2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST) | 978-1-6654-6633-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICRTCST54752.2022.9781887

Demonstration of Integration of Blockchain in IoT

*

Somya Suhans Mahapatra
School of Electronics Engineering
Kalinga Institute of Industrial Technology (KIIT)
Bhubaneswar, India
ritul.mahapatra@gmail.com

Chandan Kumar Jha
Dept. of Electronics & Communication Engineering
Indian Institute of Information Technology Bhagalpur
Bhagalpur, India
ckjha.ece@iiitbh.ac.in

Abstract—In the modern era, blockchain technology has achieved a substantial growth with rapid research developments. Blockchain technology is widely used in the field of cryptocurrency. However, it can also be applied in other field such as internet of things (IoT). In IoT, data security and integrity is a prime concern where many problems exist such as data reliability and unauthorized access. It creates huge problem in deploying an IoT system on a smaller or larger scale. Hence, this paper reports a possible integration of blockchain technology in IoT to create a secure network. To demonstrate this, the game of Tic-Tac-Toe is implemented by following the rules of blockchain. The main goal of this implementation is to explore the application of blockchain in IoT and practically merge these two fields to get the service of IoT with the security and integrity that the blockchain technology promises.

Index Terms—Cryptocurrency, Blockchain, IoT, Proof of work, Merkle tree.

I. INTRODUCTION

The world is moving towards a very tech-centric era, where the IoT devices around us become a very essential part of our daily lives [1]. With development of IoT along with embedded systems and wireless communication systems, it is trying to make internet more accessible to everyone [2], [3]. Nowadays, IoT is one of the most influential emerging fields which has domestic to industrial scale applications. In general, an IoT network consists of heterogeneous devices which produce and exchange data among themselves. In IoT system, it is critical to maintain the security of data that is vulnerable to cyber attacks [4]. Presently, IoT consists of centralized architecture by connecting heterogeneous devices to cloud services through the internet. Various cyber security problems may be there in this network. In addition to this, the centralized architecture of IoT also puts all the connected devices/ nodes at the risk of failure when the central server poses any failure or problem [5], [6]. Hence, it is very important to make a secure decentralized network of IoT devices which should be fault tolerant as well. One of the potential solution to accomplish this is by using the concepts of blockchain [7].

Blockchain is an emerging field of research that is yet to expand its horizon beyond the world of cryptocurrency. Blockchain explores the idea of making a decentralized network of interconnected devices where each device that is connected to the network forms a trust with one another based on the concept of proof of work which lets them share a ledger to which all the devices can agree upon [8], [9]. It makes use of the peer to peer network to make the system decentralized and it tolerates any faults from any device on the blockchain network through the use of proof of work system [2]. It can provide a viable solution to make the IoT devices more secure.

In past, few research works have been carried out which explore the idea of combining IoT and blockchain together. In [10], Liu et al. proposed a blockchain based access control system in IoT which consists of three kinds of smart contracts: device contract, policy contract, and access contract. This access control system is based on hyper-ledger fabric blockchain framework and attribute based access control (ABAC) model. A decentralized authorization system is developed in [11] which works without a central trusted party. It leverages the idea of blockchains smart contracts combined with protected DoTs to maintain the security of the resources delegated on the blockchain. This approach provides means of federating networks of embedded networks and supports the life cycle of connected devices. In [2], Lei et al. outlines the approach for implementation of decentralized IoT platform to address its scalability, identity and data security challenges based on blockchain network. In this work, raspberry pi development boards are used for the implementation of physical devices. This paper presents comparative analysis of the designed system with the the existing works. In [12], a proof of block and trade algorithm is proposed which enables the security of block at trade and block creation phases. A lightweight consensus algorithm is also proposed which incorporates peers based on the amount of nodes participating in a session. This work reduces the computational time required by peers, and allows higher transaction rates for the IoT devices.

Integration of blockchain technology with IoT may pose different challenges. First of all, it is difficult to establish a true peer to peer connection over a wireless communication channel using Wi-Fi network [5]. This problem can be tackled using mesh network architecture, which is implemented using a decentralized network without establishing a peer to peer connection amongst the nodes [6], [13]. Secondly, memory storage of IoT devices is an important factor to consider when these devices use a micro-controller with very small storage

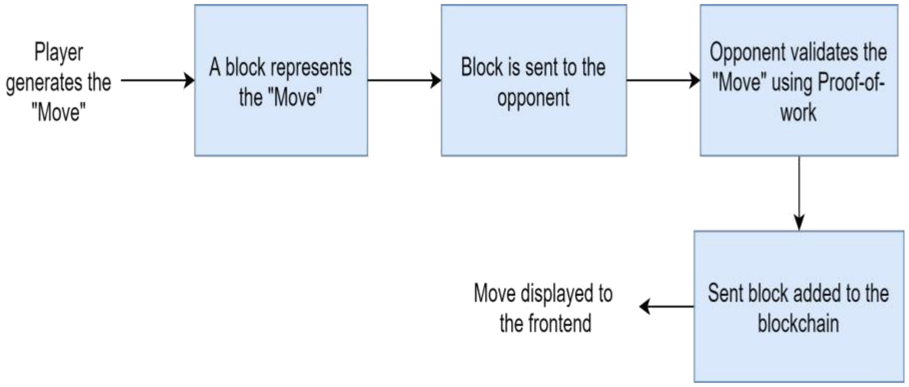

Player generates the "Move"
A block represents the "Move"
Block is sent to the opponent
Opponent validates the "Move" using Proof-of-work
Sent block added to the blockchain
Move displayed to the frontend

Fig. 1. Block-diagram of blockchain design of tic-tac-toe game

capacity [4]. This problem can be dealt using the concept of Merkle tree which is a binary hash tree used to store data in an efficient manner [8]. Lastly, mining in blockchain network is an important problem which has to be resolved when integration is being done with IoT devices. However, results of the mining step can be achieved using the the nodes present on the network itself without adding any additional mining nodes [2]. Thus, the goal of the mining process which is also called the proof of work can be fulfilled.

Considering the above mentioned challenges, this paper presents the demonstration of blockchain technology in IoT using implementation of the game ”Tic-Tac-Toe”. The game of ”Tic-Tac-Toe” has its own set of rules and regulations. The game features total nine moves and it can be correlated with the fact that there are a limited number of cryptocurrency on a blockchain network. Hence, nine moves are correlated to nine cryptocurrency present on the blockchain network. In the game of ”Tic-Tac-Toe”, each player can make a move with the agreement of both the parties. Hence, the game is implemented to be played autonomously between the two devices just by letting the devices follow the rules of blockchain. It is assumed that the devices have to maintain the integrity of the game by themselves without the involvement of any centralized server. Hence, it can be proved out to be the ideal game to expand the scope of IoT and blockchain together. Although, it is a crude idea based on which the implementation of blockchain network and IoT is built, still a lot of research that needs to be done for the ease of implementation and to make this useful for wide applications.

II. Methodology

In the proposed work, the game of ”Tic-Tac-Toe” is de-signed and implemented in such a way that it follows the rules of blockchain. The game is played between two devices. The overall system consists of several layers which are working independently from each other. If problems arise in one layer it does not affect any of the other layer present in the system. It helps to deal with any fault that arises in the system and also lets someone modify one part of the system without affecting the rest of the system. For maintaining the integrity of data, simple consensus algorithm is used. In comparison with existing algorithms, the consensus algorithm is computationally less expensive and it is most suitable for resource constrained low cost micro-controller. The proposed implementation does not need any extra mining devices. As a result of the implementation, the ”Tic-Tac-Toe” game is played between two devices and it is displayed on a front-end web application for monitoring the data. For the display of the game using front-end web application, flask framework is used to develop the application programming interface (API).

A. Blockchain design and implementation

Figure.1 illustrates the idea of the high level implementation of the ”Tic-Tac-Toe” game which works on the principle of blockchain. In this implementation, first, the game starts off with the player which generates their move with initialization of a new block on the network. The player then broadcasts this block to opponent’s device present on the network. The opponent then runs proof of work on the received block and if its a valid block then it gets added to the blockchain, else it gets discarded and the player has to send a new valid block in order to get added to the ledger. The updated blockchain then gets displayed on frontend web application. In the proposed implementation, low-cost ”NodeMCU 12-E ESP8266” development board is used which also features an inbuilt Wi-Fi module.

B. Proof of work for the game

In the proposed work, new blocks are added to the blockchain ledger using a consensus algorithm which is con-sidered as proof-of-work [9] for the game. All the devices from players side have to be agreed to this ledger. In the game, the generated move by a player should not be illegal or duplicate in order to get added it to the blockchain. For this, the generated move is validated using the proof-of-work. In conventional blockchain implementation, this proof-of-work is done by mining devices connected to the peer to peer network [8] in which 5-10 minutes duration is taken to complete the process and to add a new block to the blockchain depending upon the cryptocurrency. In the case of IoT based implementation, the mining process proves to be unessential because it just adds extra cost and complexity to the implementation which

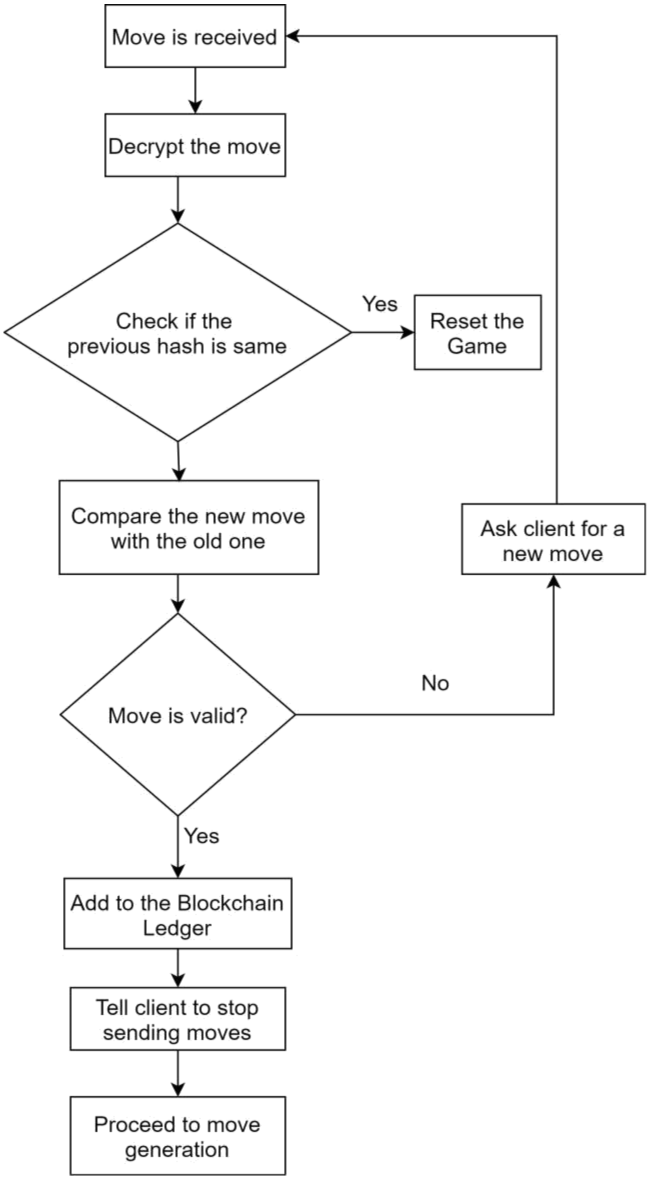
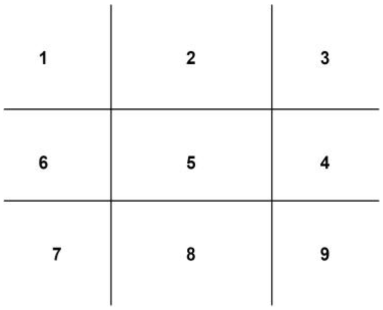

Move is received
Decrypt the move
Check if the previous hash is same
Yes
Reset the Game
Compare the new move with the old one
Ask client for a new move
Move is valid?
No
Yes
Add to the Blockchain Ledger
Tell client to stop sending moves
Proceed to move generation

Fig. 2. Flowgraph of proof of work



1	2	3
6	5	4
7	8	9

Fig. 3. Grid of tic-tac-toe game

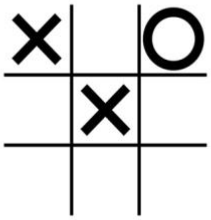


Fig. 4. Grid of tic-tac-toe game

effectively making it less feasible [2], [4]. In the proposed blockchain based implementation of ”Tic-Tac-Toe” game, the nodes present on the network itself are used to run the proof of work without the need of extra mining nodes. Hence, this implementation of proof of work eliminates the need of mining. Figure 2 illustrates the flow-graph of proof of work for the game which is designed to validate the move.

C. Move/Block Generation

The important and the most integral part of any turn based game lies in decision of both the players to make certain moves to outsmart the opponent. In the game of ”Tic-Tac-Toe”, there are two moves which are represented by the symbol ”X” and ”O”. Any player can make either one of the move throughout the game. The game features a 3x3 grid and any player who captures a line in this grid either vertically, horizontally or diagonally wins the game. At the start of the game, both the devices decide to choose their symbol either ”X” or ”O” with the help of simulation of tossing a coin. The device who wins the toss that plays the symbol ”X” or ”O” in their move throughout the game. The toss losing device get the other symbol respectively. When a device generates a move, it chooses a random number between 1-9 based on which the move is placed on the respective position of the grid (which is shown in Figure 3). A generated move is also a like transaction in the blockchain network. Hence, it proceeds to add this move to the ledger. The generated move is encoded in the following format: ”fPlayer NamegfPlayer SymbolgfPlayer Positiong”. Hence, a move like ”AO5” means player ”A” made the move ”O” at the 5th block of the grid. All the moves made by both the players are embedded into a single string which serves as ledger. Moves made by both players are embedded in the format: ”!fPlayer1 Moveg!fPlayer 2 Moveg!fPlayer 1 Moveg!...”. This can be done upto 9 moves and maximum 5 moves can be played by a player. Figure 4 shows the game ”Tic-Tac-Toe” is in progress with three moves. The encoded string for this game so far looks like !Ax5!Bo3!Ax1!000!000!000!000!000!000!000!.

The string is formatted in such a way to follow the principle of hashing. It is a way to transform a string of characters to a shorter fixed length which represents the original string [14]. There are several other ways of carrying out hashing but in the proposed implementation this design choice is made such that it becomes easy to demonstrate how the concepts of the blockchain carry out over to the game of ”Tic-Tac-Toe” in a more understandable manner. By following this format, the length of the string is fixed at the length of 37 throughout the whole game. Upon exhausting all the 9 moves, the game restarts and the string becomes

!000!000!000!000!000!000!000! which represents an empty grid. It is implemented in such a way to follow the concept of a Merkle tree which is discussed in detail in the next section.

D. Merkle tree for the ledger

In the proposed implementation of blockchain, a data structure called Merkle tree [8] is used. It is a binary hash tree which efficiently stores and manages data. In this tree, each parent node can only consist upto 2 child nodes which continues down to the leaf nodes. The leaf nodes contain the information about each of the new block that gets generated. Figure 5 shows the Merkle tree which works in our application. Every move/block that is generated by either of the devices gets added to this structure and then gets hashed together into one root hash containing the information of the whole game. Hence, the root hash contains details of all the moves that have been generated over the course of the game. This gives a secure, fast and efficient solution to encode the blockchain data. This method also helps in quick verification of the blockchain data and allows the data to be broad-casted to another device on the network in a very fast and efficient manner.

E. Securing the data using cryptography

Cryptography is a very essential part of a blockchain network which maintains the integrity and security of data that is being broad-casted over to the network. A conventional blockchain network uses SHA encryption to maintain the integrity of the blockchain ledger [15]. It offers more security but it is computationally expensive. Hence, it is beyond the scope of micro-controller with limited computing power. Furthermore, a micro-controller generally has to exchange real time data with one another. Therefore, a symmetric cryptography technique called secret key cryptography [16] is being used in the implementation of ”Tic-Tac-Toe” game using micro-controller devices. In the proposed implementation, each device has its own private key. This private key gets added to each character of the message from the root node of the Merkle tree. It encrypts the data in such a way that the original message is recovered only when someone knows the private key of the device, else the proof of work will reject the recovery message and render it invalid. Each device stores its own private key along with the private key of the other device present on the network. Any node can decrypt the encrypted message easily using that private key from the other node, which programmatically stored in each of the devices during the initialization. The reason for the use of private key cryptography is that it can be decoded very swiftly and it is very fast.

Another advantage of this cryptography is that when it is used in micro-controller or module like Arduino, there is no possible way to extract the private key from these devices. It proves to be very efficient and reliable in exchanging real time data between two devices.

F. Proposed System Architecture

The proposed IoT-blockchain implementation uses a layer based architecture which is shown in Figure 6. This archi-tecture provides a feasibility of making a modular system. It makes each layer separate from the other due to which modification in any layer without affecting the other layer is possible. As shown in Figure 6, the system architecture is divided into 4 layers which are IoT physical layer, connection layer, IoT-blockchain service layer and application layer.

The IoT-physical layer deals with various nodes which are linked to each other in a decentralized manner. All the nodes work homogeneously to exchange meaningful data from each other. In this layer, mesh topology is used to create decentralized network over the devices connected through Wi-Fi. The benefit of using mesh topology is that it provides the broadcasting of any message from any device to the rest of the devices present on the IoT network without third party server. It also provides the fidelity to run proof-of-work on the devices and share a ledger over the network without the need of a centralized server. A centralized server can also manage all the devices present on the network but it administers lot of problems such as any kind of server failure affects all the devices [5], [6]. In addition to this, any kind of cyber attack on the central server affect the entire system. Hence, decentralize network of devices is used in the proposed system architecture.

The connection layer consists of a router which is used to link the IoT physical layer and IoT-blockchain service layer for communication. It handles the management and routing of data. The IoT-blockchain service layer is required to keep track of all the data that are being exchanged through the IoT devices. Essentially, it keeps track of the ledger data but it doesnt affect the IoT physical layer in any way. This layer is responsible for fetching the ledger data from the IoT physical Layer for creating a database to store the fetched data. Lastly, the application layer features a front-end web application. Its main function is to display the data that is being stored in the IoT-Blockchain service layer. Hence, this layer is important to display, visualize and monitor the data from the database.

III. Implementation of IoT-blockchain platform

In the proposed implementation of ”Tic-Tac-Toe” game, data exchanging occurs between two devices. For this, simple server-client communication is used between two devices. For this, one device is treated a station while the other as an access point. The station device establishes connection with the access point device and exchanges data by making use of TCP/ IP protocol. Figure 7 illustrates all the TCP/ IP operations that are taking place between the two devices.

For ”Tic-Tac-Toe” game, all the blockchain operations are performed in the IoT physical layer. The game initially starts with the coin-toss operation which simulates a real life coin toss between the two devices. The network selects one device randomly through making a coin toss between the two devices. It starts at every round of the game because giving starting advantage to a single player would lead to an unfair game. Whichever device wins the coin toss proceeds to sending new

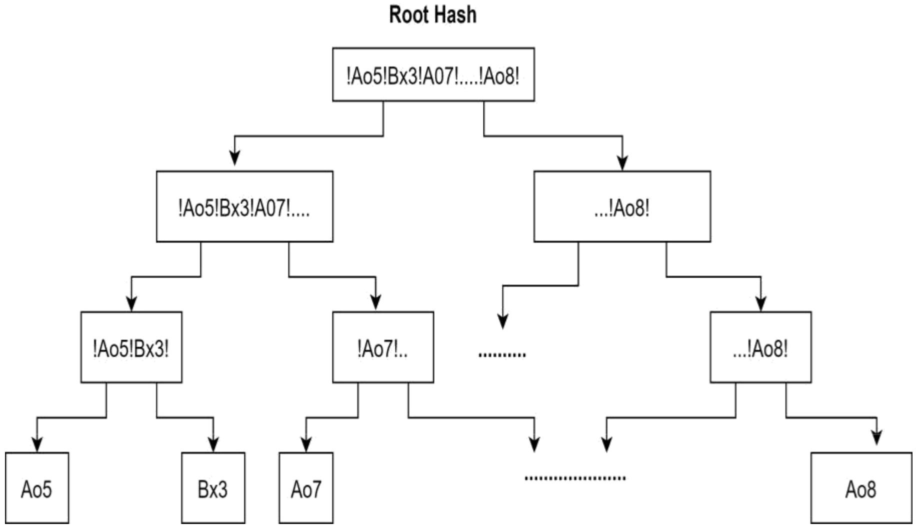


Fig. 5. Merkle tree for the tic-tac-toe game

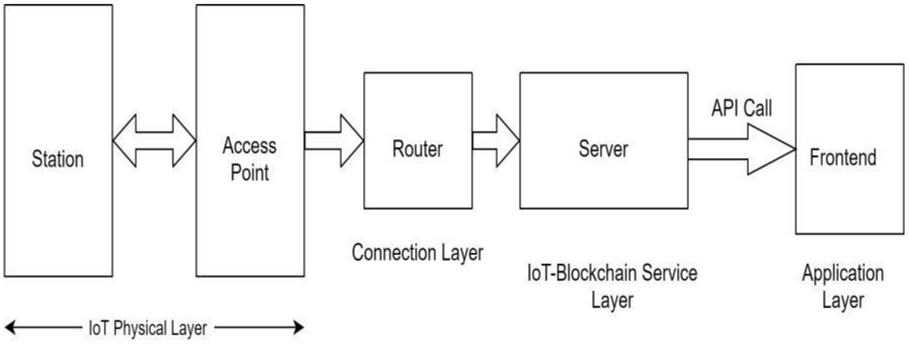


Fig. 6. Proposed system architecture

blocks/moves to the opponent while the device that lost the coin toss proceeds to proof of work to verify the incoming block/move through the other device. The two IoT devices between which the game is performed use ”NodeMCU 12-E ESP8266” development boards. These development boards are based on ”Tensilica 32-bit RISC CPU Xtensa LX106” micro-controller and it have a built-in Wi-Fi module. These development boards are low cost compared to other.

Connection between the two IoT devices is established based on the architecture of the connection layer which acts as a message broker between the IoT physical layer and the IoT-blockchain service layer. It is important to establish a connection between these two layers for for the management and routing of data.

The encoded data is exchanged between the IoT physical layer to the IoT-blockchain service layer and gets decoded by the IoT-blockchain service layer to be used in a meaningful manner. IoT-blockchain service layer serves as a mediator between the IoT physical layer and the application layer. It also provides an application programming interface (API) for the application layer. In the proposed implementation, pythons ”Flask library” is used to make the API. This API features a set of functions which allows applications to access the data or interact with external software components. The developed API is a light weight ”WSGI” web application framework which can be scaled up for complex applications. The ”Flask library” interatcs with the ”SQLite 3 library” to create the database from the encoded data received from the IoT Physical layer. The ”SQLite 3 library” maintains the database.

The blockchain database is visualized and monitored by the application layer. This layer fetches data from the IoT-blockchain service layer using API call to the respective route. For this, ”axios” is used which is a promise-based HTTP client. It offers asynchronous routine calls to the API. It is used to routine call to the respective route which in turn sends the data in ”JSON” format. After that ”React” component is used to create a dynamic table with infinite scroll feature. It displays the fetched data in a tabular manner and can be scrolled down infinitely till the end of the data. The table row gets updated dynamically whenever a new entry gets added to the database that is being maintained over the IoT-blockchain service layer. Figure 8 shows the ”Tic-Tac-Toe” dashboard which is the tabular display of the game data. In the proposed implementation, ”react.js library” is used to build dynamic and

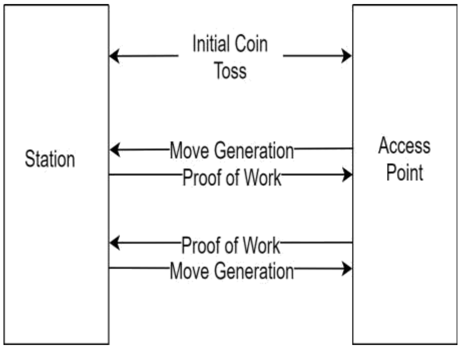
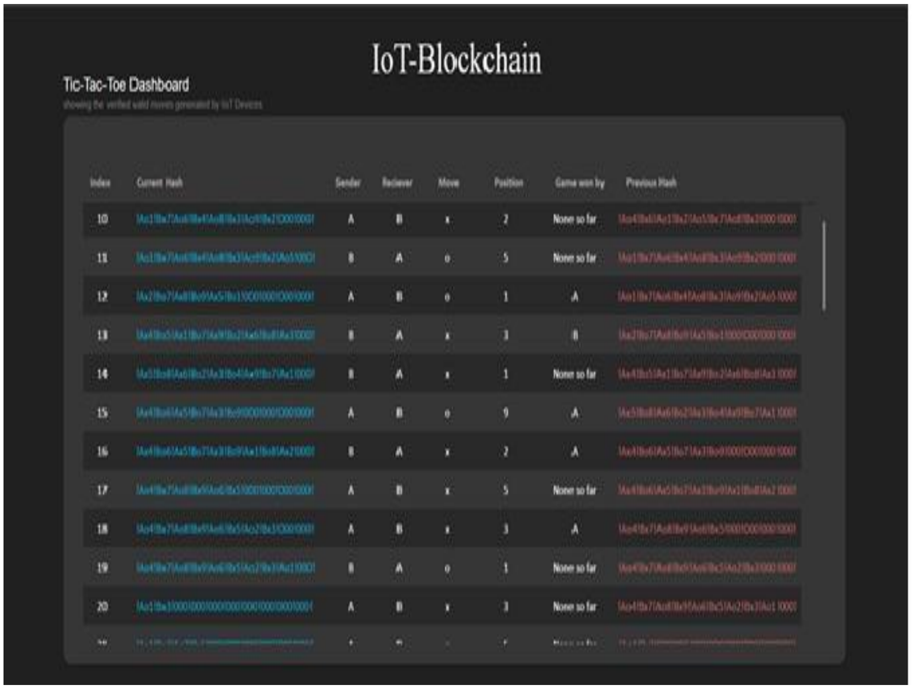


Fig. 7. TCP/IP operations between the IoT devices



Tic-Tac-Toe Dashboard

showing the verified valid moves generated by IoT Devices

Index	Current Hash	Sender	Reciever	Move	Position	Game won by	Previous Hash
10	[illegible]	A	B	x	2	None so far	[illegible]
11	[illegible]	B	A	o	5	None so far	[illegible]
12	[illegible]	A	B	o	1	A	[illegible]
13	[illegible]	B	A	x	3	B	[illegible]
14	[illegible]	B	A	x	1	None so far	[illegible]
15	[illegible]	A	B	o	9	A	[illegible]
16	[illegible]	B	A	x	2	A	[illegible]
17	[illegible]	A	B	x	5	None so far	[illegible]
18	[illegible]	A	B	x	3	A	[illegible]
19	[illegible]	B	A	o	1	None so far	[illegible]
20	[illegible]	A	B	x	3	None so far	[illegible]

Fig. 8. Tic-Tac-Toe game dashboard

interactive user interface (UI) for web application in a very easy and reliable manner.

IV. Conclusion

Gradually, the role of IoT is becoming prominent in our daily life for several applications. IoT performs data exchange between different inter-connected devices. In IoT, security and integrity of data is crucial and important. Blockchain tech-nology provides useful tools and concepts that address issues concerning to security and integrity of data. But, integration of blockchain technology with IoT is challenging. Hence, this paper presents the implementation of the game ”Tic-Tac-Toe” which demonstrates the integration of blockchain in IoT. The rules and regulations of the game ”Tic-Tac-Toe” make it suitable for this demonstration. The proposed implementation explores the idea of merging of IoT and bockchain technology for resource constrained and low cost IoT devices. It can provide a promising solution towards cyber-security required with the growing influence of IoT. In future, the proposed work can be made more scalable. In addition to this, the consensus algorithm can be improved using hashing techniques to make more standardized for any kind of data exchange.

References

[1] Schachtner, Christian. ”Essey 2.0 The future impact of IoT (Internet of Things) on your daily life .” (2020).

[2] Hang, Lei, and Do-Hyeun Kim. ”Design and implementation of an integrated iot blockchain platform for sensing data integrity.” Sensors 19, no. 10 (2019): 2228.

[3] Bhattacharjee, Shameek, Mehrdad Salimitari, Mainak Chatterjee, Kevin Kwiat, and Charles Kamhoua. ”Preserving data integrity in iot networks under opportunistic data manipulation.” In 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data In-telligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 446-453. IEEE, 2017.

[4] Reyna, Ana, Cristian Martn, Jaime Chen, Enrique Soler, and Manuel Daz. ”On blockchain and its integration with IoT. Challenges and opportunities.” Future generation computer systems 88 (2018): 173-190.

[5] Alencar, Mrcio, Raimundo Barreto, Horcio Fernandes, Eduardo Souto, and Richard Pazzi. ”DARE: A decentralized association rules extraction scheme for embedded data sets in distributed IoT devices.” International Journal of Distributed Sensor Networks 16, no. 10 (2020): 1550147720962999.

[6] Singh, Raman, Andrew Donegan, and Hitesh Tewari. ”Framework for a Decentralized Web.” In 2020 30th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1-7. IEEE, 2020.

[7] XIAOYU YANG, (2021), “Power Grid Fault Prediction Method Based On Feature Selection And Classification Algorithm” Int. J. of Electronics Engineering and Applications, Vol. 9, No. 2, pp. 34-44, DOI 10.30696/IJEEA.IX.I.2021.34-44..

[8] Nakamoto, S. ”Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot.” (2019).

[9] Porat, Amitai, Avneesh Pratap, Parth Shah, and Vinit Adkar. ”Blockchain Consensus: An analysis of Proof-of-Work and its applications.” (2017).

[10] Liu, Han, Dezhi Han, and Dun Li. ”Fabric-IoT: A blockchain-based access control system in IoT.” IEEE Access 8 (2020): 18207-18218.

[11] Andersen, Michael P., John Kolb, Kaifei Chen, Gabriel Fierro, David E. Culler, and Raluca Ada Popa. ”Wave: A decentralized authorization system for iot via blockchain smart contracts.” University of California at Berkeley, Tech. Rep (2017).

[12] Biswas, Sujit, Kashif Sharif, Fan Li, Sabita Maharjan, Saraju P. Mohanty, and Yu Wang. ”PoBT: A lightweight consensus algorithm for scalable IoT business blockchain.” IEEE Internet of Things Journal 7, no. 3 (2019): 2343-2355.

[13] Mandava Siva Sai Vighnesh, MD Shakir Alam and Vinitha.S, (2021), “Leaf Diseases Detection and Medication” Int. J. of Electronics Engineering and Applications, Vol. 9, No. 1, pp. 01-07, doi 10.30696/IJEEA.IX.I.2021.01-07.

[14] Swathi, Edem, G. Vivek, and G. Sandhya Rani. ”Role of hash function in cryptography.” Int. J. Adv. Eng. Res. Sci.(IJAERS) (2016).

[15] Swathi, Edem, G. Vivek, and G. Sandhya Rani. ”Role of hash function in cryptography.” Int. J. Adv. Eng. Res. Sci.(IJAERS) (2016)..

[16] Rajesh Kumar Tiwari (2020). ‘Human age estimation Using Machine Learning Techniques’, International Journal of Electronics Engineering and Applications, Vol. 8, No. 1, pp.01-09, DOI-10.30696/IJEEA.VIII.I.2020.01-09.