A LIGHTWEIGHT PAYMENT VERIFICATION USING BLOCKCHAIN ALGORITHM ON IoT DEVICES

Rajagopalan.B[1], Revanth.R[2], Sandhiya.G[3], Shamsiya Banu.A.R[4], Ms. Abirami .S[5]

[1,2,3,4] *Department of Electronics and Communication Engineering, SRM Valliammai Engineering College*
[5]*Department of Electronics and Communication Engineering, SRM Valliammai Engineering College*

Abstract - A blockchain is a upcoming revolutionary one with crypto smart contract that is used for token transaction with the help of unique address id. In this blockchain transactions, each block contains unique id ,hash rate and the content of the previous block .In this manner all the blocks are interconnected to ensure security. In terms of privacy and security it fulfils everything, here the sender and receiver cannot be known by the third man. Tampering these integrated blocks will be difficult. All the blocks in the blockchain are encrypted If one has to tamper or steal the data from the blocks, they have to hack 60-70% of the blocks. If they fail to do ,the system will automatically initialize the tamper blocks as NIL so that the tokens that are hacked by hacker will be declared as void. Image if we add this type of security to our IOT and next gen devices, we can reduce the tampering and data stealing can be minimal. Here we are done a basic payment verification blockchain coding in python and we implemented it on the IOT device (ESPN kit)

INTRODUCTION

A blockchain is simply a distributed database of records or public ledger of all completed and shared transactions or digital occurrences. Every transaction in the public ledger is confirmed by a majority of the system's members. Information cannot be deleted once it has been entered. Every every transaction ever made is recorded in the blockchain, which is certain and provable .To give a simple analogy, stealing a cookie from a cookie jar stored in an isolated location is far easier than stealing a cookie from a cookie jar placed in a market place when hundreds of people will watch the process.

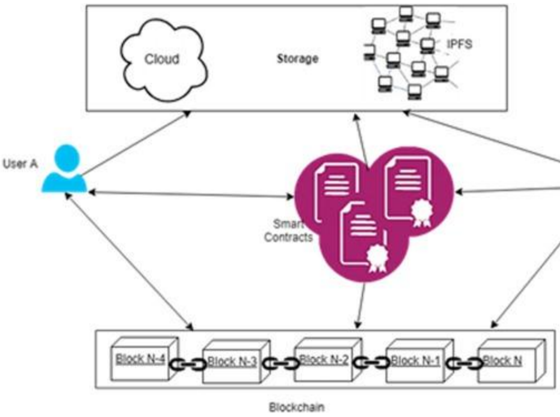
A blockchain is simply a distributed database of records or public ledger of all completed and shared transactions or digital occurrences. Every transaction in the public ledger is confirmed by a majority of the system's members. Information cannot be deleted once it has been entered. Every every transaction ever made is recorded in the blockchain, which is certain and provable .To give a simple analogy, stealing a cookie from a cookie jar stored in an isolated location is far easier than stealing a cookie from a cookie jar placed in a market place when hundreds of people will watch

Blockchain on IOT

Engineers can utilise blockchain data sharing to enable IoT devices to communicate with one another in the IoT. The gadgets accomplish this without the use of a centralised network. The distributed network of computer systems that makes up the blockchain makes those communications tamper-proof. Hundreds of billions, if not trillions, of devices will be connected to the Internet of Things. However, most of these devices now interact through centralised computing systems, which can fail at times. Other issues are caused by hackers. And the costs are enormous. Blockchain, on the other hand, avoids this by establishing a digital ledger of data, such as transactions. By confirming and adding to the blockchain, each data block builds on the previous one.

Leasing a truck. According to the Gartner Inc. research "Integrating Blockchain With IoT Strengthens Trust in Multiparty Processes," IoT sensors installed in leased vehicles may record crucial events on a blockchain to better monitor fleet whereabouts and returns, as well as to enable more meaningful payment methods. With IoT sensors on board vehicles, truck leasing businesses will be able to charge renters fees depending on the torque of the loads rather than miles, as is now the case," according to the article. "The blockchain distributed ledger technology allows people to share a single version of the truth." The data is not controlled by any single institution, and truckers and leasing businesses may independently check their own copies of the distributed ledger. This blockchain/IoT connection should aid leasing organisations in increasing income while lowering costs.

All of this means that the information cannot be tampered with. It provides for efficient embedded system verification in the IoT. As a result, IoT devices can use the technology to connect safely.



Existing System

In Early 2008, some group of anonymous experts developed blockchain like peer-peer network lately in 2009, the bitcoin was developed (first digital currency in the world). Transaction in Ethereum smart contract and ripple currency are done in blockchain. In India, the CBSE exam results are published through blockchain. In smart contracts, it requires high hash rate to process the data which is too expensive. However, there is no support for low-end devices because the process is very complicated and difficult to process.

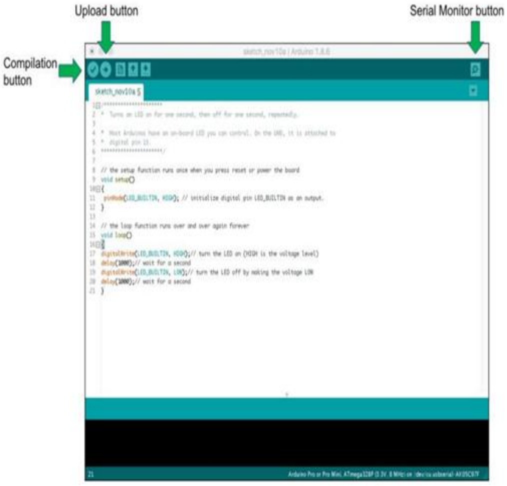
Proposed System

Here we are sorting out the problem in low end IOT devices also. To prove this, we demonstrated through ESPN kit (IOT Device), Node MCU, RFID card which contains unique information about the user and we implemented blockchain code through python. The RFID card works like Wi-Fi hard here, RFID reader is connected to the ESPN kit which has Wi-fi and Bluetooth connection for access. Also contains 32-bit LX106 RISC microprocessor for high processing rate. Every customer information is dumped in these cards like debit/credit cards. And the kit is connected to monitor to conduct the experiment and the output is verified

METHODOLOGY

SHA256 ALGORITHM IN BLOCKCHAIN: SHA256 is a patented cryptographic hash function that returns a 256-bit value. What is a hash? Encryption transforms data into a secure format that cannot be read unless the recipient has the key. In encrypted format, the size of the data is unlimited and is often the same as unencrypted. This algorithm is used in blockchain technology that has been used to secure the data of transaction in this project.

ARDUINO IDE: The Arduino Integrated Development Environment - or Arduino Software (IDE) -contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino hardware to upload programs and communicate with them. In this project, Arduino IDE is used to read the data from the RFID reader to Serial Monitor and verify the data for further processing.



```
/*********************
 * Turns an LED on for one second, then off for one second, repeatedly.

 * Most Arduinos have an on-board LED you can control. On the UNO, it is attached to
 * digital pin 13.
 *********************/

// the setup function runs once when you press reset or power the board
void setup()
{
 pinMode(LED_BUILTIN, HIGH); // initialize digital pin LED_BUILTIN as an output.
}

// the loop function runs over and over again forever
void loop()
{
digitalWrite(LED_BUILTIN, HIGH);// turn the LED on (HIGH is the voltage level)
delay(1000);// wait for a second
digitalWrite(LED_BUILTIN, LOW);// turn the LED off by making the voltage LOW
delay(1000);// wait for a second
}
```

EMBEDDED C

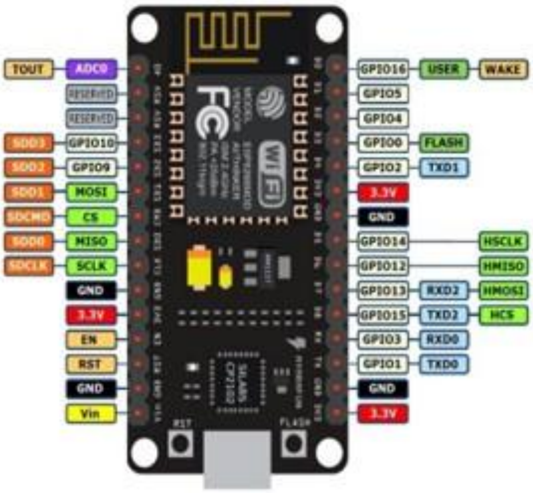
Embedded C is most popular programming language in software field for developing electronic gadgets. Embedded C programming plays a key role in performing specific function by the processor. In this project, Embedded C is used for Arduino IDE.

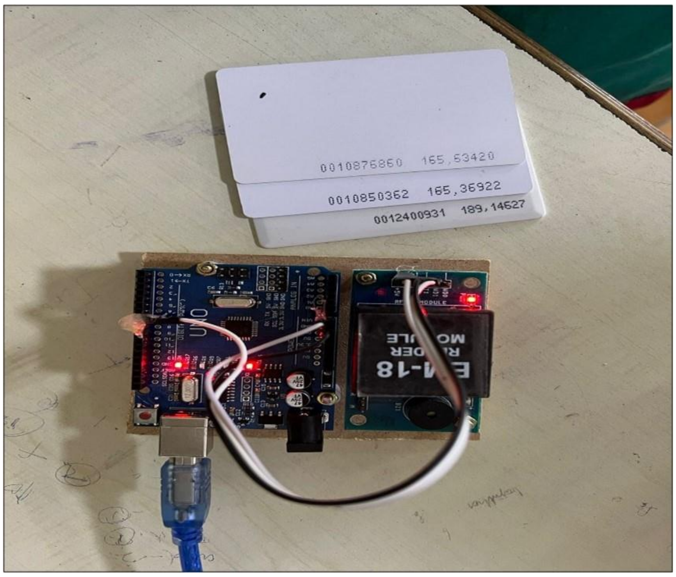
PYTHON IDLE

Python IDLE is a IDE for Python which has inbuilt libraries in it. It helps us to code faster and it has automatic indentation features. In this project, Python IDLE is used as the main language for generating Blockchain algorithm.

NODE MCU AND RFID CARDS:

Node MCU ESP8266 development board is the controller used in the project. It is based 32-bit LX106 RISC microprocessor and supports RTOS. It has in-built Wi-Fi / Bluetooth features used for remote access. Consumes Less energy. RFID (Radio Frequency Identification) cards are used for transaction purpose.

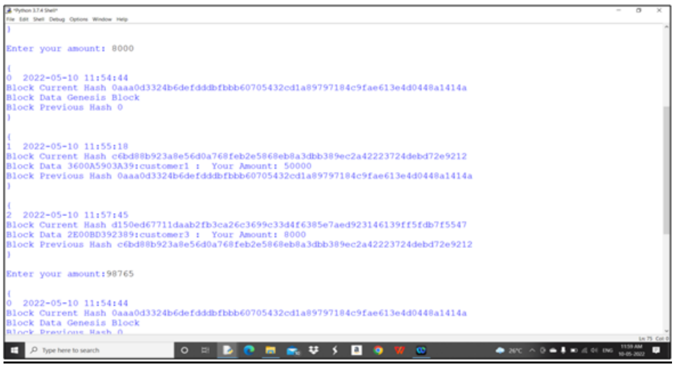




REPRESENTATION:

This is the real-time representation of our project. ESP8266 kit is used to receive the data from the user. Here we are going to use RFID (Radio Frequency Identification) cards for scanning the data. This data is scanned by RFID reader and verified by the SERIAL MONITOR ('tether' between the computer and Arduino). The RFID card number has been already pre-registered in the program (Only registered RFID cards can be used). GPIO (General Purpose Input Output) is used to connect the kit with the system through USB. The data travels through the PROOF OF WORK. Once it passes the PROOF OF WORK, the data will be entered into the program and saved in the ledger. The first data enters the first ledger called Genesis Block. The hash value of the block is generated and previous hash will be zero since there is no previous block. Then when the second data enters, same steps are followed and the second data is stored in second ledger. The previous hash of the second block will be the current hash of the first block (Genesis Block). Then the current hash of second ledger will be the previous hash of third ledger. This is the way blockchain algorithm works. The hash value we get is of 256-bit value (64 characters) since we are using SHA256 algorithm. The information of the user will be stored as blocks and if any changes occur in hash value, then we can easily detect the malicious act. However, hacking this technology is not easier to do and this will be the safest way for low-end devices to protect the information against hackers.

OUTPUT



```
}

Enter your amount: 8000

{
0  2022-05-10 11:54:44
Block Current Hash 0aaa0d3324b6defdddbfbbb60705432cd1a89797184c9fae613e4d0448a1414a
Block Data Genesis Block
Block Previous Hash 0
}


{
1  2022-05-10 11:55:18
Block Current Hash c6bd88b923a8e56d0a768feb2e5868eb8a3dbb389ec2a42223724debd72e9212
Block Data 3600A5903A39:customer1 :  Your Amount: 50000
Block Previous Hash 0aaa0d3324b6defdddbfbbb60705432cd1a89797184c9fae613e4d0448a1414a
}


{
2  2022-05-10 11:57:45
Block Current Hash d150ed67711daab2fb3ca26c3699c33d4f6385e7aed923146139ff5fdb7f5547
Block Data 2E00BD392389:customer3 :  Your Amount: 8000
Block Previous Hash c6bd88b923a8e56d0a768feb2e5868eb8a3dbb389ec2a42223724debd72e9212
}

Enter your amount:98765

{
0  2022-05-10 11:54:44
Block Current Hash 0aaa0d3324b6defdddbfbbb60705432cd1a89797184c9fae613e4d0448a1414a
Block Data Genesis Block
Block Previous Hash 0
```

The program prints several information so we can get a clear understanding about the process. The information of the user is stored in blocks and protected by hash function. The program asks for the amount to be transacted as an input and the output shows the current hash of the block (ledger), block data code, RFID card name (customer name), amount to be transacted and the previous hash of the block. The hash value has 64 characters and it is a 256 bit value. The program also use inbuild functions from Python Library to display the exact time and date when the transaction occurs to add more accuracy to the output. This output is just a real-time representation of how the data are protected in blockchain algorithm.

CONCLUSION

The program prints several information so we can get a clear understanding about the process. The information of the user is stored in blocks and protected by hash function. The program asks for the amount to be transacted as an input and the output shows the current hash of the block (ledger), block data code, RFID card name (customer name), amount to be transacted and the previous hash of the block. The hash value has 64 characters and it is a 256 bit value. The program also use inbuild functions from Python Library to display the exact time and date when the transaction occurs to add more accuracy to the output. This output is just a real-time representation of how the data are protected in blockchain algorithm.

REFERENCES

[1] J. A. Stankovic, I. Lee, A. Mok, and R. Rajkumar, "Opportunities and obligations for physical computing systems," Computer, vol. 38, no. 11,pp. 23–31, Nov. 2005.

[2] W. Wolf, "Cyber-physical systems," Computer, vol. 42, no. 3, pp. 88–89,Mar. 2009.

[3] Bellare, Mihir; and Rogaway, Phillip. (September 21, 2005). "Introduction." In Introduction to Modern Cryptography (p. 10).

[4] Fundamentals and Applications in Contactless Smart Cards and Identification, May 2003

[5] ESP8266 Node MCU Using Arduino IDE: Getting Start With ESP8266 (IoT hands on projects)May 2018

[6] Python: A Beginners Complete Reference Guide to Learn The Python Programming Language, June 2019

BIOGRAPHIES

B.Rajagopalan pursuing his B.E., in Electronics and Communication in 2022 from the college of SRM Valliammai Engineering College.

R.Revanth pursuing his B.E., in Electronics and Communication in 2022 from the college of SRM Valliammai Engineering College.

G.Sandhiya pursuing her B.E., in Electronics and Communication in 2022 from the college of SRM Valliammai Engineering College.

A.R.Shamsiya Banu pursuing her B.E., in Electronics and Communication in 2022 from the college of SRM Valliammai Engineering College.