DESIGN AND DEVELOPMENT OF A BLOCKCHAIN NETWORK FOR TRUSTED IOT

Gude Abhinav sai[1], Badugu Anand Babu[2], Chilakala Hemanth Sri Lakshmi Narayana[3]

[1,2,3]Under Graduate Students,
[1] Department of Electronics and Communication Engineering,
[1]Vasireddy Venkatadri Institute of Technology, Nambur, India.

Abstract : Blockchain is one of the emerging technologies which builds trust and transparency to an industry where transactional progressions plays a major role. In this digital transformation era of business, Internet of Things (IoT) is an additional trending technology that denotes to the billions of physical devices around the world that are associated to the internet, assembling and distribution of data. In this paper we project our work by using Hyperledger Fabric, an open source blockchain framework, and the Watson™ IoT platform through Node-RED to handling the assortment of data on a distributed network unchangeably. The aim of this investigation goal is to design a proof of concept for equally Blockchain and IoT. Rather than developing an application with complete abilities, our resolution will be much more reasonable and informative. This paper can be stretched and improved according to new-fangled business representations by adding new organizations to the distributed network and emerging innovative smart agreements depending on the logic. In this paper, we intend to build a Hyperledger Fabric network, design APIs with the Hyperledger Fabric SDKs to interact with the network, collect information or data from the sensor (such as temperature), demonstration of data on the dashboard with Node-RED, and a UI where we can see the sensor data history.

Key words: Internet of Things (IoT), Node-RED, Application Programming Interface (API), Docker.

I. INTRODUCTION

Blockchain is designed to reveal any interference with the contents which is a tamper evident that allocate digital ledger that records public or private peer-to-peer network transactions. Circulated to all member nodes in the network, the ledger permanently records, in a chronological chain of cryptographic hash-linked blocks, the history of exchanges that take place between the peers in the network. Transaction blocks are chained and linked with each other from the starting node. So, it is named as blockchain. Blockchain in Internet of Things is an innovative and emerging technology that performs a distributed, decentralized, public and real-time ledger to stockpile the transactions amongst IoT nodes. Blockchain contains series of blocks and each block is connected to the preceding one. Every block contains cryptographic hash code, preceding block hash along with its data. Block chain transactions are used to share the data between IoT nodes. The aim of Blockchain in IoT is to contribute a technique to process secured records of data through IoT nodes. Blockchain is a secured technology that can be used publicly and openly. The usage of blockchain shared ledger transactions cannot be altered once it is validated by consensus which helps us to save time and cost while reducing risk and enables businesses to build new revenue streams to interact with clients.

Hyperledger is an open-source effort to improve cross-industry Blockchain technologies for business use. It is an international collaboration, introduced by The Linux Foundation, with leaders in finance, banking, Internet of Things, supply chain, manufacturing and technology. It assists as a neutral home for several circulated ledger frameworks including Hyperledger Fabric, Sawtooth, Indy as well as tools like Hyperledger Caliper and libraries like Hyperledger Ursa. The Hyperledger Fabric framework assists distributed ledger resolutions on permissioned networks, where the clints are well known to one another, for a widespread variety of industries. Its integrated architecture increases the privacy, pliability, and flexibility of blockchain resolutions.

II. REVIEW OF LITERATURE

Peichang Shi, Huaimin Wang, Shangzhi Yang Chang Chen, Wentao Yang [1] has examined a study on a block chain- grounded reliable data distribution between trusted shareholders in IoT. in this paper the author has proposed a secure and Lightweight triple-trusting architecture (SLTA) which works on blockchain technology. This architecture contains an oracle-based data collection which do not allow any modifications in collected IoT data and secure the system through digital identities the design of new software in this architecture has a blockchain model and an algorithm named as byzantine fault-tolerant helps in decentralized data collection, management of identities and in transfer of data too. In SLTA having DID mechanism for management used to ensure that the data collection form IoT node cannot be modifies and not allows to third party without identification.

Juah C Song, Mevlut A Demir, John J Prevost, Paul Rad [2] has experimented on Design of blockchain for decentralized networks of IoT In this paper the Author Investigated about the challenges as well as opportunities of blockchain execution and shown a case of blockchain integration. Linking of blockchain with internet of things resulted a decentralized way to accomplish the increasing figure of networked devices. By the allowance of dynamic reconfiguration of blockchain constraints lead to stable changing environments. The design of blockchain elements for an IoT system resulted the securing the acquisition of sensor data.

Tanweer Alam [3] described about the importance of blockchain technologies in IoT In this paper the author explained about Blockchain in IoT which may help to improve the security of Communication along with its challenges and opportunities. These Blockchain units are used to transfer the data between IoT nodes. Role of blockchain and opportunities like cost and time reduction, social and financial services, cost reduction etc., along with challenges such as Scalability, Interoperability etc.,

Lei Hang and Do-Hyeun Kim*[4] has an investigated-on Design and Implementation of an integrated IoT Blockchain Platform for Sensing Data Integrity in this paper the author proposes an integrated IoT platform using blockchain technology to guarantee sensing data integrity. The aim of this platform is to afford the device owner a practical application that provides a comprehensive, immutable log and allows easy access to their devices deployed in different domains explores the potential applications of IoT and blockchain to improve efficiency and bring automation, to revolutionize robust business solutions in various IoT scenarios.

Kotaro Kataoka, Saurabh Gangwar and Prashanth Podili [5] explained about the IoT traffic Management using blockchain and SDN -in this paper the author investigated about the authenticity of IoT devices, services and their communication also to prevent unwanted traffic from IoT devices in a trustworthy, scalable, and distributed manner. This paper proposes a Trust List that represents the distribution of trust among IoT-related stakeholders and provides autonomous enforcement of IoT traffic management at the edge networks by integrating blockchains and Software-Defined Networking (SDN). The principle of Trust List is automating the process of doubting, verifying, and trusting IoT services and devices to effectively prevent attacks and abuses.

Ana Reyna *, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz [6] has explained about the opportunities and challenges on blockchain and integration with IOT This paper focuses on the challenges in Blockchain technology IOT application a survey has conducted to how blockchain could potentially improve the IoT. The integration of the IoT and blockchain will greatly increase the use of blockchain, in such a way as to establish cryptocurrencies on the same level as current fiduciary money.

Jollen Chen [7] has developed a hybrid blockchain for a secure trusted IOT networks the author explained solution of problems for secure and trusted IOT networks by implementing emerging technologies of Blockchain. In this paper they proposed a new hybrid technology to discourse the trusted IOT issues delve deeper the algorithms of the hybrid consensus to provide the capabilities for our hybrid blockchain technology.

Abid Sultan, Muhammad Azhar Mushtaq, Muhammad Abubakar [8] published a review paper on the issues of blockchain with IoT**.** This author's investigation on addressing substantial security problems of IoT and maps IoT security problems in contradiction of prevailing solutions. literature review on Blockchain and Internet of Things and highlighted issues linked to an IoT atmosphere, the different properties and characteristics of the blockchain network are highlighted such order to remove the issues in IoT.

Zibin Zheng, Sun Yat-Sen Yan Zhang [9] has conducted a survey on blockchain for IOT in this paper the author has investigated blockchain technology integration with IOT and named it as blockchain and IoT as Blockchain of Things (BCoT) architecture and discusses about the insights of it. and also, the convergence of IoT and blockchain with BCoT and its industrial applications has discussed. Applications and future research directions with BCoT architecture has explained.

III. RESEARCH METHODOLOGY

Here are the steps followed to design and develop blockchain technology for a trusted IoT:

- Inspecting the installation prerequisites and clone the repository in Linux OS.
- Generating & Accessing IBM cloud Kubernetes cluster.
- Installing Hyperledger fabric.
- Deploying Hyperledger fabric SDK for node.js.
- Deploying Node- RED.
- Obtaining Sensor Data.

IV. DESIGN AND DEVELOPMENT OF BLOCKCHAIN NETWORK FOR IoT

We have used Linux which is an open-source operating system software that straightly manages a system's hardware and resources, like CPU, memory, and storage. The Software installation and the external reference was from IBM. In this paper we are going to visualize the Temperature variation through a blockchain network connected with IoT.

- Watson IoT Platform which an IBM's entirely managed, cloud-hosted service which makes it easy to originate value from Internet of Things (IoT) devices.
- Node-RED is a flow-based progress tool for visual software design established by IBM for equipping organized hardware devices, Application Programming Interface (APIs) and operational facilities as part of the Internet of Things.

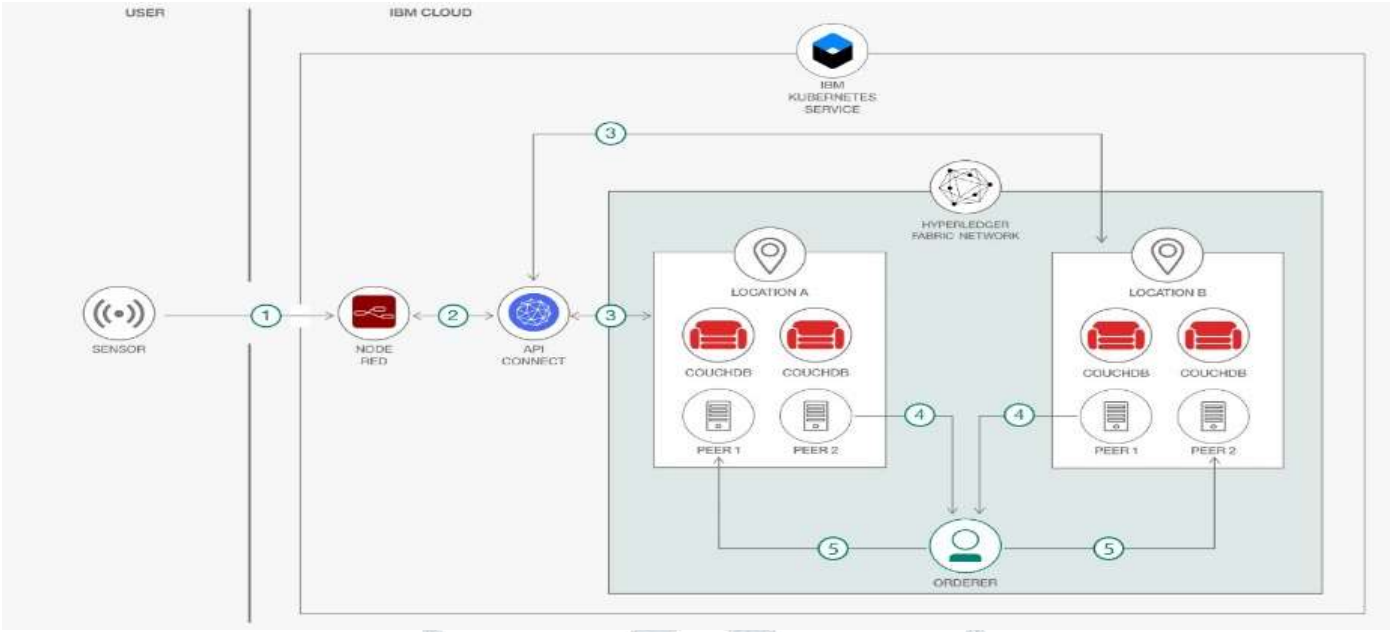

Figure 1: The Architecture of Blockchain for IOT

The above architecture from Figure 1 explains that input node from Waston IoT platform that ensconce with Node-RED receives the sensor data. To invoke and to read and write the data which is ledger query of nodes present in the Node-RED accomplish Hypertext Transfer Protocol (HTTP) requests and returns the reply to the APIs. APIs distinct based on Hyperledger Fabric Client software development kit (SDK) for Node.js interrelate with the chaincode within the Hyperledger Fabric Network and informs or recites the ledger. Endorser Peers implements the purpose that is well-defined in the chaincode according to the appeal and directs it to the orderer. The orderer generates the blocks and directs it back to the Anchor Peers which will program the blocks to the Endorser Peers. In this case we used CouchDBs as state database.

Components such as IBM Cloud Kubernetes combines Docker containers and this technology has an instinctive experience of user which builds security and remoteness to systematize the distribution, operation, scaling, and supervising of containerized apps in a cluster of compute hosts and Node-RED is also a component which is a software design implementation for connecting organized hardware devices are used. Technologies such as Hyperledger Fabric that is a platform for circulated ledger resolutions supported by an integrated architecture distributing elevated degrees of privacy, resiliency, flexibility, and scalability. GoLang is another technology which is an open-source programming language that makes it simple to build easy, consistent, and well-organized software. Node.js is also an open basis, cross-platform runtime setting for emerging server-side and networking submissions. To run the Applications, we need go for few steps and Prerequisites such as Creating an IBM Cloud account, IBM Cloud CLI, Docker.

- IBM Cloud Command Line Interface (CLI) delivers directions for handling resources in IBM Cloud.
- Docker is an open platform for emerging, distributing, and running requests.it enables us to distinct applications from our substructure so that we can deliver software rapidly.

4.1 Development of Hyperledger fabric for trusted IoT

Linux Operating system was installed in Virtual box and then the first step is to verify the installation by following command.

Commands	Operation
$ docker version $ ibmcloud –version	Checking installed prerequisites
$ git clone https://github.com/yigitpolat/Hyperledger-IoT command.	Cloning the repository in folder

Table 1: Commands and operations

Hyperledger Fabric comprises of various components, we are using microservice architecture on IBM Cloud Kubernetes Service. Next step is to signing up and accessing IBM Cloud Kubernetes Cluster which is a “free” type.

Command	Operation
$ ibmcloud ks cluster config --cluster c36bb0nd0l111ovk8crg	Accessing the cluster

Table 2: Commands and operations

The third step is Installing Hyperledger Fabric by using Commands. We create a Persistent Volume (PV) is a section of storage in the cluster provisioned by an administrator. PersistentVolumeClaim (PVC) is an appeal for storage by an operator. This storge is used for chaincode and configuration file. Copy Artifacts can be reprocessed by copying prevailing artifacts. The copied artifacts can be altered without affecting the original one. Further we generate Hyperledger Fabric key resources and channel configurations related artifacts here we are using Cryptogen material for creating Hyperledger Fabric key material. The configtxgen command

allows users to generate and inspect channel config related artifacts. A peer node on a channel that all other peers can discover and communicate with.

Commands	Operation

$ cd Hyperledger-IoT
$ cd volume commands
$ kubectl create -f createPVandPVC.yaml
	Deploying Hyperledger

$ cd ../jobs
$ kubectl apply -f copyArtifactsJob.yaml
$ pod=$(kubectl get pods --selector=job-name=copyartifacts output=jsonpath={.items..metadata.name})
$ kubectl cp ../artifacts $pod:/shared/
	Creating copyartifacts pod

$ kubectl apply -f generateCryptoConfig.yaml	Generating Membership Service Providers (MSPs)
$ kubectl apply -f generateGenesisBlock.yaml	Generating genesis.block
$ kubectl apply -f generateChanneltx.yaml	Generating channel1.tx
$ kubectl apply -f generateAnchorPeerMSPs.yaml	Generating Org1MSPanchors.tx and Org2MSPanchors

Table 3: Commands and operations

After Completing the prerequisites for network installation, we go for installing the Hyperledger fabric components, deployments position to be developed successively to prevent any conflicts, pod status by executing "kubectl get pods" we go for network configuration.

Commands	Operation
$ cd ../network-deployment $ sh deployAll.sh	Deploying Network
$ cd ../jobs $ kubectl apply -f create_channel.yaml	Creating channel1
$ kubectl apply -f join_channel.yaml	Joining all peers to channel1
$ kubectl apply -f chaincode_install.yaml	Installing chaincode to peers
$ kubectl apply -f chaincode_instantaite.yaml	Instantiate the installed chaincode to the channel
$ kubectl apply -f updateAnchorPeers.yaml	Updating the channel and setting the peers

Table 4: Commands and operations

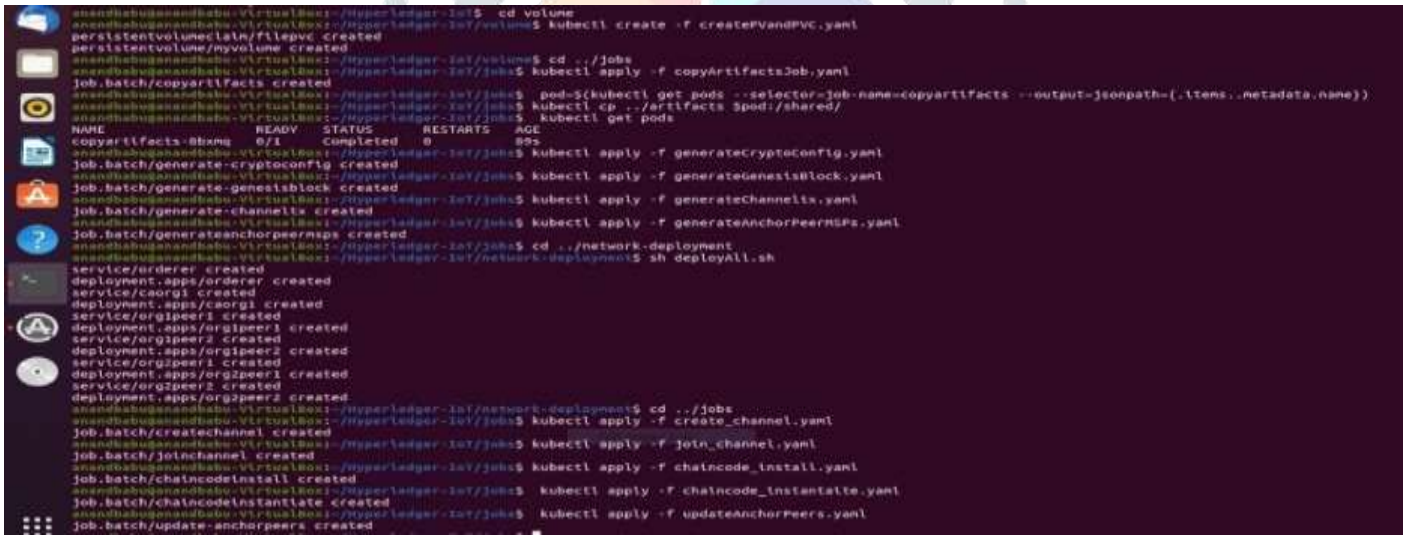

Figure 2: Deploying Hyperledger Fabric

The fourth step is to install Hyperledger Fabric Software Development Kit (SDK) for Node.js in order to attach the back-end and the front-end. Hyperledger Fabric Client SDK for Node.js which makes it possible to use APIs to interact with a Hyperledger Fabric blockchain. And we have created a DockerHub Account in order to push and pull our container images.

Commands	Operation

$ cd ../API
$ docker build . -t <account name>/rest-api
$ docker push <account name>/rest-api
	Creating a container image and pushing it into container registry.

$ cd ..
$ kubectl create deployment rest-api --image=<account_name>/rest-api
$ kubectl expose deployment rest-api --port=3000 --target-port=3000
	Deploying and exposing the Rest-api.

Table 5: Commands and operations

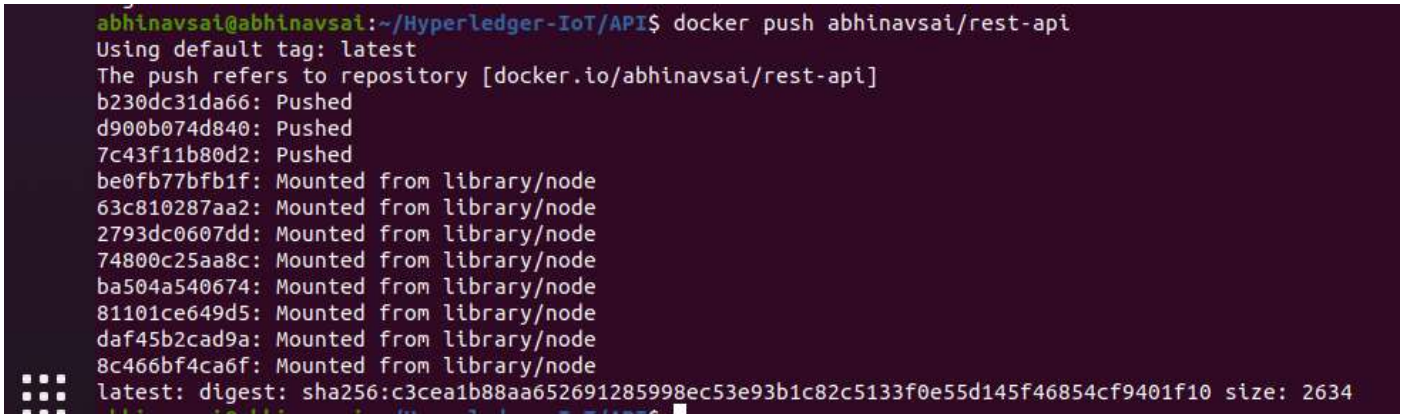

Figure 3: Deploying Hyperledger Fabric SDK for node.js

The fifth step is to deploy Node-RED. The Node-RED dashboard is our front-end. The incoming sensor data and the history of the ledger is visible from this dashboard. Besides, all the HTTP requests will be executed via this tool. The following commands will first pull the container image from Dockerhub and creates a deployment named "node-red" and then creates a Kubernetes Service which exposes this deployment.

Commands	Operations
$ cd node-red $ kubectl create deployment node-red --image=yigitpolat/hyperledger-iot-nodered	Creating a deployment named node-red.
$ kubectl apply -f node-red-svc-nodePort.yaml	Making nodered deployment accessible from network.
$ kubectl get pods -o wide $ kubectl get nodes -o wide	Getting Kubernetes worker nodes external Ips.

Table 6: Commands and Operations

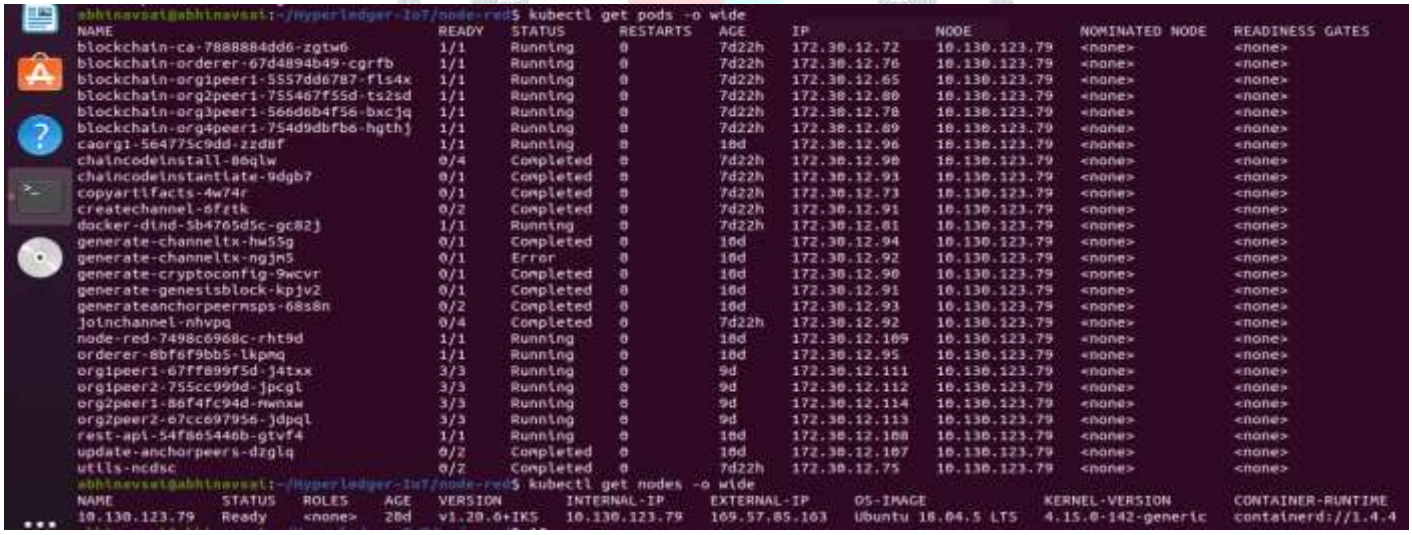

Figure 4: Obtaining external IPs of worker nodes

V. RESULT

By adding ':30002' at the end of the obtained external IP of the worker node and navigating it through a browser we can find Node-RED service. Registration can be done by enabling the status of Node-RED. Then it is deployed and the HTTP post requests are to be executed.

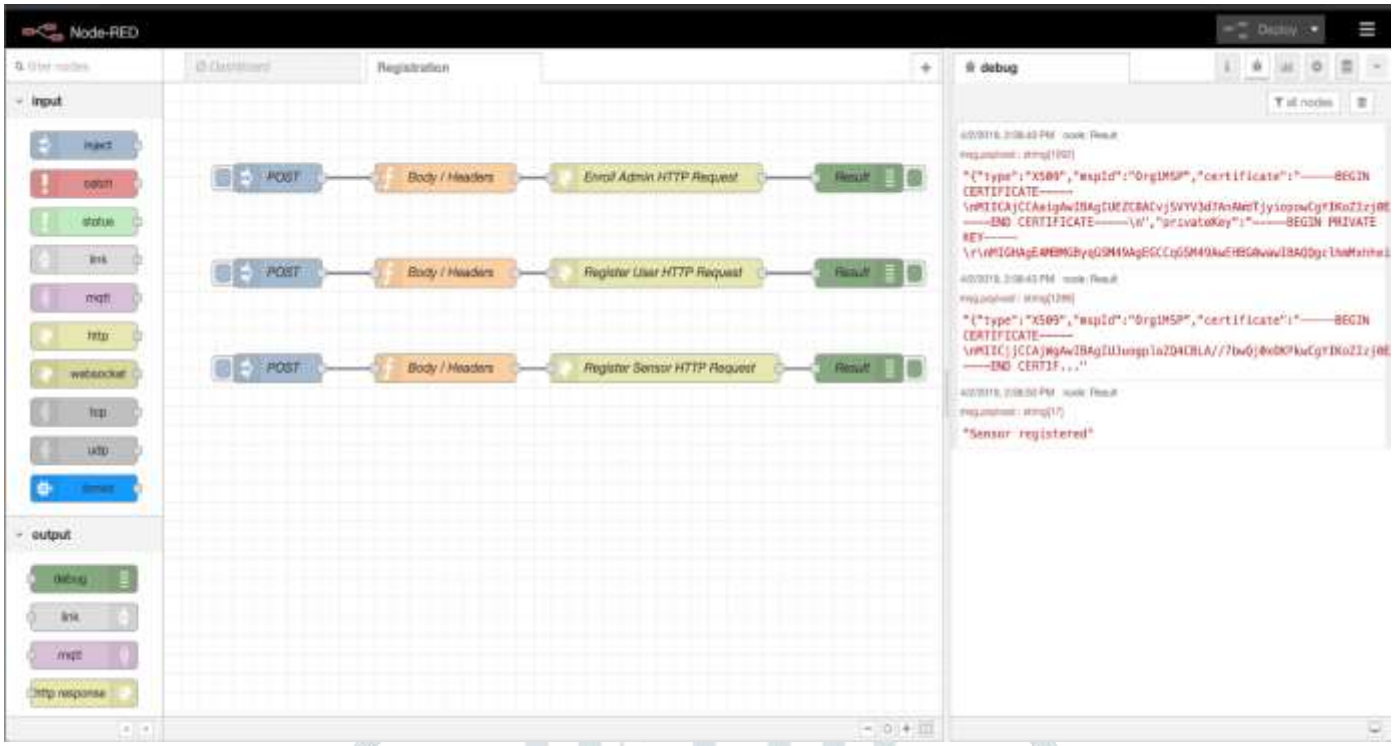

Figure 5: Registration of Node-RED

In the Dashboard tab, the status is set to 'Enabled' and it is deployed. As we are not providing any sensor, we are using dummy data generator to generate data.

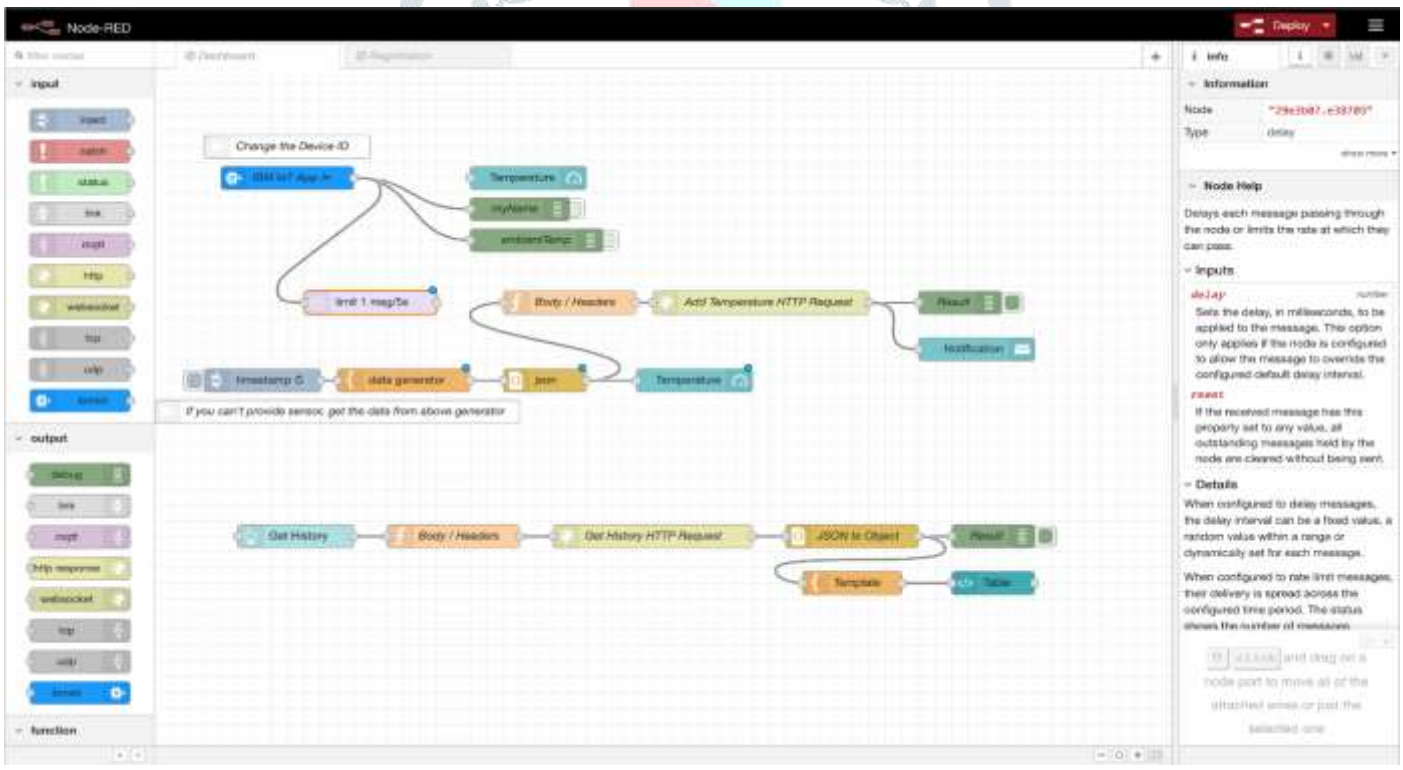

Figure 6: Dashboard of Node-RED

For obtaining the sensor data, navigate to the address making an extension ':30002/ui' to the obtained external IP of the worker node. Finally, we can see the sensor data likewise in the figure 7 which is coming from the ledger where the data is storing immutably in the blockchain.

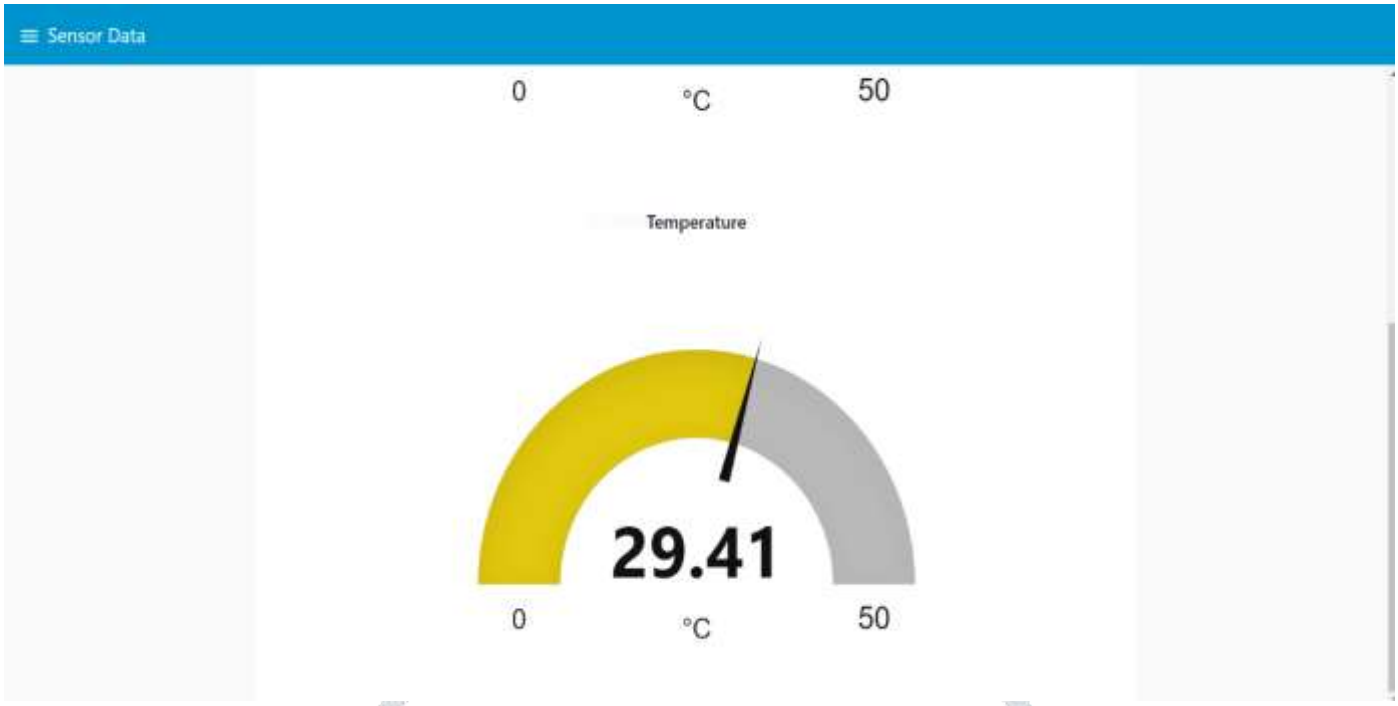

Figure 7: Sensor data (Temperature) from Node-RED UI

VI. CONCLUSION

From this we can conclude that, by using Blockchain technology for a trusted IoT, security of the system is enhanced. Since all the confirmed and validated blocks of the blockchain network are linked and chained from end-to-end, it acts as a single source of truth. Instead of developing an application with full capabilities, this minimum viable product is much more understandable and instructive. However, it can be extended with several modifications and the research gap will be sorted by adopting and adding new functions to the chaincode that will bring new features to the application according to new functions, API endpoints needed to be updated to fulfill the HTTP requests. Dashboard must be modified depending on the upcoming data.

VII. REFERENCES

1. Peichang Shi, Huaimin Wang, Shangzhi Yang Chang Chen, Wentao Yang, 2019 "Blockchain-based trusted data sharing among trusted stakeholders in IoT" DOI: https://doi.org/10.1002/spe.2739
2. Juah C Song, Mevlut A Demir, John J Prevost, Paul Rad, 2018 "Blockchain Design for Trusted Decentralized IoT Networks" DOI: 10.1109/SYSOSE.2018.8428720
3. Tanweer Alam, 2022 "Blockchain and its Role in the Internet of Things (IoT)" DOI:10.32628/CSEIT195137
4. Lei Hang and Do-Hyeun Kim *, 2019 "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity" DOI: https://doi.org/10.3390/s19102228
5. Kotaro Kataoka, Saurabh Gangwar and Prashanth Podili, 2018, "Trust List: Internet-wide and Distributed IoT Traffic Management using Blockchain and SDN" DOI: 10.1109/WF-IoT.2018.8355139
6. Ana Reyna *, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz, 2018 "On blockchain and its integration with IoT. Challenges and opportunities" DOI: https://doi.org/10.1016/j.future.2018.05.046
7. Jollen Chen, 2018 "Hybrid Blockchain and Pseudonymous Authentication for Secure and Trusted IoT Networks" DOI: 10.1145/3292384.3292388
8. Abid Sultan, Muhammad Azhar Mushtaq, Muhammad Abubakar, 2019 "IoT Security Issues Via Blockchain: A Review Paper" DOI: 10.1145/3320154.3320163
9. Zibin Zheng, Sun Yat-Sen Yan Zhang, 2019 "Blockchain for Internet of Things: A Survey" DOI: 10.1109/JIOT.2019.2920987
10. https://github.com/IBM/Hyperledger-Fabric-for-Trusted-IoT