IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

Online Bank Transaction Using Blockchain Technology

Joel Christopher J[1], Karthikeyan S.E[2], Mukesh K[3], Balaji A.S[4]

Student, B.E. Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[1, 2, 3]

Assistant Professor - CSE, Anand Institute of Higher Technology, Chennai, India[4]

Abstract: Bank Systems require a better security to protect the Accounts, User Information and Money from hackers and intruders. User needs higher level of protection for their data during Money Transaction through Online Payment systems. There are some possible ways for hackers to retrieve user information through SQL (Structured Query Language) injection attacks. By implementing Blockchain technology, we can overcome SQL injection attacks and it is secure when compared to existing security systems. To prevent from unauthorized users, we use OTP (One Time Password) verification and Automatic generated call alert through Google account instead of SIM (Subscriber Identity Module) card based SMS (Short Message Service) alert.

Keywords: Blockchain, Bank, Transaction, OTP, SQL injection attack.

I. INTRODUCTION

Blockchain is a growing list of records, called blocks and they are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Blockchain are decentralized. The decentralized transaction ledger of Blockchain could be employed to register, confirm, and send all kinds of contracts to other parties in the network. 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 alteration of all subsequent blocks, which requires consensus of the network majority. Although Blockchain records are not unalterable, Blockchain are considered secure by design. In addition to Blockchain, OTP (One Time Password) verification and Call alert feature through Google account instead of SIM (Subscriber Identity Module) card OTP verification provides more security from unauthorized access. As banks need to make numerous transactions every day, Blockchain technology could be of enormous significance by bringing in security and genuineness in transactions. Endorsing an idea of trust economy, Blockchain can give financial institutions an opportunity to win the faith and confidence of their customers. Blockchain is a technological advancement that will transform the financial services provided by banks. The global financial system serves billions of individuals and businesses, bringing in trillions of dollars in circulation every day.

II. EXISTING SYSTEM

The existing Blockchain frameworks in Online Bank transaction can be used for constructing Blockchain system. But, existing Bank transaction systems use Blockchain for only retrieving data. User can voted twice or thrice. No attackers used in previous process. SIM (Subscriber Identity Module) card based OTP and call verification systems are used in Existing systems.

III. SYSTEM ARCHITECTURE

The System uses SHA-256 (Secure Hash Algorithm - 256 Bit) Encryption and Decryption. Blockchain frameworks are used for constructing blocks during the transaction process. Permissioned Blockchain builds on the idea of P2P (Peer-to-Peer) networks and provides a universal data set that every actor can trust, even though they might not know or trust each other. It provides a shared and trusted ledger of transactions, where immutable and encrypted copies of information are stored on every node in the network. OTP generator used in the Transaction module helps in identifying user, if wrong OTP entered the call alert functionality makes immediate call and automatically abort the transaction.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

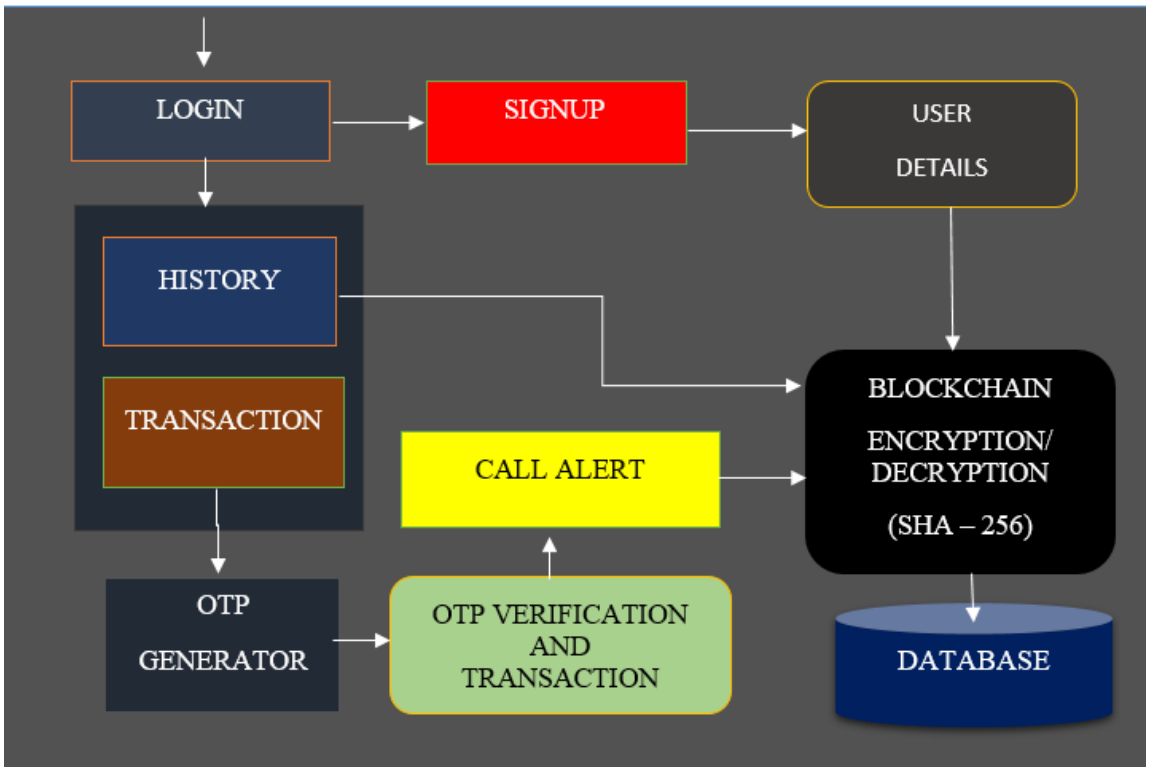

Fig .1 Architecture of proposed Bank Transaction system.

IV. MODULES

A. UI (User Interface) Module

This module provides Front end UI of our system without Blockchain support/storage. It shows banking transactions without Blockchain i.e. using simple database storage. It allows to client signup with system and makes transactions, request fund from trusted party by exchanging currency. Trusted party has rights to transfer fund on request. System generates account identifier using SHA-256 algorithm and uses GUID (Globally Unique Identifier) to differentiate transactions from each other. In addition of that, it provides interfaces for login, dashboard, history, signup and transaction. To make system more secure it uses OTP and Call alert during transaction process.

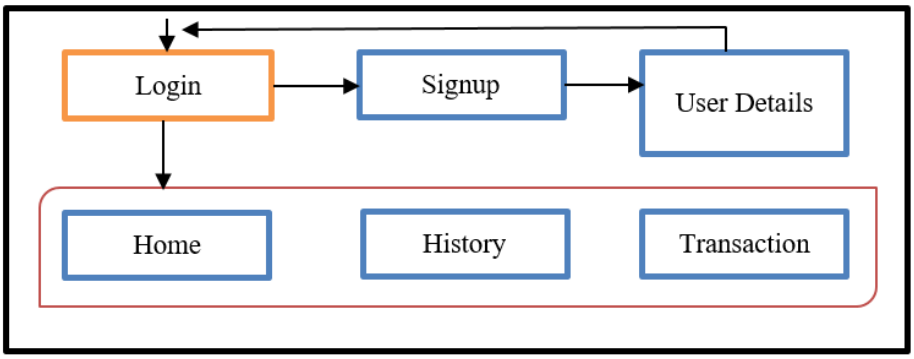

Fig .2 User Interface Module

B. OTP Verification and Call alert Module

In this module, the OTP generator automatically generates OTP and send to the user's Gmail and the user should enter the OTP during Transaction process. Then OTP is verified. If the OTP is wrongly entered then Call alert is made to the User's device (Mobile) through registered Google account. Then the Transaction is automatically aborted. By using internet based OTP, provides more security compared to the existing SIM card based SMS OTP verification.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

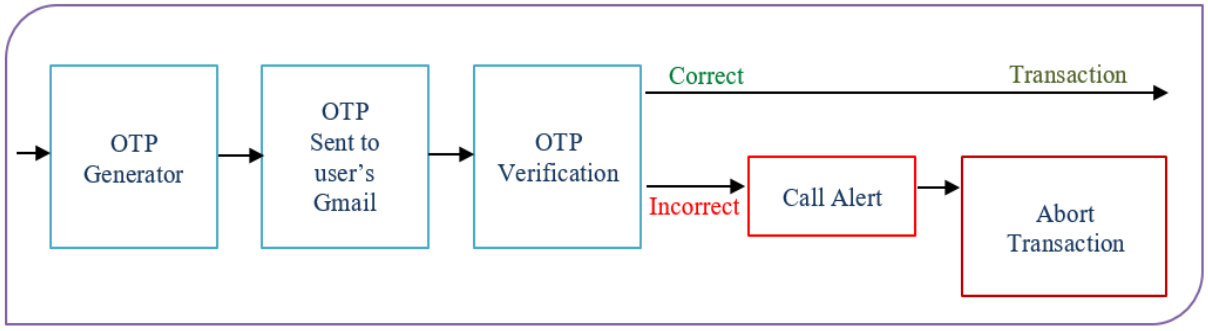

Fig .3 OTP and Call alert Module.

C. Block Generator and Web Miner Module

In this module Blockchain is on a single node/server and a simple proof of work (mining) System. Blockchain is a chain/list of blocks. Each block has their own hash/digital signature. Once Blockchain is formed then integrity by looping through blocks in Blockchain can be verified i.e. checking current block previous hash is same as previous block hash and current hash with newly calculated hash. This is called as "Proof of Work". Any tampering with old block requires to create whole block chain again. The Permissioned Blockchain system is used for the construction of block. When we compared permissioned Blockchain to public Blockchain, they offer better performance. The core reason behind is the limited number of nodes on the platform. This removes the unnecessary computations required to reach consensus on the network, improving the overall performance. On top of that, permissioned networks have their own pre-determined nodes for validating a transaction. Permissioned networks also make proper use of Blockchain, including utilizing its decentralized nature for data storage.

Permissioned networks do come with an appropriate structure of governance. This means that they are organized. Administrators also require less time to update the rules over the network, which is considerably faster when compared to public Blockchain. Public Blockchain network suffers from the consensus problem as not all nodes work together to get the new update implemented. These nodes might place their self-interest above the needs of the Blockchain, which, in return, means slower updates to the whole network. In comparison, permissioned Blockchain doesn't have the problem, as the nodes work together to move the updates faster.

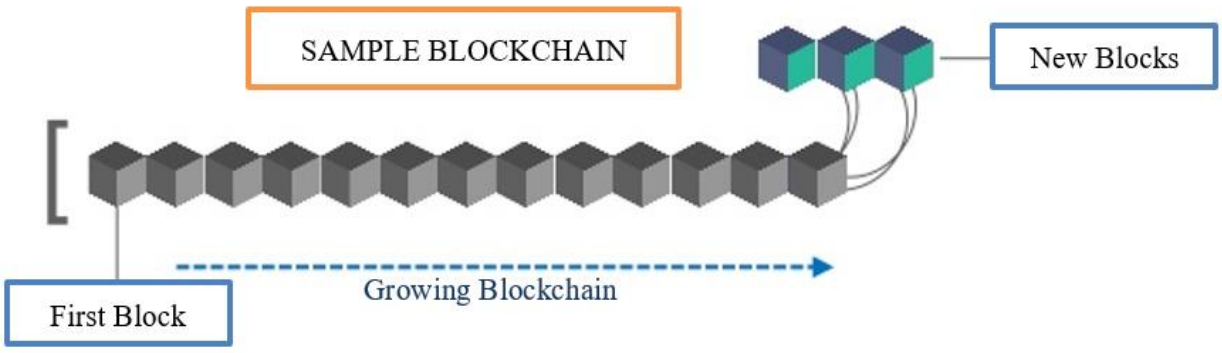

Fig .4 Blockchain Generation.

D. Transactions and Wallet Module

Here, data is replaced with Transaction details and customer's wallet with public and private keys generated using Elliptic-curve cryptography. Here, public key will acts as sender address hence it is OK to send share public key with others to receive payment. Our private key is used to sign our transactions so that nobody can spend/use our amount other than owner of private key. During transaction, public key will be sent and can be used to verify that our signature is valid and data is not tampered. Because, signature consists of Sender + receiver + amount. The private key is used to sign the data we don't want to be tampered with. The public key is used to verify the signature i.e. its integrity.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

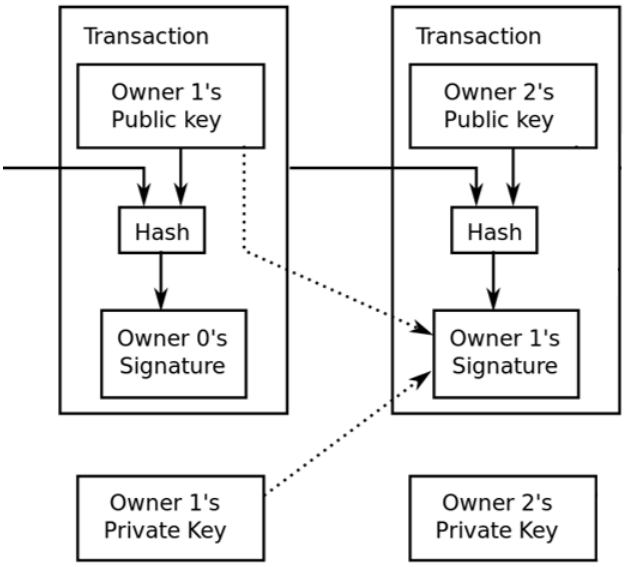

Fig .5 Transaction representation.

E. Peer to Peer Networks to Node

In this 2/3 nodes are used to form P2P networks. Each node will maintain their copy of Blockchain and Web miner will verify integrity throughout network. Here, Proof-of-Authority (PoA) used as a consensus algorithm which can be used for permissioned ledgers. It uses a set of 'authorities', which are designated nodes that are allowed to create new blocks and secure the ledger. Ledgers using PoA require sign-off by a majority of authorities in order for the Block creation. And Block Storage is nothing but ledger and database to store details of Blockchain. "Proof-of-Work" is mechanism that enables distributed control over ledge. It is based on the combinations of economic incentives and cryptography. "Proof-of-Work" makes it very difficult to falsify the Blockchain, due to the prohibitively large amount of computing power that would be required to do so. Blockchain therefore uses traceability as well as a higher statistical security against counterfeiting than conventional information system, without the need for trusted intermediaries.

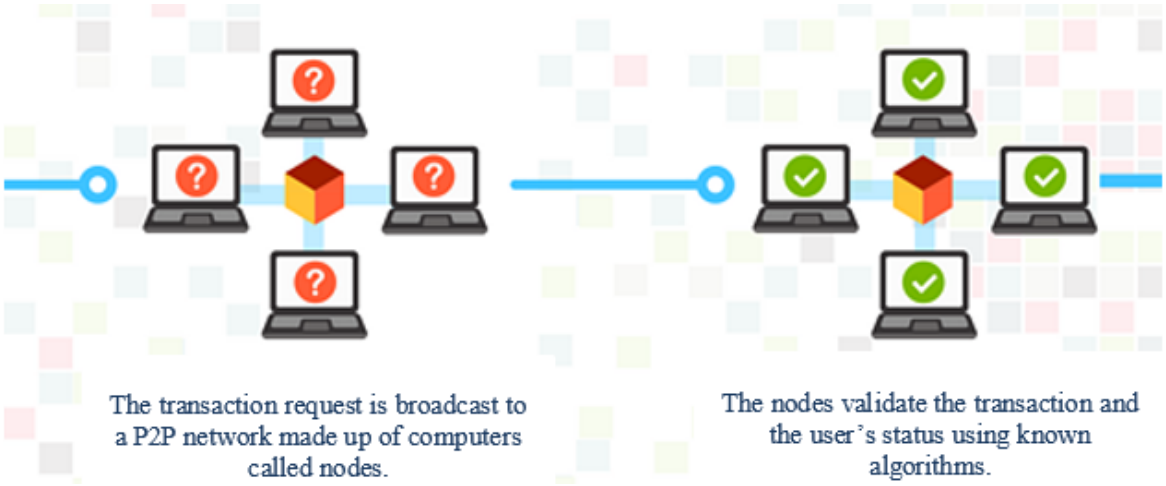

Fig .6 Peer-to-Peer Network validation.

V. APPLICATIONS

1. Asset Management: Trade processing and Settlement.
2. Insurance: Claims Processing
3. Payment: Cross-Border Payments
4. Smart contracts
5. Blockchain Internet-of-Things
6. Blockchain Healthcare
7. Blockchain Government Blockchain identity

DOI 10.17148/IJARCCE.2020.9315

VI. CONCLUSION

Although, the potential of Blockchain is widely claimed to be at par with early commercial Internet, banking firms needs to understand the key features of the technology and how it can solve the current business issues as on one hand, internet enabled exchange of data while on other, the Blockchain can involve exchange of value. Banks need to identify opportunities, determine feasibility and impact, and test proof of concepts. However, the questions around regulations will have to be resolved through focused discussions with competent regulatory authorities and incorporation of their thought-process. . They concluded that regulators should engage, intervene at early stage and shape the innovation. This will allow them to understand the technology, assess the risk, and enable the tailor made solutions to their specific obstacles.

VII. FUTURE ENHANCEMENTS

In future the privacy issue in Blockchain can be removed and this theory can be actually implemented in the actual banking system s, which will not only make the banking systems more secure and fast, but also it will help the banks and the government to eradicate the black money problem.

REFERENCES

[1]. Samuel Agbesi ; George Asante " Electronic Voting Recording System Based on Blockchain Technology" DOI: 10.1109/CMI48017.2019.8962142 Date Added to IEEE *Xplore*: 20 January 2020.

[2]. Emre Yavuz; Ali Kaan Koç ; Umut Can Çabuk ; Gökhan Dalkılıç "Towards secure e-voting using ethereum Blockchain" DOI: 10.1109/ISDFS.2018.8355340 Date Added to IEEE *Xplore***:** 07 May 2018.

[3]. Xiwei Xu ; Ingo Weber ; Mark Staples ; Liming Zhu ; Jan Bosch ; Len Bass ; Cesare Pautasso ; Paul Rimba " A Taxonomy of Blockchain-Based Systems for Architecture Design" DOI: 10.1109/ICSA.2017.33 Date Added to IEEE *Xplore*: 18 May 2017.

[4]. Hui Yang ; Haowei Zheng ; Jie Zhang ; Yizhen Wu ; Young Lee ; Yuefeng Ji "Blockchain-based Trusted Authentication in Cloud Radio over Fiber Network for 5G" DOI: 10.1109/ICOCN.2017.8121598 Date Added to IEEE *Xplore*: 01 December 2017.