information

Article

IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field

Shaik Arshiya Sultana [1], Chiramdasu Rupa [1,*], Ramanadham Pavana Malleswari [1] and Thippa Reddy Gadekallu [2,3,4,5,6,*]

[1] Department of Computer Science and Engineering, VR Siddhartha Engineering College, Vijayawada 520007, India; shaikarshiyasultana1@gmail.com (S.A.S.); nlramanadham@gmail.com (R.P.M.)
[2] Department of Electrical and Computer Engineering, Lebanese American University, Byblos P.O. Box 36/S-12, Lebanon
[3] College of Information Science and Engineering, Jiaxing University, Jiaxing 314001, China
[4] Zhongda Group, Haiyan County, Jiaxing 314312, China
[5] Division of Research and Development, Lovely Professional University, Phagwara 144411, India
[6] School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, India
* Correspondence: rupamtech@gmail.com (C.R.); thippareddy@ieee.org (T.R.G.)

Abstract: In the digital age, ensuring the authenticity and security of academic certificates is a critical challenge faced by educational institutions, employers, and individuals alike. Traditional methods for verifying academic credentials are often cumbersome, time-consuming, and susceptible to fraud. However, the emergence of blockchain technology offers a promising solution to address these issues. The proposed system utilizes a blockchain network, where each academic certificate is stored as a digital asset on the blockchain. These digital certificates are cryptographically secured, timestamped, and associated with unique identifiers, such as hashes or public keys, ensuring their integrity and immutability. Anyone with access to the blockchain network can verify a certificate's authenticity, using the MetaMask extension and Ethereum network, eliminating the need for intermediaries and reducing the risk of fraudulent credentials. The main strength of the paper is that the data that are stored in the blockchain are unique identifiers of the encrypted data, which is encrypted by using an encryption technique that provides more security to the academic certificates. Furthermore, IPFS is also used to store large amounts of encrypted data.

Keywords: academic certificates; encryption; blockchain; MetaMask; Ethereum; IPFS

Citation: Sultana, S.A.; Rupa, C.; Malleswari, R.P.; Gadekallu, T.R. IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field. *Information* **2023**, *14*, 446. https://doi.org/10.3390/info14080446

Academic Editor: Kun She

Received: 5 July 2023
Revised: 1 August 2023
Accepted: 2 August 2023
Published: 7 August 2023

1. Introduction

In the digital age, the importance of securely storing and verifying academic certificates is important. These certificates represent vital proof of an individual's educational achievements and serve as credentials for the various professional opportunities [1–3]. However, the traditional methods of issuing and verifying certificates are susceptible to fraud, manipulation, and loss, posing significant challenges to individuals, institutions, and employees. According to a survey, 60% of educational organizations are hit by phishing attacks. Targeting cloud data, the highest result of all verticals analyzed that the majority of educational organizations experienced phishing attacks (60%) and account compromise (33%) in 2020. Phishing was the most common incident, faced by all verticals analyzed in the report, but the frequency of this type of attack in the educational sector was much higher than the average of 40%. Additionally, 27% of educational organizations experienced ransomware, and 49% were unaware of the infection for days. The majority of respondents attribute their high level of vulnerability in the cloud to understaffed IT and security teams (53%), lack of expertise in cloud security (52%), and lack of budget (49%). To address these challenges, innovative technologies such as blockchain and encryption have emerged as powerful tools for enhancing the security and reliability of academic

certificates [4–7]. Blockchain, the decentralized and immutable ledger technology that is used in cryptocurrencies like bitcoin offers a transparent and tamper-resistant framework for storing and managing digital records [8–11]. Encryption, on the other hand, ensures the confidentiality and integrity of data by encoding it using complex algorithms. It aims to explore the potential of blockchain and encryption in securing academic certificates, luteinizing the way educational credentials are managed and verified. By leveraging the inherent features of blockchain, such as decentralization, transparency, and immutability, coupled with robust encryption techniques, the integrity, authenticity, and accessibility of academic certificates can be significantly enhanced [12–14].

Figure 1 Represents a common blockchain environment for securing academic certificates. The user has to be authenticated by the educational institution authority, then only the user is allowed to enter the details in the front-end application. Later, the data is encrypted using the MetaMask extension and connects to any Ethereum network to store encrypted data on the blockchain.

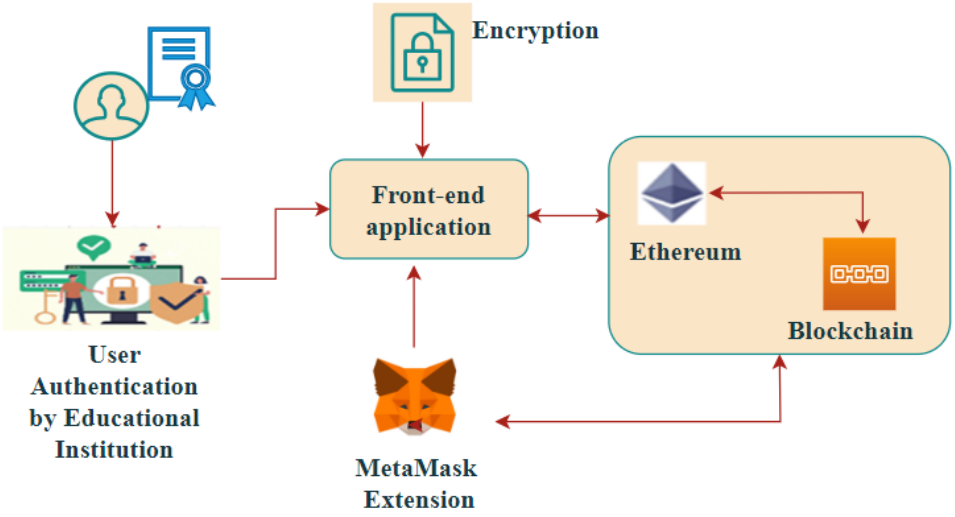

Figure 1. A generic Blockchain Scenario for securing Academic Certificates (Using MetaMask).

1.1. Research Contributions

The contributions of this paper are summarized as follows:

- Analyse several existing blockchain applications and their limitations, as described in the literature survey section.
- The paper presents a well-designed and implemented system that ensures the security of academic data on the blockchain by employing robust encryption techniques. Additionally, the system leverages the MetaMask extension for efficient storage and seamless execution of operations on the encrypted data.
- Perform a detailed security analysis of the proposed system so that it is highly secured against various potential attacks on the blockchain and encrypted data.
- Investigate the regulatory and legal implications of using blockchain technology for securing academic data, offering insights into compliance requirements and data privacy considerations.
- Discuss potential challenges and future directions in the adoption of blockchain-based solutions for academic data security, paving the way for further research and development in the field.

1.2. Road Map of the Paper

The remaining paper is organized in the following way: In Section 2, we present the literature survey. Preliminaries are discussed in Section 3. In Section 4, we discuss the proposed methodology. In Section 5, we describe the security analysis. In Section 6, we describe the results and analysis. In Section 7, we present the conclusion.

2. Related Work

Sun et al. [11] proposed a storage solution for health care information security built on the hyperledger fabric and the attribute-based access control framework. The solution first makes use of attribute-based access management, which enables dynamic and fine-grained access to medical data and then stores the data on the blockchain, which can be made secure and impervious to tampering by creating appropriate smart contracts. Additionally, to reduce the strain on the blockchain's storage, this solution also uses IPFS technology. The advantage is high throughput when accessing medical information. Potential disadvantages of the proposed solution include scalability challenges, adoption complexities, governance and compliance considerations, access control complexity, and network and security risks.

Wang et al. [12] described a decentralized architecture for safe EHR exchange. A secure platform for health care facilities to communicate their encrypted EHR is created by the design, which makes use of the blockchain's smart contract technology. A constant-size attribute-based encryption (ABE) system is developed, in which the access policy is encoded in the search result on the blockchain, taking into consideration that fine-grained access control is required in actual EHR sharing services. The recommended remedy is a successful system that enables authorized MedShare users to do multiple-keyword boolean searches across encrypted EHR. The outcomes show how effective MedShare is for exchanging EHRs. Potential limitations of the MedShare framework include scalability and performance challenges when dealing with a large volume of encrypted EHR data.

Zeng et al. [13] propose a framework for collaborative data training that is based on federated learning and blockchain technology. The gradients of the model are also encrypted and decrypted by the suggested homomorphic encryption approach to protect privacy. To be more specific, the framework is as follows: (i) they trained the local model using a novel capsule network for segmentation and classification of COVID-19 images; (ii) they used homomorphic encryption to secure the local model that encrypts and decrypts the gradients; and (iii) finally, the model is shared over a decentralized platform through the proposed blockchain-based federated learning algorithm.

Rahman et al. [14] proposed a solution to verify the authenticity and make the assertion of the decentralized system secure by deploying a blockchain-based academic credential authentication method. Academic certifications will be created by the system, authenticated, and corrected. Blockchain technology was used to develop a blockchain-based certificate authentication system. where the administrator might create, validate, and, if required, update the certificate. The administrator can also look up the number of times a certificate has been altered. To make fixes possible, they used two blockchains. This method will ensure prompt responses, dependable storage, and an end to questions regarding the validity of certificates. Any disruptions or failures in the blockchain network, such as network congestion, latency, or downtime, could impact the system's performance and availability.

Farouk et al. [15] proposed a decentralized, trustworthy, and highly regarded ledger that can be used by a student information system (SIS) to hold crucial data. The proposed models place a strong emphasis on data accessibility, which is exemplified by students' constant access to their data. This study suggests three approaches for implementing fully functional SIS on blockchains that store transactions like student marks, faculty member records, and course registration records, keeping away from being a super administrator or a centralized exposed storage where data integrity is at risk. The suggested model creates, validates, and publishes the certifications quickly to the interested parties without engaging a centralized administration. Ensuring interoperability and compatibility with other systems or platforms used in the education sector could pose challenges during implementation.

Ullah et al. [16] propose a decentralized distributed storage and sharing system based on blockchain that supports end-to-end encryption and granular access management. The suggested IoTChain paradigm uses the Ethereum blockchain as an auditable access control layer based on fine-grained permission on attribute-based access control (A-BAC) policy.

The IoTChain concept, which combines the Ethereum blockchain and the interplanetary file system (IPFS), is designed for smart contracts. They share secret keys between data owners and consumers using the elliptic curve Diffie–Hellman key exchange protocol and an advanced encryption standard (AES) for encryption. The outcomes show that the strategy for IoT data is practical and cost-effective. The limitation here is the delays and impact on real-time data processing and also sharing in IoT applications.

Agyekum et al. [17] provided a proxy re-encryption strategy for safe data exchange in cloud settings. Identity-based encryption allows data owners to send their encrypted files to the cloud, while proxy re-encryption construction allows only authorized users to access the files. An edge device serves as a proxy server to conduct demanding calculations because the Internet of Things devices are resource-constrained. They improved the quality of service and made efficient use of the network capacity by utilizing some information-centric networking capabilities to provide cached material in the proxy. Additionally, the system paradigm is based on blockchain, a groundbreaking technology that permits decentralized data sharing.

Hao et al. [18] suggest a simple blockchain-based architecture for an intelligent autonomous access control system for Internet of Things devices. With the help of a token accumulation mechanism, the intelligent blockchain architecture makes it possible to store access policies, provide authentication services for data access control, and assess the trustworthiness of access request nodes. In particular, the blockchain network must confirm the user's access request before it can be granted. A compromised resistant consensus algorithm is modified and put into use to protect against no more than 1/3 compromised authenticators, ensuring the authenticity's dependability. It may require additional computational resources and introduce network overhead, which could impact the overall performance and scalability of the IoT system.

The summary of the literature survey is presented in Table 1, which provides an overview of the different blockchain technology types, admin Encryption, blockchain technology tools, applications, and integrity check measures discussed in various research papers.

Table 1. Summary of Related Work.

Author	Admin	BCT Type	Encryption	BCT Tool	Integrity Check	Application
Sun et al. [11]	Yes	Hyperledger	No	Not Specified	Yes	Health care information
Wang et al. [12]	No	Not Specified	Yes	Ethereum	Yes	EHR data
Zeng et al. [13]	No	Not Specified	Yes	Not Specified	No	Medical image data
Rahman et al. [14]	Yes	Not Specified	No	Not Specified	Yes	Academic Certificates authentication
Farouk et al. [15]	No	Not Specified	No	Not Specified	No	Student information system
Ullah et al. [16]	No	Not Specified	Yes	Ethereum	Yes	IoT data
Agyekum et al. [17]	No	Not Specified	Yes	Not Specified	No	IoT data
Hao et al. [18]	No	Consortium	No	Not Specified	Yes	Access control for IoT devices

3. Preliminaries

3.1. IPFS

IPFS (Interplanetary File System) is a decentralized file storage system that operates using a distributed network to store and retrieve files [19,20]. In this scenario, IPFS can be used to store files, documents, or other data related to the application as shown in Figure 2. The encrypted files uploaded by the admin are stored in IPFS. IPFS provides a unique content identifier (CID) for each file, allowing easy retrieval and verification. IPFS utilizes content addressing, ensuring redundancy, fault tolerance, and easy retrieval of files by referencing their content rather than their location [21].

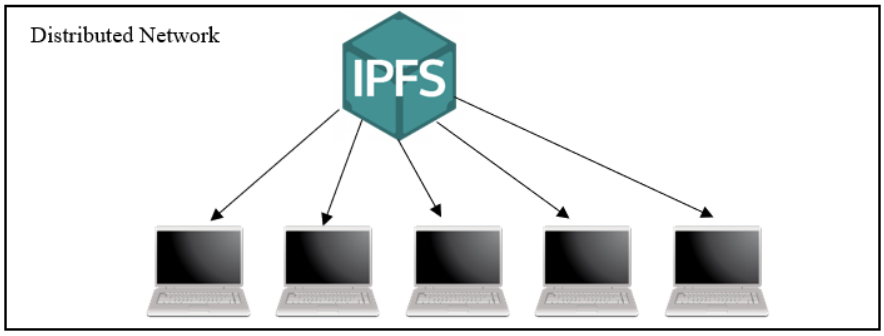

Figure 2. Distributed network.

3.2. MetaMask

MetaMask is a popular browser extension and digital wallet that allows users to interact with decentralized applications (DApps) and blockchain networks, primarily Ethereum. It provides a user-friendly interface for managing Ethereum accounts, storing cryptocurrency assets, and interacting with decentralized applications. In the given scenario, MetaMask serves as a digital wallet and a gateway between Web browsers and blockchain networks. Users can install the MetaMask extension, create and manage their Ethereum accounts, and securely store private keys. It provides secure authentication and authorization for the admin and user. MetaMask allows the admin to sign transactions and interact with the blockchain network, ensuring that only authorized actions are performed. It enables users to interact with blockchain-based applications by providing a user-friendly interface and handling transaction signing.

3.3. System Model

Figure 3 illustrates the overview of the proposed system. Admin can perform two operations on the proposed system, i.e., storing and viewing the data whereas the user can only access(view) the stored data. First, the admin enters the academic details into the Web interface application. An identity (ID) is generated and the data is encrypted [22–24]. Now, the Cipher Text (CT) is transferred to nodes that are connected to IPFS (Interplanetary File System) where the hash values are stored for the CT. The corresponding hash values are stored in the blockchain only if there is enough ETH balance in the wallet (MetaMask). So, whoever wants to access the data should have a sufficient ETH balance in their wallet. Then, the corresponding encrypted data associated with the hash value is decrypted. Finally, the data is displayed to the user in the Web interface with the help of Web-based knowledge management.

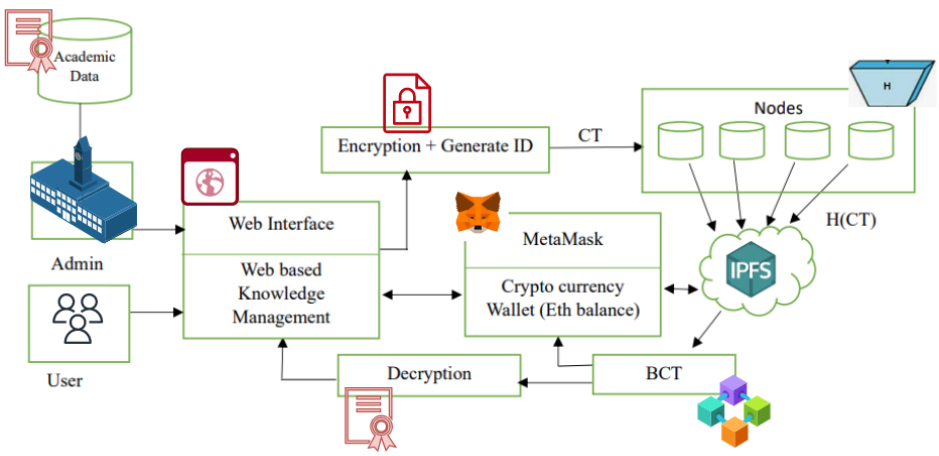

Figure 3. Overview of the Proposed architecture.

4. Proposed Methodology

The distributed ledger technology known as blockchain enables safe and open record-keeping. It functions as a decentralized database that is managed by a distributed computer network as opposed to a single entity [25]. Regarding this, the proposed architecture has mainly 4 modules. Mainly Admin & user, Encryption, Blockchain, and Decryption. In a decentralized application scenario, the admin holds the responsibility of managing the application and overseeing its operations. The admin can upload files with a unique ID. The content is encrypted and stored in IPFS along with the ID. The User can then access the content stored on IPFS. To ensure that the content is tamper-proof and has not been modified, a hash of the content can be stored on the blockchain [26]. This provides a record of the content's existence and ownership and can be used to verify the authenticity of the content.

The admin can use the tool MetaMask to interact with the blockchain and manage transactions related to the content. The user can then decrypt the content. This system provides a secure way for users to view content stored by an admin while ensuring that the content is protected and cannot be tampered with.

Figure 4 depicts the proposed system's logical view. We assumed that the user's request and the admin's request are authenticated by the educational institution's authority. If the integrity check is failed then that request is discarded. Else, it is sent to the system application in which operations such as issue (), verify (), revoke (), and view () can be performed. Then, the input data is encrypted in the secure communication channel (EHBC) and the output CT is given as input to the Ethereum module by using MetaMask if the ETH balance is greater than the threshold value.

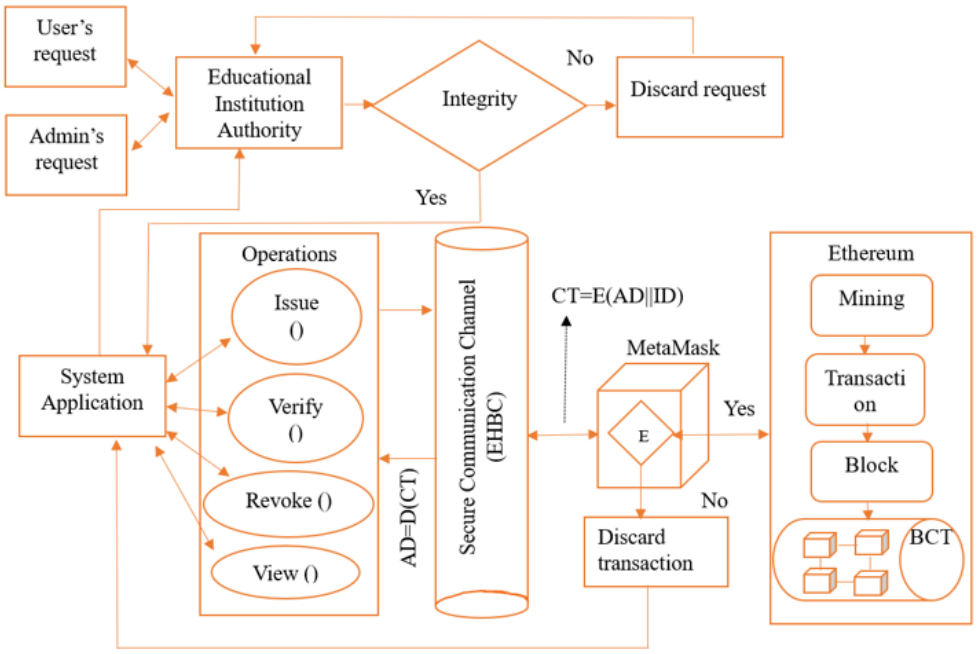

Figure 4. Logical view of the Proposed architecture.

Finally, the data are stored in the blockchain [27,28]. If the ETH balance is less than the threshold value then the transaction is discarded and displayed to the system application. To get the data from the blockchain, they are decrypted in a secure communication channel (EHBC) and then displayed to the system application. Notations and their descriptions are shown in Table 2.

Table 2. Notations and their Descriptions.

Symbol	Description
BCT	Blockchain
CT	Cipher Text
C	Original Message
T_s	Tetrahedral-based Secret key
P_s	Pentatope-based Secret key
C_a	ASCII value of the character
BO	Binomial Coefficient
HO_1	Homomorphic operation-1: Homomorphic division
HO_2	Homomorphic operation-1: Homomorphic modulus
HO_3	Homomorphic operation-3: Homomorphic multiplication
HO_4	Homomorphic operation-4: Homomorphic addition
AU	Admin/User
D()	Decryption
H(CT)	Hash digest of the cipher text
App_{data}	Applicant credentials
Eth_{Bal}	Ethereum Balance (ETH value)
CP	Certificate Type
CI	Certificate Issuer
RP	Certificate receiving Person
AD	Academic Data
E()	Encryption
BCT_{ID}	ID of the Encrypted data
ID	Admin/User id
$Trans_{tp}$	Transaction Throughput
$Trans_{lt}$	Transaction Latency
n_t	Total no. of transactions
t_s	Total time in seconds
n_{t1}	Time that the transaction's block is added to the blockchain
n_{t2}	Time that the transaction was started and sent to the network

4.1. Admin and User

The administrator and the user are the two primary roles in this system. The user can obtain and read the decrypted data, while the admin is responsible for safely uploading and storing the data. The admin is responsible for managing the decentralized application, who is an authorized user, and uploads and manages data within the system as shown in Table 3. They have the authority to encrypt the files before uploading them. They set up permissions, manage user access, and ensure the smooth functioning of the system. The admin's primary goal is to ensure the security and integrity of the stored data [29,30]. The user is an individual who interacts with the application to perform various actions or access specific features. They have an appropriate access right and can retrieve and view the encrypted files stored in IPFS.

4.2. Encryption

To ensure data privacy and security, sensitive information exchanged between the admin and users can be encrypted before uploading them [31]. A new lightweight homomorphic encryption algorithm is used to encrypt the data, having two keys. Encryption transforms the data into an unreadable format, making it difficult for unauthorized parties to access or understand the information. Algorithm 1 represents the encryption process, which involves two main operations, Binomial Coefficient (BO) and homomorphic operations HO_1, HO_2.The two Keys Tetrahedral-based $(T_s \rightarrow \{T_{s0}, T_{s1}, \ldots, T_{s(m-1)}\})$ and Pentatope-based keys $(P_s \rightarrow \{P_{s0}, P_{s1}, \ldots, P_{s(m-1)}\})$ of variable length are generated randomly. Now, convert each character of plain text to its corresponding ASCII value

$C_{aj} \leftarrow ASCII(C_j)$ as shown in Figure 5. Then, apply XOR operation $BO_j \leftarrow C_{aj} \oplus T_{sj}$. Now perform homomorphic operations, division, and modulus on the obtained data by using the Pentatope-based key. Concatenate the results of division and modulus with alphabet characters 'f' and 'r', which gives us our final cipher text $CT_t \leftarrow Concat(f, DH_j\, r, MH_j)$.

Table 3. Operations of Admin and User.

Actor	Operation	Description
Admin	Registration ()	Each administrator must register with a distinct ID (ID).
	Issue certificate ()	It requires user document IDs, the type of certificate, the certificate's issuer, the date, and the recipient.
	Certificate Details ()	By using the user ID, the information from the blockchain provided by the relevant authority for the matching user certificate data is presented.
	Verify Certificate()	When checking a certificate, the registration number and ID are required.
	Authentication ()	No admin can issue or get certificate details unless they are authorized.
User	Registration ()	Every user should register using a special ID (ID).
	Verify Certificate ()	To check the certificate, the registration number and ID must be present.
	Authentication ()	Unless they are authorized, no user is ever able to obtain certificate details.

Algorithm 1 Algorithm for Encryption

Input: Original Message
Output: Cipher Text
1: Read the original message as $C \rightarrow (C_0, C_1, \ldots, C_{(m-1)})$
2: Generate random keys,
Tetrahedral-based Secret key, $T_s \rightarrow (T_{s0}, T_{s1}, \ldots, T_{s(m-1)})$
Pentatope-based Secret key, $P_s \rightarrow (P_{s0}, P_{s1}, \ldots, P_{s(m-1)})$
3: For $j = 0$ to $m - 1$ do upto step 7.
4: Convert to the ASCII value of each character,
$C_{aj} \leftarrow ASCII(C_j)$
5: Perform Binomial Coefficient on ASCII of the original message.
$BO_j \leftarrow C_{aj} \oplus T_{sj}$
6: Apply homomorphic operations on BO_j
$HO_1 : DH_j \leftarrow Div(BO_j, P_{sj})$
$HO_2 : MH_j \leftarrow Mod(BO_j, P_{sj})$
7: Concatenate the result of homomorphic operations as shown below
$CT_t \leftarrow Concat(f, DH_j, r, MH_j)$
8: The result is a Cipher Text CT_t.

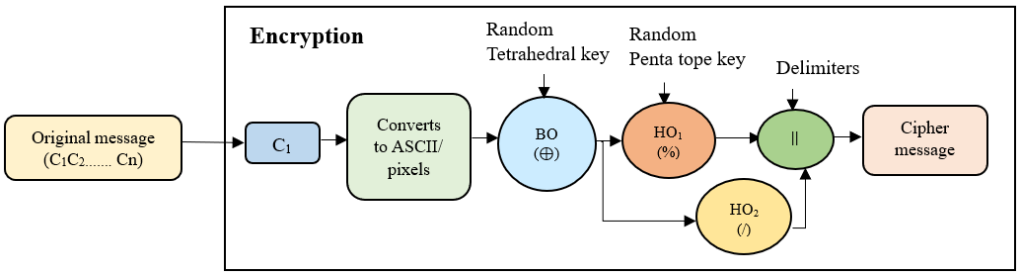

Figure 5. Encryption Process.

4.3. Blockchain

Blockchain is a decentralized and distributed ledger technology that makes it possible to record transactions and data in a safe and transparent manner. It functions as a chain of interconnected blocks, each of which holds a list of transactions or other data and is connected to the one before it by a cryptographic hash function. A permanent and unchangeable record of all transactions and data saved on the blockchain is produced by this connection. The decentralized nature of blockchain is one of its fundamental characteristics. The blockchain network, which comprises of several nodes or computers that participate in the authentication and verification of transactions, does not rely on a central authority, such as a bank or government [32]. Since there is no single point of failure due to this decentralization, the network's security and resilience are improved. Bitcoin and Ethereum are two examples of cryptocurrencies that are frequently linked to blockchain technology.

In the described scenario, The Ethereum blockchain-based antifalsification Solution for academic diplomas and certificates is carried out in a Web application. IPFS assigns each file a unique content identifier (CID), enabling easy retrieval and verification. These unique IDs are stored on the blockchain, ensuring immutability and tamper resistance. When a user or administrator wants to access a file from IPFS, then an ID should be verified. After the ID is confirmed, a hash value or a reference number from the blockchain is obtained. Metamask wallet is a browser extension used to obtain ETH. ETH is a monetary unit that is necessary to carry out any actions on a blockchain network. The Web application is running under the Ethereum blockchain, on localhost 8080.

Algorithm 2 depicts the Admin and User recognition and block creation of the block. Here, the applications prompt the use to enter the credentials belonging to them $\text{App}_{data} \leftarrow Name(AU)||Password(AU)||\text{Authority}_{name}$. After that integrity check Integrity App_{data} will be done with the credentials given by the Admin/User. If the credentials are valid then a unique ID will be issued. If the details provided by the Admin/User are wrong then the request is rejected. The encrypted academic data E(AD) must be stored in IPFS after the admin verification is complete, and the corresponding id BCT_{ID} hash code H(CT) must be stored in the blockchain. Before storing the data, the Eth_balance must be verified to carry out the transaction. If there is a minimum Eth_balance $\text{Eth}_{Bal} \geq \text{Threshold}_{value}$, then the operation is carried out $\text{Eth}_{Bal} \leftarrow (\text{Eth}_{Bal} - \text{Threshold}_{value})$. If there is not enough Eth_balance, then the operation is not performed and a message will be displayed to the admin that there is no sufficient Eth_balance.

Algorithm 2 Algorithm for Admin/User enroll and creation of Block

Input: Name, Password, Authority name, AD, CT, Eth_Bal
Output: Unique ID to AU, CT, Block formation
1: Submit the details of AU to the System such as Name, Password, Authority_{name}
2: $\text{App}_{data} \leftarrow Name(AU)||Password(AU)||\text{Authority}_{name}$
3: Verify the information
  IF(Integrity(App_{data})==True) THEN
  Issue unique ID
  ELSE reject the request
4: IF Admin
  Submit the academic data (AD).
5: Check Eth_Bal
  IF Eth_Bal $\geq$ Threshold_value THEN
    a block (block[i]) is created
  ELSE no block is created.
6: Eth_Bal $\leftarrow$ Eth_Bal $-$ Threshold_value
7: Store data in the created new block
  block[i] $\leftarrow$ BCT_ID/H(CT)
  IPFS $\leftarrow$ CT

Algorithm 3 illustrates the process of an Academic certificate being granted to the user by the Education authorities, using Certificate$_{issue}$() and validation by Certificate$_{Verify}$(). The user must first submit the necessary certification information, Certificate$_{type}$(CP) (UG or PG), Certificate issuer (CI) (either jntuk or their college itself), Date and the name of the receiving person to the education department through the Web application. Additionally, an authorized staff member from the education centers confirms the information by saving it in the facilities' local database (valid(credentials)==True && Present$_{system}$). After completing the verification process, the academic Certificate is encrypted and successfully transfer the Encrypted certificate into an Ethereum-based blockchain to create a blockchain-based ID. Any operation over a blockchain requires a balance in the Metamask Wallet. At the time of validation, the inputs from the user ID are taken and credentials are checked to see if they are stored in the blockchain or not (ID==True). If the user exits, then verified, otherwise denied.

Algorithm 3 Algorithm for Certificate$_{issue}$( ) and Certificate_Verify()

Input: CP, CI, Date, RP, ID, Name
Output: Certificate issued details
1: Validate the credentials provided by the admin
IF (valid(credentials)==True && Present$_{system}$)
Cipher$_{cer}(CT) \leftarrow E(\text{Exist}_{cer})$
IF (valid(credentials)==True && Pnew$_{ap}$)
Store the credentials in local database
The procedure is carried out on the blockchain network.
2: Link up with MetaMask
3: If the MetaMask request is confirmed,
If the connection has been made, proceed to Step 4; otherwise, the con nection is not set up.
4: IF Eth$_{Balance} \geq$ Operation$_{Balance}$ THEN
Set up the credentials on a blockchain.
Distinct BCT$_{ID}$ will be assigned to certificate
ELSE
Due to a lack of ETH balance, it is not possible to generate a BCT-based certificate
5: Decrypt the data retrieved from the IPFS with help of BCT$_{ID}$
AD $\leftarrow$ D(IPFS)
6: Fill out the Web-based application with ID, Name.
7: **IF** Certificate_Verify(ID is valid) **THEN**
Successfully Verified
ELSE
Invalid Entry, deny the user's request.

4.4. Decryption

When the user or admin requests to view a file, the system retrieves the encrypted file E(Exit$_{Cer}$) from IPFS. With the appropriate authorization, by using the appropriate decryption algorithm Description ( ) and the corresponding decryption keys, the encrypted data is converted back into its original readable format [26]. Decryption allows the user to access and understand the data securely.

Algorithm 4 represents the process of decryption and the input as cipher text; (CT) as shown in Figure 6, the Description procedure first extracts the number between f and r $E_j \leftarrow CM_t[f_j : r_j]$ and then also draws another number after r that is in between r and n $RE_j \leftarrow CM_t[r_j : f_{j+1}]$. Use a pentatope-based secret keys $P_s \rightarrow (P_{s0}, P_{s1}, \ldots, P_{s(m-1)})$ to perform homomorphic operations, multiplication (HO_3), and addition (HO_4) on the recovered data [33]. Utilize the Tetrahedral secret keys $T_s \rightarrow (T_{s0}, T_{s1}, \ldots, T_{s(m-1)})$ to perform a Binomial Coefficient on the data that is produced. The outcome is the ASCII value of the original text. The original plain text is produced by translating the ASCII value to a similar character and concatenating them.

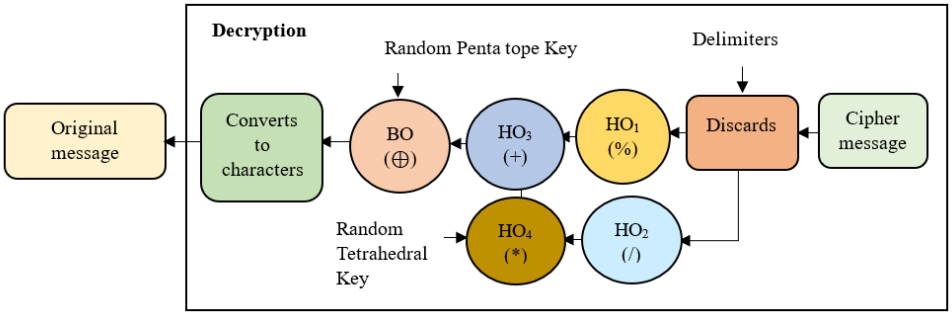

Figure 6. Decryption Process.

Algorithm 4 Algorithm for Decryption

Input: Cipher Text
Output: Original Message
1: Read the cipher text as CT.
2: Generate random keys, i.e.,
Tetrahedral-based Secret key, $T_s \rightarrow (T_{s0}, T_{s1}, \ldots, T_{s(m-1)})$
Pentatope-based Secret key, $P_s \rightarrow (P_{s0}, P_{s1}, \ldots, P_{s(m-1)})$
3: For $j = 0$ to $m - 1$ do up to step 7
4: Extract the substring between f_j, r_j and r_j, f_{j+1}, i.e.,
$E_j \leftarrow CT[f_j : r_j]$
$RE_j \leftarrow CT[r_j : f_{j+1}]$
5: Perform homomorphic operations
HO_3: $D_j \leftarrow Mul(E_j, Ps_j)$
HO_4: $S_j \leftarrow Add(D_j, RE_j)$
6: Apply Binomial Coefficient and convert it to the original message
$BO_j \leftarrow S_j \oplus Ts_j$
$C_j \leftarrow Ori(BO_j)$
7: Concatenate the result as shown below
$C_t \leftarrow Concat(C_j)$
8: The final result is the original message C_t.

Figure 7 represents the sequence diagram of the proposed methodology. Admin can perform two operations on the proposed system, i.e., storing and viewing the data, whereas the user can only access (view) the stored data. First, the admin enters the academic details into the Web interface application. An identity (ID) is generated and the data is encrypted. Now, the Cipher Text (CT) is transferred to nodes that are connected to IPFS (Interplanetary File System) where the hash values are stored for the CT. The corresponding hash values are stored in the blockchain only if there is enough ETH balance in the wallet (MetaMask). So, whoever wants to access the data should have a sufficient ETH balance in their wallet then the corresponding encrypted data associated with the hash value is decrypted [34]. Finally, the data are displayed to the user in the Web interface with the help of Web-based knowledge management.

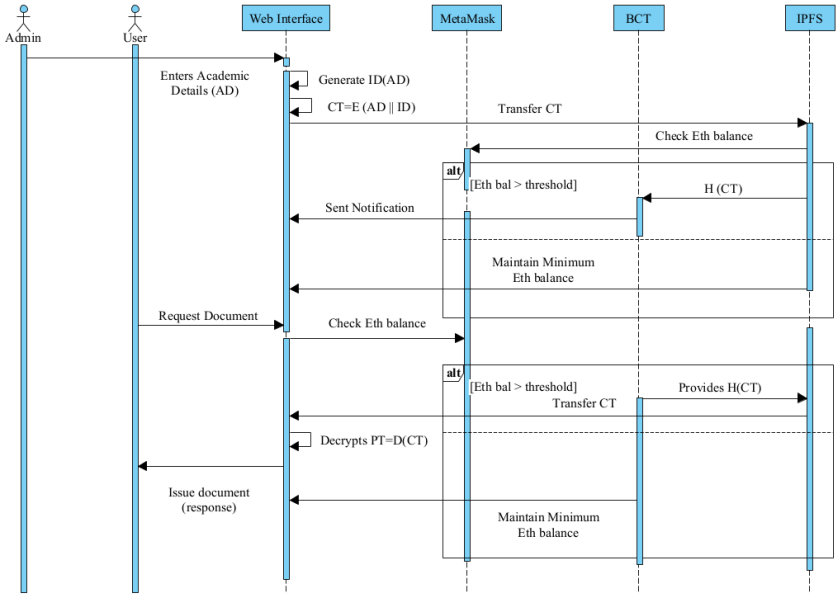

Figure 7. Flow of System Transactions.

5. Security Analysis

In order to provide secure storing and access control mechanisms, this section demonstrates how the proposed system may withstand additional attacks [35].

Proposition 1. *The proposed system is secure against the Known Plain Text Attack.*

Proof. Generally, this type of attack is performed when the attacker has access to both the plaintext (original message) and its corresponding ciphertext (encrypted message). This attack aims to deduce the encryption key or other secret parameters used in the encryption algorithm. During the encryption process the plain text PT $\rightarrow (PT_0, PT_1, \ldots, PT_{m-1})$ of length m, undergoes various operations HO_1 and HO_2 with two different keys, tetrahedral key TH_K and pentatope key PT_K, which are generated based on m, finally generates a ciphertext CT. Hence, even when the PT and CM are known to the attacker cannot be able to break the key that is used because it is not shared among the receiver and sender and are different for each message. Two keys (TH_K, PT_K) are employed here to increase the threat to an attacker. Additionally, the algorithm may be able to fend off this assault. □

Proposition 2. *The suggested method is resistant to the ciphertext-only attack.*

Proof. It is a type of cryptographic attack where the attacker can access only ciphertext and does not possess any knowledge of the corresponding plaintext. The objective of a ciphertext-only attack is to analyze the ciphertext to get information about the plaintext. With the reference of algorithm 1, the ciphertext produced during encryption will be of the form Concat(f,DH_j,r,MH_j). If the Invader 'Ï' extracts DH_j and MH_j using passive attacks, the invader can't achieve the plain text because there is no key at the Invader 'Ï'. So, it is difficult to crack the plain text from the cipher text because the CT is concatenated with the results of HO_1, HO_2 operations and the delimiters 'f' and 'r' which will make more complex to break. □

Proposition 3. *The proposed approach is immune to the Brute force Attack.*

Proof. In this method, an attacker systematically tries all possible combinations of keys to decrypt encrypted data. It is a straightforward and exhaustive approach that relies on the attacker's computational resources and time. Suppose the Adversary Å has different

number keys (NK) $NK_0, NK_1, NK_2, \ldots\ldots\ldots, NK_n$, if he tries to decrypt the cipher text by using the keys one after other, it takes nxm times, but the problem here is that two keys are used which are different to each other and for every letter we have used the two keys so it takes n^3Xm times. The Adversary $\mathring{A}$ should have to correctly guess, that up to where the n value must be taken, also it may not decrypt because we have used Tetrahedral key TH_K and pentatope key PT_K The Adversary $\mathring{A}$ cannot be able to guess that. Therefore, the proposed system is against the Brute force Attack. □

Proposition 4. *The proposed system is secure against 51% Attack.*

Proof. In a 51% attack, an attacker gains control over the majority (51% or more) of the mining power in a blockchain network. This allows the attacker to manipulate the blockchain's consensus protocol and potentially execute fraudulent transactions, reverse transactions, or double-spend cryptocurrencies. If an attacker A, tries to gain access over the blockchain network, there is an integrity check $\text{Integrity}(\text{App}_{\text{data}}) == \text{True}$; the data is authenticated by the educational authority if it is authorized and only allowed for operations in the blockchain. Preventing and mitigating 51% of attacks is a complex task. Networks with many participants and a high level of decentralization are less vulnerable to these attacks. Additionally, some blockchain networks employ alternative consensus mechanisms, such as proof-of-stake (PoS), which require participants to hold and lock a certain amount of cryptocurrency to validate transactions, making 51% attacks more difficult to execute. □

Proposition 5. *The recommended strategy is robust against Sybil's attack.*

Proof. A Sybil attack is a type of attack in which an attacker creates multiple fake identities or nodes in a peer-to-peer or decentralized network to gain control or influence over the network's operations. Assume an Adversary $\mathring{A}$ had created fake identity credentials Fake_{data}; at the time of integrity, check that the data is verified, whether it is present in the database or not $\text{Integrity}(\text{Fake}_{data}) == \text{Not\_Existed}$; then, the request is not processed. Hence, Identity Verification can address this issue. □

Table 4 compares the present works and proposed system to the various security qualities that can endure.

Table 4. Security Properties Comparison.

Security Property	[23]	[24]	[25]	Proposed System
Known Plain Text Attacks	✓	✓	✓	✓
Cipher-text only analysis Attacks	✓	✗	✓	✓
Brute Force Attacks	✗	✓	✓	✓
Chosen ciphertext Attack	✓	✗	✓	✓
51% Attack	✓	✓	✗	✓
Eclipse Attack	✓	✗	✓	✓
Sybil Attack	✗	✓	✓	✓

6. Results and Analysis

The proposed blockchain system provides a secure way of maintaining academic certificates. It consists of functions such as Issue (), Verify (), Revoke (), and View (), i.e., the cost of operations is as shown in Table 5 it has gas limit, gas price, and nonce etc. So, in order to perform any operation in the blockchain, the system has to connect with the MetaMask extension and the Ethereum network used is localhost 8485. Then, as shown in Figure 8, if the transferring account contains a minimum ETH balance, then the transaction

proceeds. Else, that transaction is discarded. After issuing the certificate, the total count of no. of certificates is incremented by 1 as shown in Figure 8.

Table 5. Cost of Operations in Proposed Model.

Function Name	Nonce	Gas Limit (Units)	Gas Used (Units)	Gas Price	Transaction Hash
Issue()	8	239,653	159,769	20	0x0219261e01550957dd8baa8527790c a1f8526fda956d93ce6f229f90bcf114B9
Verify()	4	239,653	256,962	24	0x7dE16Fb7f44E2715c614C15B9aB6 2b6a4184aa84c007763213d3141913Dc
Revoke()	5	239,653	195,774	18	0x1201c0b33b37b034ec879d21648952 d0f14a01205e3f83b19e6c8334cc245d5
View()	7	239,653	137,924	14	0x5c895c20880c429595ef922b23bd52 94a43aec183358471265875l152D5431

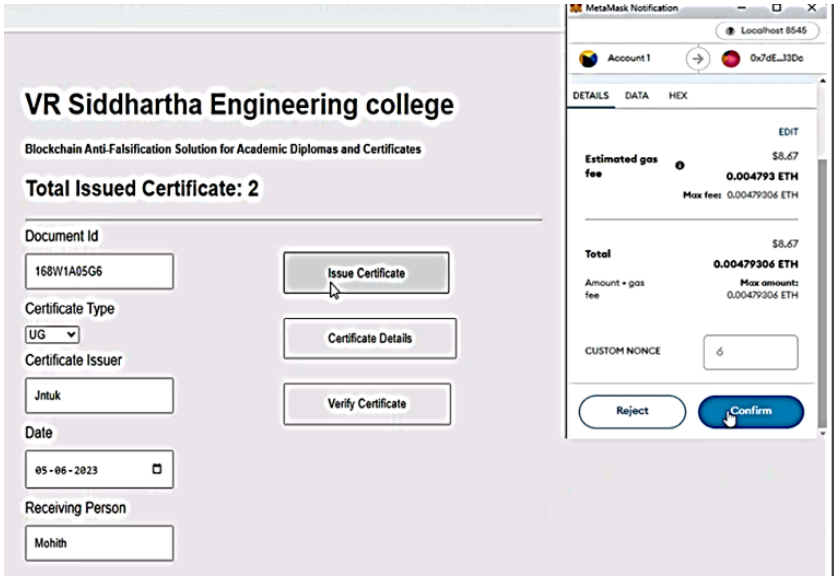

Figure 8. Issuing the certificate to the receiving person.

Table 6 shows that as the number of certificates increases, both the encryption time and blockchain storage time also increase. For instance, when there are 2 certificates, the encryption time is 0.00078 ms, and the blockchain storage time is 0.00023 ms. As the number of certificates increases to 50, the encryption time expands to 0.12 ms, and the blockchain storage time extends to 0.098 ms.

Table 6. Encryption and BCT storage time with respect to the number of certificates.

No of Certificates	Encryption Time (ms)	BCT Storage Time (ms)
2	0.00078	0.00023
9	0.0019	0.00098
15	0.006	0.0021
25	0.013	0.0086
37	0.056	0.027
50	0.12	0.098

Table 7 describes that as the no. of certificates and total ETH value. As the no. of certificates increases, the total ETH value required for the transaction increases.

Table 7. Total ETH value w.r.t. no. of certificates.

No of Certificates	Total ETH Value
1	0.01124786
5	1.25874638
10	3.58746931
15	5.18796248
20	7.15298648
25	12.2580136

A graph is plotted between the no. of certificates and the total ETH value, it represents that the graph is linearly increasing and the total ETH value required for the transaction increases w.r.t. no. of certificates as shown in Figure 9.

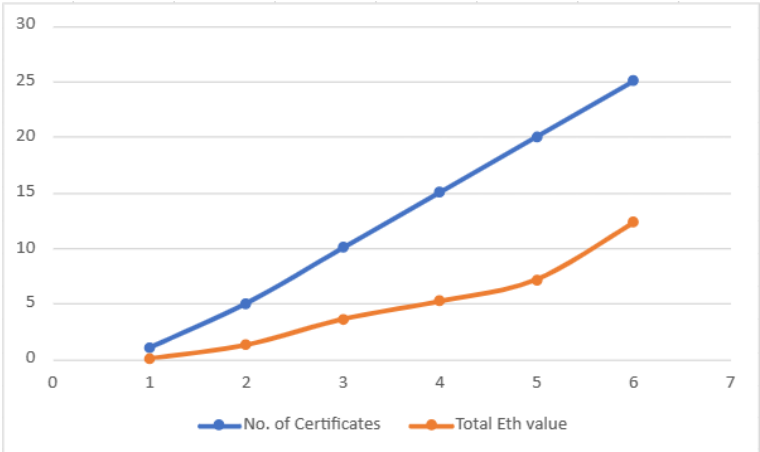

Figure 9. No. of certificates vs. Total ETH value.

Performance Analysis

The performance of the proposed system is obtained using Hyperledger Calliper. The testing tool Hyperledger Calliper is used to monitor the success rate, transaction throughput, and transaction latency (min latency, max latency, average latency) for the Ethereum network.

- Transaction Throughput: The rate at which transactions are committed to the network during a given period of time is known as transaction throughput.

$$\text{Trans}_{tp} = \text{n}_t / \text{t}_s \quad (1)$$

where n_t is the total no. of transactions and s is the total time in seconds.

- Transaction Latency: It is the amount of time needed for the network to process and verify a transaction. It takes into account the time required for a transaction to be broadcast, included in a block, and approved by network users.

$$\text{Trans}_{lt} = \text{n}_{t1} - \text{n}_{t2} \quad (2)$$

where n_{t1} is the time that the transaction's block is added to the blockchain and n_{t2} is the time that the transaction was started and sent to the network.

Table 8 represents the performance between the throughput, latency (max, min, avg) w.r.t. the no. of transactions. The performance metrics are measured for the transaction and the number of transactions starts from 10 and goes up to 50 with an increment of 10 each time. Latency is increasing linearly with the increase in the no. of transactions as shown in Figure 10. The graph is plotted between latency (max, min, avg) and no. of transactions.

Table 8. Performance measured between no. of transactions, throughput, and latency.

No. of Transactions	Throughput	Max Latency (s)	Min Latency (s)	Avg Latency (s)
10	3.4	42.16	0.12	21.14
20	4.6	54.31	0.18	27.25
30	3.7	72.49	0.13	36.31
40	5.1	104.57	0.15	52.36
50	4.2	112.78	0.17	56.48

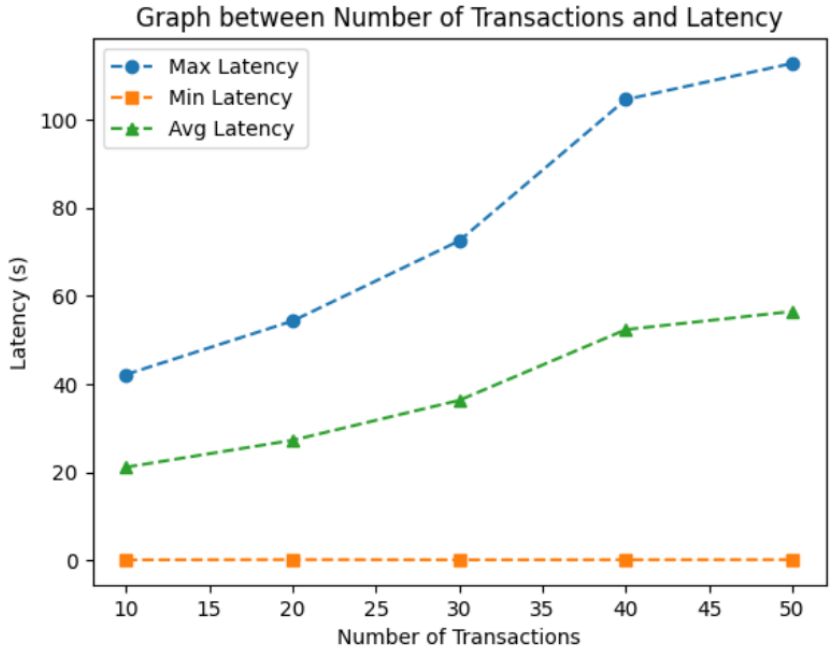

Figure 10. No. of Transactions vs. Latency.

A graph is plotted between the no. of transactions and throughput as shown in Figure 11. From the graph, it is observed that the throughput of a blockchain network typically rises and falls with the number of transactions due to the underlying consensus mechanism and the limitations of the network's processing capacity. They are consensus mechanism, block size and block time, and network congestion.

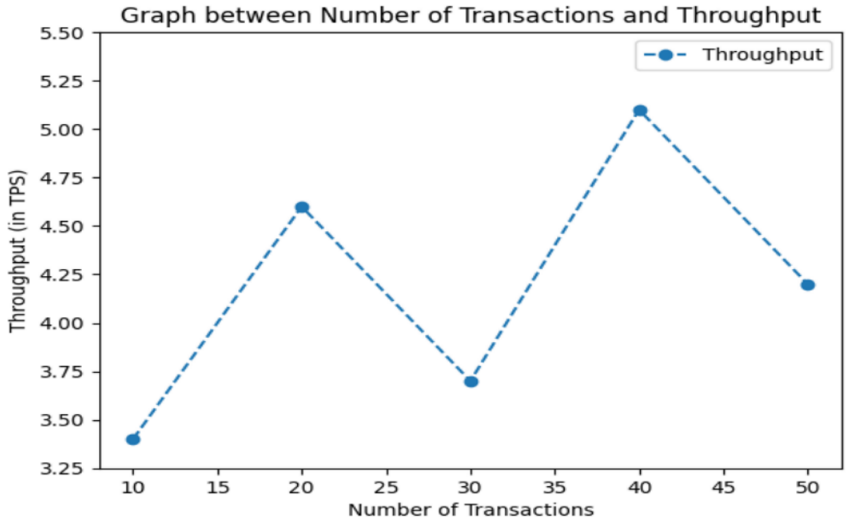

Figure 11. No. of Transactions vs. Throughput.

Comparison with the previous works with the proposed system is depicted in Table 9. It contains the following features: crypto services, is it BCT-based or not, smart contract, is cloud-based.

Table 9. Comparison Analysis with related systems.

Authors	Crypto Services	BCT Based	Smart Contract	Cloud Based
[32]	Authentication Confidentiality	Yes	Yes	Yes
[33]	Authentication Integrity	Yes	No	No
[35]	Authentication	No	Yes	Yes
[36]	Authentication Integrity	No	No	No
[37]	Authentication	Yes	Yes	No
Proposed System	Confidentiality Integrity Authentication	Yes	Yes	Yes

7. Conclusions

Blockchain technology provides a distributed ledger system where certificate records are stored in a decentralized manner, eliminating the need for a central authority to verify and authenticate them. The proposed system resists attacks by encrypting the data before transmitting it into the blockchain, ensuring the security of the data, because any modifications to the certificate data would require consensus from numerous nodes in the blockchain network. This decentralization makes fraudulent operations such as certificate forging or tampering extremely difficult. Furthermore, encryption is critical for maintaining the confidentiality of certificate information. By encrypting the certificate data, only authorized persons with the right decryption keys may access and validate the information, preventing it from being disclosed or manipulated without authorization.

Furthermore, the use of blockchain and encryption enables seamless verification of academic certificates. Through a decentralized network, employers, educational institutions, and other relevant parties can easily validate the authenticity of certificates without relying on time-consuming manual processes or contacting the issuing institution directly. This streamlined verification process saves time and resources while enhancing trust and confidence in the credentials.

Author Contributions: Conceptualization, S.A.S. and C.R.; Methodology, S.A.S.; Software, C.R. and R.P.M.; Formal analysis, C.R.; Resources, T.R.G.; Data curation, R.P.M.; Writing—original draft, S.A.S. and R.P.M.; Writing—review and editing, T.R.G.; Visualization, R. P. M. and T.R.G.; Supervision, T.R.G.; Funding acquisition, T.R.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1917–1927. [CrossRef] [PubMed]
2. Qu, J. Blockchain in medical informatics. *J. Ind. Inf. Integr.* **2022**, *29*, 100258. [CrossRef]
3. Liang, W.; Zhang, D.; Lei, X.; Tang, M.; Li, K.C.; Zomaya, A.Y. Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1410–1420. [CrossRef]
4. El Azzaoui, A.; Chen, H.; Kim, S.H.; Pan, Y.; Park, J.H. Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preserving in Medical Supply Chain Systems. *Sensors* **2022**, *22*, 1371. [CrossRef] [PubMed]
5. Gao, J.; Yu, H.; Zhu, X.; Li, X. Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption. *IEEE Syst. J.* **2021**, *15*, 5233–5244. [CrossRef]
6. Butt, G.Q.; Sayed, T.A.; Riaz, R.; Rizvi, S.S.; Paul, A. Secure Healthcare Record Sharing Mechanism with Blockchain. *Appl. Sci.* **2022**, *12*, 2307. [CrossRef]
7. Liu, J.; Jiang, W.; Sun, R.; Bashir, A.K.; Alshehri, M.D.; Hua, Q.; Yu, K. Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 2231–2242. [CrossRef]

8. Zhang, S.; Liu, Y.; Han, Z.; Yang, Z. A Lightweight Authentication Protocol for UAVs Based on ECC Scheme. *Drones* **2023**, *7*, 315. [CrossRef]
9. Nagasree, Y.; Rupa, C.; Akshitha, P.; Srivastava, G.; Gadekallu, T.R.; Lakshmanna, K. Preserving Privacy of Classified Authentic Satellite Lane Imagery Using Proxy Re-Encryption and UAV Technologies. *Drones* **2023**, *7*, 53. [CrossRef]
10. Du, R.; Ma, C.; Li, M. Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains. *Tsinghua Sci. Technol.* **2023**, *28*, 13–26. [CrossRef]
11. Sun, Z.; Han, D.; Li, D.; Wang, X.; Chang, C.C.; Wu, Z. A blockchain-based secure storage scheme for medical information. *J. Wirel. Commun. Netw.* **2022**, *2022*, 40. [CrossRef]
12. Wang, M.; Guo, Y.; Zhang, C.; Wang, C.; Huang, H.; Jia, X. MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain. *IEEE Trans. Serv. Comput.* **2023**, *16*, 438–451. [CrossRef]
13. Kumar, R.; Kumar, J.; Khan, A.A.; Ali, H.; Bernard, C.M.; Khan, R.U.; Zeng, S. Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images. *Comput. Med Imaging Graph.* **2022**, *102*, 102139. [CrossRef] [PubMed]
14. Rahman, M.M.; Tonmoy, M.T.K.; Shihab, S.R.; Farhana, R. Blockchain-Based Certificate Authentication System with Enabling Correction. *J. Comput. Commun.* **2023**, *11*, 73–82. [CrossRef]
15. Ali, S.I.M.; Farouk, H.; Sharaf, H. A blockchain-based models for student information systems. *Egypt. Inform. J.* **2022**, *23*, 187–196. [CrossRef]
16. Ullah, Z.; Raza, B.; Shah, H.; Khan, S.; Waheed, A. Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment. *IEEE Access* **2022**, *10*, 36978–36994. [CrossRef]
17. Agyekum, K.O.B.O.; Xia, Q.; Sifah, E.B.; Cobblah, C.N.A.; Xia, H.; Gao, J. A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. *IEEE Syst. J.* **2022**, *16*, 1685–1696. [CrossRef]
18. Hao, X.; Ren, W.; Fei, Y.; Zhu, T.; Choo, K.K.R. A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things. *IEEE Trans. Serv. Comput.* **2023**, *16*, 773–786. [CrossRef]
19. Mubashar, A.; Asghar, K.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Wang, D.; Shabbir, M. Storage and proximity management for centralized personal health records using an ipfs-based optimization algorithm. *J. Circuits Syst. Comput.* **2022**, *31*, 2250010. [CrossRef]
20. Rupa, C.; Chakkarvarthy, D.M. Web-Based Knowledge Management Distributed Application for Medical Certificates Using Blockchain Technology. In *Knowledge Management and Web 3.0: Next Generation Business Models*; Walter de Gruyter GmbH & Co KG: Berlin, Germany, 2021; pp. 141–162.
21. Gadekallu, T.R.; Manoj, M.K.; Kumar, N.; Hakak, S.; Bhattacharya, S. Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications. *IEEE Internet Things Mag.* **2021**, *4*, 30–33. [CrossRef]
22. Xu, G.; Qi, C.; Dong, W.; Gong, L.; Liu, S.; Chen, S.; Liu, J.; Zheng, X. A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 698–709. [CrossRef]
23. Sirajuddin, M.; Rupa, C.; Bhatia, S.; Thakur, R.N.; Mashat, A. Hybrid Cryptographic Scheme for Secure Communication in Mobile Ad Hoc Network-Based E-Healthcare System. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9134036. [CrossRef]
24. Lutfiani, N.; Apriani, D.; Nabila, E.A.; Juniar, H.L. Academic Certificate Fraud Detection System Framework Using Blockchain Technology. *Blockchain Front. Technol.* **2022**, *2*, 55–64. [CrossRef]
25. Selvi, C.; Victor, N.; Chengoden, R.; Bhattacharya, S.; Maddikunta, P.K.R.; Lee, D.; Piran, M.J.; Khare, N.; Yendri, G.; Gadekallu, T.R.; et al. A Comprehensive Analysis of Blockchain Applications for Securing Computer Vision Systems. *arXiv* **2023**, arXiv:2307.06659.
26. Rupa, C.; Greeshmanth; Shah, M.A. Novel secure data protection scheme using Martino homomorphic encryption. *J Cloud Comp.* **2023**, *47*, 1–12. [CrossRef]
27. Rupa, C.; MidhunChakkarvarthy, D.; Patan, R.; Prakash, A.B.; Pradeep, G.G. Knowledge engineering–based DApp using blockchain technology for protract medical certificates privacy. *IET Commun.* **2022**, *16*, 1853–1864. [CrossRef]
28. Bhattacharya, S.; Victor, N.; Chengoden, R.; Ramalingam, M.; Selvi, G.C.; Maddikunta, P.K.R.; Donta, P.K.; Dustdar, S.; Jhaveri, R.H.; Gadekallu, T.R. Blockchain for internet of underwater things: State-of-the-art, applications, challenges, and future directions. *Sustainability* **2022**, *14*, 15659. [CrossRef]
29. Chaganti, R.; Varadarajan, V.; Gorantla, V.S.; Gadekallu, T.R.; Ravi, V. Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture. *Future Internet* **2022**, *14*, 250. [CrossRef]
30. Zhang, L.; Zhang, T.; Wu, Q.; Mu, Y.; Rezaeibagha, F. Secure Decentralized Attribute-Based Sharing of Personal Health Records with Blockchain. *IEEE Internet Things J.* **2022**, *9*, 12482–12496. [CrossRef]
31. Jangirala, S.; Das, A.K.; Vasilakos, A.V. Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7081–7093. [CrossRef]
32. Niu, S.; Chen, L.; Wang, J.; Yu, F. Electronic Health Record Sharing Scheme with Searchable Attribute-Based Encryption on Blockchain. *IEEE Access* **2020**, *8*, 7195–7204. [CrossRef]
33. Jia, X.; Luo, M.; Wang, H.; Shen, J.; He, D. A Blockchain-Assisted Privacy-Aware Authentication Scheme for Internet of Medical Things. *IEEE Internet Things J.* **2022**, *9*, 21838–21850. [CrossRef]
34. Ch, R.; Kumari, D.J.; Gadekallu, T.R.; Iwendi, C. Distributed-Ledger-Based Blockchain Technology for Reliable Electronic Voting System with Statistical Analysis. *Electronics* **2022**, *22*, 3308. [CrossRef]

35. Ghazal, T.M.; Hasan, M.K.; Abdullah, S.N.H.S.; Bakar, K.A.A.; Al Hamadi, H. Private blockchain-based encryption framework using computational intelligence approach. *Egypt. Inform. J.* **2022**, *23*, 69–75. [CrossRef]
36. Sultana, S.A.; Ch, R.; Malleswari, R.P. Keyless Lightweight Encipher using Homomorphic and Binomial Coefficients for Smart Computing Applications. In Proceedings of the International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), Vellore, India, 5–6 May 2023; pp. 1–6. [CrossRef]
37. Kiania, K.; Jameii, S.M.; Rahmani, A.M. Blockchain-based privacy and security preserving in electronic health: A systematic review. *Multimed. Tools Appl.* **2023**, *82*, 28493–28519. [CrossRef]