Internet of Things Based Blockchain Technology for Gas Station

Samaher A.Yousiff¹, Raad A. Muhajjar¹

¹Department of Computer Science, College of CSIT, University of Basrah, Basrah, Iraq

**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.

**Keywords:** Internet of Things, Blockchain, ESP32, Consensus algorithms

**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
dge 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.
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 ESP32 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.

![Diagram](image-url)

**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.

![Transmitter algorithm diagram]

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.
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 Algorithm Diagram](image-url)
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 Algorithm Diagram](image)

**Figure 6**: POA's 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.
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.
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

<table>
<thead>
<tr>
<th>Nonce Range</th>
<th>POW</th>
<th>POA</th>
</tr>
</thead>
<tbody>
<tr>
<td>483</td>
<td>112</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>207</td>
<td></td>
</tr>
<tr>
<td>141</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td>371</td>
<td>229</td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>319</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>141</td>
<td></td>
</tr>
<tr>
<td>904</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>169</td>
<td></td>
</tr>
<tr>
<td>155</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>179</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>171</td>
<td></td>
</tr>
<tr>
<td>535</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td>457</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>877</td>
<td>437</td>
<td></td>
</tr>
<tr>
<td>418</td>
<td>272</td>
<td></td>
</tr>
<tr>
<td>484</td>
<td>107</td>
<td></td>
</tr>
<tr>
<td>194</td>
<td>93</td>
<td></td>
</tr>
</tbody>
</table>

Figure 9: Nonce Range
Table 3: (POW vs POA) Total time

<table>
<thead>
<tr>
<th>Total Time</th>
<th>POW Total Time</th>
<th>POA Total Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.4</td>
<td>3.26</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>3.2</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>3.8</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>31.5</td>
<td>3.1</td>
<td></td>
</tr>
<tr>
<td>31.8</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>39.5</td>
<td>3.3</td>
<td></td>
</tr>
<tr>
<td>29.9</td>
<td>2.9</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>32.85</td>
<td>2.8</td>
<td></td>
</tr>
<tr>
<td>33.1</td>
<td>2.9</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>3.1</td>
<td></td>
</tr>
<tr>
<td>34.3</td>
<td>3.15</td>
<td></td>
</tr>
<tr>
<td>34.64</td>
<td>2.95</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>2.98</td>
<td></td>
</tr>
</tbody>
</table>

Figure 10: (POW vs POA) time

Figure 11: (POW vs POA) Total time
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


