ECTI Transactions on Computer and Information Technology
Journal homepage: https://ph01.tci-thaijo.org/index.php/ecticit/
Published by the ECTI Association, Thailand, ISSN: 2286-9131

Security-Aware and Privacy-Preserving Blockchain Chameleon Hash Functions for Education System

P. Sheela Rani[1] and S. Baghavathi Priya[2]

ABSTRACT

The most crucial properties of decentralized, immutable blockchain technologies are being transparent, tamper-proof, and have total traceability. With an increase in overseas students globally, the problem of diploma forgery, and the sale of forged credentials, the management and dissemination of student educational information continue to encounter several problems. Privacy violation issues like security, privacy, trustworthiness, consistency challenges, and traceability issues are considered when managing student academic records in educational sectors. The proposed work is a novel decentralized Chameleon Hash Function and it is applied to overcome these privacy violation issues. Security-aware and privacy-preserving blockchain Chameleon hash functions for Education System are suggested because every redaction needs to be approved by numerous blockchain nodes. A Proof of Continuous Work (PoCW) consensus algorithm entirely based on Blockchain is proposed for data storage and sharing, which minimizes processing power wastage to enhance the accessibility and transparency of the procedure for students receiving educational degree certificates. By consistently giving proof of storage, miners can gain an edge in the mining procedure. Without any outside help, Blockchain has created a reliable blockchain-based storage system that does not depend on a third party. The simulation and theoretical study's findings demonstrate that the proposed scheme has enhanced security, trustworthiness, and traceability.

Article information:

Keywords: Chameleon Hash Function, Blockchain, PoCW, Security, Trustworthy, Traceability

Article history:
Received: March 18, 2023
Revised: April 1, 2022
Accepted: May 20, 2023
Published: June 3, 2023
(Online)

DOI: 10.37936/ecti-cit.2023172.252014

1. INTRODUCTION

Educational credentials are required by college students, colleges, and businesses. Hard copies of certificates are tampered with and give rise to many fraudulent measures. Hard copies of certificates have been essential in the education sector in recent times. A student's ability to pursue higher education and find a job depends on their holding the appropriate educational credentials. These certifications have been recognized and are currently developed into commercial applications for colleges, students, universities, educational institutions, and organizations. The fact that these certificates have the basic quality that enables records to replicate the original historical circumstances makes them particularly significant for students, universities, educational institutions, and organizations. Widely considered a good thing, the advent of information technology has led to the digitization of educational records. Digital records can be modified more easily during the storage, transmission, and sharing processes because they are held on a storage medium with a high degree of variability. This appears to be a widespread issue, similar to the sale of fake certificates, fake diplomas, and degree production facilities [5]. However, it is not advisable to store all information in built-in record storage since this traditional storage method is susceptible to the leakage of private information and illegal alteration [1],[12],[13],[20],[23].

Prior research has been carried out less in number in support of secured storage and conditional exchange of private data, such as student educational records. Additionally, universities or educational institutions need to grant permission to outside groups to access student data [19]. A new strategy is re-

[1] The author is with Panimalar Engineering College, Anna University, Chennai, India, E-mail: rpheelaranipit@gmail.com
[2] The author is with Rajalakshmi Engineering College, Chennai, India, E-mail: baghavathipriya.s@rajalakshmi.edu.in

quired by companies that need a faster way to verify the legitimacy of student diplomas from domestic and international institutions. The purpose of this research is to utilize blockchain technology to create Security-aware and privacy-aware systems using the Chameleon Hash functions in Educational Institutions.

This approach deals with the issue of authenticity of a degree, or certification in an employment-intensive, operation. Students who wish to apply for studies abroad may require to submit language translations and international authentications or legalizations as proof of the validity of their original documents. This challenging issue can be resolved using this technique. The legitimacy and provenance of certificates and degrees have been progressively ensured throughout the past two decades. There are no difficulties with awarding a degree from an institution, which is essential for educational credentials and employment opportunities [19].

1.1 Privacy violation issues

Data integrity, authentication and access control, and privacy concerns are considered while transferring data. Among objects that allow manufacturing, transportation, and business to serve users more effectively in everyday activities data integrity and authentication are very important. A practical and equitable data trade system is required because these data are not usually accessible. Unauthorized use of the facilities and leakage of confidential data is a further security issue. A centralized organization that provides a suitable key according to its access regulations provides the basis for conventional authentication and allows access control for administration for a third-party entity.

Internet of Things (IoT) system gathers information using a range of sensors and smart appliances to make a thorough choice that is compatible with specific needs. Privacy can be easily broken in the intricate IoT system, nevertheless, through several processes, including data interchange, raw data processing, and information collection. Consequently, it is crucial and difficult to maintain privacy in IoT devices, such as entity and information privacy [24].

The information holder must consider serious users privacy violation issues when distributing information gathering for use outside the purview of data acquisition companies [20]. In the decade or so that ensued, several anonymization methods have been suggested to deal with these issues as they are susceptible to attacks on personal data, this model, which focuses on timing data releases, has privacy violation issues. [26],[28] LKC-Privacy methodology is used to overcome the problems using trajectory datasets although, the datasets about trajectories may cause privacy violations [27].

Numerous different elements contribute to the real risk of privacy violations. The first factor that can breach someone's privacy is the kind of information that is gathered by various entities in a network. Blockchain has a significant potential impact on social Internet of Vehicles (SIoV) privacy management. For instance, with this technology, authentication, and permission for accessing data in SIoV may be done quickly, in a safe, trustworthy, and decentralized manner, with full transparency, traceability, and availability to all participants or players throughout the existing blockchain network [25].

1.2 Privacy preservation models in Blockchain

The prototype presents a blockchain-based solution for the secure storage and accurate sharing of educational certificates and sorts out privacy issues. The system enables the sharing of credentials while fostering complete trust between certificate receivers, corresponding issuing authorities, and end users, who use smart contracts for the verification of certificates [17]. Blockchain helps in scrutinizing education credentials as a blockchain is like a perpetual ledger where entire communications are recorded in sequential order [2].

The research aims to make higher education certificates more accessible and visible, thereby enhancing quality [14]. This process eliminates fraudulent activities and prevents scams that were carried out in the decentralized process [3]. The institution or university uploads student profile data, including academic results, extracurricular activities, diplomas, and other transcripts at the end of the course, and then a blockchain is created from this data. Throughout the recruitment process, the recruiters rely on the data kept in the blockchain, thereby eliminating the chance of candidates supplying fake documents. The development of Blockchain and smart contracts with immutable, decentralized, secure, traceable, and consensus functions is an excellent addition of establishing a robust anti-fraud solution for digital certificates. Sets of information with breaches of privacy are examined to find a combination that can be utilized to provide specific information to individuals.[26]. A privacy preservation model addresses the LKC-Privacy system's revealed vulnerability. The model has been more effective and highly secure than LKC-Privacy [27].

The Proof of Continuous Work Algorithm and a Decentralized Chameleon Hash Function algorithm are considered for privacy preservation models in this proposed system. The theoretical research demonstrates that the proposed scheme is more reliable and secure when compared to the authorized allocation process. Considering the findings, this system also looks at real-world node failure scenarios and makes it beneficial for other parameter recommendations.

This research has the following contributions.

- The proposed system has developed a Proof-of-Continuous-Work (PoCW) method to store the data of miners. Miners accumulate mining benefits by consistently storing information and providing evidence.
- To address the issue of the trusted party, the proposed system suggests a Decentralized Chameleon Hash Function that ensures that the key is produced by numerous blockchain nodes cooperatively and without the aid of a third party. The scheme substantially expands the decentralized Chameleon Hash Function to enable proactive maintenance and threshold redacting while taking node dynamics into account.
- The architecture is an entirely new design that creates a redaction chain by connecting the redaction history of one block to address traceability issues. The majority of current blockchain systems can employ this structure for security and traceability issues.
- The system evaluates the redactable Blockchain and compares it with a different decentralized system. The test results indicate that redactable Blockchain is effective in real-world usage.

This work describes the recent research on the application of Blockchain in educational institutions like universities, colleges, etc., and describes the experimental results of authenticating an academic degree system. The rest of this paper covers the related research conducted in the blockchain field. The methodology section discusses the method used in the recommended system.

2. RELATED WORKS

In this trending world, Blockchain has become one of the most reliable systems for storing information in this era. Blockchain application in specific fields is incredible among many domains. Blockchain technology is widely researched in recent years. Researchers are interested in exploring new applications using blockchain technology. Distributed ledgers and enhanced security are some of the areas of interest in this research.

Liangming et al. [8] proposed a system by looking at the key features of blockchain technology and based on all the features, they created a model. The consensus algorithm determines and filters the node to practice accounting power to determine whether the output should be validated before it gets written into the ledger. This helps prevent the production of low-quality data but this idea failed as it could not access the other system files.

Jungi et al. [4] introduced a model to help students avoid document forgery during the hiring process and make it easier to assess a candidate for employers. The model tried to make the process simple by using Ethereum, which gives shape to the prototype. The advantage of this system is that it is made in a real-world environment. The major drawback was that the meta-analysis did not verify the standard issues.

Murat Yasin Kubilay et al. [9] proposed a new architecture called PKI. This architecture is intended to remove split attacks and provide certificate transparency. On a private Ethereum, a prototype was created by smart contract through experimental results. Compared to other protocols, this new architecture produced maximum performance. Yet this mechanism, which runs without human intervention, has a significant flaw. Muhammed Turkanovi et al. [10] proposed the concept of a credit platform for higher education that is based on a global blockchain and submitted an open-source platform as proof. This is helpful for students and faculty members, as they can easily trace their course records and prevent fraud. This concept is also implemented among stakeholders and not only in education and when they attempted to continue their work in a real-world setting, the process failed.

[21] Jia, M. et al. suggested incorporating the Chameleon Hash function into redactable blockchains to address the problems with consistency and traceability. This technique enables data stored on a decentralized system to be more trustworthy, accessible, and transparent. Results show that realistic use offers effective redaction and blocks consistency checks.

[22] Yin, H. et al. proposed the POCW method and hash ring-based algorithms for efficient information management and preservation in the storage device. The drawback noted in this system is that expanding evidence-based research was necessary and ongoing efforts were needed to preserve credible data.

Rui Xie et al. [15] described storing the certificate information and preserving the documents and electronic certificates safely. It is a decentralized certificate system that provided standard certificates to college students while conducting events. The technique used here is simple: smart contracts. The added advantage of the technique was that the total information of the user could be retrieved with the click of a button without having to pester the students for their information again and again. Its major flaw was that it would collapse if any user information was missed and was not secured. Muhammad Aamir et al. [11] provided a solution to verify and validate academic records using blockchain technology. They did this through digital ledgers, which is one of the features of blockchain technology. The significant merit of this framework is that it provides high security for the data. The method used here is Hyper-Ledger Fabric. In this case, the advantage becomes a flaw as the students' academic details should be more secure and needed more security.

A secure authentication protocol for private data on blockchain technology was made and pioneered work without third-party verification was carried out. They created this using proof of work (POW) and proof of stake (POS). PBFT stands for Practical Byzantine Fault Tolerance. The secret key is used in the model, which also curbs fraud. However, due to the extensive network infrastructure and increased activities, this task has failed. Shi Xiong Yao et al. [16] presented a model of public key infrastructure that prevents real-world attacks. A public key is used in digital diplomas to authenticate the web server's identity.

Jerinas Gresch (B) et.al. [6] designed the DCBF, which is used for recording the entire data revocation in the up-to-date block. For efficiency, dual-count bloom filters were designed. DCBF is used for recording the entire data revocation in the up-to-date block. But the significant defect here is that they could store only minimal information.

Jerinas Gresch et.al. [7] proposed a system that was called as UZHBC that is based on blockchain technology and is mainly used for student diplomas and serves as an authorized testimony of education. It is used to certify an individual's degree of education and skills. Frauds could be reduced using this model because digital proofs were more secure than manual ones. Enterprises were still having problems finding efficient professionals to fill the jobs. It was difficult to quantify how many people throughout the world "possess" forged credentials.

Yuqin Xu et.al. [18] proposed the Blockchain Educational Certificate (ECBC). This work was done by a consensus algorithm, such as Dynamic Quorums, Merkle Trees, and Ethereum. The major disadvantage of this work was using more computer resources.

3. PROPOSED SYSTEM

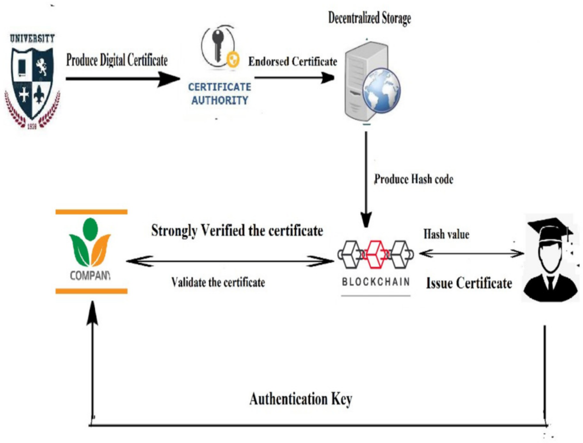


Fig.1: Architecture of the proposed system.

The decentralized scheme of digitalization of certificates is shown in Figure 1 based on blockchain solutions. The credits and marks obtained by a student will be fed into the system for each semester or each year. The critical evidence of the credentials is saved, and the diploma's data is categorized into issuer information, receiver material, and certificate information. The data from the academic institutes or universities aid in deciding these modules. The administrator then verifies the endorsed certificates and after verification, the data related to the certificates is sent to IPFS (the Planetary File System) for storage. IPFS is an InterPlanetary system that stores and shares certificates in a decentralized manner. The certification authority verifies the endorsed certificate and sends it to the administrator for final verification. The admin sends the certificates and relevant information which are stored in IPFS after verification. The records keep information about the delivering consultant, the key pair applied by the consultant, and the key pair used by the administrator who added the authority's report. IPFS sends only the hash value of the certificate to the blockchain storage.

When the student has finished his degree course, a prototype will issue the digital certificate to the student. At the time of convocation, the student will receive a degree certificate and a unique identifier like the registration number and hash value of their academic credentials. In case students lose or damage their certificates, they can collect the certificates by using their unique identifier. The number has either their registered number, date of birth, or hash value.

This system will reduce the workload of the administrator in issuing and maintaining the certificates. An organization needs to verify the student's certificate, which means it can use the identifier for verifying the transcripts from the Blockchain because academic data is stored on an immutable blockchain. When a company needs to authenticate a student's certificate, it can use the identification to verify the blockchain transcripts as academic records are immutable since they are on the Blockchain.

4. IMPLEMENTATION

This system has explored a consensus along with the appropriate incentive system for storage allocation. The trusted party problem, the traceability issue, and the block consistency issues have been resolved using a decentralized chameleon hash function. To evaluate this proposal, this scheme is implemented with the Python language and the consensus algorithm proof of continuous work.

4.1 Proof Of Continuous Work Algorithm (POCW)

The proposed system employs PoCW to offer a trustworthy decentralized storage service while also reducing the waste of computational power.

Since the first proof transaction contains a reference to the prior proof transaction that belonged to the same miner, it is a registered action. This could be used to resolve the next two problems. The transaction first makes a specific block reference, pointing to a predetermined state. The state can be used to manage data distribution by miners. Additionally, while processing the transactions, the block hash and transaction indices were both inconsistent. Miners should hold off on creating their subsequent transaction until the previous one has been added to the Blockchain. It successfully stops miners from producing a series of proofs in advance so that they can discard or outsource the data.

NOTATION USED IN PoCW

π	-	proof of storage
R	-	Random challenge
P_k,S_k	-	Public key and secret key
Idx	-	index
bid	-	Block hash id
cr	-	counter
nm	-	number
Ha	-	Cryptographic hash function
Ti	=	Transaction in this block
Z	-	Target value
BI	-	ith Block

$$tx_{proof} := (bid, idx, pk, R, \pi) \tag{1}$$

Each block has a hash bid, and the transaction list index IDX is used to retrieve the prior transaction. It has limited communications. So the hash value for this one should be lower than the target value of V by using the PoCW algorithm. Therefore, miners must try to complete a variety of arbitrary tasks.

Based on the observation that more reliable miners have longer transaction chains and more extensive storage. To alter the mining complexity, this system considers the following two factors. To gauge the miner's workload, first, let CTR stand for the duration of the Proof transaction chain. The second option, nm, specifies the amount of allocated data. To protect the miners who do not provide space, the suggested scheme reserves the PoCW basic difficulty for them.

The formula for calculating mining difficulty is as follows:

$$H(BI)<(ct * nm + 1) * Z \tag{2}$$

Proof of Continuous Work Algorithm (POCW)

```
Function invocation ()

Generate a pair of keys (Pk,Sk) as a codename

Make a counter for the subsequent evidence counter = 0

Put a value of number = 0 as that of the quantities of information.

Add a pointer to ptr = null in the final validation operation.

Functional mining ()

for real to do

Find the final block and synchronize the longest chain Bl.

Gather events ets from the memory cache.

Pack a new block using a random number nonce.

(ets||H(Bl)||nonce) = Bl+1

If Ha(Bl+1) < (cr* nm + 1) * O then

Share this new block with the network

If this block was approved by the Blockchain,

set the counter to 0 to clear it

Computational proof ()

Network transmission trevince = (Pk)

Allow for such an event to be added to the Blockchain
Make the final evidence communication ptr= Ha.(trevince)

for correct do

Access the block's hash blno then the total communication index indx as as of Blockchain.

Examine the information collection I with miner group M

Apply L = allocate (pk, I, M) for allocated data

If true, do.

Choose a challenge number at random. Ra

To calculate a proof, go $\pi$ = Verify (SK, Ra, L).

Create trevince = (blno, indx, Pk, Ra),

broadcast it and shatter it if H(trevince) < Ve

watch for this event to be added on the blockchain.

Add the final confirmation event to ptr = H(trevince)
```

Key function ()

Initialize the nodes by calling invocation ().

Establish the primary thread for mining ()

Make a thread to carry out proof () behind the scenes.

In Algorithm 1, the pseudocode for PoCW is displayed. The mining functions are used by miners who do not provide storage in a manner like that of PoW. However, the computation proof function of the demonstrating procedure establishes an alternative duty for them.

If Ha(Bl+1) < (cr * nm + 1) * O then

The mining complexity in this line in the above algorithm is impacted by the parameter of the counter cr and the number nm, which are changed when miners construct a thread to submit evidence continually. To ensure that the oldest miner is always in charge of the Blockchain and prevent an unchecked increase in the cumulative cr.

set the counter to 0 to clear it

In the above algorithm, they add a rule that states that whenever a miner creates a new block on the Blockchain, the counter will be cleared and recalculated.

4.2 Decentralized chameleon hash function:

The decentralized Chameleon Hash Function saves all the original data and certificates relevant information about the students for traceability when redacting rather than changing the actual transactions or the associated blocks. To be more precise, a replica of a block is created for transcription, in which edited transactions are substituted for the original ones. The original block and the truncated block are then stacked on top of each other in the blockchain to create a redaction chain. The traceability property is made possible by extending each redaction chain with a copy of the most recent redacted block.

The field's previous hash (ph) in subsequent blocks need not be masked because headers should contain the same hash code as the initial one. To accomplish this, simply switch the code that creates the previous hash from the conventional hash, such as SHA-256, to the decentralized chameleon hash. Consequently, a block in the redactable Blockchain simultaneously points to the block before it and all its redactions. This proposed system design has a new structure for organizing blocks that contain redactable transactions, which also changes the fields in the block header.

***Table 1:** Notation Used in a chameleon hash function.*

SLNO	Notations	EXPLANATION
1	DCH	decentralized chameleon hash functions
2	Dsn	Digital Signature
3	KG	Key Generation
4	**r**	Randomness
5	**P**	Participants
6	(P_1 to P_n) n	number of participants
7	SHh	Special Hash
8	Puk, Prk	Public Key, Private Key

$$\text{DCH} = (\text{GenKey, Hash, Rehash, Adapt, Verify}) \quad (3)$$

The blockchain nodes generate the system's cryptographic keys and initialize the RSA buffer. As with conventional blockchain applications, peers establish public and -private key pairs when signing and validating the transactions. To disclose the blocks, the entire nodes cooperatively build a public and private team of chameleon hash functions.

Algorithm for generating block

```
createchamke(b, tx, cs, and c)
headerl, rl, al obtainHR(B)
ph ← DCH.RH (cs, (headerl − rl , rl ))
    if DH (g, gs , rl ) then
        for item in tx do
            if RTTx(itm) then
                lhl ← obtainSHh(itm)
a1 ← a. insert (a1, lh1 )
end if
        end for
      a ← al
      mr ← MH (tx )
      : ex ← zp*
      r ← (ce , cse )
header ← con (ph, ⊥, mr , a, r )
        return (header, tx )
    end if
    return ⊥
end procedure
```

Following the creation of a chameleon hash key by peers in algorithm 2, nodes may join or leave the blockchain network. A malicious party that wants to recover the private key can steal more than n shares over time from the blockchain network. Therefore, the full nodes need to proactive the claims regularly.

Digital sign key generation = The blockchain node P uses DS.KG (1); to create a set of cryptographic functions (pukDS, prkDS). The blockchain node then releases the public key (puk DS) while maintaining the secret of the private key (prk DS).

Chameleon hash key generation:
The chameleon hash key generation entails three categories. If there are n ordered complete nodes, indicated as P1,. . ., Pn.

To share a secret key, the first n complete nodes first run the decentralized chameleon hash function's key distribution process.

The network nodes then change the criteria to

$$2n - 1\ (2n - 1 > (n- 1)+(n - 1)) \qquad (4)$$

For sharing updates, take into consideration that a challenger may compromise n - 1 nearly a full node separately before and during the share update phase.

Security analysis:
The proposed system maintains the same level of security even when there are no miners contributing storage space. However, miners get mining rewards by gathering storage commitment data, which is reset after a miner utilizes it to extract a new block. The proposed consensus is mostly secure for the current blockchain network.

5. RESULTS AND DISCUSSION

This proposed system is executed using a desktop computer running Windows 10 with an AMD processor and 8 GB of RAM to implement the simulation. In this system, set the total number of miners in the simulation to 1000 and the actual data saved to 5000.

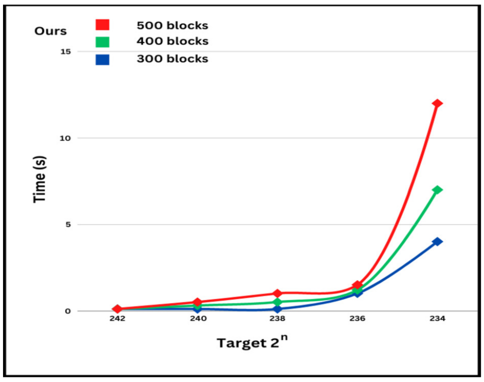


Fig.2: *Time (Seconds) of Proof-of-Continuous Work consensus with various targets 2^n and different sizes of blocks using our method and the decentralized chameleon hash function.*

The Time of Proof-of-Work consensus with various targets and numbers of blocks using our method and the decentralized chameleon hash function is depicted in Figure 2. The time required to calculate the nonce grows as the total number of blocks and the targets reduce. As a result of the PoCW in the proposed system being predominantly exponentiation operations, which takes less time to perform the identical tasks as [21].

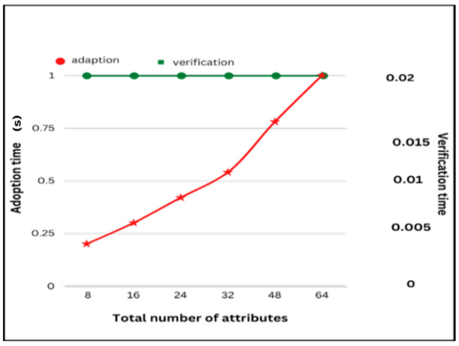
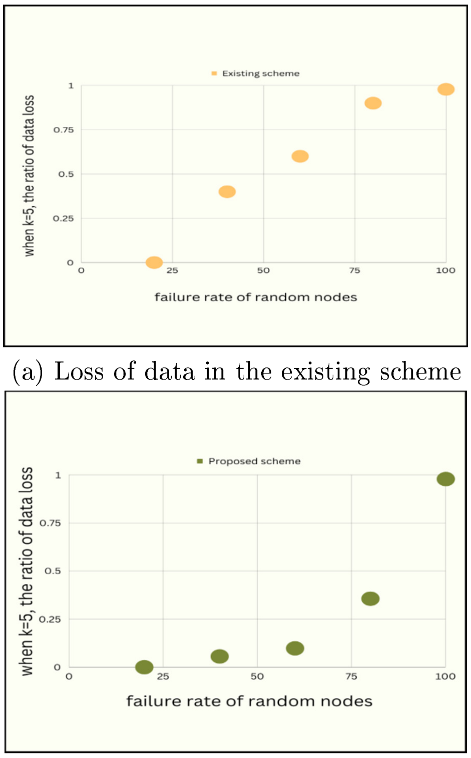


Fig.3: *Various thresholds are used to determine the duration of an adaptation and to validate its adaptability.*

The effect of the threshold on the adaptation time and the combination is shown in Figure 3, with the transformation taking the longest time due to the extensive calculation of the Lagrangian coefficients.

Additionally, when the threshold rises, the time it takes to verify a block stays constant, demonstrating that the entries have no impact on how well redaction occurs on-chain.

The blockchain nodes in our solution store two different sorts of proofs locally. In contrast to unredacted blocks, which do not require membership verifiable evidence, redacted blocks demand membership evidence.



(a) Loss of data in the existing scheme

(b) Loss of data in the proposed scheme

Fig.4: *Assessment of system reliability.*

Hash ring-based data distribution is compared with the existing system in Figure 4 (a) to the distributor database and in Figure 4(b), the selected outcomes are represented where the quantity of data backup k = 5. Any unexpected failure is handled better by the developed framework. To improve reliability, users can also increase the volume of information recovery. Nevertheless, a high level of k reduces the system's total storage capacity while simultaneously increasing the storage cost for data owners. The system must choose a suitable variable in a real-world scenario to balance risk and expense.

Discussion

The proposed platform helps better school establishments for their college students and offers the opportunity for fraud detection and prevention. As a result, the need for a more complicated checking method for a student's instructional statistics may be eliminated. Additionally, the students are given the opportunity of transparency and a top-level view of their instructional duties within the scope of their observation programs. A scholar can immediately test their finished route statistics. An apparent benefit for all the concerned stakeholders is the opportunity for an audit trail. In this way, fraud could be prevented.

Reliability: This framework offers entire certificates and facts, avoiding meaningless hash values, while the company has need not to verify the credentials further.

Authority separation. The system provides the authority processes for the administrator, department head, issuer, and receiver.

Persistent Storage and Speed: All academically pertinent information will be kept in IPFS even though this system uses it. Blocks of data and all continuous data in IPFS are aspects of sustainability. The IPFS maintains permanent data that cannot be manipulated. The SHA 256 algorithm employed in this method increases the speed of record access.

A maximum of 1500 queries can be made of the Application Programming Interface (API) API by this system per second to retrieve IPFS data. The proposed method has achieved a speed of approximately 17% faster than traditional blockchain systems. Original designs are slower than the present scheme since they are not decentralized, and lack the use of IPFS.

High Security

The proposed POCW algorithm maintains the same level of security even if no miner offers local data storage. To obtain mining rewards, miners use the stored contribution value, which is reset each time it is used and gets a new block. This framework has investigated the factors affecting system reliability and looked for relationships between them. To check the system's condition, miners move backward over the Blockchain to look at any prospective transactions. Therefore, while confirming every new block they receive, miners should temporarily store the data. To diminish storage resources and prevent the miner from processing new blocks, security breaches employ the problem of flooding a miner's storage with fake blocks. This method, fortunately, only records the most recent blocks.

Since IPFS is a decentralized data storage system, no individual or group has gained control over the data. This approach is safer than typical conventional centralized file storage systems. Data hashing and encryption are just two of the protective techniques that IPFS uses to safeguard files.

By incorporating IPFS for storage, POCW approaches for authentically identifying people, and a decentralized chameleon hash algorithm to solve violation of privacy problems with security, privacy, reliability, consistency, and traceability. Most remarkable protection is achieved by using this system. This system maintains privacy, decentralization, and fault tolerance.

6. CONCLUSIONS

In real-world applications, smart contracts are entirely used for keeping and managing diplomas deprived of trusting several external systems, which are decentralized and relish excellent reliability. The details of the diploma recipient have not been completely preserved, which means removing the user's discretion based on making sure of the trustworthiness of credentials details. The protocol for this scheme is so flexible and self-governing of diploma control because this slight amendment allows acquiring generalized record storage. PoCW not only provides a dependable decentralized storage solution but also reduces the wastage of computing power. The current research confirms that this technique could be utilized to prevent forgeries and manipulations of certificates. The Simulation research supports the theoretical analysis, which demonstrates the proposed method achieves higher consistency and traceability issues by applying the Chameleon Hash Functions and POCW algorithm.

References

[1] B. Liu, L. Xiao, J. Long, M. Tang and O. Hosam, "Secure Digital Certificate-Based Data Access Control Scheme in Blockchain," in *IEEE Access*, vol. 8, pp. 91751-91760, 2020.

[2] D. Shah, D. Patel, J. Adesara, P. Hingu and M. Shah, "Integrating machine learning and Blockchain to develop a system to veto the forgeries and provide efficient results in the education-sector," *Visual Computing for Industry, Biomedicine, and Art*, vol. 4, no. 18, pp. 1-13, 2021.

[3] H. Li and D. Han, "EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme," in *IEEE Access*, vol. 7, pp. 179273-179289, 2019.

[4] D. Lizcano, J. A. Lara, B. White and S. Aljawarneh, "Blockchain-based approach to create a model of trust in open and ubiquitous higher education," *Journal of Computing in Higher Education*, vol. 32, pp. 109-134, 2020.

[5] J. Guo, C. Li, G. Zhang, Y. Sun and R. Bie, "Blockchain-enabled digital rights management for multimedia resources of online education," *Multimedia Tools and Applications*, vol. 79, pp. 9735-9755, 2020.

[6] J. Gresch(B), B. Rodrigues, E. Scheid, S. S. Kanhere and B. Stiller, "Post digital Prospects for Blockchain-Disrupted Higher Education: Beyond the Theater," *Memes and Marketing Hype*, Springer Nature Switzerland AG , pp. 185–196, 2019.

[7] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere and B. Stiller, "The proposal of a blockchain-based architecture for transparent certificate handling," *Business Information Systems Workshops*, vol. 339, pp. 185-196, 2019.

[8] L. Wen, L. Zhang and J. Li, "Application of blockchain technology in data management: advantages and solutions," *Big Scientific Data Management. BigSDM 2018. Lecture Notes in Computer Science*, vol. 11473, pp. 239-254, 2019.

[9] M. Y. Kubilay, M. S. Kiraz and H. A. Mantar, "CertLedger: A New PKI Model with Certificate Transparency Based on Blockchain," *Computers & Security*, vol. 85, pp. 333-352, 2019.

[10] M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," in *IEEE Access*, vol. 6, pp. 5112-5127, 2018.

[11] M. Aamir, R. Qureshi, F. A. Khan and M. Huzaifa, "Blockchain-based academic records verification in smart cities," *Wireless Personal Communications*, vol. 113, pp. 1397-1406, 2020.

[12] P. Ocheja, B. Flanagan, H. Ueda and H. Ogata, "Managing lifelong learning records through Blockchain," *Research and Practice in Technology Enhanced Learning*, vol. 14, no. 4, pp. 1-19, 2019.

[13] Q. Tang, "Towards Using Blockchain Technology to Prevent Diploma Fraud," in *IEEE Access*, vol. 9, pp. 168678-168688, 2021.

[14] R. Q. Castro and M. Au-Yong-Oliveira, "Blockchain and higher education diplomas," *European Journal of Investigation in Health, Psychology, and Education*, vol. 11, no. 1, pp. 154-167, 2021.

[15] R. Xie et al., "Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System," in *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 44-50, June 2020.

[16] S. Yao, J. Chen, K. He, R. Du, T. Zhu and X. Chen, "PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management," in *IEEE Access*, vol. 7, pp. 6117-6128, 2019.

[17] T. C. Dao, B. M. Nguyen and B. L. Do, "Challenges and Strategies for developing Decentralized Application based on Blockchain Technology," *Advanced Information Networking and Applications. AINA 2019. Advances in Intelligent Systems and Computing*, vol. 926, pp. 952-962, 2020.

[18] Y. Xu, S. Zhao, L. Kong, Y. Zheng, S. Zhang and Q. Li, "ECBC: A High-Performance Educational Certificate Blockchain with Efficient Query," *Theoretical Aspects of Computing – ICTAC 2017. ICTAC 2017. Lecture Notes in Computer Science*, vol. 10580, pp. 288–304, 2017.

[19] Z. Li and Z. Ma, "A blockchain-based credible and secure education experience data management scheme supporting for searchable encryption," in *China Communications*, vol. 18, no. 6, pp. 172-183, June 2021.

[20] S. Riyana, "Privacy Preservation Models for the Independent Data Release of High-Dimensional Datasets," *Research Square*, 2023.

[21] M. Jia et al., "Redactable Blockchain From Decentralized Chameleon Hash Functions," in *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2771-2783, 2022.

[22] H. Yin et al., "Proof of Continuous Work for Reliable Data Storage Over Permissionless Blockchain," in *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7866-7875, 2022.

[23] Senthilkumar, G., Tamilarasi, K., Kaviarasan, S., & Arun, M. (2022). Trusty authentication of devices using blockchain-cloud of things (B-CoT) for fulfilling commercial services. International Journal of System Assurance Engineering and Management, 1-11. [Google Scholar]

[24] Y. Yu, Y. Li, J. Tian and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," in *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12-18, December 2018.

[25] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily and Y. Jararweh, "Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions," in *IEEE Access*, vol. 7, pp. 79694-79713, 2019.

[26] S. Riyana, S. Nanthachumphu and N. Riyana, "Achieving privacy preservation constraints in missing-value datasets," *SN Computer Science*, vol. 1, no. 227, pp. 1-10, 2020.

[27] S. Riyana and N. Riyana, "A privacy preservation model for RFID data collections is highly

secure and more efficient than like-privacy," in *IAIT2021: The 12th International Conference on Advances in Information Technology*, no.15, pp. 1-11, 2021.

[28] S. Riyana, "Achieving Anatomization Constraints in Dynamic Datasets," *ECTI-CIT Transactions*, vol. 17, no. 1, pp. 27–45, Feb. 2023.

P. Sheela Rani currently working as an Associate Professor in the Department of Information Technology at Panimalar Engineering College. She received M.E degree in Dept of Computer Science & Engineering from Anna University, Trichy, India in 2011. She is currently working toward the Ph.D. degree at the dept of Computer Science and Engineering, Anna University, Chennai, India. Her research interest includes Blockchain, Network Security, Computer Networks. She has published more than 25 journals and presented more than 25 papers in National and International Level Conferences. She is a member of ISTE and IAENG for life.

S. Baghavathi Priya a Professor of Department of Computer Science and Engineering at Rajalakshmi Engineering College since 2008. She graduated B.E Computer Science & Engineering from Manonmaniam Sundranar University, M.Tech Computer Science & Engineering from Dr.M.G.R Educational and Research Institute. She received Ph.D. from Jawaharlal Nehru Technological University Hyderabad. She has guided many U.G and P.G projects. She has published over 40 peer reviewed research articles. Her research is focused on Grid Computing, Network Security, Machine learning and Big Data Analytics. She received gold medal in M.Tech degree. She was awarded a gold medal for her M.Tech degree. She won best paper awards at the ICTIS 2015 conference in Ahmedabad and the CAASR International conference in Dubai in 2017. She received Top 20 Influential Women Educators award in TamilNadu by The Academic Council of uLektz She visited several countries for presenting papers and chairing sessions. She is a life time member of CSI and IAENG.