International Journal On Engineering Technology and Sciences – IJETS
ISSN (P):2349-3968, ISSN (O): 2349-3976 Volume XIII - Issue IV, April - 2026

UNIVERSAL BLOCKCHAIN-BASED VERIFICATION PLATFORM

Dharshini B V
B.E Student (Third Year)
Department of Computer Science and Engineering
Francis Xavier Engineering College
Tirunelveli, Tamil Nadu, India
dharshupreni2006@gmail.com

Hylin Jessica D
B.E Student (Third Year)
Department of Computer Science and Engineering
Francis Xavier Engineering College
Tirunelveli, Tamil Nadu, India
hylinjessica02@gmail.com

Jayashree Meenakshi B
B.E Student (Third Year)
Department of Computer Science and Engineering
Francis Xavier Engineering College
Tirunelveli, Tamil Nadu, India
jayashreemeena295@gmail.com

Mrs. J. Brigil Qurinus (M.E)
Assistant Professor
Department of Computer Science and Engineering
Francis Xavier Engineering College
Tirunelveli, Tamil Nadu, India
brigilqurinus@francisxavier.ac.in

Abstract

The main objective of this project is to develop a universal verification system based on blockchain technology. The Universal Blockchain-Based Verification Platform will enable users to verify digitally any document securely and efficiently with the use of blockchain technology. Traditionally, documents have been verified by some authority who checks for any tampering in a document. However, there are various shortcomings to this process; it can take up a lot of time, is prone to fraud and can be manipulated easily by any third party. In the suggested project, a blockchain-based verification system will be used. The document is converted into a hash that will be stored in the blockchain network whenever a document is uploaded into the system. During verification, the document hash will be compared to the stored hash to authenticate the document.

Keywords: Blockchain, Verification System, Smart Contracts, Data Security, Decentralization, Cryptographic Hashing

Introduction

The contemporary digital age requires that verification of certain documents like certification, ID cards, and legal papers should be given utmost priority due to the increased likelihood of forgery in digitalized information.

The traditional methods of verification rely on centralized third-party systems like the concerned university, governmental body, or other firms. Such methods tend to be both ineffective and time-consuming while at the same time lacking security and reliability.

However, with the advent of blockchain technology, it is possible to ensure security and transparency ofinformation. Blockchain is a decentralized database that

provides security and transparency in information management.

Any kind of modification and manipulation of data stored on the blockchain is impossible. In this project, we aim to create a platform for verification of documentsutilizing blockchain technology.

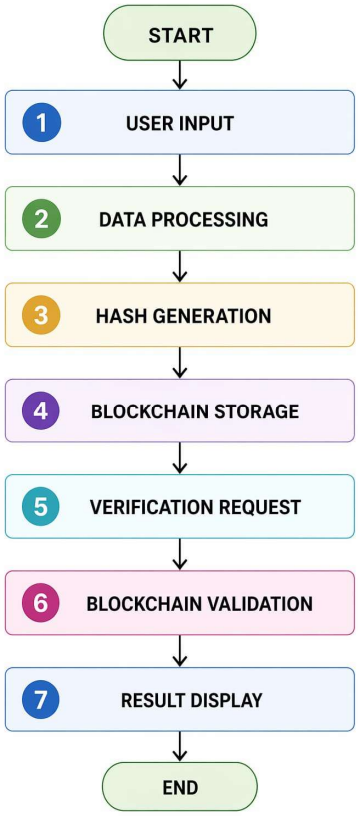

Diagram of the proposed Universal Blockchain-Based Verification Platform

Existing System

Currently, there are two kinds of verification methods for documents – centralized and decentralized models. A centralized model is usually based on the fact that a single institution, like an educational organization, governmental department, etc., maintains records and validates the documentation. The verification process itself is usually conducted manually by checking the authenticity of documents using internal resources like databases or record collections. Though this method may be relatively effective, it requires too much time. Users should visit the office personally or send several copies of their document.

Some organizations also implement digital verification methods; in this case, a centralized database is used. It provides convenient services allowing users to conduct the verification via the Internet. At the same time, centralized databases are very prone to corruption since they depend greatly on the work of central institutions. In addition, if cyber attacks happen or if an insider makes changes to data, all the information stored will be at risk. What is more, centralized verification cannot provide any guarantees that the stored information has not been changed.

Proposed System

A Universal Blockchain-based Verification Platform would be used for overcoming limitations of conventional methods of document validation, which would be made possible by adopting the benefits of blockchain technology. Documents are verified through decentralization wherein storage is made across different nodes rather than centralized. This means that there will not be any central body in control of information.

When the document is uploaded to the system, a unique cryptographic hash is created, which is the digital signature of the document. The hash value thus generated is then placed on the blockchain with the help of smart contracts. Because of the immutable nature of blockchain data, any alteration is impossible, and thus the hash value would provide security to

the document. During the process of verification, another hash would be generated using the document and compared against the existing one on the blockchain.

Methodology

The method of the proposed system can be described in this sequence:

1. Document Input / System Input
2. Data Processing and Hashing
3. Storage in Blockchain
4. Verification Process
5. Execution of Smart Contract
6. Result Evaluation

The methodology of the proposed system aims to provide an efficient and secure verification procedure via several steps. First, document input will be followed by data processing and hashing. After that, the results will be stored in the blockchain and verified before evaluating the result.

Document Input/ System Input

The very first stage of the system entails retrieving the document from the end-user's computer. Depending on the nature of the application, the document could be retrieved in any digital format such as a PDF, image, or text format. This stage helps make the system flexible in handling documents of different natures. Some of the common examples include academic certificates, identity proof, and legal papers.

The next stage entails preparing the document for hashing and storage on the blockchain platform. This stage is particularly important because it prepares the input document before it undergoes the process of being hashed. The quality and authenticity of the input document influence the entire process of verifying its credibility.

Data Processing and Hash Generation

Once the file has been uploaded, the system performs some preprocessing wherein extra information is filtered out, thus making the file consistent before its hash can be created. Once this is done, the document goes through a series of computations using a cryptographic hash algorithm which outputs a unique value representing the document.

The process of creating hashes is one of utmost security, as the slightest changes made in the original document will result in an entirely different hash value. This makes the hash function vital in identifying any forms of alteration or forgery that may occur. The hash itself acts as the digital signature of the file.

Blockchain Storage

When hashing occurs, the hash is then stored within the blockchain network through the use of smart contracts. The decentralization aspect of the blockchain technology ensures that the information stored within the network is spread out among different nodes and not stored at one particular point. The decentralized nature makes the information more reliable and secure.

The immutable nature of blockchain technology ensures that once hashing occurs, there is no way that the hash can be changed or even deleted. This ensures the integrity of the information as no alterations can be made after recording the hash.

Verification Process

Verification is another important part of the whole system. Once a user opts to verify a particular document, they simply upload it into the system. A new hash is calculated based on the document provided by the user, after which the hash associated with the document on the blockchain network is retrieved.

Then comes comparison of the two hashes to see if they are identical. The identity of the two hashes guarantees the document's integrity. The failure of the hashes to match one another means that the document has been changed, and therefore, can't be accepted.

Smart Contract Execution

It is extremely important for smart contracts to be included within the automation process. Smart contracts are automated contracts placed on the blockchain, which work based on certain triggers. For the purpose of implementing such an automatic verification method, smart contracts are used for hashing, fetching, and verifying the data.

By using smart contracts, there is no need for any middle man or person, which avoids any possibility of errors. This not only makes the entire process faster but also helps in getting consistent results.

Prediction and Performance Evaluation

Performance assessment of the system will be done according to its effectiveness in verification of the documents and detection of any frauds. The performance measurement of the system includes metrics like True Positive, True Negative, False Positive, and False Negative.

True Positive refers to a case where there is a verification of a genuine document, and False Positive refers to rejection of a valid document. False Negative and False Positive denote erroneous results of the system, which can be mitigated through appropriate implementation and evaluation of the system.

Implementation

In terms of how this system will be implemented, there are different technologies that should be involved in it, namely blockchain platforms, programming languages, and frameworks for creating interfaces for the user side. For the frontend part, one should pay attention to the fact that it allows uploading documents and verifying their hashes. There are some frameworks that can be used for creating frontend, for instance, React or Flutter.

Concerning the backend part, its task is to process information and to communicate with the blockchain. In order to do all the necessary things at the back-end side, one should use such programming languages as Python or Node.js. As far as blockchains go, they play a role in storing hashes, and such platforms as Ethereum or Hyperledger can be used here.

Result and Discussion

Results from the suggested system have proved its efficiency in document verification. Blockchain provides high-level data security by ensuring that there is no tampering of information, while hash comparison enables the accuracy of the verification process.

The suggested system helps to shorten the time spent during the verification process, while the elimination of manual processes enhances reliability and transparency in the verification process. Despite being efficient, the suggested system might encounter certain technical issues

concerning its implementation and scalability in the network.

Conclusion:

Universal Blockchain-based Verification Platform is a very innovative approach to addressing the problems inherent in traditional document verification mechanisms. The platform uses the latest technologies and guarantees data authenticity and reliability. There is no need for intermediaries involved in the processes carried out.

It is very effective, and its use cases include such fields as education, healthcare, and even government. It can thus be said that the described platform is a revolutionary innovation in digital verification.

Future work:

Future improvements include the ability to connect the system with government and institution databases, creating a better platform for verifying information. Mobile applications could be used in developing this system to make the system more user-friendly. Features such as verification using QR codes and the application of artificial intelligence in detecting fraud could also be considered.

Further advancements may come from utilizing the latest technology such as advanced blockchain technology and scalability technology. It is important that the future expansion of the system involves incorporating different document types and verification standards internationally.

Reference:

[1] A. Shakeela Joy and R. Ravi, "Smart card authentication model based on elliptic curve cryptography in IoT networks",International Journal of Electronic Security and Digital Forensics, vol.13, no.5, pp.548-569, 2021.

[2] R. Ravi, R. Kabilan, G. Prince Devaraj, Zahariya Gabriel, J. Monica Esther, and U. Muthuraman, "Malicious Finding and Validation Scheme Using New EnhancedAdaptive Ack",IEEE Proceedings of the International Conference on Sustainable Computing and Data Communication Systems, pp.1220-1224, 2022.

[3] V. Sindhiya, M. Navaneetha Krishnan, and R. Ravi, "Analyzing and improving the security of cryptographic algorithm against side channel attack",International Journal of Computer Science and Mobile Computing, vol.5, no.4, pp.491-498, 2016.

[4] M. Karthika and R. Ravi, "CCT: An Efficient and Affordable User Authentication Protocol Defiant to Password Pinching and Reclaiming", International Journal of Advance Research in Computer Science and Management Studies, vol.2, no.2, pp.304-310, 2014.

[5] A. Monika, T. Samraj Lawrence and R. Ravi, "Secure and Continuous Wireless Dispatch using Lock-Timeout Puzzles", International Journal of Innovative Science, Engineering & Technology, vol.1, no.2, pp.201-205, 2014.

[6] M. Crosby et al., "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, 2016.Highlights blockchain use in multiple domains with focus on transparency and data integrity.

[7]A. Dorri et al., "Blockchain in IoT: Challenges and Solutions," FGCS, 2019. Focuses on enhancing security and preventing data tampering using blockchain technology.

[8]Hyperledger Foundation, "Blockchain Technologies Overview," 2023. Provides details on enterprise blockchain frameworks like Hyperledger for secure systems.

[9]IBM, "Blockchain for Business Solutions," 2024.Explains real-world use of blockchain in improving trust and reducing fraud.

[10]E. Androulaki et al., "Hyperledger Fabric Architecture," EuroSys, 2018. Describes a permissioned blockchain system suitable for enterprise-level verification.

[11]N. Szabo, "Smart Contracts: Digital Market Blocks," 1996.Introduces self-executing contracts used for automation in blockchain systems.

[12]D. Tapscott and A. Tapscott, "Blockchain Revolution," 2016.Explains how blockchain transforms industries through secure and transparent systems.

[13]J. Benet, "IPFS: Peer-to-Peer File System," arXiv, 2014.Introduces decentralized storage used alongside blockchain for secure data handling.

[14]World Economic Forum, "Blockchain Beyond the Hype," 2023.Provides practical guidance on implementing blockchain in real-world applications.