IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11593

Developing an E-Commerce Website with Blockchain intergrade.

YUVANRAJ.K[1], THULASIKA.G[2], Mr. SUDHAKAR.G[3]

[1]Dept of Information Technology, Sri Sai Ranganathan Engineering College, Coimbatore, Tamil Nadu, India.

[2]Dept of Computer science engineering, Sri Sai Ranganathan Engineering College, Coimbatore, Tamil Nadu, India.

[3]Asst professor, Dept. of computer science engineering, Sri Sai Ranganathan Engineering College, Coimbatore, Tamil Nadu, India.

Abstract- In this time of web, online business is developing huge amounts at a time keeping the development of physical organizations in the residue. By and large, physical organizations are falling back on having a partner which is web or online business driven. Individuals in the created world and a developing number of individuals in the creating scene currently use online business sites consistently to make their ordinary buys. And the integration of Blockchain technology is an interlinked systematic chain of blocks that contains transaction history and other user data. It is a revolutionary technology that earned its emerging popularity through the usage of digital cryptocurrencies. Even though Blockchain holds a promising scope of development in the online transaction system, it is prone to several security and vulnerability issues.

Keywords: domain modelling; e-commerce; object oriented programming; Blockchain, decentralized, distributed, ledger, security.

1. INTRODUCTION

Electronic trade or web based business alludes to a wide scope of online business exercises for items and administrations. It is typically connected with web based trading over the web or managing any exchange including the exchange of possession or freedoms to utilize labour and products through a PC interceded network. In our eyes we see it as another aspect to the fluctuated utilization of the web and our motivation is to make it popular in our nation where its utilization is especially exceptionally low. As a result of the great setting society it is vital to foster trust among individuals keen on an exchange. Internet business in Bangladesh really began in the extended time of 1999 situated in USA for certain non-inhabitant Bangladeshis. Our aphorism is to create an advanced internet business site in our country that ought to be to a great extent acknowledged by the clients. And Blockchain technology is a peer to peer architecture network. It is decentralized and comprised of a series of blocks known, hence it is called Blockchain. After the initial concept derived and implemented by Satoshi Nakamoto in bitcoin, Blockchain has become a topic of interest among the researchers. Moreover the blocks include hash code, which is a unique and unchangeable value derived using complex mathematical hash function. For this reason, immutability is ensured .Among other characteristics, transparency is ensured by the reasons mentioned above. As the transaction does not happen in traditional way as in with individual real user id and address, there are several scopes to make both the sender and the receiver anonymous.

2. THE PLANNING PROCESS OF WEB DEVELOPMENT

Our objective was to foster a web application that would be adequately alluring, have an expert look and easy to use. So that individuals of all age gatherings would be its end clients. Our occupation began with partitioning the whole undertaking and setting achievements. The achievements would be a marker of level of the work really refined and example of overcoming adversity. The whole arranging process made the accompanying strides.

2.1. Characterizing Use Case Models

Composing use cases or accounts of utilizing a framework - a magnificent strategy to comprehend and portray necessities. An end client with web perusing office empowered registers into our webpage and logs into our website. Adds them into the shopping basket lastly arranges the items online when the electronic duplicate of the bill is consequently produced. In this way, from the expressed use case model we figured out the accompanying to be the essential necessities.

2.2. Space Modelling

As with the majority of the web applications created utilizing the Object Oriented Programming (OOP) we followed something very similar. So we pushed ahead for Object Oriented (OO) investigation. Which accentuates on finding and portraying the articles - or ideas - in the issue space. For instance an item in our framework is an article.

2.3. Design Pattern

Our application has been created utilizing the norm "Model-View-Controller" design. Model view regulator (MVC) is an application compositional example for carrying out UIs. It isolates the application into three interconnected parts; to isolate inner portrayals of data from the manners in which that data is introduced to acknowledge from the client. 'Code igniter' is an open source web improvement system that gave us the help to construct our application utilizing PHP following MVC design. Consequently view fills in as the UI. Regulator has the fundamental class documents to control the information put away in the backend for example the data set.

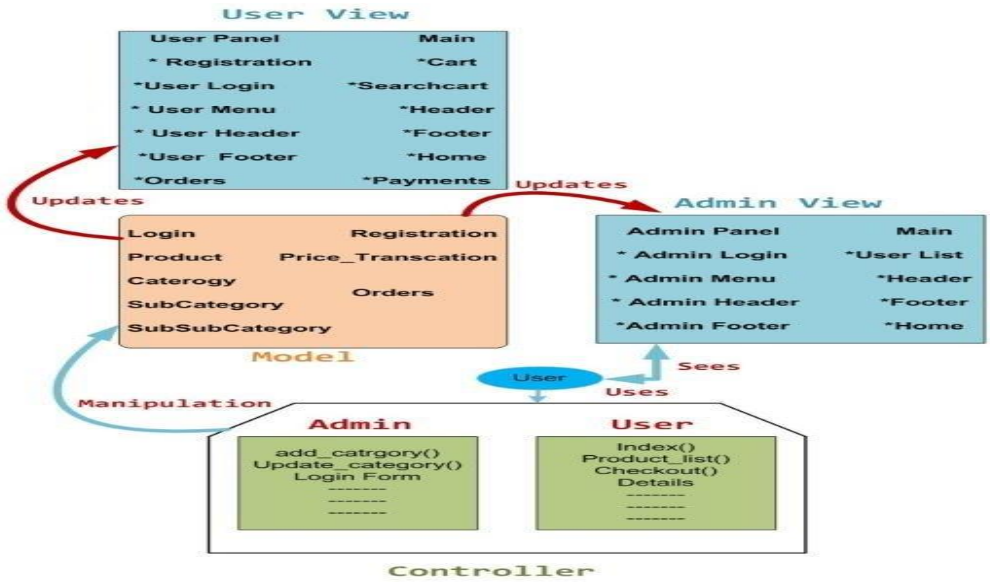

Fig-1.Diagram of model, view and controller of the application.

It really functions as a traffic between the model and view. In any case, it doesn't have the admittance to collaborate with the information base straightforwardly. It can pass data from the view and refreshed data to the view. At long last, the model has the main admittance to our data set it refreshes any data login, enlistment pages additionally costs and items entered by the executive or the end-client.

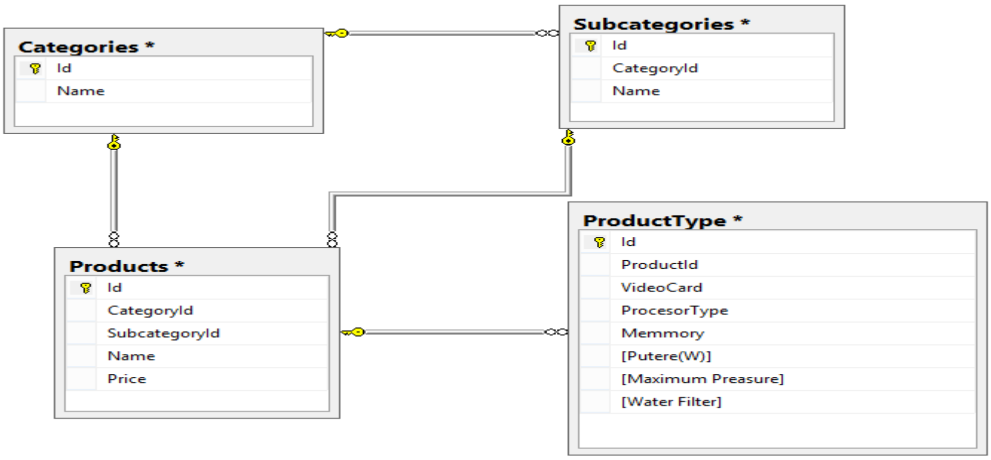

Fig-2. Table of product, Category and customer database

DOI: 10.17148/IJARCCE.2022.11593

3. HOW THE WEB APPLICATION WORKS

A powerful website page is a site page that is created by a server-side program or content. So when we run the program on our neighbourhood PC the web server is the nearby web server. The program makes a Hypertext Transfer Protocol (HTTP) solicitation to the web server for a particular powerful page, the web server then, at that point, looks into the expansion of the mentioned document to figure out which application server ought to handle the solicitation. Frequently, this content purposes the information that it gets from the internet browser to get the fitting information from a data set server. At the point when the application server wraps up handling the information, it creates the HTML for a page and gets back to the webserver.

4. BLOCKCHAIN INTERGRATION

Various Types OF Blockchain

- Public Blockchain
- Private Blockchain
- Hybrid Blockchain
- Consortium Blockchain

4.1. Public Blockchain

Public Blockchain are completely open and follow the idea of decentralisation to the T. Bitcoin and Ethereum are both examples of public Blockchain. Anyone in the network can access the chain and add blocks. A public Blockchain is an open-source, decentralized Blockchain with no restriction of users that can participate in the network. No individual entity has control over the network instead anyone can join the network and read/write/audit the Blockchain with no order for processing the transactions. , the decisions here are made by several consensus algorithms such as Proof of Work (POW), Proof of Stake (POS), and many more.

4.2. Private Blockchain

A private Blockchain has a centralised network that quickens the transaction process. Having a centralised network also raises the issue of trust, which is resolved in a public Blockchain. A transaction's validity cannot be verified on private networks and relies on the authorised nodes' credibility. Private Blockchain restricts the users who can participate and make a transaction in the network.

4.3. Hybrid Blockchain

A hybrid Blockchain is a unique type of Blockchain technology that amalgamates components of both public and private Blockchain or tries to utilise the ideal part of both public and private Blockchain solutions. A hybrid Blockchain is a combination of both the public Blockchain and private Blockchain. It combines the advantages characteristics of each Blockchain, respectively, that is, a hybrid Blockchain inhibits the privacy benefits of private Blockchain and transparency benefits of a public Blockchain according to necessity. The patented Interchain ability gave rise to the hybrid nature of the Blockchain enabling the hybrid Blockchain to have multiple chain networks of Blockchain. . Even though the hybrid Blockchain is controlled by a group of individuals, the transactions made are kept private and yet can be verified whenever needed.

4.4. Consortium Blockchain

Consortium blockchain offers the new kid on the block to join the established structure and share information instead of starting from scratch. This technology helps organizations to find solutions together and save time and development costs. Consortium Blockchain are also known as Federated Blockchain. The primary objective of a consortium blockchain is to ascend cooperation effects to meet the constant challenges of a particular industry. Organizations with common goals can opt for consortium blockchain to revamp transparency, accountability, and workflow. The Deloitte research exhibits that approximately 74% of organizations are opting for blockchain consortiums. Many blockchain platforms are offering themselves as a backbone for various organizational solutions.

5. METHODOLOGY

The digital cryptocurrency Bitcoin uses the first-ever Blockchain technology [2]. For the validation of a transaction, the network must confirm the following conditions: The sender account holds sufficient Bitcoin balance that it intends to transfer. A digital wallet or a cryptocurrency wallet is a string of letters and numbers forming a public address associated with each block in the Blockchain. However, to prove the ownership of the public address there is a private key associated with the wallet that serves as the user’s digital signature that is used to confirm the processing of any transaction. For example, let us consider someone is trying to send you some digital currency such as Bitcoin, as the transaction is being processed, the private key in your wallet should match the crucial public address of your wallet that the currency has been assigned to. If both these keys match, then the digital currency amount is transferred to the public address of your wallet.

6. APPLICATION OF BLOCKCHAIN

Blockchain application can be applied to many sectors in Bangladesh. It either uplifts the existing process or creates new technologies. It will change our lives and protect us from fraud, thief, or any crime. Blockchain provides a secure way of sending digital assent without even knowing third parties. In many sectors, we can use Blockchain. Some of the sectors are:

6.1. Healthcare

Security of Personal information like health data is very important for everyone. These health related information are very valuable as pharmacy companies thrives on these data. Most of the time these data are kept on a hospital server and not in a secured environment too. To prevent health data from falling on the wrong hands and to prevent misuse of these data public Blockchain can be used where health data can on be seen by the doctors if the owner of the data i.e. the patient permits it [6]. Building a system like this will make sure proper security for these data.

6.2. Equity Crowdfunding

Getting money from crowd or supporters of a company/product in exchange of equity/shares in that company known as equity crowdfunding. As people from different background participate in these crowdfunding and they follow different rules and regulations, it becomes very tough to maintain policies. Also not all people will trust the party that is handling all the transactions thus affecting the total amount of money generated.

6.3. Banking

It needs to use blockchain in the tax sector. Blockchain can change the whole system, the way our tax is collected. As blockchain provides accurate information, so if we use this in the tax sector then it will be beneficial for all the people. Sometimes people are argued about paying taxes. They denied paying taxes and claim false information. When someone lying about paying tax, blockchain can immediately give the correct information about tax. As this is immutable people could change the information if they want.

6.4. Smart Power Grid

Blockchain is also used in power grid to supply electrical power to customer. This eliminates fraud. Everyone power consumption will be recorded in the Blockchain ledger. Since everyone has the same ledger no one just claim they used less power than they actually have. Authority also cannot overcharge a customer.

6.5. Smart Delivery System

Making sure we get the right product we ordered online can be a tough job for distribution companies. Delivery relying on third parties can be easily hacked, single point of failure. Once compromised attacker can procure item that was intended for others. Blockchain can remedy this using smart [7]. But using Blockchain for every single item is not practical. There is no need to create a Blockchain system for grocery delivery instead we need one for very valuable items like gold, statues, documents etc. Smart contract based Blockchain can make sure that the right person gets the item.

7. SECURITY ISSUES AND CHALLENGES IN BLOCKCHAIN TECHNOLOGY

Despite cryptographic hash protection and immutability, blockchain suffers from vulnerabilities and challenges. Vulnerabilities lie within the feature itself. Some of the security issues are described below:

7.1. 51% Attack

The consensus algorithm is responsible for selecting the miners to solve the mathematical problem. After solving the mathematical problem, the block is added to the chain, and it is broadcast all over the network. To solve the mathematical problem, it takes a considerable amount of computing power, and the average time is 10 minutes. Owning 50 percent of the total computing power in the network makes that specific miner or the group to control the bitcoin network.

- Moreover, previous blocks can also be changed as the computing power owned by the user/user group is fairly a lot.
- Miners receive it and try to solve the mathematical problem, which is called hashing.

7.2. Unlawful incidents

To buy something online using online, users use third party websites. These third-party websites can be used to buy illegal materials such as weed, drugs, prescriptions, etc. So, the identity of people who are buying it is very much challenging to find out. Wannacry ransomware attacks harmed many people in May 2017. Due to this attack the files were encrypted, and those files were not restored till a ransom has been paid [8]. It was spread through mail attachments and the files were encrypted till the ransom was paid. The ransom was transferred using the bitcoin and the transaction could not be tracked.

DOI: 10.17148/IJARCCE.2022.11593

Table-1: Amount of Each Category Available in Silk Road.

S.No	Category	Item	Percentage (%)
1	Weed	3338	13.7
2	Drugs	2194	9.0
3	Prescriptions	1784	7.3
4	Benzos	1193	4.9
5	Books	955	3.9
6	Cannabis	877	3.6
7	Hash	820	3.4
8	Cocaine	630	2.6
9	Pills	473	1.9
10	Blotter(LSD)	440	1.8

7.3. Inefficient Transaction time

Blockchain uses a distributed ledger system, and it needs proof of work to execute a transfer. For this reason, a mathematical problem has to be solved which takes 10 minutes in case of bitcoin. Bitcoin can transfer only seven transactions per second (TPS). Though other cryptocurrencies can handle more than that, still the transaction time per second is somewhat limited by blockchain. After 2010 study shows that cryptocurrencies can handle a lot more TPS. A chart is given below for understanding - [8] another necessary calculation is transaction confirmation time. Transaction time varies from currency to currency same as the transaction time. Though there is no formal study for both of those but an overview is shown in a tabular form below:

Table-2: Transaction confirmation time for various Cryptocurrencies

Name of the Cryptocurrency	Transaction Confirmation Time
Bitcoin	78 minutes
Ripple	4 seconds
Bitcoin Cash	60 minutes
Litecoin	30 minutes
Ethereum	6 minutes
EOS	1.5 seconds
Tron	5 minutes

7.4. Cryptographic Key

Another vulnerability exists in the cryptographic key. Blockchain uses two keys- public and private keys. Private Key encrypts the data and executes the transfer. Blockchain has no central authority that is why if the private key is lost, there is no way to retrieve the key. Moreover, if the key falls into the wrong hands, there is a high chance of the node to be compromised.

7.5. Distributed Ledger Vulnerability

Blockchain users, distributed ledger. Each node in the network has a copy of the total transaction. If one node is vulnerable and is compromised, the transaction history will be at the hand of the attacker. This is a severe privacy and security issue. In the case of financial transactions, the financial transfer log will be compromised.

7.6. Hard Forks in Blockchain

A hard fork (or hard fork), as it relates to blockchain technology, is a radical change to a network's protocol that makes previously invalid blocks and transactions valid, or vice-versa. A hard fork requires all nodes or users to upgrade to the latest version of the protocol software. Forks may be initiated by developers or members of a crypto community who grow dissatisfied with functionalities offered by existing blockchain implementations.

7.7. Soft Forks in Blockchain

In blockchain technology, a soft fork is a change to the software protocol where only previously valid transaction blocks are made invalid. Because old nodes will recognize the new blocks as valid, a soft fork is backwards-compatible.

DOI: 10.17148/IJARCCE.2022.11593

8. CONCLUSION

One can quit slacking of his internet based business with the assistance of online business application advancement and web improvement arrangements. It is perhaps the least expensive mean of carrying on with work as it is online business improvement that has made it conceivable to decrease cost of advancement of items and administrations. So we are of the assessment that enormous organizations ought to contribute more on innovative work for web based business. As the future scope, the foremost priority is to handle the several security issues that arise from different types of blockchain network such as private blockchain network which is often implemented by a business organization and big enterprises. So trying to develop improved consensus algorithm would result in a cost-effective and more efficient blockchain network.

REFERENCES

[1] “How Blockchain Technology Works. Guide forBeginners,”Cointelegraph. [Online].Available: https://cointelegraph.com/bitcoin-for-beginners/howblockchain-technology-works-guide-for-beginners. [Accessed: 10-Jun-2019].

[2] D. B. Amaba, P. C. Leed, D. T. Ahram, D. A. Sargolzaei, D. J. Daniels, and D. S. Sargolzaei, “Blockchain Technology Innovations,” p. 5, 2017.

[3] M. Wachal, “What is a blockchain wallet? - SoftwareMill Tech Blog,” Medium, 02-Apr-2019. [Online].Available:https://blog.softwaremill.com/what-is-a-blockchain-walletbbb30fbf97f8. [Accessed: 15-Jun-2019].

[4] F. Tschorsch and B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” IEEE Commun. Surv. Tutorials, vol. 18, no. 3, pp. 2084– 2123, 2016. [14]

[5] I.-C. Lin and T.-C. Liao, “A Survey of Blockchain Security Issues and Challenges,” International Journal of Network Security, vol. 19, no. 5, pp. 653–659, Sep. 2017.

[6] A. Rosic, "proof-of-work-vs-proof-of-stake," Blockgeeks, 2017.[Online]. Available: https://blockgeeks.com/guides/proof-of-work-vs-proof-ofstake/. [Accessed tuesday august 2019].

[7] H. Z. &. Z. Z. Zhou, "Analysis and outlook of applications of blockchain technology to equity crowdfundinginChina".:https://www.allerin.com/blog/heres-why-the-tax-sectordesperately-needs-blockchain-now.

[8]H. R. H. a. K. Salah, "Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters," vol. 6, pp. 46781-46793, 2018.