Block-Chain Platform for Internet of Things: An Application Oriented Approach

Chandini A.G[1] , Ganesan P[2], S.V. Sathyanarayana[3] , G.K Patra[4],

[1]*DE & CS, JNNCE, Shivamogga, Karnataka, India*
[2]*CSIR Fourth Paradigm Institute, Bengaluru, Karnataka, India.*
[3]*Professor, JNNCE, Shivamogga, Karnataka, India.*
[4]*CSIR Fourth Paradigm Institute, Bengaluru, Karnataka, India.*

Abstract-Internet of Things (IoT) which is inter-networking of devices are adopted for many applications. The basic concept of IoT is connectivity where in machines are internally linked to the cloud, in real time basis. Thus Cloud-Based concept came into existence that is making maximum use of IoT technologies. While Cloud requires a trusted intermediary for transactions between the users who wish to avail services. However, Cloud enables ubiquitous, convenient access to shared pool of resources, this will increase the costs substantially, as it forms a centralized network. Existing IoT solutions are more expensive because of the high infrastructure and maintenance cost associated with centralized clouds. Our aim is to design a decentralized, peer-to-peer model called 'Block Chain Platform for Internet of Things' that inherits the Block-Chain technology. Block-Chain forms a core technology behind Bit-Coin. This platform enables peers in a decentralized, peer-to-peer network to interact with each other securely without the need for a trusted intermediary. The proposed mechanism in this project is to implement Block-Chain into Internet of Things (IoT) which forms a decentralized system that eliminates single point of failure and also this provides a platform to assure Non-Repudiation and Integrity for non-financial transactions. In this proposed work, implementation is accomplished by using Arduino UNO and Sensors which measure environmental parameter like Air Quality data. A set of Raspberry Pi 3 Model B's forms a Block, connection of Raspberry Pi 3 Model B to Arduino UNO R3 with sensor forms a Block-Chain and Qt-Creator a Software Cross-platform IDE(C++) is used in which GUI is created and thus security is established in a Block-Chain network. Block is created and Hash value is validated that provides Integrity in a Block-Chain network.

I. INTRODUCTION

Block-Chain is a peer-to-peer (P2P) decentralized system used to store the pseudonymous transaction records in a trust-less environment. It is stated that Block-Chain can be used in future as internet interaction systems, such as in smart system contracts like Smart Homes employing Internet, public services, Internet of Things (IoT),reputation systems and in security system services rather than financial systems only.

The wide application of Block-Chain technology is in the field of IoT, to establish connection or inter-networking between many devices.[1] Block-Chain is essentially a public ledger used to store the data, in which all committed transactions are stored in a list (or a chain).This chain continuously grows when the new transactions are added to the list. In this way it forms a Block-Chain by adding each and every transaction that is communicated to the Block in a network. A complicated but secure mechanism (based on asymmetric cryptography) has to be implemented in order to protect Block-Chain from tampering in distributed systems.

The Block-Chain technology essentially has the key characteristics, such as decentralization, persistency, anonymity, fault-tolerance and auditability,[2] which allows a transaction to take place in a decentralized fashion without the need of central intermediary or any central authority, since it is cost inefficient and causes high traffic signaling. As a result, Block-Chains can greatly save the cost and improve the efficiency and eliminates single point of failure as it overcomes congestion of signaling. Blockchain can work in a decentralized and trust-less environment, which is enabled by integrating several core technologies such as cryptographic hash, digital signature (based on asymmetric cryptography) and distributed consensus mechanism- a distributed general agreement mechanism.[3]

To integrate the Block-Chain technology into IoT and to transfer some non-financial data measured from environment such as Air-Quality data, is transacted within the blocks and at the same time to ensure security in a Block-Chain network is main concern. So, this paper is to consider the Block-Chain implementation into IoT that forms an application oriented approach for non-financial transactions.[4]

In the proposed mechanism Block-Chain Platform is built by using hardware such as Arduino UNO R3 interface board and Air Quality Sensor-MQ135, Raspberry Pi 3 Model B, SD card for storing the data. Here, data from sensor measured is sent to Arduino UNO R3 interface board is which is fed to Raspberry Pi 3 Model B. Here, four Raspberry Pi's are considered to form a network. Then, these four Raspberry Pi 3 Model B's forms four Blocks (devices).Each Raspberry Pi Model B has a Ledger to store sensed data and this sensed data is transacted in a Block-Chain Network. Raspberry Pi Model B's as blocks along with the Arduino UNO and sensor that are interconnected to each other to form a Block Chain network through internet. The Air Quality data once fed to one of this block,is updated in all other blocks connected in the form of a network.Thus Block-Chain forms a decentralized network where each and every node or device or block acts as both sender and recipient.Each associated block checks and validates the data and provides the security.

Each Block internally consists of Block Header and Block Body in which many fields like Article Name, Block number, Current Hash Value, Previous Hash value, Next Hash value, Version number ,Sensor reading, Time-Stamp that gives time at which data is measured, Host-name and Merkle Tree Root hash and Nonce are present. Using the Hash values the integrity is checked.

The existing IoT solutions are expensive because of the high infrastructure and maintenance cost associated with centralized clouds, since more number of devices are connected or interlinked in a huge network[5]. The large amount of communications that will have to be handled when there are tens of billions of IoT devices in large scale that will increase the costs substantially. Thus, a cloud server which forms a centralized approach will remain a bottleneck and point of failure that can disrupt the entire network when large amount of devices exist. This is the motivation to establish a decentralized network which eliminates single point of failure, signaling traffic where Block-Chain Platform for IoT is concerned that is cost effective.[6]

Application that uses Block-Chain Technology is in the field of crypto-currency (Digital currency) and Bit Coin. The advantage of using crypto currency is that online money transaction is possible without need of central trusted intermediary. Thus, Block-Chain Platform for IoT solves the problem of high infrastructure and maintenance cost associated with centralized clouds and provides security by ensures non-repudiation and integrity for non-financial transactions.

A. Hash function

Hash function is a function that can be used to specifically map the data of arbitrary size to data of fixed size. The values given by hash functions are the hash values, hash codes, digests or hashes. Hash tables are used to quickly locate data records given by its search key. Hashes are mainly used to assure Integrity of the transmitted data and they form a building block to provide message authentication. Hash function can be uniquely used to identify secret information. Hashis a Collision-resistant function. Collision-resistance is accomplished by generating very large hash-values. For example Secure Hash algorithm-SHA-1, most widely used in cryptography, that generates 160 bit Hash function.

B. Methodology

The proposed methodology or block-diagram of Block Chain Platform for IoT is as shown in the Figure 1.

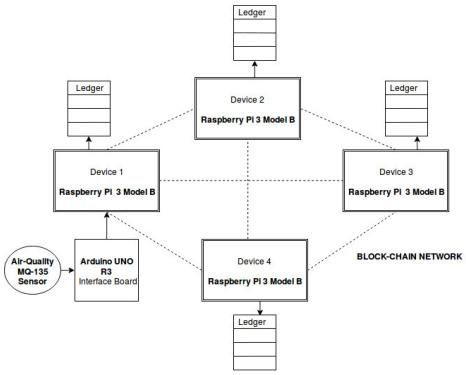

Figure 1: Methodology of Block-Chain Platform for IoT

Block diagram of Block-Chain platform for IoT consists of a sensor, Interface board, and four devices which forms a decentralized distributed network and a ledger for all four devices. Here specifically Sensor is Air-Quality MQ135 Sensor, interface-board is Arduino UNO R3 and device is Raspberry Pi 3 Model B is used.SD card acts as a ledger.

First from the Sensor the Air-Quality data measured is taken, connected with interface board(Arduino UNO R3) and thus sensed data is recorded and stored in the ledger of Device1 which is a Single Board Computer-Raspberry Pi 3 Model B.

Then the measured Air-Quality data is further updated in all the other device ledgers(Other 3 Raspberry Pi's B Models), as each device is

connected in the form of a distributed network and has peer to peer communication.

Here each and every device which is Raspberry Pi Model B acts as block to implement Block-Chain mechanism into Internet of Things (IoT) that is responsible to assure authenticity, non-repudiation, integrity for non-financial transactions.

Since all four devices have peer to peer communication, the data is stored in ledger and it is not deleted or modified.

The Air-Quality data which is measured as non-financial transaction in real-time basis is stored in a Block, then the other Block fields along with the Air-Quality data such as,Block-number, Article-ID, Hash Value, Nonce, Version number, Timestamp which measures time of arrival of the data from sensor, Merkle tree root hash is taken.

Thus Air-Quality Sensor MQ135, Arduino UNO R3 interface board along with Raspberry Pi 3 Model B device connected via Internet through wireless Communications forms a Block-Chain Network. The data measured from sensor is thus transacted in a Block-Chain network and validation is made by all the devices in a network by securely transferring the data by using Block-Chain Technology.

This forms Block-Chain Platform for IoT where Raspberry Pi 3 Model B devices are connected through Internet. Thus, proposed solution maintains security in IoT networks and offers some form of Validation of updated records and Consensus for transaction to prevent spoofing and theft.

C. Results & Discussion

This paper enumerates the creation of a Block with Raspberry Pi 3 Model B, employed in Qt Software application.

Initial Setup of Hardware Model

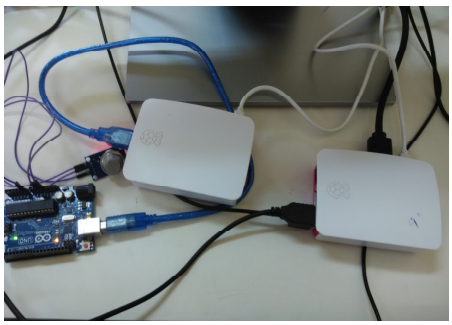

Figure 2: Set-up of Proposed Block-Chain Platform

As shown in Figure 2 the Air Quality Sensor named MQ135 having 3 pins such as Vcc, Gnd and Analog pins is connected to Arduino UNO R3 Interface board, intern the Arduino UNO R3 interface board is connected via USB Port to Raspberry Pi 3 Model B, Keyboard, Mouse are connected to Raspberry Pi 3 Model B and thus it forms a Mini computer.

Two Raspberry Pi 3 Model B devices are as shown in Figure 2.These are connected through Wi-Fi, thus forms an inter-networking application. Likewise four Raspberry Pi 3 Model B devices can be connected in similar way forms a Block Chain Network, in which each Raspberry Pi 3 Model B forms a BLOCK which collects the real time Air Quality data and transacts securely within a network.

Raspberry Pi 3 Model B is connected to Monitor via HDMI Cable, to the system installed with Raspbian Operating System.

Thus Block is created using Qt Cross Platform IDE, and the BLOCK is displayed on the Monitor, executed using Command line.

D. Block Creation with Raspberry Pi 3 Model B

The following illustrates the Block Creation, creating block, which is to measure the data from the environment, record and store it in a Block created using Qt Software-Cross Platform IDE.

- BLOCK is created using Qt- Software Cross Platform IDE.
- BLOCK is consisting of Block Header and Block Body.

Intern Block Header consists of following fields: Article Name, Block Number, Previous Hash, and Current Hash Value/Hash Value.

And Block Body consists of following fields: Version Number, Air Quality Reading, Host Name, Timestamp, Merkle Tree Root Hash, and Nonce.

- Block also consists of Network session for communication from the server with corresponding port number. Raspberry Pi 3 Model B forms Block1 and has IP configuration as 192.168.102.99 for communication to store the measured values.
- Run the code with device 1 with IP address 192.168.102.99, with port number on client side, put port number on which system is running. Port number is 51633 as shown in Figure 3.

Block also contains Push buttons such as Prev Block button, Close button, Get button.

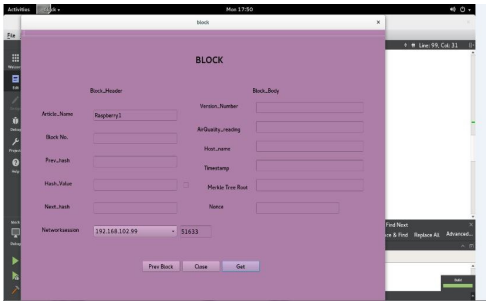

Figure 3: Block 1

- Command Line Execution in Raspbian OS, making a Project file which leads to output.

- Next press on Get button, at this time Air Quality reading measured from the sensor is recorded that is displayed in the Block in the Air Quality field as shown in Figure 4.

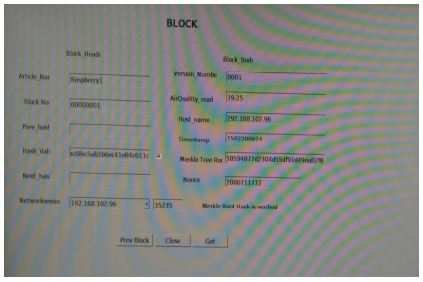

Figure 4: Block1 with Sensor data measured

For the first Block the Previous hash value doesn't exist since it is a Genesis Block.

- Along with Air Quality reading, Article Name, Block number, Version number,Host Name, Timestamp, time at which the data is measured in epoch time is recorded,Nonce which is random number for each and every transaction, and lastly Merkle tree Root hash value for a set of eight transactions(eight reading) is calculated. Then embedding all these values, current Block Hash is calculated as shown in Figure 5.

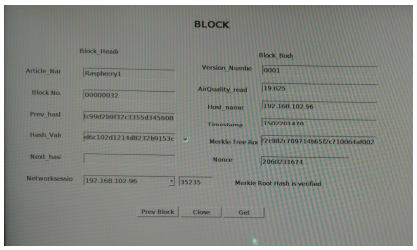

Figure 5: Previous Hash value displayed in Block1

When going to Next Block Previous Hash value is calculated as shown.

- To validate the transaction values, Merkle tree Root Hash is verified with current hash Value. The set of eight transactions is verified since it is equal to Current Hash value which proves Integrity.

- Thus, the Statement Merkle Tree Root Hash value verified appears which provides Integrity of the transactions in a Block.

- To go to previous block, Click on Previous Block push button, the previous Block (block number 00000028) appears as shown in the Figure which is in blue color.

Here Previous hash value and next hash value is got. This is as shown in Figure 6.

Figure 6: Block with Previous and Next hash value

- To go to Next Block, click on the Next block push button, Next Block with Block number 00000033 appears as shown in Figure consisting of both Previous Block Hash value and Next Block Hash value. This is as shown in Figure 7.

Figure 7: Block with Previous and Next hash value with Hash value verified

- Merkle tree root hash values are also validated with current Hash values and thus integrity is checked.

- This Block, consists of buttons like Previous Block, Next Block, Close and Validate.

Thus now two blocks are connected in a Block-Chain network. Likewise four Raspberry Pi 3 Model B can be connected in a network.

- After this again to move to next Block, once all the Merkle tree root is validated, then a statement called Reached the current block! Please receive New block is displayed.

Thus, the two Raspberry Pi3 Model B forms a block where hash values are used to validate and verify transactions at each and every node. Thus Block-Chain as also ensures Non-Repudiation where the falsifying of data is not allowed, as Merkle tree root hash is involved in a Transaction.Thus the real-time Air Quality data measured is securely transacted between two or more nodes in a Network forming Block-Chain and by verifying and validating Hash Values at each node, the Non-repudiation and Integrity is achieved.

CONCLUSION

IoT thus paves a way to ensure a securable,transaction in support with the concept of Block-Chain Technology.In this proposed project work,a real-time environmental parameter called Air Quality data is measured through a sensor,and Raspberry Pi 3 Model B is used which acts as Block to store the sensor readings that is displayed in BLOCK created using Qt-software Cross Platform IDE.

The BLOCK is subdivided into Block header and Block body and consisting of all internal fields such as Article Name,Block Number,Previous Block Hash value,Current Hash Value,Next Block Hash value,version number,Air Quality reading, Host Name,Merkle tree Root Hash value and Nonce.Here the corresponding Current Hash value for entire Block is calculated.This current Hash Value is verified with the Merkle Tree Root Hash Value.

The Hash Value thus provides Integrity, Merkle tree root hash value detects the malicious nodes and thus provides Integrity. Thus Merkle Tree Root hash value is verified with current Hash Value.If this two values are verified, it provides validation of a particular BLOCK which involves Air-Quality data,a non-financial transaction.

Then the four blocks are connected forming Block-Chain network, where the transactions are securely made and integrity check within the transactions is assured, by validating each and every BLOCK in a network. Thus Block-Chain provides an efficient Platform where the data is securely transacted between the nodes, whichforms a decentralized Platform in connection with Internet of Things. Thus this proposed project gives an application oriented approach that forms a Block-Chain Platform for Internet of Things.

ACKNOWLEDGMENT

This work is developed at CSIR-4PI, Bangalore and supported by Student Programme for Advancement in Research Knowledge (SPARK).Authors are grateful to the Head, CSIR-4PI for giving us the opportunity to carry out the work.

REFERENCES

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system," vol. www.bitcoin.org.

[2] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, Block chain challenges and opportunities: A survey."

[3] S. Huckle, R. Bhattacharya, M. White, and N. Belo, Internet of things, block- chain and shared economy applications," Procedia Computer Science, vol. Published by Elsevier B.V., pp. 461,468, 2016.

[4] E. Hillbom and T. Tillstrom, Applications of smart-contracts and smart- property utilizing block chains," in Chalmers University of Technology ,University of Gothenburg, Department of Computer Science and Engineering Goteborg, Sweden, 2016, p. February.

[5] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, Blockchain the gateway to trustfree cryptographic transactions," Association for Information Systems AIS Electronic Library (AISeL), p. 153 paper, 2016.