



# Secure Access and Storage of Military Data based on Blockchain Technology.

3777

Jash Pradeep Jain<sup>1\*</sup>, Dr. Balaso Nivruti Jagdale<sup>2</sup>

<sup>1</sup> PG student of M.Tech. NMCS, School of Computer Engineering, Dr. Vishwanath Karad MIT World Peace University, Pune.  
E-mail:- [jash.p.parmar@gmail.com](mailto:jash.p.parmar@gmail.com)

<sup>2</sup> Professor in the School of Computer Engineering, Dr. Vishwanath Karad MIT World Peace University, Pune.  
[balaso.jagdale@mitwpu.edu.in](mailto:balaso.jagdale@mitwpu.edu.in)

\*Corresponding Author: - Jash Pradeep Jain

## Abstract

As we reach the fourth industrial revolution and the IT age, blockchain technology is gaining popularity and may affect our way of life in the future. Blockchain is a decentralized and distributed ledger system that enables users see each other's transactions in real time. Anyone with an internet connection may view the blockchain database. No one can claim control of a blockchain since it's spread over a network of computers, and its content is immutable. Decentralized and transparent information transmission make it a breakthrough technology. Blockchain technology is perfect for storing military data because to its decentralized nature and durability, security, and immutability. Blockchain's cryptography principle and algorithm secure data (In our case we have use AES 256bits). Cryptographic hashes provide secure blockchain transactions and data storage. Hashing a message of any length yields a fixed-length message digest. Each new block retains the preceding block's hash, ensuring immutability. Asymmetric cryptography ensures blockchain data integrity and accountability.

**Keywords:** Blockchain, security, certificates, Documents.

**Number:** 10.14704/nq.2022.20.7.NQ33467

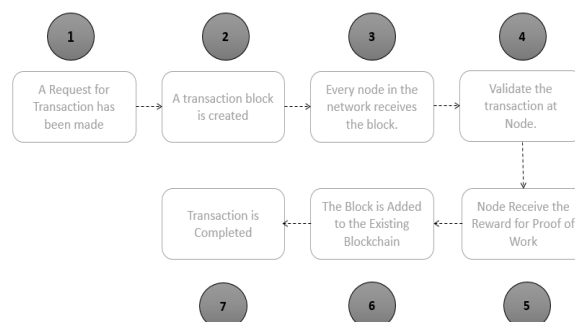
**Neuro Quantology 2022; 20(7):3777-3781**

## I. INTRODUCTION

Blockchain technology has proven to be a game-changer having the ability to revolutionize not just a few industries, but the whole business environment. Blockchain is a technology for handling electronic data that can help with transparency [1][2][6][7] and accountability [1]. Blockchain is a distributed ledger [1] of transactions that are available to all members of a computer network, which might avoid the possibility of a single point (centralized authority) of failure.

The collection of sequential records organized in a block structure that comprises the collections of transactions and the preceding block's hash is nothing but the blockchain. Every block is chronologically associated to the preceding one, and the records present on the Blockchain network is unchangeable.

A diagram of the fundamental phases involved in the functioning of Blockchain technology is depicted in figure 1.



**Diagram 1:** Steps involved in the operation of Blockchain technology

When it comes to healthcare, Quality health care facilities supported by emerging technologies are required. Blockchain could help to alter the healthcare industry.

While talking about traditional healthcare systems, acute information is typically spread across numerous systems and may not be readily available when needed. Today's healthcare infrastructure is insufficient to handle the exchange of information and requires some pinches.

The main objective of this research is to highlight the existing issues related to the educational



institutes and to find suitable blockchain features that could resolve them. We have adopted a systematic literature review approach for the identification and the extraction of relevant information from the shortlisted studies.

We have adopted a systematic literature review approach for the identification and the extraction of relevant information from the shortlisted studies. This study describes existing issues in three aspects physical, digital and financial. The results of the analysis shows that the manipulation risk, difficulty in verification and exchanging record between institutions are the major issues faced by the educational institutions. This study, then explores blockchain features including decentralization, traceability and consensus mechanism that can be used to address the issues related to the educational institution.

The paper is structured into four sections. Section I contains entire introduction. Section II provides the technological advancements executed by various researchers in blockchain in Education. The major works have been depicted in this section. Section III provides the overall architecture of the proposed system. The conclusion of the survey has been summarized in Section IV.

### Benefits of Blockchain in Education

Blockchain technology has limitless benefits in the field of education some are mention as following:

- **Decentralization:** considering P2P distributed architecture over a centralized one brings an improvement of the fault tolerance, by eliminating the central points of failures and bottlenecks.
- **Scalability:** allows the elimination of situations where one or several entities control the storage and processing of information of a large number of people.
- **Reliability:** the information can remain unchanged, immutable and distributed over time in blockchain. Any system participant can verify the authenticity of data.
- **Security:** information and communications can be secure if considered as transactions of the blockchain, based on cryptographic protocols. Thus, for example, blockchain offers the potential to make degree records more secure.

## II. LITERATURE REVIEW

Blockchain technologies are under active development globally, and there may be recent advances that impact our findings. To mitigate this, we have endeavored to follow advances in blockchain technologies by monitoring international technology conferences, published academic papers, and grey literature (such as white papers, and blogs).

3778

A blockchain is a distributed digital ledger that enables the information recording and sharing by a community in which each member keeps his/her own copy of the information and must validate collectively any update. The blockchain is a “trust-free, tamper-proof, auditable, and self-regulating system, with no human intervention required to execute computation”

M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia [2] the data centers hardware and software is what we will call a cloud. When a cloud is made available in a pay-as-you-go manner to the general public, they call it a public cloud; the service being sold is utility computing. They use the term private cloud to refer to internal data centers of a business or other organization, not made available to the general public, when they are large enough to benefit from the advantages of cloud computing that we discuss here. Thus, cloud computing is the sum of SaaS and utility computing, but does not include small or medium-sized data centers, even if these rely on virtualization for management. People can be users or providers of SaaS, or users or providers of utility computing. They focus on SaaS providers (cloud users) and cloud providers, which have received less attention than SaaS users

S. Kamara and K. Lauter [3] in this paper consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. They describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. Survey the benefits such architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.



B. Wang, B. Li, and H. Li, in this paper, we propose Knox, a privacy-preserving auditing scheme for shared data with large groups in the cloud. They utilize group signatures to compute verification information on shared data, so that the TPA is able to audit the correctness of shared data, but cannot reveal the identity of the signer on each block. With the group manager's private key, the original user can efficiently add new users to the group and disclose the identities of signers on all blocks. The efficiency of Knox is not affected by the number of users in the group.

The last benefit identified in this review is enhancing user interactivity and system interoperability. The model for e-learning systems based on blockchain technology. They used a learning reward system for participating in learning activities. The learning resources can be shared through all nodes in the peer-to-peer network. All learning records are merged into a block and can be easily checked to track the learners' progress of interactivity and interoperability.

Improving the efficiency of managing students' records is a great benefit of blockchain technology. Using blockchain in education can potentially reduce the risks of trading mistakes between the intended parties. Instead, it uses one ledger for a faster and more efficient method to exchange data. With the help of blockchain, digital records and certificates can be managed more effectively due to its flexibility and transparency.

### III. PROPOSED SYSTEM

Paper-based documents and manual processes are still the norm in the defense industry when it comes to maintaining records to meet regulatory requirements. Manual documentation, on the other hand, is prone to errors and difficult to manage. Data duplication is also a significant concern with this type of storage, due to the fact that multiple groups are working simultaneously to process and update the data records. A major issue with data sharing is that people are afraid that their data will be misused or interpreted incorrectly. In the context of trust, data sharing approaches are still immature.

An interplanetary file system (IPFS) based blockchain data sharing platform was proposed in this paper to address these issues. If you want a secure data network, a distributed ledger

system is an excellent option. Cryptography is used to ensure the security and integrity of the data stored and shared by the peer-to-peer system, as defense information is often highly confidential. Uploading a document to IPFS and encrypting it ensures its safety. Our public and private keys safeguards for confidentiality and authenticity of the military data.

Using blockchain technology, the proposed system enables us to provide a more transparent method of document storage. The system's use of the IPFS decentralized file-sharing platform ensures even more secure data transfer by removing the reliance on a single point of storage, minimizing the risk of data loss or destruction. The document is initially encrypted using the AES (256 bit) algorithm. The key used to encrypt the data is again encrypted using the RSA algorithm. After that, the encrypted data is forwarded to the IPFS. Thus, only a genuine user is able to decrypt the data. Thus, it provides some level of security through the use of double encryption.

#### 1. Proof of Ownership

Data Owner/Seller uploads property related document, metadata on a decentralized platform after encryption using keys. Also, each and every document of the property has a digital e-signing. And all such related documents should be able to be modified by authorized users.

#### 2. Proof of Authentication

Each user has a one unique username and password which is used for authentication of users. Each user has a unique digital e-sign because they are used for uploading property documents.

#### 3. Upload Property File with Digital Signature

Prior uploading the property document, digitally sign every individual document. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer. So we use digital signatures for Uploading property file.

#### 4. Upload property File & Grant permissions

Suppose Data owner/seller upload property documents with Encryption format and using digital signature. If XYZ user want to access this property document which is uploaded by authorized person that time XYZ user will sent



the request to authorized person then authorized person can give permission to XYZ user. With its permissions, because now a day security is very important. Permissions are Read, Write and Append.

### 5. Share Property File

Document owner/seller can share data with other users by using this decentralized platform. It provide different types of permissions to users.

### 6. Store Property File Using Blockchain

It is a decentralized, distributed system in which the digitally signed property file is stored in consecutive blocks. IPFS is a protocol is designed here to store a peer-to-peer distributed file storage.

Encryption is the process of transforming information in such a way that an unauthorized third party cannot read it, a trusted person can decrypt data and access it in its original form though. There are a lot of popular encryption/decryption methods, but the key to security is not a proprietary algorithm. The most important thing is keeping the encryption key (password) a secret so only trusted parties know it. Encrypt everything to protect your data so each property file will be stored in Encrypted Format.

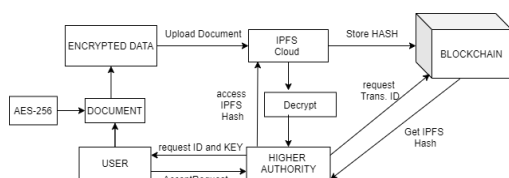


Figure: - System Architecture and Flow

### IPFS - Inter Planetary File System

- ❑ IPFS is a distributed system for storing and accessing files, websites, applications, and data.
- ❑ IPFS can be rightly called as the Hard drive for blockchain. It is a storage system that facilitates direct interaction via a secure and global peer-to-peer network.
- ❑ It stores data using a distributed hash table, once the hash is obtained, we ask the peer network for the user who has the content located in that hash, and we download directly from the node that has the required data.

### Advantages: -

- ❑ The data will be directly delivered by IPFS and pulled from the blockchain.
- ❑ Safe social networks as the information will be available to only those whom you give the permission.
- ❑ Uncensored communication without any intermediaries.
- ❑ Your private keys will be the only account needed as an identity for Documents.

3780

### IPFS and Blockchain

- ❑ Blockchain is a decentralized peer-to-peer network that provides immutability and thus, is the best choice to support traceability of data on a distributed file system like IPFS.
- ❑ IPFS and blockchains share a similar structure and work well together.
- ❑ As IPFS would connect all different blockchain quite like how the internet connects all websites.
- ❑ It might as well act like a backbone structure for the new web. Like we link one page to another using a link, a link can be placed in Ethereum in order to link to some other network.

## IV. RESULT AND ANALYSIS

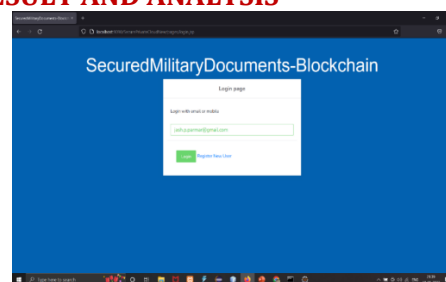


Figure: - Login Page

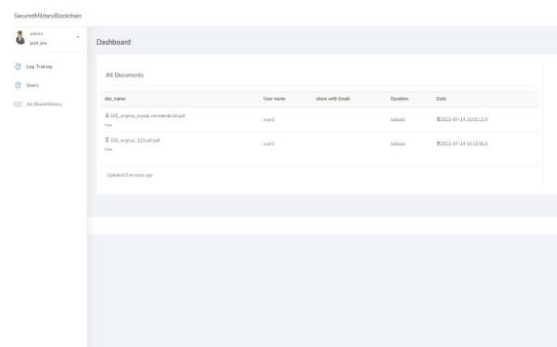


Figure: - Home-Dashboard Page



