isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 3 ,Apr,2024 ,ISSN_NO: 2321-3337

IMPLEMENTATION OF TRACEABILITY AND SINGLE CARD BASED SECURED TRANSACTION SYSTEM USING BLOCK CHAIN TECHNOLOGY

Mohamed Ashik T[1], Naveenprasanth R[2], Surya R[3], Shanmugavalli H[4*]

[123]UG Scholar-Dept.CSE, GRT Institute of Engineering & Technology, Tiruttani.

[4*]Assistant Professor-Dept.CSE, GRT Institute of Engineering & Technology, Tiruttani.

mashik10695@gmail.com, 124naveenprasanth@gmail.com, surya05121997@gmail.com,

***Corresponding Author: shanmugavalli.h@grt.edu.in**

Abstract

This project introduces a novel approach to enhance blockchain technology by integrating single card-based transactions to ensure traceability and security. The current limitation faced in India is the ban on bitcoin transactions and blockchain banking systems due to their untrace ability. In this project, we propose a solution that deploys a user unique/single ID-based transaction system, enabling all transactions to be conducted through a single card. Each user ID is mapped to a single ID, ensuring traceability and security. This system not only facilitates secure banking implementation using blockchain but also enables easy tracking of all transactions by the government. Additionally, we incorporate fog computing concepts for efficient data transfer to the cloud.

Keywords: *Blockchain, Single Card Transactions, Traceability, Security, Fog Computing, Banking.*

1. Introduction

Cryptocurrency, originating from the 2008 white paper authored by the pseudonymous "Satoshi Nakamoto," emerged via a cryptography mailing list. This seminal document resembled an academic paper and introduced the concept of cryptocurrency—a digital currency aiming to blend the advantageous characteristics of physical cash with electronic transaction capabilities. To comprehend the unique attributes of physical monetary units and the impetus for digital cash development, it is imperative to analyze a basic cash transaction. Physical cash manifests as tangible objects, typically coins or notes. Upon transfer to another individual, the unit of value contained within the physical object is similarly transferred, obviating the need for intermediary involvement. This direct exchange engenders anonymity between buyer and seller, establishing clear ownership rights. Notably, possession of the physical object confers ownership of its value, ensuring unambiguous property rights without central authority oversight. Moreover, participation in cash transactions is unrestricted, fostering a permissionless ecosystem. However, the necessity for physical proximity between transacting parties poses limitations on cash's utility in certain scenarios. In contrast, digital cash represents an ideal payment system wherein monetary value can be electronically transferred via cash data files. These files, akin to physical cash, possess the advantages of direct ownership transfer and anonymity but can circulate freely on electronic networks. However, a critical challenge arises in the form of the "double spending problem." This problem stems from the ease with which digital data can be copied at negligible cost, rendering duplicates indistinguishable from the original. Consequently, if cash data files are susceptible to duplication and subsequent use as currency, they fail as a viable payment instrument.

2. Related Work

Crypto coin is a popular decentralized digital cash system, but its public blockchain storing transaction details can raise privacy concerns. The zero-coin protocol was developed to hide

transaction links without relying on third parties, but it also opens the door to illegal activities like money laundering. This paper proposes a solution: an auditable decentralized e-cash scheme based on the zero-coin protocol. In this scheme, designated auditors can access transaction link information without granting additional powers such as stopping transfers or confiscating funds. A key technical aspect is the use of non-interactive zero-knowledge proofs (NIZKPs) to embed audit information securely, utilizing the standard Schnarr protocol for discrete logarithms without complex techniques like zk-snarks. This prevents abuse by malicious senders and ensures the integrity of the system without compromising decentralization.[1]

These days, educational databases are growing quickly and hold important details to help students do better. Higher education performance in India is crucial for students, but it's influenced by many things. That's why it's important to create a predictive data mining model. This model helps us figure out the difference between students who excel and those who struggle. In this study, we used an experimental approach to build a database. We cleaned up the raw data by fixing missing information and changing some values. Then, we picked out the most important details. After all this, we had 300 student records. We used these records to build a prediction model based on Bayesian classification.[2]

Predicting stock prices is a fascinating and tough area of research. In developed countries, the strength of their economy is often measured by their stock market performance. Nowadays, stock markets are seen as a lucrative field for trading because they offer potential profits with relatively low risks. This paper explores using data mining techniques to predict stock prices for six major companies listed on the Jordanian stock exchange. The goal is to help investors, managers, decision-makers, and others make informed investment choices. The study applies the k-nearest neighbor algorithm and non-linear regression approach to make these predictions. The results show that the k-nearest neighbor algorithm performs well with a small error rate. This means the predictions were sensible and reasonably accurate. When comparing the predicted prices with the actual stock prices, they were found to be very close and in line with each other.[3]

This paper demonstrates the utility of data mining algorithms in uncovering pedagogically valuable insights within databases sourced from web-based educational platforms. These insights serve a dual purpose: aiding educators in effectively managing their classrooms, gaining deeper insights into student learning behaviors, and facilitating reflective teaching practices; and supporting learners by fostering self-reflection and offering proactive feedback. By leveraging data mining techniques, educators can gain valuable insights into student performance trends, identify areas for improvement in teaching strategies, and tailor instructional approaches to better meet the needs of individual learners. Similarly, learners benefit from the ability to reflect on their own learning progress, receive timely feedback, and engage in self-directed learning activities. Overall, the integration of data mining algorithms into educational systems holds promise for enhancing both teaching and learning experiences by leveraging the wealth of data available in digital learning environments.[4]

New web-based educational tools give researchers a great chance to understand how students learn and what helps them succeed. These tools collect lots of data on how users interact with them, and we can use data mining to analyze this information. In this paper, we describe a method for sorting students into groups to predict their final grades. We look at data from an online education system and use different methods to see which ones work best. By combining these methods, we get much better at predicting grades. We also use a special algorithm called a genetic algorithm to make our predictions even more accurate. This approach helps us identify students who might be struggling early on, especially in big

classes, so teachers can give them the support they need right away.[5]

3.Objective

In the current landscape, transactions involving Bitcoin or other cryptocurrencies pose a significant challenge due to their inherent difficulty in tracking, attributed to the secure blockchain technology they employ. This issue has prompted the Indian government to ban such transactions, citing the inability to effectively monitor them. Consequently, the primary concern identified is the lack of traceability in cryptocurrency transactions. To address this challenge, our project aims to develop a system capable of tracking all financial transactions conducted using blockchain technology. By creating such a system, we seek to enhance transparency and accountability in cryptocurrency transactions, thereby aligning with regulatory requirements and facilitating better oversight by authorities. This endeavor represents a crucial step towards mitigating the risks associated with untraceable transactions and fostering greater trust and confidence in the cryptocurrency ecosystem.

4. Proposed System

A breakthrough has been achieved by integrating single card-based transactions with blockchain technology, addressing the challenge posed by the ban on Bitcoin and blockchain banking in India. The innovative solution involves the introduction of a user-specific or single ID-based transaction system, where each individual is assigned, a unique identifier linked to an overarching ID. This pioneering approach ensures comprehensive transactional capabilities through a single card, enhancing the security and efficiency of banking operations utilizing blockchain technology. Furthermore, it provides the government with effortless traceability and tracking of all transactions, thereby bolstering regulatory oversight. The exclusive reliance on a single card for transactions further simplifies the monitoring of user transaction patterns by governmental authorities. Additionally, the adoption of fog computing concepts facilitates seamless data transfer to the cloud, enhancing operational efficiency and ensuring smooth transaction processing. This integrated system represents a significant advancement in financial technology, offering a secure and transparent framework for banking transactions while meeting regulatory requirements.

5. Architecture Diagram

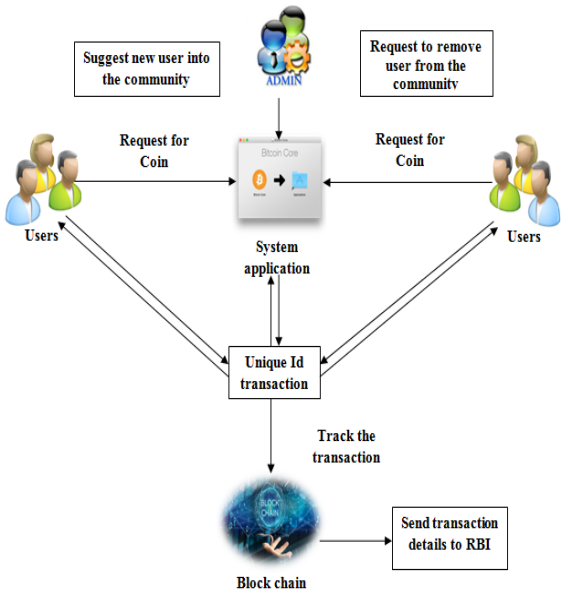

Fig:5.1 Architecture Diagram

6. Algorithms

6.1 Asymmetric Key Cryptography

Asymmetric key encryption, also known as public-key cryptography, involves the use of two keys: a public key and a private key. The public key is shared openly and is used for encryption, while the private key is kept secret and is used for decryption. Messages encrypted with the public key can only be decrypted by the corresponding private key, and vice versa. This system allows for secure communication between parties without the need to exchange secret keys beforehand.

6.2 Digital Signature

A digital signature is a cryptographic technique used to verify the authenticity and integrity of a digital message, document, or software. It works by creating a unique digital fingerprint of the content using a hashing

algorithm and then encrypting that fingerprint with a private key. The recipient can then use the sender's public key to decrypt the signature and verify both the identity of the sender and that the content has not been altered since the signature was created.

6.3 Secure Hashing Algorithm 256

SHA-256 is a widely-used cryptographic hash function that belongs to the SHA-2 (Secure Hash Algorithm 2) family. It takes an input message of any length and produces a fixed-size (256-bit) hash value, which serves as a unique digital fingerprint of the original data. SHA-256 is designed to be computationally secure, meaning that it is computationally infeasible to generate the same hash value for two different inputs or to reconstruct the original message from its hash value.

6.4 Merkle Hashing Tree

A Merkle tree, named after computer scientist Ralph Merkle, is a hierarchical data structure used to efficiently verify the integrity and consistency of large datasets. It is constructed by recursively hashing pairs of data (or hashes) until a single root hash is obtained, called the Merkle root. Each leaf node of the tree represents a data block, and each non-leaf node is the hash of its child nodes. Merkle trees allow for efficient verification of data integrity by comparing just the root hash, and they are commonly used in distributed systems such as blockchain networks to ensure the consistency of the large datasets across multiple nodes.

7. Implementation

7.1 Network Formation

This module initiates the creation of groups within the network, where individuals sign up and become members. Each group is overseen by a Group Admin responsible for keeping track of all activities within the group. Transactions involving Bitcoin-based money transfers occur directly between individuals within the group, following a one-to-one model. This setup ensures that financial transactions are securely processed within the group environment, offering a straightforward and reliable method for exchanging money.

7.2 Group Leader & Member Governance

In this setup, the group leader wields full authority over the group's operations. Any addition or removal of members is conducted solely by the Group Admin, subject to the unanimous approval of all existing group members. When a new member is proposed by any existing member, the request is reviewed by the admin, and only upon receiving approval from every member does the new member gain entry. Should the Group Admin wish to step down, they must first appoint a successor from among the group, who will then assume administrative duties before the former admin's departure is permitted. This system ensures that decisions regarding membership and leadership transitions are made collectively and with careful consideration, fostering a sense of inclusivity and accountability within the group.

7.3 Banking Registration

In this module, every member is required to register their banking details for the purpose of conducting banking transactions within the system. These details are securely stored in the network's database to ensure the confidentiality and integrity of each member's information. It's important to note that the privacy of each member is upheld, as none of the users have access to view the banking details of others. This robust security measure not only protects sensitive financial information but also fosters trust and confidence among members, knowing that their personal data is kept confidential and in their personal data is kept confidential and inaccessible to unauthorized parties.

7.4 Cryptocoin Transfer

At the core of this project lies the main module, where members engage in

Volume: 6, Issue: 3,Special Issue: 3 ,Apr,2024 ,ISSN_NO: 2321-3337

cryptocurrency-based money transfers. When one member initiates a transaction by contacting another member, the recipient has the option to accept or decline the request. If accepted, the transaction takes place within the network using cryptocurrency. These transactions are conducted discreetly, with all details securely maintained within the network. Additionally, to ensure transparency and regulatory compliance, all transactions are updated to the main server, referred to as the model RBI, which serves as the central authority overseeing and recording cryptocurrency transactions within the system. This module streamlines the process of peer-to-peer cryptocurrency transactions while also providing a mechanism for centralized tracking and oversight to uphold security and accountability standards.

7.5 Tracking System

In this module, the banking system undergoes comprehensive tracking facilitated by the centralized main server known as RBI. This server assumes full control over the banks of all users within the network, ensuring meticulous oversight and management. A key advantage of this module compared to existing cryptocurrency systems is the implementation of a robust tracking mechanism. Unlike a to the traditional cryptocurrency, where transactions can be difficult to trace due to their decentralized nature, this module offers a streamlined solution by enabling the complete tracking of money-based cryptocurrency transactions. By centralizing control and maintaining a detailed record of all transactions, the module enhances security, transparency, and accountability within the network, addressing key limitations of with the conventional cryptocurrency systems.

8. Experimental Results

This result discuss about the implementation of the bitcoin request and user registration are identified.

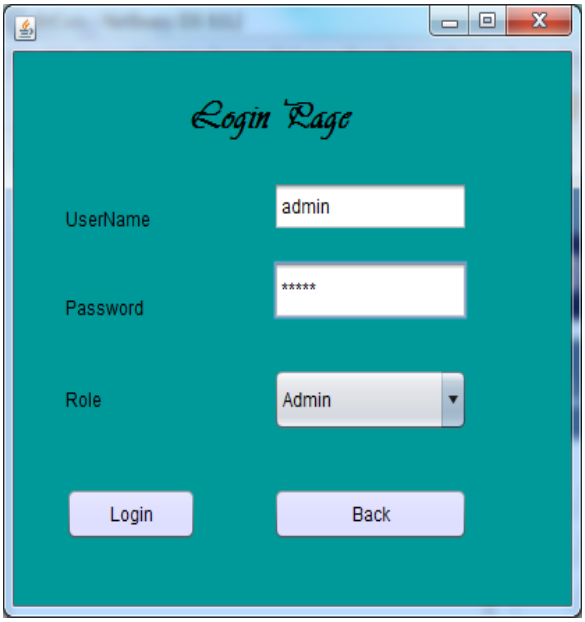

Fig.8.1 Admin Login

Fig.8.2 User Registration

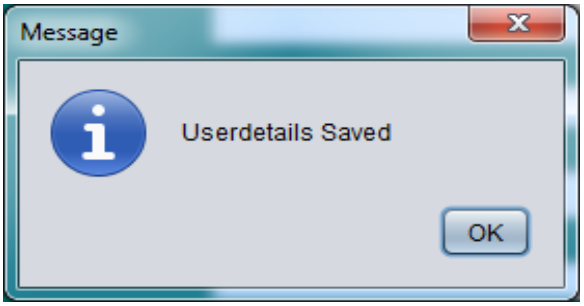

Fig.8.3 Data Saved

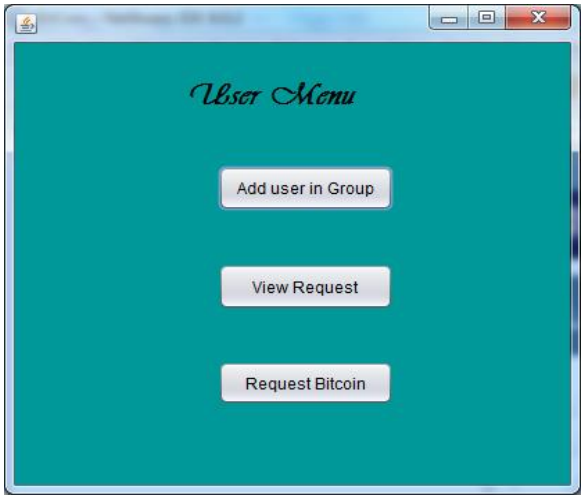

Fig.8.4 User Menu

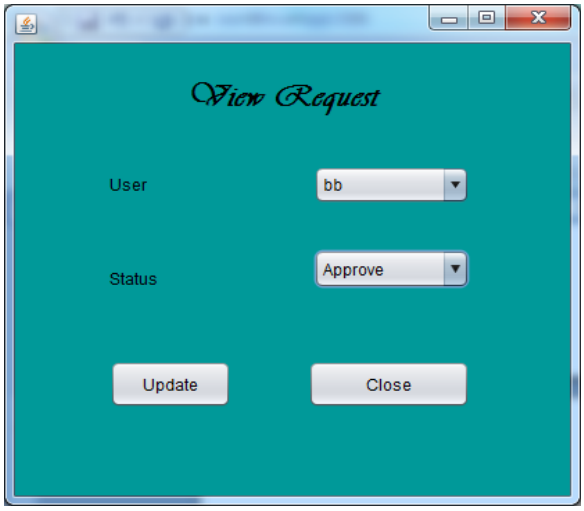

Fig.8.5 Request Menu

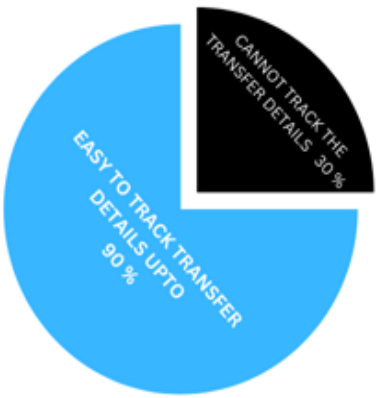

Fig.8.6 Pie Chart

10. Conclusion & Future Work

In this project, we're introducing a single ID card system for tracking purposes. To secure our transaction details, we're utilizing blockchain technology and the future enhancement of this paper has to grouping in chain its concept which should be linked with real-time money transactions to identify the Ponzi scheme of attacks while transferring the transaction.

11.Reference

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] Brijesh Kumar Bhardwaj, Saurabh Pal. “Data Mining: A prediction for performance improvement using classification”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 9, No. 4, April 2011.

[3] Khalid Alkhatib, Hassan Najadat, Ismail Hmeidi and Mohammed L. Ali Shatnawi, “Stock price Prediction Using K-Nearest Neighbor (knn) Algorithm” Vol. 3 No. 3; March 2013

[4] Merceron, A. and is to Yacef, K.,"Educational Data Mining: a Case Study" In Proceedings of the 12th International Conference on Artificial Intelligence in Education AIED 2005, Amsterdam, The Netherlands, IOS Press. 2005.

[5] Minaei-Bidgoli B., Kashy, D. Korte Meyer G., Punch W., "Predicting Student Performance: An Application of Data Mining Methods with an Educational Web-Based System". In the Processing of 33rd ASEE/IEEE conference of Frontiers in Education. 2003.

[6] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[7] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of

digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[8] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[9] A. Back, "Hash cash - a denial of service of the will counter-measure," http://www.hashcash.org/papers/hashcash.pdf , 2002.

[10] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[11] Han, J. and Kamber, M., "Data Mining: Concepts and Techniques", 2nd edition. The Morgan Kaufmann Series in Data Management System, Jim Gray, Series Editor, 2006.

[12] Pandey, U. K. and Pal, S., "Data Mining: A prediction of performer or underperformer using a classification", (IJCSIT) International Journal of Computer Science and Information Technology, Vol. 2(2), 2011, 686- 690, ISSN: 0975-9646.

[13] Alaa el-Halees, "Mining Students Data to Analyze eLearning Behavior: A case Study", 2009.

[14] Varapron P. et al. Using Rough Set theory for Automatic Data Analysis. 29th Congress on Science and Technology of Thailand. 2003.

[15] Romero, C., Ventura, S. and Garcia, E., "Data mining in course management systems: Moodle case study and tutorial". Computers & Education, Vol. 51, No. 1. pp. 368384. 2008.

[16] Bitcoin Block Explorer. [Online]. Available: https://blockexplorer.com/blocks-date/[year-month-day]. Accessed: 13-Jun-2017.

[17] A. Chen, "We Need to Know Who Satoshi Nakamoto Is," *The New Yorker*, 09-May-2016.Available: http://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is. Accessed: 10-Jul-2016.

[18] Has Craig Wright proved he's Bitcoin's Satoshi Nakamoto? BBC News, 2016.http://www.bbc.com/news/technology36191165. Accessed: 10-Jul- 2016.

[19] Cryptocurrency is the Market Capitalizations. HTTPs://coinmarketcap.com .Accessed: 15-Dec-2017.

[20] Bitcoin Charts / Bitcoin Network, Bitcoin Charts. [Online]. Available: http://bitcoincharts.com/bitcoin/. Accessed: 15-Dec-2017.