A Blockchain System for Secure Academic Credit Transfer and Certificate Verification

Prof.Abhijeet More
Department of Computer Application, Pillai HOC Collage of Engineering and Technology Rasayani, India, 410207
abhijeetdmore242@gmail.com

Sujal Gaikwad
Department of Computer Application, Pillai HOC Collage of Engineering and Technology Rasayani, India, 410207
143sujalgaikwad@gmail.com

Rushikesh Kale
Department of Computer Application, Pillai HOC Collage of Engineering and Technology Rasayani, India, 410207
1rushikeshkale@gmail.com

Siddhesh Sarvankar
Department of Computer Application, Pillai HOC Collage of Engineering and Technology Rasayani, India, 410207
siddhusarvankar@gmail.com

Abstract: ***Education industry is taking advantage of this citywide model and exploring new ways to automate the process in order to be more efficient as well as reducing fraudulence such as document forgery, unauthorized accesses to student data, etc. Under the ambit of India's new National Education Policy (NEP) 2020, The students are directed to complete online courses from certified platforms like NPTEL, Coursera and edX – posing the need for secure verification and credit transfer for the large-scale implementation. In this paper, we present a blockchain-oriented approach to secure academic certificate verification, along with NEP-compliant credit transfer and demonstrate how decentralized storage and blockchain will manage the exchange of notarized credentials (ie: certificates) using a block chain-backed registry of their metadata on proof-of-existence services. After a student completes the course, the college uploads the certificate through a special web site and smart contracts process it as per certain predetermined rules to generate an academic credit. The students initiate the process of transferring credits through a system interface, for which the administrators approve, and once approved, are placed on this ledger to be permanently written onto the blockchain where they can not be tampered with or forged. Organizations outside the issuing entity may validate a certificate with a unique token ID or upload the file and need not discuss with an issuer. This decentralised and automated solution will enhance security, reduce the time of verification process, reduces administrative burden, bring consistency in academic record management besides giving impetus to NEP 2020 for an efficient, transparent and tamper proof teacher education academic records management and credit transfer system/to enable learners to move between institutions by facilitating all academic credits earned at same level – be portable***

Keywords: Blockchain, Credit Transfer, Certificate Verification, Smart Contract, MetaMask, IPFS

I. INTRODUCTION

Online education has now shaped how students demonstrate what they've learned, but old mechanisms cling to the past. Rather than waiting for weeks, schools could rely on quicker checks embedded into digital tools. Still, many locations continue to store physical files on premises - which means breaches can happen. When grades are faked, real achievement loses value quickly. Hiring people also frequently find fake paper fast, because the real experience writes louder stories. Fears are higher when learners accumulate school credits by studying on separate systems or schools. [16] [14]. Yet blockchain helps fill a void of trust by "chaining" records together in unchangeable chains and making decisions not through central authority. The coronavirus pandemic has helped shape how students will now show what they've learned, but the old mechanisms still cling to the past. Instead of waiting weeks on end, schools could instead employ less time-intensive checks built into digital tools. Even still,

there are many places that store physical files on site so breaches can occur. When grades are faked, genuine achievement deteriorates rapidly. People who are hired also tend to find out about phony paper fast, as the authentic experience writes louder stories. The fears are stronger when students pay for school credits they earn outside of their own systems or schools. [16] [14]. But blockchain does help fill this trust gap by "chaining" records together in unchangeable blocks and through decentralizing-decisions.

A. Motivation

The explosion of e-learning platforms and virtual education has facilitated the rapid expansion of digitised academic credentials. Unfortunately, legacy certificate verification mechanisms continue to employ centralized databases and manual verification, resulting in non-real time document validation processes being slow, cumbersome and open to the forgery of certificates or the manipulation of records. Moreover, with the implementation of India's National Education Policy (NEP) 2020 that allows flexible learning and multi-institution credit accumulation as well as portability across MOOC platforms, a secure and automated verification solution is essential. such barriers pose, and drive the need for introducing a decentralized academic credential management system to avoid fake certificate, save administrative work and facilitate credible credit transfer between institutions considering blockchain technology.

The increasing need for fast and reliable academic credential verification in employment and higher education processes also motivates this research. Traditional verification methods require manual communication between institutions, which causes delays, administrative workload, and verification errors. With students earning certificates from multiple universities and online platforms, a unified and secure verification mechanism becomes essential. Blockchain technology provides a decentralized and tamper-proof approach that enables instant and trustworthy credential validation, motivating the development of the proposed system.

B. Objective

The Primary objective of this research is to design and implement a blockchain-based academic certificate verification and credit transfer system that ensures secure, transparent and tamper proof management of academic records. The following specific objectives include:

1. To construct a decentralized storage and verification platform based on blockchain and IPFS for completion certificates.
2. In the order to realize procedures using smart Contact for automatic academic credit approval and permanent ledger recording.
3. To develop role-based portals for students, administrators and verifiers to submit, approve and verify certificates.
4. To support the rapid verification of credentials using token identifiers and file-based hash comparison functions.

II. LITERATURE REVIEW

The credential verification which based on blockchain has attracted widespread attention, for ensuring the transparency,safeness, and trust of academic records. The blockchain concept was first outlined in the Bitcoin Whitepaper [11] by Satoshi Nakamoto which suggested a decentralized peer to peer form of secure transaction system. Later, the idea of smart contracts that support rule-based automatic execution is introduced by Ethereum [12]. Also, Juan Benet presented IPFS ([13]), a decentralized content-addressed storage system suitable for secure hosting of documents.

Early studies such as J.-C. Cheng et al. [9] introduced a digital certificate system on the blockchain with contract automation, which has shown that smart contracts can be used for managing issuance and validation process. Load A. M. San, Y. M. NaingA blockchain based learning credential verification system by using Reclaimable Privacy Load This proposed idea emphasized the notion of user centered data sharing and issued focused on how much authority and choice should be given to the receiver (Issue).

Some researchers concentrate on the storage of certificate hash for tampering detection. B. Jadhav et al. [1] introduced CryptoCertify which uses Ethereum to store the hashes of certificates for either authenticity or proof of ownership. Also, R. S. A. Fathima et al. [2] adopted SHA-256 hash to verify the security. Although these methods are successful in identifying tampering, they only validate and lack academic credit mapping or multi-institutional workflows.

The use of smart contract-based validation systems was investigated by A. Kumar et al. F. Recording and play back (1) The one we saw an existing applications on this is with digital media like video, tv, radio So that it can have distant viewing, phone ,sound system etc o Can be converted to analytic format(optional). [6],who proposed the automated proofs for verification of logic. M. R. Nair and S. Menon developed the rule-based algorithms model for academic certificates [5]. Nonetheless, those available today are institution-centric and failed to be interoperable and used for MOOC based credit transfer.

Tokenization and NFT-based credentialing solutions have also been suggested. B. K. Rai et al. [3] proposed NFT-style tokens for guarantee of uniqueness and ownership. Novel as these models are, they tend to focus on authenticity more so than credit transfer/recognition and meeting regulatory requirements.

For storage, E. Nyaletey and J. Kawamoto [10] combined blockchain with IPFS for the secure document storage system. Their work demonstrates an advance toward a more decentralized setting over centralized file systems, but full integration in the entire workflow of the institutionateway is oftentimes.

More general studies are presented by A. Rustemi et al. [7] were authors of a systematic literature review study on blockchain-based academic verification systems, which

they concluded that most systems handle only one side from verification or storage or privacy and not an ecosystem. A. Alammary [16] also considered scalability, governance, and regulation in educational blockchain adoption.

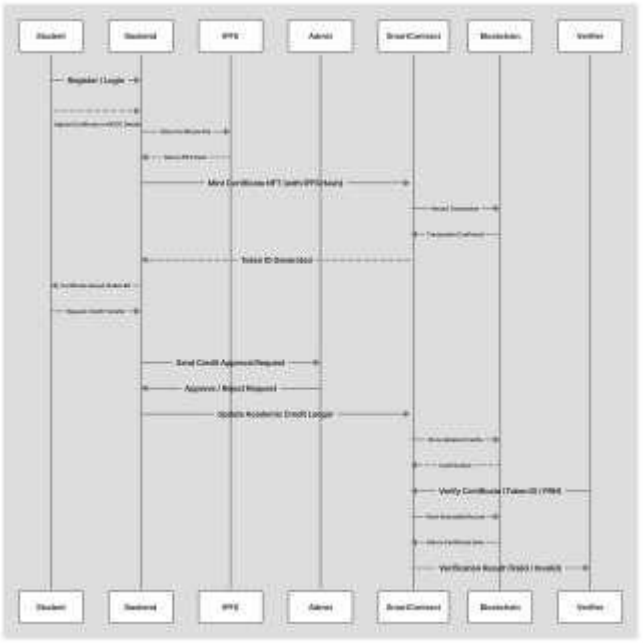
There is also a model for storing educational records in blockchain systems, which includes reputation systems was proposed by M. Sharples and J. Domingue [14] Addressing long-term academic credentials tracing, as well. The policy-level guidance under Ministry of Education, Government of India's National Education Policy 2020 [15] is to focus on digital academic bank systems and credit transfer mechanisms, which supports the case for interoperable blockchain-based credential platforms.

According to the analysis, in existing studies, authors usually handled separate parts on verification, tokenization, smart contracts or decentralized But there are very limited systems, which combine all these components together in an integrated architecture for MOOCs credit transfer that is aligned with NEP 2020. So based on these we suggest a full novel blockchain-based credential validation system with the features like smart contract automation, IPFS file storage, student academic ledger handling along with multi-stakeholder credit approval workflows.

III. METHODOLOGY

The novel system, by means of three main parts Student Portal, Admin Portal and Verification Portal, binds the university students, university staff and off-campus checkers smoothly together through block chain. The purpose with which this paper is written is to establish a secure environment storing certificates and calculating credits and at the same time verifying documents without having to depend too much on cumbersome manuals. This system is composed of three main parts: a Student Portal, an Administrator's Portal, and a Verification Portal. Every part has its ownarea of responsibility, but each is quite closely related with the same intelligent contract and decentralized storage system. Everything done inside the system is recorded in an unchangeable form, reducing the chance of human manipulation and thereby increasing the confidence people have in the system as a whole. The certificate files are stored saved across different placesby IPFS, and the blockchain layer tak per ha permanent entry of the certificate hash and credit related information. This design's aim is to reduce errors, maintain transparency, and make academic certificates easier to verify

3.1 Overall Workflow.



The process begins when a student uploads a certificate that that was gained from such platforms as NPTEL, Coursera, and edX. After receiving this file, the system uses the SHA-3 algorithm to create a hash value which reflects the file con tent uniquely and helps to check that any later changes are detected. The hash thus formed is put on the block chain by the intelligent contract written in Soli dity. The data becomes inmaterial and immune to tinker ing. The real certificate itself is uploaded to IPFS / Pinata, and even the certificate gets a unique content address (CID).

3.2 Flow Chart

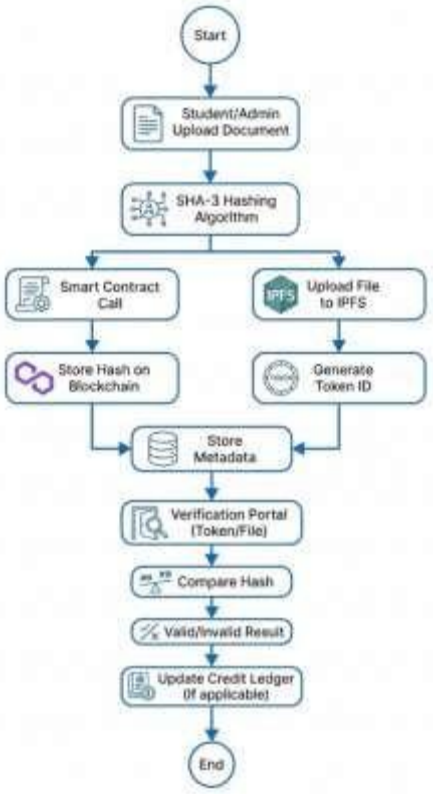


Fig. 3.2 Flow Chart

Fig. 3.2 illustrates the overall sequence of operations carried out in the system. It presents how documents move through different stages, beginning from upload, hashing, and IPFS storage, to blockchain recording and verification. It also includes the steps followed in the credit approval process, where the admin reviews student requests and updates the academic ledger upon acceptance. The flow chart helps readers understand how all components work together inside the system.

3.3 Document Upload Process (Blockchain + IPFS)

When a certificate is uploaded, the system generates a fresh SHA-3 hash from the file. Because the hash changes even if a single character in the file is modified, this method ensures strong protection against tampering. Once the hash is generated, the certificate is uploading to IPFS/Pinata, which provides a Permanent CID for the file. The smart contract then records the CID, the hash value, the students PRN and other related information. This combined strategy guarantees that the document is easily verifiable and cannot be altered in the future.

3.4 Certificate Verification Process

Verification can be done in two different ways. A verifier may enter the token ID linked to the certificate, and the system retrieves the stored information from the blockchain to confirm it. Alternatively, the verifier can upload the certificate file again, and the system will generate a new hash from the uploaded document. This new hash is compared with the on-chain hash. If the values match, the certificate is confirmed as legitimate; otherwise, it is marked as modified or invalid. This method removes the need to contact the issuing university and speeds up verification significantly.

3.5 Credit Approval Flow

Credit transfer starts from the moment a student uploads their certificate and sends in course related information. The necessary data is stored by the system in the smart contract. Admin review the pending request by cross-checking the course duration and certificate as well. Once reviewed, the admin approves or denies the request. The credits that are approved, then get written to the student's academic ledger (or history) which sits in a blockchain and cannot ever be tampered with. This further levels the playing field in credit treatment.

3.6 System Architecture

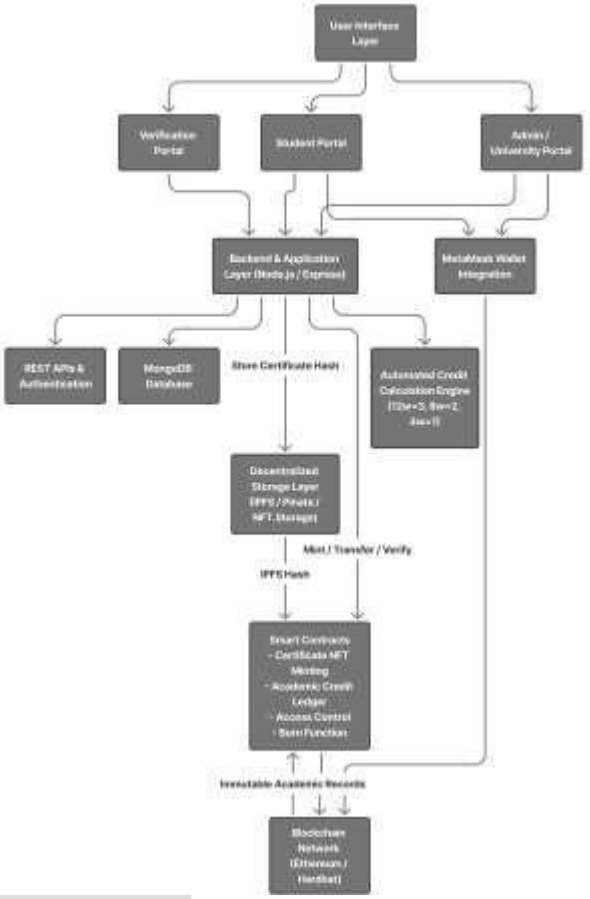


Fig. 3.6 System Architecture

Fig. 3.6 Links to all major components can also be found in the bottom navigation of this page.This user interface uses React.js,and that leads to separate dashboards for students, administrators and verifiers.In the back end, Node.js and Express.js handle requests and communicate with blockchain networks. Features like hashes of certificates, token IDs, records for creditsare managed by smart contracts written in Solidity, using Hardhat.IPFS/Pinata store documents in a decentralized way.For the authentication layer, we implemented MetaMask to manage all blockchain interactions directly, ensuring secure user access. This configuration is combined with Hipatia Wallet to simplify the way that users manage their digital assets in the application. On the backend, we have a MongoDB database to hold core student information nsuch as login credentials and PRN for centralized control. By connecting the dots, we were able to lay basis for our academic verification platform that supports complex taxonomies.

TABLE

COMPARATIVE ANALYSIS OF ACADEMIC CERTIFICATE VERIFICATION SYSTEM

Features	Traditional Academic Verification System	Existing Blockchain Certificate Systems	Proposed Blockchain Based Credit Transfer System
Certificate Storage	Held in central university databases and paper archive	File certificates are hashed to the blockchain and files are hosted centrally	Hybrid storagewith Blockchain in hashes and IPFS of certificates files.
Data Integrity	Records can be created, altered or manipulated	Tamper-detection is available but limited to storage	Full data integrity and immutability are guaranted by crypto-graphic hash
Verification Process	Manual check by email or from institutional communication	Semi-automated blockchain verification	Instant audit on the blockchain by means of smart contracts
Transparency	There is limited transparency because of the one central command and control center	Moderate transparency with blockchain logs	Full transparency with permanent academic ledger.
Verification Speed	Slow due to manual processing	Faster than traditional systems	Real time instant verfication
Audit Trail	No reliable audit history	Limited blockchain logs	Permanent on-chain audit trail
Scalability	Limited by centralized infrastructure	Moderate scalability	Very scalable via IPFS + blockchain
Compliance with NEP 2020	It is relatively easy to detect forged certificates	A tampering detector without intelligent workflow automation	Reliable detection based on instant hash comparison and token validation
Academic Credit Transfer	Manual credit conversion paperwork	Notsupported in most implementat-ions	Automated NEP-aligned credit transfer System
MOOC Integration	No incorporat-ion of third-party learning systems	Limited supports for external certificates	Facillated certificates from NPTEL,SWA-YAM, Coursera and edx

IV. SYSTEM OVERVIEW

The system is intended to offer students and employees at institutions of higher education a tamper-proof, decentralized and secure platform that encompasses the various blockchain-based mechanisms for certificate issue, verification academic credits. The platform brings together Ethereum smart contracts, IPFS decentralized storage plus wallet-based authentication in order to achieve both tamper-proof record management and automated ROS runtime behavior. When implemented, certificate uploads generated relevant IPFS Content Identifiers (CIDs) and SHA-3 cryptographic hashes that were indeed faithfully and properly recorded in Ethereum smart contracts, certifying the document contents such as shown in the table below [12], [13]. Verification tests saw that real certificates consistently produced hash matches, while any alteration in document caused an immediate mismatch. Token-based verification retrieved the real certificate metadata correctly from the blockchain, thereby demonstrating quite convincingly this system's capability for giving reliable attestation of qualifications. In an architecture that combines blockchain and IPFS, data integrity is guaranteed even while avoiding excessive on-chain storage costs [13], [1]. Ultimately, this system reduced delays for manual checks of authenticity and increased the auditability of all college credits – fully taking into account NEP 2020 objectives for trouble-free lifelong learning [5]. The design also suits EVM-compatible testnets and local deployments; thus it supports practical experimental implementation at schools even while addressing concerns about costs for mainnet transactions [7], [15].

The work available can be divided into three basic units: Administrator System, Student Compliance Supporting System, and Verification System.

4.1 Admin Portal

The Admin Portal lets authorized university administrators issue semester grade reports; at the same time they can upload a student's graduation certificates and when MOOC certificate acquisition is detected automatically verify these. Following all necessary verifications, invoking the smart contract triggers off-chain execution procedures to update a student’s blockchain-based ledger with the credited units. Since the approval itself is permanently preserved on-chain, the system offers a point from which to check verification results and dispute any manipulation [12].

4.2 Student Portal

The Student Portal allows students to submit and externally MOOC-acquired certificates, require the review of outstanding records, track the ‘credited’ status of approved courses. When an application has been granted, credits will always be included in a permanent record for that student and the certificate made securely available to everyone who needs it in education or employment. Students themselves take care of sharing their qualifications: in future they are based on tokens rather than relying on the institutions' verification process [15], [14].

4.3 Verification Portal

The Verification Portal permits businesses, colleges as well as verification agencies to automatically check certificates themselves using token identifiers or by comparing uploaded files with recorded hashes. In addition, PRN-based look-up would show authenticated verifiers the student's verified academic record – including the classes taken, credit earned, background. This spares them the bother of contacting record-holding institutions; likewise it ensures both quick commands for reliable validations and an inviolable trustless credential chain.

V. CORE DOMAINS AND MODULES

The proposed academic credential verification and credit transfer system is developed by integrating multiple technological domains and functional modules that together ensure secure certificate management, automated academic credit processing, and reliable credential verification. The system architecture combines blockchain technology, decentralized storage, web-based application interfaces, and secure authentication mechanisms to provide a complete end-to-end academic workflow.

A. Core Domains

1. Blockchain Domain::

The blockchain as the core of the system, is a domain where Ethereum smart contracts store metadata on certificates, academic credit approvals and deal records in an immutable form. After certificate or credit requests are approved by an administrator, the transaction is automatically recorded on the blockchain and academic records are immune from tampering or fraudulent behavior. This sector offers transparency, traceability and the confidence brought by academic qualification management.

2. Decentralized Storage Domain:

For keeping the certificate files, such as PDFs or images the system uses decentralized storage via IPFS to avoid large blockchain storage costs. Upon uploading a certificate, IPFS creates a specific Content Identifier (CID) and stores it in the block chain along with the hash of the certificate. This mixed protocol provides even more more sensitive storage protection and tamper detection, along with enjoying compact resource utilization while maintaining the decentralized access property.

3. Web Application Domain:

The application domain within the web application offers user-friendly interfaces with front-end technologies implemented in a contemporary manner. There are student, admin and verification user dashboards for certificate submission, credit approval and credentials verification. Backend APIs abstract calls to the user interface and take care of communication between blockchain network, decentralised storage and the interface to work smoothly.

4. Authentication and Security Domain:

The system employs a safe wallet authorization establishes access to sensitive transactions such as certificate issuance and credit approval. Access to blockchain transactions are protected using role-based access control techniques, informal and unauthorized admin users should not take part in any transaction on the blockchain service, students and verify users could securely use their respective properties. Such a discipline helps to enhance the system security mechanism against "unauthorized" record modification.

B. System Modules

1. **Admin Module:**

Authorized university administrators of the system can manage the certificate issuing process, upload authenticated (canonically signed) academic certificates and validate MOOC certificates submitted by students using secured blockchain-integrated workflows via the Admin Modules. Certificate documents are saved on IPFS decentralized storage with cryptographic hashes and metadata being written into the blockchain to provide tamper-proof verification and preserve record integrity in perpetuity.
Moreover, the system permits administrators to approve academic credit transfer requests and accordingly update a student's blockchain academic ledger through smart contracts. It offers features to access approved credits, revoke erroneously signed certificates and manage authorized minter capabilities making academic credential administrator secure and transparent.

2. **Student Module:**

In the module for students they can upload certificates of internal and external MOOCs; request recognition of credits, follow the status of its approval or check out their own recognized academic credits. The module also provides for students to have access to their independent academic record and be able to share secure verified credentials for employment or scholastic purposes.

3. **Verification Module:**

The module also gives authority to the admin to review and accept transfer of credits in academics, then smart contract will update the blockchain academic ledger of a student accordingly. It also offers capabilities to view successful credits produced, revoke mis issued credentials and control privileges for authorized minters to ensure secure and transparent academic credentialing.

VI. RESULTS AND DISCUSSION

The complete system was developed and tested across all user roles, and each module performed as expected during practical use and tested using different user roles Admin,

Student, and External Verifier. The results show that blockchain and IPFS together provide a reliable and tamper-proof method for storing academic certificates and managing credit transfer. Each screenshot below represents a working module of the system, along with a short explanation of how the module behaves in real use.

Fig. 5.1 Connect MetaMask Page

In above Fig. 5.1, the admin: Connects MetaMask wallet to the system. This is a necessary step, since all of our certificate actions (issuing, approving records) are recorded on the blockchain. To prevent the system from being corrupted and halt unwanted access, MetaMask ensures that only the authorized administrator has permission to perform these actions.

Fig. 5.2 Issue Certificate Page

In above Fig. 5.2 the admin inputs student information including PRN, semester, marks and grade to obtain final certificate. Upon form submission, the certificate is stored on IPFS and its hash on blockchain. This makes the presented certificate static and not modifiable, as altering the file would change its stored hash.

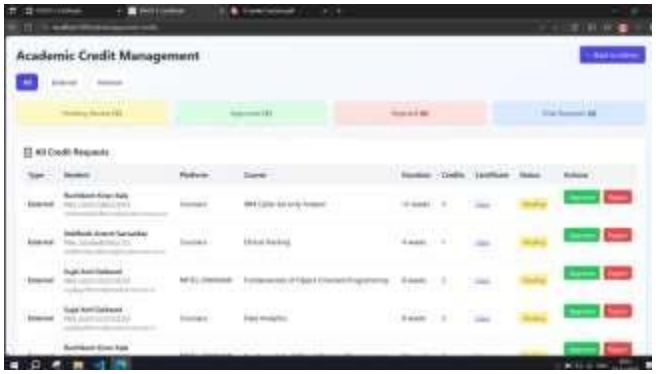


Fig. 5.3 Admin Approve Credit Page

In above Fig. 5.3 the all students' credit frezard offices have read and approve or deny each request made for transferral of credit to his/her freezard account. Multiple Course Duration (H: Hours) You can see the courses name, platform, duration, credits and uploaded certificate. An admin can then approve or deny the request after reviewing the information. Once approved, the credit is automatically written to the student's blockchain credit account.

Fig. 5.4 Student Dashboard

In above Fig. 5.4 the student dashboard displays verified credits, pending requests, total certificates, and remaining credits. Students can upload new certificates for credit transfer and also check the approval status of their previous submissions. The dashboard helps students can easily monitor their credit records and certificate status as they are updated instantly.

Fig. 5.5 Upload Certificate on Blockchain

In above Fig. 5.5 the admin uploads certificates for blockchain storage. After selecting a file, the system generates a SHA-3 hash and stores it on the blockchain. The document is uploaded to IPFS, and the IPFS CID is linked with the blockchain entry. This makes each uploaded certificate secure and permanently traceable.

Fig. 5.6 Verify Certificate Page

In above Fig. 5.6 a certificate is validated by the user who uploads its PDF or image file. The system generates a hash of the uploaded file and compares it with the stored on blockchain hash. If the two match, then the certificate is valid. If inappropriate, the document is tagged as not valid or altered.

Fig. 5.7 Verify Portal Page

In above Fig. 5.7 the verification portal provides three options: verify using token ID, verify by uploading a document, and view the student's academic ledger. Companies and universities can use this portal to instantly check whether a certificate or credit record is genuine.

Fig. 5.8 View or Verify Student Credit Using PRN Number

In above Fig. 5.8The verifier enters the student's PRN number to view all approved credits. The ledger shows details like the earned credits, course name, issuing platform, and verification status. This helps the university quickly check and confirm a student's record without doing any manual work.

VII. CONCLUSION

This study proposed a blockchain-based decentralized academic certificate verification ITS with credit transfer system to combat the increasing cases of fake certificates, delays in manual certificate verifications and an ineffective portability of academic credits. Leveraging Ethereum smart contract, IPFS decentralized storage and MetaMask-based authentication, the proposed system achieves tamper-proof certificate management, transparent academic credit approval and real-time credential verification regardless of the central authority. The proposed hybrid blockchain–IPFS model balances between security of the system and scalability and storage efficiency, while role-based portals (for students, administration, and verifier) ensure a complete end-to-end academic workflow. The realisation outcomes show that the system will reduce efforts for verification, enhance trust in digital academic records and facilitate NEP 2020 goals of flexible learning and multi-source credit accumulation. In summary, the proposed framework provides a robust and secure foundation for next-generation academic credit trust system, and could contribute to efficiency of institute work-load reduction, cross-course student credit portability, trusted industry-level resume data verification in field education ecosystem.

VIII. FUTURE SCOPE

In the future, the proposed system can be expanded into a consortium blockchain network connecting multiple universities to enable nationwide academic credit portability and unified credential verification. Additional enhancements such as encrypted IPFS certificate storage for improved privacy, QR-code-based instant verification, mobile application integration, and AI-assisted certificate validation using OCR can further strengthen the platform's security, accessibility, and scalability.

IX. REFERENCES

[1] B. Jadhav, S. Shinde, and P. Patil, "CryptoCertify: Certificate Validation and Authentication Using Blockchain Technology," Proc. IEEE IC-CGUC, 2024.

[2] R. S. A. Fatima, M. Selvaraj, and S. Kannan, "Blockchain-Powered Certificate Verification Using SHA256 Algorithm," Proc. IEEE ICISS, 2025.

[3] B. K. Rai, A. Chandel, and A. Kumar, "VaLiDiFy: Certificate Validation using Blockchain and AI," Proc. IEEE ICTBIG, 2024.

[4] A. Godase, "Certificate Validation Using Blockchain," Proc. IEEE ICSSS, 2020.

[5] M. R. Nair and S. Menon, "Securing Academic Certificate Verification with Blockchain-Based Algorithmic Rules," Proc. IEEE IMCET, 2023.

[6] A. Kumar, R. Sharma, and S. Singh, "Smart Certificate Validation System using Smart Contracts," Proc. IEEE SmartCom, 2022.

[7] A. Rustemi et al., "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, vol. 11, pp. 145321–145340, 2023.

[8] A. M. San and Y. M. Naing, "Blockchain-Based Learning Credential Verification System with Recipient Privacy Control," Proc. IEEE TALE, 2019.

[9] J.-C. Cheng, H. Wang, and T. Lin, "Digital Certificate Framework Using Blockchain and Contract-Based Automation," Proc. IEEE ICASI, 2018.

[10] E. Nyaletey and J. Kawamoto, "Blockchain-Enabled IPFS for Trusted Document Storage," Proc. IEEE Blockchain Conference, 2019.

[11] S. NaKamoto, "Bitcoin:A Peer-to-Peer Electronic cash System,'' 2008.

[12] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Whitepaper, 2014.

[13] J. Benet, "IPFS Content Addressed, Versioned, P2P File System," IPFS Whitepaper, 2015.

[14] M. Sharples and J. Domingue, "A Blockchain- Oriented Model for Managing Educational Records, Reputation, and Reward Mechanisms," European Conf. on Technology Enhanced Learning, 2016.

[15] Ministry of Education, Government of India, "National Education Policy (NEP) 2020 – Policy Document," Govt. of India, 2020.

[16] A. Alammary, "Blockchain for Education: Opportunities, Challenges, and Future Directions," Applied Sciences, vol. 9, no. 11, 2019.

[17] D. Tapscott and A. Tapscott, "Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World," Penguin, 2018