iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44813

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Preventing Identity Theft using Blockchain Technology

Gaurav Pathare[1], Ritu Patil[2], Prof. Dr. Pragati Goel[3]
[1, 2, 3]*MCA Department, university of mumbai*

Abstract: ***This paper's purpose is to describe what Blockchain Technology is and how it can be used to combat identity theft. Despite the fact that blockchain technology came to existence with Bitcoin, blockchain encompasses a comprehensive potential outside of cryptocurrency. Basically, blockchain could be a shared database that permits multiple parties to access information and verify that data in real-time It can transform the approach that we do things in various industries. It is used for a variety of things besides bitcoin, such as tracking ownership, digital assets, physical assets, and voting rights. It can store and run computer code known as smart contracts.***
Keywords: Blockchain, Bitcoin, Ethereum, Cryptocurrency, Assets.

I. INTRODUCTION

This paper presents the method of detecting or tracking the originality or the ownership of the documents presented by the students for admission purposes or by the medical practitioners whether they are genuine or not (identity theft) by using the blockchain technology. Blockchain is a distributed database system which is decentralised and secure. It is a distributed ledger that records and shares transaction details across many nodes (computers) that are part of the network so that the data is not modified. Each transaction that occurs on a blockchain network is distributed across all nodes on the blockchain, every participant has an equivalent copy of the ledger, and it is a changeless ledger once a record or a transaction is made [1].

Blockchain was originally introduced to timestamp digital documents and prevent tampering with records, in simple terms, a blockchain is a chain of blocks that contain information. When a transaction occurs, its related information is recorded into a block, so a transaction initiated in one corner of the globe can be registered on the block, which is then verified, validated, and added to the main blockchain by the miners of the public ledgers.

II. LITERATURE REVIEW

This paper provides a literature review on blockchain technology in identity theft to offer an informed understanding of the present person details where blockchain technology can be implemented in the other fields of identity theft. Our Literature Review is mainly focused on Blockchain Technology, an advanced Storage System, and Digital Certificate Validations.

Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen "Blockchain and Smart Contract for Digital Certificate" [2] To solve the issue of identity theft, a digital certificate system based on blockchain technology would be proposed. Due to the immutable property of blockchain, a digital certificate with anti-counterfeit and verifiability can be made. The aim given for issuing the digital certificate in this system is as follows. To begin, the development of an electronic file of a paper certificate goes hand in hand with the insertion of other associated data into the database, as well as the computation of the electronic file's hash value. In conclusion, the hash value will be saved in the chain system's block of nodes. A QR-code and inquiry string code concerning the certificate is going to be generated by the system to affix to the paper certificate. A demand unit can be provided to verify the genuineness of the paper certificate by scanning through mobile phones or by website inquiries. Due to the unchangeable properties of the blockchain, the system enhances the credibility of various paper-based certificates and put together electronically minimizing the loss risks of various kinds of certificates.

S. Sunitha kumara, D. Saveetha "Blockchain and Smart Contract for Digital Document Verification" [3] In the proposed system, the degree certificate's entire personality and behaviour activities of the person using the id will be uploaded to the blockchain. Because of inalterable property, it is stored in the blockchain Firstly, the user will submit the certificate or personal id to the electronic certificate system and request an e-certificate. After requesting for e-certificate, the system can then review the certificate from the university or faculties, or the organization and obtain the reassurance and store the serial range and e-certificate to the blockchain. The system will generate the QR code/Address code and send it to the user. When applying for an organization users will send only the certificate serial range and QR code received from the e-certificate system.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

III. PROBLEM DEFINITION

Identity is more than an important thing regarding you as a person. This includes data like birth, name, license, and so on, all these are data points that are utilized by governments and stored in centralized databases.

A bad person can misuse your identity. They can now use your identity to destroy a reputation. In fact, faked documents are widely available, both for free and for a cost. Hence, we can use blockchain technology to avoid identity theft.

In existing system, identity theft is a major threat. Companies that hire thousands of freshers spend a significant amount of money to have applicants' educational certificates and transcripts confirmed, and while visiting a doctor or clinic, it is impossible to know if the person has a genuine degree or not. To overcome this issue, we suggested the notion of a Digital Certificate System that uses blockchain technology to verify various certifications and documents.

IV. OBJECTIVE

The main objective of this paper is to inform others about how blockchain technology can be used to verify fraud such as counterfeit certificates, documents, passports, and so on. Identity theft has become one of the most pressing worries in today's fast-paced world, and we can combat it by utilising blockchain technology.

One of the areas where blockchain offers a well-timed and primary solid solution technique to use significantly extended that provides a powerful public blockchain that can be used for secondary purposes such as a verification device in a variety of markets is the simple, trustworthy, and reasonably-priced verification of authentic documents, such as various certificates, and college degrees.

V. RESEARCH METHODOLOGY

Nowadays many folks achieve numerous academic certificates, documents, passports, etc. It's not uncommon for these folks to produce forged certifications or documents, and it's difficult to track them down [4]. This drawback of faux documents and certificates has been a long issue within the various sectors, and communities. Because it is the potential to make such certificates at a low price and also the method to verify them is extremely complex, as they are manually required to be verified. This problem can be addressed by storing digital certificates on the Blockchain. To create the blockchain-based system of unalterable documents /certificates, in the beginning, the departments ought to get registered. Any transaction is frequently sent through the registered departments' wallet addresses. Only the owner of the smart contract has the authority to create new departments. The department will be able to access the system and create documents/certificates with data fields once it has been added. Each document/certificate that is created will be saved in the Interplanetary file system (IPFS). It can return a unique hash address SHA-256, This will serve as a distinctive identity for each document. This will generate a hash node and the details of certificates and papers that can be saved in the blockchain, and the person will be provided with the resultant transaction id. Using the IPFS hash value recorded with the data and this transaction id, anyone can verify certificate information and inspect the authentic copy of certificates. And it isn't viable to alter these certificates or to create faux certificates, and documents using the same data. As a result, we can solve the problem of identity theft.

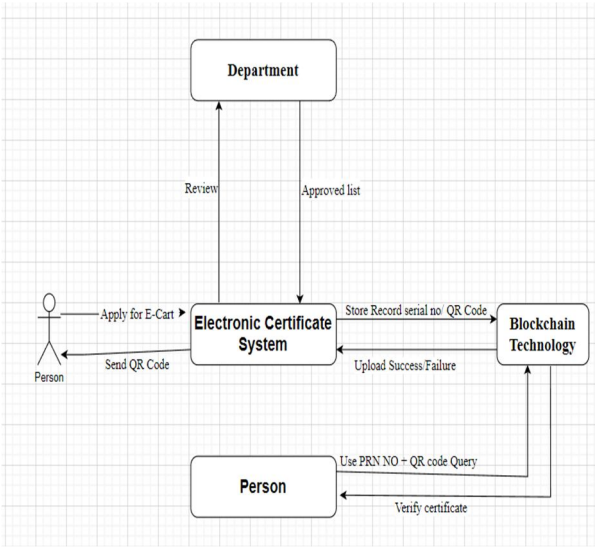


Fig 1: System Architecture.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

VI. ANALYSIS AND FINDINGS

According to our findings, approximately one out of every fifteen people becomes a victim of identity fraud. In 2019, 650,572 people were victims of identity theft. From the research on the prevention of identity theft, we analysed to that there are various methods where one can create fake documents/certificates available at a low cost. Blockchain technology can be used to prevent forgery of documents/certificates. Our research covers the information about the prevention of identity theft and it is an interrelated solution to the current forgery problem.

VII. LIMITATION AND FUTURE SCOPE

One of the most important elements of blockchain is data immutability. Wherever a node in the network validates and saves continuous data, it acts as a huge public ledger. Any organisation can verify the data of any certificate used in this system because the certificate creation process is an open and transparent system.

As it is immutable, one cannot make any modifications to any of the records. For scalability, every participating node in a blockchain, such as bitcoin, is required to verify the transaction. It restricts the number of transactions that may be processed by a blockchain network.

In future we can focus on the overall scalability and speed over time to improve the user experience.

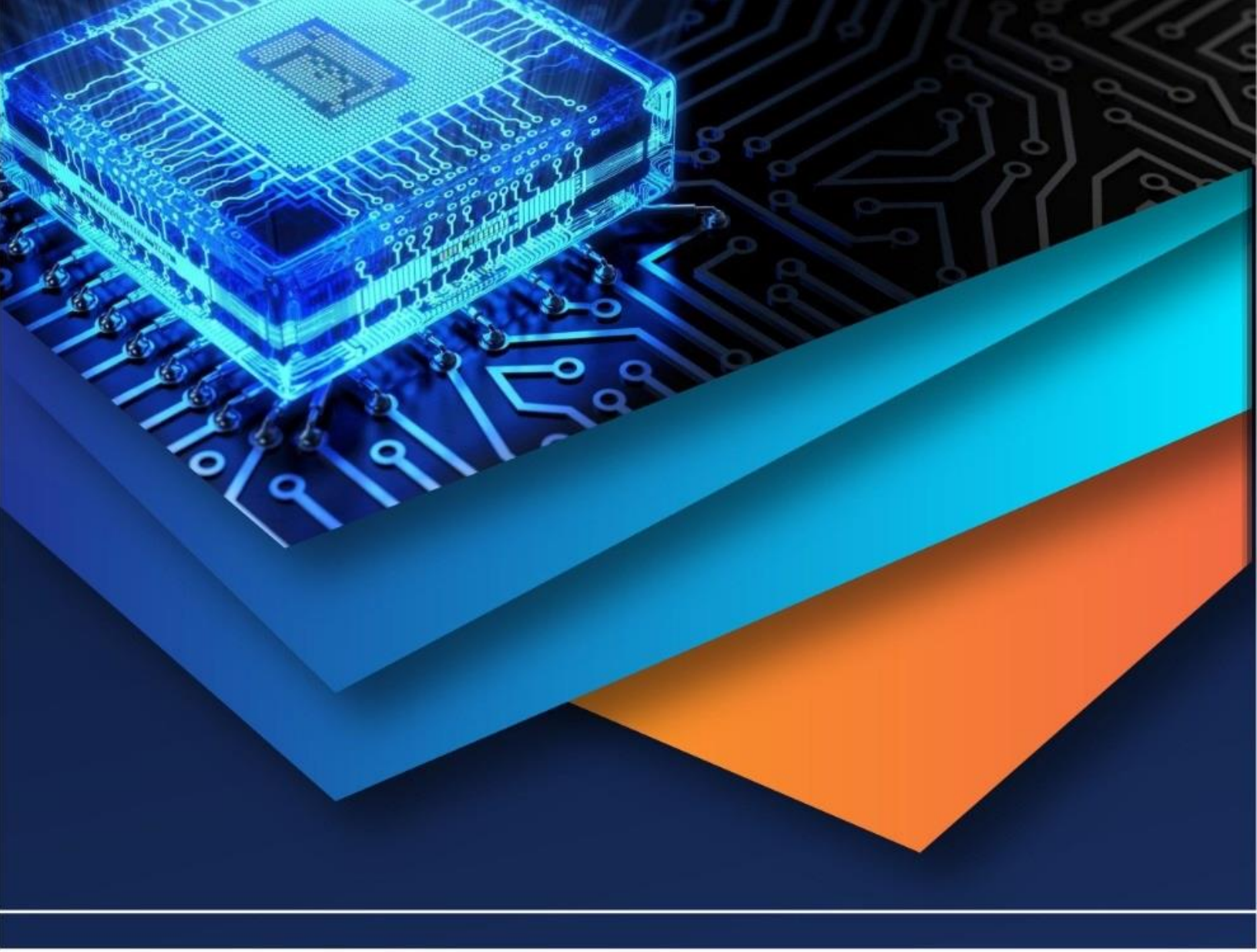
VIII. CONCLUSION

Although there are numerous restrictions to data security and privacy, various technologies are suggested to reduce the incidence of fraud and ensure the safety, authenticity, and secrecy of various documents. A new blockchain-based approach is helping to reduce identity theft. The system's automated certificate giving is transparent and easy to understand. Companies or organisations can thus query the system for information about any certificate. The recommended approach lowers administrative costs, prevents document fraud, and ensures that data on digital certificates is accurate and reliable.

REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, IEEE 6th International Congress on Big Data, 2017.
[2] Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen "Blockchain and Smart Contract for Digital Certificate" Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam (Eds)
[3] S. Sunitha kumara, D. Saveetha "Blockchain and Smart Contract for Digital Document Verification"
[4] Gunit Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, Dr. Seema Shah, Blockchain Based Identity Verification Model, International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019
[5] Neethu Gopal, Vani V Prakash "Survey on Blockchain Based Digital Certificate System" International Research Journal of Engineering and Technology (IRJET) Nov 2018
[6] Maharshi Shah, Priyanka Kumar, Tamper Proof Birth Certificate Using Blockchain Technology, International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-5S3, February 2019.
[7] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni and Luca Spalazzi Certificate “Validation hrough Public Ledgers and Blockchains” In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17) 2017

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)