[1]Dhananjay Pai,
[2]Hrishikesh Patil,
[3]Yash Sahane,
[4]Varad Deshmukh,
[5]Dr. Nupur Giri

DeCAT: Decentralized Certificate Authority - A Blockchain based Service Aligned to India Stack

JES Journal of Electrical Systems

Abstract: - The prevailing challenges within the realm of issuing and authenticating certificates for achievements, skills, or commodities, involve issues of duplication, document tampering, malpractice and lack of trustworthiness. This research proposes a solution leveraging blockchain technology to improve the credibility and legitimacy of certificates. The system employs soul-bound tokens (SBTs) to accurately represent individuals' skills and qualifications, ensuring certificate authenticity. Credibility is reinforced by endorsements from verified certificate holders, which can be prominently displayed in a portfolio. The system facilitates verification through QR codes embedded in SBT certificates. The system has a Reputation Score mechanism, dynamically assessing individuals' proficiency based on various parameters, thereby providing a tangible metric for evaluating candidates' expertise. The system uses LLM for generating casual granular statistical insights of the certificates in the particular wallet address. This research underscores the system's potential to revolutionize credential validation in the market by offering a transparent, efficient, and trustworthy project.

Keywords: Blockchain, Decentralized Applications, Non-Fungible Tokens, Soul-Bound Tokens, InterPlanetary File System, Ethereum Request for Comment-5192

I. INTRODUCTION

In recent years, the landscape of certificates, achievements, and credentials management has encountered significant challenges within various industries and organizations. Traditional methods of issuing and verifying certificates have been plagued by several issues, including duplication, document tampering, malpractices in issuance, and a general lack of trustworthiness. These shortcomings undermine the credibility and value of individuals' accomplishments, leading to skepticism and uncertainty in the validity of their claims. Moreover, the ease with which individuals can falsify their portfolios exacerbates these concerns, further eroding confidence in the integrity of certificates and achievements.

According to the report given in [9], the worldwide certificate authority market is projected to expand at a compound annual growth rate (CAGR) of 12.2% during the period 2022-2030, from its 2021 valuation of USD 127.34 million.

A study by L. Ndlovu et.al in [8] discussed the issueslike false claims affecting the job market and the law being imposed to minimize the side-effects of these dishonest practices in South Africa. The topic of perceived risk and trust, specifically the nature of purchasing associations among the pricey, sophisticated, high-risk, and credibility items like jewels, was the focus of another research[11].

According to CareerBuilder Survey [10], companies facean average loss of $15,000 for each incorrect hire or for recruiting individuals with fraudulent qualifications. This financial setback is compounded by potential risks to public safety, such as buildings designed by unqualified engineers or medical treatments administered by fake doctors. Properly validating certificates before hiring individuals is crucial to mitigating these risks. However, the challenge lies in the complexity and resource-intensive nature of credential verification, which consumes

[1] Department of Computer Engineering Vivekanand Education Society's Institute of Technology Mumbai, India 2020.dhananjay.pai@ves.ac.in
[2]Department of Computer Engineering Vivekanand Education Society's Institute of Technology Mumbai, India 2020.hrishikesh.patil@ves.ac.in
[3]Department of Computer Engineering Vivekanand Education Society's Institute of Technology Mumbai, India 2020.yash.sahane@ves.ac.in
[4]Department of Computer Engineering Vivekanand Education Society's Institute of Technology Mumbai, India 2020.varad.deshmukh@ves.ac.in
[5]Department of Computer Engineering Vivekanand Education Society's Institute of Technology) Mumbai, India nupur.giri@ves.ac.in

significant time, money, and organizational resources. As a result, there has been a growing demand for innovative solutions that address these shortcomings and provide a more secure, transparent, and reliable means of managing credentials.

	Credly	**Accredible**	**DeCAT**
Issuance	Uses blockchain to store digital certificates	Uses Bitcoin blockchain to issue digital certificates.	Uses Ethereum and Layer-2 Blockchain (Polygon) to issue certificates as Soul-Bound tokens.
Verification	Provides verification through blockchain	Offers verification through secure verification	Provides Verification through blockchain Using QR codes
Analytics	Provides detailed analytics and insights	Offers analytics on badge engagement	Provides detailed insights and analysis using AI
Reputation Mechanism	No such system	No such system	Uses a dynamic reputation scoring system.

Table 1. Comparison with existing platforms.

Table.1. demonstrates the comparative study of features provided by various platforms currently present in the certificate industry.

Against this backdrop, initiatives like DeCAT (Decentralized Certificate Authority) have emerged, proposing groundbreaking solutions that harness the potential of blockchain technology and non-fungible tokens (NFTs) to revolutionize the management of certificates and achievements. DeCAT aims to redefine the way certificates are issued, verified, and managed, ensuring the security, integrity, and traceability of each credential.

According to the case study in [14], IndiaStack is a set of digital infrastructure components that form the backbone of India's digital ecosystem. It comprises various layers that enable the seamless delivery of digital services to citizens, businesses, and the government. The key components of IndiaStack include Aadhar ,UPI, DigiLocker, eKYC. IndiaStack has solved various problems by serving as a central entity in the digital ecosystem. It has facilitated financial inclusion by providing a digital identity and payment system to underserved populations. By enabling interoperability and competition through open standards, IndiaStack has fostered innovation and allowed for the development of a vibrant digital economy.In lieu of a singular use case like IndiaStack, DeCAT itself serves as thefocal point of innovation, revolutionizing the handling of certificates and achievements.

At the core of DeCAT's solution are Soul Bound NFTs, which serve as unique identity tokens that cannot be transferred or tampered with once minted to a user's wallet address. This ensures the authenticity and uniqueness

of each certificate or achievement, mitigating the risks associated with forgery and falsification. By leveraging blockchain technology, DeCAT provides a decentralized platform that offers transparency, immutability, and verifiability, addressing the shortcomings of traditional certificate management systems.

One of the key features of DeCAT is its ability to execute transactions in a multi-batch fashion, by bundling the transactions together for a single execution instead of paying gas fees for each individual transaction, thereby reducing transaction costs by 99.8%, and streamlining the issuance process. The platform's Layer-2 architecture is significantly more scalable and efficient than Ethereum, offering up to 382% more transactions per second (65,000
compared to Ethereum's 17 transactions per second), while minimizing transaction fees. This simplifies and ensures a secure certificate issuance process for the organizations.

Furthermore, DeCAT's decentralized application facilitates the creation of academic and professional profiles, fostering incentivization and growth within the community. It enables easier tracing for hiring and recruitment processes, providing employers with a reliable means of verifying candidates' credentials.

NOVELTY AND IMPACT

The integration of the Central Unit of Issuance and Control of Certificates with the DeCAT platform promises a plethora of transformative outcomes for stakeholders and the nationat large. Serving as the national centralized authority for certificate issuance and validation, DeCAT establishes a unified framework for certificate management across all organizations, streamlining processes, eliminating redundancy, and ensuring consistency and standardization incredential validation. Moreover, this integration facilitates the creation of comprehensive student profiles within the DeCAT ecosystem, incorporating not only certificates but also additional relevant information such as achievements, skills, and reputation. This holistic view of students enhances their job prospects by better aligning their profiles with employer requirements, thereby fostering improved labor market dynamics and reducing the skills gap. Furthermore, DeCAT's utilization of blockchain technology ensures the secure issuance of certificates, mitigating the risk of fraud or forgery and bolstering confidence in credential authenticity. Its cost-effective certification services democratize access to certification for organizations, especially smaller institutions or start-ups, promoting inclusivity in education and employment. Additionally, the scalability of the integrated platform enables it to accommodate increasing demand without compromising performance or reliability. The national impact of widespread DeCAT adoption is profound, contributing to the enhancement of education quality, fostering innovation, and catalyzing economic development.In essence, the integration of the national central unit with the DeCAT platform signifies a paradigm shift in certificate management, with far-reaching implications for education, employment, and overall national progress.

II. LITERATURE SURVEY

In Reference [2] the author has developed a secure certificate verification system which involves creating a web application that allows universities to upload or generate certificates, which are then stored on IPFS in a decentralizedand encrypted manner.

Reference [7] implements the same system as SBTCERT and has a decentralized credential recovery mechanism in case the credential holder loses their private key. Reference
[1] has implemented BeCertify , the platform utilizes a peer-to-peer distributed network system to transfer higher education degrees onto the blockchain, providing a secure and efficient way to store and exchange academic qualifications.Reference [3] proposes a government-owned private blockchain where universities, students, and third parties can register and obtain private keys. The process involves generating tokens for third parties and storing themon the blockchain.

In Reference [4] the system allows schools to grant e-certificates containing a quick response (QR) code to graduates, with each graduate receiving an inquiry number and electronic file of their certificate. Reference [6] proposes a framework called NFTCert, which utilizes Non-Fungible Tokens (NFTs) and blockchain technology tocreate digital certificates. It introduces an online payment gateway to facilitate transactions without relying on cryptocurrency.

Our work through DeCAT proposes to address the shortcomings that exist in the market of certification. The issues like duplication, editing and malpractices in the issuance of certificates, can be resolved by leveraging the potential of blockchain technology and introducing the identity token concept using SoulBound token in order to

preserve the authenticity and security of the certificate against outside interference. The platform is a one stop solution for all the academic and professional needs and alsoserves as an individual's portfolio and increases potential participation to better oneself for better ranking in the domain through platform's gamification algorithms.

I. PROPOSED SOLUTION

A. Overview

The system architecture depicted in fig.1 is based on thepublic layer-2 blockchain network in order to create a transparent platform that is efficient and delivers high performance in terms of speed and cost efficiency.

The platform features services that allow 1. Authorized Issuance 2. Verification and 3. AI driven Reputation score which are integrated as service models through the website.

1. *Certificate Issuance (SOUL BOUND TOKENS)*

The certificate issuance on the platform is performed bythe organization's authorized personnel by logging into the system. The credentials are whitelisted into the system and hence provide a secure way to interact with the platform.

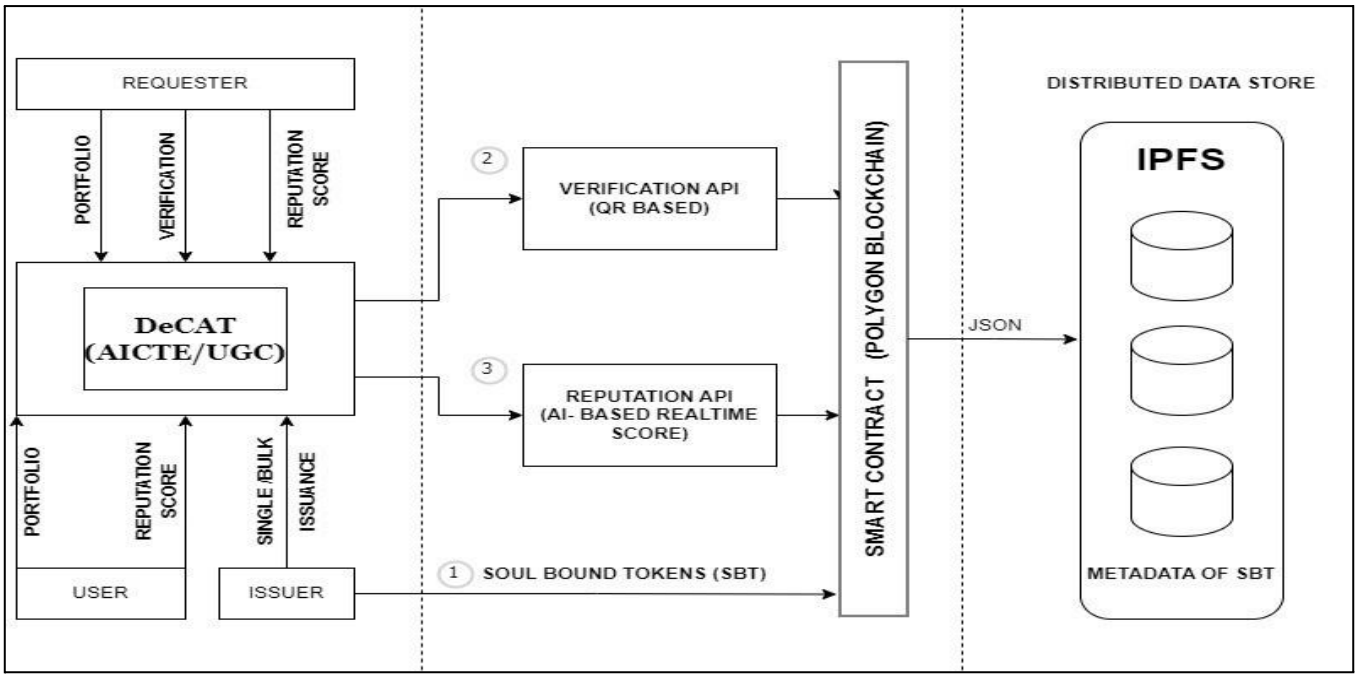

Fig. 1. Block Diagram and System Design

Following the login authentication, the entity isexpected to provide the metadata of the certificate like title, image, description, subject etc. for certification information. A smart contract is deployed on Ethereum and Polygon blockchain, adhering to the EIP5192 and ERC 721 standard which defines the outline for the SBTs.

The platform supports both **single min**t and **multi-batch mint** functionalities as displayed in Fig.1. Single mint allows the creation of individual SBTs, while multi-batch mint leverages multi-batch transactions for efficient bulk minting in terms of cost and time as given in Table.2.

The credibility of the certificate can be ensured as this certificate could not be burned or transferred further to any other user.

The issued certificate is subsequently stored on the InterPlanetary File System (IPFS) using Lighthouse.storage,a decentralized storage solution. The certificate can be viewed in the account of a candidate by any entity using his/her respective public wallet address on the platform or a marketplace like OpenSea.

2. *Verification Module*

One of the platform's distinguishing features is the authentic and credible method of handing out the

certificatesin order to address the issues like duplication and malpractices in issuance that are plaguing the market. This credibility can be demonstrated by the verification moduleof the system wherein with every certificate that is minted, aunique **QR Code** is generated, that could be scanned in order to verify the authenticity of the certificate.

The issued certificates can be verified by scanning the QR Code of the certificate and identifying its details on the website which cross-checks the data stored on blockchain asdepicted in Fig.1. The certificate's metadata like minting hash, title, description etc., is displayed post scanning whichdetermines the verification of its authenticity.

3. *Profile Reputation Score Module*

The platform's flagship feature involves scoring a user profile based on the number of certificates earned as a measure of the skills acquired by the individual. The calculations also considers current market conditions and the certificate endorsement, meaning any entity can vouch for another individual for being proficient in a skill. This endorsement is limited to the number of certificatesacquired by the entity that is vouching.

The calculation is performed by a proprietary dynamic reputation scoring algorithm that involves relative grading of the certificate based on the market response and market value. The current job market statistics is fetched by using autonomous agents that use LLM to gather the live job demographics and based on the results, respectively assigns a normalized weight to the certificates for calculating the score of a profile. Reputation scores are seamlessly integrated into user profiles, allowing individuals to showcase their proficiency and credibility within the job market ecosystem. The score calculation process is transparent and auditable, with all relevant data and transactions recorded on the blockchain.This feature is designed for scalability, capable of handling a large volume of users and transactions within the system. The smart contract employs efficient algorithms to handle reputation score calculations and updates, ensuring responsiveness and accuracy.

The score thus calculated is displayed on a leaderboard of the platform, mentioning the top users of the platform with the highest acquired skills. The leaderboard creates a healthy learning environment with a competitive spirit with a tendency for users to interact more with the platform.

DeCAT utilizes Generative AI, specifically the Gemini Pro LLM, to process the prompt received from a recruiting entity to filter the candidates according to their requirementsthus providing a hassle-free and reliable shortlisting process.For evaluating a particular candidate, any entity can enter a wallet address to view a user's portfolio, the system compiles all certificates associated with that address into a single, easily readable text format and provides clear, comprehensive statistics about the individual's achievements. Thus, by leveraging Generative AI, we streamline the process of accessing and analyzing certification data, offering users insightful statistical insightsin a casual, understandable manner.

. This makes the hiring and job seeking procedure mucheasier and transparent while being trustworthy.

II. OPTIMIZATION AND STRATEGIES

The proposed system includes various optimizations and strategies to enhance scalability, efficiency, and usability of the project. One of the key optimizations in the proposed system is the utilization of Soul Bound Tokens (SBT) to represent certifications of various skills possessed by the individual.

Unlike traditional Non-Fungible Tokens(NFT), Soul Bound Tokens are non transferable digital identity tokens that are publicly verifiable. SBTs offer a more flexible and efficient way to manage certifications. SBTs are minted by whitelisted organizations specified in the smart contract, allowing for a streamlined process of certification issuance and verification. Users can showcase all their SBTs in their portfolio, providing a comprehensive view of their skills andexpertise.

To address scalability, transaction speed and gas (transaction) fees concern, the smart contracts are deployed on Layer 2 blockchain such as Polygon. It is estimated that gas fees on Ethereum are more than 400 times more expensive than on Polygon. In addition to being compatible with Ethereum, Polygon is many times faster, processing up to 10,000 transactions per second (tps) as opposed to Ethereum's 14 tps. By leveraging Layer 2 solutions, we mitigate the limitations of the Ethereum mainnet, including high gas fees and slower transaction confirmation times. The use of Polygon enables faster and more cost-effective transactions, enhancing the overall user experience of the certification and reputation system.

Another strategy employed to improve transaction speed is the utilization of MultiBatch transactions. Multi-batch transactions on Ethereum refer to the process ofgrouping multiple transactions into a single transaction to

reduce the overall gas fees and improve transaction speed. By bundling multiple transactions into a single batch, we minimize network congestion and optimize resource utilization.

No. of transactions (bulk mints)	Transaction time(in secs)	Cost of transaction (Sepholia eth)
Single mint	8 - 10 seconds	0.0010 eth
10 - 20	10-14 seconds	0.0043 eth
20 -30	16 - 23 seconds	0.0091 eth
30 - 40	25 - 28 seconds	0.0142 eth

Table 2. Bulk mint statistics.

The comparative study of multi-batch transactions on the Sepholia Ethereum testnet has led us to conclude that there are important implications for efficiency when it comes to cost and speed when compared to minting individual certificates. According to our research, distributing SBTs to 10, 30, and 50 wallet addresses using multi-batch transactions resulted in lower average transaction costs per certificate in comparison to certificates that were minted one at a time for each address. Furthermore, although the computational load associated with bigger batch sizes resulted in a modest increase in transaction times, overall efficiency improvements in terms of lower gas expenses per certificate exceeded the marginal increase in transaction times. This demonstrates how batch processing may help SBT distribution operations optimize speed and lower transaction costs.

This approach not only accelerates transaction processing but also reduces the overall time required for interactions within the system. MultiBatch transactions contribute to a more responsive and efficient user experience, particularly in scenarios with high transaction volumes. The optimizations and strategies outlined above significantly enhance the scalability and effectiveness of theproposed system.

Through the use of Soul Bound Tokens, deployment on Layer 2 blockchain, and implementation of MultiBatch transactions, the system ensures a robust and user-friendly platform for identity verification and skill assessment in the job market. These optimizations pave the way for a more seamless and reliable recruitment process, empowering hiring managers to make informed decisions based on candidates' reputation scores and certifications.

CONCLUSION AND FUTURE WORK

The project proposes a significant advancement in leveraging blockchain technology for enhancing trust and transparency in professional credentials. The utilization of SBTs provide individuals with a secure and immutable method of storing and presenting their certifications. The legitimacy and dependability of the certifications are verified using QR code verification. Users' trust networks are further strengthened by an endorsement system, enabling the recognition and validation of skills based on the SBT-associated metadata. The Reputation Score mechanism serves as a pivotal component, dynamically generating scores based on various factors. This novel method not only authenticates an individual's expertise in particular domains but also enables hiring managers to makewell-informed choices while searching for exceptional talent.

Overall, the project highlights how blockchain technology has the ability to completely change identity verification and credentialing procedures in the employmentmarket. The EIP5192-compatible Decentralized Certification Authority and Reputation System is a critical component in creating an employment ecosystem that is more inclusive and meritocratic by improving efficiency, transparency, and reliability.

REFERENCES

[1] Maestre, Raúl Jaime, Javier Bermejo Higuera, Nadia Gámez Gómez, Juan Ramón Bermejo Higuera, Juan A. Sicilia Montalvo, and Lara Orcos Palma. "The application of blockchain algorithms to the management of education certificates." Evolutionary Intelligence 16, no. 6 (2023): 1967-1984.

[2] Tumati, Tarun Vihar. "SBTCERT: A SOULBOUND TOKEN CERTIFICATE VERIFICATION SYSTEM." PhD diss., CALIFORNIA STATE UNIVERSITY, NORTHRIDGE, 2023.

[3] Shrivastava, Ajay Kumar, Chetan Vashistth, Akash Rajak, and Arun Kumar Tripathi. "A decentralized way to store and authenticate educational documents on private blockchain." In 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), vol. 1, pp. 1-6. IEEE, 2019.

[4] Cheng, Jiin-Chiou, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen. "Blockchain and smart contracts for digital certificates." In 2018 IEEE international conference on applied system invention (ICASI), pp. 1046-1051. IEEE, 2018.

[5] Igboanusi, Ikechi Saviour, Jae Min Lee, and Dong-Seong Kim. "Batch Minting-enabled Digital Certificates Based on Soulbound Token for Achievement Verification."

[6] Zhao, Xiongfei, and Yain-Whar Si. "NFTCert: NFT-based certificates with online payment gateway." In 2021 IEEE International Conference on Blockchain (Blockchain), pp. 538-543. IEEE, 2021.

[7] Reddy, Siddhant, and Dharmender Singh Kushwaha. "Framework for privacy preserving credential issuance and verification system using soulbound token." In ITM Web of Conferences, vol. 56, p. 06002. EDP Sciences, 2023.

[8] Ndlovu, L. and Leslie, A.B., 2022. "False or Fake Qualifications in an Employment Context: A South African Perspective." Yuridika, 37(3), p.715.

[9] Certificate Authority Market Share, Size, Trends, Industry Analysis Report, By Vertical (BFSI, Retail & eCommerce, Government & Defense, Healthcare & Life Sciences, IT & Telecom, Travel & Hospitality, Education, Others); By Certificate; By Services; By Organization Size; By Region; Segment Forecast, 2022 - 2030 Available: https://www.polarismarketresearch.com/industry-analysis/certificate-a uthority-market

[10] Available: https://press.careerbuilder.com/2017-12-07-Nearly-Three-in-Four-Em ployers-Affected-by-a-Bad-Hire-According-to-a-Recent-CareerBuilde r-Survey

[11] D'Alessandro, S., Girardi, A. and Tiangsoongnern, L., 2012. Perceived risk and trust as antecedents of online purchasing behavior in the USA gemstone industry. Asia pacific journal of marketing and logistics, 24(3), pp.433-460\

[12] Lim, Joe Onn, and Diyana Kamarudin. "NON-FUNGIBLE TOKENS: ITS POTENTIAL ROLE IN COMBATING CERTIFICATE FRAUDULENCE IN MALAYSIAN EDUCATION." International Journal of Entrepreneurship, Business and Technology 1, no. 1 (2023).

[13] Saeidnia, Hamid Reza. "Welcome to the Gemini era: Google DeepMind and the information industry." Library Hi Tech News ahead-of-print (2023).

[14] Alonso, Cristian, Tanuj Bhojwani, Emine Hanedar, Dinar Prihardini, Gerardo Uña, and Kateryna Zhabska. Stacking up the benefits: Lessons from India's digital journey. International Monetary Fund, 2023.