Proof of File Existence

Mahipal Singh
Cyber Security Systems and Networks Amrita Vishwa VidyaPeetham University Amritapuri, India

Abstract - **Blockchain is a modern open-source, decentralized distributed ledger platform that is still in its infancy. The Blockchain network verifies and tracks transactions through several machines in a permanent and verifiable manner. So that the record cannot be modified without modifying the blocks immediately following it, and so that nodes will agree.**

The first use of blockchain was when it was released as the underlying technology for the world's first decentralized digital cryptocurrency, Bitcoin. Blockchain technology has recently received a lot of attention and is now being used by a lot of financial institutions and high-tech companies all over the world. Blockchain is thought to have the potential to revolutionize the planet, and it is constantly emerging in both the private and public sectors. Many are still in the experimental or learning process, while others are working on solutions or even making their own. In this paper, we propose a realistic solution for Aca- demic Certification Verification and Recordkeeping by Incorp- rating private blockchain as our next-generation database, which can include encryption, cryptographically hashed, and digitally stamped certificates, as well as remove the need for a third party and reduce the verification time from days to seconds. This method establishes the trust, accountability, and transparency that educational institutions require in order to ensure that their assets are always valid, verifiable, and decentralized documents that cannot be altered by third parties. As a result, Proof Analyzer claims to comprehend vast scalable functionalities that guarantee academic certificates' validity, credibility, and non-repudiation.

Index Terms - **ProofAnalyzer, Recordkeeping, Cryptographi- cally.**

I.INTRODUCTION

A paradigm changes in technology quietly debuted at the start of 2008, when the world was in the midst of a significant financial crisis. The innovation was bitcoin, a digital currency that has become the most visible innovation of the twenty-first century to date. The blockchain is an undeniably brilliant invention; the primary implementation of today's blockchain advancement was created by Satoshi Nakamoto, a pseudonym for an anonymous individual. In 2008, Satoshi Nakamoto publishes a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," in which he discusses a purely P2P payment system based on cryptographic authentication that will allow online transactions. The Bitcoin protocol's code is open source, which means that anybody who knows it can see what it does and how it does it, so there's no need to trust the developer. The terms "block" and "chain" were used interchangeably in their paper, and the technology was initially dubbed "blockchain." By 2015, the concept had merged into a single word: "Blockchain," which refers to modern implementations of the immutable, tamper-proof, and open distributed ledger that keeps track of any transaction made across the Blockchain network. Any peer in the network should have access to all transactions and the ability to make them.

With millions of graduates per year, the certificate issuing authorities seem to have been compromised in terms of the scholar information's security credentials. Since there is no effective anti-forgery scheme in place, incidents that cause the graduation certificate to be faked are often identified. Aca- demic credential fraud is a fact, and duplicating declarations is a common problem that is becoming easier to solve.

In today's world, counterfeit documents are common, and as most of you know, there's no risk in acquiring them because they appear to be originals. This is the most common way for the average person to distinguish between authentic and forged documents.

Educational institutions may use ProofAnalyzer to create digitally sealed academic certificates. Our system ensures decentralized, unalterable, and safe data storage by using Blockchain technology.

This enables educational institutions to implement the most cutting-edge technologies available and produce credentials that are always legitimate, always verifiable by the employer, and impossible to replicate or hack.

II.SYSTEM OVERVIEW

The following is a summary of the system:

Academic institutes issue a certificate and enter the student’s information into a database. The framework code uses cryptography to transform document content to one-way hash code, which is then stored in the blockchain. The one-way hash code appears to be a duplicate of the text, but it is actually a code made up of strings. These code strings will be used as the document’s key.

Degree holders whose data has been successfully validated and processed are awarded an e-certificate with a quick response (QR) as a replacement for traditional hard copies. When the students use this credential elsewhere, the code re- mains the same as it was when it was stored in the blockchain.

When applying for a job, an individual may simply submit the e-certificate with QR code to the desired companies.

The companies submit a request for authentication to the system, and the system responds that the university’s certificates are valid if the hash matches the information stored on the blockchain. If they are modified, the hash will not fit.

III.PURPOSE

Since information technology has advanced so quickly in recent years, data security is more important than ever. As far as people are concerned, document authentication is a collective phenomenon. be it a birth, marriage, court proceedings, job purposes, or some other new phase in their life path, people come from all walks of life [1]. Graduates may need multiple certificates for interviews, regardless of whether they want to pursue their education or begin looking for work. However, they often discover that their educational and acclamation certificates have been lost [2]. Since certificates are issued by various entities and in-person applications may be required, submitting an application or requesting hard copies again may be time consuming. Despite popular belief, requesting a digital copy will save both paper and time. Graduates can easily apply for any credential by supplying details for identity verification. Nonetheless, forgeries of degree certificates, licenses, and certificates are popular due to their convenience. As a result, colleges and businesses are unable to immediately verify the documents they obtain. This study developed a certificate framework based on Blockchain to solve this problem. Data is stored in various nodes, and anyone wishing to change an internal datum must request that other nodes change it at the same time. As a result, the system is extremely dependable [3].

Our system’s goal is to provide secrecy, anonymity, and a decentralized proof of documentation that cannot be altered or deleted by third parties or governments. Regardless of whether the system is threatened or down, the presence of the paper is a permanent store in private blockchain [4].

IV.SYSTEM DESIGN

A usage case diagram is a graphical description of the relationships between the various components of a device. A use case is a tool for identifying, clarifying, and organizing system specifications in system research. In the following usage case, there are two players that can serve as an entity and as inexperienced users. The company may also import the folder, validate it, bind to it, and disconnect it. mine, as well as granting authorization to mine or issue the documents Upload files as a user the web explorer and calculate its hashes before sending it to Blockchain to be timestamp. As an answer, you will receive a verification note. The user demands authorization from the server, and the server responds in response to the action. In the link function, the user sends a connection request to the server and receives a response; in the reconnect function, the user sends a connection request to the server and receives a response. The user sends a disconnection request to the server and receives a response.

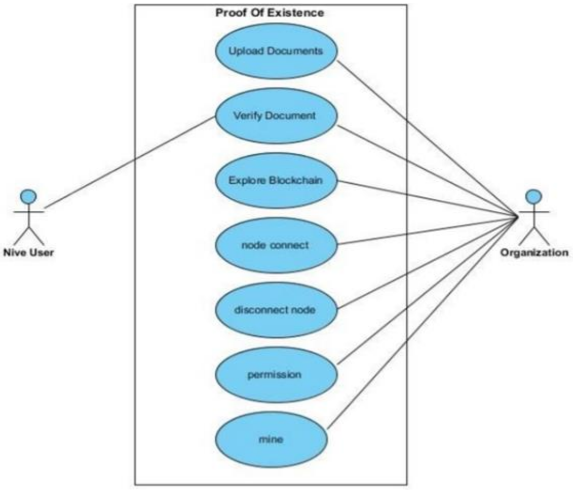


Fig. 1. Use Case

V. IMPLEMENTATION

A. Private Blockchain Configuration

Multichain is a blockchain network for creating and deploying private blockchains for businesses. Multichain is an open- source tool built on the Blockchain architecture of Bitcoin.

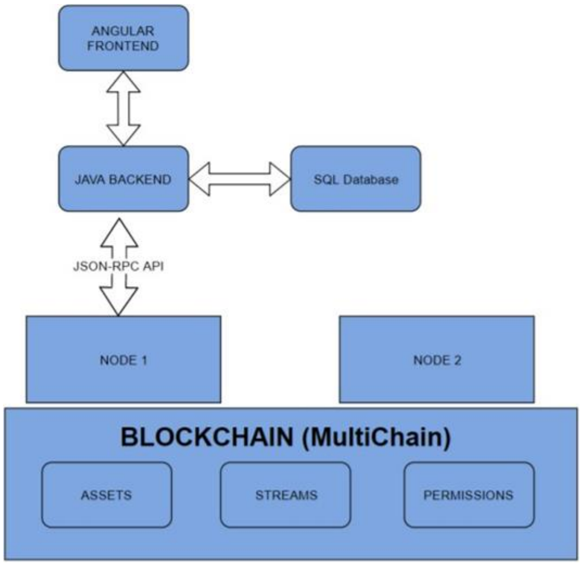


Fig. 2. MultiChain Architecture

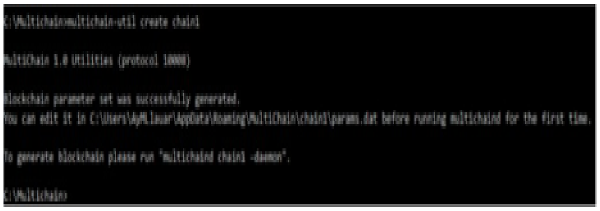
The following are the features of MultiChain:

- Multiple Currencies
- Faster Than Bitcoin
- Permissioned Architecture
- Fast Deployments
- Supported languages such as Python, JavaScript, PHP, Ruby.

Multichain is a fork of the Bitcoin Blockchain registry that allows you to build a private or public chain with a variety of configuration options such as target time for blocks, maximum block size, and metadata. To configure the chain, Multichain offers an API and a command-line interface.

B. Creating Blockchain

1) Creating Blockchain: Creating blockchain using "multichain-util create poe".

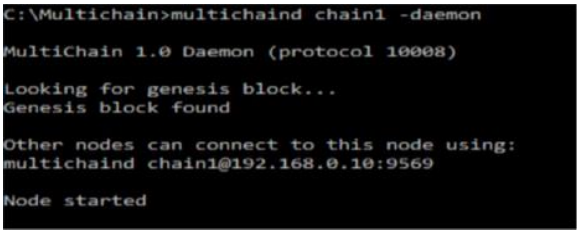


```
C:\Multichain>multichain-util create chain1

MultiChain 1.0 Utilities (protocol 10008)

Blockchain parameter set was successfully generated.
You can edit it in C:\Users\AyM.lauar\AppData\Roaming\MultiChain\chain1\params.dat before running multichaind for the first time.

To generate blockchain please run "multichaind chain1 -daemon".

C:\Multichain>
```

Fig. 3. Creating Blockchain

2)Configure BlockChain: Configure blockchain in c:/users/yourname/appdate/MultiChain/poe/params.d at

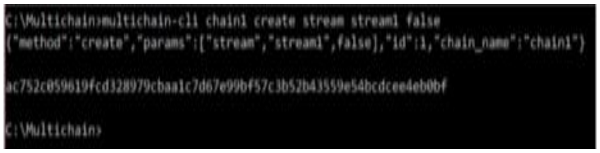
3)Node Start: Start creating a blockchain with "multi-chaind poe -daemon".



```
C:\Multichain>multichaind chain1 -daemon

MultiChain 1.0 Daemon (protocol 10008)

Looking for genesis block...
Genesis block found

Other nodes can connect to this node using:
multichaind chain1@192.168.0.10:9569

Node started
```

Fig. 4. Node Start

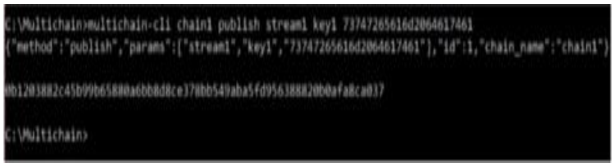
4)Create Stream: Create Stream using "create stream mainstream false"



```
C:\Multichain>multichain-cli chain1 create stream stream1 false
{"method":"create","params":["stream","stream1",false],"id":1,"chain_name":"chain1"}

ac752c059619fcd328979cbaa1c7d67e99bf57c3b52b43559e54bcdcee4eb0bf

C:\Multichain>
```

Fig. 5. Create stream

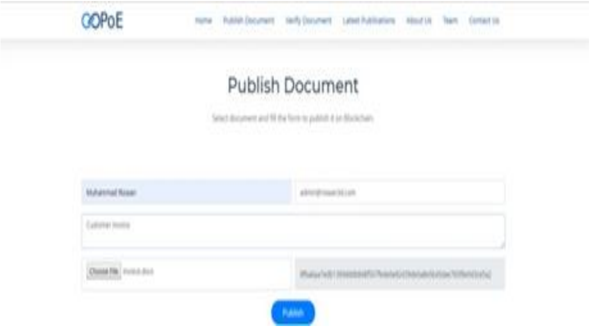
5)Subscribe Stream: subscribe stream by "subscribe main- stream" install apache and configure PHP with it and enable CURL run test curl commands.



```
C:\Multichain>multichain-cli chain1 publish stream1 key1 73747265616d206461746l
{"method":"publish","params":["stream1","key1","73747265616d2064617461"],"id":1,"chain_name":"chain1"}

0b1203882c45b99b65880a6bb8d8ce378bb549aba5fd956388820b0afa8ca037

C:\Multichain>
```

Fig. 6. Subscribe stream

6)Publish Document: This is Front-end view of the application.

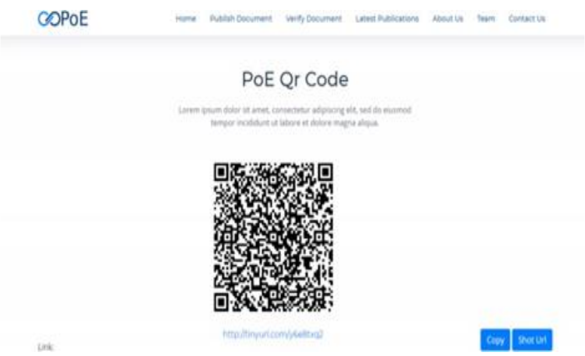


Publish Document

Select document and fill the form to publish it on Blockchain

Fig. 7. Publish Document

7)Get QR Code and Verification Link: After uploading the file QR code and verification link is generated.



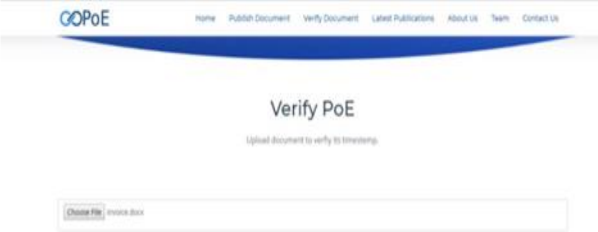
PoE Qr Code

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Link: http://tinyurl.com/y6e8txq2

Fig. 8. Get QR Code and Verification Link

8)Verify Document by Uploading: You can upload a document to verify them.



Verify PoE

Upload document to verify its timestamp.

invoice.docx

Fig. 9. Verify Documents

VI.CONCLUSION

A private blockchain is well-thought-out to have significant promise in the area of record authentication. ProofAnalyzer is a stable asset management device with massive scalable features that promises permanent, decentralized, and distributed structures. This encourages educational agencies to embrace cutting-edge technologies to ensure that their assets are still legitimate, verifiable, and decentralized. Document evidence that cannot be altered or deleted by third parties or governments. The method reduces paper use, lowers management costs, avoids record forgery, and delivers precise and dependable records on digital certificates.

REFERENCE

[1] K. Chopra, K. Gupta, and A. Lambora, “Proof of existence using blockchain,” in 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon).IEEE, 2019, pp. 429–431.

[2] Zˇ . Turk and R. Klinc, “Potentials of blockchain technology for construc- tion management,” Procedia engineering, vol. 196, pp. 638–645, 2017.

[3] G. Irving and J. Holden, “How blockchain-timestamped protocols could improve the trustworthiness of medical science,” F1000Research, vol. 5, 2016.

[4] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman et al., “Blockchain technology: Beyond bitcoin,” Applied Innovation, vol. 2, no. 6-10, p. 71, 2016.