff[1], Raad A. Muhajjar[1]
[1]Department t of Computer Science, College of CSIT, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received November 9, 2022
Revised November 29, 2022
Accepted December 3, 2022

Keywords:

Internet of Things
Blockchain
ESP32
Consensus algorithms

ABSTRACT

The protection of information sent over the Internet has become very important because of the possibility of being hacked and leaking important or confidential information. Therefore, many studies have been conducted in the field of information security and many ways have emerged to protect the information, but blockchain technology is the most prominent technology currently due to its high potential in maintaining the study was conducted on the most important blockchain algorithms, namely the Proof of Authority (POA) algorithm and the Proof of Work (POW) algorithm. The study aimed now at the best and most reliable algorithm to protect the parameters sent via the Internet of Things technology. The POA algorithm is the first candidate to win the advantage in theory, but After applying the study and verifying the actual results, it was confirmed that the POA algorithm is superior and highly capable of protecting information, in addition to speed in executing calculations, less memory consumption, less execution time, fewer Nonce to obtain the correct hash, and many other advantages, and the obtained result was the PoA algorithm is significantly faster with a difference of 46/s to create the blockchain, and it also requires less memory than the PoW algorithm, with a difference of 1024KB.

Blockchain (B.C) algorithms will be applied to the Internet of Things (IoT) technology to obtain IoT technology that is completely encrypted from hacking and information cannot be tampered with. The transmission within the network, whether it is a local or global network. The new technology will be applied to a gas station information transmission system to generate electric power. The aim of this paper are to make the smart grid of the gas station more secure and private.

Corresponding Author:

Samaher Ahmed Yousiff
Department of Computer Science, College of CSIT, University of Basrah, Basrah, Iraq
Email: samaheraltumma@gmail.com.

1. INTRODUCTION

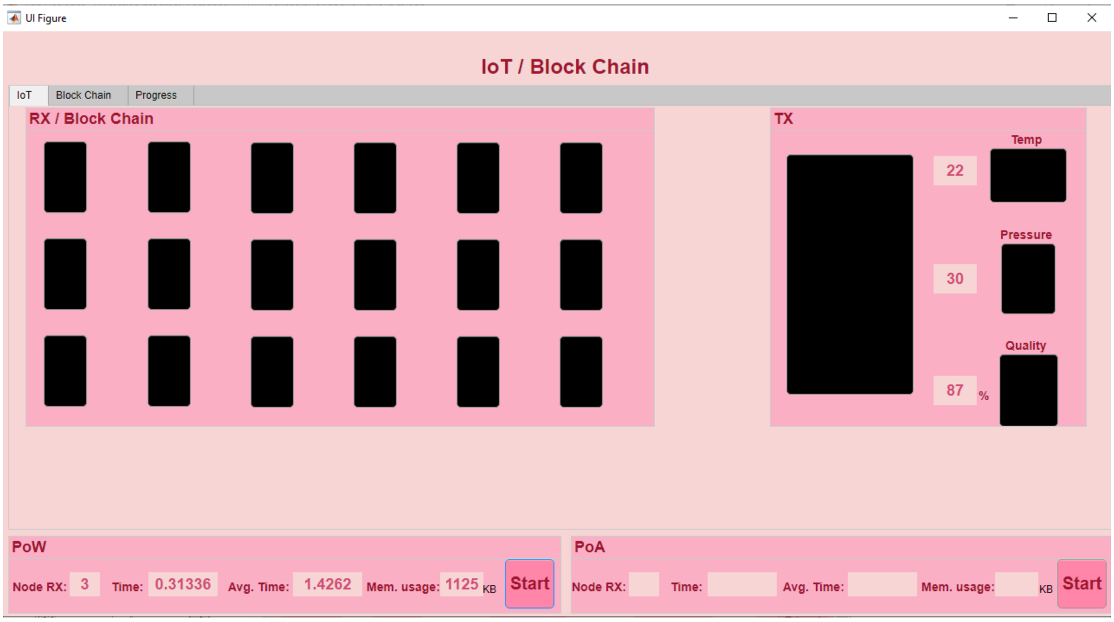
Effective network management is critical because IoT devices are carried sensitive data, and the amount of data created by IoT devices are so huge, These systems are regarded as an important part of ubiquitous computing[1],[2],[3], and the data is stored using cloud storage technologies. Large amounts of data can be quickly processed in the cloud[4],[5]. The Internet of Things and wireless networks are used in various control systems, home automation, environmental monitoring, and other applications[6]. The literature offers a wide range of solutions to IoT network issues. IoT networks have various difficulties, including efficient data-sharing, permission management, security, and access control. These solutions are created utilizing established approaches, such as Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), and others. On the other hand, traditional systems have flaws, including centralization, unreliability, and unauthorized data access[7],[8],[9]. The blockchain or the B.C is the largest distributor and open digital record that allows the transfer of ownership from one party to another at the same time without the need for an intermediary while achieving a high degree of security for the transfer process in the face of fraud and manipulation attempts, and all individuals around the world participate in this record In this technology[10]. The blockchain system was used for the first time in 2008 as the main platform for the bitcoin currency, which derived its strength thanks to this technology, and many people confuse bitcoin and the blockchain and consider it one block even though this is not true, the blockchain is the backbone of Bitcoin, which distinguishes it from other virtual currencies [11],[12],[13] It is worth noting that any process that takes place within the blockchain is stored in a record that does not tamper able or modified. The blockchain consists of nine basic components, namely: 1- The nodes that It is represented the users, 2- The transaction, which is the smallest part of the blockchain, such as records, information, etc., 3- The block is the unit of data building used to store a set of transactions that are distributed to nodes, 4- The chain, which represents a chain of blocks, 5- The miners, which are nodes that operate on To verify the blocks before adding and distributing them to the nodes, 6- The protocol that represents the rules and data for the implementation of the blockchain, 7- The entry process, which is the sub-process that takes place within a single block, 8- The hash represents the distinctive DNA of the block and the digital signature of the block may be forgotten, 9- And finally the time imprint, which is the time when the operation was performed within the chain[14].

2. PREVIOUS WORKS:

B.C technology provides a secure exchange of money, shares, or rights. It acts as an electronic record for processing transactions and recording them, allowing all parties to track information through a secure network that does not require third-party verification (Nakamoto, 2008)[15],[16], B.C technology contributes to rationalizing the consumption of electrical energy by connecting the electricity network with microcontrollers that can monitor the consumption of electric current, thus reducing consumption and facilitating the process of withdrawing the proceeds of electricity use. In addition, this technology helps reduce the price of electrical units[17], The use of IoT technology enhanced by B.C technology in smart cities that depend on IoT in its work to maintain financial transactions and security of users' information, in addition to protecting medical information for patients and hospitals[18],[16]. Develop smart shopping systems by adding layers of fuzzy logic and B.C technology to obtain the best possible results in the online shopping process. Used Blockchain Technology to develop a multi-layer method for IoT Network Security[15]. For applications in smart cities, they presented a hybrid network architecture based on blockchain. To enhance efficiency, two core networks and two edge networks make up this hybrid system [19]. Designed the Lightweight Integrated Blockchain (ELIB) concept in this study to fulfill the needs of the Internet of Things [20]. Discuss that security, comparability, energy usage, and device heterogeneity are all long-standing issues in the IoT. Security and energy issues are crucial when transmitting data over IoT and edge networks since networked devices have limited energy and computation (such as processing and storage) capabilities[21]. in this study, They proposed a Blockchain-based Service-Centric Networking (SCN) solution for secure IoT data[22]. The proposed concept combines localization via RSSI-based triangulation and proprietary blockchain technology[23]. A secure industrial system based on Blockchain has been built to access data to enhance cloud performance[24]. Blockchain is used with fuzzy logic in healthcare in order to provide solutions to problems faced by blockchain in healthcare applications.[25].

3. SUGGEST METHOD:

A B.C network simulation will be implemented using Matlab language. A computer will be used that contains a Core5 M520 processor - 2.4GHz, with 6GB RAM, with a 2GB Intel graphics processor, in addition to the Matlab R2020a environment. As for the devices that will be simulated. In MATLAB are the ESP32 microcontroller and a group of sensors that will be connected to the microcontroller to monitor the initial gas state before entering the power station. The sensors used are an MQ2 Gas Sensor, Pressure Sensor, and Quality Sensor. It is worth noting that the MATLAB language does not support the ESP32 microcontroller. In the simulation, therefore, the App Designer program will be used to design a graphical interface that contains sensors and controllers, and it will be divided into two parts, the first part is the transmission part represented by an ESP32 controller and the previously mentioned sensors, and the second part is a B.C network consisting of 18 nodes, all of which are ESP32.



Temp 22

Pressure 30

Quality 87 %

PoW

Node RX: 3 Time: 0.31336 Avg. Time: 1.4262 Mem. usage: 1125 KB

PoA

Node RX: Time: Avg. Time: Mem. usage: KB

Figure 1: Main User Interface

The previous figure shows the user interface through which one of the two algorithms can be dealt with and the results obtained from the implemented algorithm appear. In the right part, there is the TX section, which contains ESSP32 and three sensors connected to it, and in the left part, we notice that there are 18, all of which are ESP32 which represents the B.C network. Both algorithms work in the same graphical interface where you can select the algorithm to be executed by pressing Start in one of the options in the bottom bar.
In the following figure, the full workflow for the project.

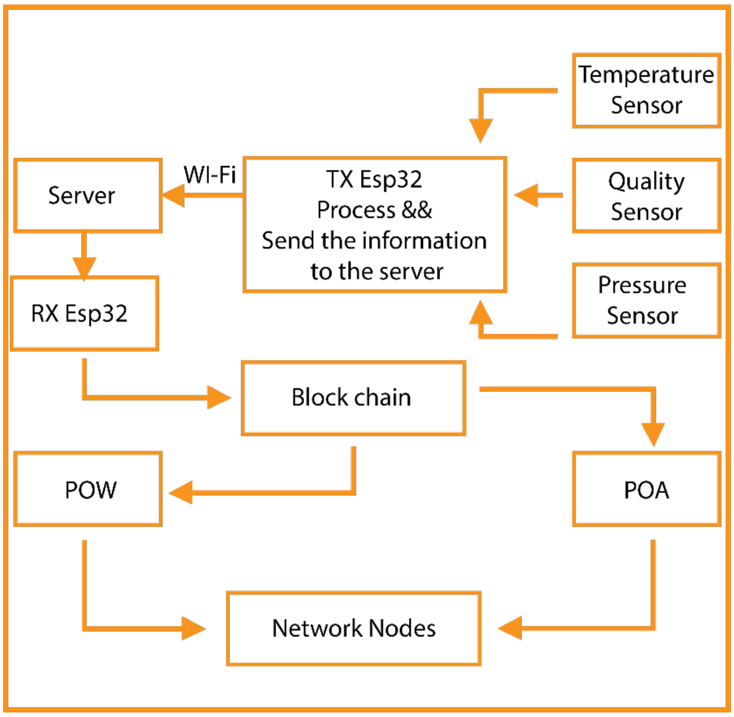


Figure 2:working algorithm

3.1 TX USING ESP32:

We also mentioned that the system consists of two parts, the first is the transmitter and the second is the receiving device connected to B.C technology, and here TX (ESP32) is connected to three sensors used in the gas station: Temperature Sensor, Quality Sensor, and Pressure Sensor. These three sensors will be programmed to give random values within a permissible range. It is not allowed to obtain values when checking them in the verification process in the B.C algorithm whose results are acceptable and the block is added, and again the results of the verification process are not acceptable and the block addition is canceled.

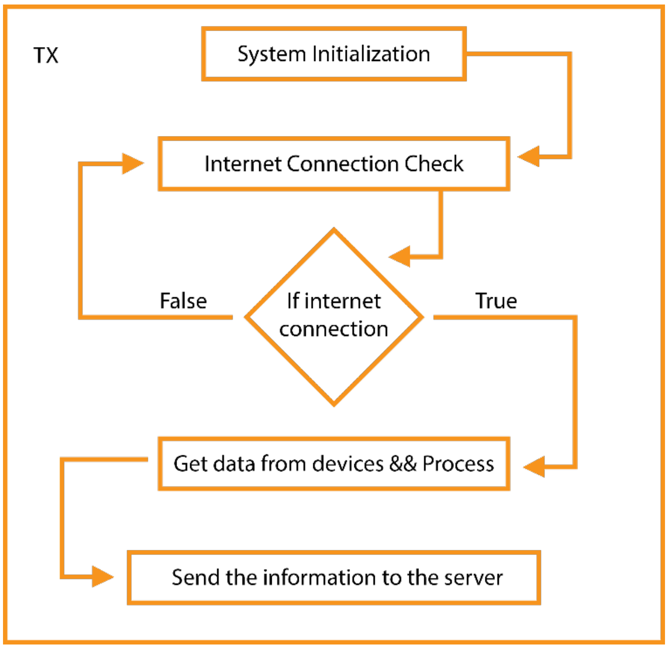

TX
System Initialization
Internet Connection Check
False
If internet connection
True
Get data from devices && Process
Send the information to the server

Figure 3: transmitter algorithm

3.2. SERVER

After obtaining the results of the sensors in the TX part, the information is sent to the server for storage, where the server acts as an intermediary between the transmitter and receiver to achieve the principle of the Internet of Things. In this case, the server will be a function that simulates the server's work in storing information, and the receiving device can access the information of this function and deal with it.

3.3. RX USING ESP32:

In this part, the information is received from the server and sent to one of the B.C algorithms, either POA or POW, according to the algorithm that was called from the main user interface. After the algorithm work is completed and the block is added, the information is shared with the network nodes.

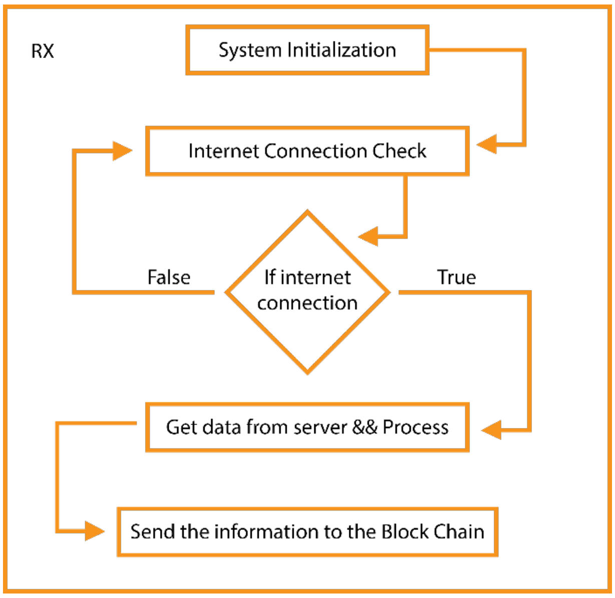

RX
System Initialization
Internet Connection Check
False
If internet connection
True
Get data from server && Process
Send the information to the Block Chain

Figure 4: Receiver algorithm

After the information reaches the receiving part, the information is sent to one of the B.C algorithms that will verify the received information based on the previous information stored in the last block and the difference between it and the new information. If the difference is more than the normal rate of change of readings in the same period, the block is canceled but if the difference is within the normal rate of change of readings, a new block is added and the information is shared with network nodes.

3.4. POW ALGORITHM

The POW algorithm works by fetching the information to be shared with the network, where this process takes place after the competition between the network nodes called mining clauses, and the competition is to find the correct hash and the fastest miner finds this hash, receives the information and verifies it and then adds the new block if the information is the received is correct. Figure 5 shown the PoW's work.

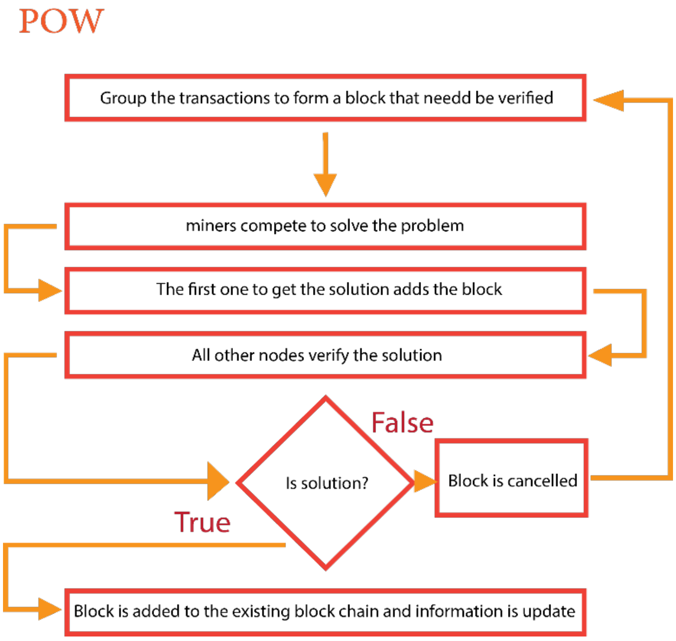

POW
Group the transactions to form a block that needd be verified
miners compete to solve the problem
The first one to get the solution adds the block
All other nodes verify the solution
False
Is solution?
Block is cancelled
True
Block is added to the existing block chain and information is update

Figure 5: POW. Algorithm

3.5. POA ALGORITHM

This algorithm works in a slightly different way as it specifies a certain number of nodes that can add a block and they are called high-powered nodes. We want a new one again randomly, and this process is very fast compared to the previous algorithm. After that, the received information is verified in a similar way to the verification process in the previous algorithm, and the block is added to solve the fact that the new information is correct, otherwise, the block is canceled. Figure 6 shown the PoA's work

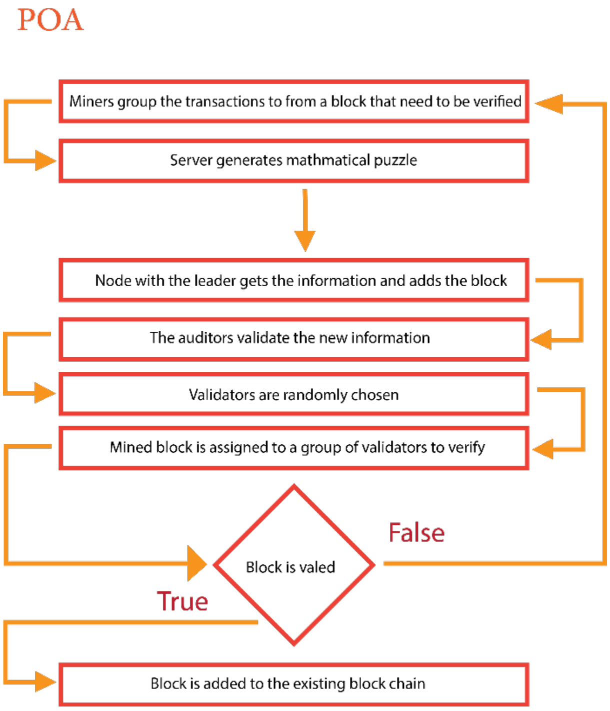
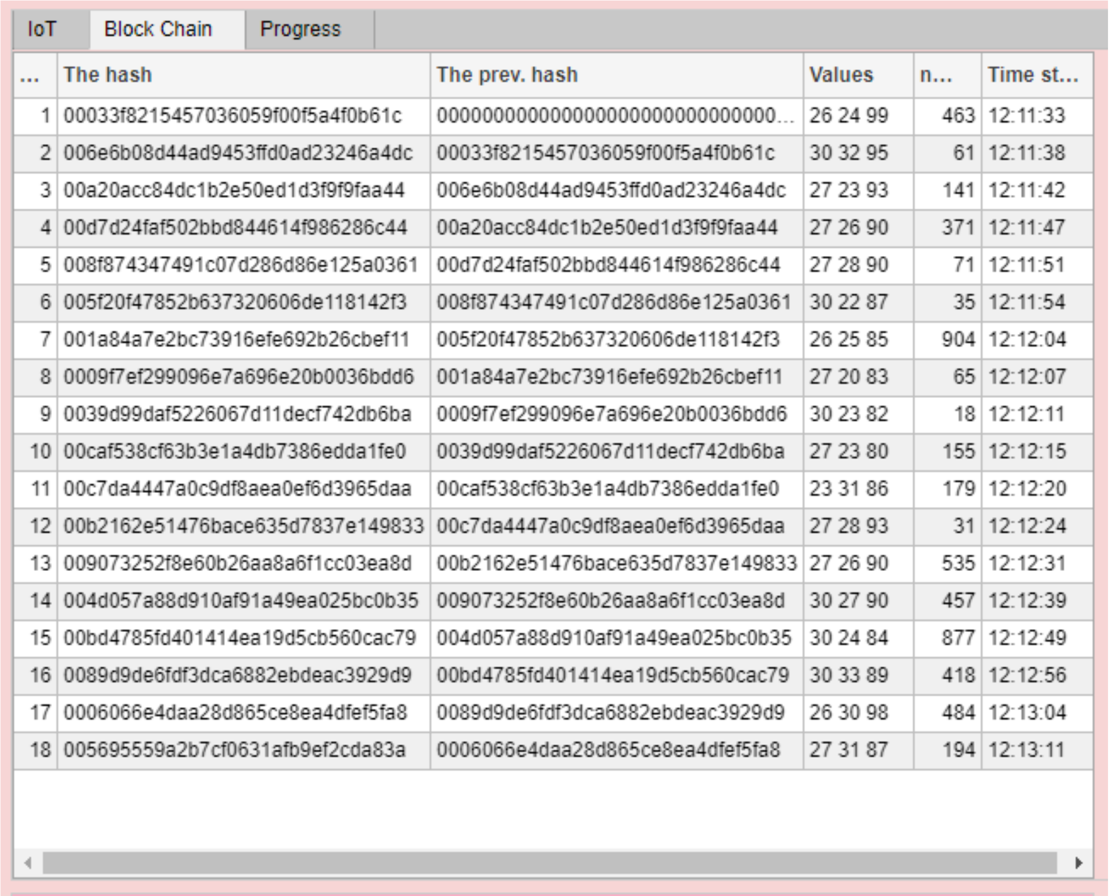

POA
Miners group the transactions to from a block that need to be verified
Server generates mathmatical puzzle
Node with the leader gets the information and adds the block
The auditors validate the new information
Validators are randomly chosen
Mined block is assigned to a group of validators to verify
Block is valed
False
True
Block is added to the existing block chain

Figure 6: POA. algorithm

4. RESULTS AND DISCUSSION

The processes that occur in the blockchain are depicted in the following figure, which are:

1- The hash.
2- The prev. Hash.
3- The values.
4- The nonce.
5- The time Stamp.

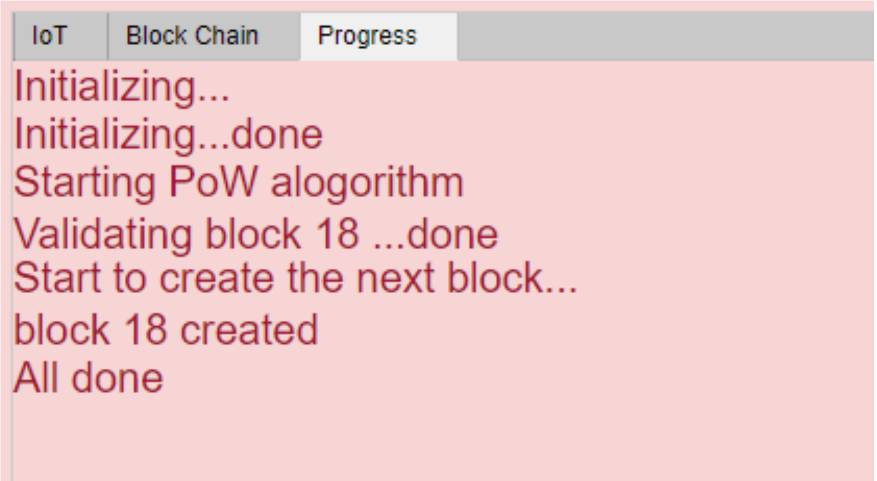


...	The hash	The prev. hash	Values	n...	Time st...
1	00033f8215457036059f00f5a4f0b61c	0000000000000000000000000000...	26 24 99	463	12:11:33
2	006e6b08d44ad9453ffd0ad23246a4dc	00033f8215457036059f00f5a4f0b61c	30 32 95	61	12:11:38
3	00a20acc84dc1b2e50ed1d3f9f9faa44	006e6b08d44ad9453ffd0ad23246a4dc	27 23 93	141	12:11:42
4	00d7d24faf502bbd844614f986286c44	00a20acc84dc1b2e50ed1d3f9f9faa44	27 26 90	371	12:11:47
5	008f874347491c07d286d86e125a0361	00d7d24faf502bbd844614f986286c44	27 28 90	71	12:11:51
6	005f20f47852b637320606de118142f3	008f874347491c07d286d86e125a0361	30 22 87	35	12:11:54
7	001a84a7e2bc73916efe692b26cbef11	005f20f47852b637320606de118142f3	26 25 85	904	12:12:04
8	0009f7ef299096e7a696e20b0036bdd6	001a84a7e2bc73916efe692b26cbef11	27 20 83	65	12:12:07
9	0039d99daf5226067d11decf742db6ba	0009f7ef299096e7a696e20b0036bdd6	30 23 82	18	12:12:11
10	00caf538cf63b3e1a4db7386edda1fe0	0039d99daf5226067d11decf742db6ba	27 23 80	155	12:12:15
11	00c7da4447a0c9df8aea0ef6d3965daa	00caf538cf63b3e1a4db7386edda1fe0	23 31 86	179	12:12:20
12	00b2162e51476bace635d7837e149833	00c7da4447a0c9df8aea0ef6d3965daa	27 28 93	31	12:12:24
13	009073252f8e60b26aa8a6f1cc03ea8d	00b2162e51476bace635d7837e149833	27 26 90	535	12:12:31
14	004d057a88d910af91a49ea025bc0b35	009073252f8e60b26aa8a6f1cc03ea8d	30 27 90	457	12:12:39
15	00bd4785fd401414ea19d5cb560cac79	004d057a88d910af91a49ea025bc0b35	30 24 84	877	12:12:49
16	0089d9de6fdf3dca6882ebdeac3929d9	00bd4785fd401414ea19d5cb560cac79	30 33 89	418	12:12:56
17	0006066e4daa28d865ce8ea4dfef5fa8	0089d9de6fdf3dca6882ebdeac3929d9	26 30 98	484	12:13:04
18	005695559a2b7cf0631afb9ef2cda83a	0006066e4daa28d865ce8ea4dfef5fa8	27 31 87	194	12:13:11

Figure 7: Blockchain implementation

From the previous figure, we find that Prev. Hash is only zeros because there is no previous hash
The value is the obtained information and represents temperature, pressure, and purity.
The nonce is the number of iterations or attempts that lead to the correct hash.
Time Stump The actual time of adding the new block is considered one of the most important parts of B.C because it calculates the time difference between the previous block and the new block and ensures the correctness of the information through the ratio of the change in the readings to the time difference.

The next interface displays the information that is taking place in the program at present. When the program is run, the initializing process is performed, and after the completion of the initializing process, Initializing is displayed. After that, one of the algorithms starts to work. Either POW or POA displays the name of the algorithm in progress, and as in the previous figure, an algorithm was implemented POW, then the new block information is verified. If the verification result is correct, Validating Block Done is displayed and the block to be added is displayed. If the information is not verified, Block Canceled is displayed and the work is done again. If the block is added, Block Created is displayed in addition to a number. The block that has been added and then the operations are finished.

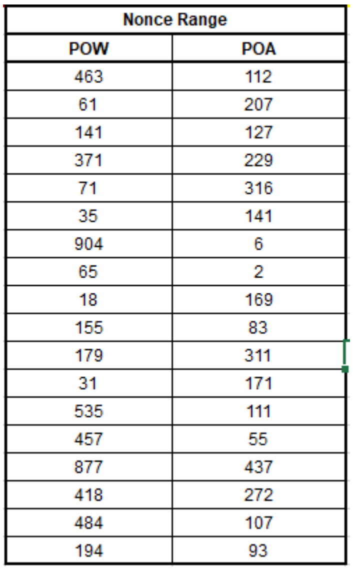


Initializing...
Initializing...done
Starting PoW alogorithm
Validating block 18 ...done
Start to create the next block...
block 18 created
All done

Figure 8:Blockchain progress

When the two algorithms are executed, the following results of Nonce (the number of iterations to get the correct solution), the time that taken to add one block, the total time of (POW vs POA) work, and (POW vs POA) memory used are obtained, as shown in table 1, figure 9, table 2, figure 10, table 3, figure11, table4, and figure12.

Table 1: Nonce Range



Nonce Range	
POW	POA
463	112
61	207
141	127
371	229
71	316
35	141
904	6
65	2
18	169
155	83
179	311
31	171
535	111
457	55
877	437
418	272
484	107
194	93

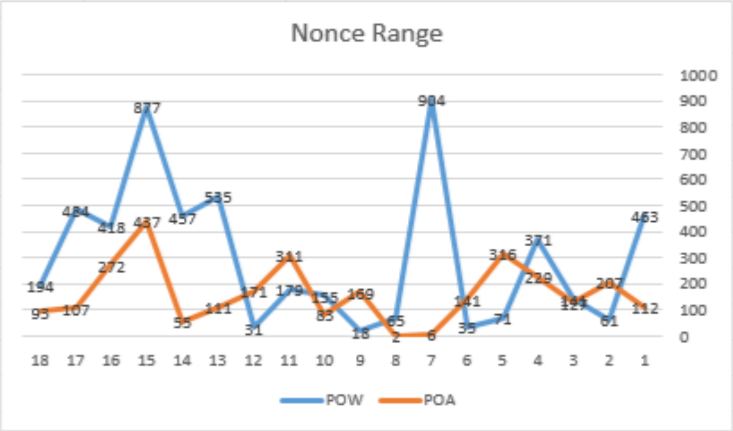


Figure 9: Nonce Range

Table 2: (POW vs POA) time

POW Time	POA Time
3.8	0.12
1.2	0.19
0.5	0.2
0.2	0.06
1.5	0.4
0.2	0.1
1.48	0.4
2.55	0.2
2.8	0.04
1.9	0.5
1.5	0.3
1.6	0.1
0.6	0.3
5.45	0.01
4.3	0.08
0.6	0.16
0.04	0.06
0.18	0.04

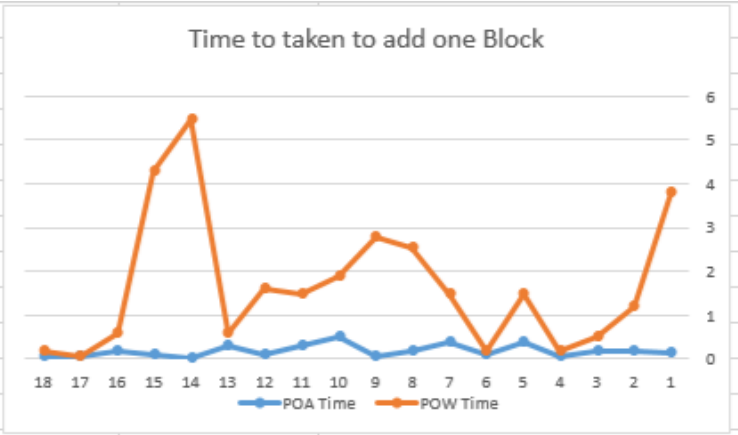


Figure 10 :(POW vs POA) time

Table 3:(POW vs POA) Total time

Total Time	
POW Total Time	POA Total Time
30.4	3.26
31	3.2
30	3.6
32	3
31.5	3.1
31.8	3
30.5	3.3
29.9	2.9
33	3
32.85	2.8
33.1	2.9
35	3.1
34.3	3.15
34.54	2.95
30.7	2.98

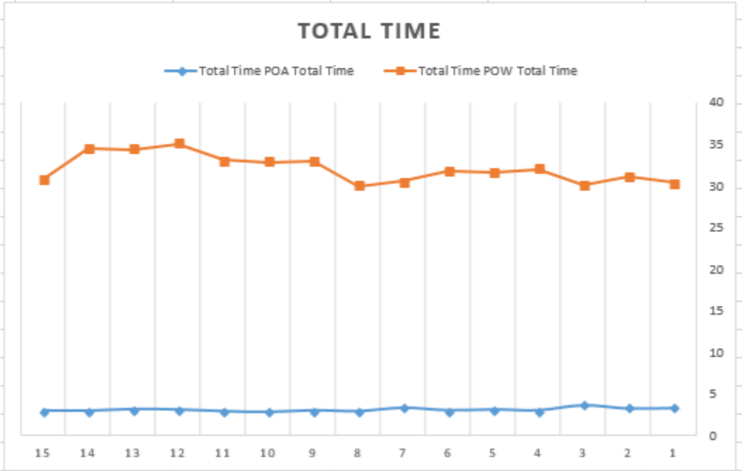
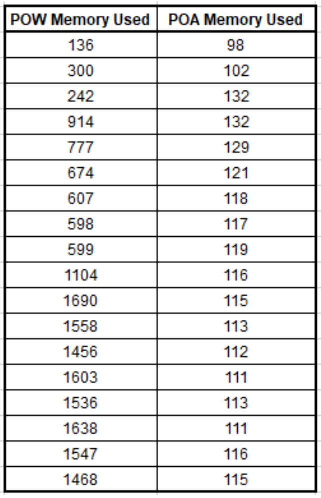


Figure 11 :(POW vs POA) Total time

Table 4:(POW vs POA)
Memory used



POW Memory Used	POA Memory Used
136	98
300	102
242	132
914	132
777	129
674	121
607	118
598	117
599	119
1104	116
1690	115
1558	113
1456	112
1603	111
1536	113
1638	111
1547	116
1468	115

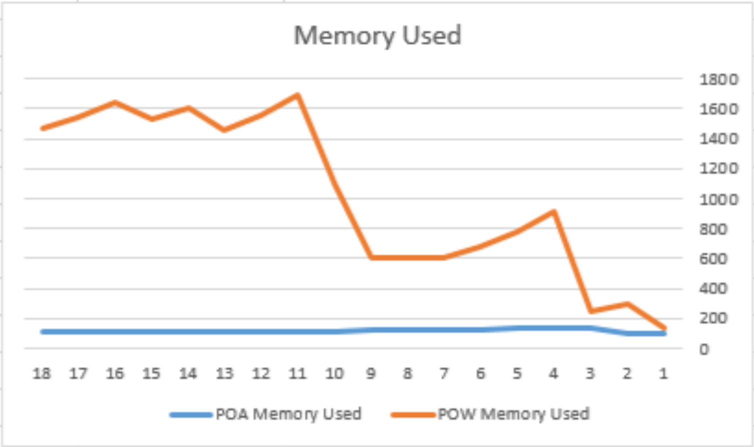


Figure 12 :(POW vs POA) Mmory used

5. CONCLUSIONS

This suggested design makes use of private blockchain technology since it provides anonymity and security and may be used with IoT to increase efficiency, making it appropriate for enterprises and organizations. To test which was faster in terms of execution time and memory consumption for a gas power plant project, it was developed using the blockchain consensus algorithms, notably the PoW algorithm and the PoA algorithm. PoA was already demonstrated to be more efficient than PoW. As can be observed, creating a blockchain using the PoA algorithm takes only 46 fewer seconds than it does using the PoW algorithm, and it also uses 1024 fewer bytes of RAM. Additionally, the ESP32 device was utilized in this work due to the benefits indicated above. This work was created in Matlab 2021a because it is appropriate for our purpose and has all the libraries we need to create a network simulation. A local server network was also included in this design for increased anonymity, and it turned out that this tactic was appropriate for the task at hand.

REFERENCES

[1] J. A. Hassan and B. H. Jasim, "Design and implementation of internet of things-based electrical monitoring system," *Bull. Electr. Eng. Informatics*, vol. 10, no. 6, pp. 3052–3063, 2021, doi: 10.11591/eei.v10i6.3155.

[2] J. AL-Hammoudi and B. Jasim, "Design and implementation of monitoring and warning (IOT) system for electricity poles," *Iraqi J. Electr. Electron. Eng.*, vol. sceeer, no. 3d, pp. 105–111, 2020, doi: 10.37917/ijeee.sceeer.3rd.15.

[3] A. A. Okandeji, F. Onaifo, M. T. Kabir, and K. Yakubu, "DESIGN AND IMPLEMENTATION OF INTERNET OF THINGS BASED IRRIGATION SYSTEM," vol. 16, no. 4, pp. 663–674, 2020, [Online]. Available: https://ieeexplore.ieee.org/document/8907168

[4] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT," *IEEE Access*, vol. 7. pp. 38431–38441, 2019. doi: 10.1109/ACCESS.2019.2905846.

[5] A. A. Abdullah and W. K. Oleiwi, "a Survey of the Blockchain Concept and Mitigation Challenges in Different Networks," *J. Hunan Univ. Sci.*, vol. 48, no. 10, pp. 890–905, 2021, [Online]. Available: https://www.researchgate.net/publication/355351692

[6] M. Majid *et al.*, "Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review," *Sensors*, vol. 22, no. 6, 2022, doi: 10.3390/s22062087.

[7] M. S., N. P., and M. S. V. M.E, "a Block Chain-Based Access Control Framework for Big Data," *Ijarcce*, vol. 10, no. 4, pp. 331–334, 2021, doi: 10.17148/ijarcce.2021.10458.

[8] M. Ma, G. Shi, and F. Li, "Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario," *IEEE Access*, vol. 7. pp. 34045–34059, 2019. doi: 10.1109/ACCESS.2019.2904042.

[9] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices," *Appl. Sci.*, vol. 10, no. 2, 2020, doi: 10.3390/app10020488.

[10] A. Lewis, "Blockchain Technology Explained," *Blockchain Technologies*. pp. 1–27, 2015. [Online]. Available: http://www.blockchaintechnologies.com/blockchain-definition

[11] K. Scholer, “An Introduction to Bitcoin and Blockchain Technology,” *Arnold Porter Kaye Sch.*, no. February, p. 14, 2016, [Online]. Available: http://files.apks.com/docs/IntrotoBitcoinandBlockchainTechnology.pdf

[12] P. Martino, K. J. Wang, C. Bellavitis, and C. M. DaSilva, “An Introduction to Blockchain, Cryptocurrency and Initial Coin Offerings,” *New Front. Entrep. Financ. Res.*, pp. 181–206, 2019, doi: 10.1142/9789811202766_0007.

[13] A. Bolfing, “Introduction to Blockchain Technology-2,” in *Cryptographic Primitives in Blockchain Technology*, 2020, pp. 199–240. doi: 10.1093/oso/9780198862840.003.0006.

[14] 조주현, “Block chain,” *Posri 이슈리포트(포스코경영연구원)*, vol. 10. pp. 1–11, 2017. [Online]. Available: https://openknowledge.worldbank.org/handle/10986/28962%0Ahttps://en.bitcoin.it/wiki/Block_chain

[15] T. Impact and A. Responsibility, “The Impact of Blockchain on Auditor Responsibility.” pp. 1–58.

[16] M. Banerjee, J. Lee, and K. K. R. Choo, “A blockchain future for internet of things security: a position paper,” *Digit. Commun. Networks*, vol. 4, no. 3, pp. 149–160, 2018, doi: 10.1016/j.dcan.2017.10.006.

[17] M. J. A. Baig, M. T. Iqbal, M. Jamil, and J. Khan, “Design and implementation of an open-Source IoT and blockchain-based peer-to-peer energy trading platform using ESP32-S2, Node-Red and, MQTT protocol,” *Energy Reports*, vol. 7, pp. 5733–5746, 2021, doi: 10.1016/j.egyr.2021.08.190.

[18] S. M. Alrubei, E. Ball, and J. M. Rigelsford, “The Use of Blockchain to Support Distributed AI Implementation in IoT Systems,” *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14790–14802, 2022, doi: 10.1109/JIOT.2021.3064176.

[19] C. Li and L. J. Zhang, “A blockchain based new secure multi-layer network model for internet of things,” in *Proceedings - 2017 IEEE 2nd International Congress on Internet of Things, ICIOT 2017*, 2017, pp. 33–41. doi: 10.1109/IEEE.ICIOT.2017.34.

[20] J. Islam *et al.*, “Blockchain-SDN based Energy Optimized and Distributed Secure Architecture for IoTs in Smart Cities,” no. November, pp. 1–20, 2020.

[21] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K. K. R. Choo, “An Energy-Efficient SDN Controller Architecture for IoT Networks with Blockchain-Based Security,” *IEEE Trans. Serv. Comput.*, vol. 13, no. 4, pp. 625–638, 2020, doi: 10.1109/TSC.2020.2966970.

[22] “IoT Data Security Via Blockchain Technology and Service-Centric Networking.” [Online]. Available: http://ieeexplore.ieee.org/document/4275759/metrics%0Ahttp://ieeexplore.ieee.org/document/4275759/metrics

[23] M. J. Baucas, S. A. Gadsden, and P. Spachos, “IoT-Based Smart Home Device Monitor Using Private Blockchain Technology and Localization,” *IEEE Netw. Lett.*, vol. 3, no. 2, pp. 52–55, 2021, doi: 10.1109/lnet.2021.3070270.

[24] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, “A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things,” *J. Ind. Inf. Integr.*, vol. 21, 2021, doi: 10.1016/j.jii.2020.100190.

[25] B. Adanur, B. Bakir-Gungor, and A. Soran, “Blockchain-based Fog Computing Applications in Healthcare,” in *2020 28th Signal Processing and Communications Applications Conference, SIU 2020 - Proceedings*, 2020. doi: 10.1109/SIU49456.2020.9302168.