THINK INDIA JOURNAL ISSN: 0971-1260

Vol-22-Issue-16-August-2019

A Framework For Securing Online Transaction Through Block Chain

Nikhil Ravi[1], *Deepak Prashar[2], Amandeep Nagpal[3]

Research Scholar, Department of CSE, LPU, nikhil.11607935@lpu.in

Associate Professor, Department of CSE, LPU, Deepak.prashar@lpu.co.in

Associate Professor, Department of CSE, LPU, Amandeep.nagpal@lpu.co.in

Corresponding Author :- Deepak Prashar

Abstract- This paper focuses on the one of the major cyber fraud pertaining to online payment and its impact on society. Online payment methods are quick and easy. One can get access of online services on our finger tips and can have the record of all payments that are executed. But with the growing popularity of online shopping, the fraudulent activities are increasing simultaneously. E-Commerce fraud is an illegal or false transaction based made though online mode. Fraudulent activities in online payment systems are quite common and are one of the serious problems in most of the e-commerce transactions. In this paper a approach based on the usage of block chain in the online transactions has been given for securing them and also mitigating the effect of various cyber attacks.

Keywords- Block chain, peer to peer, decentralize network, OTP, vishing, fishing, digital signatures, hashing

1. INTRODUCTION

Fraud detection and prevention are too much necessary nowadays. Nowadays, online fraud is increasing extremely high such as credit card fraud, internet banking fraud, and vishing. Vishing is primarily is used by the attackers on a higher note [1]. In vishing, attacker call to target person and talk to them pretending as a bank officer. They ask their card details with One Time Password (OTP). Once they got the same withdraw the amount or make any payment and thus the amount is debited from the victim account. To mitigate the impact of these online threats and attacks there is a need of some techniques or counter measures for securing our transactions. One of the solutions can be block chain technology that is prevailing in the current scenario [2]. Block chain is a decentralized computation and information sharing platform which enables multiple authoritative domains that do not trust each other to collaborate to coordinate and collaborate in a responsible decision-making process. This paper focuses on the working nature of the block chain technology driven by its decentralized nature and also depicts the various advantages that this technology offers owing to its decentralized platform. People prefer online transactions instead of physically going to the shopping stores or banks. The major reasons are the ease of access and you can have the variety of products sitting at one place instead of going out. This paper explores the extent and nature of this problem. The fraudsters usually contact with the victims to get the important information in a tricky way. They can also try to steal the

private data by sending them an email or SMS, can also redirect them to a fraudulent website that look much similar to the payment module of the original website called fishing, or even give them a call. The difference between physical and online payment fraud is, that there is no need of the card while making an online transaction. There are various technologies with which one can secure payment transactions and one of them is to be discussed in this paper that is Block chain thoroughly. Block chain is a highly recommended process to check such illegal issues rising due to the online transactions [3].

According to the 2014 Federal Reserve Board reports, the number of customers using their mobile phones transaction activity is very high. Generally, transaction is an economic activity or financial activity that requires two parties that exchange things happily. Transaction in simple language can also be defined as process of exchanging of products or services that has economic effect to business. In exchanging products or services, must be beneficial for both seller and the buyer. But in case the transactions become havoc for the customers and the seller then definitely its impact can easily be seen on the business gains. So, there is a need of adopting some measures to secure the online transactions and in this direction block chain is one of the best constituents. First of all we should know that why the online payments are more in demand and what are the risks that are associated with them before moving towards the measures to counter them.

2. EASE OF USING FOR ONLINE MODES AND THEIR IMPACT

There are many factors that lead to the growth of online transactions usage and also the alarming affects that seen from these trends. Here, the impact of online transactions is discussed along with the description of various frauds through the online transaction process in hand.

2.1. Online fraud is rising: Online fraud is increasing day by day and it's taking place across various platforms such as one can see in Amazon, Flip Kart or any other commercial website and there are also various institutions which are spending a lot of money so that all these frauds could be stopped [4]. But despite all the efforts fraudsters every time are able to find loop holes and again fraud takes place. It's a crucial problem which needs to be taken into consideration and various methods are required to stop all these from false payment methods and Copycat persons who pretend someone and take control over the network.

2.2. Online payment is an Expanding Trouble: As the online payments are increasing day by day and are in demand more than ever, especially with the help of mobile payments. Not all people are technically aware and knew that there are some fraudsters that are sitting online and are watching their online movements of various users. They send some virus or other malicious links, if user clicks that link the fraudsters have access to their device and that is when frauds happen. Even though having security protocols in our operating systems like firewall and some other inbuilt security features, attack still happens.

2.3 Payment frauds: Fraud is an unethical activity the purpose of which is to harm other parties [5]. Payment fraud is an illegal transaction completed by an unauthorized person. The cyber-

criminals try to steal victim's money, personal property related information, or sensitive information like credit card details, OTPs etc.

2.3.1 Types of payment frauds: The following are the methods of payment fraud:

a) Phishing - The process of fraud in which the sensitive and confidential data like victim's usernames, passwords, credit card information, network credentials and many more are stolen is termed as phishing [6]. It occurs when the unauthorized person behaves as a trusted entity and makes other person to do some specific tasks such as clicking on a malicious link or attachment or sharing the confidential data.

b) Identity theft - A process in which there is an unauthorized use of someone else's identity, for the purpose of gaining financial advantage by fraud means.

c) Page jacking- Hackers try to redirect the users using ecommerce website to a different website which seems very much similar to the original website. The clone website may contain malicious material that hackers can use to disturb a network security system.

d) Merchant identity fraud- In these method cyber criminals creates a merchant account on behalf of seemingly legal business and then they charge stolen credit cards [7]. The criminals then disappear before the cardholders get to know the fraud happened to them.

2.3.2 How does a fraud happen?

Fraudsters are expert in obtaining sensitive information illegally. Hackers usually pretend to behave as authorized person and contact the victims to obtain their sensitive information, then through e-mails, injecting malware to smart phones, instant messaging, phone calls and many more they try to steal their personal data. Cyber criminals usually attack large companies and organizations, to obtain any kind of personal or financial information. When they get the required data successfully, they immediately try to make illegal use of that information. Sometimes in some cases the information obtained illegally is sold to a 3rd party, and usually not used by the initial thieves themselves. Criminals usually check the stolen credit cards that whether they are of any use or not by making small online transactions and if the transaction is successful, they will try to make purchases larger.

Impacts of online payment frauds on the financial sector:

a) Loss of reputation: Such security issues can affect the company's reputation badly and the reputation can affect new clients and the relationships with old clients, partners and investors.

b) Loss of client trust: Online fraud causes a loss of clients or affects the relationship with the existing clients. It can lead to the loss of trust from client

c) Loss of income: Loss of clients leads to loss in business, somehow affecting the business.

d) Profit or Loss: Online fraud has an impact on the financial sector that can or cannot be recovered.

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

Transaction Entities involved in online payment: There are two modes of transactions:

a) **Paper based methods**: Cheque, Demand Draft

b) **Electronic based methods**: Credit & Debit card E-cash coupon, Internet banking system Mobile wallet, National Electronic Funds Transfer (NEFT), Real Time Gross Settlement (RTGS)

3. BLOCK CHAIN AND ITS ROLE IN ONLINE TRANSCTION

In easy language one can define block chain as a chain of blocks where block means digital information and chain means public databases where the information is being stored. Blocks store the information of the transaction made like date, time, who is involved in the transactions. Each block stores a unique code called "hash" that distinguishes each block from every other block. Block chain allows users to keep records of all transparent, cryptographically encrypted transactions [8]. The records are kept and maintained in a decentralized manner independent of local authorities and banks, therefore it provides better security, and is much more difficult to cause damage or to make unauthorized changing in the records. Once a payment is verified, it is kept in a block. Each node on the network keeps a copy of blocks and the blocks are connected to each other creating a chain. Complete process happens in a much secure way, and quickly, therefore there are lesser chances of occurring fraud in payments. If the criminals even try to do the alterations to the data, he has to gain the at least 70% access to that network which is practically not possible.

3.1 Block chain Architecture:

Block chain include a block chain and a shared network, a distributed accountability-tolerant database and a block-only add on system for managing records. All block chain users must use the blocks available; once changed cannot be removed [9]. Moreover, block also contains a time stamp that represents the block's creation time and a random number for the cryptographic operations. The block chain network contains joints that hold the block chain distributed peer-to-peer. The working of the block chain network is described in the Fig.1 below.

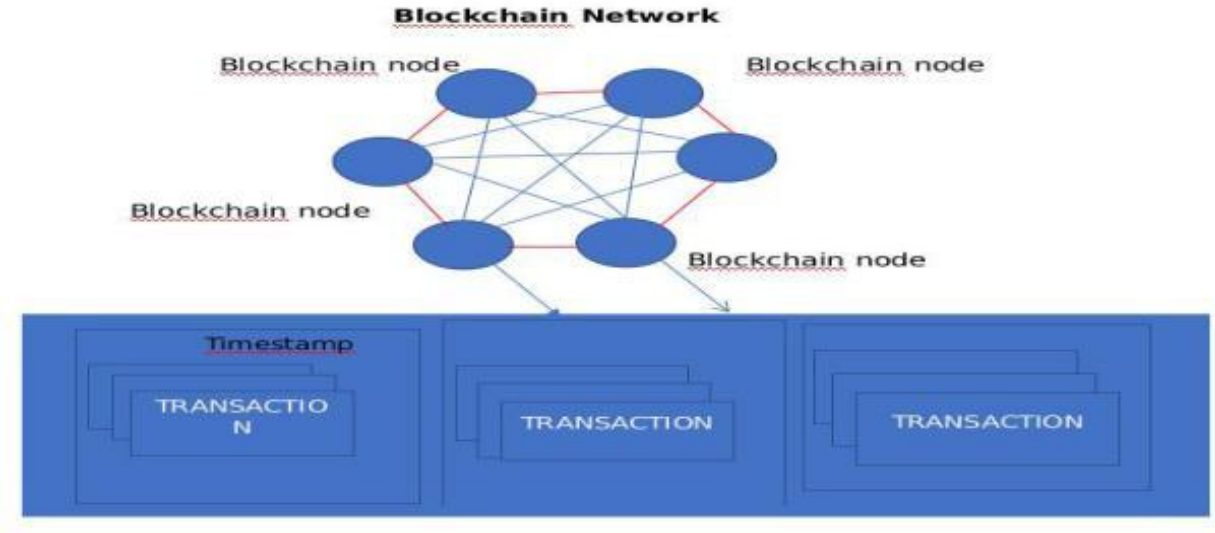

Fig1. Block chain network and its connectivity with the online transaction attributes

3.2 How can Block chain technology is beneficial in prevention of payment fraud:

Block chain has some important and valuable features that can prevent illegal activities in payment processing and can stop payment frauds [10-14]. It is impossible to disable the system as it functions on various devices worldwide at same time and all the systems storing the records of transactions cannot be hacked at once. As it is a chain or a collection of blocks that are distinct in nature, system keeps a record of transactions in each block. If any corrections or alterations are done in these records, it is easier to verify and check in complete system of block validates. Any Illegal action is noticed immediately and the involved parties are disabled from making such transactions. Also the record entered to the system cannot be deleted, in this way it provides a benefit for fraud detection. In Block chain technology validation and confirmation of the transactions are only possible with digital signatures.

Reasons for using block chain to secure online payments: Hackers mostly target banks, companies etc where the data is stored in a single database.

- Block chain provides the complete authorization of payments and transactions [14].
- As the users have the access to all the records of transactions on block chain ledger, it makes it secure and unchangeable.
- Transaction records can be reviewed any time and this is possible as each block of data contains the details of previous blocks.
- Once a transaction record is stored into the block, a hash (security key or password) is assigned to it, because of which it becomes unbreakable and more secure.
- Block chain makes the international transactions private, pocket friendly and safe.

In traditional architecture of World Wide Web, the server keeps all the information in one place because the server is a centralized database which is controlled by various administrators. But, in case of block chain the network is distributed, each entity in the network is capable of approving, maintaining and updating new entries. The system is decentralized and not controlled by every individual in the network. This network consists of many computers but the data records cannot be updated or altered without the permission of whole network.

4. BLOCK CHAIN PROTOCOLS AND WORKING

In this section, we are discussing about the protocols that are required in order to deploy any block chain based application as per the requirement of the user. In this case we are considering the online transaction that is to secure using block chain.

4.1 Protocol design:

Block chain is two types, which is single chain and another is multi chain. It is supports both of them. We have to design and apply different protocol for trustable online transaction. These are divided into protocols like inter-chain and intra-chain communications.

4.1.1 Intera-chain protocol:

It is based on single block chain, which is used to achieve on single data. The common agreement protocols used for single block chains, they have own are: PoW, PoS, DPoS.

a) **PoW(Proof of Work):-** It is the first exploit agreement protocols so, that is calculation based. It has data item, which is time taking to give the output. It is easy to verify by someone, which is specifies [15].

b) **PoS(Proof of Stack):-** It is offer that decide who will be add the next block in block chain [16].

c) **DPoS(Delegated Proof of Stack):-** It is a newer agreement structure. The users have to select some delegate nodes which check the validate block [17]. The performance is calculated such as (network, resource consumption's).

4.1.2 Inter-chain protocol:

It is a systematic and secure communications protocol over the internet. Nowadays, it is very demanding technology for block chain based online transaction, because it is too secure rather than other technology. As per requirement, multi-chain block chain has allowed for huge amount of data storage capacities with high amount of data integrity and transparency. Multi-chain is perfect solutions to protect online transaction from any attack.

5. PROPOSED APPROCH FOR SECURE ONLINE TRANSCTION

In this section the proposed framework for securing the online transaction is discussed thoroughly in terms of the block chain implementation. In this proposed framework there are some major requirements like the digital signatures for the authenticating of the entities that are involved in the transaction in hand , hashing algorithms or approach so that the integrity

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

of the blocks is maintained and last but not the least the integration of the same with the transaction module.

Digital signature approach: Here the concept of public and private keys is used and signatures are generated while the transaction is initiated and they need to be verifying by each one of the blocks before the transactions committed. Hence, the authenticity of each entity is being checked [18]. The working is expressed below:

When Nikhil want Deepak to communicate then the public and private key are required to be generated before starting the dialogue as mentioned below. The steps are described as:

1. The public and private key of Deepak Prashar is:

a) Deepak Prashar is selecting large quantifier's *q* and cyclic function *Fq*.

b) At any time, *g* or element is selected such that *gcd(a,q)=1* and this has been chosen from the cyclic group *Fq.*

c) Then, Deepak calculates *h=ga*

2. Now the values like *F, h = ga, q,* and *g* are published by Deepak Prashar as his public key, retaining a private key.

a) In the cyclic group *F* of the *k* items Nikhil selects *gcd(k,Q)=1*

b) *P=gk* and *s=hk* are determined and *ga* determined and *gak*

c) Nikhil multiples *s* with *M*.

d) Send it*(p, M*s) = (gk, M*s).*

3. Deepak Prashar decrypts the cipher text as

a) Deepak Prashar calculates
$$s' = pa = gak.$$

b) To get *M* as *s=s'* , Deepak divides *M*s* by *s'*

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

Now, we have to think of secure of data block of transaction through implementing of Merkle tree and hash function.

In the Merkle tree, the every leaf node is defined by a data block hash and each node that is anti-blade is set to the labels that are child nodes by cryptography hash. Hash broom tests the quality of large data systems efficiently and safely. Hash trees represent a common number of hash lists and hash chains. One of the key issues is cross-chain communication. Once the hashing of the blocks and their representation is done using the tree then it can be deployed in any platform that supports transactions such as hyper ledger etc. The proposed deployment is represented in the Fig.2 below.

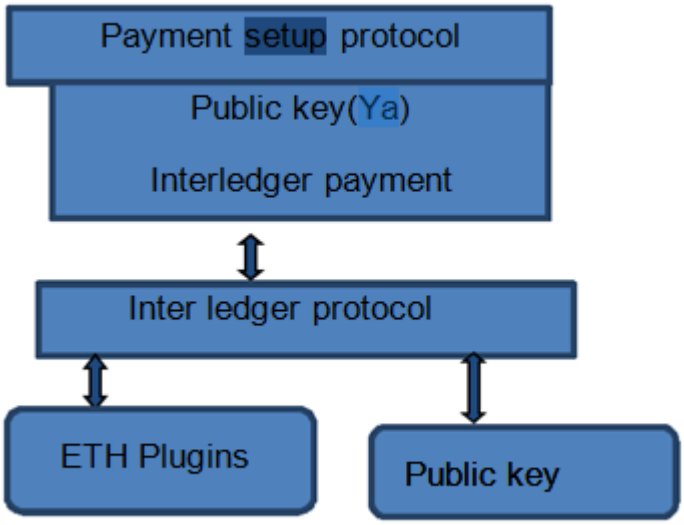

Fig. 2. Proposed deployment model for online transaction based on blockchain

6. CONCLUSION

One of the major challenges which are prevailing in the e-commerce is online frauds and the number is increasing day by day as the online payment platforms are evolving. In order to secure online transitions there is a need of full proof measure and block chain is foreseen as one of the technology that can be used in this context owing to its distributed nature. Block chain can be implemented in online transactions through the integration of some requirements like digital signatures, hashing pertaining to the online transitions. This paper presents a framework for the deployment of block chain in the online transitions to make them secure form cyber threats and

attacks. Once this proposed model is deployed in the applications they become more secure as the possibility of various attacks are reduced to large extent.

REFRENCES

[1] Zhu, Bonnie, Anthony Joseph, and Shankar Sastry. "A taxonomy of cyber attacks on SCADA systems." *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*. IEEE, 2011.

[2] Lewenberg, Yoad, Yonatan Sompolinsky, and Aviv Zohar. "Inclusive block chain protocols." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2015.

[3] Uhr, Joon Sun, Jay Wu Hong, and Joo Han Song. "System and method for verifying forgery of financial institution proof documents on basis of block chain." U.S. Patent Application No. 15/845,224.

[4] Button, Mark, et al. "Online frauds: Learning from victims why they fall for these scams." *Australian & New Zealand journal of criminology* 47.3 (2014): 391-408.

[5] Levi, Michael. "Organized fraud and organizing frauds: Unpacking research on networks and organization." *Criminology & Criminal Justice* 8.4 (2008): 389-419.

[6] Jagatic, Tom N., et al. "Social phishing." *Communications of the ACM* 50.10 (2007): 94-100.

[7] Fichtman, Paul. "Preventing credit card fraud and identity theft: A primer for online merchants." *Information systems security* 10.5 (2001): 1-8.

[8] Gueron, Shay. "Memory encryption for general-purpose processors." *IEEE Security & Privacy* 14.6 (2016): 54-62.

[9] Sharma, Pradip Kumar, Seo Yeon Moon, and Jong Hyuk Park. "Block-VN: A distributed blockchain based vehicular network architecture in smart City." *JIPS* 13.1 (2017): 184-195.

[10] Underwood, Sarah. "Blockchain beyond bitcoin." *Communications of the ACM* 59.11 (2016): 15-17.

[11] Pilkington, Marc. "11 Blockchain technology: principles and applications." *Research handbook on digital transformations* 225 (2016).

[12] Hyvärinen, Hissu, Marten Risius, and Gustav Friis. "A blockchain-based approach towards overcoming financial fraud in public sector services." *Business & Information Systems Engineering* 59.6 (2017): 441-456.

[13] Hoy, Matthew B. "An introduction to the blockchain and its implications for libraries and medicine." *Medical reference services quarterly* 36.3 (2017): 273-279.

[14] Fanning, Kurt, and David P. Centers. "Blockchain and its coming impact on financial services." *Journal of Corporate Accounting & Finance* 27.5 (2016): 53-57.

[15] Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." *International workshop on open problems in network security*. Springer, Cham, 2015.

[16] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 2017.

[17] Chen, Zhixong, and Yixuan Zhu. "Personal archive service system using blockchain technology: case study, promising and challenging." *2017 IEEE International Conference on AI & Mobile Services (AIMS)*. IEEE, 2017.

[18] Anjum, Ashiq, Manu Sporny, and Alan Sill. "Blockchain standards for compliance and trust." *IEEE Cloud Computing* 4.4 (2017): 84-90.

