A Blockchain and IPFS-Based Smart Contract Framework for Preventing Certificate Fraud in Academia

Ezra Natanael
Department of Information Systems
Soegijapranata Catholic University
Semarang, Indonesia
ezrantn@proton.me

Ridwan Sanjaya
Department of Information Systems
Soegijapranata Catholic University
Semarang, Indonesia
ridwan@unika.ac.id

Erdhi Widyarto Nugroho
Department of Information Systems
Soegijapranata Catholic University
Semarang, Indonesia
erdhi@unika.ac.id

***Abstract*—This innovative initiative aims to enhance the academic credential verification process by establishing a decentralized platform specifically designed for educational institutions to issue diplomas. By leveraging blockchain technology, this platform will empower students to securely store their academic credentials in a manner that is both accessible and tamper-proof. Furthermore, it will help employers effortlessly validate the qualifications of potential candidates, thereby streamlining the hiring process. The overarching goal of this initiative is to bolster the reliability and transparency of academic achievements, thereby fostering greater trust among stakeholders in the educational ecosystem and contributing to a more efficient labor market.**

***Index Terms*—blockchain, decentralized verification, credential fraud prevention, verification systems, education**

I. Introduction

Effectively managing student and graduate records is imperative for ensuring accuracy, accessibility, and security within the educational landscape. Traditional centralized systems often reveal significant limitations, including inefficiencies and vulnerabilities that can compromise data integrity. As such, there is an increasing necessity for innovative digital verification methods. These advancements enhance the reliability of record-keeping and facilitate easier access for stakeholders, thereby fostering a more streamlined and secure educational environment [1].

In recent years, the issue of counterfeit diplomas and transcripts has gained considerable attention. In 2019, Nuril Furkan underscored the growing threat of fraudulent academic credentials—especially during general elections—emphasizing the urgent need for stringent verification processes [2]. Proactively addressing this issue allows universities to safeguard their academic integrity, enhance student learning experiences, and foster a culture of trust.

Blockchain technology establishes a decentralized framework that guarantees the integrity and immutability of data by employing robust cryptographic techniques. This ensures secure transactions and fosters trust among participants in various digital ecosystems [3].

Blockchain technology and IPFS provide a robust framework for decentralized and secure solutions, ensuring that certificate verification is robust and trustworthy, enhancing transparency and reliability for all users. IPFS provides a way to store data in a decentralized manner [4]. It brings promise and difficulty for the systems that will come after it. This innovative approach ensures enhanced security and decentralization, empowering users with greater control over their credentials. By leveraging both technologies' strengths, the system aims to facilitate a seamless and user-friendly experience, thereby revolutionizing the landscape of credential verification processes.

Blockchain has evolved beyond cryptocurrencies, enabling innovative solutions in various industries and enhancing transparency and trust. This technology is applicable across various sectors, including supply chain management and healthcare, due to its inherent capabilities in secure data storage and management [5]. This versatility positions blockchain as an ideal solution for applications demanding high levels of trust and transparency.

The InterPlanetary File System significantly boosts the safety and accessibility of digital credentials by utilizing decentralized storage, ensuring that sensitive information is protected while remaining easily accessible to authorized users, as shown in Fig. 1. Improving data integrity involves reducing vulnerabilities within centralized systems and carefully controlling access, ensuring that sensitive information remains secure and trustworthy for all users [6].

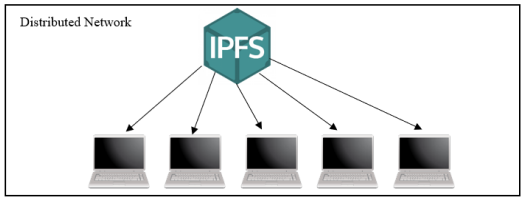

Fig. 1: IPFS Distributed Network

This research comprehensively analyzes Blockchain and InterPlanetary File System (IPFS) architectures, aiming to propose a robust framework. This framework is designed to significantly enhance the security and reliability of academic data management and dissemination in the digital landscape.

In Indonesia, the online diploma verification system SIVIL was introduced in 2017 to combat the persistent issue of counterfeit diplomas and transcripts [2]. Despite these efforts, challenges remain, underscoring the need for continuous improvements in verification processes and greater

public awareness regarding the authenticity of academic records.

Recent implementations of blockchain-based verification systems—such as those by Kanan et al. at Al-Zaytoonah University and by Cheng et al.—demonstrate the potential of this technology to streamline and secure academic credentialing. These innovative approaches reduce fraud risks and enhance trust in educational qualifications, offering a promising path forward for institutions globally [7], [8].

II. Problem Statement

The subsequent problem statements delineate the principal challenges that underscore the necessity for such a system. As digital transformation intensifies, the demand for secure and efficient credential verification has become increasingly pressing. Traditional systems that depend on centralized authorities are often characterized by slow processing times, high costs, and susceptibility to fraud, rendering the validation of educational qualifications both inefficient and unreliable. In this context, blockchain technology—renowned for its transparency and immutability—emerges as a promising solution to these challenges. It offers a decentralized, secure, and tamper-resistant platform for credential verification.

We propose harnessing the power of blockchain smart contracts in conjunction with IPFS to create a decentralized system that enhances transparency and security in transactions. Secure storage of digital content while ensuring robust traceability. By embedding IPFS hashes within smart contracts, we enable seamless access to documents through their unique hashes. This approach enhances the integrity of the content and ensures that any alterations made to the original material are immediately reflected through a corresponding change in the hash. Consequently, this mechanism provides a reliable audit trail, fostering trust and accountability in digital content management [9].

This research investigates the potential of blockchain to fundamentally alter the diploma verification process, enhancing security, accessibility, and efficiency for all stakeholders involved.

1) Escalating Diploma Fraud: Fake diplomas and mark sheets are deceitful documents that undermine the value of genuine education [10]. Conventional mechanisms for verifying educational credentials are susceptible to manipulation, making counterfeit diplomas and credentials challenging to differentiate from authentic ones. The pervasive problem of tampering and forgery in certificate issuance and accreditation significantly impacts developing countries. This undermines the integrity of educational and professional qualifications, creating barriers for individuals seeking employment and recognition, ultimately stunting economic growth and perpetuating cycles of inequality within these nations [11].
2) Inefficiencies in Conventional Verification Systems: Existing verification methodologies frequently depend on centralized authorities or intermediary services, which may lead to protracted processing times, elevated costs, and susceptibility to human error [12]. Such inefficiencies contribute to processing delays, increased verification expenses, and a general deficiency in responsiveness, particularly when verifying credentials across international borders.
3) Insufficient Transparency and Security: Numerous current systems fail to offer clear insights into the methods used to organize and preserve academic records effectively. Without a secure and immutable verification process, there is a significant risk of data alteration or loss [13]. This security deficiency raises concerns for educational institutions and employers, who necessitate dependable evidence of academic accomplishments.
4) Restricted Accessibility: Conventional verification systems often restrict access to academic records, necessitating the involvement of intermediaries or third-party services [14]. This introduces additional procedural steps and obstacles for employers and students, complicating individuals' ability to obtain and manage their credentials. Consequently, this limitation can impede prompt verification processes and adversely affect career advancement.
5) Excessive Expenses and Risks Associated with Data Mismanagement: Centralized verification systems frequently entail substantial operational expenditures, particularly for institutions overseeing extensive collections of academic records. Furthermore, such systems are prone to data mismanagement, breaches, and security vulnerabilities, which can compromise sensitive student information and expose it to unauthorized access or exploitation. In contrast, a decentralized, blockchain-based framework has the potential to alleviate these concerns by lowering costs and enhancing the security and management of sensitive educational data [15].

III. Objectives

The old ways of checking credentials have their flaws. They are slow and often lead to doubt. We need something better, something that is secure and clear. Blockchain technology stands out. It offers a way to keep records that cannot be changed, and it allows everyone to see them. This research uses blockchain and IPFS to create a system that builds trust in verifying educational credentials. By combining these technologies, the aim is to cut down on fraud in academic certificates, storing them as unchangeable digital assets [16].

Before delving into the research questions, it is imperative to critically evaluate the applicability of blockchain technology within the realm of education. As highlighted by Tapscott and Kaplan (2018) [17], understanding the potential advantages and challenges associated with blockchain integration can provide valuable insights. This foundational consideration will ultimately guide the exploration of its transformative capabilities in educational contexts.

Many students encounter significant challenges in leveraging blockchain technology for personal and professional development despite its considerable potential to bolster the security of identity-related data. This difficulty is

compounded by the increasing shift toward decentralized ownership of credentials, which necessitates that students cultivate digital literacy and a robust set of technical skills for proficiently using blockchain wallets. To bridge this knowledge gap, educational institutions and policymakers must prioritize initiatives integrating blockchain education into curricula. Such initiatives include the development of specialized courses, workshops, and hands-on training programs that familiarize students with blockchain applications. By fostering a comprehensive understanding of this transformative technology, institutions can effectively empower students to navigate the evolving landscape of digital identity and credentialing, ultimately enhancing their prospects for future success [18].

The subsequent objectives delineate how this proposed system will confront the identified challenges and improve the verification process.

1) Addressing Diploma Fraud: This research proposes implementing a blockchain-based framework aimed at diminishing the incidence of diploma fraud through the assurance of the authenticity of educational credentials. By capitalizing on the inherent properties of blockchain, specifically its immutability and transparency, the proposed system guarantees that once a diploma is conferred, it remains unalterable and resistant to counterfeiting. This innovation offers a robust mechanism for the verification of educational qualifications.
2) Enhancing Verification Efficiency: To address the shortcomings inherent in conventional verification systems, we propose developing a decentralized platform that obviates the necessity for centralized authorities or intermediary services. This innovation facilitates expedited, real-time validation of academic credentials, thereby markedly diminishing delays and associated expenditures.
3) Enhancing Transparency and Security: The proposed system revolutionizes how we handle diploma records by harnessing the power of blockchain technology. This innovative approach ensures that all educational credentials are not only secure but also transparent and easily verifiable by independent parties. By creating an immutable record of diplomas, the system significantly reduces the risk of fraud, building a solid framework that strengthens the value of education and inspires trust in employers and institutions.
4) Enhancing Accessibility: Our initiative seeks to augment the accessibility of educational records by permitting students to submit their credentials securely and enabling employers to verify these qualifications directly. The system's decentralized architecture ensures that credentials are readily available to all stakeholders, eliminating the need for intermediaries and promoting more efficient and expedient access to verified qualifications.
5) Cost Reduction and Mitigation of Data Mismanagement: To decrease operational expenses and address the risks associated with data mismanagement, we advocate for implementing a blockchain-based framework that lessens dependence on centralized infrastructure. This approach not only reduces verification costs but also diminishes the likelihood of unauthorized access or misuse of sensitive academic data, thereby enhancing control and security for all stakeholders involved.

IV. Theoretical Foundation

This chapter provides a comprehensive overview of the foundational technologies that support decentralized degree verification systems. It examines blockchain's immutable ledger capabilities, the decentralized storage mechanism of the InterPlanetary File System (IPFS), and the interoperability of the Binance Smart Chain (BSC) network.

Blockchain technology represents a revolutionary advancement in data management by utilizing a distributed ledger system that guarantees secure, immutable, and transparent data storage across a decentralized network [19]. This paradigm shift is characterized by its fundamental features: immutability, transparency, and decentralization, features that collectively uphold data integrity while eliminating the need for centralized intermediaries. Once information is recorded on a blockchain, it becomes resistant to unauthorized alterations—a crucial safeguard that reduces the likelihood of credential fraud, particularly in academic contexts [19].

The immutable nature of blockchain ensures that once a credential is validated and added to the ledger, it cannot be altered or deleted, thereby preserving its authenticity over time [20]. Additionally, the transparent framework of blockchain enables various stakeholders, such as employers and educational institutions, to independently verify the accuracy of academic qualifications. This independence not only enhances trust but also streamlines the verification process, fostering a more efficient system of credentialing that benefits both job seekers and hiring organizations.

In the realm of decentralized diploma verification, the InterPlanetary File System (IPFS) is preferred over conventional cloud platforms, such as Amazon Web Services (AWS) or Google Cloud Platform (GCP), because it adheres to the foundational principles of decentralization and trustless systems. In contrast to centralized cloud service providers that retain authority over data storage and access, IPFS offers a more distributed and autonomous approach to data management.

IPFS is a peer-to-peer distributed file system that allows data to be stored and accessed in a decentralized manner, overcoming the drawbacks of centralized systems such as single points of failure and arbitrary control [21]. Pinata is a service that facilitates the use of IPFS by providing an easier interface to upload and manage data in IPFS [22]. The implemented system utilizes the InterPlanetary File System (IPFS) protocol to securely upload users' academic degrees, which are subsequently stored via the Pinata platform.

A significant advantage of the InterPlanetary File System (IPFS) is its implementation of content-addressable storage, whereby each file is designated by a unique cryptographic

hash [23]. This mechanism offers a reliable guarantee of data integrity, as any alteration to the file will result in a distinct hash value, thus facilitating the immediate detection of any tampering. In contrast, centralized platforms employ location-based addressing for data storage, a strategy that does not inherently validate the authenticity of the content.

Binance Smart Chain (BSC) is a blockchain infrastructure specifically engineered to facilitate the creation of decentralized applications (DApps), prioritizing high transaction throughput and minimal transaction costs. BSC is frequently evaluated alongside other blockchain networks, including Ethereum, Solana, and Cardano, with respect to various parameters such as transaction velocity, scalability, fee structures, and community engagement [24]. Binance Smart Chain (BSC) is recognized for its superior transaction speeds and reduced fees in comparison to Ethereum, rendering it a compelling alternative for decentralized applications (DApps) that necessitate a high volume of transactions with minimal user intervention [24].

Binance Smart Chain (BSC) operates on a dual-chain architecture that is designed to balance high performance with smart contract capabilities. This structure consists of two parallel blockchains—Binance Chain (BC) and Binance Smart Chain (BSC)—which function independently but are tightly coupled through a cross-chain communication mechanism as shown in Fig. 2. This design enables developers and users to benefit from both high-speed trading and flexible smart contract functionalities.

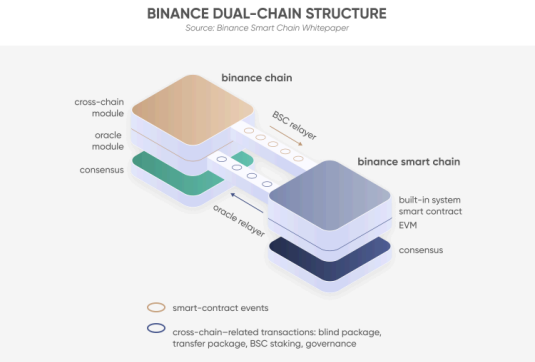

Fig. 2: Binance Smart Chain Architecture

Binance Chain (BC) facilitates high-speed asset transfers and decentralized trading but does not support complex smart contracts. Binance Smart Chain (BSC). The two chains communicate through cross-chain modules using BSC and oracle relayers, enabling token transfers, staking, governance, and other interactions. This architecture balances performance and flexibility, making it suitable for applications like academic credential verification that require both scalability and cost efficiency.

Although Binance Smart Chain (BSC) provides advantages in terms of cost efficiency and transaction speed, these benefits are attained at the cost of a diminished degree of decentralization. In comparison to other blockchain platforms, such as Cardano and Polkadot, BSC exhibits a comparatively lower level of decentralization [25]. This trade-off is deemed acceptable within the context of this research. The system places greater emphasis on efficiency, accessibility, and cost-effectiveness rather than on achieving maximal decentralization. The primary objective is to establish a verifiable, tamper-resistant, and scalable platform for the credentialing of academic qualifications.

It is important to highlight that the Binance Smart Chain (BSC) has functioned as a platform for a range of token-related activities, several of which have elicited ethical considerations, including phenomena such as "rug pulls" and the utilization of high-frequency trading algorithms, exemplified by sniper bots [26]. These challenges reveal specific vulnerabilities within the Binance Smart Chain (BSC) ecosystem. Nevertheless, when considering non-financial assets such as diploma credentials—where speculative trading is absent—the potential for exploitation is considerably diminished. Additionally, the implementation of comprehensive smart contract audits can further alleviate these risks.

The decision to utilize Binance Smart Chain (BSC) for this research is primarily influenced by its capacity to deliver high transaction throughput and cost efficiency—qualities that are critical for a diploma verification system, which is likely to involve numerous on-chain interactions.

A notable advantage of Binance Smart Chain (BSC) lies in its compatibility with the Ethereum Virtual Machine (EVM), enabling developers to leverage existing Ethereum-based smart contracts and tools. This interoperability not only accelerates development but also promotes adherence to established standards for credential issuance and verifications [27]. This compatibility not only expedites the development process but also enhances the incorporation of widely recognized standards for the issuance and verification of credentials.

References

[1] Y. Shakan, B. Kumalakov, G. Mutanov, Z. Mamykova, and Y. Kistaubayev, "Verification of University Student and Graduate Data using Blockchain Technology," *INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL*, vol. 16, p. , 2021, doi: 10.15837/ijccc.2021.5.4266.

[2] N. Chaniago, P. Sukarno, and A. Wardana, "Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 7, p. 149, 2021, doi: 10.26594/register.v7i2.1959.

[3] P. Ocheja, F. Agbo, S. Oyelere, B. Flanagan, and H. Ogata, "Blockchain in Education: A Systematic Review and Practical Case Studies," *IEEE Access*, p. 1, 2022, doi: 10.1109/ACCESS.2022.3206791.

[4] T. V. Doan, Y. Psaras, J. Ott, and V. Bajpai, "Toward Decentralized Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations," *IEEE Internet Computing*, vol. 26, no. 6, pp. 7–15, 2022, doi: 10.1109/MIC.2022.3209804.

[5] R. Chatterjee and R. Chatterjee, "An Overview of the Emerging Technology: Blockchain," 2017, p. . doi: 10.1109/CINE.2017.33.

[6] N. Patil, Y. Mane, A. Vasoya, A. Agrawal, and S. Raut, "Secure File Sharing Using Blockchain and IPFS with Smart Contract-Based Access Control," *Journal of Information Systems Engineering & Management*, p. , 2025.

[7] T. Kanan, A. T. Obaidat, and M. Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019, pp. 629–633. doi: 10.1109/JEEIT.2019.8717505.

[8] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE International Conference on*

Applied System Invention (ICASI), 2018, pp. 1046–1051. doi: 10.1109/ICASI.2018.8394455.

[9] N. Nizamuddin, H. Hasan, and K. Salah, "IPFS-Blockchain-Based Authenticity of Online Publications," 2018, pp. 199–212. doi: 10.1007/978-3-319-94478-4_14.

[10] M. Sheikh, "ORICERT – FRAUDULENT DEGREE AND MARKSHEET DETECTION," *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, 2024, doi: 10.55041/ijsrem30071.

[11] Z. A. Shaikh *et al.*, "A Blockchain Hyperledger and Non-Linear Machine Learning: A Novel and Secure Educational Accreditation Registration and Distributed Ledger Preservation Architecture," *Applied Sciences*, 2022, doi: 10.3390/app12052534.

[12] N. Bhuvaneswary, J. Deny, and A. Lakshmi, "Hybrid Optimized Verification Methodology using Deep Reinforcement Neural Network," *J. Intell. Fuzzy Syst.*, vol. 45, pp. 3715–3728, 2023, doi: 10.3233/jifs-232132.

[13] A. Goyal, D. Pushpendra, and K. Verma, "Blockchain for Academic Integrity Preventing Fraud and Enhancing Transparency in Education," *Advances in Nonlinear Variational Inequalities*, 2024, doi: 10.52783/anvi.v28.2853.

[14] D. V. S. Castillo, C. N. B. Co, K. G. R. Maranan, D. J. Quinio, and J. Pedrasa, "Creducate: Blockchain-based Academic Record Management and Verification System Built in the Solana Network," *TENCON 2022 - 2022 IEEE Region 10 Conference (TENCON)*, pp. 1–6, 2022, doi: 10.1109/TENCON55691.2022.9977896.

[15] N. Nousias, G. Tsakalidis, G. Michoulis, S. Petridou, and K. Vergidis, "A process-aware approach for blockchain-based verification of academic qualifications," *Simul. Model. Pract. Theory*, vol. 121, p. 102642, 2022, doi: 10.1016/j.simpat.2022.102642.

[16] S. A. Sultana, R. Chiramdasu, R. P. Malleswari, and T. Gadekallu, "IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field," *Inf.*, vol. 14, p. 446, 2023, doi: 10.3390/info14080446.

[17] C. Banga and F. Ujager, "Blockchain Revolution in Education and Lifelong Learning," 2023, pp. 131–154. doi: 10.4018/979-8-3693-0405-1.ch006.

[18] M.-F. Steiu, "Blockchain in education: Opportunities, applications, and challenges," *First Monday*, p. , 2020, doi: 10.5210/fm.v25i9.10654.

[19] R. Beck, M. Avital, M. Rossi, and J. Thatcher, "Blockchain Technology in Business and Information Systems Research," *Business & Information Systems Engineering*, vol. 59, pp. 381–384, 2017, doi: 10.1007/s12599-017-0505-1.

[20] U. Rahardja, A. Hidayanto, P. Putra, and M. Hardini, "Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol," *Journal of Applied Research and Technology*, 2021, doi: 10.22201/icat.24486736e.2021.19.4.1046.

[21] E. Politou, E. Alepis, C. Patsakis, F. Casino, and M. Alazab, "Delegated content erasure in IPFS," *Future Gener. Comput. Syst.*, vol. 112, pp. 956–964, 2020, doi: 10.1016/j.future.2020.06.037.

[22] R. Vaidya, A. Tembhurnikar, C. Mohite, S. Puri, S. Kulkarni, and A. Buchade, "Blockchain-Powered Certificate Authentication: Enhancing Trust and Transparency," *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, pp. 1–5, 2024, doi: 10.1109/ICBDS61829.2024.10837062.

[23] T. Doan, Y. Psaras, J. Ott, and V. Bajpai, "Toward Decentralized Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations," *IEEE Internet Computing*, vol. 26, pp. 7–15, 2022, doi: 10.1109/MIC.2022.3209804.

[24] J. Gjorgjev, N. Sejfuli-Ramadani, V. Angelkoska, P. Latkoski, and A. Risteski, "Use Cases and Comparative Analysis of Blockchain Networks and Layers for DApp Development," *2024 13th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–5, 2024, doi: 10.1109/MECO62516.2024.10577885.

[25] Y. Jia, C. Xu, Z. Wu, Z. Feng, Y. Chen, and S. Yang, "Measuring Decentralization in Emerging Public Blockchains," *2022 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 137–141, 2022, doi: 10.1109/iwcmc55113.2022.9825341.

[26] F. Cernera, M. L. Morgia, A. Mei, and F. Sassi, "Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens in Ethereum and in the Binance Smart Chain (BNB)," pp. 3349–3366, 2022.

[27] Monika and R. Bhatia, "Cross-blockchain decentralized asset transfer protocol for public blockchains," *International Journal of Communication Systems*, vol. 37, 2024, doi: 10.1002/dac.5709.