A Secure Transaction Authentication Scheme using Blockchain based on IoT

Dr.A.Nirmal Kumar, Dr.R.Jegadeesan, Dr.C.N.Ravi, J.Greeda

Abstract—Blockchain technology that underpins the crypto currency bit coins has played a vital role in decentralized, transparency and data intensive applications. It is an emerging innovative technology with open ledger for secure transaction has becoming crucial factor around the world, as they are responsible for the development of decentralized approach for creating the applications. Since its generating significant interest across a wide range of industries, here we customize and tailor the technology to fit multiple use cases. We explore our model based on the blockchain that fits assessment has performed for banking transaction via IOT and various applications. Internet of Things (IoT) has been found in many important applications for security and privacy applications. It is an emerging innovative technology with open ledger for secure transaction authentication scheme for IOT. Transaction packages are made with two codes by interlinked and chained called hash codes. Concepts of mining are used for validating transactional information for secure transaction and authentication scheme for IoT. We provide an overview of blockchain architecture firstly and compare some typical consensus algorithms used in different block chains. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future trends for blockchain.

Index Terms — Blockchain, Crypto Currency, IoT, Authentication.

1 INTRODUCTION

Blockchain the mostly known as backbone technology behind bit coin, since currently it’s an one of emerging technology because of attracting lot of attentions from the enterprises in market, start-ups and media. Blockchain has an potential to transform multiple industries and make every processes more democratic, secure, transparent and more efficient with huge volumes of data getting generating everyday owing to digitization of records, as we need to manage the effective security threats and cost efficiency. Blockchain promises with decentralized ownership, immutability and cryptographic security of data, is made to catch the attention of the c-suite executives. Since everyone started realizing the disruptive potential of this technology.

The financial players are first to move upon to capitalize this technology still in a nascent stage. As the study proved by the world economic forum that predicts banks and regulators around world. More than 90 central banks engaged in blockchain discussion globally, more than 2500 patent fields over last 3 years, eighty percent bank predicate to initiate blockchain and distributed ledger technology (DLT).

Nonfinancial services industries like telecom cyber security, supply chain management, forecasting, insurance industry, private transport, ride sharing, cloud storage, crowd funding, voting, cinema industries, reservations, governance, energy management, retail, real estate are on the way to establish potential blockchain use cases to positively disrupt the traditional business model or already implemented their pilot blockchain use cases. Nonfinancial services industries like telecom cyber security, supply chain management, forecasting, insurance industry, private transport, ride sharing, cloud storage, crowd funding, voting, cinema industries, reservations, governance, energy management, retail, real estate are on the way to establish potential blockchain use cases to positively disrupt the traditional business model or already implemented their pilot blockchain use cases.

1.1 Overview of the Project

The overview for the blockchain based financial system. The system consists of ethereum private blockchain, frontend application on the cloud or local web server, smart contract deployed on the private blockchain. Blockchain comprises of multiple Peer to Peer connected nodes of different Internet of Things devices such as arduino, laptop or personal computer, etc. Every node must install ethereum client and connect to same chain id or network id to become part of one network; when they become part of the same chain then they can execute transactions, calls, perform mining and take part in the consensus process. The smart contract is the business logic of Digital app, and it is not centralized like traditional applications. The contract is deployed on the blockchain by the contract owner using his ethereum account. Once contract deployment transaction mined by miners, then it will be available on every node on the network on a specific address. For customers to interact with the blockchain such as buy ticket, check the validity of ticket or for contract owner to
change the ticket fee, transfer either from contract to another account there is a user-friendly GUI. To use the GUI, the user must have to use Mist browser or Meta mask plugin for chrome and an ethereum account. Mist or Meta mask allow the user to import his ethereum account to the system he is using and will enable the system to connect to blockchain network by making the user system a virtual blockchain node. The transformation of data such as coding and decoding and allow a lot of other functionalities to interact RPC port provided by blockchain. If a user is using a direct blockchain network node and is capable of handling command line, then he does not need Mist or Meta mask. The frontend application can be stored on the cloud or local web server or personal computer web server. Banking service is decentralized because of the business logic "smart contract." is available on every node of the network and the front-app access the contract using the unique address of every transaction.

1.2 Objective of the Project

The objective of the project is how the data is processed through the Arduino and transact the data from the each and every transaction. Each transaction there is a hash code is generated for both the transmitter and receiver. When the transmitter is connected with the Arduino UNO then the hash key is checked for each and every transaction from both the transmitter and receiver for secure transaction in each and every process. Then the process is connected with the locking system using the blockchain and the verification is done by the hash key. If the hash key is matched or similar to transmitter and the receiver then the encryption and decryption process is done with the blockchain transmitter and receiver. Whenever the power supply is connected the blockchain is built and the hash key is generated for secure transaction between the sender and receiver. When the power supply is connected to the arduino to the DC motor then the power is transmitted for each and every transaction towards the blockchain approach with the help of automation in the Arduino UNO.

1.3 Problem Definition

Now a day, there is no secure transaction for banking and any financial sectors, which are being used in the locking system and the transaction is being done by the process of secure transactions with the automation of the process. Then the process is done by the automation, but there is no secure transaction is not there. In which the process of transaction was being done by the client.

1.4 Scope of the Project

The main function of blockchain development was firstly for the financial application but later the introduction of smart contract, Blockchain applications have no boundaries anymore. Blockchain can now be used as for the financial and the non-financial applications. One of these applications was IoT. Blockchain allow us to have a distributed Peer to Peer network where without trust members can interact with each other without a mediator, in a provable way. Smart contracts scripts that beside on the blockchain that allows the automation of multiple step processes. Blockchain facilitates the sharing of services and information leading to the creation of a market place of services between devices and to automate in a cryptographically verifiable manner several existing, time-consuming workflows. Then the workflow of the project is to be based on the encryption and decryption process when the data id being transmitted and received in the reception along with the generated hash key and encrypted data and in the receiver side the data is received along with the generated hash key for the reference of their transaction which is being transacted in the concept of blockchain and internet of things. The blockchain and internet of thing is mainly used for the safe and secure transaction when done.

2 SYSTEM ANALYSIS

2.1 Existing System

The BlockChain was been used as a distributed transaction ledger at the crosswords of game theory, cryptography, computer networking and data transmission and economic and monitory theory. Massively duplicated across network nodes shared with a peer to peer (P2P) file transfer protocol. Updated by a peculiar nodes know as miners, appending new blocks of transaction. Blockchain is used for the security and transaction of the process which is to be maintained for the purpose of the data. When the data is being made and the process can be financial services and the process is monitored and inspected by the other process. From the processed data monitored and the implemented by the blockchain with the peer to peer network. When the peer to peer network is connected to the blockchain with the less security and the difficult to maintain to data handling.

2.2 Literature Survey

A Decision Framework for Block chain Platform for IOT And Edge Computing

A Decision Support System for Block chain Platform Selection. The novelty of this Decision Support System lies in being a feature-based artifact which incorporates ISO software quality This Decision Support System was evaluated in three different case-studies with organizations creating blockchain. Block chain Platform Decision Support System (BPDSS) capable of assisting developers sufficiently during the selection process between different block chain platforms. There are various potential in order to disrupt currently it is an overcame of the challenging software producing organization to have an identified selection process on multi-criteria on decision making problems. In decision support system the aids for developing during technology, the selection process of blockchain platform. They are contemporary solutions to solve problems were only few rather form of simplistic decision-trees, where struggles with complexity of adaptations. The various novelty of the decision support system being featured based on the artifact which they incorporates the ISO software quality of their aspects and features based on the prioritization based on MOSCOW-technique.

A Software Defined Fog Node Based Distributed Block chain Cloud Architecture for IoT

In the future, we will explore the various energy harvesting technique aspects of our proposed model for energy efficient communication among devices at the edge of the IoT network.
The proposed architecture was designed to support. Because of high availability and scalability the data is to be made by the easier to maintain and the handling of data is easier. Then the more important merits in the distributed network is that it can share the data whenever it needs.

**Ethereum: A Secure Decentralised Generalised Transaction Ledger**

Decentralized secure social operating system. Contracts may be authored in order to algorithmically specify and autonomously enforce rules of interaction. Provide to the end developer a tightly integrated end-to-end system. Basically the decentralization helps us to transact the data from one to another. Nowadays there would be massive form of consumption of vast energy in excavating the crypto currencies, for miners in transaction network in proposal to authenticate transaction using an significant quantity in computing power. The integrated concerns of blockchain technology based on the application they typically provide a solution in decentralized system. They require essential modification for current security systems. Thus, in order to make a successful shift, at companies to prepare various strategies based on desire to make a complete switch. The complete change over a distributed network, which they require the buy-in form of its users and operators. They are made in a massive task in order to receive the crypto currencies as substitute currency. The uncertainty of the blockchain technology is not high yet, due to limited on popular creativities to generate an undefined form of situations.

**2.3 Proposed System**

Due to consensus in a distributed network with faulty (or malicious) nodes is a hard problem for making a secure transaction based on any lot. For secure storage and transaction authentication scheme has been proposed. Here, all network nodes perform a transaction validation and clearing with compensated for the proof of work by miners.

**3 RESEARCH METHODOLOGY OF IMPLEMENTATION**

The project modules are decomposed into two ways:

1. Contract Owner
2. Customer

**3.1 Contract Owner**

Contract owner has most of the rights of the application. It can perform the following actions:

- Create ethereum ether base account for deployment of contract.
- Deploy contract on the blockchain network.
- Change transaction/ day, using his ether base account address.
- Transfer one ether account to another ether account.
- Destroy contract, to make it inaccessible including its ether and data.

**3.2 Customer**

The customer is the majority entity of the application. The customer can use application to buy, validate and check the history of all transport tickets. The actions of customer are:

- Create ethereum account to buy a ticket.
- Purchase a ticket for specific days and class.
- Check validity of the currently available ticket.
- Check the list of all ticket purchased.
- Check the balance of his account.

**3.3 Better Availability and Accountability for IoT of a Blockchain**

The key components are a web portal, blockchain infrastructure based on Multichain, and IoT devices as given. The web portal enables manufacturers to deploy software updates securely and efficiently. The web portal has access to the blockchain infrastructure, which is shared between manufacturers. Each manufacturer is required to provide at least one worker node to improve the availability and the computing power of the infrastructure. For the prototype, blockchain nodes are implemented as Virtual Machine (VM) s and are hosted on a XenServer server. The web portal and the IoT devices can exchange software updates and confirmations, using the blockchain infrastructure. The system relies on asymmetric cryptography to guarantee data confidentiality and integrity.

**3.4 CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT**

The solution presented by (DPKS17) is called CONNECT. It defined Two different kinds of nodes

- Virtual nodes or VNodes are logical nodes in the form of blockchain peers. These nodes are responsible for handling all the operations that involve the blockchain such as creating and validating transactions as browsing the blockchain to find information among other peers.
- Physical Nodes or PNodes represent the devices. Each VNode belongs to a layer which describes a particular blockchain application (might be data, audio and video services). The following three possible interactions for PNodes and VNodes are:
  - PNode to PNode: the connection between two physical devices in the network.
  - PNode to VNode: the connection between a physical device and a blockchain peer who can be either executed by the same PNode or by others. Otherwise, they need to reach the other the physical node running the peer and download all its information.
  - VNode to VNode: the connection between two peers, for the sake of simplicity and clarity, called VNodes and VNode for sender and receiver respectively. If the VNode belongs to a different blockchain than VNodes, then the PNode hosting it has to
    - Download the VNode blockchain from the client and
    - Browse it for the required information.
3.5 System Design

When the transaction is being made by the user the hash key is generated for individual transaction with the help of automation of Arduino which connects to the LCD display to ensure each and every records that are maintained in ledger each one shared by database are replicated to user who can access scenario and signature verification is done. The block of code of transaction is sent to large network where authentication of code is confirmed without compromising.

void Delay(unsigned int);
void delay(unsigned int delay);
void Serial_Init();
void Serial_Out(unsigned char);
void Serial_string(unsigned char *);
void Receive(unsigned char);
void main()
{
ADCON1=0x02;
TRISB=0x0F;
PORTB=0x00;
TRISC=0x80;
PORTC=0x00;
TRISD=0x00;
PORTD=0x00;
TRISE=0x00;
PORTE=0x00;
GIE=1;
PEIE=1;
RCIE = 1;

Lcd_Init();
Lcd_Command(0X80);
Lcd_Command(0XC0);
Lcd_string("Blockchain");
Lcd_string("BC Receiver");
Delay(65000);
Delay(65000);
}

The test process is initiated by developing a comprehensive plan to test the general functionality and special features on a variety of platform combinations. Strict quality control procedures are used. The process verifies that the application meets the requirements specified in the system requirements document and is bug free. The following are the considerations used to develop the framework from developing the testing methodologies.

5 CONCLUSION

Blockchain is still prevailing at its early stage of its research and development. Pioneer researchers in the domain of security and Cryptography have come forward to take it further to newer highs. It is going to a great help for the financial and Non-Financial sectors. It will pay heed to the issues of reliability, scalability, reusability and the implementable way of the process and the responsibilities is to be made by the blockchain and Internet of Things which uses the process for the implementation for the blockchain which has the time limit to secure and transact the data from one user to another.
6 REFERENCES


