WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure Banking Transaction Using Blockchain Technology

Sanket A. Adhav[1], Nisar R. Shaikh[2], Kiran S. Tarate[3], Prof. Rote R. R.[4]

Department of Computer Engineering, Samarth Group of Institution College of Engineering Belhe, India
sanketadhav2454@gmail.com, shaikhnisar107@gmail.com, kirantarate800@gmail.com, roterohini4@gmail.com

ABSTRACT:

Banking systems can transition from their traditional methodologies to a digital, immutable, distributed ledger that can be implemented via Blockchain thanks to ever-evolving technologies. Blockchain technology is a peer-to-peer linked distributed structure that can solve the problem of maintaining and recording transactions in a banking system. Transparency, robustness, auditability, and security are all characteristics of blockchain. This paper aims to provide these functionalities in a distributed banking system based on blockchain that is comparable to current methodologies. It will also cover the limitations of blockchain implementation as well as the future scope.

Keywords: *Banking, Blockchain Technology, Transaction, Security.*

1. INTRODUCTION

A blockchain system may be considered as a simply incorruptible cryptographic database where vital and confidential user's information will be recorded. The system is maintained by a net- work of computers, which is accessible to anyone running the software. Blockchain operates as a pseudo-anonymous system that has nonetheless privacy problem in view that all trans- actions are exposed to the general public, even though it is tamper-proof inside the sense of data-integrity. The access control to manage heterogeneous user's confidential records across a couple of MNC establishments and devices had to be cautiously designed. Blockchain itself isn't designed as a massive-scale storage system. Within the context of framework for secure banking, a decentralized storage solution would significantly complement the weak point of blockchain within the perspective. The blockchain network as a decentralized system is extra resilient in that there is no single-point assault or failure compared to centralized systems. However, because all the bit coin transactions are public and everyone has got right of entry to, there already exists analytics equipment that picks out the members within the community based totally on the transaction records [2]. The most important module is blockchain implementation comprises two kinds of records: blocks and transactions. In every block contains a timestamp and a link to a preceding block is supplied via the secure hash algorithm. During the storage, the transaction information into the blockchain system executes various algorithms like SHA for hash generation, mining for generating a valid hash, smart contract for system policy, and consensus for validating current blockchain on all Peer to Peer nodes. Therefore, banking application is more secure. Second thing is that data storage and accessibility. For this point use the Secret Shamir hashing technique and keyword as well as content-based cryptography techniques.

2. PROBLEM DEFINITION AND OBJECTIVES

The world is changing incredibly fast, and we are not all aware of it. Block chain technology and cryptocurrencies are an irreversible advancement that is disrupting established industries and the ways in which we interact financially. For that reason, I believe understanding and being aware of this block chain wave is incredibly important. The existing systems work as centralized architecture in database system.

GOALS AND OBJECTIVES

To implement a decentralized application and designed a online banking security system based on Custom blockchain.

To address the feature of this technology which is it is incorruptible, encrypted, and traceable and permits data synchronization.

To improves the efficiency operations at each stage.

Project Scope & Limitations

In order to overcome weaknesses and inconvenience of online banking security, our pro- posed authentication system is designed to provide greater security and convenience by using user & transaction verification, authentication server & authorization. To address existing security problem, we implementation of a trusted framework for online banking in public cloud using multi-factor authentication using Blockchain Framework. To design and develop an own (custom) blockchain to store all transaction records in se- cure manner. Deploy a dynamic smart contract with consensus algorithm to enhance the transaction clarity to end user.

3. LITERATURE REVIEW

Satoshi Nakamoto et.al [4] mentioned a peer to peer electronic cash system (Bitcoin). 2016. Online Payments or transaction where directly send from one party to another without going through a financial institution which undergoes peer to peer communication. Digital signatures play a role in protection at a limit. The proposed system uses a verification of data and secure transmission of money through bank validation.

Smart Contracts also called crypto-contract, it is a computer program used for transferring / controlling the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy / agreement. These smart contracts are stored on block-chain and BC is an ideal technology to store these contracts due to the ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred / returned or since the transaction actually happened.

Currently CSIRRO team has proposed a new approach to integrate Block on IOT with [2]. In its initial endeavor, he uses smart-home technology to understand how IOT can be blocked. Block wheels are especially used to provide access control system for Smart- Devices Transactions located on Smart-Home. Introducing BC technology in IOT, this search again provides some additional security features; however, every mainstream BC technology must have a concept that does not include the concept of comprehensive algorithms.

4. MOTIVATION

To migrate the centralization of banking transaction into the decentralized approach.

To create a single platform where user can access all bank accounts using blockchain authentication.

To eliminate all physical things dependency which is must require for banking transaction.

To implement such approach on global environment using secure time less time consuming manner. We notice that the decentralized architecture provides the automatic data recovery from different attacks.

According to Ilya Sukhodolski. The Al [3] system presents a prototype of multi-user system for access control over datasets stored in incredible cloud environments. Like other unreliable environments, cloud storage requires the ability to share information securely. Our approach provides access control over data stored in the cloud without the provider’s investment. Access Control Mechanism The main tool is the dynamic feature-based encryption scheme, which has dynamic features. Using Blockchain based decentralized badgers; our systems provide an irrevocable log for accessibility requests for all meaningful security incidents like large financing, access policy assignment, alteration or cancellation. We offer a set of cryptographic protocols that make the secret or secret key of cryptographic operation confidential. The hash code of the sifter text is only transmitted by the block on laser. Our system has been tested on prototype smart contracts and tested on Iterium Blockchain platforms.

5. PROPOSED SYSTEM

A security system is developed by using blockchain for security. The Four important modules in the system are user authentication, user & transaction verification, authentication server & authorization.

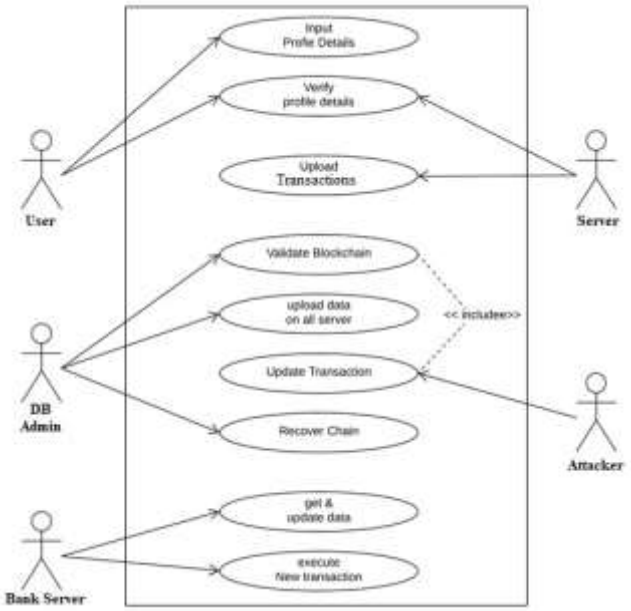
A Blockchain is a digital, immutable, distributed ledger that chronologically records transactions in near real time. Our protection gateway is an extension of the work proposed by blockchain framework.

A blockchain implementation comprises of two kinds of records: blocks and transactions. In each block contains a timestamp and a link to a previous block is provided by the secure hash algorithm.

6. ALGORITHMS

- **Smart Contract:** Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome
- **SHA256 Hash generation:** SHA-256 stands for Secure Hash Algorithm 256-bit and it's used for cryptographic security. Cryptographic hash algorithms produce irreversible and unique hashes. The larger the number of possible hashes, the smaller the chance that two values will create the same hash.
- **Mining:** "Mining" is a metaphor for the computational work that nodes in the network undertake in hopes of earning new tokens. In reality, miners are essentially getting paid for their work as auditors.
- **Consensus:** A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger.
- **Custom Blockchain:** It is a real-time, upgrading technology, supplying users with access permission with an accurate and trustworthy single source

7. USE CASE DIAGRAM



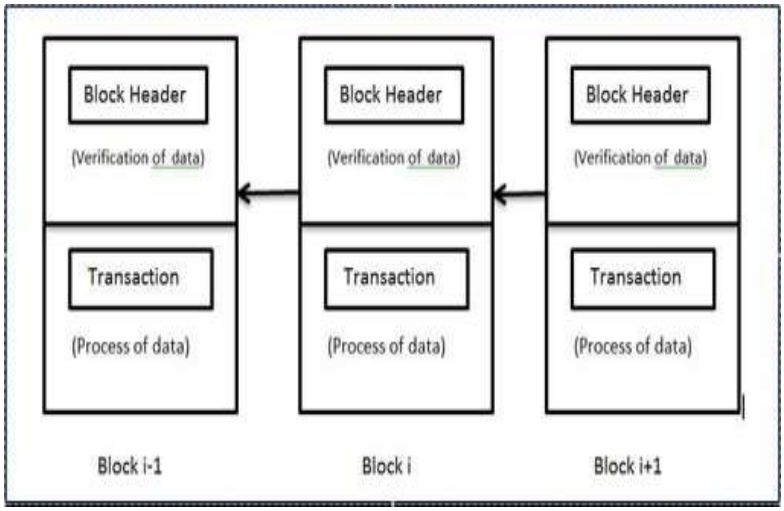
8. ARCHITECTURE OF BLOCKCHAIN

The blockchain is sequence of blocks which hold the information about transactions between nodes of a network.

Block Header consists of Block version, Merkle tree, Time Stamp, n Bit, Nonce, and Parent Block Hash.

- Block version consist of validation rules to be followed by block.
- Hash values of transactions are calculated by merkle tree.
- Current time is saved in time stamp.
- Target Threshold of a legitimate block hash in n-Bit.
- A varied accessory parameter is called Nonce, a 4- Byte (32 bits) field whose values is adjusted by miners during hash calculation.
- Parent Block Hash indicates the pervious block hash value, where block i-1 is executed, block i is under execution and block i+1 is yet to be executed.

Transaction Counter stores the number of transactions that are completed by the block [12].



9. RESULT

Thus, this system would be able to implement a distributed system as well as the banking nodes could be semi automat zed so as to reduce work. We can further have additional banking facilities integrated in the system. And as the finances are involved not all the power is given to the user node i.e. the customers.

A Cryptographically linked Immutable Ledger (Similar to the one used by Bit coin, see Literature Review section for details)

- A Peer-to-Peer Network (Again similar to the one used by Bitcoin which uses DNS Seeding) There are two types of user entities in this protocol:
- **Users:** Read and Write-after-approval to the Blockchain
- **Approvers (Bank):** Reads and Approves writes to the blockchain. But cannot directly write to the Blockchain.

10. CONCLUSION

This proposed system suggests or summaries a secure and efficient way to store data on the cloud. Blockchain-based cloud storage with data encryption gives data security in a decentralize zed structure. The proposed framework for security model is suitable for measures initially used in banking transactions included blockchain technology. The algorithms used to implement the system model are efficient and required less time and give high security for the data which is being stored on the cloud. This kind of architecture makes the system more robust and resistant to different security attacks which are performed by unauthorized users who try to steal and disclose the information in the data files of the user for their benefit. Finally, we conclude that the security level of banking transactions has considerably increased, thus making the overall process of banking much more convenient.

REFERENCES

1. SaboutNagaraju and LathaParthiban, “Trusted framework for online banking in public cloud using multifactor authentication and privacy protection gateway,” Open Access Journal of Cloud Computing: Advances, Systemsand Applications (2015)
2. Dorri, S. S. Kanhere and R. Jurdak, “Blockchainin internet of things: Challenges and Solutions,” arXiv: 1608.05187 [cs], 2019.
3. Sukhodolskiy,Ilya, and Sergey Zapechnikov. “A blockchain-based access control system for cloud storage.” Young Researchers in Electrical and Electronic Engineering (EICon- Rus), 2018 IEEE Conference of Russian IEEE, 2018.
4. Yang, Huihui, and Bian Yang. “A Blockchain-based Approach to the Secure Sharing of Healthcare Data.”Proceedings of the Norwegian Information Security Conference. 2020.
5. Goyal, Vipul, et al. “Attribute-based encryption for fine-grained access control of en- crypted data.” Proceedings of the 13th ACM conference on Computer and communica- tions security. Acm, 2006.
6. Wang, Hao, and Yujiao Song. ”Secure cloud-based EHR system using attribute-based crypto-system and blockchain.” Journal of medical systems 42.8 (2018): 152.
7. Michalevsky Y, Joye M. “Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy”.
8. Wu, Axin, et al. “Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing.” Sensors 18.7 (2018): 2158.
9. Khan S, Khan R. “Multiple authorities’ attribute-based verification mechanism for Blockchain micro-grid transactions”. Energies. 2018 May;11(5):1154.
10. Guo, Rui, et al. “Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems.” IEEE Access 776.99 (2018): 1-12.