A Project Report on

Monitoring Health of IIOT Devices using Blockchain

Submitted in fulfillment of the requirements for the award
of the degree of

Bachelor of Engineering

in

Information Technology

by

Rutuja Patole(17104011)
Rushika Ramane(17104064)
Soundarya Nevrekar(17104066)

Under the Guidance of

Prof. Anagha Aher
Prof. Neha Deshmukh

Department of Information Technology
NBA Accredited
A.P. Shah Institute of Technology
G.B.Road, Kasarvadavli, Thane (W), Mumbai-400615
UNIVERSITY OF MUMBAI

Academic Year 2020-2021

Approval Sheet

This Project Report entitled ***"Monitoring Health of IIOT Devices using Blockchain"*** Submitted by ***"Rutuja Patole" (17104011),"Rushika Ramane" (17104064)*** and ***"Soundarya Nevrekar" (17104066)*** is approved for the fulfillment of the requirement for the award of the degree of ***Bachelor of Engineering*** in ***Information Technology*** from ***University of Mumbai***.

Prof. Neha Deshmukh
Co-Guide

Prof. Anagha Aher
Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Place:A.P.Shah Institute of Technology, Thane
Date:

CERTIFICATE

This is to certify that the project entitled ***"Monitoring Health of IIOT Devices using Blockchain"*** submitted by ***"Rutuja Patole" (17104011), "Rushika Ramane" (17104064), "Soundarya Nevrekar" (17104066)*** for the fulfillment of the requirement for award of a degree ***Bachelor of Engineering*** in ***Information Technology***,to the University of Mumbai, is a bonafide work carried out during academic year 2020-2021.

Prof. Neha Deshmukh
Co-Guide

Prof. Anagha Aher
Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Place:A.P.Shah Institute of Technology, Thane
Date:

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, We have adequately cited and referenced the original sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

_____

(Signature)

_____

Rutuja Patole (17104011)
Rushika Ramane (17104064)
Soundarya Nevrekar (17104066)

Date:

Abstract

Nowadays, we are encircled by countless IoT (Internet of Things) gadgets and sensors. These gadgets are intended to make life simpler and more agreeable. Blockchain innovation, particularly its mass application, is speedily developing into a profitable venture. A blockchain additionally called a circulated shared record, is a permanent information base of records by cryptography. It permits trade and capacity of computerized resources without the requirement for outsider oversight. Gadgets that download a setup record from an incorporated worker need to believe that power and in the event that it is undermined the gadget gets defenceless. With a blockchain, the requirement for focal authority is missing. Gadgets trade resources straightforwardly between one another. Reception of blockchain into big business networks actually has a couple of provokes that should be handled. Using blockchain can bring expanded security and proficiency of gadget upkeep. The vital component of the blockchain, immutability, carries protection from unapproved alterations. The entire history of gadget arrangement changes is put away in the blockchain, consequently recuperation after occurrences is exceptionally direct. Observing of gadget execution and traffic assumes working organization gadgets and their interconnection. Gadget and interface statuses should be followed for picking up an extensive review of organization conditions. This paper elaborates on monitoring the organization data and the idea is dependent on blockchain innovation. Organization heads control network gadgets by implicating by recording the change of gadget arrangement into the blockchain. The critical curiosity of our answer is a circulated executives of setup documents of IoT gadgets in big business networks using blockchain innovation. This is basically improving security and capacity alternatives for arrangements in the blockchain.

Contents

List of Figures

List of Abbreviations

IoT:	Internet of Things
IIoT:	Industrial Internet of Things
P2P:	Peer to Peer
PoW:	Proof of Work
ACL:	Access Control List
CIA:	Confidentiality, Integrity, Accesibility
AI:	Artificial Intelligence
BoSMoS:	Blockchain Based Status Monitoring System
S2Ghost:	Space-Structured Greedy Heaviest-Observed SubTree
JS:	JavaScript
JSON:	JavaScript Object Notation
HTML:	Hyper Text Markup Language
FBI:	Federal Bureau of Investigation
DHS:	United States' Department of Homeland Security
IBM:	International Business Machines

Chapter 1

Introduction

Two of the foremost charming technologies these days are unit blockchain and Internet-of-Things (IoT). The alliance concerning blockchain and IoT has nice prospects and can explore new ways in which of developing different applications in varied domains. Blockchain technology maintains a distributed and consistent ledger at each node among the network with none trusty the third party.

IIoT tools remain stationed inside firms to support production organizations (e.g. automotive) to obtain in-depth acumen into the diverse phases of production, and hence enhancing product competence and attaining price rebates. The foremost draw of IIoT devices is that they will improve safety, dependability, and energy efficiency. These devices integrate sensors that collect real-time or consecutive data and hook up with data analytics and control methods. As the number of combined devices increases, so do conceivably devastating cyber threats. Cyber threats on crucial infrastructure can have much more damaging and extensive effects.

In this article, we recommend a blockchain-based scheme used to monitor the well-being of IIOT devices. This method is devised to observe the software situation of IIoT instruments to identify and acknowledge unidentified spiteful operations (e.g. invasions). The software catches the snap from the device and stocks it in the database and monitors their files and the system calls. To make sure the software probity data, we use a blockchain because the distributed record stocks a snap of software state. The evaluation of monitoring, scalability, security, and accessibility exhibits that the method can provide deployment of large-scale IIoT tools also assure validated software updating, to recognize unlawful malicious software status.

Chapter 2

Literature Review, Project Conception and Initiation

2.1 Literature Review

2.1.1 BoSMoS

The paper titled A Blockchain-based Status Monitoring System for Defending against Unauthorized Software Updating in Industrial Internet of Things (2020) [1] was published by Sen He, and Wei Ren, Tianqing Zhu, Kim-Kwang, Raymond Choo

Approaches to consensus: Each proof of work consensus necessitates the validation of a block through nodes unveiling that they expect some work and are public to an arbitration of the effects. The task is typically a combination of intricate calculations on how nodes consent to the appropriate answer before annexing a block to the blockchain. This is frequently executed by miners and demands tons of computation power within the proof of stake consensus, nodes prove that they retain a stake on the Blockchain consequently approving of the accretion of the new block to the Blockchain. The aforementioned is usually achieved by owners of a stake inside the blockchain and isn't inevitably resource-intensive in terms of computation power.

Benefits: Ledger will be the system of record for the business - Transactions (asset transfer) and Contracts (conditions for a transaction to occur).

Drawbacks: The entire system may be malfunctioning, communication can be faulty.

2.1.2 Tornado

The article titled Tornado Enabling Blockchain in Heterogeneous Internet of Things through A Space-Structured Approach (2020) [2] published by Yinqiu Liu, Kun Wang, Kai Qian, Miao Du, and Song Guo

Internet of things has made its way as an emerging technology in many well-known sectors such as healthcare, industrial manufacturing, etc.
Generally, this technology is used in in-depth applications where there are issues related to

security, authorization, and certification.
The before-mentioned centralized approaches are profoundly exposed to Denial of Service, Sybil attacks, or tampering leading to the whole IoT network crashing. Deploying blockchain in such systems in an append-only database stored in a peer-to-peer (p2p) network, assuring data probity, non-tampering, and traceability.
Even after stationing blockchain in IoT there still endures many concerns which can't be completely diminished.
Thus to take care of the above problems the blockchain system with space-structured ledger architecture called Tornado to enable blockchain in IoT was developed. They have used the collaborative proof of work consensus algorithm and along with it is the protocol known as Space-Structured Greedy Heaviest-Observed SubTree (S2Ghost). This protocol secures the uprightness of data and devices.

Benefits: Enhanced connectivity with partners, customers, suppliers.

Drawbacks: Differentiated mining difficulty, Parallel workflows.

2.1.3 Towards Secure Industrial IoT

The paper titled Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism (2019) [3] was published by Junqin Huang, Ling Kong, Guihai Chen, Min-You Wu, Xue Liu, Peng Zeng

The integration of IoT and blockchain helps us achieve many factors such as data integration, authorization, and scalability. But still, there are many challenges to be addressed.

Major issues include the trade-off between efficiency and security where the consensus algorithm comes into the picture to defend against malicious attacks but results in overloaded IoT devices.Then comes the issue related to privacy and transparency where the data collected is sensitive and needs to be only viewed by the authorized users.
Lastly the concern with high concurrency and low throughput where the throughput of blockchain is limited by various mechanisms.

To deal with all these matters a blockchain system with a credit-based consensus mechanism for IIoT was proposed. This paper deals with all the three major concerns mentioned above by proposing a general, scalable and secure blockchain system for IIoT, where we outline a moderate-cost credit-based PoW mechanism and a sufficient access control system for power-constrained IoT devices.

Benefits: It has immensely helped to further strengthen the industrial systems by offering benefits like secure data sharing, privacy preserving data aggregation, data confidentiality etc.

Drawbacks: Single point failure, Sybil attack and tampering of data.

While blockchain credentials continue being broadly extended, multiple concerns should still be discussed. Through this, blockchains will enhance not only extra scalable and skilled

but more strong as well. The characteristics they contribute are exceptional if arbitrated independently, including the majority of the devices people imply are recognized for years. Despite, the combining of all these traits makes them perfect for many applications acquitting the intense interest of several industries.

2.2 Existing System

The existing security measures undertaken by corporations deploying IIoT are:

2.2.1 Risk assessment models

Before installing and operating IIoT systems, a risk assessment model should be employed to identify all the digital and physical components to be protected. Through vulnerability and risk assessments all risks should be discovered and classified as acceptable or unacceptable. Risk assessments should continue on an annual basis with periodic reviews.

2.2.2 Segmentation

IIoT systems should be divided into sub systems which have common security requirements, and then logically isolated from each other. Information flow and access is restricted and protected using firewalls, ACLs, VLANs etc. Partitioned networks also boost system performance and improve efficiency by controlling traffic and reducing complexity.

2.2.3 Device integrity and availability

The CIA triad is a widely accepted industry standard that is implemented by most organisations to develop their security policies and protect their interests.
CIA stands for

- Confidentiality: Only authorised personnel and processes have access to data of their corresponding security level.
- Integrity: Data should maintain its intended form and should be protected from unauthorised modification or deletion.
- Availability: Authorised personnel and processes should be able to access data as per their requirement.

Using CIA models, devices and components that are classified as critical are protected with mechanisms that provide support to them.

2.2.4 Encryption

The IIoT systems must employ up to date cryptography protocols and support advanced forms of encryption. Many industrial protocols currently in use were not designed with security in mind and lack basic authorization and encryption features. Data is at risk at both rest and in transit.

2.2.5 Privacy

Encryption of confidential data needs to be ensured through widely used security protocols to ensure privacy in transit as well as storage. Data leaks, whether due to unintentional errors or malicious tampering, could lead to great loss of capital and must be avoided at all costs.

2.3 Problem Statement

As more and more industries plan to incorporate IIoT devices to perform various services, the need to secure the data generated because of this arises with greater urgency. The requirement of the market is such that all parties involved in such an industry collaboration, which do not necessarily trust each other, can rely on a secure system to ensure their interests are being protected. Even minor mishaps could result in loss of sensitive data, or capital. The security measures currently being taken are not very effective due to the complexity of IIoT networks.

The threat of a cyber attack on IIoT networks isn't hypothetical, as hackers have already deployed malware to exploit inter connected sensors and gained access to private networks. Globally, industries face critical threats to their infrastructure because of unauthorised intrusions intending to disrupt, degrade, or destroy systems. Industrial operations were forced to close down in the Middle East due to use of a malware called Triton, a new type of Trojan. Power was also shut off in a region of Ukraine due to hackers. Numerous attacks have been observed to be the work of Russian, US, Iranian, North Korean, Chinese and Israeli organisations. Corporations from the sectors of energy, water, aviation, and manufacturing are at risk of having their data stolen, according to the FBI and US Department of Homeland Security (DHS). [3] [4]

Even so, companies like Cisco Systems, IBM Corporation, Intel Corporation, and many others in the market wish to connect millions of IIoT devices to analyse data and optimise business processes. By utilising IIoT devices, it would be possible to offer products as services. However, to bring this idea to fruition, it is essential to absolutely eliminate all present risks and vulnerabilities to create an airtight network that cannot be broken into.

We intend to do exactly that by creating a reliable product that makes use of blockchain technology. Our aim is to protect smaller scale industries from encountering disaster in their regularly scheduled operations by continuously monitoring activities and making sure that procedures are being carried out as intended.

Chapter 3

Project Design

3.1 Objectives

3.1.1 Accuracy

To ensure the precision of the monitoring module, wrong negative values and wrong positive values can have a severe influence on the whole network.

3.1.2 Monitoring

The monitoring module is supposed to identify the alteration of the current status of the target program and alert the admin terminal.

3.1.3 Security

To guarantee the elimination of any vulnerabilities of the blockchain network to avoid the framework from being damaged by attackers.

3.1.4 Soundness

To ensure that other nodes interacting with the node are genuine, the other nodes will acknowledge the node's request and direct the intended information to the trusted block.

3.1.5 Scalability

To grant access to a huge number of nodes to connect or exit the network and their presence and actions won't cause discrepancy within the network.

3.2 Proposed System

By observing the status of it, the product holds the trustworthiness of the app. The program's status data contains data on computer program judgment and record data that's critical to the program. By comparing reliable program status depictions, the gadget can decide program status and will alarm the chairman in the event that the status changes. The fundamental components of the item would be:

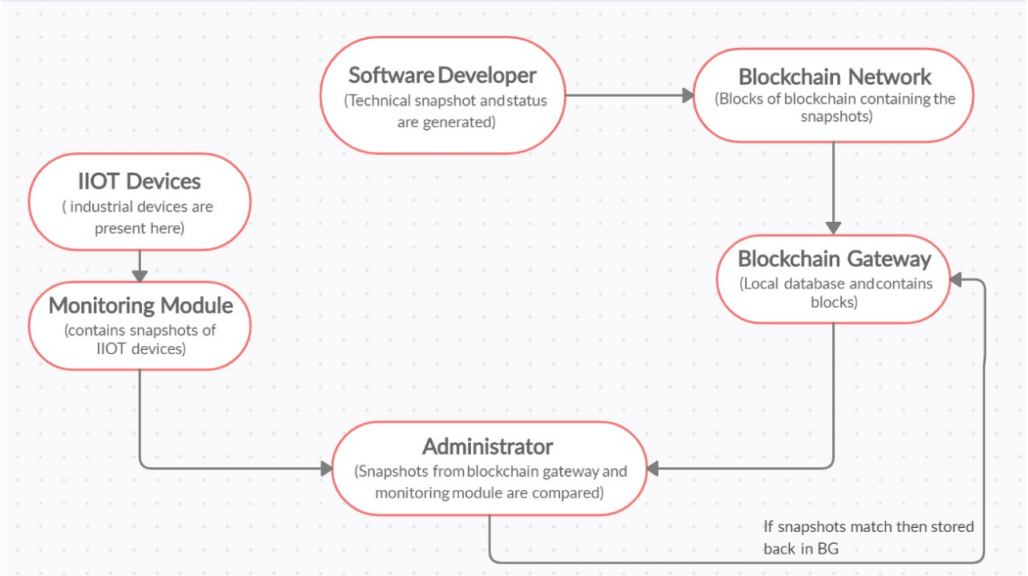

Figure 3.1: Proposed System Working

3.2.1 Software Developer

The software developers make dependable computer program mechanical status depictions and each keeps up a blockchain node. On the off chance that an unused form or computer program overhaul is discharged, a status depiction must be taken. The snapshot, along with the package and public key, is to be broadcast on the blockchain organize and marked with the developer's private key.

3.2.2 Blockchain Network

It is utilized to store trusted program specialized status depictions as a trusted, decentralized, distributed database. It incorporates total gateways and blockchain nodes. The network is overseen by the complete nodes and communicates through the P2P convention. Depictions would not be altered with within the blockchain organize and are dependable gadget following sources.

3.2.3 Blockchain Gateway

For IIoT gadgets, they give blockchain information and react to block requests. They support IIoT devices to get reliable information from the blockchain. They don't create new blocks, but new blocks are obtained, checked, and processed.

3.2.4 IIoT Devices

The key tracking modules are IIoT devices. The same observing module is run by all the gadgets, including blockchain portals and total nodes. In any case, IIoT devices do not contribute to the blockchain network like any other node. They don't hold attained blockchain records, but they store the same hash values. Block Information is sought from the blockchain gateways.

3.2.5 Monitoring Module

It chooses the program status by means of comparing gadget previews and recording record framework calls. The results will be submitted to the admin terminal. When permitted by the rules set by the admin, it'll hinder the anomalous program by itself.

3.2.6 Administrator

The Administrator gets status data that the company keeps up in genuine real-time for all IIoT gadgets, blockchain gateways, and total nodes.

Chapter 4

Project Implementation

We utilise IBM Watson IoT platform as the basis of this project. We have simulated IoT devices with parameters of Temperature and Humidity. A Node-Red Flow of the same was consequently built, and the data generated is stored in the Cloudant database, which is available within IBM facilities.

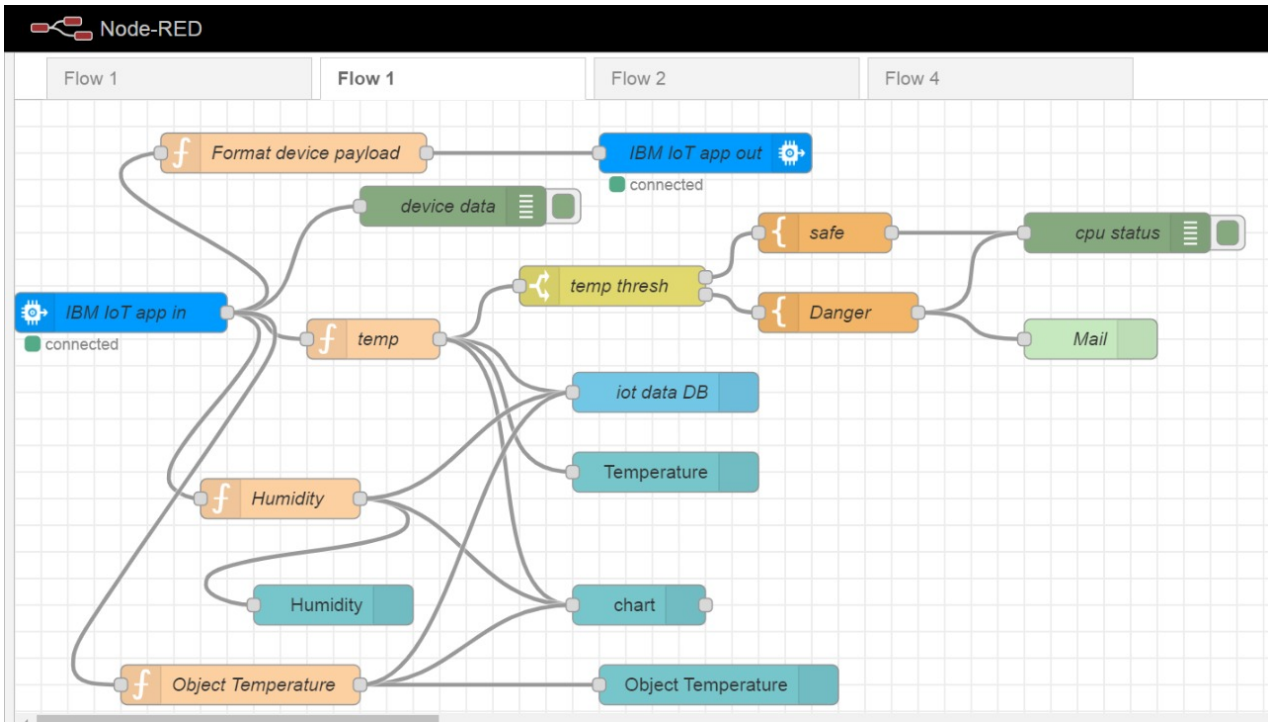

Figure 4.1: Node-Red Flowchart

The first node of the above Flow is the IBM IoT App In. It acts as the input node for the entire flow. We have chosen the Quickstart service for the configuration. It links the virtual IoT device with the Node-Red Flow through the unique Device ID.

This first mode is further connected to three function nodes, “temp,” “Humidity” and “Object Temperature,” which display the payload message obtained from the device onto the Debug window. The “temp” node is connected to a switch node, “temp thresh” which

leads to two more nodes, “safe” and “danger”. They denote whether the input temperature is classified to be in the safe zone or if the situation is critical.

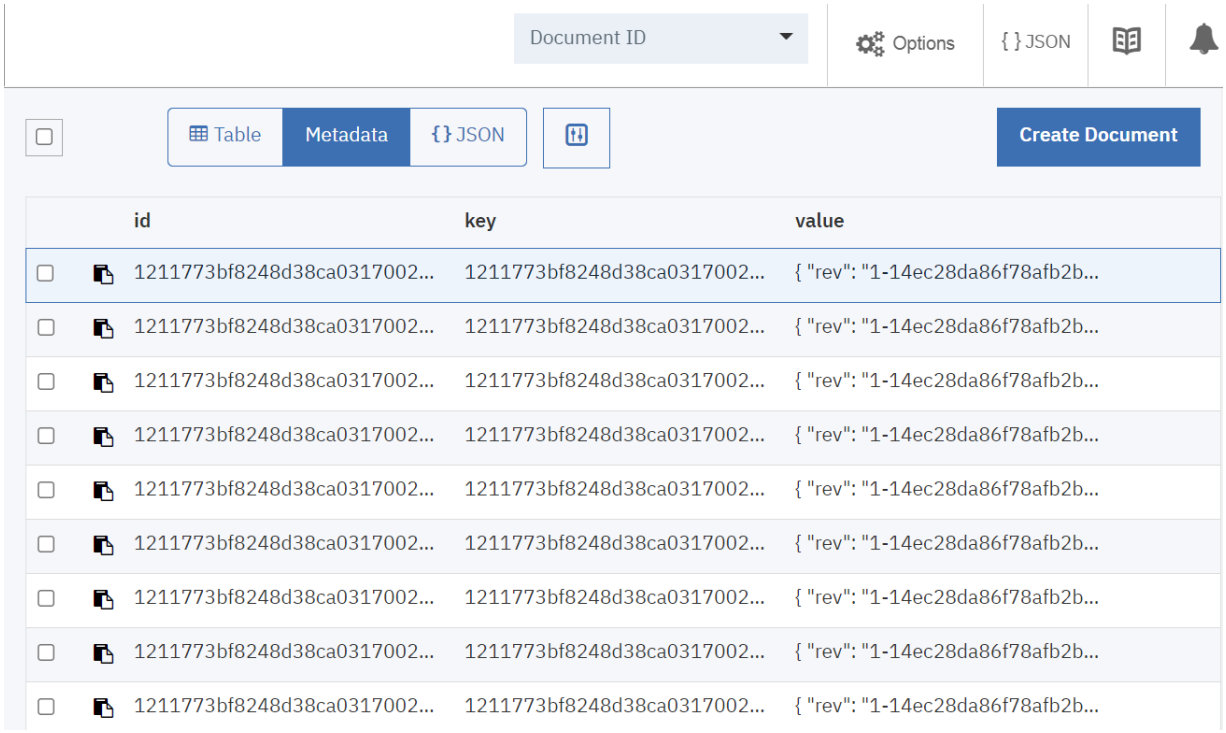

Figure 4.2: IoT Cloudant Database: Overview

The next node is IoT Data DB which acts as the Database for this system. Upon linking the Node-Red App with the Cloudant Database, two procedures called Building and Staging were carried out, resulting in a combined service. This same service was used to configure the node, to ensure that the data would be stored in the Cloudant Database. The operation specified was Insert.

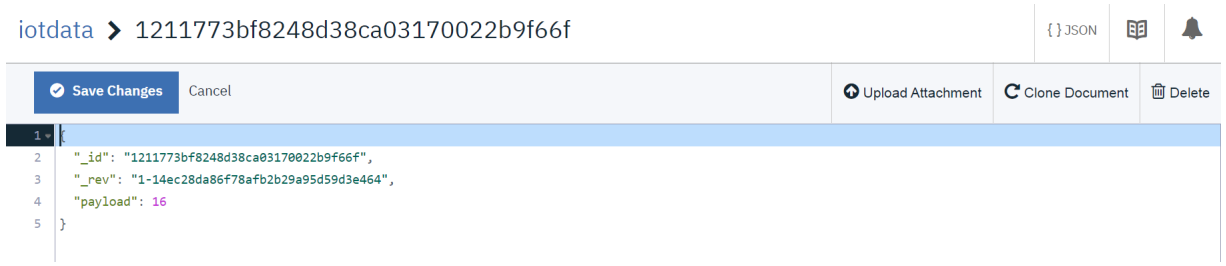

Figure 4.3: IoT Cloudant Database: Temperature Properties

The Translator node is responsible for converting the input source language into the target language.

The following nodes, Device Data, CPU status, and Msg Payload, display the result in the Node-Red Debug window.

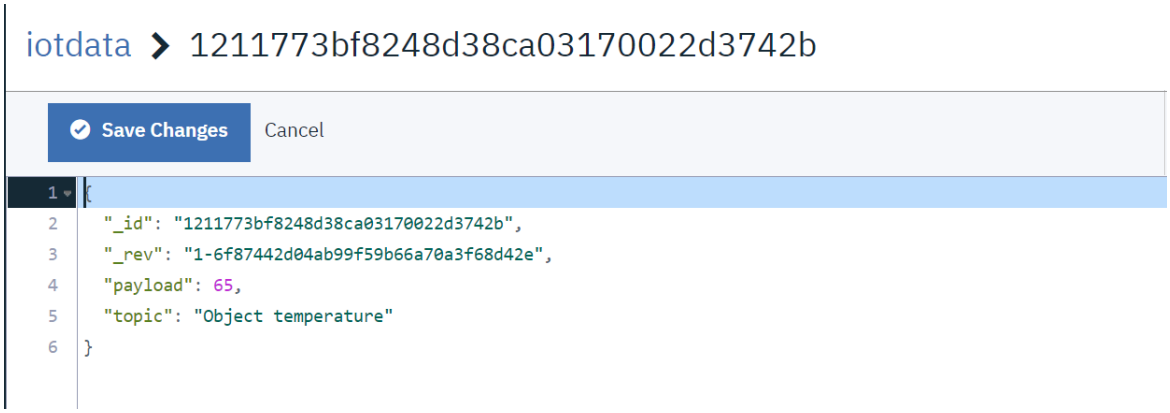

Figure 4.4: IoT Cloudant Database: Object Properties

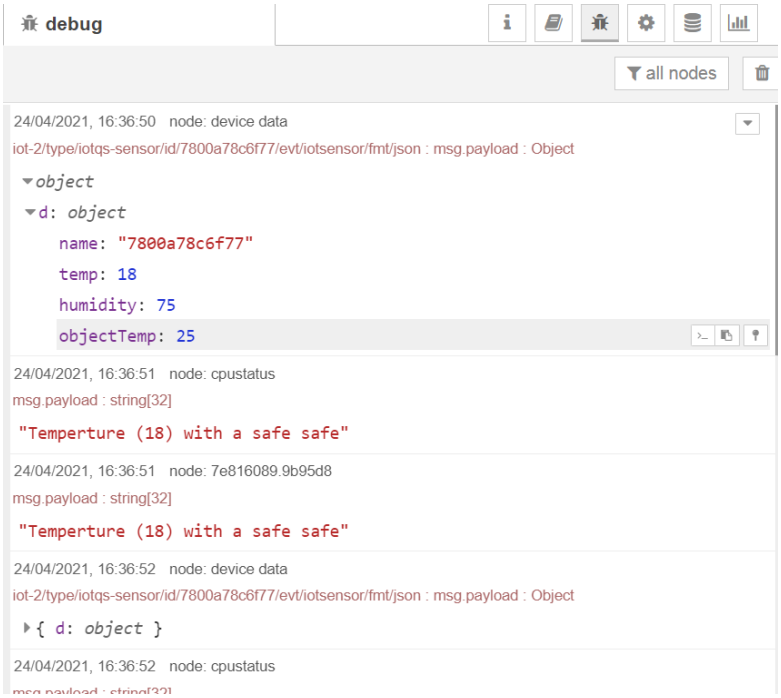

Figure 4.5: Debug Window

The IBM Watson platform offers a Text to Speech service, which when linked with the Node-Red platform converts the Alerts generated by the process from text to speech. An Alert node is present in the given flow, which notifies the user in case the device temperature has risen above the specified limit. Mails detailing the current status of the system are sent periodically to the Administrator to keep her up to date.

The Test Text Change node performs the task of transforming the message received from its predecessor into a new one before passing it forward towards the Msg Payload node.

The Node-Red platform also provides the Dashboard functionality, where the current status of the device parameters is graphically represented for easier understanding. The user is free to choose between various styles of data display, with colours giving additional information regarding how close the system is to the danger zone. With the comparison

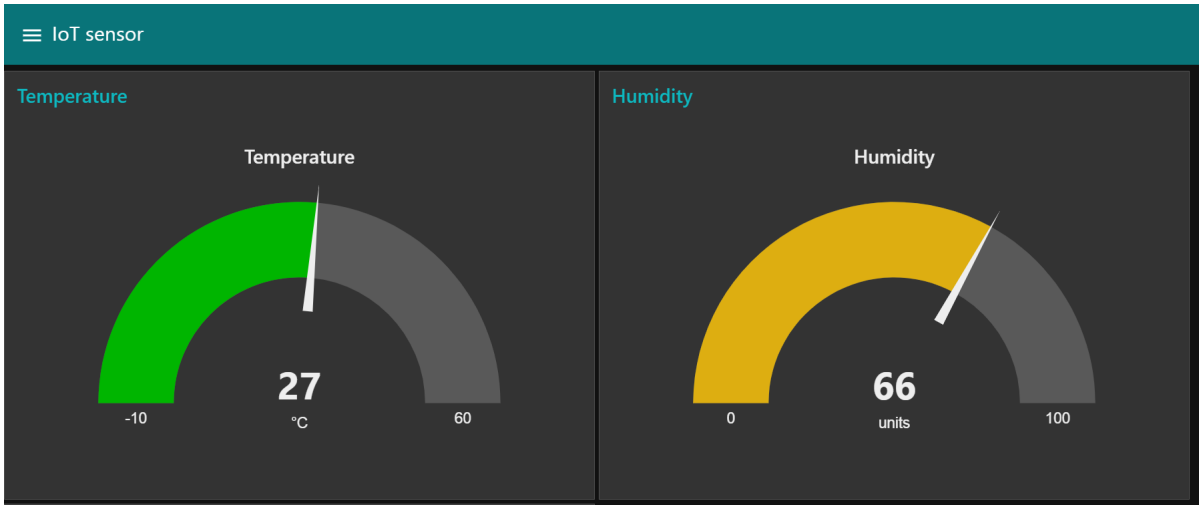

Figure 4.6: Dashboard: Humidity and Temperature

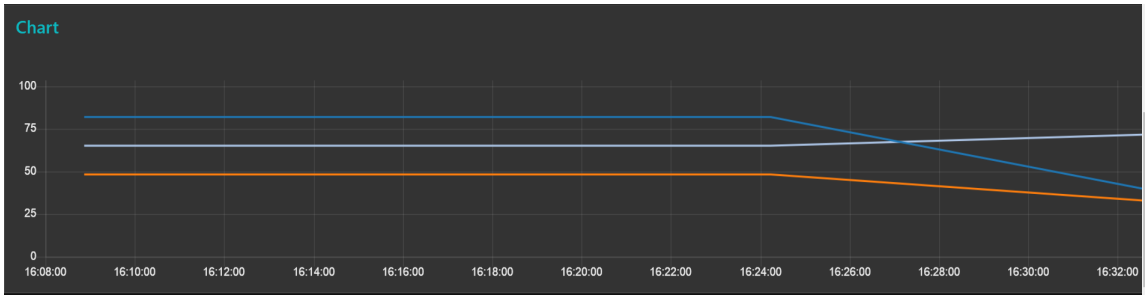

Figure 4.7: Dashboard: Comparison Chart

chart showing all relevant factors together along with timestamps, one can easily deduce and pinpoint major changes occurring in the device's environment.

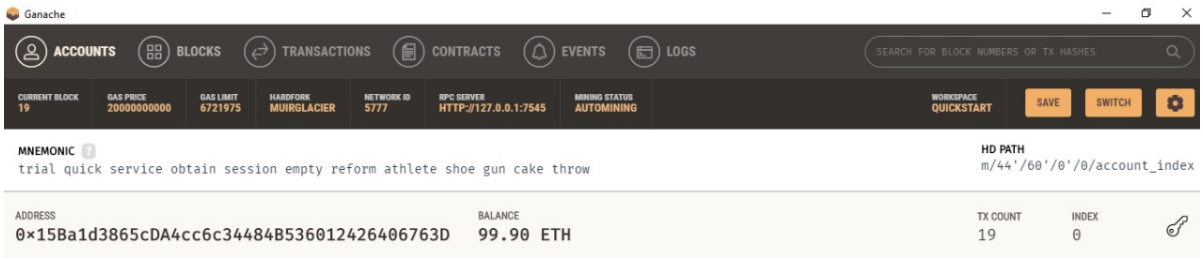

Figure 4.8: Ganache Account

When a blockchain is created, the created blocks, address and occurred transactions are visible in the specified Ganache windows.

Ganache is a personal blockchain for rapid Ethereum distributed application development. We used Ganache across the entire development cycle; enabling you to develop, deploy, and test your dApps in a safe and deterministic environment.

We are able to set the values of server address and the port number for the Ganache

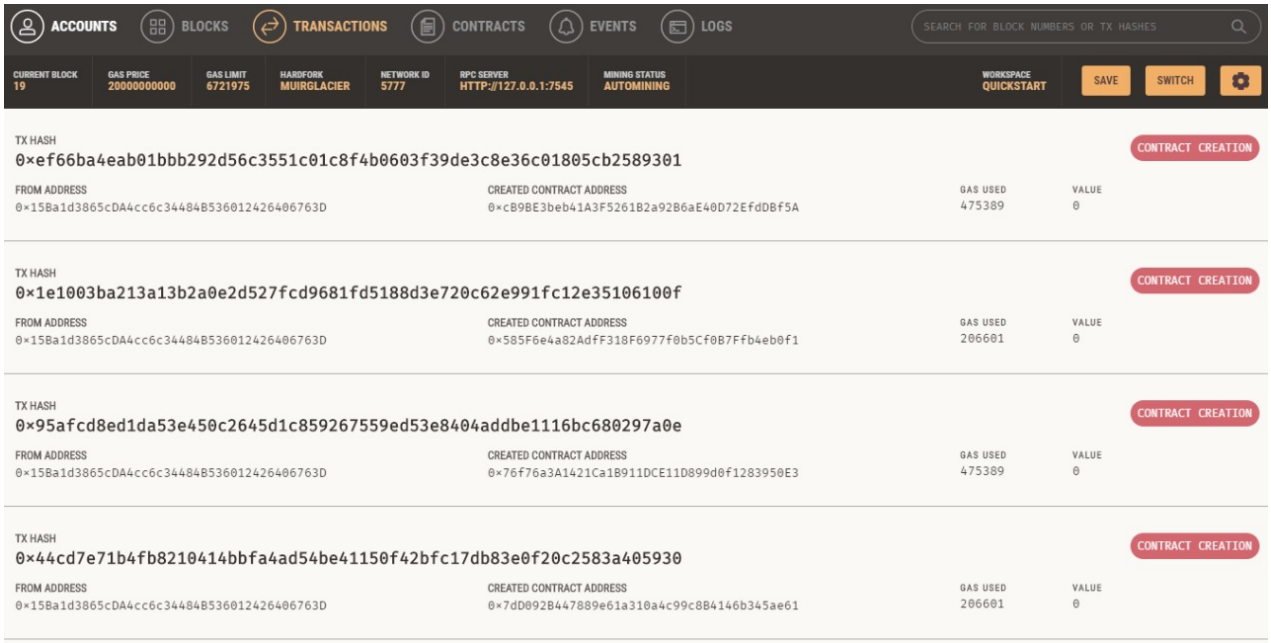

Figure 4.9: Ganache Transcations

server. The Network ID is an internal Blockchain identifier of Ganache server that we have specified in our code. The Automine button is in the ON state indicating that the transactions would be processed instantly.

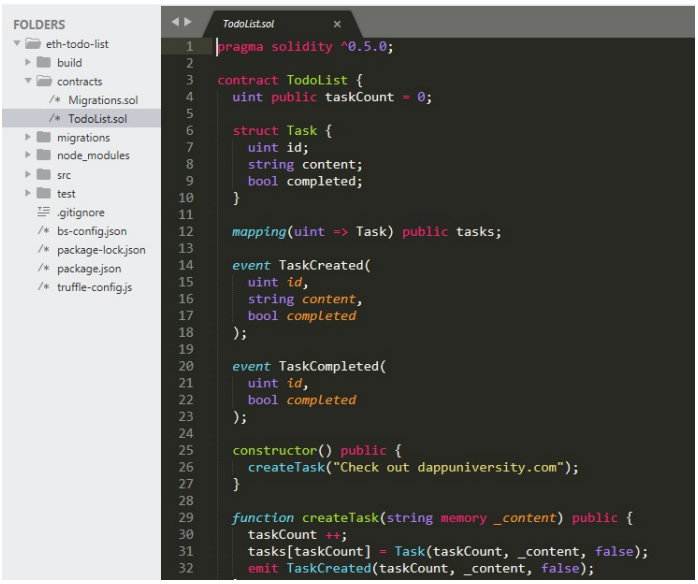

Figure 4.10: Solidity Code

A smart contract is created in the Solidity language. The following needs to be carried out:

- List tasks in the smart contract
- List tasks in the console

- List tasks in the client side application
- List tasks in the test cases

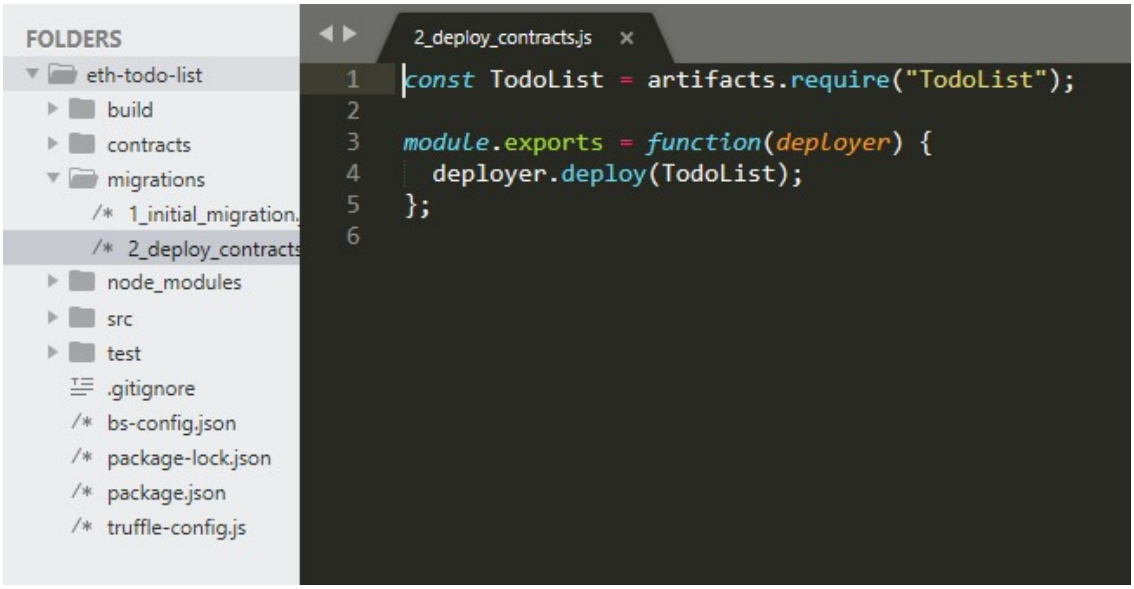

Figure 4.11: Migrations

We use the migration file to get the smart contracts out of the blockchain to deploy. The state of the blockchain is also updated.

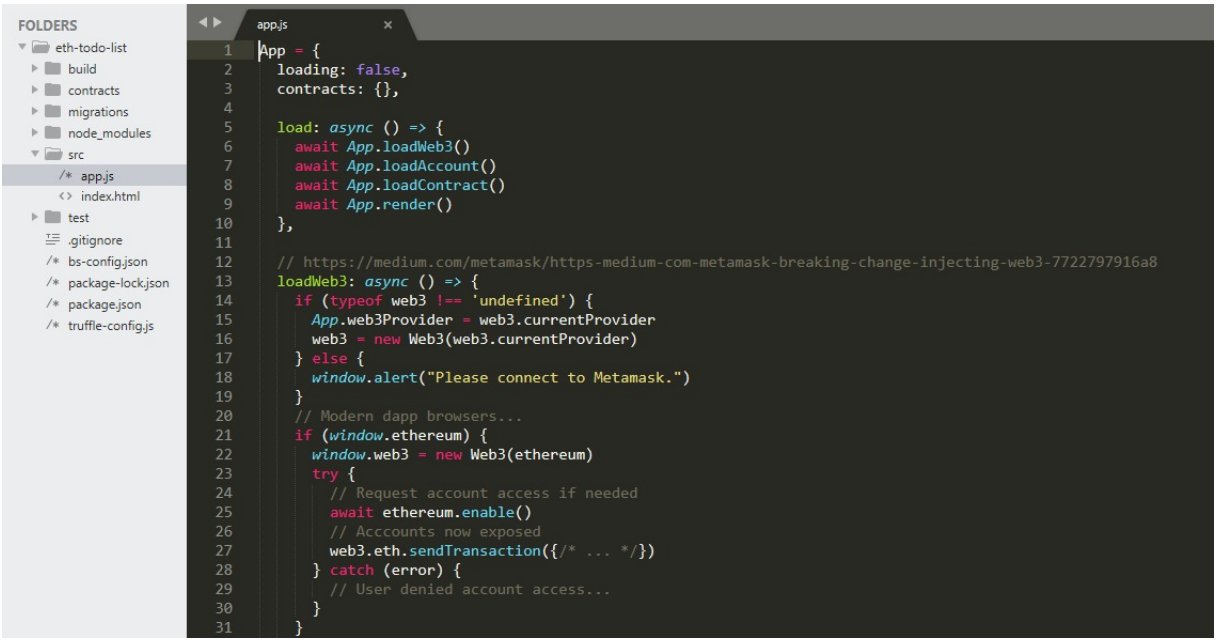

Figure 4.12: Application JS

The Application JS has the driver script of the app attached to the blockchain. It loads the app and connects it to the client side application with Web3.js. To display the client

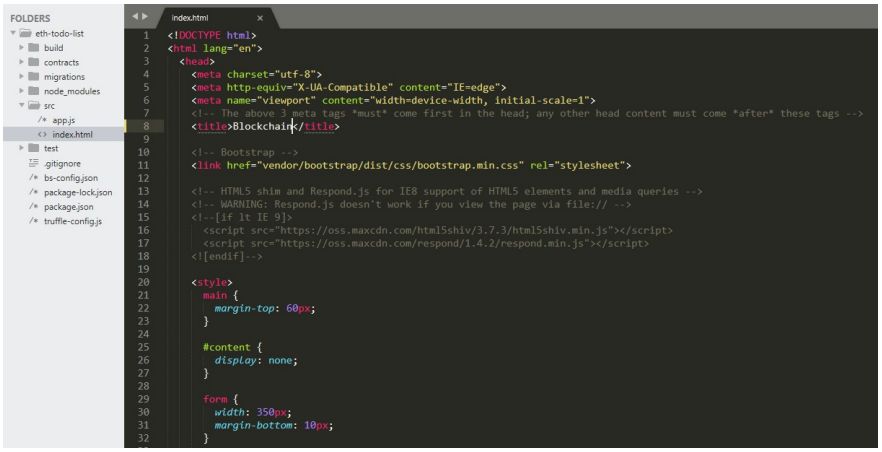

Figure 4.13: HTML Code

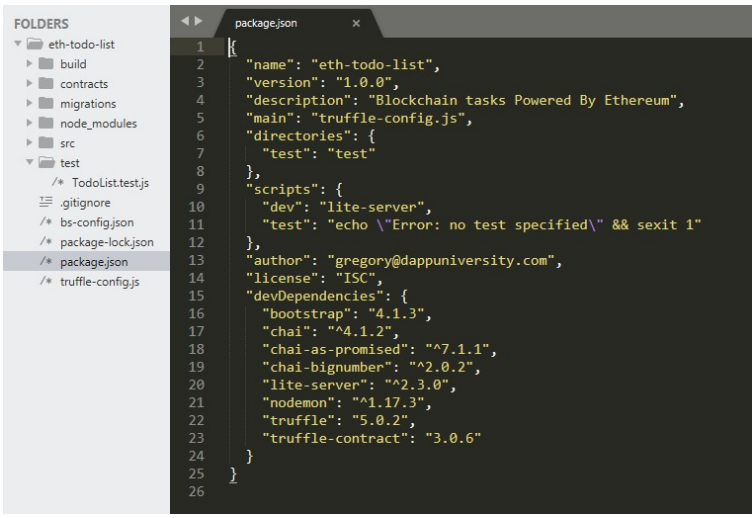

Figure 4.14: JSON Package

side application, we make use of HTML, Bootstrap framework and CSS.

The JSON package lists the dependencies required for the project. It can be performed by using the npm install command.

The truffle-config.js file is responsible for specifying the network required to connect to Ganache, with localhost and port number 7545.

Both Ganache and Truffle Develop are significantly faster than other clients when running automated tests. Moreover, they contain special features which Truffle takes advantage of to speed up test runtime by almost 90 percent.

For the development of the smart contracts Truffle is utilised. It offers some degree of automation for compiling, deploying, and testing smart contracts.

As a general workflow, we recommend you use Ganache or Truffle Develop during normal development and testing, and then run your tests once against official Ethereum client.

```
1_initial_migration.js
======================

   Deploying 'Migrations'
   ----------------------
   > transaction hash:    0x1e1003ba213a13b2a0e2d527fcd9681fd5188d3e720c62e991fc12e35106100f
   > Blocks: 0            Seconds: 0
   > contract address:    0x585F6e4a82AdfF318F6977f0b5Cf0B7Ffb4eb0f1
   > account:             0x15Ba1d3865cDA4cc6c34484B536012426406763D
   > balance:             99.91376968
   > gas used:            206601
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00413202 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00413202 ETH


2_deploy_contracts.js
=====================

   Replacing 'TodoList'
   --------------------
   > transaction hash:    0xef66ba4eab01bbb292d56c3551c01c8f4b0603f39de3c8e36c01805cb2589301
   > Blocks: 0            Seconds: 0
   > contract address:    0xcB9BE3beb41A3F5261B2a92B6aE40D72EfdDBf5A
   > account:             0x15Ba1d3865cDA4cc6c34484B536012426406763D
   > balance:             99.9042619
   > gas used:            475389
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00950778 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00950778 ETH
```

Figure 4.15: Deploying Smart Contract

In the Command Prompt, we can see the migration being reset, and return to the beginning of the process by choosing the Reset option. We also test this blockchain on Ganache locally.

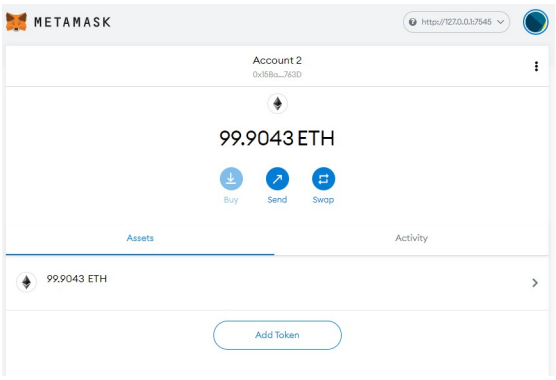

Figure 4.16: Metamask

By importing a private key, we can connect to Metamask through Ganache. Metamask eases communication between web applications with Ethereum Blockchain.

Chapter 5

Testing

We created a test directory and a test file to test smart contracts before deploying. Inside this file, we can scaffold a test for the smart contract with the help of the Chai assertion library that comes bundled with the Truffle framework.

```
const SocialNetwork = artifacts.require('./SocialNetwork.sol');

require('chai').use(require('chai-as-promised')).should()

contract('SocialNetwork', ([deployer, author, tipper]) => {
    let socialNetwork

    before(async () => {
        socialNetwork = await SocialNetwork.deployed()
    })

    describe('deployment', async () => {
        it('deploys successfully',  async () => {
            const address = await socialNetwork.address
            assert.notEqual(address, 0x0)
            assert.notEqual(address, '')
            assert.notEqual(address, null)
            assert.notEqual(address, undefined)
        })

        it('has a name', async () => {
            const name = await socialNetwork.name()
            assert.equal(name, 'This is my post')
        })
    })

    describe('posts', async () => {
        let result, postCount

        before(async () => {
            result = await socialNetwork.createPost('This is my first post', { from: author })
            postCount = await socialNetwork.postCount()
        })
```

Figure 5.1: Including Libraries

This basic test checks for 2 things: The smart contract was successfully deployed, i.e., it has an address and The name is correct, i.e., "This is my first post". The operations in the test file should be same as that of the operations in the console after we deployed the very

first smart contract.

```
it('creates posts', async () => {

    assert.equal(postCount, 1)
    const event = result.logs[0].args
    assert.equal(event.id.toNumber(), postCount.toNumber(), 'id is correct')
    assert.equal(event.content, 'This is my first post', 'Content is correct')
    assert.equal(event.tipAmount, '0', 'tip amount is correct')
    assert.equal(event.author, author, 'author is correct')

    await socialNetwork.createPost('', { from: author }).should.be.rejected;
})

it('lists posts', async () => {
    const post = await socialNetwork.posts(postCount)
    assert.equal(post.id.toNumber(), postCount.toNumber(), 'id is correct')
    assert.equal(post.content, 'This is my first post', 'Content is correct')
    assert.equal(post.tipAmount, '0', 'tip amount is correct')
    assert.equal(post.author, author, 'author is correct')
})
```

Figure 5.2: Creating Posts

This test checks for all the behavior we just added:
It checks that the post count was incremented, and that is now equal to 1.

Then, it digs into the transaction logs to inspect the post value from the event that we triggered inside the function. We check that the post id, content, tip amount, and author are correct.

Finally, we check that the function rejects posts that don't have any content.

Also, we modified the test suite to include 3 different users: deployer, author, and tipper.

We can do this instead of using the accounts variable that was injected by default.

First, we fetch the post from the blockchain and store a new copy in memory.

Next, we store the post author to a variable.

Then, we send the cryptocurrency to the author with the transfer function. Solidity allows us to read the cryptocurrency value with the special msg.value variable. Next, we increment the tip amount for the post.

Finally, we save the updated post values by adding it back to the mapping, and storing it on the blockchain.

```
        it('allows users to tip posts', async () => {

            let oldAuthorBalance
            oldAuthorBalance = await web3.eth.getBalance(author)
            oldAuthorBalance = new web3.utils.BN(oldAuthorBalance)

            result = await socialNetwork.tipPost(postCount, { from: tipper, value: web3.utils.toWei('1', 'Ether') })

            const event = result.logs[0].args
            assert.equal(event.id.toNumber(), postCount.toNumber(), 'id is correct')
            assert.equal(event.content, 'This is my first post', 'Content is correct')
            assert.equal(event.tipAmount, '1000000000000000000', 'tip amount is correct')
            assert.equal(event.author, author, 'author is correct')

            let newAuthorBalance
            newAuthorBalance = await web3.eth.getBalance(author)
            newAuthorBalance = new web3.utils.BN(newAuthorBalance)

            let tipAmount
            tipAmount = web3.utils.toWei('1', 'Ether')
            tipAmount = new web3.utils.BN(tipAmount)

            const expectedBalance = oldAuthorBalance.add(tipAmount)

            assert.equal(newAuthorBalance.toString(), expectedBalance.toString())

            await socialNetwork.tipPost(99, { from:tipper, value: web3.utils.toWei('1', 'Ether') }).should.be.rejected;

        })
    })
})
```

Figure 5.3: List and Tip Posts

We then run the tests. If the test give us the success message in the console, it means we have deployed the smart contract correctly. One the smart contract is deployed , we can't change it or modify it.

Chapter 6

Result

If the system detects anomalies in the device's temperature readings, immediately mails are dispatched to the Administrator, alerting her of the situation. Further action is up to the Administrator on how to handle it.

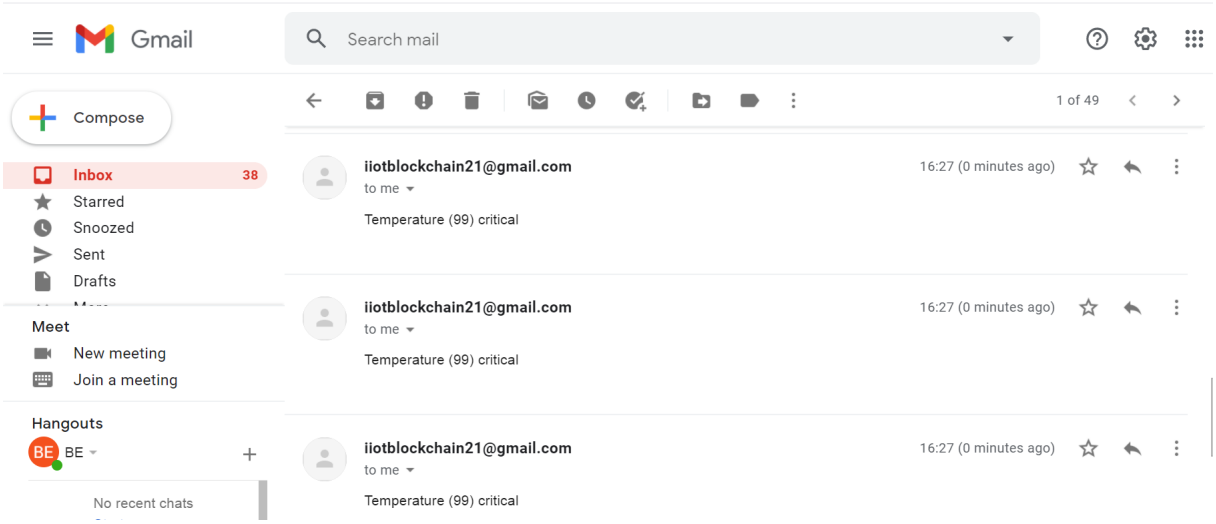

Figure 6.1: Mail Notifications

The Administrator can use the blockchain functionality to manually add the verified device temperature readings.

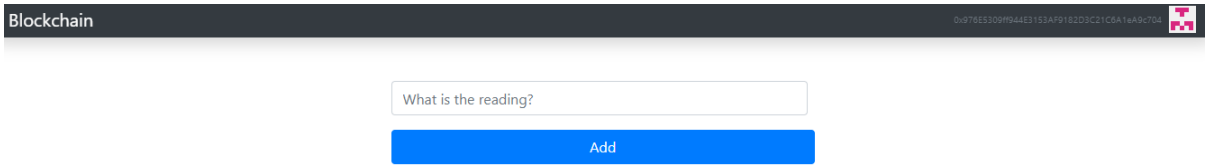

Figure 6.2: Blockchain Home Display

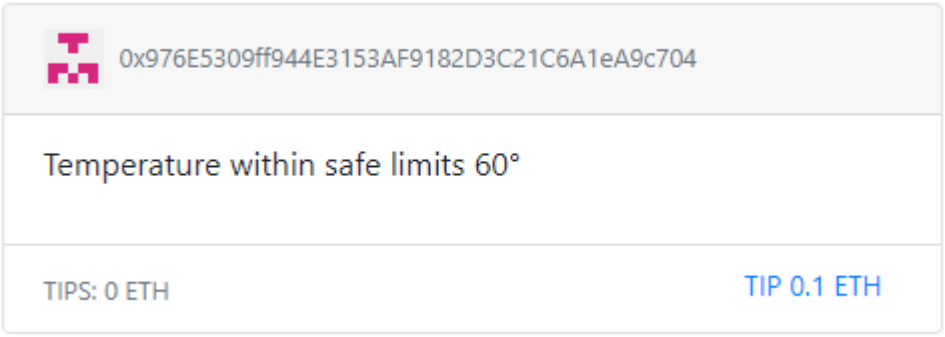

Figure 6.3: Reading is added into Blockchain

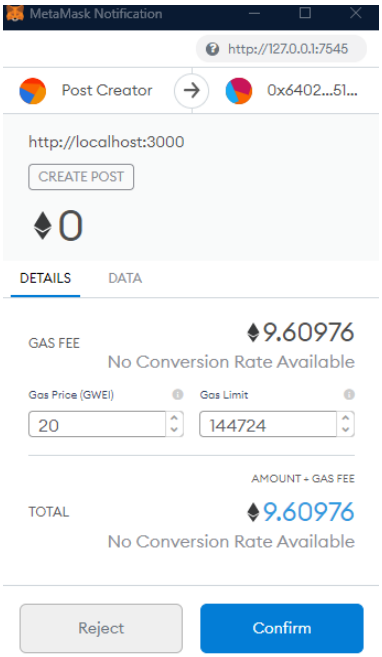

Figure 6.4: MetaMask Transaction

The readings included by the Administrator are displayed on the same.

MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows us to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

MetaMask and other "web3" focused applications aim to decentralize control over personal data and increase user privacy.

It can connect to the main Ethereum network, any of the testnets (Ropsten, Kovan, and Rinkeby), or a local blockchain such as the one created by Ganache or Truffle Develop. MetaMask injects its own web3 instance.

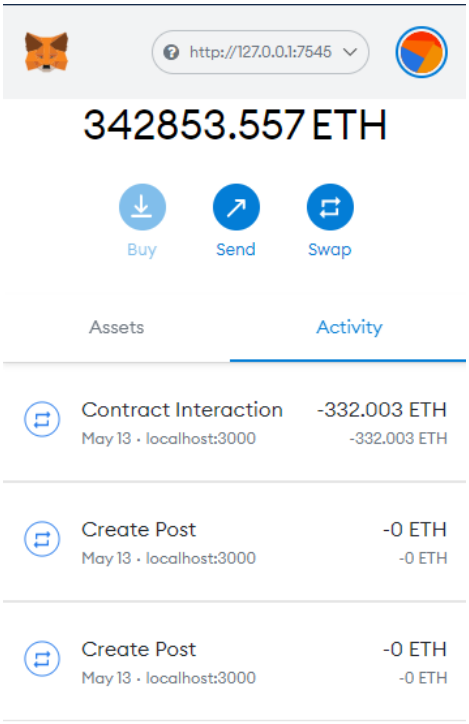

Figure 6.5: MetaMask Wallet Activity

Before we interact with smart contracts in a browser, we make sure they're compiled, deployed, and that you're interacting with them via web3 in client-side JavaScript.

To perform the above action, a specified gas fee of 20 GWEI is required by the MetaMask Wallet.

The resulting transaction details are noted in the MetaMask Wallet's Activity section for that particular user account.

Chapter 7

Conclusions and Future Scope

This project intends to make a way for IoT devices to achieve industrial-grade accuracy for information transfer from remote sensing systems to AI systems using blockchain technologies. Consistently, updated security and reliability of acknowledged data inside the IoT network might be resolved on an application level. Therefore, a light-weight and effective communication protocol supporting blockchain principles was devised. This paper focuses on this relationship, examines challenges in blockchain IoT applications, and inspects the foremost appropriate work to research how blockchain could conceivably improve the IoT.

Future expansions incorporate planning a reasonable consensus algorithm for this scheme and deploying the amplified framework in reality. The sensor data quality control plans in blockchain-based frameworks can be investigated. Implementation of incentive mechanism will offer assistance proving the reliability of IIoT devices. With suitable incentives, IIoT devices, particularly power-sufficient machines, will contribute to computing power in maintaining the ledger. A world of large scale industrial collaborations where substantial amounts of data can be processed safely is envisioned.

Bibliography

[1] S. He, W. Ren, T. Zhu and K. R. Choo, "BoSMoS: A Blockchain-Based Status Monitoring System for Defending Against Unauthorized Software Updating in Industrial Internet of Things," in IEEE Internet of Things Journal, Feb 2020

[2] Y. Liu, K. Wang, K. Qian, M. Du and S. Guo, "Tornado: Enabling Blockchain in Heterogeneous Internet of Things Through a Space-Structured Approach," in IEEE Internet of Things Journal, Feb. 2020

[3] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu and P. Zeng, "Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism," in IEEE Transactions on Industrial Informatics, June 2019

[4] Hemsley, Kevin E., and E. Fisher, Dr. Ronald. History of Industrial Control System Cyber Incidents. United States: N. p., 2018.

[5] Anawar, Syarulnaziah and Zakaria, Nurul and Masud, Zaki and Zulkiflee, M. and Harum, Norharyati and Ahmad, Rabiah. (2019). IoT Technological Development: Prospect and Implication for Cyberstability. International Journal of Advanced Computer Science and Applications.

[6] Casino, Fran and Dasaklis, Thomas and Patsakis, Constantinos. (2018). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics.

[7] Zheng, Zibin and Xie, Shaoan and Dai, Hong-Ning and Chen, Xiangping and Wang, Huaimin. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.

[8] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems," in 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing. IEEE, 2011

[9] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015

[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead,"

[11] D. Arora, S. Ravi, A. Raghunathan, and N. K. Jha, "Hardware-assisted run-time monitoring for secure program execution on embedded processors," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2006

[12] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, 2017

[13] Z. Li, A. V. Barenji, and G. Q. Huang, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," Robotics and Computer-Integrated Manufacturing, 2018

[14] H. Feng, W. Fu, Study of recent development about privacy and security of the internet of things, in: 2010 International Conference on Web Information Systems and Mining (WISM), Sanya, 2010

[15] R.H. Weber, Internet of things - new security and privacy challenges, Comput. Law Secur. Rev. 26 (1) (2010)

[16] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Networks 57 (10) (2013)

Acknowledgement

We have great pleasure in presenting the report on **Monitoring Health of IIOT Devices using Blockchain.** We take this opportunity to express our sincere thanks towards our guide **Prof. Anagha Aher** & Co-Guide **Prof. Neha Deshmukh** Department of IT, APSIT thane for providing the technical guidelines and suggestions regarding line of work. We would like to express our gratitude towards their constant encouragement, support and guidance through the development of project.

We thank **Prof. Kiran B. Deshpande** Head of Department, IT, APSIT for his encouragement during progress meeting and providing guidelines to write this report.

We thank **Prof. Vishal S. Badgujar** BE project co-ordinator, Department of IT, APSIT for being encouraging throughout the course and for guidance.

We also thank the entire staff of APSIT for their invaluable help rendered during the course of this work. We wish to express our deep gratitude towards all our colleagues of APSIT for their encouragement.

Student Name 1: Rutuja Patole
Student ID 1: 17104011

Student Name 2: Rushika Ramane
Student ID 2: 17104064

Student Name 3: Soundarya Nevrekar
Student ID 3: 17104066

Publication

Paper entitled **"Monitoring Health of IIOT Devices using Blockchain"** is presented at **"International Conference on Intelligent Engineering and Management (ICIEM 2021)"** by **"Rutuja Patole, Rushika Ramane, and Soundarya Nevrekar."**