VeriZKP: A Privacy-Preserving, Gas-less, and Granular Educational Credential Verification System on Ethereum using Zero-Knowledge Proofs

Kadhim Abdulfadhil Gatea[1], Ehsan Shoja[1], Parviz Rashidi-Khazaee[2*], Hossein Nahid-Titkanlue[3]

[1] Department of Information Technology and Computer Engineering, Urmia University, Urmia, Iran
[2] Department of Information Technology and Computer Engineering, Urmia University of Technology, Urmia, Iran
[3] Assistant Professor, Department of Industrial Engineering, Payame Noor University, Tehran, Iran

*** Corresponding author email address**: p.rashidi@uut.ac.ir

Received: 2025-06-17 **Revised:** 2025-10-12 **Accepted:** 2025-10-19 **Initial Publish:** 2025-10-19 **Final Publish:** 2026-07-10

Abstract

The digital transformation of education necessitates secure, private, and learner-centric methods for verifying academic credentials. Conventional verification processes expose sensitive personally identifiable information, creating privacy risks that conflict with data protection regulations like GDPR. Existing blockchain solutions for educational credential verification face persistent challenges including prohibitive transaction costs, privacy vulnerabilities, and inflexible verification models. This paper presents VeriZKP, a proof-of-concept architecture demonstrating gas-free credential verification on Ethereum using zero-knowledge proofs. The core innovation lies in separating on-chain trust anchoring from off-chain cryptographic computation, enabling a novel cost-elimination mechanism. The system leverages Ethereum's view functions through pre-compiled verifier contracts to achieve zero gas consumption for verification operations while preserving privacy through selective disclosure mechanisms. Our prototype, evaluated on Ethereum Sepolia testnet, validates the fundamental feasibility of this approach. Results demonstrate complete elimination of verification costs, practical client-side proof generation times of 1.02-1.63 seconds on standard hardware, and support for multi-attribute credential verification. The architecture proves both economically viable and performant for blockchain-based identity systems.

Keywords: *Zero-Knowledge Proofs (ZKP), zk-SNARKs, Blockchain, Educational Credentials, Privacy Preservation, Ethereum.*

How to cite this article:
Abdulfadhil Gatea, K., Shoja, E., Rashidi-Khazaee, P., & Nahid-Titkanlue, H. (2026). VeriZKP: A Privacy-Preserving, Gas-less, and Granular Educational Credential Verification System on Ethereum using Zero-Knowledge Proofs. Management Strategies and Engineering Sciences, 8(4), 1-12.

1. Introduction

The global transformation toward online learning, remote work, immersive metaverse environments, and continuous professional development has fundamentally altered the nature of academic credentials, evolving them from static documents into dynamic digital assets [1-4]. Within this transformed landscape, the verification of educational credentials has emerged as a foundational pillar of trust in modern society, serving as the primary mechanism through which employers validate applicant qualifications, academic institutions assess student prerequisites, and licensing bodies confirm professional expertise. However, the legacy infrastructures governing this critical verification process are increasingly misaligned with the demands of our globalized and privacy-conscious digital ecosystem, creating significant challenges for stakeholders across educational, professional, and regulatory domains [5, 6].

Traditional verification methods, reliant on centralized databases and manual correspondence, are notoriously slow, costly, and vulnerable to sophisticated forgery [7-9]. Furthermore, they create substantial privacy risks by compelling individuals to over-share sensitive personal data, a practice fundamentally at odds with modern data

protection principles like the General Data Protection Regulation (GDPR) [4].

Blockchain technology offers a paradigm shift, providing a decentralized, immutable, and transparent ledger for creating a tamper-proof record of academic achievements [10, 11]. By anchoring a cryptographic fingerprint of a credential on a distributed ledger, an institution can issue a digital certificate that is perpetually and independently verifiable [12]. Despite this promise, the practical application of this technology, particularly on public permissionless blockchains like Ethereum, is fraught with challenges that have hindered widespread adoption [11, 13]. Public ledgers, while offering maximum security, introduce two primary obstacles. First, every state-changing operation incurs a transaction fee ("gas"), which can become prohibitively expensive for institutions at scale. Second, the inherent transparency of the ledger creates a privacy paradox: while necessary for auditability, it can expose transactional patterns that may compromise user privacy [11, 14].

Zero-Knowledge Proofs (ZKPs) emerge as a promising cryptographic primitive for addressing these limitations. ZKPs enable a prover to demonstrate possession of certain information or satisfaction of specific conditions without revealing the underlying data itself [4]. In the context of credential verification, ZKPs could theoretically allow individuals to prove, for example, that their GPA exceeds 3.5 without disclosing the exact value, or that they have completed required coursework without revealing specific grades or enrollment details.

Despite their theoretical promise, practical implementation of ZKPs for credential verification faces significant technical and economic challenges. Traditional ZKP implementations require on-chain verification of cryptographic proofs, incurring substantial gas costs that can exceed those of conventional verification methods. The computational complexity of proof generation has historically required specialized hardware or extended processing times, limiting accessibility for typical users. Additionally, the rigid nature of most ZKP circuits makes it difficult to support the dynamic and composite verification requirements common in educational contexts [4].

Recent advances in ZKP technology, particularly in zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) and related proof systems, have begun to address some of these technical limitations. Improved proving algorithms, browser-based proof generation, and more efficient verification procedures have made ZKPs increasingly practical for real-world deployment [4, 15-17]. However, the economic barriers associated with on-chain verification remain largely unresolved in existing literature and implementations [4].

This paper confronts this critical economic challenge head-on. We present VeriZKP, a novel architectural framework and proof-of-concept (PoC) implementation designed to demonstrate the fundamental feasibility of achieving privacy-preserving, cost-free, and granular educational credential verification on the Ethereum blockchain. Our approach is not to present a production-ready system but to provide an empirically validated blueprint that resolves the core tension between on-chain security and economic viability.

Our approach leverages three key technical innovations: (1) a strategic separation of on-chain trust anchoring from off-chain computation, ensuring that sensitive data never leaves the credential holder’s control; (2) the exploitation of Ethereum’s view function architecture to achieve truly gas-less verification through read-only smart contract calls; and (3) the implementation of a flexible challenge-response protocol that supports dynamic composite proofs while preventing replay attacks. Through our PoC, we aim to validate these architectural principles and establish a performance baseline for future, production-grade systems.

Related Works

Legacy verification systems—spanning paper-based mechanisms and isolated digital databases—exhibit systemic shortcomings that render them ill-suited to contemporary educational contexts. Such systems suffer from operational inefficiencies, heightened susceptibility to fraud, and a fundamental absence of the interoperability required within an increasingly globalized educational ecosystem [1, 7, 12, 18].

The integration of blockchain technology with privacy preserving cryptography has spurred notable advancements in educational credential verification. This section surveys existing approaches across three interrelated domains: blockchain based credentialing architectures, zero knowledge proof (ZKP) implementations, and hybrid verification frameworks. While these systems have made significant strides, they consistently fail to resolve the fundamental tension between on-chain cryptographic security and economic viability, particularly concerning verification costs. This review will demonstrate that a critical gap remains for a solution that proves the fundamental feasibility of zero-cost verification, thereby

positioning VeriZKP's contribution as a vital proof-of-concept for the field.

2. Blockchain-Based Educational Credentialing Systems

The foundational appeal of blockchain technology in educational credentialing lies in its core properties: decentralization, immutability, and cryptographic security. By leveraging a distributed ledger, institutions can issue tamper-proof digital records anchored to the blockchain, creating a permanent and verifiable "single source of truth" without relying on a central authority [8, 19].

Early pioneering efforts demonstrated the feasibility of this approach. The Blockcerts open standard, originating from the MIT Media Lab, provides a comprehensive framework for issuing cryptographic credentials that are registered on public blockchains (e.g., Bitcoin or Ethereum), owned by the recipient, and independently verifiable [11, 14]. Other significant contributions, such as EduCTX, proposed a consortium blockchain model specifically for higher education networks to streamline credit transfer and recognition among member institutions [20]. These systems successfully established a paradigm for decentralized issuance and learner-centric control.

Despite these advances, these foundational architectures share critical limitations that have hindered widespread adoption. First, they are constrained by a binary disclosure model, where verification requires revealing the entire credential. This "all-or-nothing" approach severely restricts applicability in scenarios demanding selective attribute disclosure—such as proving degree completion without revealing grades—and fundamentally conflicts with modern data minimization principles like GDPR. Second, they face persistent economic barriers. Every on-chain operation, such as issuance or revocation, incurs transaction fees ("gas"), a cost that contradicts the expectation of low-cost, high-frequency access essential for practical applications [4, 21].

Recent architectural proposals, particularly those involving Layer-2 solutions like optimistic rollups or permissioned networks, have attempted to mitigate these scalability and cost issues [4]. While platforms like Hyperledger Fabric can offer higher throughput and reduced fees [22], this efficiency comes at the cost of sacrificing the trustless properties and global accessibility that make public blockchains uniquely suited for a universal credentialing ecosystem. Consequently, a solution that simultaneously provides decentralization, privacy, and economic viability remains an open challenge.

3. Zero-Knowledge Proof Applications in Credentialing

Zero-Knowledge Proofs represent a paradigmatic shift toward privacy-preserving verification, enabling mathematical proof of statement validity without revealing underlying information. Originally formalized by Goldwasser [23], Micali, and Rackoff in the 1980s, ZKPs have evolved through practical implementations including zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) and zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge). zk-SNARKs generate extremely compact proofs with rapid verification but require trusted setup procedures, while zk-STARKs eliminate setup requirements and provide quantum resistance at the cost of larger proof sizes [4, 21].

Educational applications of ZKPs directly address pervasive issues of credential fraud and excessive data disclosure. Systems like ZUni demonstrate practical implementation by leveraging zk-SNARKs and Decentralized Identifiers on Ethereum, enabling students to prove specific qualifications without exposing comprehensive academic records [24]. Similarly, ZKBAR-V integrates ZKPs with dual-blockchain architecture, generating off-chain proofs verified by smart contracts while ensuring regulatory compliance including GDPR requirements [16].

The theoretical advantages of ZKP-based credentialing are substantial: data minimization limits information exposure to verification requirements; privacy preservation protects sensitive academic details; trustless verification eliminates reliance on issuing institutions; and identity unlinkability prevents cross-verification correlation [4, 21]. However, practical implementation faces significant technical barriers. Computational complexity traditionally requires specialized hardware or extended processing times on consumer devices [22]. More critically, on-chain proof verification incurs substantial gas costs often exceeding those of conventional verification methods, negating economic advantages while adding cryptographic complexity.

Current ZKP circuits exhibit limited flexibility for dynamic verification requirements common in educational contexts. Verifiers frequently need to construct complex logical statements involving multiple credentials, temporal constraints, and composite achievement requirements that rigid circuit designs cannot efficiently accommodate [4].

This limitation severely restricts practical deployment in real-world scenarios requiring adaptive verification logic.

4. Advanced Architectures and Remaining Trade-offs

Recognizing the limitations of purely on-chain solutions, several advanced architectures have emerged to address the dual challenges of privacy and cost. These approaches, while innovative, each introduce their own set of trade-offs [16].

One hybrid model involves adaptations of state and payment channels, which enable private, off-chain verification between parties while retaining the blockchain for dispute resolution [9]. However, their reliance on pre-established relationships makes them ill-suited for the spontaneous, open verification scenarios common in educational and professional contexts.

Orthogonal to these architectural shifts, standardization efforts like the W3C Verifiable Credentials (VC) framework have provided comprehensive data models and protocols to support selective disclosure and interoperability [6]. While the VC standard is blockchain-agnostic and highly flexible, many practical implementations depend on centralized or federated trust registries. This can reintroduce single points of failure and may not offer the robust, global security guarantees of a fully decentralized public blockchain, a critical requirement for cross-jurisdictional credentialing [25].

More recently, Layer-2 (L2) scaling solutions such as Polygon, Arbitrum, and optimistic rollups have gained prominence as a direct approach to gas optimization [16, 24]. By processing transactions off-chain and posting proofs to the mainnet, these solutions drastically reduce verification costs—from tens of dollars to mere cents. Despite this significant improvement, L2 solutions introduce new layers of complexity, potential security trade-offs in their consensus mechanisms, and critically, still fail to achieve the zero-cost verification that is ideal for enabling frequent, ubiquitous credential checks.

Our literature review identifies a fundamental trilemma in blockchain-based credentialing systems, wherein existing solutions face persistent challenges in simultaneously achieving decentralization, privacy preservation, and cost-effectiveness. The comparative analysis presented in Table 1 starkly illustrates the trade-offs inherent in prominent solutions, highlighting a clear gap in the field that VeriZKP is meticulously designed to address.

Table 1. Comparative Analysis of Credentialing Paradigms

Paradigm / System	Core Privacy Model	Verification Cost Model	Granularity (Flexibility)	Primary Trade-Off
1. Public Hash-Based (e.g., Blockcerts)	Full Data Reveal (Off-Chain)	Low (Simple On-chain Hash Check)	None (All-or-Nothing)	Sacrifices Privacy
2. Consortium Chain (e.g., EduCTX [20])	Permissioned Ledger	Low (Internal) (No Public Gas Fees)	None (All-or-Nothing)	Sacrifices Decentralization
3. On-Chain ZKP (e.g., ZKBAR-V [16], Zuni [24])	Selective Disclosure (zk-SNARK)	High (On-chain SNARK Verification Tx)	Limited (Predefined Claims)	Sacrifices Cost-Effectiveness
4. VeriZKP (Ours)	Selective Disclosure (zk-SNARK)	Zero Gas (On-chain view Call)	High (Dynamic Composite Queries)	Achieves the Trilemma (Relies on Prover Availability)

This comparative analysis reveals three fundamental gaps that prevent existing solutions from achieving widespread, practical adoption:[16]

1. Economic Viability of Verification: The high gas cost of on-chain ZKP verification remains the most significant barrier to scalability [3]. A truly practical system must reduce this cost to near-zero to encourage widespread adoption by verifiers.
2. Lack of Granularity in Proofs: Most existing systems are rigid in what can be proven, typically supporting the verification of an entire credential or a simple, predefined attribute. There is a clear need for a flexible protocol that allows a user to dynamically construct and prove composite claims (e.g., GPA > 18.00 AND course 'X' completed).
3. Practical Security and Performance: Not all ZKP-based systems explicitly address practical threats like replay attacks. Furthermore, the client-side computational overhead for generating complex proofs must remain within an acceptable threshold for a positive user experience.

VeriZKP directly addresses this combined research gap by proposing a system architecture on a single public blockchain that simultaneously (1) makes on-chain ZKP verification economically viable by reducing its cost to zero, (2) provides a flexible protocol for generating proofs of

complex and granular claims, and (3) is secured against replay attacks while demonstrating acceptable client-side performance.

5. System Architecture and Design

The architecture of VeriZKP is meticulously designed to validate our core hypothesis: that truly zero-cost, privacy-preserving credential verification is architecturally feasible on a public blockchain. The system presented here serves as a minimal and robust implementation to demonstrate the viability of a novel interaction pattern between on-chain trust and off-chain computation.

5.1. Design Principles

The entire architecture is founded upon two fundamental principles that collectively address the trade-offs limiting existing systems.

1. **Strict Separation of Data from Commitments:** In our model, the blockchain is not a database. Its sole purpose is to act as an immutable and universally accessible "bulletin board for cryptographic commitments." All Personally Identifiable Information (PII) and sensitive academic data are kept exclusively off-chain, under the full control of the credential holder. The only on-chain footprint is a single, fixed-size cryptographic hash (a Poseidon commitment), which acts as a tamper-evident anchor to the off-chain data without revealing anything about its content.
2. **Selective Disclosure through Verifiable Computation:** The system empowers users to move beyond the restrictive "all-or-nothing" disclosure model. Using a flexible Zero-Knowledge Proof circuit, a credential holder can generate a proof for complex, composite claims (e.g., "I have a GPA above 3.5 AND I passed the 'Advanced Algorithms' course") tailored to a specific verifier's request. The proof attests to the validity of these claims without disclosing any superfluous underlying information.

5.2. Dual-Layer Architecture

VeriZKP operates on a dual-layer architecture that strategically delegates responsibilities to the environment best suited for them, maximizing security, privacy, and cost-effectiveness. This architectural separation, visualized in Figure 1, is the key to resolving the tension between on-chain immutability and off-chain computational efficiency.

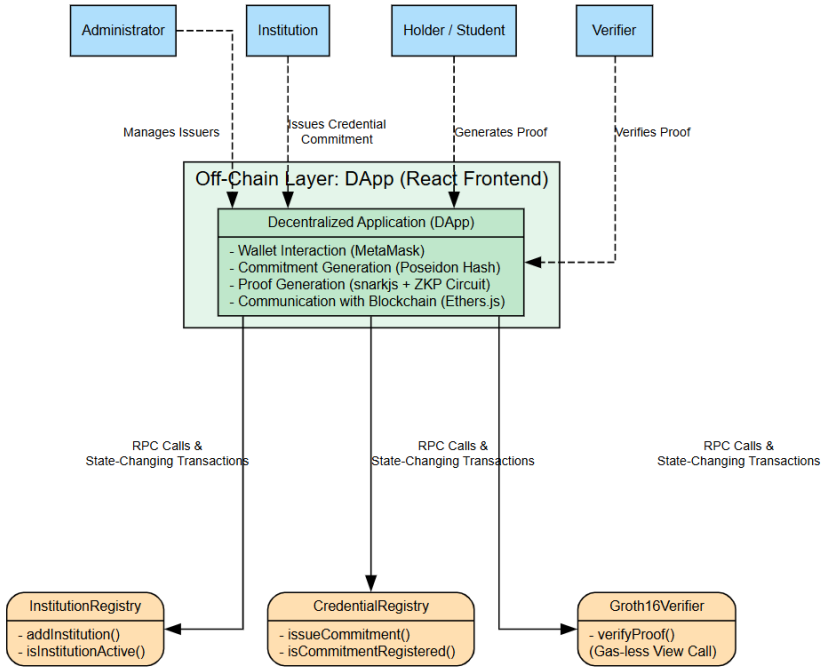

Figure 1. High-Level Architecture of the VeriZKP System

The diagram illustrates the system's actors, the separation between the client-side Off-Chain Layer (DApp) and the minimalist On-Chain Layer (Smart Contracts), and the flow of interactions for key operations.

As depicted at the bottom of Figure 1, the On-Chain Trust Layer resides on the Ethereum public blockchain and serves as the decentralized and immutable root of trust. Its responsibilities are deliberately minimalist to reduce complexity, attack surface, and gas costs. This on-chain component is composed of a suite of specialized smart contracts responsible for three critical functions:

- Managing Institutional Trust: Maintaining a transparent, on-chain whitelist of accredited institutions authorized to issue credentials.
- Notarizing Credential Existence: Acting as a public notary by recording the cryptographic commitments of issued credentials.
- Enabling Zero-Cost Verification: Providing a universal, on-chain endpoint for validating ZK-SNARK proofs without requiring a state-changing transaction.

The Off-Chain Computation Layer, shown as the central component in the diagram, encompasses all processes that occur outside the blockchain, primarily within the client's web browser via a Decentralized Application (DApp). This off-chain component is responsible for all data-intensive and privacy-sensitive operations:

- Data Sovereignty: Storing and managing the full, private credential data, ensuring it never leaves the user's device.
- Cryptographic Operations: Performing the computationally heavy tasks of generating the Poseidon commitment and, most importantly, constructing the Zero-Knowledge Proof.

This separation ensures that expensive and sensitive computations are handled in a private, user-controlled environment, while the blockchain is used only for what it does best: providing a global, censorship-resistant source of verifiable truth.

5.3. Core Architectural Components

The implemented system is built upon a set of core components whose interaction enables the novel gas-less verification mechanism.

The on-chain layer is implemented with three minimalist Solidity smart contracts:

1. InstitutionRegistry.sol: A simple, ownable contract that maintains a mapping of addresses corresponding to trusted educational institutions. It acts as the foundational trust anchor for the entire system, answering the question: "Who is allowed to issue credentials?"
2. CredentialRegistry.sol: An immutable ledger that stores the bytes32 Poseidon commitments. Its primary function, issueCommitment(), is protected to ensure only registered institutions can add new entries. It answers the question: "Has this credential been validly issued?"
3. Groth16Verifier.sol: This is the cornerstone of our economic model. It is a pre-compiled contract, auto-generated by the snarkjs toolchain, containing the verification key for our specific ZKP circuit. Its verifyProof() function is a pure function in Solidity. This technical property is critical, as it allows any Ethereum node to execute the verification logic via a simple RPC call (eth_call) without broadcasting a transaction, thereby consuming zero gas for the user initiating the call. It answers the question: "Is this cryptographic proof valid?"

The heart of VeriZKP's privacy and flexibility lies in its AdvancedCredential circuit, written in the Circom language. The circuit is designed to be both comprehensive and modular:

- **Inputs:** It takes private inputs (the *witness*), which include the full credential details, and public inputs, which form the statement being proven (the commitment hash, the specific claims, and a verifierChallenge).
- **Anti-Replay**
  Mechanism: The verifierChallenge is a unique nonce provided by the verifier for each verification request. This nonce is included as a public input to the ZKP circuit and is cryptographically bound to the proof. This ensures each proof is single-use and context-specific, rendering it useless for any other request and effectively preventing replay attacks.
- **Conditional Constraints:** The circuit uses a powerful algebraic technique to enable granular proofs. Public boolean flags control whether a particular constraint (e.g., checking the GPA) is enforced. This allows a single, unified circuit to generate proofs for a wide variety of composite claims without needing a separate trusted setup for

each potential scenario, thus maximizing flexibility while minimizing cryptographic overhead.

6. Security Model and Workflows

The operational workflows of the system demonstrate the practical application of these design principles. The credential issuance process involves an institution performing a single, low-cost on-chain transaction to register a commitment. The verification process, however, is an interactive, gas-free protocol (as shown in the sequence diagrams in the appendix A) that protects user privacy while eliminating economic barriers for verifiers. This asymmetrical design, where the infrequent operation (issuance) has a minimal, predictable cost and the frequent operation (verification) is free, is the key to the system's scalability and practical viability. Appendix B provides key user interfaces that illustrate these operational workflows.

7. Implementation

To validate our proposed architecture, we developed a fully functional implementation of the VeriZKP system. This section details the technological stack and highlights the key technical aspects of the on-chain and off-chain components, demonstrating the practical realization of our architectural principles.

7.1. Environment and Toolchain

The system was developed using a modern, open-source stack, chosen for its maturity, security, and robust developer support in the blockchain and zero-knowledge domains.

- Blockchain and Smart Contracts: The on-chain components were developed for the Ethereum blockchain using Solidity. The entire development lifecycle, including testing and deployment to the Sepolia testnet, was managed using the Hardhat framework. For secure access control, we utilized the widely-audited Ownable contract from the OpenZeppelin library.
- Zero-Knowledge Proofs: The arithmetic circuit at the core of our system was written in Circom, a domain-specific language (DSL) for ZKPs. The entire zk-SNARK lifecycle—compilation, trusted setup (Groth16), and proof generation—was managed by the snarkjs library.
- Decentralized Application (DApp): The client-side user interface was built as a single-page application using the React.js framework. Interaction with the Ethereum blockchain and user wallets (e.g., MetaMask) was handled via the Ethers.js library.

On-Chain Component Implementation

The on-chain layer was realized as a set of modular and gas-efficient smart contracts. A key security feature is the immutable link between the CredentialRegistry and the InstitutionRegistry, which is established in the constructor of the CredentialRegistry upon deployment.

The most critical component, Groth16Verifier.sol, was automatically generated via the snarkjs toolchain. The resulting contract exposes the verifyProof function, whose signature is determined by the public inputs of our circuit:

```
// Generated Function Signature in
Groth16Verifier.sol
function verifyProof(
    uint[2] memory a,
    uint[2][2] memory b,
    uint[2] memory c,
    uint[14] memory input // Flattened array of all
public signals
) public view returns (bool);
```

The view modifier is fundamental to our architecture. It designates the function as a read-only operation, allowing it to be executed via a gas-less eth_call from any Ethereum node, thereby confirming the economic feasibility of our zero-cost verification approach.

7.2. Off-Chain Component Implementation

The off-chain components handle all complex and privacy-sensitive operations entirely within the user's browser, ensuring data sovereignty.

The AdvancedCredential circuit in Circom was designed to support granular and composite proofs through conditional logic. To enforce a constraint only when requested by a verifier, we employed a specific algebraic technique. A public "flag" input (e.g., checkGpa) controls the enforcement of the corresponding constraint, as illustrated below:

```
// Snippet from credential.circom
// gpaCheck.out is 1 if the private GPA meets the
public minimumGpa
(checkGpa * gpaCheck.out) + (1 - checkGpa)
=== 1;
```

This equation elegantly implements the conditional logic. If checkGpa is 0 (false), the expression simplifies to 1 ===

1, which is always true, effectively disabling the constraint. If checkGpa is 1 (true), the expression enforces that gpaCheck.out must be 1. This modular pattern was applied to all optional claims, enabling a single, unified circuit to handle multiple verification scenarios.

The DApp orchestrates the proof generation process client-side by calling the snarkjs.groth16.fullProve function. This function takes the user's private and public inputs, along with the compiled circuit (.wasm file) and the proving key (.zkey file), which are fetched by the browser at runtime.

```
// Snippet from the DApp's React component
const { proof, publicSignals } = await
snarkjs.groth16.fullProve(
    inputs, // Object with all private & public
signals
    "/credential.wasm",
    "/credential_final.zkey"
);
```

This seamless integration of snarkjs, which internally uses WebAssembly for high performance, demonstrates that complex cryptographic operations can be executed efficiently within a standard web application, providing a practical and responsive user experience.

8. Evaluation and Results

We conducted a rigorous empirical evaluation of the VeriZKP implementation to validate its performance, economic viability, and practical feasibility. This section presents the quantitative results from our experiments, which provide strong evidence supporting the core architectural claims of this research.

8.1. Evaluation Methodology

To ensure the validity and reproducibility of our findings, a structured experimental methodology was employed. The system's smart contracts were deployed on the Ethereum Sepolia test network, providing a realistic testing environment. All client-side operations, including proof generation and verification initiation, were performed within a standard web browser (Google Chrome, Version 128.0) on a consumer laptop. Our evaluation centered on two primary scenarios designed to measure the performance of the system's core functionalities. The first scenario, Credential Issuance, evaluated on-chain costs by issuing six unique credentials with varying data complexity, containing from zero to five associated courses. The second scenario, Proof Generation and Verification, assessed computational performance by generating proofs for five cases of incrementally increasing complexity, ranging from a simple proof of a single attribute (Major ID) to a composite proof involving multiple attributes (Major ID, a minimum GPA, and three course completions). To ensure statistical stability, each reported performance timing represents the arithmetic mean of 30 consecutive runs, captured using the high-precision performance.now() browser API.

8.2. Economic Efficiency Analysis: Validating the Zero-Cost Model

The economic viability of a public blockchain system is critically dependent on its on-chain transaction costs (gas). Our analysis focused on the two primary operations in the VeriZKP lifecycle.

Issuance Cost: The cost of issuing a new credential was measured by the gasUsed value from the issueCommitment transaction receipt. As shown in Table 2, the gas cost is remarkably low and, more importantly, constant, averaging approximately 54,304 gas units regardless of the complexity of the off-chain credential data.

Table 2. On-Chain Gas Cost of Credential Issuance.

Number of Courses in Credential	Gas Cost (units)
0	54,293
1 to 5	54,305

This stability is a direct result of our architectural principle of separating data from commitments. Since the on-chain transaction only involves storing a single, fixed-size bytes32 hash, the underlying data complexity has no impact on the transaction cost. This provides predictable and scalable budgeting for issuing institutions.

Verification Cost: The on-chain cost for a verifier to validate a proof was analyzed by inspecting the DApp's network interactions with the Ethereum node. As architected, the verification process exclusively uses eth_call RPC requests to the Groth16Verifier and CredentialRegistry contracts.

Result: The gas cost for the entire end-to-end verification process is zero (0). This empirical result is arguably the most critical finding of our research. It confirms that by leveraging read-only view calls to a pre-compiled verifier contract, the entire computational and economic burden of ZKP verification can be shifted off-chain, eliminating the primary barrier to scalability and adoption for verifiers.

8.3. Computational Performance Analysis: Assessing Practical Feasibility

This analysis focuses on the off-chain computational overhead, measuring client-side proof generation time and the end-to-end verification latency experienced by the verifier.

Table 3. Proof Generation and Verification Timings by Claim Complexity.

Scenario ID	Claims Proven	Proof Generation Time (s)	Proof Verification Time (ms)
1	Major ID Only	1.02	494
2	Major ID + GPA	1.32	497
3	Major ID + GPA + 1 Course	1.48	532
4	Major ID + GPA + 2 Courses	1.52	548
5	Major ID + GPA + 3 Courses	1.63	643

The data in Table 3 reveals several key characteristics of the system's performance. First, the client-side time to generate a ZKP, ranging from 1.02 to 1.63 seconds, is well within the bounds of acceptable latency for an interactive web application. This empirically demonstrates that performing complex, composite ZKP computations directly in a browser is a feasible and user-friendly approach with modern toolchains like snarkjs and WebAssembly. Second, the results show a linear and modest growth in proof generation time that correlates directly with the complexity of the active ZKP circuit constraints. This efficient scaling indicates that the system remains performant even for highly composite proofs. Finally, the total end-to-end time for a verifier to receive a validation result is consistently under one second (ranging from 494 to 643 ms). This duration, which encompasses two sequential network round-trips to an Ethereum node and the execution of the cryptographic logic, validates our architectural choice and provides a near-instantaneous user experience.

In summary, the empirical evaluation confirms that the VeriZKP architecture is not only economically viable but also highly performant in its off-chain computations, making it a practical and effective solution for real-world use cases.

9. Discussion

The empirical results from our evaluation provide strong evidence supporting the viability and effectiveness of the VeriZKP architecture. This section provides a detailed discussion of the broader implications of these findings, contextualizes them within the existing literature through a rigorous and sourced comparative analysis, and critically examines the study’s limitations to chart a clear path for future research.

Our evaluation yields three significant insights that contribute to the broader field of decentralized identity and applied cryptography.

First, this research provides a definitive answer to a critical economic question: on-chain ZKP verification on a public blockchain can be made economically frictionless. The confirmation that the verification process is zero-cost (0 Gas) is a direct and impactful achievement. While the literature extensively documents the prohibitive cost of on-chain cryptographic computations as a major barrier to scalability, our approach demonstrates a practical and elegant solution. By leveraging a pre-compiled verifier contract that is called via gas-less view functions, we shift the entire computational burden of ZKP verification away from the blockchain's state-changing mechanism. This fundamentally alters the economic model for ZKP-based dApps, making the most frequent operation in the ecosystem—verification—completely free for the verifier.

Second, our results directly address the persistent concern regarding the practicality of client-side proof generation. The literature often highlights the computational overhead of generating ZKPs as a significant user experience challenge, particularly on user-owned devices. Our empirical data, showing that generating a complex,

composite proof takes between 1.0 to 1.7 seconds in a standard browser, is highly encouraging. This demonstrates that for a well-defined application domain like credential verification, the performance of modern ZKP toolchains (snarkjs and WebAssembly) is more than sufficient for a positive user experience.

Finally, the successful implementation of proofs for composite claims validates the core novelty of our flexible ZKP circuit design. This capability represents a significant functional advancement over many existing systems. Unlike solutions that focus on proving the validity of an entire credential (e.g., ZUni) or are limited to predefined data sets (e.g., ZKBAR-V), our system demonstrates a protocol that is highly dynamic. It allows a holder to construct, on-demand, a single, atomic proof precisely tailored to a verifier's specific and potentially complex requirements.

Comparative Analysis with State-of-the-Art Systems

To quantitatively assess VeriZKP's contributions, we compare its performance and economic characteristics against prominent systems from the literature. Table 4 provides an updated and sourced comparison based on data reported in the respective studies.

Table 4. Sourced Comparative Analysis of Blockchain-Based Credentialing Systems.

System	Issuance Cost (Gas)	Verification Cost (Gas)	Privacy / Granularity	Proof Gen. Time
VeriZKP (Ours)	~54,304 (Constant)	0 (Gas-less view call)	High / Full Granularity	1.0s - 1.7s
BZDIMS [26]	153,859 - 256,865 (Scales)	304,962 (On-chain Tx)	High / Partial Granularity	4.2s - 14.3s
Zuni [23]	N/A (Polygon L2)	Off-Chain (Centralized)	High / No Granularity	8s - 9s
ZKBAR-V [16]	226,858 (on zkEVM L2)	Off-Chain (5.8ms latency)	High / Partial Granularity	2.8s
ElimuChain [27]	~418,888 (BSC)	0 (Read-only call)	Low / No Granularity (Hash)	N/A
CrossCert [28]	660,478 (on Viction)	1,195,474 (On-chain Tx)	High / Not Specified	N/A

Note: Gas units provide a stable metric for computational footprint, independent of volatile crypto prices.

The economic model is where VeriZKP provides its most significant contribution. The key differentiator is the zero-cost verification. On-chain verification transactions in systems like BZDIMS and CrossCert are prohibitively expensive for frequent use. While systems like ZKBAR-V and ZUni also achieve zero-cost verification for the user, they do so by moving the process entirely off-chain, which can introduce dependencies on specific services or infrastructures. ElimuChain offers free verification but at the complete expense of privacy, as it only validates a hash and requires revealing the full original document. VeriZKP architecturally eliminates this trade-off, providing a robust, on-chain cryptographic security guarantee at zero cost to the verifier—a novel and highly practical contribution.

Furthermore, VeriZKP's issuance cost of ~54k gas is not only exceptionally efficient but also constant, contrasting sharply with the scaling costs of BZDIMS or the higher fixed costs of ZKBAR-V and CrossCert. This offers predictable budgeting for institutions. In terms of performance, our client-side proof generation time (1.0s - 1.7s) is highly competitive and substantially better than the times reported by ZUni and BZDIMS, validating that a fully browser-based ZKP experience is both possible and responsive for this application domain.

10. Limitations and Future Work

While this research successfully demonstrates the viability of the proposed model, we acknowledge the limitations inherent to its scope as a proof-of-concept.

- Security and Production Readiness: The implementation has not been subjected to a formal security audit. Most critically, it lacks a fully developed on-chain mechanism for credential revocation, an essential feature for any production-grade identity system. Additionally, our use of the Groth16 protocol necessitates a circuit-specific trusted setup, which would require a multi-party computation (MPC) ceremony in a production environment.
- **Evaluation Scope:** All performance metrics were collected on the Sepolia test network. Real-world conditions on the Ethereum mainnet, such as network congestion and volatile gas prices, could impact the cost and latency of issuance transactions.

These limitations define a clear roadmap for future research. Promising directions include implementing a robust and privacy-preserving revocation mechanism (e.g., using Merkle trees or accumulators); migrating the system to Layer-2 scaling solutions like ZK-Rollups to drastically

reduce issuance costs; exploring "transparent" ZKP schemes like PLONK or STARKs to eliminate the trusted setup requirement; and ensuring full compliance with W3C DID/VC standards to enhance interoperability.

11. Conclusion

This paper confronted the persistent trade-offs between cost, privacy, and flexibility that have hindered the widespread adoption of blockchain-based educational credential verification. We introduced VeriZKP, a novel system architecture designed as a proof-of-concept to demonstrate the fundamental feasibility of a new paradigm: truly zero-cost, granular, and privacy-preserving verification on a public blockchain. By strategically combining a minimalist on-chain trust anchor with powerful client-side cryptographic computations, our work provides an empirically validated blueprint for the future of decentralized digital identity. The successful validation of our zero-cost economic model, achieved by leveraging gas-less view functions, fundamentally alters the viability of ZKP-based applications on public ledgers.

The contributions of this research are significant. We have established a crucial performance baseline, confirming that generating complex, composite zero-knowledge proofs on standard client-side hardware is both feasible and highly practical, with generation times consistently under 1.7 seconds. Furthermore, the dual-layer, asymmetrical design of VeriZKP serves as a reusable and efficient architectural framework for other decentralized identity systems that must balance practical usability with robust, on-chain security guarantees. In essence, the VeriZKP system successfully resolves the core tensions that have challenged previous approaches. The demonstration of zero-cost verification, combined with practical client-side performance and high functional granularity, represents a significant step toward building more secure, efficient, and user-centric identity systems, establishing both the technical feasibility and a clear research roadmap for the next generation of digital credentialing solutions.

Authors' Contributions

Authors equally contributed to this article.

Acknowledgments

Authors thank all participants who participate in this study.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

References

[1] A. S. Alammary, "Building a Sustainable Digital Infrastructure for Higher Education: A Blockchain-Based Solution for Cross-Institutional Enrollment," *Sustainability*, vol. 17, no. 1, 2025, doi: 10.3390/su17010194.

[2] S. Feng, X. Xu, S. Li, Z. Li, and D. Gibson, "Is metaverse a buzzword in education? Insights from a systematic review," *Educational technology research and development*, vol. 72, no. 6, pp. 3349-3390, 2024, doi: 10.1007/s11423-024-10398-2.

[3] A. C. Y. Leung, D. Y. W. Liu, X. Luo, and M. H. Au, "A constructivist and pragmatic training framework for blockchain education for IT practitioners," *Educ Inf Technol (Dordr)*, vol. 29, no. 12, pp. 15813-15854, 2024, doi: 10.1007/s10639-024-12505-5.

[4] L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, p. 103678, 2024, doi: 10.1016/j.jisa.2023.103678.

[5] M. Gottlieb, C. Deutsch, F. Hoops, H. Pongratz, and H. Krcmar, "Expedition to the blockchain application potential for higher education institutions," *Blockchain: Research and Applications*, vol. 5, no. 3, p. 100203, 2024, doi: 10.1016/j.bcra.2024.100203.

[6] M. Sporny, G. Noble, D. Longley, D. C. Burnett, and B. Zundel, "Verifiable Credentials Data Model v1.1," W3C, 2022.

[7] T. Chandra, M. Kaur, N. Rakesh, M. Gulhane, and S. Maurya, "Novel blockchain-based framework to publish, verify, and store digital academic credentials of universities," *International Journal of Information Technology*, vol. 16, no. 5, pp. 3273-3281, 2024, doi: 10.1007/s41870-024-01842-w.

[8] F. Loukil, M. Abed, and K. Boukadi, "Blockchain adoption in education: a systematic literature review," *Educ Inf Technol (Dordr)*, vol. 26, no. 5, pp. 5779-5797, 2021, doi: 10.1007/s10639-021-10481-8.

[9] R. Poorni, M. Lakshmanan, and S. Bhuvaneswari, "DIGICERT: a secured digital certificate application using blockchain through smart contracts," in *2019 International Conference on Communication and Electronics Systems (ICCES)*, 2019, pp. 215-219, doi: 10.1109/ICCES45898.2019.9002576.

[10] A. Choudhary, M. Chawla, and N. Tiwari, "Analyzing functional, technical and bibliometric trends of blockchain applications in education: A systematic review," *Multimed*

Tools Appl, pp. 1-46, 2024, doi: 10.1007/s11042-024-20303-x.

[11] X. Wang, M. Younas, Y. Jiang, M. Imran, and N. Almusharraf, "Transforming Education Through Blockchain: A Systematic Review of Applications, Projects, and Challenges," 2025, doi: 10.1109/ACCESS.2024.3519350.

[12] M. F. Steiu, "Blockchain in education: Opportunities, applications, and challenges," *First Monday*, vol. 25, no. 9, 2020, doi: 10.5210/fm.v25i9.10654.

[13] A. Mohammad and S. Vargas, "Challenges of using blockchain in the education sector: A literature review," *Applied Sciences*, vol. 12, no. 13, p. 6380, 2022, doi: 10.3390/app12136380.

[14] P. Rani, R. K. Sachan, and S. Kukreja, "A systematic study on blockchain technology in education: initiatives, products, applications, benefits, challenges and research direction," *Computing*, vol. 106, no. 2, pp. 405-447, 2024, doi: 10.1007/s00607-023-01228-z.

[15] E. Ben Sasson, S. Micali, N. Zcash, and et al., "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE symposium on security and privacy*, 2014, pp. 459-474, doi: 10.1109/SP.2014.36.

[16] J. A. Berrios Moya, J. Ayoade, and M. A. Uddin, "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System," 2025, doi: 10.3390/s25113450.

[17] M. Lupu and I. Aciob\uani\ctei, "Enhanced Blockchain-Based e-Voting System Using Zero-Knowledge Proofs," in *International Conference on Informatics in Economy*, 2024, pp. 237-246, doi: 10.1007/978-981-96-0161-5_21.

[18] E. Tan, E. Lerouge, J. Du Caju, and D. Du Seuil, "Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy," *Big Data and Cognitive Computing*, vol. 7, no. 2, 2023, doi: 10.3390/bdcc7020079.

[19] Z. Ziyi Li and et al., "Blockchain-based Solutions for Education Credentialing System: Comparison and Implications for Future Development," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022, pp. 79-86, doi: 10.1109/Blockchain55522.2022.00021.

[20] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," *IEEE Access*, vol. 6, pp. 5112-5127, 2018, doi: 10.1109/ACCESS.2018.2789929.

[21] X. Xu, "Zero-knowledge proofs in education: a pathway to disability inclusion and equitable learning opportunities," *Smart Learning Environments*, vol. 11, no. 1, p. 7, 2024, doi: 10.1186/s40561-024-00294-w.

[22] W. Yin, "Zero-knowledge proof intelligent recommendation system to protect students' data privacy in the digital age," *Applied Artificial Intelligence*, vol. 37, no. 1, p. 2222495, 2023, doi: 10.1080/08839514.2023.2222495.

[23] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," in *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, *STOC '85*, 1985, pp. 291-304, doi: 10.1145/22145.22178.

[24] M. C. Nguyen-Ngoc, T. V. Tran, T. Nguyen, K. T. Vo, T. A. Nguyen-Hoang, and N. T. Dinh, "ZUni: The Application of Blockchain Technology in Validating and Securing Educational Credentials," in *International Conference on Intelligence of Things*, 2023, pp. 258-268, doi: 10.1007/978-3-031-46749-3_25.

[25] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K. K. R. Choo, "Blockchain-based identity management systems: A review," *Journal of network and computer applications*, vol. 166, p. 102731, 2020, doi: 10.1016/j.jnca.2020.102731.

[26] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Comput Secur*, vol. 99, p. 102050, 2020, doi: 10.1016/j.cose.2020.102050.

[27] 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 & Applied Science Research*, vol. 13, no. 5, pp. 11691-11704, 2023, doi: 10.48084/etasr.6170.

[28] T. D. Tran, P. K. Minh, T. L. T. Thuy, P. T. Duy, N. T. Cam, and V. H. Pham, "CrossCert: A Privacy-Preserving Cross-Chain System for Educational Credential Verification Using Zero-Knowledge Proof," in *International Conference on Industrial Networks and Intelligent Systems*, 2024, pp. 256-271, doi: 10.1007/978-3-031-67357-3_18.