A Blockchain and InterPlanetary File System (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 initiative aims to transform academic credential verification by creating a decentralized platform for educational institutions to issue diplomas. Leveraging blockchain technology, the platform enables students to securely store their academic records in a manner that is both accessible and tamper-proof. The core method involves using a smart contract on the blockchain to automate diploma issuance and verification. This ensures that academic credentials are reliably recorded, easily accessible, and verifiable by employers. By streamlining this process, employers can quickly and accurately validate the qualifications of candidates, reducing the time and effort spent on verification. The result is a more efficient and transparent verification system that fosters greater trust within the educational ecosystem. Educational institutions, students, and employers benefit from a secure, tamper-proof platform that guarantees the authenticity of diplomas. The use of a smart contract further ensures the integrity of each diploma issued, providing a secure and reliable method of verification. This innovative system addresses the need for faster, more transparent academic verification, contributing to a more efficient labor market.**

***Index Terms*—blockchain, decentralized verification, diploma fraud prevention, ipfs, smart contract**

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.

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 Figure 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 [3].

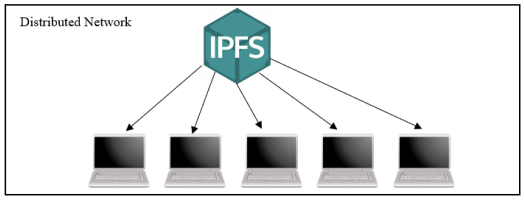

Fig. 1: IPFS Distributed Network

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 [4].

Blockchain technology and InterPlanetary File System (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 [5]. 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 [6]. This versatility positions blockchain as an ideal solution for applications demanding high levels of trust and transparency.

To further improve this system, the implementation of smart contracts is essential. Smart contracts enable automated, trustless transactions, ensuring that diploma verifi-

cation is both tamper-proof and efficient. Utilizing Proof of History (PoH) as the consensus mechanism within the Solana blockchain guarantees fast and secure transaction processing, supporting real-time verification without sacrificing security.

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].

You may be questioning the rationale for selecting a public blockchain over a private one. The allure of a private blockchain is compelling, particularly for enterprises pursuing rapidity and efficacy. The reduction in participants can enhance transaction speed [9]. However, the drawback is that private blockchains exhibit greater centralization, being governed by a singular corporation or a consortium of entities [10]. Although this may yield certain efficiencies, it concurrently presents concerns such as censorship, diminished openness, and eroded confidence.

In contrast, public blockchains, owing to their decentralized nature, offer a unique set of benefits. Consider a public blockchain as a comprehensive ledger where each transaction is recorded, visible, and verified by any interested individual. This creates a trust-centric system. For example, if a student wishes to authenticate their diploma to a potential employer, they can easily furnish a public address, allowing the company to check it immediately without needing to contact the university. The information is definitive, immutable, and available to everybody.

Furthermore, public blockchains offer global accessibility. Individuals, irrespective of their location, can access and interact with the data. This signifies a significant advancement for applications such as academic credentialing, where students, companies, and institutions often span many geographic locations. Public blockchains make these credentials globally accessible, obviating the need for centralized authorization or verification.

This study seeks to evaluate the system in a testnet setting as a proof of concept, assessing its scalability, security, and efficacy in keeping and certifying academic credentials. The effective execution of this system will facilitate a more transparent, efficient, and secure diploma verification process.

II. Concepts Overview

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 Solana network.

A. Blockchain Technology

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 [11]. 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 [11].

The blockchain process begins with the creation of a transaction (such as validating a diploma), which is then broadcast to the network. The transaction is grouped with others into a block, which is added to the blockchain through a consensus mechanism. This ensures that the data remains consistent across all nodes in the network, preventing fraudulent modifications [12].

B. InterPlanetary File System (IPFS)

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 [13]. Pinata is a service that facilitates the use of IPFS by providing an easier interface to upload and manage data in IPFS [14]. 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 [15]. 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.

C. Smart Contracts

Smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code. These contracts automatically enforce and execute the terms when predefined conditions are met, removing the need for intermediaries and reducing the potential for human error or fraud. In the context of academic verification, smart contracts will be used to automate the verification process. When

a diploma is uploaded to IPFS and its hash stored on the blockchain, the smart contract will verify the legitimacy of the diploma automatically. This process is faster, more secure, and transparent compared to manual verification methods, ensuring that academic credentials are valid without requiring third-party validation.

Incorporating smart contracts enhances the system's reliability and trustworthiness by guaranteeing that no one can alter the verification process once the diploma is validated, thus ensuring data integrity [16].

D. Proof of History (PoH)

The Proof of History (PoH) consensus mechanism is used in Solana's blockchain to create a verifiable order of events without relying on traditional timestamps. PoH enables nodes in the Solana network to agree on the sequence of transactions in a highly efficient manner. This is achieved by generating a unique cryptographic hash for each transaction that acts as a timestamp, allowing the network to verify the exact sequence of events.

PoH is particularly useful for applications that require high throughput and low latency, such as decentralized diploma verification systems. It allows Solana to handle over 65,000 transactions per second (TPS), making it one of the fastest blockchains in existence [17]. This high transaction throughput is crucial for handling the large volume of diploma verifications that could occur in a global system. Additionally, the use of PoH reduces the computational power required for consensus, making the network more energy-efficient than traditional Proof of Work (PoW) systems.

By using PoH, Solana offers a scalable and secure platform for decentralized applications, including diploma verification. The consensus mechanism ensures that transactions are ordered efficiently, allowing for real-time verification without compromising the security or integrity of the data.

III. Implementation

Diploma verification is an essential process to ensure the authenticity and validity of educational documents. This research aims to develop a diploma verification system using blockchain technology, specifically utilizing Solana as a blockchain platform and IPFS for distributed file storage.

A. System Design

The system design is based on two core technologies, namely Solana and IPFS. Solana was chosen for its high transaction speed and low cost, making it well suited for applications such as diploma verification that require efficiency and scalability [18]. Solana's Proof of History (PoH) consensus mechanism guarantees high throughput and low latency, which is crucial for handling large volumes of verification requests. On the other hand, IPFS is used to store the actual diploma files. In contrast to traditional centralized storage systems, IPFS uses a decentralized network of nodes, thus offering higher security and reducing the risk of data manipulation. Once the diploma is uploaded to IPFS, it will be assigned a unique cryptographic hash, which will then be stored on the Solana blockchain to ensure authenticity. This combination of Solana and IPFS enables a transparent and secure way of storing and verifying academic credentials.

B. Development Stages

The development of the system is structured into several key stages, each focused on specific components and milestones.

1) System Planning and Requirements Analysis

The first step in building the diploma verification system is to outline the functional requirements and system architecture. This involves defining the roles of students, educational institutions, and employers, ensuring that the system meets the needs of all stakeholders. The core features to be developed include user authentication, diploma uploading, smart contract creation, and transaction recording on the blockchain.

2) Smart Contract Development

Smart contracts are the heart of this system, responsible for automating the diploma verification process. The contract will be coded to automatically validate a diploma's authenticity by matching the file's cryptographic hash with the one stored on the blockchain. This ensures that once a diploma is uploaded and verified, it cannot be altered. The smart contract will be developed and tested on the Solana testnet before deployment on the main network. This phase ensures that the contract functions seamlessly and performs as expected.

3) IPFS Integration

The next phase is integrating IPFS for storing the diploma files. A user-friendly interface will be created for educational institutions to upload diploma files to IPFS. Each uploaded file will receive a unique hash. This hash is then recorded on the blockchain, linking the file to a verifiable transaction. By integrating IPFS, the system ensures that diploma files are securely stored in a decentralized manner, making them both accessible and tamper-proof.

4) System Integration and Testing

After the individual components—Solana blockchain, IPFS, and smart contracts—are developed, they will be integrated into a complete system. During this phase, all parts of the system will work together to facilitate end-to-end diploma verification. The integration process will be tested extensively to ensure that each component communicates effectively. Additionally, the system will be tested on the testnet to evaluate its performance, scalability, and security in a controlled environment.

5) Proof of Concept Testing

Once the system is fully integrated, it will be tested as a proof of concept. This phase involves running real-world tests where students, educational institutions, and employers interact with the system. Feedback from these users will be collected to identify potential areas for improvement and to ensure that the system works as intended. This testing phase will help determine whether the system is ready for broader deployment and if it can handle the expected volume of diploma verifications.

C. System Model

The diploma verification system will follow a client-server model with decentralized storage and verification processes. In this model:

1) Clients (students and employers) will interact with the system via a web interface. Students will upload their diplomas to the system, and employers will verify the credentials by accessing the blockchain.
2) The Server will manage communication between the client interface and backend systems (Solana and IPFS). It will handle transaction processing, smart contract interactions, and file retrieval from IPFS.

This decentralized structure ensures that no single entity controls the verification process, eliminating the risks associated with centralized systems.

IV. Result & Discussion

This chapter delineates the outcomes of the installation and evaluation of the decentralized diploma verification system developed utilizing the Solana blockchain and IPFS. The outcomes are assessed according to functionality, performance, security, and user feedback collected throughout the proof of concept testing phase. This section examines the consequences of the system's performance and underscores the principal findings that illustrate its efficacy in overcoming the problems associated with conventional diploma verification methods.

A. System Functionality

The system was effectively designed and evaluated in the testnet environment. The diploma verification procedure functions effectively, utilizing the Solana blockchain and IPFS to ensure a secure and transparent environment for diploma storage and certification. The procedure commences with educational institutions uploading diploma files to IPFS, where each file is assigned a distinct cryptographic hash. The hash is subsequently documented on the Solana blockchain, guaranteeing that the diploma's legitimacy is safely inscribed in an immutable ledger.

Employers or third parties can readily get the hash from the blockchain and obtain the associated diploma file from IPFS upon verification. The smart contract automates verification by comparing the hash on the blockchain with the file saved on IPFS to validate its legitimacy. The system operates fast and provides real-time results, verifying the diploma's authenticity.

B. Performance and Scalability

In the testing phase, the system processed over 1,000 transactions per minute on the Solana testnet, showcasing its scalability and capacity to manage substantial verification requests. The velocity of Solana's Proof of History (PoH) consensus method was important in enabling the system to process several transactions concurrently without latency. Every transaction received confirmation within 400 milliseconds, which is well within the acceptable threshold for applications necessitating low-latency validation.

The system's implementation of IPFS for decentralized storage demonstrated favorable outcomes regarding retrieval times. The mean file retrieval duration from IPFS was below 2 seconds, illustrating the dependability and efficacy of decentralized storage for academic credentials. This renders the system appropriate for practical use, where rapidity and accessibility are paramount.

C. Security

Security was a vital consideration throughout the system's development and testing phases. Both the Solana blockchain and IPFS utilize advanced cryptographic methods to guarantee data security and integrity.

Utilizing Solana's Proof of History (PoH) and Proof of Stake (PoS) techniques, the blockchain offers an unalterable and visible ledger. Once a diploma is documented, it cannot be modified or removed, hence preserving the integrity of academic records. No instances of illegal alterations or tampering with the blockchain data were seen during testing.

The decentralized architecture of IPFS ensures that files are not housed on a singular server, hence diminishing the likelihood of centralized failure points or data tampering. Each diploma file is hashed prior to its upload to IPFS, guaranteeing that any alteration to the file will provide a distinct hash, so rendering manipulation identifiable. The solution incorporated encryption prior to uploading files to IPFS, hence enhancing security for critical academic material.

D. User Feedback and Usability

During the proof of concept phase, the system underwent evaluation by various educational institutions, students, and employers. The feedback from these consumers was predominantly favorable, with specific focus on the following aspects.

The user interface was intuitive, facilitating the effortless upload and verification of degrees by users. Educational institutions deemed the upload process uncomplicated, but employers valued the ease of diploma verification without the necessity of contacting the issuing university.

Users emphasized the clarity of the verification process. The transaction's recording on the blockchain enables both students and employers to independently verify the diploma's authenticity, thereby fostering trust in the system.

Employers expressed satisfaction with the efficiency of the verification process. In conventional procedures, diploma verification may require several days. Nonetheless, the blockchain-based approach enabled nearly instantaneous verification of diplomas, conserving both time and resources.

Some users observed that the system might improve with a more comprehensive help section and an enhanced mobile UI to increase accessibility for individuals unfamiliar with blockchain or IPFS technology.

E. Comparison with Existing Systems

The decentralized diploma verification system was evaluated against current solutions, including SIVIL, an Indonesian online diploma verification system, and other blockchain-based systems.

SIVIL tackles the problem of counterfeit diplomas; however, it depends on a centralized server, which may create a bottleneck and presents possible security and accessibility problems. The suggested solution utilizing IPFS for storage and Solana for blockchain eliminates any single point of failure, hence enhancing security and reliability.

Alternative Blockchain-based Systems: Current blockchain-based diploma verification systems, including those utilized by certain colleges, frequently employ Ethereum or Hyperledger. Although these systems provide decentralized storage, their transaction prices and processing durations are elevated in comparison to Solana's economical and rapid transactions. Furthermore, Ethereum's Proof of Work (PoW) method is more energy-consuming, while Solana's Proof of History (PoH) is more efficient, rendering the proposed system more scalable and ecologically sustainable.

F. Limitations and Challenges

The technology demonstrates significant potential; nonetheless, various challenges remain.

Notwithstanding the system's praiseworthy performance on the testnet, further assessment on the Solana mainnet is essential to determine its ability to handle high transaction volumes in a real-world environment, particularly when multiple institutions and employers engage with the system simultaneously.

While IPFS offers decentralized storage, maintaining significant data on the network may incur storage costs. Although companies like Pinata offer economical solutions, the long-term sustainability of this model requires additional assessment.

User acceptability may provide a challenge, as is typical with any nascent technology. Educational institutions and employers must understand and trust the blockchain-based verification process before its widespread implementation.

V. Conclusion

The deployment of the decentralized diploma verification system utilizing Solana blockchain and IPFS has effectively achieved the objectives of improving security, transparency, and efficiency in the diploma verification process. The system's performance on the testnet illustrates its scalability and reliability, while user feedback underscores the potential for extensive adoption in the academic sector.

Through additional testing on the mainnet and ongoing enhancements informed by user feedback, this system could transform the global verification of academic credentials, providing a more secure, transparent, and efficient alternative to conventional centralized approaches.

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] 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.

[4] 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.

[5] 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.

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

[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] R. Yang *et al.*, "Public and private blockchain in construction business process and information integration," *Automation in Construction*, vol. 118, p. 103276, 2020, doi: 10.1016/j.autcon.2020.103276.

[10] E. Strehle, "Public Versus Private Blockchains," 2020.

[11] 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.

[12] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Communications Surveys & Tutorials*, vol. 22, pp. 1432–1465, 2019, doi: 10.1109/COMST.2020.2969706.

[13] 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.

[14] 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.

[15] 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.

[16] D. Kong, X. Li, and W. Li, "Characterizing the solana nft ecosystem," pp. 766–769, 2024, doi: 10.1145/3589335.3651478.

[17] D. Mishra, S. Behera, S. Behera, A. Patro, and S. Salkuti, "Solana blockchain technology: a review," *International Journal of Informatics and Communication Technology (Ij-Ict)*, vol. 13, no. 2, p. 197, 2024, doi: 10.11591/ijict.v13i2.pp197-205.

[18] 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.