

NFT-Based Academic Credential System Using Blockchain

Mrs. Bindu H G¹, Nanditha L², Sanjana K S³, Shiroodarshini⁴, Yukthi Patel H M⁵

^{1,2,3,4,5}*Department of Computer Science and Business Systems, Malnad College of Engineering, Hassan, Karnataka, India*

Abstract—Most of us still trust a degree certificate the same way our parents did: a printed page, an official seal, and the implicit assumption that if anyone ever doubts it, the issuing college will pick up the phone and confirm it. That assumption is quietly breaking down. Certificates get forged with nothing more than a scanner and a decent printer, PDFs are easier still to alter, and a genuine verification request can sit in a registrar's inbox for days before anyone replies longer if the request crosses a border. This paper looks at an alternative built on two pieces of blockchain technology working together: Non-Fungible Tokens minted under the ERC-721 standard to represent each credential as something a graduate genuinely owns in their own wallet, and the Interplanetary File System to hold the actual certificate document off-chain, linked back to the token by nothing more than a cryptographic hash. A Solidity smart contract handles the parts that matter who is allowed to mint, how a token gets checked, how it can be revoked without needing the institution to be involved once the token exists. We walk through why this combination makes sense, set it against roughly thirty recent papers covering everything from early platform prototypes to zero-knowledge privacy extensions, and point out where the field still has gaps: GDPR-aligned handling of personal data, dependable revocation, and transaction costs low enough for routine use. This is a design and literature paper; the working prototype and its test results are reported separately.

Index Terms—Non-Fungible Token, Blockchain, Academic Credentials, Ethereum, ERC-721, IPFS, Smart Contracts, Decentralized Verification.

I. INTRODUCTION

Every degree certificate carries an unspoken promise: that the institution whose name sits on it will, if asked, vouch for it. For most of the history of formal education that promise rested on paper a signature, a seal, sometimes a watermark and checking it meant a

letter or a phone call to the registrar. That basic model has barely changed even as everything around it has gone digital.

And paper, frankly, was never built to resist this kind of pressure at scale. Anyone with a scanner, an image editor, and a reasonably good printer can produce something that passes a glance. PDFs are if anything worse, since the text inside one isn't ink at all but editable content sitting in a file format nobody expects to need protecting. Talk to people who screen large volumes of applications and most will admit, off the record, that they assume some share of submitted certificates have been touched up in some way and that they rarely have the time to check properly. Diploma mills survive on exactly this gap: a document only has to look plausible enough, because verifying it properly costs more than most organizations are prepared to spend.

Putting the certificate online doesn't close that gap by itself. A PDF is no harder to alter than a printout, and while digital signatures exist, almost nobody on either side of a verification issuer or verifier has built the habit of actually checking one. What we're left with is a process that is, underneath the technology, still a phone call: slow, inconsistent from one institution to the next, and entirely dependent on that institution still being around and still willing to answer.

Blockchain offers a genuinely different starting point. Once something is written to a sufficiently decentralized public chain, no one not the institution that wrote it, not an attacker, not anyone else can quietly go back and edit it. NFTs add a second property on top of that immutability: a token under ERC-721 is unique and tied to a specific wallet, which happens to be exactly what a credential needs to represent something that belongs to one person and one person only. Pairing that with IPFS for the

document itself, rather than putting the document on-chain, keeps blockchain costs down and, just as importantly, keeps personal data off a ledger that can never be edited or deleted which matters a great deal the moment data-protection law gets involved.

This paper lays out the reasoning behind a credentialing design built on those two ideas. Rather than walking through implementation details and test numbers, which are kept for a separate paper, the goal here is to explain why this particular design is justified, how it sits alongside the substantial body of work already published on blockchain credentialing, and where the real gaps still are.

The rest of the paper runs as follows. Section II works through the literature on blockchain- and NFT-based academic credentialing published over roughly the last decade, grouped loosely by what each strand of work is actually trying to solve. Section III closes with what those papers collectively leave open and the direction this points the proposed system toward.

II. LITERATURE REVIEW

A. Early Platforms and Foundational Attempts

A good chunk of the earliest work in this area was less concerned with formal guarantees and more focused on simply getting something working. Mujezinović, Joksimović, Kostić, Jolović, and Simić, presenting at SINTEZA 2025, describe a platform that records student achievements on chain as they happen rather than waiting until graduation, which gives an institution a running, auditable trail of a student's progress instead of one certificate at the very end [1]. A related effort out of the University of Belgrade, by Kostić, Joksimović, Radovanov, Muļjajić, Košević, and Naumović, builds on that same idea but pushes harder on the issuance side, aiming for a workflow an institution could actually use day to day rather than just a backend verification API [20].

Nikolić, Vukmirović, Matić, Nedić, and Čapko, at TELFOR 2022, describe one of the earlier applications built specifically around digital education certificates, and their main point still relevant is that even fairly modest infrastructure is enough to get tamper-evidence that paper simply can't offer [2]. Between these and a handful of similar early papers, a pattern emerges that almost everything since has followed in some form: anchor a hash (or the full token) on-chain,

keep the document itself somewhere else, and give verifiers a simple lookup.

B. NFTs Specifically, Rather Than Generic On-Chain Records

A later and more specific strand treats the certificate as an NFT outright rather than a generic blockchain entry, which changes how ownership and transfer actually work. Zhao and Si's NFTCert, from the 2021 IEEE Blockchain conference, is among the first to frame a certificate this way, and they go a step further by wiring in an online payment gateway so an institution can charge a minting fee as part of issuance itself [4]. Kumawat and Naik, at ICCCNT 2024, widen the lens past academic certificates to document verification more broadly, arguing that an NFT is a reusable trust primitive for more or less any document where provenance and a single owner matter [3].

Naik and Naik, at ESCI 2024 in Pune, dig more directly into what the NFT itself contributes not just storage, but the actual basis on which a credential can claim to be authentic [9]. Aung and Thein have two papers worth noting from 2024: one on NFT-based certificates and proof-of-delivery on Ethereum [7], and a follow-up comparing Ethereum against Polygon for the same purpose, concluding that Layer-2 networks cut cost enough to matter for anything beyond a small pilot [8]. Utsahawattanasuk, Mahapakulchai, and Jariyanorawiss tested an NFT-based approach against a real case the GSPP certificate program at Kasetsart University's Graduate School which is useful simply because it shows the idea surviving contact with an actual institution [10].

C. Identity, Privacy, and Self-Sovereign Models

A separate thread cares less about how minting works mechanically and more about who actually controls the credential afterward. Linn, Myat, Naing, Zaw, Min, Aung, and Mon describe verifiable credentials and skill endorsements built into an academic-to-career platform, stretching the idea of a credential past a single static certificate into something more like an evolving, endorsable record [5]. Shidaganti, Manojkumar, Bathinanna, and Gouda push privacy further still, bringing in zero-knowledge proofs so a holder can prove they have a qualification without exposing the document or any personal detail at all a noticeably stronger guarantee than a plain hash comparison [11].

Cheikhrouhou, Turki, Kallel, Abid, and Jmaiel pair self-sovereign identity with off-chain caching, cutting down both privacy exposure and the delay of repeated verification lookups on the same credential a useful reminder that privacy and performance aren't necessarily in tension [21]. Vardhan, Hiranayachatri, Lele, and Tewari go a different direction entirely, building a blockchain-native PKI for X.509 certificates on the XRP Ledger, which is a useful counterpoint to the Ethereum-only framing most of this literature defaults to [28].

D. GDPR and Regulatory Fit

Blockchain's immutability sits awkwardly against a data subject's right to be forgotten, and a growing slice of the literature treats that tension head-on rather than as something to patch later. Delgado-von-Eitzen, Fernández-Iglesias, and Anido-Rifón present a GDPR-compliant architecture for credential verification where data protection is part of the design from the start, not bolted on afterward [29]. The same group, joined by Ruiz-Molina, followed up with a qualitative look at how such a system is actually received by institutions and users under the GAVIN project — one of the few papers here that studies adoption attitudes rather than only the architecture [30].

Alj, Akkaoui, and Alj look at verification and revocation through a Moroccan case study, making the point that these data-protection concerns aren't confined to the EU and that revocation gets treated as a regulatory necessity rather than a nice-to-have in serious deployments [12]. Soares, Wibowo, and Anwar approach the question legally rather than technically, analyzing an NFT-based digital vaccine certificate used in international trade — the cross-border recognition problem they describe maps fairly directly onto the same problem facing academic credentials issued in one country and checked in another [16].

E. Verification Speed, Revocation, and Robustness

Another cluster cares less about the conceptual framing and more about whether verification actually holds up at scale. Ramya, Logeswari, Sri, Sakthivel, and Esaiyaazhini propose a PBFT-enhanced framework aimed specifically at keeping verification fast and reliable under transaction volumes well beyond a typical pilot [23]. Priyadarshini, Pandey,

Ankit, Bhandari, Khadka, Barik, and Saikia, in IEEE Access, build an integrated system that checks not just the certificate but the issuer to a distinct and often-skipped problem of confirming the issuing party is actually a legitimate institution [25].

Kučak, Hrgović, and Juričić look at something most papers skip entirely: how a verification system behaves on genuinely limited hardware, which matters a lot for institutions that can't assume high-end infrastructure [27]. Rani, Sachan, and Kukreja describe BT-CNV, a decentralized notarization and verification system built for academic use on a public chain, with particular care given to the notarization step that comes before verification itself [13]. Singh, Maan, Aggarwal, Gupta, and Pandey propose XGENESIS, a hybrid framework blending public and permissioned blockchain elements to balance openness against institutional control [18].

Anandapadmanaban, Umesh, Anilkumar, Das, and Joseph present EduChain, aimed squarely at efficient and secure certificate verification, and Kabir, Hasan, and Islam describe BCVVS, which extends the same tamper-evidence idea to résumé claims rather than just formal degrees [6], [22]. Rahul, Shashank, Maiya, and Annapurna describe a more conventional issuance-and-verification system, useful mainly as a baseline against the more specialized work above [24]. Pratap, Khushi, Khajuria, and Kumar widen the scope again, treating a learner's whole digital portfolio — not just one certificate as something worth securing on-chain [26].

F. Microcredentials and Interoperability

The most recent cluster looks past the single formal degree certificate toward shorter, more granular credentials and the standards needed for different systems to talk to each other. Tanim, Hossain, Saria, and Mansoor, in IET Software, describe a decentralized framework built specifically for microcredentials, on the reasonable grounds that short courses and badges are now institutionally significant enough to need their own approach rather than being forced into a model designed for four-year degrees [15]. Shaumen, Baktybaiuly, Omirgaliyev, and Zhakiyev describe a similar platform presented at the STIoT workshop in Almaty, again working at the level of individual achievements rather than only the final credential [17].

Rustemi and Dalipi, in IET Blockchain, move from

concept toward something closer to practice, focusing on what it actually takes to get a system like this out of the lab and into a university's hands [19]. Limborea, Ștefan, Oprea, and Ciocîrlan describe Demacert, presented at RoEduNet, which treats certificate management as an ongoing institutional process rather than a single issuance event [14].

G. Where This Leaves Us

Put together, this body of work makes a fairly solid case for the underlying idea: certificates anchored to a blockchain whether as a plain hash, a full NFT, or something wrapped in a zero-knowledge proof — are measurably harder to forge and faster to check than their paper or PDF counterparts, across a wide range of implementations. What's less settled is everything around that core idea. GDPR-aligned design shows up in only a handful of papers and is largely missing from the earlier platform-focused work. Revocation gets serious treatment in some systems and isn't mentioned at all in others. Cost is acknowledged almost everywhere as a problem on Ethereum mainnet, with Layer-2 and alternative-chain options only appearing in the more recent papers. And although individual systems are regularly shown to work on their own, very few papers ask whether a credential minted under one system could be recognized by a different, independently built one — interoperability remains the thinnest part of this literature. These are the gaps the proposed system is built to address: ERC-721 minting paired with off-chain IPFS storage, on-chain revocation handled explicitly rather than as an afterthought, and a data-locality separation designed around GDPR's right to erasure from the outset.

III. CONCLUSION

Taken as a whole, the literature points in a fairly clear direction: blockchain- and NFT-based academic credentialing is well past the proof-of-concept stage, and the open questions now are about the details — privacy guarantees, revocation, regulatory fit, transaction cost, and how a system holds up under real institutional load rather than a demo. What's still missing, across the roughly thirty systems and studies covered here, is a single design that treats GDPR-aligned data handling, full lifecycle management including revocation, and low operating cost as equally essential from day one rather than features

added later. The system this paper is building toward is aimed at closing exactly that combination of gaps; its architecture, implementation, and evaluation are reported in a separate paper.

REFERENCES

- [1] Mujezinović, A. Joksimović, D. Kostić, M. Jolović, and M. Simić, "Blockchain-Based Platform for Tracking Students' Achievements," in *Proc. SINTEZA 2025 Int. Sci. Conf. Inf. Technol., Comput. Sci., Data Sci.*, Belgrade, Serbia, 2025, pp. 267–273.
- [2] S. Nikolić, S. Vukmirović, S. Matić, N. Nedić, and D. Čapko, "Development of a Blockchain Based Application for Digital Certificates in Education," in *Proc. 30th Telecommun. Forum (TELFOR)*, Belgrade, Serbia, 2022, pp. 1–4.
- [3] N. Kumawat and D. Naik, "Utilizing NFTs to Revolutionize Document Verification and Authentication through Blockchain: Redefining Trust in the Digital Era," in *Proc. 15th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, IIT Mandi, India, 2024.
- [4] X. Zhao and Y.-W. Si, "NFTCert: NFT-Based Certificates with Online Payment Gateway," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Melbourne, Australia, 2021, pp. 538–543.
- [5] H. P. Linn, A. K. Myat, H. K. Naing, H. M. Zaw, S. M. Min, C. K. K. Aung, and A. C. Mon, "Blockchain-Enabled Verifiable Credentials and Skill Endorsements in an Academic-to-Career Platform," in *Proc. 6th Int. Conf. Adv. Inf. Technol. (ICAIT)*, 2025.
- [6] B. Anandapadmanaban, A. V. Umesh, A. Anilkumar, A. K. Das, and R. B. Joseph, "EduChain: A Blockchain-Based System for Efficient and Secure Certificate Verification," in *Proc. 2nd Int. Conf. Trends Eng. Syst. Technol. (ICTEST)*, 2025.
- [7] M. T. Aung and N. N. M. Thein, "NFT-based Certificates and Proof of Delivery in Education Sector with Ethereum Blockchain," in *Proc. IEEE Conf. Comput. Appl. (ICCA)*, 2024.
- [8] M. T. Aung and N. N. M. Thein, "A Comparative Study of Ethereum and Polygon for Implementing NFT-Based Certification Systems," in *Proc. 5th Int. Conf. Adv. Inf. Technol. (ICAIT)*, 2024.
- [9] G. R. Naik and P. G. Naik, "Role of Non-Fungible

- Tokens in Transforming Academic Credentials for Trust and Transparency,” in Proc. Int. Conf. Emerg. Smart Comput. Inform. (ESCI), Pune, India, 2024.
- [10] P. Utsahawattanasuk, S. Mahapakulchai, and T. Jariyanorawiss, “NFT-Based Verification of Academic Credentials: Case Study for GSPP Certificate, Graduate School, Kasetsart University,” in Proc. Int. Tech. Conf. Circuits/Syst., Comput., Commun. (ITC-CSCC), Bangkok, Thailand, 2024.
- [11] G. Shidaganti, A. Manojkumar, B. Bathinanna, and S. Gouda, “Securing Educational Credentials with Zero-Knowledge Proofs and Blockchain Technology,” in Proc. Int. Conf. Comput. Sci. Inf. Technol. Syst. Services (CSITSS), 2025.
- [12] K. S. Alj, R. Akkaoui, and Y. S. Alj, “A Blockchain-Based Framework for Academic Credential Verification and Revocation: Morocco Case Study,” in Proc. Int. Conf. Intell. Syst. Technol. (CiSt), 2025.
- [13] P. Rani, R. K. Sachan, and S. Kukreja, “BT-CNV: A Distributed and Decentralized Solution for Certificate Notarization and Verification for Academia Using Public Blockchain,” *Peer-to-Peer Netw. Appl.*, vol. 18, no. 60, 2025.
- [14] G. Limborea, M. Ștefan, F. Oprea, and Ș.-D. Ciocîrlan, “Demacert – Decentralised Management of Certifications,” in Proc. 24th RoEduNet Conf.: Netw. Educ. Res. (RoEduNet), 2025.
- [15] A. M. Tanim, M. F. Hossain, H. Saria, and N. Mansoor, “Design and Development of a Blockchain-Enabled Decentralized Framework for Academic Microcredentials,” *IET Software*, vol. 2026, Art. ID 7326873, 2026.
- [16] V. S. Soares, S. G. Wibowo, and S. Anwar, “Legal Analysis of the NFT-Based Digital Vaccine Certificate System in Digital Free Trade: Security, Privacy, and International Recognition Aspects,” *Indonesian Cyber Law Rev.*, vol. 2, no. 2, pp. 107–127, 2025.
- [17] A. Shaumen, A. Baktybaiuly, R. Omirgaliyev, and N. Zhakiyev, “Development of a Decentralized Platform for Managing and Verifying Educational Achievements,” in Workshop Smart Technol. IoT (STIoT 2025), Almaty, Kazakhstan, 2025.
- [18] R. Singh, P. Maan, M. Aggarwal, R. Gupta, and A. Pandey, “XGENESIS: A Hybrid Blockchain Framework for Secure and Scalable Credential Verification,” in Proc. IEEE Conf. Blockchain Credential Verification Syst., 2025.
- [19] A. Rustemi and F. Dalipi, “From Concept to Practice: A Blockchain-Based Solution for Secure and Efficient Academic Credentials in Higher Education,” *IET Blockchain*, vol. 6, Art. no. e70030, 2026.
- [20] D. Kostić, A. Joksimović, K. Radovanov, M. Muljajić, S. Košević, and T. Naumović, “Decentralized Platform for Issuing and Verifying Student Achievements,” Univ. of Belgrade, Serbia, 2025.
- [21] S. Cheikhrouhou, M. Turki, S. Kallel, A. Abid, and M. Jmaiel, “Blockchain-Powered Certificate Verification Enhanced by Self-Sovereign Identity and Off-Chain Caching,” in Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), 2025.
- [22] M. H. Kabir, R. Hasan, and M. S. Islam, “BCVVS: Blockchain-Based CV Verification System for Secure and Tamper-Proof Credential Validation,” in Proc. 28th Int. Conf. Comput. Inf. Technol. (ICCIT), Cox's Bazar, Bangladesh, 2025.
- [23] R. M. Ramya, M. Logeswari, S. R. Sri, K. Sakthivel, and C. K. Esaiyaazhini, “A PBFT-Enhanced Blockchain Framework for Secure and Efficient Certificate Verification,” in Proc. IEEE Int. Conf. AI Eng. Innov. (AIEI), 2026.
- [24] Rahul, S. Shashank, U. A. Maiya, and A. D. Annapurna, “Block-Chain Based Certificate Issuance Verification,” in Proc. 3rd Int. Conf. Recent Adv. Inf. Technol. Sustain. Dev. (ICRAIS), 2025.
- [25] R. Priyadarshini, R. Pandey, K. C. Ankit, D. Bhandari, B. Khadka, R. K. Barik, and M. J. Saikia, “A Faster, Integrated, and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain,” *IEEE Access*, vol. 13, pp. 27037–27050, 2025.
- [26] P. Pratap, Khushi, D. Khajuria, and A. Kumar, “Secure and Verifiable Credentials of Digital Portfolio Using Blockchain,” in Proc. Int. Conf. Blockchain Web3 Technol., 2025.
- [27] D. Kučak, B. Hrgović, and V. Juričić, “Implementation of Blockchain-Based System for Academic Certificate Verification on Device

with Limited Resources,” in Proc. 13th Int. Conf. Inf. Educ. Technol. (ICIET), 2025.

- [28] H. Vardhan, P. Hiranayachatri, A. Lele, and H. Tewari, “A Blockchain-Native PKI: Secure X.509 Certificate Management on the XRP Ledger,” in Proc. IEEE Int. Conf. Distrib. Ledger Technol. (ICDLT), 2025.
- [29] C. Delgado-von-Eitzen, M. J. Fernández-Iglesias, and L. Anido-Rifón, “A GDPR-Compliant Blockchain Architecture for the Verification of Educational Credentials: Design, Implementation, and Evaluation,” SSRN Electronic Journal, 2025.
- [30] C. Delgado-von-Eitzen, L. Anido-Rifón, M. J. Fernández-Iglesias, and M. Ruiz-Molina, “Qualitative Analysis of a Blockchain-Based System Adoption for Academic Credentials Verification That Complies with the GDPR: GAVIN Project,” Applied Sciences, vol. 15, no. 22, Art. no. 11958, 2025.