International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Applicability of Blockchain Technology in Communication of Data using Raspberry Pi as Server

Siva Naga Lakshmi Pavani Kallam, BVNR Siva Kumar

Abstract: ***The main things we used to build the project in this paper are one raspberry pi as server, two Arduino's as two nodes which are configured to connect to Wi-Fi using ESP8266 (node mcu). We will connect temperature and humidity sensor to one Arduino and RFID Reader module to another Ardunio Board to demonstrate the entire process. The working follows as the data is taken from DTH sensor and RFID Reader module which is sent to Raspberry Pi. Arduino's acts as nodes from which data transmission starts. The Raspberry Pi acts as gateway between two Arduino's and it is the server. All the components are connected to the Wi-Fi. The data from the sensors is taken and will be sent to server in hash, hash includes all the previous data and we already know that block chain is a decentralized network. We cannot manipulate the values of data at any point because of their data contains both previous and local hash. This is why usage of block chain provides more security to IOT devices. Henceforth, we implemented this exceptional way of blockchain technology for communication of data for safety and immense security.***

Index Terms**:** ***Blockchain Technology, Cryptographic hash, IoT, peer to peer communication***

I. INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

The blockchain is a framework which apparent rundown of exchanges with the timestamp, information, past hash and nonce made in bitcoin or cryptographic money.

Data hung on a blockchain exists as a common and consistently accommodated database. This is a method for utilizing the system that has evident advantages. The blockchain database isn't put away in any single area, which means the records it keeps are really open and effectively undeniable. No incorporated rendition of this data exists for a programmer to degenerate. Facilitated by a great many PCs at the same time, its information is open to anybody on the web. The chain of blocks in the blockchain is framed by containing the past hash in the present square. The following block should possibly be added to the chain if the miners check the present block contains the past hash which is produced by utilizing the exchange information, time stamp, nonce and target. The principal hinder in a blockchain is called as beginning block. The beginning block is quite often hardcoded into the product. The exception case in the chain of blocks is beginning block does not refer to past block. In each blockchain, there is just a single path to the beginning block. There are uncommon hubs called miners to tackle the computational riddles to make and affirm obstructs in the chain. They are called as miners. The exchanges before they added to a blocks are supported in the zone which is called as mempool. The miners will get these exchanges in the cluster astute. Proof Of-Work is the first agreement calculations in a Blockchain organize. With PoW, miners contend with one another to get them compensated on the off chance that they complete the riddle in any case. On the off chance that somebody attempts to hack or misrepresent a block, they have to hack the whole chain which is basically unthinkable. Most presumably, for each exchange to be affirmed, it requires least of eight blocks of miners' acknowledgment of legitimate rightness of exchange is required.

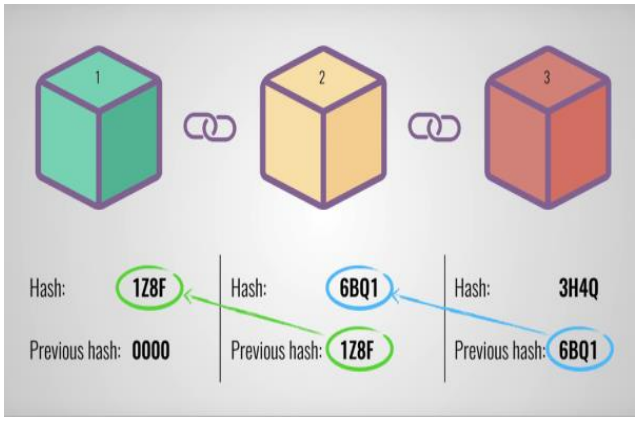

Fig1. Blockchain Working Illustration

In the decentralized system, the data isn't put away by one single element. Truth be told, everybody in the system possesses the data. In this framework, we can straightforwardly interface with our friends without the need of outsider. Despite the fact that there are decentralized substances before bitcoin, heaps of focuses to be considered to make it effective including computational power which needs more to deal with handling steps. Furthermore, even adaptability is additionally the mission of taking care of the nodes in the concentrated system which is particularly restricted contrasted with the decentralized system in light all things considered and handling force are housed in a solitary server.

Manuscript published on 30 August 2019.
*Correspondence Author(s)
Siva Naga Lakshmi Pavani Kallam, Electronics and Communication Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, 521230, INDIA.
BVNR Siva Kumar, Associate Professor, Electronics and Communication Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, 521230, INDIA.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Going to the blockchain innovation, there will be a difficulty in power of miners take 10 minutes to include the new block. Consequently, it takes tremendous computational power. Thus, we surely understood mindful of an impediment in the decentralization that if the entrance is disseminated every single node will be experts. Consequently, there will be a few contrasts among them while the system needs to settle on basic choice. In any case, in the blockchain innovation, on the off chance that one miner got remunerated for tackling the riddle and add another block to the chain arrangement, different miners will check for affirmation other than making contrasts among the nodes.

Thus, in the wake of including another block in the chain, there are affirmation blocks which demonstrate to us the Proof-Of-Work. Along these lines, it is simpler to verify the information in the IOT case by utilizing trustless blockchain innovation.

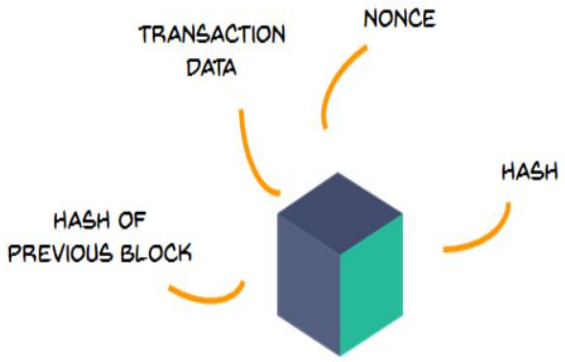

Fig.2. Block Representation

The extent of protection that a blockchain can give is the one of most winning perspectives. In the blockchain innovation the information which we transmitted is covered up by means of complex cryptography. The genuine data we are sharing is pseudo unknown. Blockchain is one framework made to unravel the test of how to believe the system when all clients are unknown. Thus blockchain gives huge organizations a stage to act with veritable respectability towards their locale and clients. In any case, blockchain can possibly add straightforwardness not exclusively to the money related part of business. Blockchain is the innovation which gives this force of protection which has never done in previous. Not to confine the range of progressive advantages given by the blockchain innovation which is the model that does not expect trust to securely interface and execute, we are coordinating it in the IOT to own the expression of protection dead false. Blockchain's open record isn't a book with numbered pages. There is no grouping of pages to confirm the record out of which we are hoping to be all together. In this way, for all intents and purposes it is conceivable that tearing a page in center and supplanting it with the other can be a noteworthy danger to confide in this innovation. Thus, it's anything but a sort of arrangement of blocks yet a progression of blocks of which we can run keeps an eye on it get similar hashes by utilizing a similar mark of data exchange. Hashing is the fundamental imperative and essential capacity in the blockchain innovation. The most engaging property of hashing calculation is reversible property. We can see a similar hash yield in the event that we review the capacity with a similar info. The blockchain comprises of hash pointer which focuses to its past block, consequently making the chain. A hash pointer is like a pointer, however rather than simply containing the location of the past block, it likewise contains the hash of the information inside the past block. This one little change is the thing that makes blockchains so incredibly dependable and trailblazing. In the following area we will see the equipment prerequisites and how the combination of blockchain is executed. One of the essential focal points that blockchain gives over other record writing computer programs is that it relies upon cryptography and is adjusted to be constant, one can't retreat to a particular point on the blockchain and change information. There is a great deal of discussion about the blockchain being a "trustless" framework. Cooperation is actually classified, and this PC code which speaks to our shared plan is set into a kind of open record, or goliath spreadsheet which can be seen by anybody. The made contract is built up crosswise over time and political and topographical limits. Agreement is expected to make the framework work by and large obviously, every cooperation on the blockchain being checked and confirmed by autonomous "miners" of the information, nobody believing the data until it is confirmed by accord. The formation of smart contracts incorporated with the blockchain record framework has opened an entryway to the likelihood of interfacing individuals, gadgets and information to changeless procedures. I have heard it alluded to as a potential Internet of everything (IoE). Everything sounds magnificent, and in truth, it appears that the entire framework still has far to go to understand its maximum capacity. In any case, trust is an incredible power, and the blockchain is by all accounts creative enough, "troublesome" enough, to be a ground-breaking weapon in the hands of the individuals who both have trust in a superior future and in the hands of the individuals who have none. The suggestions are huge. On the off chance that such a decentralized database of advanced resources can be consistently ensured by solid cryptography, cooperation and data ceaselessly confirmed and recorded, the potential grows a long ways past just digital money. This procedure would not depend on the institutional quality of country states. Whenever progressed admirably, this innovation could fall existing open record frameworks, change the substance of land, loaning and other money related administrations businesses, and on in the process of childbirth markets. The registering force required to process exchanges on the blockchain and confirms the code is critical to say the least. Blocks may need to increase to deal with more exchanges being prepared on the blockchain. There likely could be a requirement for a kind of overall administration to the blockchain, making the standards and conventions that can guarantee the central standards so essential to the achievement of the innovation are kept up. Also, unexpectedly enough, despite the fact that the blockchain and shrewd contracts could engage autonomous laborers, the stages and procedures based on the blockchain could drive numerous out of work.

© Copyright: All rights reserved.

In our genuineness to drive upheaval and tackle issues, as we run quickly into the guarantee of things to come, I wonder that we can really draw the world together past our divisions and contrasts into solidarity of importance and reason.

II. IMPLEMENTATION OF COMMUNICATING DATA OVER BLOCKCHAIN TECHNOLOGY

We need some data to establish communication between gateway and nodes. So, we integrated DTH sensor and RFID Reader Module in the two Ardiuno's. Communication of data from those two nodes to server happens only through blockchain technology. Whenever the DTH sensor senses the data, it will communicate to the Raspberry Pi in the form of blocks i.e. each block has the data which is sensed by DTH Sensor and the time stamp at which the data has been sensed and the previous hash and current hash using cryptographic hash function and a nonce value.

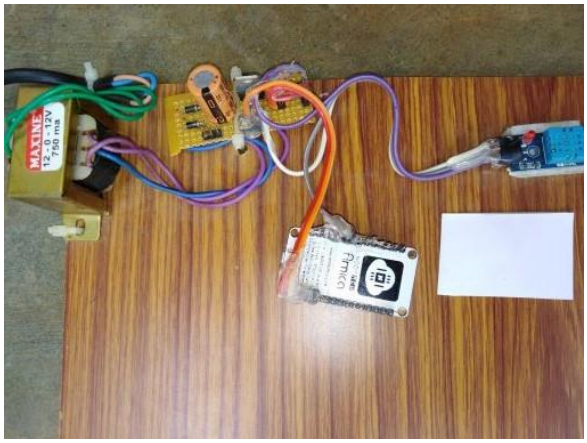

Fig.3. Node integrated with DTH Sensor

In the first block, the previous hash is an exception. So, to add the next sensed information to the first block, the current hash in the previous block must match with the previous hash in the current block. In order to check this paradigm we have miners to work. These miners will only have to integrate the next block if the hashes match according to statement above. The paramount significant thing in the blockchain technology is done by the miners. Also, if any block of data has been manipulated during the way it reaches to the gateway, then the hash will be changed. Because, the cryptographic hash will be generated based on the data it has. As this is a case sensitive, even if any alphabet case change results in changing the cryptographic hash. If any manipulations have occurred in the data, then the hash will also be changed. Hence the manipulated cryptographic hash does not match with the original previous hash; it is not acceptable to integrate the block. Then we must have a doubt that what happens if any corrupted miner integrates the manipulated block in the chain? Here comes the answer. The blockchain technology works on the consensus algorithm; which means the integrated latest block should be confirmed as the secured block by the remaining miners. Minimum, it should be confirmed by the 8 miners to agreeable by the technology that the data has not been manipulated. So, it is very significant to know the reason we are implementing the communication using blockchain technology is mainly it is impossible to integrate the manipulated data in the chain. So, we may have another doubt raised here i.e. what are the chances of blocks in the blockchain technology to be get hacked even though we are maintaining secured information in the series of blocks forming a chain?. Right, it is a valid one. So, basically in any centralized systems, hacking is not a big task even though they have their own measures. Simply by managing a few resources, hackers have enough to get through a lot of data to hack. Here in the blockchain technology we already discussed in the above section that it is a decentralised distributed ledger. So, in order to hack the data they need to crack everyone's systems. In the blockchain technology if any particular block has to be hacked, then the previous hash should be known. In order to get the previous hash, they need to peep the previous block which again they need to know the previous hash of those previous hashes. So, totally if any particular block has to be hacked, for every block they need to crack the previous hashes. So, it is impossible and never ending process of hacking the blocks in the blockchain technology which makes the hacking merely impossible. This advantage along with all those discussed raised the cryptocurrency platform.

After all making a clear path to the reason of implementing communication through blockchain technology, let us discuss the way how we approached. As mentioned above, the DTH sensors will be sending the information it sensed through blocks form and each time it senses again will be integrated to the chain which is collecting at the gateway. The same case belongs to the RFID Reader Module. Whenever the RFID Tags has been shown to the EM-18 Reader Module, it will display the unique ID to the tag we used. The same formation of blocks in the chain manner has been applied to this Ardunio board of which the data is collected at the Raspberry Pi gateway. Here we used MQTT dashboard, hivemq.com as server. Whenever the nodes publish the data regarding the information they sensed, the MQTT server published it.

We are using Raspberry Pi 3 Model B as server as it has inbuilt Wi-Fi to connect to the nodes. The nodes here are also connecting to the same account of Internet of which Raspberry Pi is connected. Hence, all the devices we are using to build this project are connected to the same network to communicate. The Ardunio boards have node McU integration along with the DTH sensor and RFID Reader Module in order to have connection to the network we are using in the gateway. The nodes which we are using in this project can be seen in the figures 3 and 4.

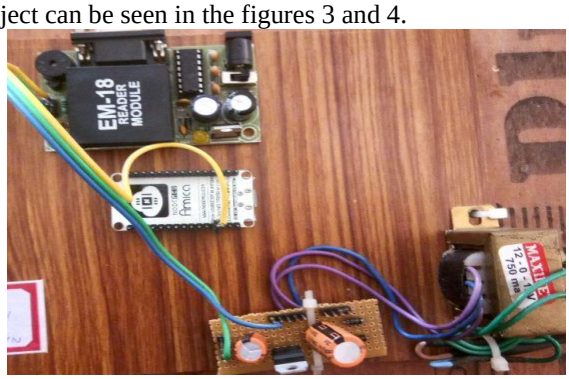

Fig.4. Node integrated with EM-18 RFID Reader Module.

© Copyright: All rights reserved.

III. RESULTS

The blockchain technology for communication purpose can be implemented using python language. Since it's bolstered by a huge and enthusiastic network of engineers, Python has altogether developed as a language and is presently at a propelled stage, which ensured steadiness and unwavering quality. Python has a delicate expectation to absorb information, making it simpler for engineers to ace it inside a sensible time allotment. Straightforwardness and moderation are at the centre of Python's way of thinking. Its straightforwardness gets from a wide range of highlights for instance, in python empty areas mean code blocks, and designers don't have to stress over including curly brackets and keywords. We can utilize python to code a blockchain without composing a ton of code. In python, we can undoubtedly perform numerous assignments with a solitary command. It makes crafted by structure blocks with the applicable data and connecting them together a much simpler one to do. Python is clean and has a colossal collection of libraries officially accessible, which are the reasons why we utilized python. Consequently forward, in light of the above discourse, production of handy outcomes is to be done to demonstrate how this thought winds up legitimate. In this way, we previously associated every one of the gadgets we referenced, for example, two nodes, one Raspberry Pi to the same network utilizing a Wi-Fi module and run the code which has been written in the python 2.7.9 Shell in Raspberry Pi to see the outcomes. The two nodes will distribute the information when they constantly sense and send the messages with respect to temperature, humidity and RFID unique ID to the Raspberry Pi which is acting as a gateway.

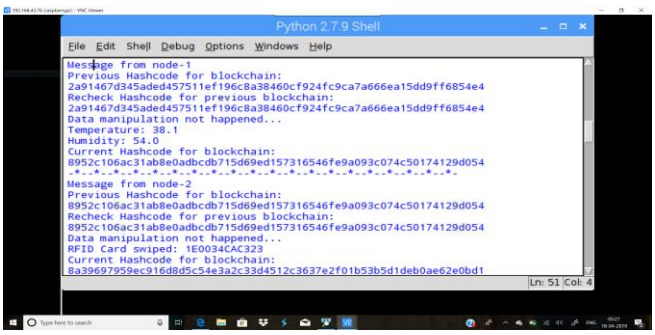

Fig.5. Communication Of Nodes To Server Using Blockchain Technology

So, here in the figure of snapshot above, we can see that the messages are being sent to the server from the nodes representing as messages from node-1 which shows the data regarding Temperature value and Humidity value along with the previous and current hashes of that particular block. And from node-2 we are evident of the information about the RFID Tag's unique ID that is used for that particular block also representing along with current and previous hashes. So, the line in between any two messages indicates the separation of two blocks. Hence, the information we are receiving in the VNC Viewer can be seen in the form of blocks in the blockchain illustration. So, whenever the information has been sent by the nodes to the Raspberry Pi, it will integrate the blocks only if the cryptographic current hash of the previous block matches with the previous cryptographic hash of the next block. In this way, the blocks are integrated throughout the communication forming a blockchain using the blockchain technology. Even, as the additional task, we have proved that the data manipulation can never be happened in this technology as the blocks are tightly secured. The specifications and qualities we have discussed justifies that this technology is immensely secured and hence we used this for communication purpose proving that the cases we are going through like no privacy in the IoT statement is false. We proved that range of blockchain technology is beyond financial sector and crypto currencies through this project. Hence, we established communication using blockchain technology using Raspberry Pi as server and two nodes.

IV. CONCLUSION

We knew that the blockchain technology has more dimensions than the financial sector and crypto currency platforms. We need an ideology to implement blockchain in the more useful way as it has more secured properties and trustless options as we ever have. So, in this paper we proposed an application level of communication from the two nodes to server by using blockchain technology making use of those properties. Python helps us in evidencing how the blocks are formed, how the integration of blocks happened in forming a chain and how well secured we are to communicate through this technology. So, drawing forth, we conclude that this is more eminent way of communication to proceed in our real-time which is highly profoundly capable.

V. FUTURE SCOPE

Blockchain technology has a wide range of applications and more dimensions to explore. We can even expand this paper further by using more nodes to communicate each other as well as to gateway by integration of blocks in a chain manner using more data exchanges.

REFERENCES

1. L. Law, S. Sabett, and J. Solinas, "How to make a mint: the cryptography of anonymous electronic cash," American University Law Review, vol. 46, no. 4, pp. 1131-1162, 1996.
2. F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, March 2016.
3. S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008, available at: https://bitcoin.org/bitcoin.pdf
4. R. Merkle, "A digital signature based on a conventional encryption function," In: Pomerance C. (eds) Advances in Cryptology — CRYPTO '87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg, pp. 369-378, 1987.
5. Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in Bitcoin," Financial Cryptography, pp. 507-527, 2015.
6. T. Dryja, "Hashimoto: I/O bound proof of work," 2014.
7. G. Wood, "Ethereum: a secure decentralised generalised transaction ledger, Byzantium version," 2018, available at: https://ethereum.github.io/yellowpaper/paper.pdf
8. S. Underwood, "Blockchain beyond bitcoin," Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.
9. W. E. Summary and S. Plants, "Power and the Industrial Internet of Things (IIoT)," no. January, pp. 1–14, 2015. [
10. K. Delmolino, M. Arnett, A. E. Kosba, A. Miller, and E. Shi, "Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab.," IACR Cryptol. ePrint Arch., vol. 2015, p. 460, 2015

© Copyright: All rights reserved.

AUTHORS PROFILE

Siva Naga Lakshmi Pavani Kallam born on 10th August 1996 and is graduated from NRI Institute of Technology Affiliated to JNTUK in the stream of ECE. And pursuing Master's in the stream of VLSI &Embedded Systems in Lakireddy Bali Reddy College of Engineering, Mylavaram, INDIA. Area of Interest is Embedded Systems and VLSI.

BVNR Siva Kumar born on 26th March 1965. Post Graduated from JNTUEC, KAKINADAA in the year of 2004 and presently pursuing PhD in Amity School of Engg. &Tech. And working as Associate Professor in Lakireddy Bali Reddy College of Engineering, Mylavaram, INDIA. Area of Research is Medical Robotics.

© Copyright: All rights reserved.