European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 10, 2020

BLOCKCHAIN BASED IDENTITY AUTHENTICATION USING IPFS AND HYPERLEDGER FOR VERIFICATION OF DOCUMENTS

Priya N[1], Dr. Ponnavaikko M[2] , Rex Aantonny[3]
[1]Research scholar, Department of computer science, Bharath Institute of Higher Education And Research, Chennai, India
priyabiher@gmail.com
[2]Provost, Bharath Institute of Higher Education And Research, Chennai, India,
ponnav@gmail.com
[3]Founder & CEO, Rex Cyber Solutions Pvt Ltd, Bangalore, India,
rex@rexcybersolutions.com

Abstract
Document verification and authentication plays a vital role in everyday life. These documents can be any type like educational certificates, business transactions, images containing seals, billing receipts, tenders, etc. Scams on documents could have happened in any stage of transactions. Currently, the blockchain became a trustable secure mechanism for maintaining and giving up the data in a distributed, immutable, and trustable way without any intermediaries. Blockchain keeps all business across two parties in a confirmable and unchangeable. Because of that transparent and trustable nature many fields like medicine, finance, education, insurance, procurement, and supply chain handling their transactions by blockchain mechanisms. In this research, an identity management system has been framed for any type of document verification and validation using blockchain technologies like hyperledger and IPFS algorithms. Existing identity-based security methods having some drawbacks like leakage, forgery of confidential documents. Facial recognition and extracting the specific features could provide the uniqueness and protecting the documents used. By applying blockchain methods in identity-based authentication improves security with the increase in the speed of transactions at lower cost with high performance.Analyzing hyperledger and IPFS results yields a secure framework for identity-based document verification systems. Implementation results have shown the specific advantages of both blockchain methods.
Key words: Identity, Authentication, hyperledger, IPFS, documents verification, blockchain.

1. Introduction

Identity-based crime will affect everybody's life and that occurred in all domains like finance, medicine, education, insurance, and supply chain. The consequences of these identity stolen cases would affect the entire economy and financial conditions and brings corruption. Identity authentication involves password authentication and biometric authentication methods[1]. The presence of a few vulnerabilities in traditional biometric authentication procedures brought risks to information security. Identity-based authentication is very much essential in the document verification system to avoid any serious security issues. Mishandling of confidential documents must have been avoided by applying cryptographic methods and provide a highly secure and privacy-protecting system. Existing security methods like password authentication, two-factor authentication. biometric authentication are providing secure identity authentication in various applications.

By introducing blockchain in these identity authentication methods providing a more covered protection in the existing security methods. Blockchain is a shared ledger that records transactions between peer-to-peer networks. This mechanism offers transparent tamper-proof transactions that tend to resolve the issues like fraud, high transaction costs, and evaluate the trustworthiness of all participants involved. In our research hyperledger and IPFS protocol are applied for creating identity-based authentication and verification in documents. Permissioned blockchain hyperledger

is mainly applied for many business applications similar to smart Contracts.Hyperledger is distributed ledger technology in which the members are familiar with one another. Consensus is created because of maximum supporters of the decision with maximum benefits. This network is operated under an authority build over the agreements for handling disputes.IPFS mainly provides the deduplication with secure peer to peer data sharing of records at low costs with high performance.

Motivation of research:

Identity authentication and validation of records are essential in many domains like medical, finance, insurance, procurement, education, and supply chain. The documents taken for verification may be forged or altered. That would lead to affect the accuracy of the results. In upcoming research work, Each field of data used is hashed. The image of documents used are verified by analyzing the features like image size, width, processing time. Identity authentication is done with IPFS stored documents and hyperledger.To analyze both results based on the above methods and find the insights from them and providing the optimal solutions. This paper is organized as follows.Section II involves the related works for identity authentication using blockchain.

Section III involved the technical background of hyperledger and ipfs. Section IV explains the system architecture with workflow. Section V provides the experimentation with results. Finally in section VI discussed the performance results and Section VIII's conclusion is added with reference.

2.RELATED WORKS

This section reviewing the related works involved identity authentication using hyperledger. Zhihua Cui et al, [3] proposed a multi WSN authentication method for internet of things devices using blockchain. A hybrid permissioned blockchain model is constructed that provides authorized communication in various scenarios build on public and private nodes that preserving privacy with a rise in security. Xiny in Xiang team [4] introduced a protected framework for health records that supports the credential updates with reduced the suspended communication and providing high efficiency with security. Xingxiong Zhu et al [1]constructed an authentication in identity registration with the abnormal behavior of users and skilled the effectiveness of a process with minimal cost. Akash Suresh et al [5] framed a computational model by a physically unchangeable function. blockchain and this PUF model guarantees the privacy tests with IoT networks. Heping Huang, Xiaoqun Chen[6] created a blockchain identity authentication for mobile terminal tends to resolve the security defects occurred and proves the advantages of decentralization and non-tampering. Brindha Devi et generated the document verification using decentralized applications with ipfs. Two-way key verification with digital signature [7]is done using blockchain.

The above researches presented their work on providing authentication in the verification of documents. Scalability and cost are the main issues.Our contribution is to optimize the techniques used for document verification and provide the integrity with security.

3.BACKGROUND

To understand the technologies behind our research work it is necessary to know about the basic things about blockchain,hyperledger ipfs, and its functioning process in detail.

A. Blockchain

Blockchain was originally framed by using bitcoins and cryptocurrency by Satoshi Nakamoto in 2008.[8].The main goals of using blockchain are low cost with high speed and more security and reduced risk and fraudulent factors. There are two types of models in blockchain i.e permissionless and permission. A permissionless framework is applied for cryptocurrency. The permission blockchain is mainly for smart contracts. Every transaction is accepted by the participants of the system using smart contracts. Validating new transactions and creating a block is done by the consensus mechanism. The consensus is created after making an agreement with the participants and maintain reliability and established trust. Each block inside the blockchain contains a header, timestamp, and a list of total transactions using Merkle root. Every new block comes from the earlier block by its cryptographic hash value of the existing block. That would be used to form a new block's hash which will make blockchain tamper-proof

B. Hyperledger Indy

Linux foundation released a Hyperledger which is a blockchain framework in December 2015. Many enterprises are dealing with the most sensitive information. Hyperledger provides a high-security by using the decentralization and immutability nature of blockchain[9]. By using hyperledger, hackers never get system access and manipulating the records. The modules inside the Hyperledger are ordering services, membership service providers, and peer to peer services and smart contracts. Transactions reach consensus in hyperledger by ordering and validating the transactions. Hyperledger frameworks are hyperledger fabric, sawtooth, Indy. The tools involved are hyperledger caliper with the library called hyperledger Ursa.

Hyperledger Indy is the blockchain platform mainly used for identity-based solutions. Indy induced the users to preserve the confidentiality of the data. By using this all users could have complete control over their self-identity. Others cannot take over that identity credentials. For documents, verification Indy plays a main role in exposing the sensitive information with identity verification.

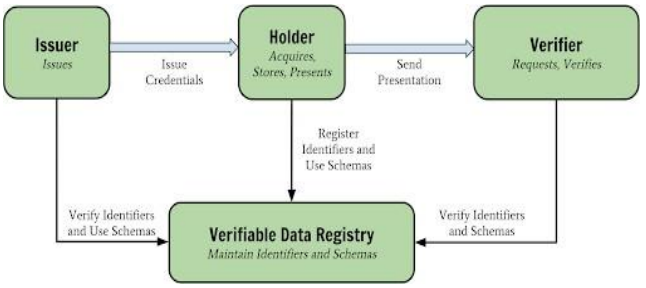

Fig 1: The W3C Verifiable Credentials Model

World Wide Web Consortium (W3C) presented The above model [10] provides the features of issuer, holder, verifier, and the data registry which verifies all encrypted keys of identifiers. These credentials are verifiable which stored in a registry and checking the data authentication. Self-sovereign identity (SSI) is the identity provided over the user's credentials without any main authority to control the identities. By using SSI users can determine where, how to share the identity information. A decentralized identifier (DID) is a main key that allowed the credentials which would follow the W3C standard. These DIDs have unique identities with cryptographic credentials that can be created anytime with a new resource location. Hyperledger can be worked with two types of approaches with zero-knowledge proof (ZKP). It is about proving the credentials without revealing the secret keys. Indy confirmed that the prover holds the given verifiable credential, the verifier combines all accepted the prover's identity.

C.InterPlanetary File System (IPFS)

Interplanetary File System (IPFS) is an open-source project developed by Juan Benet.[10] IPFS is a peer to peer protocol mainly used in decentralized network used to holding and sharing the data with unique identity. Each file stored with its hash value will be saved in a distributed hash table. Ipfs is used to remove any duplicate or irrelevant files in the registry. It provides a blockchain-based secure storage model to the clients. It mainly works to achieve the reliability and security of the data with the minimum storage cost. Merkle tree using a directed acrylic graph verifies the blocks of data in the blockchain network. Each data content has its own hash value so that it's impossible for doing changes with the original values. Merkle DAG structure created a distributed file system with permanently storing the hash objects. While sharing the files the hash value is only shared.

4. Methodology

Here identity authentication techniques on blockchain which provide a solution for clients in decentralized architectures will be discussed.

A System flow architecture:

The following flowchart given the workflow of our proposed system. Document verification is performed with the identity authentication and verification then issued the trustworthiness of the records. After verifying the identity then the certificates will be issued.

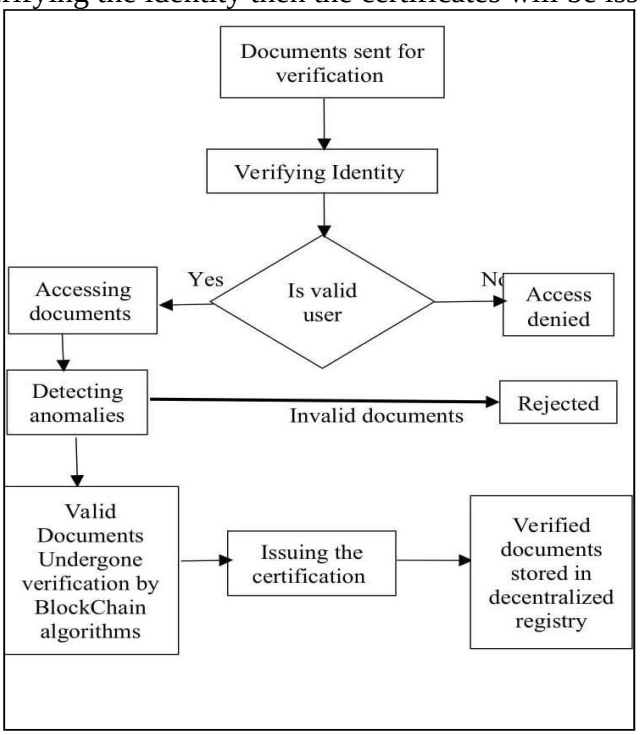

Fig:3 System Flow architecture

B. Authentication of records using IPFS algorithm:

A secure framework system is designed for the authentication of all transaction records using IPFS protocol.This system mainly concentrates on the permissioned document retrieval accessing documents and tracking the changes that occurred in the life cycle of entire transactions. Each document is protected by a private key using a unique identifier. Usage of smart-contracts protected the system until the final stage of complete transactions. IPFS algorithm took each records and generated its hash values.The total number of records increased never affect the speed of hash generation and cost.The hash values of records took the minimal amount of memory.

Hashing	Time for 2 million matching	Matching per 1sec	Size
48bit Length	1.003sec	53 million / sec	47 MB

Table 1.Performance results on validating documents using IPFS

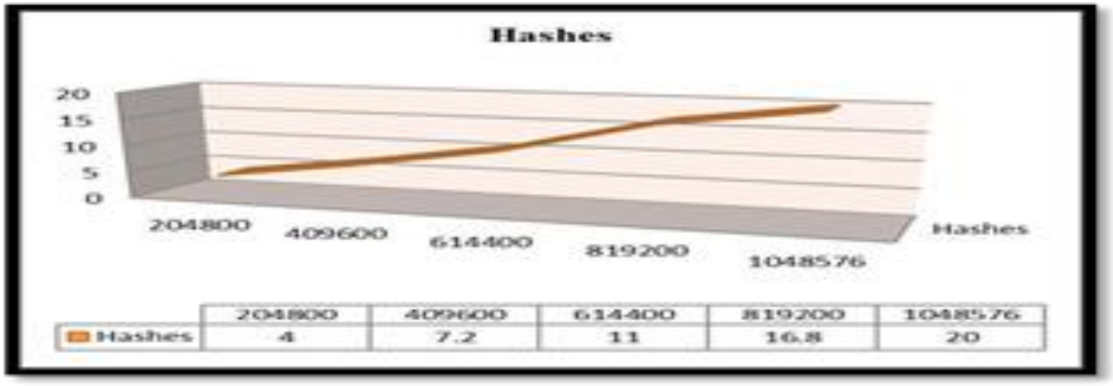

Fig 4: No of Transactions Vs Responses

C. Identity authentication using hyperledger Indy:
Indy generates a schema that contains the attributes of identity like name, date of birth, educational qualifications, driving license, unique citizenship number like Aadhar in a JSON array. All these entities are arranged and submitted in the decentralized ledger. The credentials are created with the transcript name. Then the requests are sent to the recipient with its decentralized identifier (DID). Indy creates a relationship with the sender which sends the connection request with the authorized holder. A proof request is received and a response will be sent for the proof of a new transcript. Again a new relationship is established with another node and creates a credential definition, and is submitted to the ledger. Holder got messages from a verifier with credentials to offer then the relationship got established. The verifier gets the established connection with the existing DID. Finally, verification is done by both sides in issuer to a holder or holder to a verifier.For this implementation system required is with a normal laptop with Intel Core i5 processor and Windows 10 Operating System with 4GB RAM and 1TB HDD.Table 2 shown the results for authentication of records with hashing values.

Hashing	Time for 2 million matching	Matching per 1sec	Size
48bit Length	**0.0098 sec**	**46 million / sec**	**35 MB**

Table:2 Performance results on validating documents using hyperledger

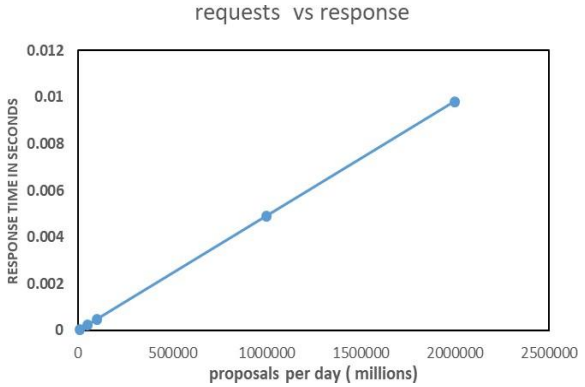

Fig :5 No of requests Vs Response time

By experimenting with this hyperledger for validating documents the results clearly shows the cost-effectiveness and high efficiency. Time taken for validating documents is less than a second. our research concludes that the storage required for this validation process is less due to the hash values of the raw data. The cost factor involve for storage also less with optimized results.

5. Discussion

Identity authentication is the biggest challenge in the cyber world. Many models related to identity issues were created and solved. However, we can resolve the self-identity issues and secure storage, and maintain the confidentiality of the personal data. Our proposed research work is to evaluate a few factors involved in the identity authentication of records. Our experimental results have shown the performance of hyperledger and ipfs algorithms. The effectiveness and low cost with minimal time are found more accurate in the implementation of hyperledger that will be contrast in the ipfs protocol. Specific features like Verifiability, Accessibility, backup recovery, Confidentiality, storage control are best in the case of hyperledger

6. Conclusion

Documents verification is important in all aspects. Globally document verification is mandatory in each field of business. Blockchain technology is most suitable for issuing solutions in identity authentication problems. According to our proposed ipfs and hyperledger using a robust security system framework that assures the transparency of records authentication and verification. By comparing the results from both blockchain methods reviews about the better output from hyperledger and that is mostly user-friendly protocol when compared with IPFs.Both methods

ultimately supports the scalability with lower cost. Finally, in terms of implementation, multiple clients registered for verification share with other parties in a most trustable way.

References

1. Xingxiong Zhu, "Blockchain-Based Identity Authentication and Intelligent Credit Reporting" , 2019 2nd International Symposium on Big Data and Applied Statistics doi:10.1088/ 1742-6596/ 1437/1/ 012086
2. Yan Ren , Qiuxia Zhao, Haipeng Guan and Zhiqiang Lin, "A novel authentication scheme based on edge computing for blockchain-based distributed energy trading system",EURASIP Journal on Wireless Communications and Networking (2020) 2020:152 https://doi.org/10.1186/s13638-020-01762-w.
3. Zhihua Cui, Fei Xue, Shiqiang Zhang, Xingjuan Cai, Yang Cao, Wensheng Zhang,and Jinjun Chen, "A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN"IEEE,2019.
4. Xinyin Xiang, Mingyu Wang, Weiguo(Patrick) Fan, "A Permissioned Blockchain-based Identity Management and User Authentication Scheme for E-health Systems" IEEE Access,2016.
5. AkashSuresh Patila,, Rafik Hamzaa,, Alzubair Hassana,, Nan Jiang, HongyangYana,, Jin Lia,"Efficient
6. Privacy-Preserving Authentication Protocol Using
7. PUFs with Blockchain Smart Contracts", Elsevier, 2020
8. Heping Huang, Xiaoqun Chen, "Power Mobile Terminal Identity Authentication Mechanism Based on Blockchain",IEEE 2020
9. V Brindha Devi, R Skanda Gurunathan, N Keerthi vasan, "De-Centralized Certificate Creation and Verification using Block Chain (DCCVuB)" International Journal of Engineering and Advanced Technology ISSN: 2249 – 8958, Volume-9, Issue-1s, October-2019.
10.Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System",2008
11.https://101blockchains.com/hyperledger-tutorial
12.https://training.linuxfoundation.org/training/introduction-to-hyperledger-sovereign-identity-blockchain-solutions-indy-aries-an d-ursa/
13.S. Vimal,S. K. Srivatsa,"A new cluster P2P fle sharing system based on IPFS and blockchain technology" Journal of Ambient Intelligence and Humanized Computing,2019