CHAPTER I
INTRODUCTION

1.1. Background

A diploma is an official academic document that serves as proof of educational completion and plays an essential role in various purposes, such as pursuing higher education and employment recruitment. With the advancement of digitalization, diplomas have increasingly been managed in electronic form, which has been legally recognized under Law Number 19 of 2016 concerning Electronic Information and Transactions (EIT Law) [1]. However, existing verification systems remain centralized and dependent on the issuing institution, thereby limiting transparency and preventing independent verification by third parties [2]. Therefore, a system capable of ensuring document integrity and authenticity in a more open and transparent manner is required. This study proposes a hash-based diploma verification system using a hybrid architecture that integrates blockchain as the validation layer and the InterPlanetary File System (IPFS) as the document storage layer. This approach enables independent verification without relying on the issuing institution while preserving the integrity and authenticity of digital diploma documents [3].

According to a report by the Indonesian national news agency Antara, 112 cases of forged diploma usage were identified among applicants participating in the This finding indicates that the existing verification mechanism has not been sufficiently effective in detecting fraudulent academic documents at an early stage. In addition to causing administrative losses and legal implications, the incident also raised public concern regarding the authenticity of academic diplomas [4]. Therefore, a more transparent and reliable verification system is required, enabling independent verification by third parties.

As a response to these challenges, numerous studies have proposed the adoption of blockchain technology to ensure the integrity and authenticity of academic documents. This approach has emerged as an alternative to conventional verification systems, which continue to rely on centralized databases and manual administrative processes that are vulnerable to data manipulation. One such study was conducted by Suseno et al. (2024), who developed an academic document

recording system based on blockchain and the InterPlanetary File System (IPFS). In their proposed system, blockchain was utilized to immutably store document metadata and hash values through smart contracts, enabling any modification to a document to be detected by changes in its hash value. Meanwhile, IPFS was employed as a distributed storage platform for academic documents, allowing files to be stored outside the blockchain network, thereby improving storage efficiency and reducing transaction overhead. The evaluation results demonstrated that this approach strengthened data integrity and enhanced the transparency of the document recording process, thereby minimizing the risk of academic document manipulation. Consequently, the integration of blockchain and IPFS was considered a relevant approach for supporting the development of a more secure, transparent, and trustworthy academic document verification system [5].

Web-based verification approaches have also been explored by Wijayanto and Waliyullah (2024) through the development of a blockchain-enabled certificate verification system. In their study, certificate data were recorded on the blockchain to ensure transparency, integrity, and traceability through an immutable cryptographic mechanism. The proposed system enables users to verify certificates online through a web-based interface, eliminating the need to rely entirely on manual verification by the issuing institution. The implementation results demonstrated that all core system functionalities, including data recording, hash storage, and certificate verification, operated in accordance with the defined functional requirements. Compared with conventional approaches based on centralized databases, the proposed solution provides enhanced security while offering greater accessibility and convenience for stakeholders to perform certificate verification [6].

Another approach was proposed by Swari and Suartana (2024) through the development of a Decentralized Application (DApp) for digital certificate management using Non-Fungible Tokens (NFTs) based on the ERC-721 standard on the Ethereum blockchain. In their study, smart contracts were utilized to support various digital certificate management processes, including certificate issuance by the institution, ownership registration, transfer of ownership, and on-chain ownership verification. Through this mechanism, each certificate is represented as

a unique digital asset permanently recorded on the blockchain, enabling its ownership history and authenticity to be traced transparently. The adoption of NFTs also provides guarantees of uniqueness and publicly verifiable ownership without requiring a centralized authority. Nevertheless, the study primarily focused on the management and ownership representation of NFT-based digital certificates, whereas the verification of academic document integrity through hash value comparison with records stored on the blockchain, particularly within the context of formal education systems, was not the primary focus of the proposed verification framework [7].

Based on the review of previous studies, the application of blockchain technology in academic document management has primarily focused on decentralized data recording, hash value storage to preserve document integrity, the development of web-based verification systems, and the representation of digital certificate ownership through Non-Fungible Token (NFT) mechanisms. Integration with the InterPlanetary File System (IPFS) has also been widely adopted to support distributed document storage, thereby improving storage efficiency by reducing the amount of data maintained on the blockchain. Nevertheless, most existing studies have primarily treated blockchain and IPFS as platforms for data recording and storage, while document integrity verification has not been systematically established as a core component of the system architecture. In particular, the verification workflow that enables third parties to independently validate document authenticity by comparing the hash value of a document retrieved from IPFS with the corresponding hash recorded on the blockchain has not been operationally defined. Therefore, this study proposes a hash-based verification mechanism as the core component of the system by adopting a hybrid architecture that enables document retrieval from IPFS, hash recomputation, and comparison with blockchain records to be performed transparently and independently without relying directly on the issuing institution [5], [6], [7].

This study adopts a simulation-based approach to evaluate the conceptual and technical feasibility of the proposed verification system. This approach was selected because it enables the design of the system architecture, the implementation of smart contracts, and the integration of blockchain technology

with the InterPlanetary File System (IPFS) within a controlled environment without requiring direct deployment in formal educational institutions. Through simulation, each stage of the proposed workflow can be systematically evaluated, including the recording of document metadata on the blockchain, document storage in IPFS, and the verification process through hash recomputation and comparison with the corresponding hash values stored on the blockchain. This approach facilitates the assessment of workflow consistency, data integrity, and the verification mechanism that can be performed independently by authorized stakeholders. Furthermore, the simulation-based approach is employed to ensure interoperability among system components and to validate the transaction logic implemented in the smart contracts before the system is deployed in a broader operational environment [5].

1.2. Problem Formulation

Based on the background presented above, the research problems addressed in this study are formulated as follows:

1. How can a hash-based digital diploma verification system be designed using a hybrid architecture that integrates blockchain technology and the InterPlanetary File System (IPFS) to ensure the integrity and authenticity of academic documents?
2. How can the design of smart contracts support the immutable and structured recording and verification of academic documents on a blockchain network?
3. How can the conceptual and technical feasibility of the proposed digital diploma verification system be evaluated through a simulation-based approach?

1.3. Research Objectives

The research objectives represent the intended outcomes to be achieved in this study. Accordingly, the objectives of this research are as follows:

1. To design a hash-based digital diploma verification system using a hybrid architecture that integrates blockchain technology and the InterPlanetary File System (IPFS) to ensure the integrity and authenticity of academic documents.
2. To design smart contracts that support the immutable and structured recording and verification of academic documents on a blockchain network.

3. To evaluate the conceptual and technical feasibility of the proposed digital diploma verification system through a simulation-based approach.

1.4. Research Benefits

The significance of this study refers to the expected contributions resulting from the conducted research. Accordingly, the significance of this study is as follows:

1. To provide a design for a hash-based digital diploma verification system that integrates blockchain technology and the InterPlanetary File System (IPFS), enabling independent document verification through hash value comparison to ensure the integrity and authenticity of academic documents.
2. To provide a hybrid architecture model that combines on-chain and off-chain components by separating document storage from the recording of authenticity proofs on the blockchain, thereby improving storage efficiency while supporting transparency in the verification process.
3. To provide technical and academic references on smart contract design, the implementation of hash-based verification mechanisms, and the integration of blockchain technology with the InterPlanetary File System (IPFS) for the development of document verification systems using a simulation-based approach.

1.5. Research Limitations

To ensure that this study remains focused and well-defined, the following research scope and limitations are established:

1. This research focuses on the design, implementation, and evaluation of a digital diploma verification system without direct deployment in an educational institution.
2. The system verifies document integrity based on hash value consistency and does not address the legal validity of digital documents.
3. System evaluation is conducted on the Ethereum Sepolia Testnet and therefore does not represent the operational conditions of the Ethereum mainnet.
4. This research does not discuss legal and regulatory aspects related to the implementation of blockchain-based digital diplomas.

5. The system is limited to digital diploma management, including diploma issuance, verification, amendment, and reissuance, without covering other academic documents or interoperability among higher education institutions.
6. The system does not support the deletion or revocation of data that has already been recorded on the