Bank Management System using Blockchain

Nalini Jagtap
Asst. Professor
Dr. D. Y. Patil Institute of Engineering,
Management and Research, Akurdi

Vivek Salunke
Student
Dr. D. Y. Patil Institute of Engineering,
Management and Research, Akurdi

Sharvari Joshi
Student
Dr. D. Y. Patil Institute of Engineering,
Management and Research, Akurdi

Rutiksha Bhosale
Student
Dr. D. Y. Patil Institute of Engineering,
Management and Research, Akurdi

Afarin Manyar
Student
Dr. D. Y. Patil Institute of Engineering,
Management and Research, Akurdi

ABSTRACT

Only authorized and legitimate users have access to their database banking data thanks to our remote authentication system. The user will make a cash withdrawal from his account. Users can move money to various accounts by listing the account number. To withdraw money, users must first enter the amount they wish to withdraw and then decide which account they wish to withdraw from (savings account, current account) from all bank accounts of individual users. To make purchases, the user's bank account must have sufficient funds. The blockchain has made remarkable progress in bitcoin, and its decentralization concept has gotten a lot of attention from budgetary foundations, financial markets, and academics. Decentralization is the most important aspect of the blockchain, but it penalizes proficiency, while mining results in high coin exchange costs; in some projects, such as retail, high efficiency, and minimal effort are needed. The consensus algorithm is at the heart of the blockchain. They have power over how a blockchain runs. However, there are still numerous barriers to blockchain innovation, such as adaptability and security problems, that must be addressed. We provide a comprehensive overview of blockchain innovation and blockchain architectures in this article. We also correlate certain average agreement equations used in different blockchain. The proposed framework manages blockchain-based transaction management banking records and automatically recovers data from third-party attacks. It also alerts users to data inconsistency problems throughout transactions.

Keywords

cash, cashless, direct payments, local payment, cross-currency payment, digital, payment, Blockchain.

1. INTRODUCTION

People can do banking, shopping, storing and sharing personal information, and almost everything online today. To access these services securely is very critical. Many authentication methods are available such as username and password, barcode, fingerprint, and face detection. But these authentication methods come with some advantages as well as disadvantages. Username and password are not safe anymore. Common users can't afford the methods of fingerprints and face identity since they are costly. To overcome all the drawbacks the Blockchain technology is introduced for online banking transactions. Blockchain-based online banking is used in banking transactions for security; it provides more security than a barcode and other techniques. Banks provide a way to economically develop people and countries. They make it easy, safe, and convenient for financial trading. Banks are involved in welfare activities and contribute to individual social causes as well. In India, most banks provide passbooks, Automated Teller Machines (ATM), e-banking, mobile banking, and telephone banking for financial relationships. Motivation came from To migrate the centralization of banking transactions into the decentralized approach. To create a single platform where users can access all bank accounts using biometric authentication. To eliminate all physical things, dependency is required for banking transactions. To implement such an approach in a global environment using secure and less time-consuming manners. It can be noticed that the decentralized architecture can provide automatic data recovery from different attacks. E-banking and mobile banking will be more convenient for busy individuals among these financial deals. Blockchain is essentially the technique that provides for various transactional systems to store decentralized approach data. Basically, during data transactions, it is implemented to achieve the highest data security and eliminate different network and data attacks from malicious requests. They are the process that is followed by the entire system.

2. LITERATURE SURVEY

According to [1] a basic IoT Blockchain fusion model with four layers contains different types of IoT devices. Distributed file systems are considered in the model to store huge amounts of IoT data. A case study for a blockchain-based IoT program, a Machine-to-Machine (M2M) autonomous trading system, is then proposed on the Ethereum blockchain. The proof-of-concept is implemented using two Raspberry Pis to communicate with smart contracts for system registration, data storage, service provision, and fair payment. The proposed framework demonstrates how blockchain can enhance accountability, traceability, and protection in IoT applications. According to [2] Edgence (EDGe + intelligENCE) is proposed to serve as a blockchain-enabled edge-computing platform to intelligently manage massive decentralized applications (dApps) in IoT usecases1. To extend the range of blockchain to IoT-based dApps, Edgence adopts master node technology to connect a closed blockchain-based system to the real world. A master node is a blockchain full node with collateral that is deployed on a mobile edge computing edge cloud, allowing the master node to use the edge cloud's resources to operate IoT apps. HCloud, a trusted JointCloud framework for IoT systems using a serverless computing model, is described in [3]. HCloud enables the implementation of several IoT servers and schedules these functions across multiple clouds based on a schedule policy. The required functionalities, execution resources, latency, price are included in the policy specified by the client. HCloud gathers information about each cloud's status and routes serverless functions to the most appropriate cloud based on the scheduling policy. By using blockchain technology, we assure that our system can neither fake the cloud status nor wrongly dispatch the target functions. According to [4], it introduces the concept of a decentralized gasified service exchange platform where the solution providers can dynamically offer and request services in an autonomous peer-to-peer fashion. Cost and decision to exchange services are set during operation time based on gasification policies according to business goals. The proposed concept is based on technology to provide a tokenized economy where the IoT solution providers can implement gamification techniques using smart contracts to maximize profits during service offering and requesting. A gesture-based safe interaction framework with smart home IoT health devices to help elderly or special needs people, according to [5]. The platform uses a decentralized blockchain consensus to store smart home IoT health data and user identities. For storing raw multimedia IoT sensory payload and gesture data, the framework uses off-chain solutions. A smart homeowner or service provider will build a cyber-physical space with a protected digital wallet for each human resident and approve IoT health devices using our proposed health monitoring system. More than one approved home resident can use protected tokens and gestures simultaneously to communicate with IoT-based smart home monitoring sensors, register users and IoT health sensory media, and submit transactional values and raw IoT health data payload.

3. PROPOSED SYSTEM

We create multiple banking transaction data and store all transnational data into multiple data nodes. ● To design an approach for a secure multi banking transaction system where the system stores all data in a blockchain manner. ● To create a fog computing environment hierarchy for parallel data processing for end user’s applications. ● Each node will hold a specific block for each transaction. ● To design, implement your own SHA family block for the whole blockchain. Each transaction is stored on a dependent blockchain in a cloud environment. ● The same block has been replaced for all nodes and generates a valid blockchain. ● The system will retrieve data from all data nodes and commit the transaction; it should be any kind of DDL, DML as well as DCL transactional query. ● If any blockchain invalidates during the validation of data servers, then the system will automatically recover the whole blockchain using the majority of servers. ● We will address and eliminate the runtime server attacks and recover them using our own blockchain. ● The system will provide each transactional validation, for all servers ● To design and implement a new mining technique for generating new blocks for each transaction. ● To implement a verification algorithm that can validate each peer on every access request. ● Traditional online banking systems may take advantage of the cloud platform to provide customers with cost-effective and high-speed online services. ● The significance of the proposed approach is that the authentication credentials of the users are not revealed to the bank and cloud authentication servers, but allows the servers to perform remote users’ authentication. ● Then, using tokenization and data anonymization techniques, we broaden this investigated mechanism to build a privacy security portal for obscuring and desensitizing customers' account information. ● A security system is developed by using blockchain for security. The Four important modules in the system are registration and login, user & transaction verification, authentication server & authorization.

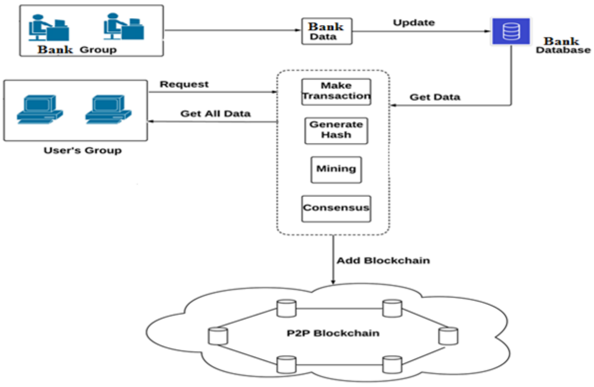

Fig. 1 System Architecture

4. METHODOLOGIES OF PROBLEM-SOLVING

A System has represented by 5 different phases, each phase works with its own dependency System S = (Q, ∑, δ, q0, F) where –

Q - finite set of states.

∑ – alphabet, is a finite set of symbols.

Δ - transition function where $\delta: Q \times \sum \rightarrow Q$

q0 – initial state from where any input is processed ($q0 \in Q$).

F – set of final state/states of Q ($F \subseteq Q$).

If all (n) data nodes have the same blockchain, they will all return 1.

Q = initial transactional data with genesis block

∑ = {SHA-256, Consensus_Val, Mining}

Δ = Validate all server ($S1 \subseteq S2 \subseteq S3 \subseteq S4$) all server validation process

q0 = Initial transaction T [0]

F = {Commit Trans, Get_History_Record}

State =>

1: if all chains are validate or same

0: if any t (n) server consist the invalid chain

5. ADVANTAGES AND DISADVANTAGES

5.1 Advantages

- The single authority can't change once any transaction has been done.
- End-users can view all supply and distribution with a single click where the system generates the transactions' clarity.
- It can easily eliminate different network attacks

5.2 Disadvantages

- Double spending Attacks may be caused due to modification in transaction data.
- To stop the block from verifying a transaction
- To stop miners mining any available block.
- When most transactions were worth considerably more than the block reward and the network hash rate was much lower and vulnerable to reorganization with the introduction of new mining technologies, a majority attack was more feasible.

6. CONCLUSION

The framework offers a stable forum for blockchain multi-banking schemes. The Consensus algorithm can also eradicate various forms of network attacks, such as SQL injection, DOS, etc. Banks can be equipped with blockchain to be able to provide smart financial solutions, speedy processing, reliable storage, and futuristic business features at a good value. Data security and privacy, residency, and legal regulatory laws remain to be top and legitimate concerns preventing banking organizations from adopting blockchain environments. In this system, we described two practical protection mechanisms, the multi-factor authentication, and protection gateway, which enables the banking organizations to maintain their own controls over the customer-sensitive data in a blockchain environment.

7. ACKNOWLEDGEMENT

Our sincere thanks to Mrs. Nalini Jagtap, an expert, for her constant support and guidance during the creation of our project, as well as the Department of Computer Engineering Of Dr. D. Y. Patil Institute Of Engineering, Management And Research, Akurdi for making numerous resources available to us.

8. REFERENCES

[1] Gong, Xinglin, Erwu Liu, and Rui Wang. Blockchain-Based IoT Application Using Smart Contracts: Case Study of M2M Autonomous Trading 2020 5th International Conference on Computer and Communication Systems (ICCCS). IEEE, 2020.

[2] Xu, Jinliang, et al. Edgence: A blockchain-enabled edge-computing platform for intelligent IoT-based dApps China Communications 17.4 (2020): 78-87.

[3] Huang, Zheng, Zeyu Mi, and Zhichao Hua. HCloud: A trusted Joint Cloud serverless platform for IoT systems with blockchain China Communications 17.9 (2020): 1-10.

[4] Gheitanchi, Shahin. Gamified service exchange platform on blockchain for IoT business agility & 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020.

[5] Rahman, Md Abdur, et al. A Natural User Interface and Blockchain-Based In-Home Smart Health Monitoring System. 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE, 2020.

[6] “Smart Contracts,” http://searchcompliance.techtarget.com/definit ion/ smart-contract, 2020, [Online; accessed 4-Dec- 2020]

[7] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain internet of things: Challenges and Solutions,”arXiv: 1608.05187 [cs], 2019. [Online].