Design and Implementation of an E-Commerce Based Trading System Using Ethereum Blockchain

Amarnath Mishra[1]
Student, Final year,
Computer Science and Engineering
Presidency University,
Bangalore, Karnataka, India
2016cse305@presidencyuniversity.in

Venkata Sai Krishna P[1]
Student, Final year,
Computer Science and Engineering
Presidency University,
Bangalore, Karnataka, India
2016cse019@presidencyuniversity.in

Mukesh Kumar [1]
Student, Final year,
Computer Science and Engineering
Presidency University,
Bangalore, Karnataka, India
2016cse311@presidencyuniversity.in

Anitha Premkumar[2]
Assistant Professor, CSE,
Computer Science and Engineering
Presidency University,
Bangalore, Karnataka, India
anithapremkumar@presidencyuniversity.in

Abstract— A supply chain involves a series of steps to get the product to the customer, with the collaboration of various entities such as producers/manufacturers, warehouses and retailers. A major issue faced in supply chains is that it becomes difficult for organizations to maintain a track of every record and provide transparency about the product to the customer. This in turn gives a chance for counterfeit goods to rise up in the market. This paper aims to overcome this challenge by designing E-Commerce based trading system using Blockchain technology. It is an effective approach as this system maintains a permanent and immutable copy of record of each action taking place in the E-commerce platform, because it secures data using cryptography. This approach will make it easier for the customers to verify the identity of the person or organization from whom they are buying the product. It will help in curbing the amount of counterfeit goods in the market. The customers will always have the exact identity of the organization who is selling the product.

Keywords— Blockchain, Supply chain, Cryptography, Trading system, E-Commerce

I. INTRODUCTION:

E-commerce [5] has become very popular and most of the payments are done digitally. The external parties include the different actors in the supply chain and the bank as well. If there is any fault occurring in the transactions, it is difficult to pinpoint the reason due to the astonishingly huge number of users and the volume of data being generated. There can also be some security issues. We aim to address the specified problems by using smart contracts (Ethereum Blockchain). Smart contract is a very easy and secure system. The basic idea is that if the customer has sufficient balance to buy a product, then he can directly buy it from the seller using smart contract. The money will be directly transferred to the seller's crypto-wallet and the ownership of the product will be transferred to the buyer without anyone interfering in between. This is all possible by using Blockchain technology.

[2] A blockchain is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp and transaction data (generally represented as a Merkle tree). By design, a blockchain is resistant to the modification of data. It is an 'open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way'. For use as a distributed ledger [9], a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires consensus of the network majority. Our approach is by using public Blockchain.

In 2013, Vitalik Buterin, a programmer and a co-founder of the Bitcoin Magazine stated that Bitcoin needed a scripting language for building decentralized applications or DApps. Failing to gain agreement in the community, Vitalik started the development of a new blockchain-based distributed computing platform, Ethereum, which featured a scripting functionality, called smart contracts. Smart contracts are programs or scripts that are deployed and executed on the Ethereum blockchain, they can be used for example to make a transaction if certain conditions are met. Developers are also able to create and publish applications that run inside Ethereum blockchain. These applications are usually referred to as DApps (decentralized applications) and there are already hundreds of DApps running in the Ethereum blockchain, including social media platforms, gambling applications, and financial exchanges. The crypto currency of Ethereum is called Ether, it can be transferred between accounts and is used to pay the fees for the computational power used when executing smart contracts.

II. PROPOSED SYSTEM DESIGN

Blockchain [3] has revolutionized the E-commerce industry by its unique decentralized distributed technology. The scenario of E-commerce based trading system using ethereum blockchain is shown in Figure 1. The system design represents the E-commerce based blockchain which manages and updates the complete trading system and storing of data related to product information, seller information, and buyer information. The seller can list the product in the system application by invoking smart contract. The products will be visible to the buyers as Eethereum is a decentralized system, if the buyer wants to buy the product they have to send the crypto currency and smart contract will be responsible for sending the payment to the seller and sending the product to the buyer.

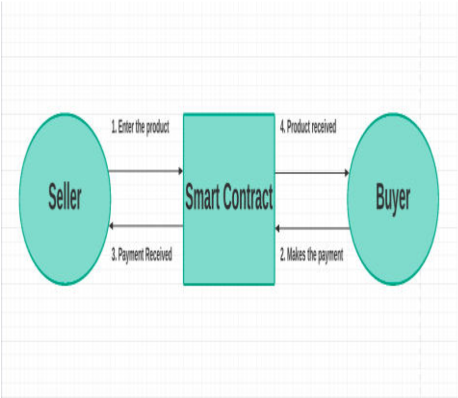


Fig 1: Overview of a proposed system

E- Commerce is an online business where one can sell and buy goods and services on the internet. These transactions are executed by transfer of data and money from one account to the other. E-commerce websites are built for secure web payments and financial transactions. With the invention of next-generation currency, the crypto currency financial and commercial transactions are much faster and secure. Blockchain technology is the next big thing that offers a distributed database providing unaltered public records of digital transactions. The chain of secured blocks is back linked and as a result they can be traced back to the very first block making it impossible to edit the records. The most interesting factor is the transparent and decentralized nature of these blockchain networks with no middle person, enabling secure online transactions between buyers, seller, and marketplace. Also, the customers can purchase online faster without disclosing their credit card or bank details. The Blockchain apps work differently unlike centralized Web applications. [8] As mentioned in figure 2, the client connects to the webpage (HTML, CSS, JS, Web3 JS) with the help of browser then the webpage will communicate directly with the Ethereum blockchain node that can access all the data in the blockchain and the Ethereum block chain node will interact with the smart contract which will be programmed by the developer, so Etherum blockchain will be central core of the system where it interacts with the client and invoke smart contract.

Component	Description
CPU	Intel(R) Core(TM) i7
Operating System	Ubuntu Linux 18.04.1 LTS
Capacity of RAM	8GB
Supporting Languages	Solidity, web3.js, ReactJS
Node	v8.11.4
Libraries and Frameworks used	Truffle Framework, Ganache Simulator
Crypto wallet	MetaMask crypto wallet

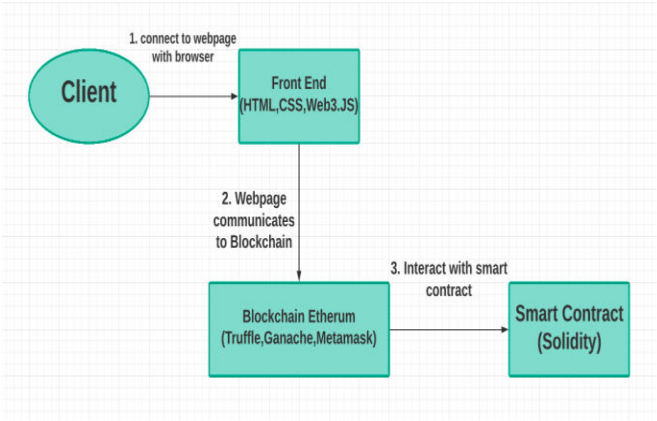

Client
1. connect to webpage with browser
Front End (HTML,CSS,Web3.JS)
2. Webpage communicates to Blockchain
Blockchain Etherum (Truffle,Ganache,Metamask)
3. Interact with smart contract
Smart Contract (Solidity)

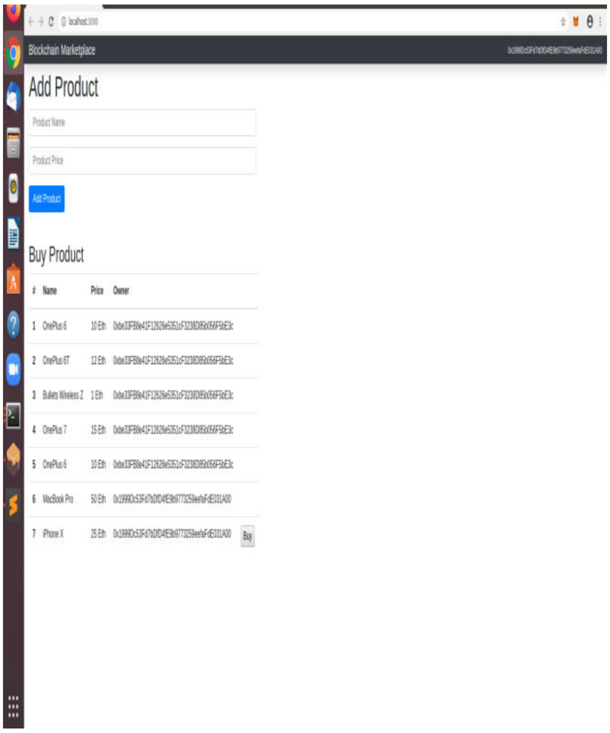
Fig 2: Working model of a proposed system using Ethereum Blockchain

III. IMPLEMENTATION OF A PROPOSED SYSTEM

The development environment of the proposed system is categorized into multiple parts, which are all interconnected and have their own particular functions. All the implementation and experimental work was carried out on a single machine running Ubuntu Linux 18.04 LTS with an Intel Core i7-4700 @ 2.4GHz processor and 8 GB memory. Moreover, we used Truffle as the development environment and Ganache v2.4.0 as a personal Blockchain using which we deployed our smart contract, developed the application and ran the required tests. We used MetaMask, which is a simple extension in the prominent browsers, as the default crypto wallet for the exchange of Ethers during transactions. One of the prerequisites was any NodeJS version above 8.9.4. The smart contract was written using Solidity, which is similar to JavaScript and is fundamental when creating smart contracts for Ethereum. We further used ReactJS for designing the user interface and established connectivity between the UI and smart contract using the web3.eth library available in JavaScript, which is used for the sole purpose of establishing connections in Ethereum. The simulations were run using the 10 sample accounts provided by the Ganache blockchain, all of which contained 100 Ethers (strictly for testing purposes, no monetary value). The client systems act as the nodes who perform the transactions.

The participants in the proposed network are the buyer and seller. The assets include the product ID, product name, and product price and product owner. Initially, the seller can upload any product with their desired price. The buyer views all the products listed in the repository. The products which have not been sold yet will have a *Buy* option. Once the buyer selects a product and sends the request to buy it, he will be shown a MetaMask confirmation which will display his current balance in Ethers. He can then confirm his order and process the transaction. Similarly, the MetaMask extension will also be responsible for showing any errors occurring during the transaction. These errors include the buyer not having enough balance to buy the product and the seller is trying to buy their own product. Once the transaction is processed, the product's *Buy* option will be removed. The product owner asset will be changed as to display the address of the buyer, confirming the purchase. The seller can view his MetaMask account to receive confirmation of the payment. For our testing purposes, we deployed our application on the Kovan test network, using which we were able to monitor the transactions taking place in each account.

Table 1: Development Environment for a proposed system



localhost:3000

Blockchain Marketplace 0x1999Dc53Fd7bDfD4E9b977325 9eefaFdE031A00

Add Product

Product Name

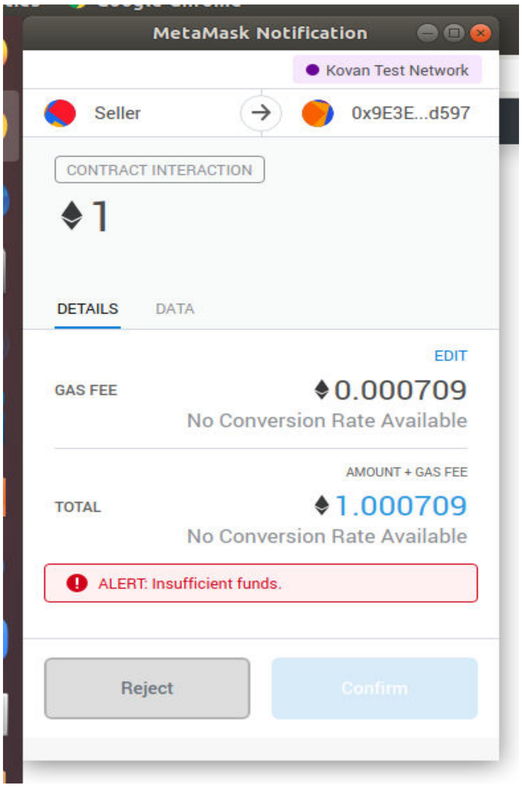
Product Price

Buy Product

#	Name	Price	Owner	
1	OnePlus 6	10 Eth	0xbe33FB8e41F12626e5351cF3238D85b056F5bE3c	
2	OnePlus 6T	12 Eth	0xbe33FB8e41F12626e5351cF3238D85b056F5bE3c	
3	Bullets Wireless Z	1 Eth	0xbe33FB8e41F12626e5351cF3238D85b056F5bE3c	
4	OnePlus 7	15 Eth	0xbe33FB8e41F12626e5351cF3238D85b056F5bE3c	
5	OnePlus 6	10 Eth	0xbe33FB8e41F12626e5351cF3238D85b056F5bE3c	
6	MacBook Pro	50 Eth	0x1999Dc53Fd7bDfD4E9b977325 9eefaFdE031A00	
7	iPhone X	25 Eth	0x1999Dc53Fd7bDfD4E9b977325 9eefaFdE031A00	Buy

Fig 3: Client Side of a proposed System

Figure 3 shows that after logging in into the system, it displays the list of products stored in the Blockchain. Unavailable items will not have an option to ***Buy***. Once the user selects an available product from the list, buyer will be sent the notification to confirm the transaction through MetaMask as given in figure 4. If the buyer and seller have same identities, MetaMask will not let the transaction to proceed. Another error that may pop up is if the user does not have enough Ether in his account to purchase the product.



MetaMask Notification

Kovan Test Network

Seller → 0x9E3E...d597

CONTRACT INTERACTION

1

DETAILS DATA

EDIT

GAS FEE 0.000709
No Conversion Rate Available

AMOUNT + GAS FEE

TOTAL 1.000709
No Conversion Rate Available

ALERT: Insufficient funds.

Fig 4: MetaMask Alert for Confirmation of Transaction and Error Displays

The MetaMask extension will notify the buyer if he has insufficient funds. Only once all the details are checked and the payment is processed, the transfer of ownership will take place.

IV. RESULTS OBTAINED

By combining the functionalities of Truffle, Ganache and MetaMask along with the power of Solidity, ReactJS and JavaScript, we have implemented our proposed work on Ethereum Blockchain for effective trading system using E-commerce platfom. By deploying our system on the Kovan Test Network, we are able to monitor all the transactions being made by the actors present in the network. This Blockchain approach will make transactions much more secure, immutable and transparent.

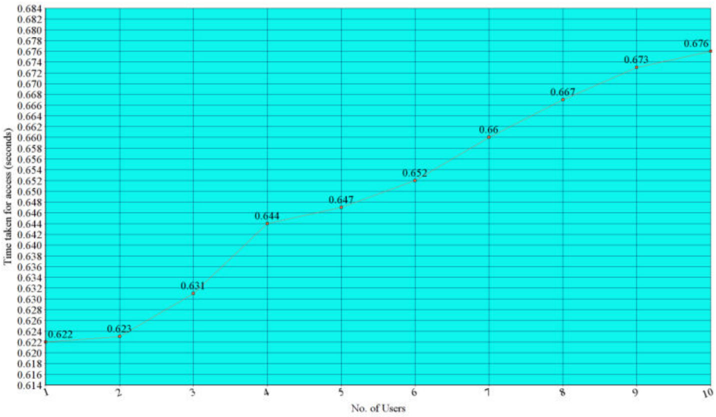


Fig 5: Time taken to access the system functionalities

Results shown in fig 5 is time taken for a user to access the functionalities provided by the system such as uploading time and buying time for a products. This results were obtained by having 10 user accounts provided by the Ganache simulator for testing purposes. As it can derived from the graph, there is a drawback of the time being proportional to the number of users accessing the system at given point of time. All these tests were done using a single browser window on a single machine, thereby increasing the latency. This problem can be reduced by accessing the system from different user machines.

V. CONCLUSION

In this paper, we have presented an efficient solution to automate and decentralized e-commerce based trading system. With the help of the system, many error rates can be reduced which occurs in different stages of the supply-chain and would improve the customer support by a great magnitude. Transaction data should not be trusted in the hands of third-parties, where they are susceptible to steals and misuse. Instead, users should own and control their data without compromising security. With a decentralized platform, making legal and regulatory decisions about collecting, storing and sharing sensitive data about user identities and product identities can be secured, transparent.

REFERENCES

[1] M.M. Aung, Y.S. Chang, "Traceability in a food supply chain: Safety and quality perspectives", Food Control, vol. 39, pp. 172-184, 2014

[2] International Conference on Communication and Signal Processing paper on ‘An Efficient Data Security in Medical Report using Block Chain Technology’ by Anigo Merjora A Published in the year 2019

[3] IEEE paper of ‘Data Management in Supply Chain Using Blockchain: Challenges and A Case Study’ by Hanqing Wu, Jiannong Cao, Yanni Yang, Cheung Leong Tung, Shan Jiang, Bin Tang, Yang Liu†, Xiaoqing Wang, Yuming Deng published in the year 2019

[4] International Conference for Convergence in Technology paper on ‘A Fully Observable Supply Chain Management System Using Block Chain and IOT’ by Vishal Naidu, Kumaresan Mudliar, Abhishek Naik Published in the year 2018

[5] International Conference on Communication and Signal Processing(COMSNETS) paper on ‘Traceability of counterfeit medicine supply chain through Blockchain’ by Randhir Kumar, Rakesh Tripathi Published in the year 2019

[6] Christo, M.S. and Meenakshi, S., 2018. Enhancing Rumor Riding protocol in P2P network with Cryptographic puzzle through challenge question method. Computers & Electrical Engineering.

[7] M. Dobrovnik, D. M. Herold, E. W. M. Frst, and S. Kummer, “Blockchain for and in logistics: What to adopt and where to start,”Logistics, vol. 2, no. 3, 2018

[8] K. Biswas, V. Muthukkumarasamy, and W. Lum, “Blockchain based wine supply chain traceability system,” in Future Technologies Conference, Nov. 2017.

[9] “EthereumblockchainSize,”https://etherscan.io/chartsync/chaindefault, Accessed: 2019-04-15.

[10]T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inf. Theory 31(4), 469–472 (1985)

[11]Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf [Accessed March 2017]

[12]source:https://en.wikipedia.org/wiki/Application_programming_interface.

[13]Y. Li, T. Marier-Bienvenue, A. Perron-Brault, X. Wang, and G. Paré, “Blockchain Technology in Business Organizations: A Scoping Review,”no. January, 2018.