International Journal of Scientific & Engineering Research Volume 10, Issue 11, November-2019 1 ISSN 2229-5518

Block chain based lock system:An overview

Gowri Sunder Ravi, Meiyappan.M.M, Sai Vishnu.R, Balaji.B

Bitcoin and other cryptocurrencies are dependent on blockchain - the underlying distributed ledger that guarantees tamper resistant permanent transactions to do business. But that's not all blockchain does, or has the potential to do. - Olawale Daniel

***Abstract*—Home security plays an important role in a large portion of our life.The impact of internet Of things is increasing day by day along with increasing number of devices growing rapidly.Due to this exponential growth of IOT,The factor of security has become very important one to consider. However,the data transmitted and received can be hacked, Therefore there is a recognizable need to manage the security problems,In this paper we propose a smart locking system using block chain. Block chain provides a decentralized structure with the means of distributed ledger,combined with strong encryption techniques. Also here the system will be able to perform 3 step authentication based on OTP,RFID and password generation and prevent remote hacking using ultrasonic sensor.**

***Index Terms*—Introduction,Literature survey,Access control,Distributed ledger,Comparison with current system,System design,System methodology,Shortcomings,Conclusion,Future enhancement.**

I. INTRODUCTION

India is a country that has a wide young population that is growing constantly, As the rate of digitization is increasing rapidly in India,The concern of data in the wrong hands is a big concern,This concern is muted out with the help of block chain,which provides a decentralized structure with the means of a distributed ledger. It also provides security via strong encryption techniques. This also helps us add full suite of electronics applications with the integration of internet of technology to the lock,by adding various sensors and processors.It also brings down the commission cost considerably lesser from around 25 percent to 1.5-2 percent. This paper extensively discusses the block chain technology and how it can be modified to provide access control,it also provides insights into developing a security system using raspberry pi.this system maintains a registry that maintains a time log of each user. Thereby providing security along with authentication.

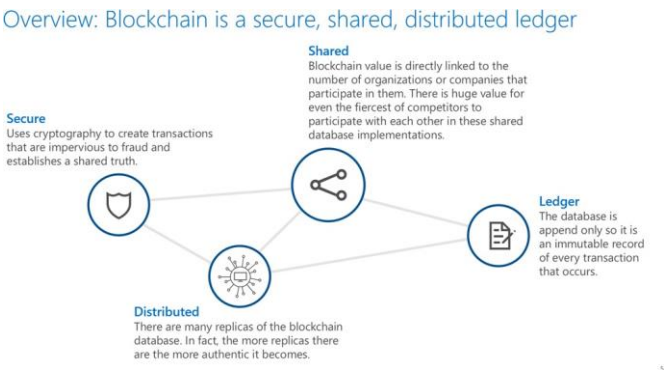


Fig. 1. **Blockchain services**

II. ACCESS CONTROL

- Ever since the beginning of civilization one of the very first things that early man did was to build a door.
- This he did to restrict entry into his personal space, He allowed people only whose identity he was sure of and also those who will not cause any harm to him.
- Access control in the digital world is analogous to this.Access control is a concept which is used to restrict access and control the data flow in sensitive areas in the system.
- Access control policies are used to define right of subject,These policies are implemented during the access request time.
- This access control is given to people based on certain attributes this could be something unique for the system to identify and understand that this is the correct person similar to a key for the door.

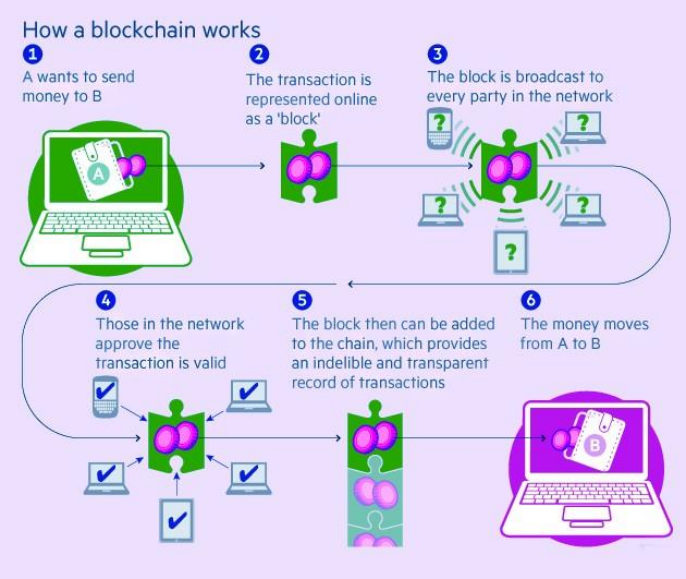


Fig. 2. **Blockchain working**

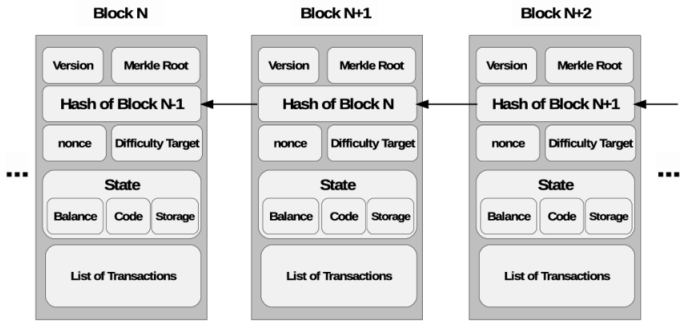


Fig. 3. **Blocks**

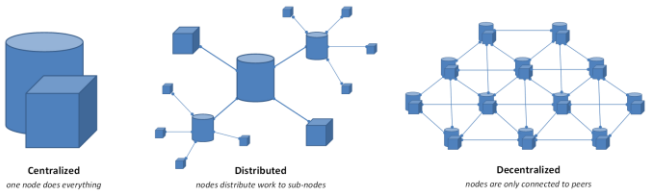


Fig. 4. **Types of network**

- These attributes could be anything ranging from a person's ID and unique password,or a one time password to controlling access based on the person's,organization,country or designation.

III. Distributed Ledger

- Ledgers are basically records or logs of transactions,ledgers are important to keep track of movement of items or in this case access.
- Though there are digital ledgers available paper based ledgers are still widely used all over over the world for transactions using physical signatures for authentication,Recent research in cryptography and increase in computing power power have given rise to distributed ledgers.
- Distributed ledger can be defined as database that is stored and which can be updated independently by each participant which are node in a distributed network.
- This distribution of records are unique and they not sent to the nodes by a central point unlike normal digital ledgers,each node in the network processes every transaction,then publish it.Thus,each transaction can be verified if the majority of results from other nodes agree with it.
- Once this has been verified,the distributed ledger is updated in the copy of each and every node of the ledger.
- Therefore distributed not only maintains authenticity of the data by verifying each entry in the ledger it also prevents loss of data if any of the nodes are compromised unlike centralized structure.

IV. Block Chain

- Block chain as in the name is basically a chain of nodes that are linked together using cryptography,the block or node where the information is hashed and stored,also it points to the previous block, maintains a time stamp, and details of transaction data.
- The blocks which contain data records are linked together.
- The design of blockchain is such that it is resistant to tampering of data,It is used as distributed ledger,It is typically managed by peer to peer network protocols for node to node communication.
- The data entered follows all the rules of a distributed ledger.Any changes in the records cannot be done without informing other nodes and following consensus protocol.
- Blockchain can therfore be defined as decentralized distributed system based on consensus protocol.

V. Comparison with Current System

- All current forms of security mechanisms make use of a centralized structure, but such a structure leads to increase in cost since there is an external vendor responsible for maintaining a register and charging a commission from the owner and guest for every transaction on the platform.
- This commission is usually paid for each entry and setting up the passwords and credentials associated with the entry.
- Block chain on the other hand is a decentralized structure which means it bring down the cost of maintaining the network very much it is responsible only for initial setting up of the network and a percentage for each node added,It also prevents any manipulation as in the centralized system as the external vendor is a weak point in the system.
- Also it intimates all the nodes in the chain and saves a copy of the transaction at each node.

Vcc- Connects to 5V of positive voltage for power
Trig- A pulse is sent here for the sensor to go into ranging mode for object detection
Echo- The echo sends a signal back if an object has been detected or not. If a signal is returned, an object has been detected. If not, no object has been detected.
GND- Completes electrical pathway of the power.

Fig. 5. **Ultrasonic sensor**

Fig. 6. **Raspberry pi 3b+**

Fig. 7. **RFID reader**

- Thereby it allows data to be retrieved even though if it is destroyed at any one of the node.
- Also, any new node can be added only through consensus protocol which means any new node can be approved only if all the already present nodes accept it.All the data are hashed with time stamp.

VI. SYSTEM DESIGN COMPONENTS

A. *MAJOR HARDWARE TOOLS:*

- ULTRASONIC SENSOR: Ultrasonic sensor HC-204 is used this sensor provides 2cm to 400cm of measurement functionality with ranging accuracy which can reach up to 3mm. Each HC-SR04 module includes an ultrasonic transmitter, a receiver and a control circuit.
- RASPBERRY PI 3b+:The Raspberry Pi 3 Model B+ is the most advanced product in Raspberry Pi 3 range,It incorporates 1.4GHz, dual-band 2.4GHz and 5GHz 64bit quad core processor, inbuilt wifi, Bluetooth 4.2/BLE,It is usually defined as a credit card sized computer.It acts a processor when connected to other peripheral devices.Usually runs using raspbian OS.
- RFID Reader: The RFID RC522 is a very low-cost RFID (Radio-frequency identification) reader and writer that is based on the MFRC522 micro controller. This micro-controller provides its data through the SPI protocol and works by creating a 13.56MHz electromagnetic field that it uses to communicate with the RFID tags.

B. *MAJOR SOFTWARE TOOLS:*

- RASPBIAN OS:It is an open source linux based operating software customised for raspberry pi,It serves as an platform for front user interaction with the hardware,It acts as bridge between front end and back end.
- HTML:Abbreviated as hypertext mark up language ,It is a very well known language used to design web pages in this case it used to design front end web page for user.
- Node JS:Node.JS is an open source java script based coding environment.It helps user to produce dynamic web page before being sent int the front end to the user.The js stands for JavaScript which is its language.Java script has various packages which provide code optimization and scalability.

VII. SYSTEM METHODOLOGY

- In this system,This project presents a prototype model and a system concept to provide a smart electronic lock using block chain.This system is intended to provide overall measures object detection, and real-time Assistance.
- The system consists of a raspberry pi 3,ultrasonic sensor, LCD display, GPIO extension board. This project aims at development of a blockchain based smart lock kit which only gets activated only when the user is within

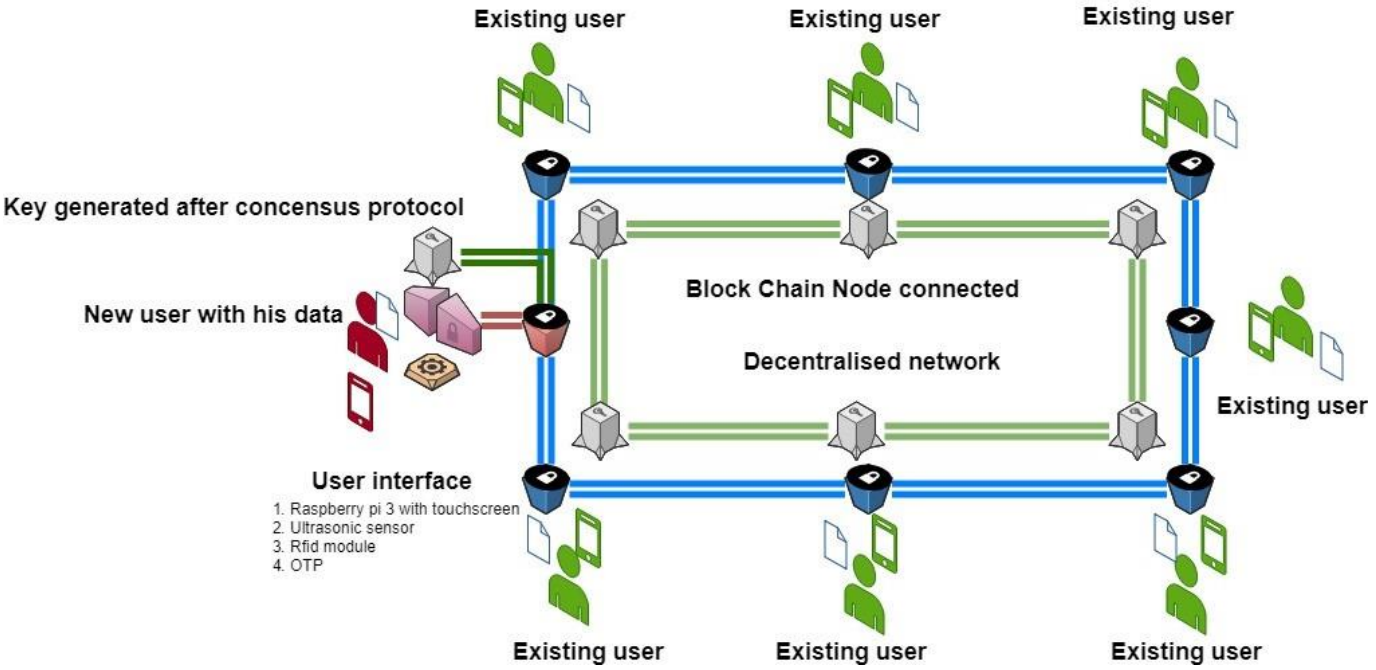
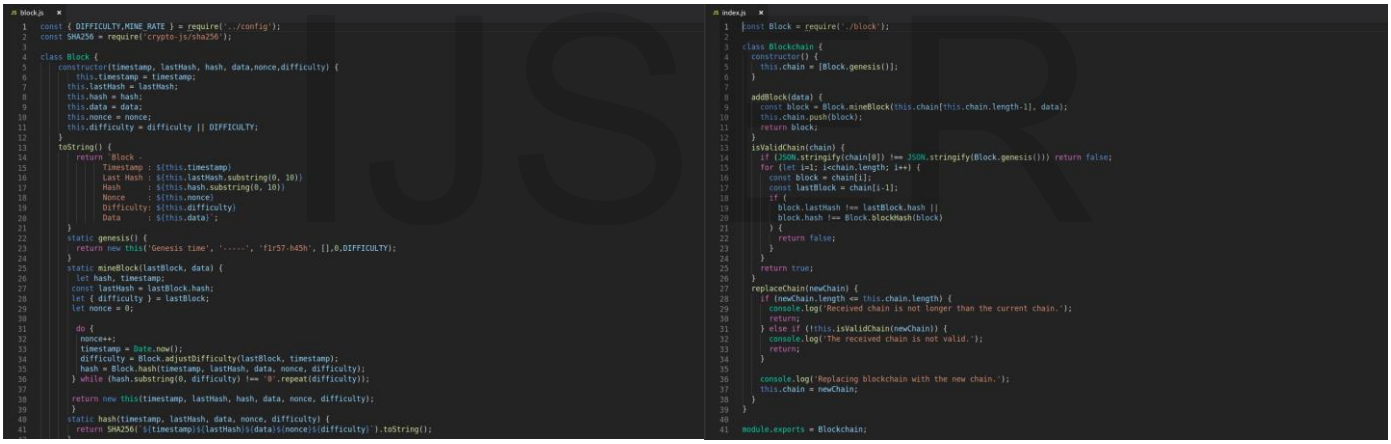


Fig. 8. **Smart lock system using blockchain**



```
const { DIFFICULTY,MINE_RATE } = require('../config');
const SHA256 = require('crypto-js/sha256');

class Block {
    constructor(timestamp, lastHash, hash, data,nonce,difficulty) {
        this.timestamp = timestamp;
        this.lastHash = lastHash;
        this.hash = hash;
        this.data = data;
        this.nonce = nonce;
        this.difficulty = difficulty || DIFFICULTY;
    }
    toString() {
        return `Block -
                Timestamp : ${this.timestamp}
                Last Hash : ${this.lastHash.substring(0, 10)}
                Hash      : ${this.hash.substring(0, 10)}
                Nonce     : ${this.nonce}
                Difficulty: ${this.difficulty}
                Data      : ${this.data}`;
    }
    static genesis() {
        return new this('Genesis time', '-----', 'f1r57-h45h', [],0,DIFFICULTY);
    }
    static mineBlock(lastBlock, data) {
        let hash, timestamp;
        const lastHash = lastBlock.hash;
        let { difficulty } = lastBlock;
        let nonce = 0;

        do {
            nonce++;
            timestamp = Date.now();
            difficulty = Block.adjustDifficulty(lastBlock, timestamp);
            hash = Block.hash(timestamp, lastHash, data, nonce, difficulty);
        } while (hash.substring(0, difficulty) !== '0'.repeat(difficulty));

        return new this(timestamp, lastHash, hash, data, nonce, difficulty);
    }
    static hash(timestamp, lastHash, data, nonce, difficulty) {
        return SHA256(`${timestamp}${lastHash}${data}${nonce}${difficulty}`).toString();
    }
```

```
const Block = require('./block');

class Blockchain {
  constructor() {
    this.chain = [Block.genesis()];
  }

  addBlock(data) {
    const block = Block.mineBlock(this.chain[this.chain.length-1], data);
    this.chain.push(block);
    return block;
  }
  isValidChain(chain) {
    if (JSON.stringify(chain[0]) !== JSON.stringify(Block.genesis())) return false;
    for (let i=1; i<chain.length; i++) {
      const block = chain[i];
      const lastBlock = chain[i-1];
      if (
        block.lastHash !== lastBlock.hash ||
        block.hash !== Block.blockHash(block)
      ) {
        return false;
      }
    }
    return true;
  }
  replaceChain(newChain) {
    if (newChain.length <= this.chain.length) {
      console.log('Received chain is not longer than the current chain.');
      return;
    } else if (!this.isValidChain(newChain)) {
      console.log('The received chain is not valid.');
      return;
    }

    console.log('Replacing blockchain with the new chain.');
    this.chain = newChain;
  }
}

module.exports = Blockchain;
```

```
    }
    static genesis() {
        return new this('Genesis time', '-----', 'f1r57-h45h', [],0,DIFFICULTY);
    }
    static mineBlock(lastBlock, data) {
        let hash, timestamp;
        const lastHash = lastBlock.hash;
        let { difficulty } = lastBlock;
        let nonce = 0;

        do {
            nonce++;
            timestamp = Date.now();
            difficulty = Block.adjustDifficulty(lastBlock, timestamp);
            hash = Block.hash(timestamp, lastHash, data, nonce, difficulty);
        } while (hash.substring(0, difficulty) !== '0'.repeat(difficulty));

        return new this(timestamp, lastHash, hash, data, nonce, difficulty);
    }
    static hash(timestamp, lastHash, data, nonce, difficulty) {
        return SHA256(`${timestamp}${lastHash}${data}${nonce}${difficulty}`).toString();
    }

    static blockHash(block) {
        const { timestamp, lastHash, data, nonce, difficulty } = block;
        return Block.hash(timestamp, lastHash, data, nonce, difficulty);
    }
    static adjustDifficulty(lastBlock, currentTime) {
        let { difficulty } = lastBlock;
        difficulty = lastBlock.timestamp + MINE_RATE > currentTime ?
        difficulty + 1 : difficulty - 1;
        return difficulty;
    }
}
module.exports = Block;
```

Fig. 9. **Screenshot of blockchain code**

a certain range and the special feature of this system is it is decentralized which provides with higher level of security this is done with the help block chain also a log of the entries is maintained.

- Also it provides security via generation of OTP and using RFID as extra layers.Initially a blockchain private network is setup between trusted users each user represents a node in the blockchain,when a new user approaches the network wishing to join it he presents his credentials to the raspberry pi,initially the raspberry pi switches on only when the ultrasonic sensor detects the person is within the acceptable range this is done to prevent remote hacking and any other form of misfeasance.
- Once the raspberry is turned on the user enters his

credentials and this is transmitted only to the people in the network,these people then implement consensus protocol,this means that each member validates the credentials thereby preventing any suspicious entry,Then these users generate a passkey which is then sent to the new user.

- Next time the user wants to gain access to this post he has to use his RFID key card,and also he will be getting an OTP in his registered device then he enters his passkey once he completes this process he is allowed entry to the port this entry is alerted to all the users in the network and logged in the ledger.
- This setup can be connected to an physical door or for virtual door to restrict access and maintaining a register that contains the details of access.

VIII. SHORTCOMINGS

- Scalability:Each time a new user is to be added other user have to be intimated though it increases the security by a huge margin,it can be done only when all the members approve it this may increase the time component.
- Storage:Since each member gets a copy of the log,though it prevents any loss of data it also requires storage space in multiple devices.
- 51 percent attack:If more than 50 percent of the nodes are compromised then they may be able to convert false inputs as true inputs and lead to manipulation of data.
- Complexity:Building an blockchain is not an easy task it takes months to build one from scratch and increase its difculty level by testing an d retesting.
- Network speed:Just as in any network dependant devices it depends on the network speed and capability.
- Unavoidable security aw:Even despite this cannot prevent human security threats,if anyone in the trust circle is compromised it may be vulnerable,though it is lesser than centralized networks since they can be immediately locked out by other members.
- Voltage fluctuations:Change in voltage may harm the electronic components and may damage them permanently.
- Physical damage:Just like any electronic devices these components are susceptible to physical damage.

IX. CONCLUSION

In this paper we have discussed developing and using blockchain to build a decentralized network and connecting it with a processor and hard-wares to design a more secure system which provides authentication via Consensus protocol,Security via cryptography,Data integrity via storing of data in each node.It also makes us of RFID,OTP and ultrasonic sensor to provide additional security.With increased research into blockchain and more financial support this system can be made more advanced.

X. FUTURE ENHANCEMENT

With increase in research in this technology and machine learning it may be incorporated with Better Scoring Mechanisms, Better Recommendation services, Predictive Forecasting, Risk assessment strategies,Hardware optimization and Community management etc.

Fig. 10. **Presenting RFID token**

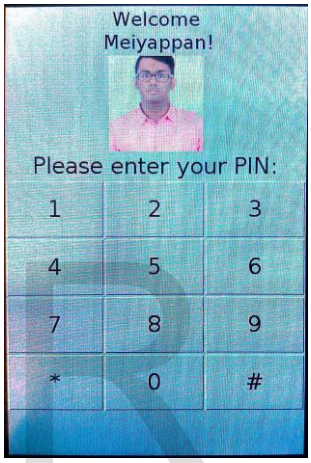


Fig. 11. **Entering unique ID**

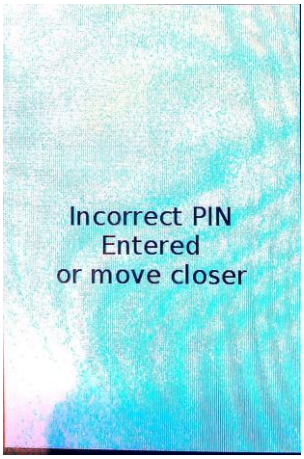


Fig. 12. **Message based on reading from sensor**

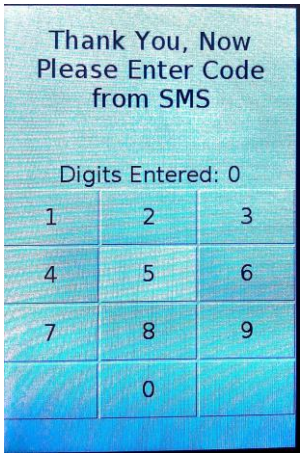


Fig. 13. **Entering OTP from the message**

Fig. 14. **After passing all 3 layers of security user sucessfully logged in**

XI. Results

As you can see in the figures numbered 10-14 the various steps involved in the system.These log in details are stored in the back end using blockchain.

References

[1] Solanke, N. Sonawane, V. Ugale and S. A. Khoje, Home Security Using Image Processing and IOT, International Journal of Emerging Technologies in Engineering Research,vol. 5, pp. 2326, June 2017.
[2] Sura Mahmood Abdullah, Design secured Smart Door Lock based on Jaro Winkler Algorithm, Tikrit Journal of Pure Science, vol. 21, pp. 154159, June 2016.
[3] O. Doh and I. Ha, A Digital Door Lock System for the Internet of Things with Improved Security and Usability, Advanced Science and Technology Letters, vol. 109, pp. 3338, August 2015.
[4] M. Crosby, Nachiappan, P. Pattanayak, S. Verma and V. Kalyanaraman.(2015). Blockchain Technology Beyond Bitcoin, Sutardja Center for Entrepreneurship Technology.
[5] K. Christidis and M. Devetsikiotis, Blockchains and Smart Constracts for the Internet of Things, IEEE Access, vol. 4, pp. 22922303, May 2016.
[6] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (accessed June 21, 2017).
[7] https://www.raspberrypi.org/help/videos/raspbiansetup
[8] I. D. Addo, S. I. Ahamed, S. S. Yau, and A. Buduru. A reference architecture for improving security and privacy in internet of things applications. In Mobile Services (MS), 2014 IEEE International Conference on, pages 108115. IEEE, 2014
[9] K. Ashton. That internet of things thing. RFiD Journal, 22(7):97114, 2009.
[10] M. Pilkington. (2016). Blockchain technology: Principle and applications, Research Handbook on Digital Transformations.