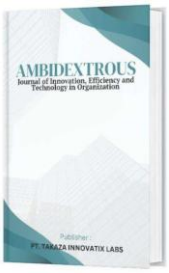
Ambidextrous: Journal of Innovation, Efficiency and Technology in Organizations

https://journal.takaza.id/index.php/ambidextrous

Vol. 05, No. 03, 2026, pp. 678-689
E-ISSN: 3031-7002

E-mail:ambidex@takaza.id



Blockchain-Based Digital Diploma Verification Mechanism Using Smart Contracts and the Interplanetary File System (IPFS)

Mukhamad Diva Mahardika Awaludin, Wina Witanti, Gunawan Abdillah
[123] Jenderal Achmad Yani University
Corresponding Author e-mail: mukhamaddiva10@gmail.com

Article History:
Received: 16-10-2026
Revised: 04-11-2026
Accepted: 04-11-2026

Keywords: *Blockchain, Digital Diploma, Document Verification, Interplanetary File System, Smart Contract*

Abstract: *This research was motivated by the need for more targeted diploma verification to reduce reliance on manual confirmation and detect document changes. This study aims to develop and test a blockchain-based digital diploma verification prototype using SHA-256, smart contracts, and IPFS. The research is a prototype development using the Evolutionary Prototyping method. The test objects consist of 30 simulated diploma documents tested using identical documents, modified documents, diploma numbers, hashes, and CIDs. Instruments include SHA-256, IPFS, Solidity, Ethereum Sepolia, MetaMask, and a block explorer. Analysis was conducted functionally using black-box testing and descriptively analyzing processing time and gas fees. The results show that document changes produce different hashes, while identical documents produce matching hashes, with a 100% test scenario suitability rate. In conclusion, the prototype can support technical checks of integrity, registration, and transaction traceability, but does not yet prove the administrative validity of diplomas.*

How to Cite: Mukhamad Diva Mahardika Awaludin, Wina Witanti, Gunawan Abdillah. (2026). Blockchain-Based Digital Diploma Verification Mechanism Using Smart Contracts and the Interplanetary File System (IPFS). *5(3)*. Pp 678-689 https://doi.org/10.61536/ambidextrous.5i03.933

https://doi.org/10.61536/ambidextrous.vx5i03.933

This is an open-access article under theCC-BY-SA License.

Introduction

Diplomas are widely used for recruitment, further study applications, job selection, and recognition of academic credentials. Therefore, the integrity and source of publication of these documents need to be verified (Jarnawansyah, 2025). However, the verification process is still often conducted through direct confirmation with the issuing institution, making the process time-consuming and increasing the administrative burden. Companies and educational institutions also have limited opportunities to conduct independent audits (Castro & Au-Yong-Oliveira, 2021; Frisch et al., 2023).

In addition to manual verification processes, falsification and misuse of academic

credentials can undermine the credibility of the education system, disrupt the job market, and reduce the quality of the workforce (Said et al., 2025). Conventional verification procedures are time-consuming, expensive, labor-intensive, and bureaucratic. Cases involving the falsification of degrees and diplomas, as well as the sale of academic credentials, further highlight the need for more targeted verification mechanisms (Tariq et al., 2023; Awang Abu Bakar et al., 2025). The use of information systems can support systematic information management and facilitate the management and recording of organizational data and assets (Rusmawanti et al., 2020).

Blockchain can support data recording through immutability, transparency, and traceability. Ledger mechanisms, consensus, and cryptographic relationships between blocks enable changes to records to be identified and data history to be traced (Dong et al., 2023). Cryptographic techniques can also be applied to support information security by protecting information from unauthorized access (Zulfikar et al., 2019). This technology has also been used in higher education for academic data management, student records, and diploma and credential verification (Jia et al., 2024; Raimundo & Rosário, 2021).

Full document storage on a blockchain has limitations in terms of storage capacity and performance. Therefore, documents can be represented using cryptographic hashes recorded on the blockchain, while the actual files are stored on IPFS using CIDs (Sultana et al., 2023; Lalli et al., 2024). The integration of blockchain, smart contracts, and IPFS has also been applied to educational certificate verification (Jaafar et al., 2024).

Previous research has applied blockchain to educational credential management and verification, including EduCTX for academic credit, traceable credential verification systems, and Ethereum smart contracts for diploma and transcript recording (Turkanović et al., 2018; Noshi & Xu, 2024; Putri et al., 2024). However, a prototype that integrates SHA-256, smart contracts, and IPFS is still needed to test document integrity, functionality, transparency, traceability, processing time, transaction costs, and implementation limitations.

This research aims to develop and test a prototype blockchain-based digital diploma verification application using SHA-256 to establish document identity, smart contracts for data recording and reading, and IPFS for file storage. This development is important to address the slowness of conventional verification, dependence on centralized systems, and the risk of forgery. The novelty of this research lies in the integration of these three components into a prototype that is tested based on document integrity, data conformity, transparency, transaction traceability, processing time, transaction costs, and implementation limitations.

Research Methods

This research is the development of a prototype for a blockchain-based digital diploma verification application. The method used is Evolutionary Prototyping, where the prototype is built in stages, then evaluated and refined iteratively until the specified functional requirements are met. This method was used because the integration of blockchain, smart contracts, and IPFS requires review and refinement at each stage of development.

The instruments used in development and testing included simulated diploma documents, the SHA-256 hash algorithm, IPFS, Solidity smart contracts, Ethereum Sepolia, MetaMask, and a block explorer. Functional testing was conducted using black-box scenarios to verify functional

https://doi.org/10.61536/ambidextrous.v5i03.933
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

suitability, document integrity, hash changes, transaction traceability, and verification results. Processing times and gas fees were recorded and analyzed descriptively to observe the characteristics of on-chain and off-chain processes.

The test object was a simulated diploma document used to examine the document recording and verification process. Testing was conducted on scenarios involving identical documents, altered documents, registered diploma numbers, different numbers, and transaction traceability. The use of simulated documents was intended because the prototype was not intended to validate genuine diplomas from specific institutions.

The research procedure followed the Evolutionary Prototyping stages: requirements gathering, rapid design, prototype development, evaluation and testing, and iterative refinement. Requirements gathering was conducted by identifying functional and non-functional requirements related to recording, verification, security, and document integrity. Next, the system architecture, process flow, smart contract data structure, database, and user interface were designed.

During the development phase, the prototype was implemented using Solidity smart contracts, an HTML-based web interface, Tailwind CSS, and JavaScript, a Node.js/Express and SQLite backend, Web3/MetaMask integration, and document storage via IPFS. The evaluation phase used simulated diploma documents to test functionality, hash integrity, transaction transparency and traceability, processing time, gas fees, and verification results. The test findings were then used to refine the prototype to ensure its intended functionality runs as expected.

Results and Discussion

Verification Mechanism Test Results

Table 1 Hash Results of Diploma Documents

No	Document Name	File Size	Hash Algorithm	SHA-256 Hash Value
1.	diploma_001.pdf	106 KB	SHA-256	4c81c3a0dca60f2332ac57a91eadf70e61af7e68a056e076ff807c76d8e5271b
2.	diploma_002.pdf	14 KB	SHA-256	64a5633112cc2630c2fce54255228bb5cc6243c92d6394e215c8e99556e44c2a
3.	diploma_003.pdf	43 KB	SHA-256	32f3333f5ebfa63813b8ce4f89a4c9fb014f961f42f37d615aca359d0d568467
4.	diploma_004.pdf	79 KB	SHA-256	0c837b9ac8b76123a501d64b0f065064668f8bbfefeb56b6468bc540c2d128ff
5.	diploma_005.pdf	19 KB	SHA-256	4945320b667d907f8a0ec04702b6f09f58ffed61060104c8b0fe933ceae0bc9b
6.	diploma_006.pdf	93 KB	SHA-256	9cdc7ae68f3ba652960d2018c8da0a5b1f6ac5f2b648a55814b934026e6aa0fd
7.	diploma_007.pdf	191 KB	SHA-256	f1d7b909106b3099d74b482e03db59b11bb9c431de97329dfc33001083b72c06
8.	diploma_008.pdf	69 KB	SHA-256	2b3eb940eceaa5459d4b654ead3010a0dc5a1e427031871b512dab0a3fd495e5
9.	diploma_009.pdf	29 KB	SHA-256	b3b9df3264d636aa89b8bc9376207a69461e8664933d04e0c7eac703fc46628a
10.	diploma_010.pdf	30 KB	SHA-256	170fafb1c1ba665629143a4153c6173278438a9b11f3480dd573914b7d9afea9

Table 1 displays 10 of the 30 simulated diplomas. Complete data is available in Appendix G. The ten documents in Table 6 generate different hashes, which are then used as file identifiers and search keys during verification. Hashes represent bytes, not readable content. The blockchain stores them as an integrity reference. Identical hashes indicate file compatibility but do not prove the authenticity of the academic data.

Table 2 Document Storage Results on IPFS

https://doi.org/10.61536/ambidextrous.v5i03.933
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

No	Document Name	*Hash*SHA-256	CID IPFS	Status
1.	diploma_001.pdf	4c81c3a0dca60f2332ac57a91eadf70e61af7e68a056e076ff807c76d8e5271b	QmZoc495fsVPFdMxiXXJtthDQVNFvNzC1Jeh812aN6667k	Succeed
2.	diploma_002.pdf	64a5633112cc2630c2fce54255228bb5cc6243c92d6394e215c8e99556e44c2a	QmeQ1FNNUeyNaANfJmAa6c7XQb57u92yk1vSZuwKXnQ4nc	Succeed
3.	diploma_003.pdf	32f3333f5ebfa63813b8ce4f89a4c9fb014f961f42f37d615aca359d0d568467	QmSMhVbfJF9xzWi8aTeMX2ChqteUnwgdRDBT64VdTvdbaG	Succeed
4.	diploma_004.pdf	0c837b9ac8b76123a501d64b0f065064668f8bbfefeb56b6468bc540c2d128ff	QmPFGe8oVXs3gav7jUwvLv3CRRkH5FhfHuAA4kQLLN2bKa	Succeed
5.	diploma_005.pdf	4945320b667d907f8a0ec04702b6f09f58ffed61060104c8b0fe933ceae0bc9b	QmQsDZDq1yNWRrVSGkV8BtBQk1ZA8bz3FUdphwZ4HaPEoM	Succeed
6.	diploma_006.pdf	9cdc7ae68f3ba652960d2018c8da0a5b1f6ac5f2b648a55814b934026e6aa0fd	QmSz55bH2QymXai8xAxMZbRs5uVLi9iqbDjeWQBjKBSMCU	Succeed
7.	diploma_007.pdf	f1d7b909106b3099d74b482e03db59b11bb9c431de97329dfc33001083b72c06	QmQA6vr15v3wBox6YlyTwMLrmcPzc8nfc3Z3KskVUUdZFk	Succeed
8.	diploma_008.pdf	2b3eb940eceaa5459d4b654ead3010a0dc5a1e427031871b512dab0a3fd495e5	Qmeg8Hw1zAiVCyZ6eyyrF6CggnZkcUmYHL8GJfaHTGELuV	Succeed
9.	diploma_009.pdf	b3b9df3264d636aa89b8bc9376207a69461e8664933d04e0c7eac703fc46628a	QmVbziBEn1xwXtdVP9CekiwBBncxiKtDruiKFpXCdvpNDu	Succeed
10.	diploma_010.pdf	170fafb1c1ba665629143a4153c6173278438a9b11f3480dd573914b7d9afea9	Qmac3pVbKZuXSeUvotos5X4qKSA5YVTsg8W524wSDJ31zf	Succeed

Table 2 shows 10 samples. All 30 data sets are available in Appendix G. These findings highlight the need for format validation and raw evidence storage. The separation of IPFS and blockchain reduces on-chain data. File availability still depends on PINs and gateways.

Table 3 Results of Data Recording on Blockchain

No	Diploma Number	*Transaction Hash*	*Block Number*	*Gas Fee*	Status
1.	742012020000107	0x5ca2ffa3a0f4033a3855a468f0e6ecb34d64dde4c085958fe9b9d4f08fd2ec7e	10788160	0.00122725 ETH	*Success*
2.	12006100869	0x7d406ce657299627bd762d70363439e0d66dcce2e6127524041ce066ceea74d8	10788169	0.00107133 ETH	*Success*
3.	701012021000241	0x85139aa854a50934bff67047c5ecbdee1d3413f5f05a688dbaecd197f22e1f1e	10788233	0.00107371 ETH	*Success*
4.	0006/S1-FT/Reg/2/2016	0x0116684a7b6abdee30abb3f49664b25d6e0024391d2f7bf91dfa3006e4d63c4d	10788240	0.00107477 ETH	*Success*
5.	13.01657.12	0x51f3d2b21f76ad831d01a689cf65b8f57050da1f394f83a6ab33944311f8f880	10788243	0.00107561 ETH	*Success*
6.	09.6.2142.2.443	0xafe9bc6499f6c7ac21c892efaba9b24a7cd8eefaa5587bfb11f3570e6a6797b4	10788247	0.00118989 ETH	*Success*
7.	11010110120008	0x1a27d370a77b64a53a8ce24bb384da780145f21e859169b00598c1114b1da2f0	10788250	0.00107793 ETH	*Success*
8.	862062021000541	0x85a81b913b265af76339f0e32c2330dedaeb457b3a84e363e4d91b378493b692	10788253	0.00107865 ETH	*Success*
9.	L2G009031	0xa7ffbbd9a0a554a44ef19f9d7a44a79d23f86f73cdf9dbb247e585692ce6913a	10788256	0.00107877 ETH	*Success*
10.	175203	0xa726c4badc14fe57498d704fe670ca31b30b170526af76197c89f374589b1451	10788260	0.00107769 ETH	*Success*

https://doi.org/10.61536/ambidextrous.v5i03.933
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

Table 3 lists 10 of the 30 documents. The gas fee is only derived from uploadDiploma, not including setTransactionHash. Each row has its own transaction hash and block number for browsing through a block explorer.

Table 4 Document Verification Results Scenario

No	Testing Scenario	*Input*Testing	Blockchain Data	Verification Results	Status
1.	Original document	diploma_004.pdf	*Hash*in accordance	In accordance	Succeed
2.	Document changed	diploma_004_edit.pdf	*Hash*it is not in accordance with	It is not in accordance with	Successfully detected
3.	Registered diploma number	742012020000107	Data found	In accordance	Succeed
4.	Diploma number not registered	42524623125	Data not found	It is not in accordance with	Successfully detected
5.	CID according to	CID according to IPFS data	CID match	In accordance	Succeed
6.	CID does not match	Different CID	CID does not match	It is not in accordance with	Successfully detected

The differences in output for the four scenarios in Table 4 are explained after the table.

1. In the first scenario, the original document produces the same hash as the hash recorded in the blockchain, so it is declared a match.
2. In the second scenario, the altered document produces a different hash and is therefore declared incompatible.
3. The third scenario shows that the registered diploma number can be used to retrieve hash and CID data from the blockchain.
4. The fourth scenario shows that unregistered diploma numbers do not generate verification data. This output distinguishes registered verification data from numbers that are not yet recorded in the smart contract.
5. The fifth and sixth scenarios use the CID as supporting data. The same CID as the record can be used to search for files in IPFS. A different CID does not match the recorded reference, but this check does not determine the document's administrative validity.

Test results rely on exact lookups and pre-recorded data. The prototype matches input against records without assessing the academic content of the diploma.

Table 5 Document Verification Results Based on Hash Changes

No.	Document Type	Test File Name	Reference Diploma Number	Registration Status	Hash Comparison Results	Information
1.	Original document	diploma_004.pdf	0006/S1-FT/Reg/2/2016	Recorded to the blockchain	*Hash*in accordance	Initial data
2.	Document renamed	diploma_004_edit_name.pdf	0006/S1-FT/Reg/2/2016	Not re-recorded	*Hash*different	It is not in accordance with
3.	Document number changed	diploma_004_edit_number.pdf	0006/S1-FT/Reg/2/2020	Not re-recorded	*Hash*different	It is not in accordance with
4.	Document modified date	diploma_004_edit_date.pdf	0006/S1-FT/Reg/2/2016	Not re-recorded	*Hash*different	It is not in accordance with
5.	Document metadata changed	diploma_004_edit_metadata.pdf	0006/S1-FT/Reg/2/2016	Not re-recorded	*Hash*different	It is not in accordance with
6.	Identical copy document	diploma_004 copy.pdf	0006/S1-FT/Reg/2/2016	Not re-recorded	*Hash*in accordance	In accordance

Table 5 shows that only the original document is recorded on the blockchain. The modified copy is used for verification only, as the same diploma number cannot be re-registered.

https://doi.org/10.61536/ambidextrous.v5i03.933
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

When changes occur to the name, number, date, and metadata, the prototype recalculates the hash of the test file and compares it to the hash of the original document that has been recorded. Each change produces a different hash. Therefore, the record is not found and the document is declared non-conforming. Conversely, an identical copy produces the same hash and demonstrates technical conformity with the record. Byte changes produce different hashes and are rejected during verification. This check does not assess administrative correctness. An erroneous original document can still be found if its hash has been recorded, so initial validation is the responsibility of the issuer.

Table 6 Transaction Traceability Details

No	Diploma Number	*Transaction Hash*	*Block Number*	Status	Tracking Media
1.	742012020000107	0x5ca2ffa3a0f4033a3855a468f0e6ecb34d64dde4c085958fe9b9d4f08fd2ec7e	10788160	*Success*	Sepolia Etherscan
2.	12006100869	0x7d406ce657299627bd762d70363439e0d66dcce2e6127524041ce066ceea74d8	10788169	*Success*	Sepolia Etherscan
3.	701012021000241	0x85139aa854a50934bff67047c5ecbdee1d3413f5f05a688dbaecd197f22e1f1e	10788233	*Success*	Sepolia Etherscan
4.	0006/S1-FT/Reg/2/2016	0x0116684a7b6abdee30abb3f49664b25d6e0024391d2f7bf91dfa3006e4d63c4d	10788240	*Success*	Sepolia Etherscan
5.	13.01657.12	0x51f3d2b21f76ad831d01a689cf65b8f57050da1f394f83a6ab33944311f8f880	10788243	*Success*	Sepolia Etherscan
6.	09.6.2142.2.443	0xafe9bc6499f6c7ac21c892efaba9b24a7cd8eefaa5587bfb11f3570e6a6797b4	10788247	*Success*	Sepolia Etherscan
7.	11010110120008	0x1a27d370a77b64a53a8ce24bb384da780145f21e859169b00598c1114b1da2f0	10788250	*Success*	Sepolia Etherscan
8.	862062021000541	0x85a81b913b265af76339f0e32c2330dedaeb457b3a84e363e4d91b378493b692	10788253	*Success*	Sepolia Etherscan
9.	L2G009031	0xa7ffbbd9a0a554a44ef19f9d7a44a79d23f86f73cdf9dbb247e585692ce6913a	10788256	*Success*	Sepolia Etherscan
10.	175203	0xa726c4badc14fe57498d704fe670ca31b30b170526af76197c89f374589b1451	10788260	*Success*	Sepolia Etherscan

Table 6 lists a unique transaction hash and block number for each diploma. This means each record has its own unique track record. If the transaction is successful, the transaction hash serves as proof that the network has received and processed the transaction.

Stakeholders can trace records through blockchain transaction trails. Document hashes and CID references reduce exposure because they don't directly reveal the file's contents. This evidence indicates the network has processed the data. However, it doesn't guarantee the accuracy of the diploma's administrative content. Network transparency also carries privacy risks. Full names, student ID numbers (NIK), birth dates, and other student data are not appropriate for direct recording on a public blockchain.

Table 7 Comparison of Off-Chain and On-Chain Processes

No	Process	Process Type	Time Range/Estimation	Transaction Fees	Information
1.	Document hash generation	*Off-chain*	0.5–1 second	0	Local, no network
2.	*Upload*documents to IPFS	*Off-chain*	2–5 seconds	0 (free pinning)	Depends on gateway & connection

https://doi.org/10.61536/ambidextrous.v5i03.933
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

No	Process	Process Type	Time Range/Estimation	Transaction Fees	Information
3.	Recording hash & CID to blockchain	*On-chain*	12–30 seconds	±0.0017 ETH (0.0011–0.0032 ETH)	Transaction only`uploadDiploma`
4.	Verification data reading	*On-chain*read-only	0.2–0.5 seconds	0 (read-only)	Does not change state
5.	Upload file hash matching	*Off-chain*	0.3–0.8 seconds	0	Local, fast

The observation timeframe only covers the uploadDiploma transaction, while setTransactionHash has not been calculated. The graph shows the minimum and maximum ranges at each stage, not averages or statistical benchmarks because raw data per document is not recorded. Advanced benchmarking requires controlled iterations with reporting of raw data, number of iterations, mean or median, and variance. Therefore, the current results should only be interpreted as a comparison of process characteristics.

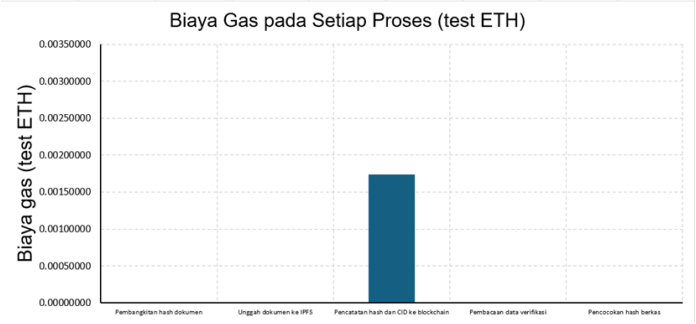


Figure 1 Graph of Transaction Costs per Process

Local hash generation and matching are faster and require no gas fees. Uploading to IPFS remains dependent on internet connection and service availability. In contrast, on-chain processes require confirmation time and gas fees due to smart contract state changes. Therefore, the prototype selectively uses the blockchain to record hashes and CIDs, while the diploma files are stored on IPFS.

Table 8 Gas Fee Observation Results

No	Activity	Transaction Type	Gas Used	*Gas Fee*	Information
1.	*Deployment*smart contract	*On-chain*	2,766,621	0.00416099 ETH	Highest cost
2.	Diploma data recording 1	*On-chain*	488,838	0.00122725 ETH	Writing mapping & array
3.	Diploma data recording 2	*On-chain*	426,858	0.00107133 ETH	Gas variation depending on string size
4.	Diploma registration 3	*On-chain*	426,870	0.00107371 ETH	*Gas used*relatively stable; gas fees vary according to network gas prices
5.	Summary`uploadDiploma`30 documents	*On-chain*	Varies	Average 0.0017 ETH (0.0011–0.0032 ETH)	Average`uploadDiploma`;`setTransactionHash`not included
6.	Verification reading via`eth_call`	*On-chain*read-only	0	0	No transactions; no state changes
7.	Verify 30 documents through`eth_call`	*On-chain*read-only	0	0	No gas; function event not saved

https://doi.org/10.61536/ambidextrous.v5i03.933
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

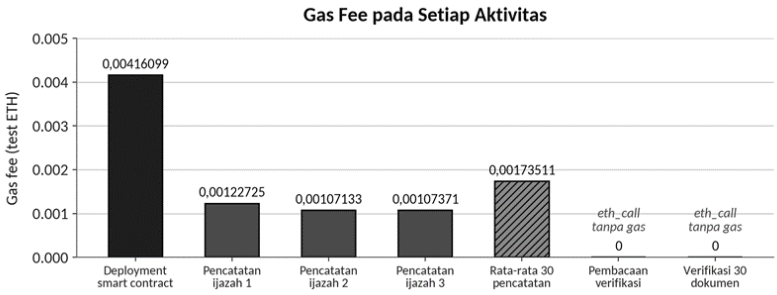


Figure 2 Gas Fee Graph

*Deployment*uses the most gas because all contract code is placed on the blockchain. For 30 uploadDiploma transactions, the average fee was recorded at 0.00173511 test ETH. This figure does not represent the entire flow. The setTransactionHash fee has not been calculated. Meanwhile, verification via eth_call does not use gas or generate persistent logs. All values are sourced from Sepolia and are subject to change depending on network conditions.

Figure 9 Conformity of Verification Results

No	Types of Testing	Amount	Expected results	Actual Results	Level of Compliance
1.	Original documents (files)	30	In accordance	In accordance	100%
2.	Document changed (file)	4	It is not in accordance with	It is not in accordance with	100%
3.	Registered diploma number	30	Data found	Data found	100%
4.	Diploma number not registered	10	Data not found	Data not found	100%
5.	*Hash*in accordance	30	In accordance	In accordance	100%
6.	*Hash*it is not in accordance with	10	It is not in accordance with	It is not in accordance with	100%
	Total	114	As per scenario	As per scenario	100%

The test results show that the original document and its corresponding hash were found, while no different documents or numbers were found. The percentages in Figure 24 only illustrate the results of the check on simulated data and do not indicate statistical accuracy or administrative authenticity. The prototype can check integrity, registration, hash-number relationships, and record traces, but the validity of the data remains dependent on the original data and the authorization of authorized institutions.

Analysis and Discussion of Test Results

1. *Blockchain*as a medium for recording evidence of integrity

Test data shows: the blockchain stores proof of integrity in the form of document hashes through a smart contract. Verification uses the hash of the tested file as a key to find the created record. The file is not stored on the blockchain, but rather on IPFS. Meanwhile, the hash and CID are recorded as technical evidence. This arrangement makes the blockchain a supporting layer for document compliance verification, not a replacement for academic administration.

https://doi.org/10.61536/ambidextrous.v5i03.933
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

2. **The Role of Hashes in Maintaining Document Integrity**

Meanwhile, a modified document produces a different hash. An unchanged document produces the same hash when re-examined. This difference is used to detect file changes. The hash only demonstrates the correspondence of the byte order and does not prove the correctness of the content or the administrative validity of the diploma. The issuing institution remains responsible for the original data recorded.

3. **The Role of IPFS as Off-Chain Storage**

Files are placed on IPFS, with the CID being a reference to their content. This type of storage avoids loading large documents onto the blockchain. There are two important limitations. The CID doesn't guarantee the file's availability and doesn't make its contents confidential. Public gateways may be able to retrieve content if the CID is known. Real academic documents require pinning, client-side encryption, access control, and retention rules before being stored in this manner.

4. **The Role of Smart Contracts in the Verification Process**

The code review identified two issues. The setTransactionHash function didn't use onlyAdmin. Meanwhile, verifyDiplomaByHash and verifyDiplomaByNumber weren't declared as views, even though they were read via eth_call. As a result, these write functions required access control, and events in the verify function weren't logged persistently. The test contract wasn't fixed because the change required redeployment and re-logging of all data to a new address. This is the immutability consequence discussed in Section 3.11.

5. **Transaction Transparency and Traceability**

Each record generates a transaction hash and block number, which can be tracked through a block explorer. This evidence supports the verification of the record trail. Because blockchain transactions are public and open, and difficult to delete, personal data should not be recorded directly. Future designs should limit on-chain data to only the evidence that is absolutely necessary.

6. **Comparison of On-Chain and Off-Chain Mechanisms**

The test data distinguishes between on-chain and off-chain functions. On-chain recording requires gas fees and network confirmation time. Hash generation, storage in IPFS, and hash matching do not change the blockchain state and therefore consume no gas. In the prototype, the blockchain only stores hashes and CIDs. Meanwhile, diploma files are stored in IPFS. This separation maintains a transaction trail without placing the entire document on the blockchain.

7. **Comparison of Verification Mechanisms with Existing Platforms**

The prototype's functionality is closest to Blockcerts, using hashes and blockchain to prove certificate integrity. Its relationship with EduCTX is more limited, as both use blockchain for academic data. CertiChain itself verifies input documents or identities by matching them against established records.

The three systems focus on different things. Blockcerts covers the issuance and verification of digital credentials. Meanwhile, EduCTX handles the exchange of academic credits between institutions. CertiChain is geared towards a single technical chain that connects document hashes, IPFS CIDs, smart contracts, transaction hashes, block numbers, gas fees, and matching outputs.

The technical contribution of this final project lies in the implementation and testing of this mechanism in a prototype. The blockchain serves as the record-keeping layer, IPFS as off-chain storage, and a smart contract as the data manager for the verification process. A comparison of the verification mechanism in this prototype development with existing platforms is shown in Table 10.

https://doi.org/10.61536/ambidextrous.v5i03.933
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

Table 10 Comparison of Verification Mechanisms with Existing Platforms

Aspect	This Development	BlockcertsBaldi et al. (2020)	EduCTXTurkanović et al. (2018)
Focus	Technical mechanism analysis	Digital credential standards	Academic credit management platform
Verification method	Document hash matching	Digital credential verification	Recognition and exchange of academic credits between institutions
Document storage	IPFS/off-chain	*File*credentials and metadata	Token-based academic credit data
Data on the blockchain	*Hash*, CID, diploma number, name, institution, and transaction metadata	*Hash*credentials	*Token*credits (ECTX) and academic data
Traceability	*Transaction hash*and block number	Through the verifier	Through the blockchain network between institutions
Scope	Technical simulation of diploma verification	Credential issuance and verification	Higher education credit exchange platform

Table 11 Advantages and Limitations of Blockchain Mechanisms

Aspect	Superiority	Limitations
Data integrity	Document changes can be detected through the hash	Does not guarantee the correctness of the initial data
Traceability	Transactions can be traced through transaction hash	Requires blockchain network access
Transparency	Transaction data can be checked via block explorer	On-chain metadata and public CIDs can pose privacy risks
Cost	Data reading is relatively cheap	Data recording requires gas fees
Immutability	Data is difficult to manipulate once recorded	Input errors are difficult to correct

Blockchain doesn't solve all diploma verification issues. It offers advantages in integrity, traceability, and transparency, along with limitations such as gas fees, network dependency, and the difficulty of data correction due to immutability. Its function in the prototype is to support technical verification. Meanwhile, administrative validity remains the responsibility of the issuing institution.

Conclusion and Recommendation

This research resulted in a CertiChain prototype for blockchain-based digital diploma verification by integrating SHA-256, smart contracts, and IPFS. Test results show that the prototype can verify document integrity, match diploma numbers to hashes, verify data registration, and verify transaction traceability. Identical documents generate matching hashes, while document changes generate different hashes and are not detected. The off-chain process is relatively quick and requires no gas fees, while the on-chain process requires confirmation time and transaction fees. Practically, this approach can support technical document verification by utilizing blockchain to record proof of integrity and IPFS to store files.

The research results still have limitations because the testing used simulated documents and Ethereum Sepolia as a testnet, so they do not represent implementation on the mainnet or administrative validation of diplomas from specific institutions. The time and cost data are also observational and cannot yet be used as statistical benchmarks. Furthermore, regulatory aspects, personal data protection, integration with academic systems, and operational validation have not been discussed in depth. Future research is recommended to conduct repeated testing with controlled device, browser, file size, and network conditions, and report raw data and appropriate statistical measures. Further development could also consider integration with

https://doi.org/10.61536/ambidextrous.v5i03.933
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

academic systems and testing in operational environments to more comprehensively assess the prototype's applicability.

References

Awang Abu Bakar, N. S., Yahya, N., Idris, N. B., Zakaria, Z., & Mohd Nordin, M. A. (2025). Enhancing academic credential integrity through blockchain-based verification systems. *Frontiers in Artificial Intelligence and Applications, 411*, 55–67. https://doi.org/10.3233/FAIA250509

Castro, R. Q., & Au-Yong-Oliveira, M. (2021). Blockchain and higher education diplomas. *European Journal of Investigation in Health, Psychology and Education, 11*(1), 154–167. https://doi.org/10.3390/ejihpe11010013

Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: An overview. *PeerJ Computer Science, 9*, e1705. https://doi.org/10.7717/peerj-cs.1705

Frisch, R., Dobák, D. É., & Udvaros, J. (2023). Blockchain diploma authenticity verification system using smart contract technology. *Annals of Mathematics and Informatics, 57*, 1–23. https://doi.org/10.33039/ami.2023.07.002

Jarnawansyah, M. (2025). Tindak pidana pemalsuan ijazah dalam perspektif hukum pidana Indonesia. *Journal of New Trends in Science, 3*(3), 41–55. https://doi.org/10.59031/jnts.v3i3.734

Jaafar, R. A., Alsaad, S. N., & Al-Kabi, M. N. (2024). Educational certificate verification system: Enhancing security and authenticity using Ethereum blockchain and IPFS. *Al-Mustansiriyah Journal of Science, 35*(1), 78–87. https://doi.org/10.23851/mjs.v35i1.1461

Jia, L., Shao, B., Yang, C., & Bian, G. (2024). A review of research on information traceability based on blockchain technology. *Electronics, 13*(20), 4140. https://doi.org/10.3390/electronics13204140

Lalli, A., Maciel, L. R., & Olmsted, A. (2024). Immortal certificates on Ethereum blockchain with off-chain IPFS storage. *International Journal of Intelligent Computing Research, 15*(1), 1242–1255. https://doi.org/10.20533/ijicr.2042.4655.2024.0152

Noshi, & Xu, Y. (2024). Development of blockchain-based academic credential verification system. *Open Access Library Journal, 11*, e12130, 1–19. https://doi.org/10.4236/oalib.1112130

Putri, I. A., Hermawan, A., & Kurniawan Maranto, A. R. (2024). Implementation of diploma and transcript verification system on the Ethereum blockchain network. *bit-Tech, 6*(3), 379–388. https://doi.org/10.32877/bt.v6i3.1288

Raimundo, R., & Rosário, A. (2021). Blockchain system in the higher education. *European Journal of Investigation in Health, Psychology and Education, 11*(1), 276–293. https://doi.org/10.3390/ejihpe11010021

Rusmawanti, S., Witanti, W., Sabrina, P. N., & Universitas Jenderal Achmad Yani. (2020). Sistem informasi manajemen aset pada PT. Gamma Solusi Karya Nusantara. *Prosiding Seminar Nasional Informatika*, 25–29.

Said, S. H., Sinde, R. S., Kosia, E. M., & Dida, M. A. (2025). A comprehensive blockchain-based system for educational qualifications management and

This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

verification to counter forgery. *IEEE Access, 13*, 31562–31589. https://doi.org/10.1109/ACCESS.2025.3542545

Sultana, S. A., Rupa, C., Malleswari, R. P., & Gadekallu, T. R. (2023). IPFS-blockchain smart contracts based conceptual framework to reduce certificate frauds in the academic field. *Information, 14*(8), 446. https://doi.org/10.3390/info14080446

Tariq, A., Binte Haq, H., & Ali, S. T. (2023). Cerberus: A blockchain-based accreditation and degree verification system. *IEEE Transactions on Computational Social Systems, 10*(4), 1503–1514. https://doi.org/10.1109/TCSS.2022.3188453

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access, 6*, 5112–5127. https://doi.org/10.1109/ACCESS.2018.2789929

Zulfikar, M. I., Abdillah, G., & Komarudin, A. (2019). Email menggunakan Blowfish dan Rivest Shamir Adleman (RSA). *Jurnal Informatika*, 19–26.

This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license