

Web3: Signature-Based Portfolio Verification

Mahendra S. Dalvi¹, Savita B. Mogare², Palak Sanjay Wadile³,

Khushi Dhiraj Koli⁴, Pavan Rajaram Rathod⁵

^{1,2} Assistant Professors, ^{1,2,3,4,5} Department of Information Technology

Sandip Institute of Technology and Research Center, Nashik, India

¹ dalvimahendra21@gmail.com, ² mogares1311@gmail.com, ³ palakwadile05@gmail.com,

⁴ kolikhushi28@gmail.com, ⁵ rpavanr25@gmail.com

Abstract: Digital portfolios are increasingly used by students and professionals to present academic qualifications, projects, certificates, technical skills, and other achievements. However, conventional portfolio systems commonly depend on centralized storage and manual verification. Such arrangements can make it difficult to establish document ownership, detect unauthorized modification, and efficiently verify submitted credentials.

This paper presents a Web3-based Digital Portfolio Verification Platform that combines blockchain technology, cryptographic hashing, digital signatures, Web3 wallet authentication, smart contracts, and optional decentralized file storage. The work builds on the blockchain-based student e-portfolio approach and extends it toward document-level verification. A submitted portfolio document is processed to generate a SHA-256 cryptographic hash. The hash is associated with the authenticated user's blockchain address and the verification record is authorized through a Web3 wallet signature. Verification metadata is recorded using a Solidity smart contract on an Ethereum-compatible blockchain. Large portfolio documents may optionally be stored using IPFS, while the blockchain maintains the information required for integrity verification.

During verification, a verifier submits a document and the system generates a new hash. The new hash is compared with the registered blockchain hash. The digital signature, owner or issuer status, and revocation status are then checked. This distinction is important: a successful hash match proves document integrity, but an institutionally verified credential additionally requires a trusted and authorized issuer. The framework therefore separates user-owned portfolio content from institutionally issued credentials.

The paper analyzes existing blockchain-based portfolio, certificate, accreditation, achievement-record, and academic transcript research and identifies a comparatively underexplored integration of portfolio management with cryptographic document-level verification. The resulting framework is intended for students, professionals, recruiters, and educational institutions.

Keywords: Web3, Blockchain, Digital Portfolio, Ethereum, Smart Contract, Digital Signature, SHA-256, IPFS, Portfolio Verification, Decentralized Identity

I. INTRODUCTION

The rapid adoption of digital technologies in education and employment has changed how students and professionals create, store, and share evidence of their achievements. Academic certificates, project records, internship documents, skill certificates, resumes, and other supporting documents are increasingly presented in digital form. A digital portfolio can therefore provide a consolidated representation of an individual's academic and professional development [1],[27]. However, the use of conventional digital portfolio systems does not by itself establish the authenticity of the information presented. Centralized databases may introduce risks related to unauthorized modification, data loss, privacy, and dependence on a trusted administrator. The base research on blockchain-based student e-portfolios



identifies similar concerns and proposes blockchain and smart contracts to improve integrity, ownership, privacy, and portfolio management [1],[25].

Blockchain provides a distributed ledger in which recorded transactions can be traced and protected against unauthorized modification. Research on blockchain applications in education has identified decentralization, traceability, immutability, security, reliability, and efficiency as important properties for educational applications [6],[21]. Blockchain-based academic certificate research has further demonstrated the use of smart contracts, digital signatures, certificate hashes, and decentralized storage for verification [2].

Nevertheless, storing a portfolio record on a blockchain does not automatically prove that a subsequently submitted document is the same document that was originally registered. A document-level cryptographic verification mechanism is therefore required [11],[29]. In addition, issuer trust remains important because blockchain can preserve information after registration but cannot independently determine whether information submitted by an issuer is truthful. This issue is discussed as the oracle problem in systematic research on blockchain-based academic transcripts [5],[17].

The objective of this research is to present an integrated Web3-based portfolio verification framework that combines the portfolio-management concepts of the base study with cryptographic hashing, digital signatures, Web3 wallet authentication, Ethereum smart contracts, optional decentralized storage, consent-based sharing, issuer identification, and revocation [1],[10].

The principal research contribution is not the use of blockchain alone. Instead, the contribution is the integration of document-level integrity verification and authorization into a portfolio-oriented workflow while explicitly distinguishing user-owned portfolio content from institutionally issued credentials [1],[17].

II. BACKGROUND AND THEORETICAL FOUNDATION

2.1 Blockchain Technology

Blockchain is a distributed ledger in which records are organized into blocks and linked using cryptographic mechanisms. The combination of distributed storage, consensus, cryptographic hashing, and transaction history provides properties such as integrity, traceability, and resistance to unauthorized alteration.

For educational applications, blockchain can be used to record evidence of certificates, achievements, learning activities, and portfolio information. Chen et al. describe decentralization, traceability, immutability, reliability, security, and efficiency as important blockchain properties [6].

II.2 Smart Contracts

A smart contract is program code deployed on a blockchain that executes predefined rules when required transaction conditions are satisfied. Smart contracts can automate registration, verification, access control, and revocation operations.

The base e-portfolio research uses smart contracts to implement portfolio-related business logic on a blockchain network [1]. The proposed system applies the same principle to portfolio registration and document verification.

II.3 Cryptographic Hashing

A cryptographic hash function maps an input message to a fixed-length digest. In the proposed system, SHA-256 is used to generate a 256-bit digital fingerprint of a portfolio document.

Let P represent a portfolio document. Its hash is:

$$H = \text{SHA256}(P) \quad (1)$$

If the content of the document changes, the generated hash changes with overwhelming probability. Therefore, the hash provides a mechanism for detecting document modification.

II.4 Digital Signatures

A digital signature provides cryptographic evidence that a message or hash was authorized using a private key associated with a specific blockchain identity. In the proposed platform, the user connects a Web3 wallet and signs a verification message.

The signed message should contain sufficient context to prevent reuse. A conceptual message is defined as:



$$M = H \parallel ID \parallel T \parallel N \quad (2)$$

where H is the portfolio hash, ID is the portfolio identifier, T is a timestamp, and N is a nonce. The signature is:

$$S = \text{SignprivateKey}(M) \quad (3)$$

This mechanism complements hashing: hashing provides integrity evidence, while the digital signature provides authorization evidence and helps associate the verification record with a blockchain identity.

2.5 Decentralized Storage

Large documents should not be unnecessarily stored directly on a public blockchain. Previous research has explored decentralized storage mechanisms such as IPFS for certificate and credential systems.

The proposed system therefore treats IPFS as an optional storage layer. When used, the portfolio document is stored in IPFS and the corresponding content identifier is associated with the blockchain verification record.

III. RELATED WORK

3.1 Blockchain-Based Student E-Portfolio

Zhao et al. proposed a blockchain-based system for student e-portfolio assessment using smart contracts. The system uses a four-layer architecture consisting of a data layer, blockchain network layer, chaincode layer, and application service layer.

The work focuses on portfolio ownership, data integrity, privacy, portfolio management, and assessment [1]. The present research adopts the e-portfolio and smart-contract foundation of this work but extends it toward automated document-level verification.

3.2 Blockchain-Based Academic Certificate Management

Bahrami et al. proposed a blockchain-based academic certificate management system using smart contracts and a permissioned Hyperledger Fabric network. The work emphasizes decentralized certificate issuance and verification, authorized issuers, multi-signature protection, privacy, and tamper resistance [10].

This research supports the proposed use of authenticated issuers, smart-contract-controlled records, and cryptographic authorization.

3.3 Blockchain-Based E-Learning Assessment and Certification

Li et al. proposed a blockchain system for e-learning assessment and certification. The system addresses learning assessment, certificate issuance, storage, and verification through blockchain and smart-contract mechanisms [22].

The proposed platform adopts the principle of reducing dependency on repeated manual verification and applies it specifically to digital portfolio documents.

3.4 Decentralized Accreditation

Sumithra et al. proposed decentralized accreditation of educational attainments using Ethereum, smart contracts, IPFS, and digital identity mechanisms [2]. The work demonstrates the value of separating document storage from blockchain verification records and providing controlled access to digital credentials.

These concepts are incorporated into the proposed architecture through Web3 authentication, optional IPFS-based document storage, and on-chain verification metadata.

3.5 Blockchain-Based Certificate Verification

The QualiChain research presents an Ethereum-based certificate verification ecosystem in which educational institutions register certificate hashes and recruiters verify documents by calculating and comparing hashes. The work also considers issuer management and certificate revocation [3].

The proposed platform applies the same fundamental hash-comparison principle to a broader digital portfolio containing multiple types of academic and professional evidence. However, a hash match alone is not treated as proof of institutional authenticity; issuer authorization is checked separately for institutionally verified credentials.



3.6 Trusted Achievement Records

Awaji et al. proposed a blockchain-based trusted achievement record system intended to connect students, employers, and educational institutions. The system aims to provide verifiable achievement records and support employment-related verification [4].

This work supports the proposed view of a portfolio as a comprehensive record of academic and professional achievements rather than only a collection of certificates.

3.7 Systematic Review of Academic Transcripts

Caldarelli and Ellul conducted a systematic literature review of blockchain-based academic transcript systems. Their work highlights standardization, interoperability, issuer trust, privacy, scalability, and the oracle problem as important research issues [5].

These findings are considered in the proposed framework by separating document storage from blockchain verification, identifying issuers, and including revocation and access-control mechanisms.

IV. PROBLEM STATEMENT

Existing digital portfolio systems can provide convenient storage and presentation of information but may not provide strong evidence of document integrity, ownership, and institutional authenticity. Manual verification of certificates and portfolio evidence can require communication with universities, organizations, or other issuing authorities.

The research problem addressed in this paper is the design of a secure and verifiable digital portfolio framework that can:

- authenticate the portfolio owner;
- generate a cryptographic fingerprint of submitted documents;
- associate the document with a verifiable blockchain identity;
- record verification evidence on a tamper-resistant ledger;
- allow authorized parties to verify submitted documents;
- detect modification of registered documents;
- distinguish user-owned portfolio content from issuer-verified credentials;
- support document or portfolio revocation;
- protect sensitive portfolio information; and
- reduce repeated manual verification.

V. RESEARCH GAP AND RESEARCH CONTRIBUTION

The reviewed literature demonstrates that different systems address different parts of the overall problem. The base e-portfolio system focuses on portfolio management and assessment, while other studies focus on certificate verification, accreditation, achievement records, decentralized storage, or academic transcript management.

The identified research gap is not the complete absence of blockchain-based educational verification. Rather, the reviewed studies address the required capabilities in different combinations and contexts. A portfolio-oriented workflow that integrates document-level integrity verification, Web3 authorization, issuer identification, and revocation remains comparatively underexplored in the reviewed literature.

The principal contribution of the proposed framework is the integration of:

- Web3 wallet-based authentication;
- portfolio-level and document-level hash generation;
- digital signature-based authorization;
- Ethereum-compatible smart-contract verification;
- optional IPFS-based document storage;
- issuer identification and authorization;
- consent-based sharing;



- revocation status; and
- automated portfolio verification.

A key design distinction is made between two types of information:

User-owned portfolio content: A user may register a project, resume, or other portfolio document. A successful hash and signature check demonstrates integrity and authorization of the registered record, but it does not by itself prove that the content is institutionally genuine.

Institutionally issued credentials: A certificate or credential is treated as institutionally verified only when it is associated with an authorized and registered issuer identity. Therefore, a hash match without issuer validation is not sufficient to classify a credential as institutionally authentic.

VI. PROPOSED SYSTEM

The proposed platform is designed as a Web3-enabled verification system in which the user remains the primary owner of the digital portfolio. The system separates the portfolio document from its blockchain verification evidence.

The major modules are:

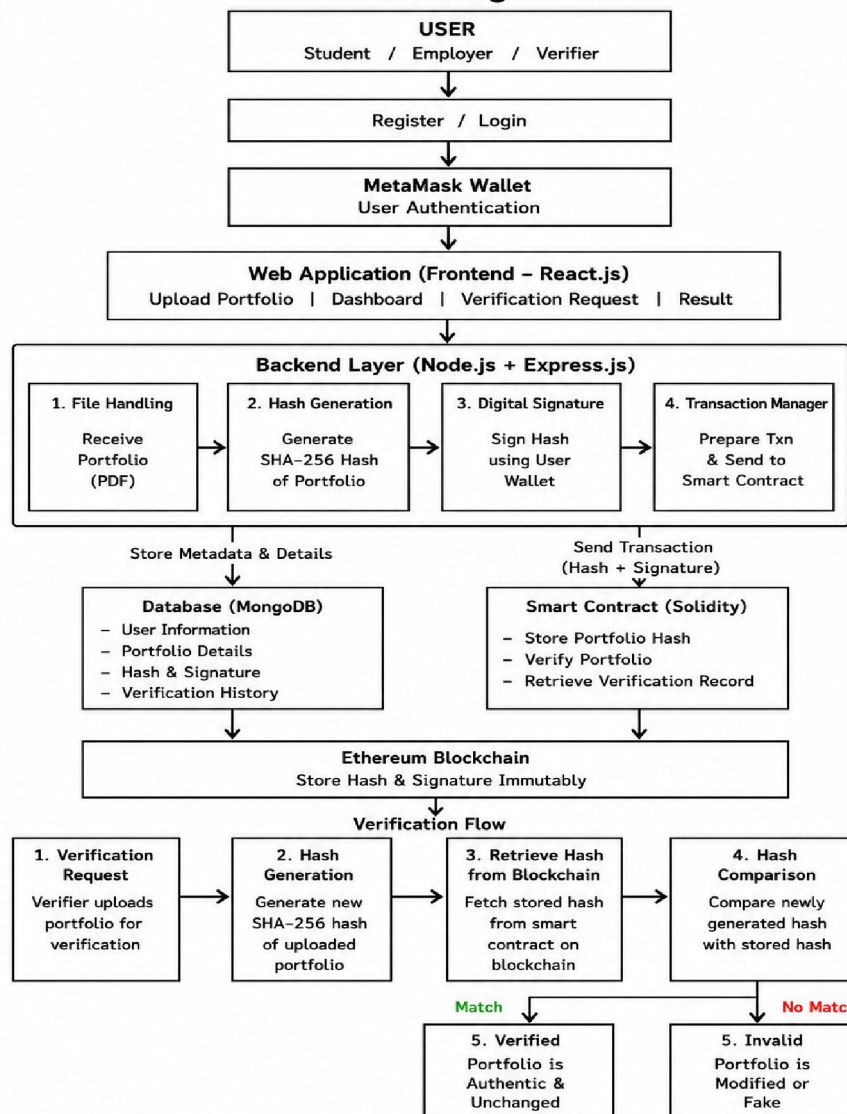
- Web3 Authentication Module
- Portfolio Management Module
- Document Processing Module
- Hash Generation Module
- Digital Signature Module
- Optional IPFS Storage Module
- Smart Contract Module
- Verification Module
- Issuer Management Module
- Revocation Module

The system supports two verification paths. The first is integrity verification of user-owned portfolio content. The second is institutional verification of credentials issued by registered organizations.



VII. SYSTEM FLOW DIAGRAM

Web3 Signature-Based Portfolio Verification Platform Flow Diagram



The proposed architecture is derived from the layered design principles of the base e-portfolio research and extends them with Web3 authentication and cryptographic verification mechanisms [1].

7.1 EXPLANATION

The architecture of the proposed Web3 Signature-Based Portfolio Verification Platform consists of multiple functional modules that work together to provide secure, decentralized, and tamper-proof portfolio verification using blockchain technology and digital signatures. The functionality of each module is explained below.



1. User

The User is the primary entity of the system and can be a Student, Employer, or Verifier. Students upload their digital portfolios, while employers and verifiers access the platform to verify the authenticity of the uploaded portfolios. This layer serves as the entry point of the proposed system.

2. Register / Login

The user first registers on the platform and logs in using valid credentials. This process ensures that only authorized users can access the portfolio management and verification services provided by the system.

3. MetaMask Wallet Authentication

After logging in, the user authenticates using the MetaMask Wallet. MetaMask verifies the user's Ethereum account and securely authorizes blockchain transactions. It also enables digital signing of portfolio hashes, ensuring secure identity verification.

4. Web Application (Frontend – React.js)

The frontend is developed using React.js and provides an interactive user interface. Through this interface, users can upload portfolio documents, access the dashboard, submit verification requests, and view verification results. The frontend communicates with the backend server for all application operations.

5. Backend Layer (Node.js + Express.js)

The backend layer acts as the core processing unit of the system. It processes user requests, performs business logic, communicates with the database, interacts with the blockchain network, and manages the complete verification workflow.

5.1 File Handling

The File Handling module receives the uploaded portfolio document (PDF), validates its format, and prepares it for further processing.

5.2 Hash Generation

This module generates a unique SHA-256 cryptographic hash for the uploaded portfolio. The generated hash acts as a unique digital fingerprint of the document. Even a minor modification in the document produces a completely different hash.

5.3 Digital Signature

The generated portfolio hash is digitally signed using the user's MetaMask wallet. The digital signature verifies the ownership and authenticity of the uploaded portfolio before storing its verification record.

5.4 Transaction Manager

The Transaction Manager prepares the blockchain transaction and securely sends the portfolio hash and digital signature to the deployed smart contract for permanent storage.

6. Database (MongoDB)

MongoDB stores application-related information such as user profiles, portfolio details, generated hashes, digital signatures, and verification history. Since blockchain storage is expensive, MongoDB stores non-critical application data, improving system performance and data management.

7. Smart Contract (Solidity)

The smart contract is developed using Solidity and deployed on the Ethereum blockchain. It securely stores portfolio verification data and provides functions for storing portfolio hashes, verifying portfolios, and retrieving verification records whenever required. The smart contract acts as the trusted verification component of the system.

8. Ethereum Blockchain

The Ethereum blockchain permanently stores the portfolio hash and digital signature in an immutable ledger. Once the verification data is recorded, it cannot be modified or deleted. This ensures transparency, integrity, and security throughout the verification process.



9. Verification Flow

The verification process begins when a verifier uploads a portfolio document through the web application. The system generates a new SHA-256 hash of the uploaded portfolio and retrieves the original hash stored on the Ethereum blockchain using the smart contract. Both hash values are then compared to determine whether the portfolio has been modified.

10. Verification Result

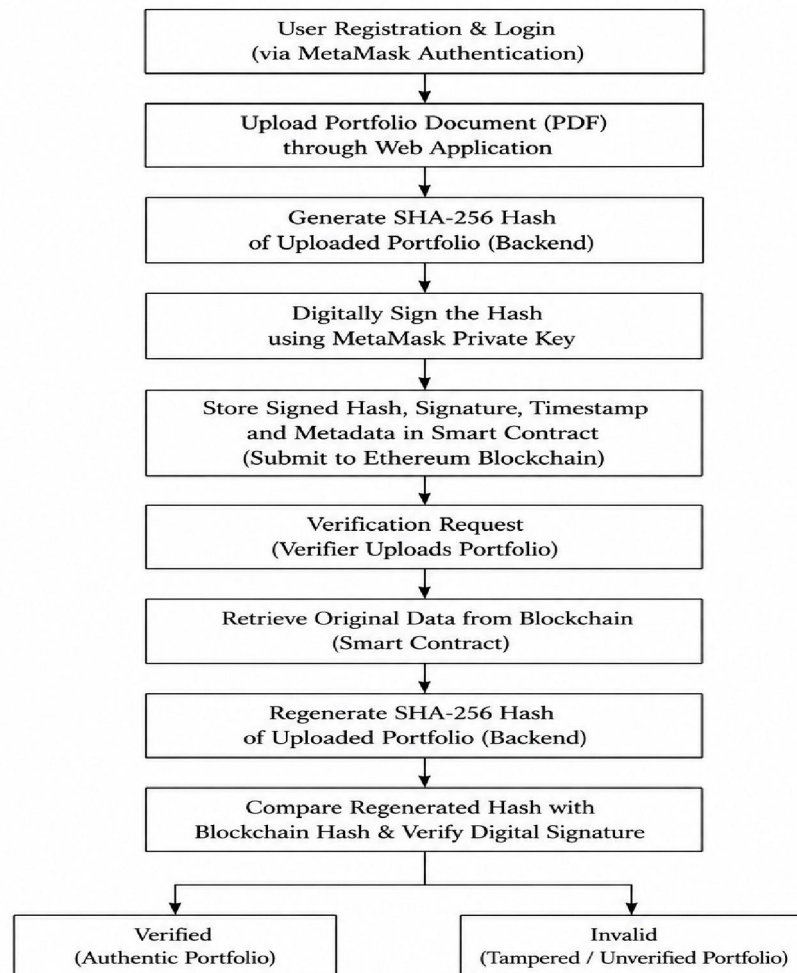
10.1 Verified

If the newly generated hash matches the hash stored on the blockchain, the portfolio is verified as authentic, genuine, and unchanged. The system confirms that the document has not been tampered with after its original upload.

10.2 Invalid

If the generated hash does not match the blockchain record, the portfolio is marked as invalid. This indicates that the document has been modified, tampered with, or is potentially fraudulent.

VIII. METHODOLOGY Methodology Block Diagram



The proposed Web3 Signature-Based Portfolio Verification Platform follows a systematic methodology to ensure secure, transparent, and tamper-proof verification of digital portfolios. The complete workflow of the proposed system is described below:

- The user registers on the platform and securely logs in using valid credentials . Authentication is performed through the MetaMask wallet . MetaMask verifies the user's blockchain identity and authorizes Ethereum blockchain transactions without exposing sensitive credentials .
- After successful authentication, the user uploads a digital portfolio document (PDF) through the React.js web application
- . The uploaded portfolio is securely transmitted to the backend server . Preliminary validation is performed to verify the document format, integrity, and completeness before further processing .
- The backend server generates a unique SHA-256 cryptographic hash of the uploaded portfolio . The generated hash acts as a fixed-length digital fingerprint that uniquely represents the uploaded document . Any modification to the document produces a completely different hash value, enabling reliable tamper detection .
- The generated hash is digitally signed using the user's private key through the MetaMask wallet . The digital signature confirms document ownership and authenticity . It also ensures that only the legitimate owner can authorize blockchain verification .
- The signed portfolio hash, digital signature, timestamp, and verification metadata are submitted to a deployed Solidity smart contract . The smart contract validates the transaction before storing it permanently on the Ethereum blockchain . Portfolio metadata, user information, and verification history are securely maintained in MongoDB for efficient retrieval and management .
- Whenever a portfolio verification request is initiated, the verifier uploads the portfolio through the web application . The backend regenerates the SHA-256 cryptographic hash using the same hashing algorithm employed during registration . The regenerated hash is then prepared for comparison with the blockchain record .
- The smart contract retrieves the original portfolio hash and digital signature stored on the Ethereum blockchain . The backend compares the regenerated hash with the blockchain-stored hash . Simultaneously, the associated digital signature is validated to verify document integrity, authenticity, and ownership .
- If both the cryptographic hash values match successfully, the portfolio is verified as authentic and unmodified . If any mismatch is detected, the system immediately identifies the document as altered or tampered . The invalid portfolio is rejected, thereby preventing fraudulent portfolio submissions.
- Finally, the verification result is displayed through the web application . The result includes the verification status, blockchain transaction reference, verification timestamp, and document authenticity . This decentralized verification mechanism provides a secure, transparent, and trustworthy solution without relying on centralized authorities or manual verification .

IX. VERIFICATION ALGORITHM

The verification process is:

- A verifier uploads the portfolio document.
- The backend generates a new SHA-256 hash.
- The blockchain record is retrieved using the portfolio identifier.
- The newly generated hash is compared with the registered hash.
- The digital signature is checked.
- The owner or authorized issuer identity is checked.
- The revocation status is checked.
- If the record is an institutionally issued credential, the issuer authorization status is verified.
- The system determines the final verification result.



- The result is displayed to the verifier.

The verification result must distinguish integrity from institutional authenticity.

X. PROPOSED IMPLEMENTATION FRAMEWORK

The proposed implementation can be organized into frontend, backend, blockchain, storage, and authentication components.

Table 1 Proposed Implementation Technologies

Component	Technology / Purpose
Frontend	React.js for user interface
Backend	Node.js and Express.js
Database	MongoDB for application-related information
Blockchain	Ethereum-compatible network
Smart Contract	Solidity
Development Framework	Hardhat
Wallet	MetaMask or compatible Web3 wallet
Blockchain Library	Ethers.js / compatible Web3 library
File Storage	Optional IPFS / Pinata
Version Control	Git and GitHub

Application-related information such as user details and verification history can be maintained in MongoDB, while documents may be stored using IPFS and verification evidence can be recorded on the blockchain. This separation avoids placing the complete portfolio document directly on-chain.

The selected Ethereum/Web3 architecture differs from the permissioned Hyperledger Fabric architecture used in the base e-portfolio study. The change is motivated by the proposed use of wallet-based authentication, Solidity smart contracts, public verification, and Web3 development tools. The blockchain platform should be reported as the actual platform used in the implemented prototype.

XI. SECURITY AND PRIVACY ANALYSIS

11.1 Document Integrity

The SHA-256 hash acts as the document fingerprint. If a document is modified after registration, the newly generated hash will not match the blockchain hash.

11.2 Ownership and Authorization

The digital signature binds the registered verification information to the authenticated wallet. This provides an additional layer of evidence beyond simple hash matching.

11.3 Blockchain Immutability

Once a verification transaction is confirmed, the recorded verification evidence is protected by the blockchain's distributed ledger mechanism. Immutability, however, does not imply that the original information supplied by an issuer is truthful.

11.4 Privacy

Sensitive portfolio documents should not be stored directly on a public blockchain. The proposed design stores only the minimum verification metadata required on-chain and uses optional decentralized storage for documents.

11.5 Access Control

The system can use user-controlled sharing and permission mechanisms so that portfolio information is disclosed only to authorized parties.



11.6 Revocation

A portfolio or credential can be marked as revoked by an authorized issuer or administrator. Verification must therefore check the current revocation state rather than relying only on the original hash match.

11.7 Replay Attack Protection

The proposed signed message includes a portfolio identifier, timestamp, and nonce. These values provide contextual information that can be used to prevent reuse of an old authentication or registration signature.

11.8 Issuer Trust and Oracle Problem

Blockchain protects the integrity of information after it is recorded, but it does not independently validate whether an issuer provided truthful information. Caldarelli and Ellul identify this issue as an important consideration in blockchain-based academic applications [5].

The proposed system therefore includes registered issuer identities, issuer authorization, and revocation. Future work should investigate decentralized issuer governance and interoperable credential standards.

XII. DISCUSSION

The reviewed research demonstrates that blockchain is useful for protecting educational records, certificates, achievements, and portfolio information. However, the systems differ in blockchain type, storage architecture, identity model, access control, and verification mechanism.

The base e-portfolio study provides the strongest foundation for portfolio management, ownership, privacy, and smart-contract-based processing [1]. Certificate-oriented research adds document hashing, digital signatures, IPFS, issuer verification, and revocation [10, 2, 3]. Achievement-record research expands the role of the portfolio toward employment and stakeholder interaction [4]. The systematic review emphasizes standardization, interoperability, and issuer trust [5].

The proposed framework integrates these complementary concepts while keeping the central research focus on digital portfolio verification. An important design principle is that a hash match alone is not treated as proof of institutional authenticity. The platform therefore distinguishes document integrity from issuer trust.

XIII. EVALUATION PLAN

No experimental performance values are claimed in this paper until the proposed implementation is tested. The completed prototype should be evaluated using measurable parameters.

Table 2 Proposed Evaluation Parameters

Parameter	Purpose
Registration Time	Time required to register a portfolio
Verification Time	Time required to verify a submitted portfolio
Revocation Time	Time required to revoke a registered record
Transaction Cost	Blockchain cost for write operations
Storage Overhead	Storage required for blockchain and optional IPFS records
Verification Accuracy	Correct identification of valid and modified documents
Tamper Detection Rate	Ability to identify modified documents
Scalability	Behavior as the number of records increases
Security	Resistance to modification and unauthorized verification
Usability	Ease of use for students and verifiers

The completed prototype should be evaluated separately for:

- portfolio registration;
- portfolio verification;



- credential verification;
- revocation;
- tampered-document detection; and
- storage and blockchain operations.

Actual measurements should be reported only after experimental testing. Results from other research papers should not be presented as results of the proposed system.

XIV. ADVANTAGES

The proposed platform provides the following potential advantages:

- Tamper Detection: Document modification can be identified using hash comparison.
- User Ownership: Portfolio records can be associated with the user's Web3 identity.
- Automated Verification: Verification can be performed without repeated manual checking.
- Transparency: Blockchain provides traceable verification records.
- Secure Authorization: Digital signatures provide cryptographic authorization of verification records.
- Decentralized Storage: IPFS can optionally be used for large portfolio documents.
- Issuer Verification: Institutionally issued credentials can be associated with registered issuer identities.
- Revocation Support: Invalid or withdrawn records can be marked as revoked.
- Reduced Administrative Effort: Recruiters and institutions can perform automated verification.

XV. LIMITATIONS

The proposed system has several limitations.

First, blockchain write operations can involve transaction fees and network latency. Second, public blockchain deployment requires careful consideration of privacy because blockchain records are persistent. Third, wallet credential loss or compromise may create identity-management challenges.

Fourth, blockchain does not completely solve the oracle problem. The authenticity of information supplied by an issuer still depends on issuer trust and governance. Fifth, a hash match proves that a document corresponds to a registered record, but it does not by itself prove that the underlying claim is truthful.

Finally, smart-contract implementation must be carefully tested and secured because software vulnerabilities can affect the verification system. The proposed framework also requires further testing for large-scale usage and interoperability with standardized digital credential systems.

XVI. FUTURE WORK

Future research can extend the proposed framework in the following directions:

- Integration of Decentralized Identifiers (DIDs).
- Support for standardized digital credentials.
- Zero-knowledge-proof-based privacy-preserving verification.
- Multi-blockchain interoperability.
- Decentralized issuer governance.
- Advanced certificate and portfolio revocation.
- Mobile application support.
- Large-scale performance evaluation.
- Formal smart-contract security analysis.
- Integration with educational institutions and recruitment platforms.

Standardization and interoperability should receive particular attention because the systematic review identifies heterogeneous blockchain approaches as an important barrier to broader adoption [5].



XVII. CONCLUSION

This paper presented a Web3-based Digital Portfolio Verification Platform that combines blockchain, cryptographic hashing, digital signatures, Web3 wallet authentication, smart contracts, and optional decentralized storage.

The research builds on the blockchain-based student e-portfolio concept and extends it from portfolio management toward document-level verification. The proposed workflow generates a SHA-256 hash for each portfolio document, associates the hash with the authenticated user's blockchain identity, creates an authorization signature, records verification evidence through a Solidity smart contract, and optionally stores the document using IPFS.

During verification, the submitted document is hashed again and compared with the registered blockchain hash. Digital signature validation, owner or issuer validation, and revocation checking provide additional controls. The framework explicitly distinguishes user-owned portfolio content from institutionally issued credentials, because a hash match alone cannot establish the truthfulness of an academic or professional claim.

The integrated approach addresses important requirements identified across the reviewed research, including integrity, ownership, transparency, decentralized verification, storage separation, issuer identification, consent, and revocation.

The framework provides a practical foundation for secure digital portfolio verification. However, actual system performance, transaction cost, scalability, and security must be established through implementation and experimental evaluation. These measurements will form the basis for validating the effectiveness of the proposed approach.

REFERENCES

1. G. Zhao, H. He, B. Di, Q. Xia, and Z. Fu, "A Blockchain-Based System for Student E-Portfolio Assessment Using Smart Contract," in Proc. 4th Int. Conf. Computer Science and Artificial Intelligence (CSAI), Zhuhai, China, 2020, pp. 34–40, doi: 10.1145/3445815.3445821.
2. S. V., S. R., D. Mukhopadhyay, and S. K. Gupta, "Decentralized Accreditation of Educational Attainments Using Blockchain," in Proc. 6th Int. Conf. for Convergence in Technology (I2CT), Pune, India, 2021, doi: 10.1109/I2CT51068.2021.9418201.
3. QualiChain Research Team, "Blockchain-Based Qualification and Certificate Verification Ecosystem," in Proc. IEEE BRAINS Conference, 2020.
4. B. Awaji, E. Solaiman, and L. Marshall, "Blockchain-Based Trusted Achievement Record System Design," in Proc. International Conference on Information and Education Innovation (ICIEI), London, U.K., 2020, pp. 46–50, doi: 10.1145/3411681.3411689.
5. G. Caldarelli and J. Ellul, "Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review," Applied Sciences, vol. 11, no. 4, p. 1842, 2021, doi: 10.3390/app11041842.
6. G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring Blockchain Technology and Its Potential Applications for Education," Smart Learning Environments, vol. 5, no. 1, 2018, doi: 10.1186/s40561-017-0050-x.
7. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
8. J. Benet, "IPFS: Content Addressed, Versioned, P2P File System," arXiv:1407.3561, 2014.
9. M. Turkanovic', M. Ho'lbl, K. Kos'ic', M. Heric'ko, and A. Kamis'alic', "EduCTX: A Blockchain-Based Higher Education Credit Platform," IEEE Access, vol. 6, pp. 5112–5127, 2018.
10. M. Bahrami, A. Movahedian, and A. Deldari, "A Comprehensive Blockchain-Based Solution for Academic Certificates Management Using Smart Contracts," in Proc. 10th Int. Conf. Computer and Knowledge Engineering (ICCCKE), Mashhad, Iran, 2020, pp. 573–578, doi: 10.1109/ICCCKE50421.2020.9303656.
11. S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, S. Mumtaz, and Z. U. Qayyum, "Docschain: Blockchain-Based IoT Solution for Verification of Degree Documents," IEEE Transactions on Computational Social Systems, vol. 7, no. 3, pp. 827–837, 2020, doi: 10.1109/TCSS.2020.2973710.
12. A. Minchev and M. Karabaliev, "Examination of Possibilities for Proving the Authenticity of Educational Achievements Using NFTs or Soulbound Tokens Recorded on Blockchain and IPFS," in Proc. 16th Int. Conf. Education, Research and Innovation (ICERI), 2023, pp. 8442–8451, doi: 10.21125/iceri.2023.2155.



13. R. A. Jaafar and S. N. Alsaad, "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric," *TEM Journal*, vol. 12, no. 4, pp. 2385–2395, 2023, doi: 10.18421/TEM124-51.
14. S. H. Said, M. A. Dida, E. M. Kosia, and R. S. Sinde, "A Blockchain-Based Conceptual Model to Address Educational Certificate Verification Challenges in Tanzania," *Engineering, Technology and Applied Science Research*, vol. 13, no. 5, pp. 11691–11704, 2023, doi: 10.48084/etasr.6170.
15. J. Moya, J. Ayoade, and M. Uddin, "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System," *Sensors*, vol. 25, no. 11, p. 3450, 2025, doi: 10.3390/s25113450.
16. D. S. Wankhede, V. S. Gaikwad, M. Karnik, and V. Mishra, "The Decentralized Smart Contract Certificate System Utilizing Ethereum Blockchain Technology," *Procedia Computer Science*, vol. 230, pp. 923–934, 2023, doi: 10.1016/j.procs.2023.12.035.
17. A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," *IEEE Access*, vol. 11, pp. 64679–64696, 2023, doi: 10.1109/ACCESS.2023.3289598.
18. M. Al Hemaury, M. Abu Talib, A. Khalil, A. Zulfikar, and T. Mohamed, "Blockchain-Based Framework and Platform for Validation, Authentication and Equivalency of Academic Certification and Institution's Accreditation: UAE Case Study and System Performance," *Education and Information Technologies*, vol. 29, pp. 18203–18232, 2024, doi: 10.1007/s10639-024-12493-6.
19. R. Q. Castro and M. Au-Yong-Oliveira, "Blockchain and Higher Education Diplomas," *European Journal of Investigation in Health, Psychology and Education*, vol. 11, no. 1, pp. 154–167, 2021, doi: 10.3390/ejihpe11010013.
20. J. Park, "Promises and Challenges of Blockchain in Education," *Smart Learning Environments*, vol. 8, p. 33, 2021, doi: 10.1186/s40561-021-00179-2.
21. C. Delgado-von-Eitzen, L. Anido-Rifo'n, and M. J. Ferna'ndez-Iglesias, "Blockchain Applications in Education: A Systematic Literature Review," *Applied Sciences*, vol. 11, no. 24, p. 11811, 2021, doi: 10.3390/app112411811.
22. C. Li, J. Guo, G. Zhang, Y. Wang, Y. Sun, and R. Bie, "A Blockchain System for E-Learning Assessment and Certification," in *Proc. 2019 IEEE Int. Conf. Smart Internet of Things (SmartIoT)*, Tianjin, China, 2019, pp. 212–219, doi: 10.1109/SmartIoT.2019.00040.
23. E. Guustaaf, U. Rahardja, Q. Aini, H. W. Maharani, and N. A. Santoso, "Blockchain-Based Education Project," *APTISI Transactions on Management*, vol. 5, no. 1, pp. 46–61, 2021, doi: 10.33050/atm.v5i1.1433.
24. G. Capece, N. Levialdi Ghiron, and F. Pasquale, "Blockchain Technology: Redefining Trust for Digital Certificates," *Sustainability*, vol. 12, no. 21, p. 8952, 2020, doi: 10.3390/su12218952.
25. Y. Zheng, "Design of a Blockchain-Based e-Portfolio Evaluation System to Assess the Education and Teaching Process," *International Journal of Emerging Technologies in Learning*, vol. 16, no. 5, pp. 261–280, 2021, doi: 10.3991/ijet.v16i05.21081.
26. A. Mikroyannidis, A. Third, and J. Domingue, "A Case Study on the Decentralisation of Lifelong Learning Using Blockchain Technology," *Journal of Interactive Media in Education*, vol. 2020, no. 1, pp. 1–10, 2020, doi: 10.5334/jime.591.
27. C.-L. Chen, K.-W. Zeng, H.-C. Chen, Y.-Y. Deng, C.-F. Lee, D.-C. Huang, and L.-C. Liu, "Secure and Efficient Graduate Employment: A Consortium Blockchain Framework With InterPlanetary File System for Privacy-Preserving Resume Management and Efficient Talent-Employer Matching," *PLoS ONE*, vol. 20, no. 8, p. e0315277, 2025, doi: 10.1371/journal.pone.0315277.

