Vineet Sen, et.al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 16, Issue 6, June 2026, pp 41-49

RESEARCH ARTICLE OPEN ACCESS

Blockchain-Based Decentralized Academic Credential Verification System with Privacy Preservation

Vineet Sen[1], Isha Sharma[2], Rakesh Kumar Tiwari[3], Onkar nath Thakur[4]
[1]*Department of Artificial Intelligence and Machine Learning*
Technocrats Institute of Technology - Computer Science and Engineering, Bhopal, India
[2]*Department of Computer Science & Engineering Technocrats Institute of Technology & Science Bhopal, India*
[3]*Department of Computer Science & Engineering Technocrats Institute of Technology & Science Bhopal, India*
[4]*Department of Computer Science & Engineering Technocrats Institute of Technology & Science Bhopal, India*

ABSTRACT—
The rapid digitization of education has exposed critical vulnerabilities in traditional academic credential systems. Paper-based certificates are easily forged, while centralized digital databases suffer from single points of failure, hacking vulnerabilities, and privacy inadequacies. Blockchain technology offers a promising solution for decentralized, immutable credential management. However, existing systems consistently fail to address three fundamental requirements simultaneously: Self-Sovereign Identity (SSI) principles, privacy-preserving selective disclosure, and compliance with modern standards such as W3C Verifiable Credentials Data Model (VCDM), Open Badges 3.0, and OpenID for Verifiable Credentials (OID4VCI/OID4VP).
This survey systematically reviews blockchain-based academic credential verification literature, drawing from three primary IEEE sources covering permissioned blockchain systems, a PRISMA-based Systematic Literature Review of 34 studies, and a comprehensive analysis of Decentralized Identifiers (DIDs) and Verifiable Credentials. Through thematic analysis, we identify six major research themes and six critical gaps. Comparative analysis of 12 existing systems demonstrates that no current implementation integrates BBS+ zero-knowledge proofs, SSI architecture, and modern credential exchange protocols within a unified framework. This survey establishes the theoretical foundation required to design next-generation privacy-preserving decentralized academic credential systems.
Keywords— *Blockchain, Academic Credential Verification, Self-Sovereign Identity (SSI), Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), Zero-Knowledge Proofs (ZKP), BBS+ Signatures, W3C Standards, OID4VCI, IPFS.*

Date of Submission: 08-06-2026 Date of acceptance: 18-06-2026

I. INTRODUCTION

Academic credential fraud is a well-documented and growing global problem. According to a Forbes study cited by Rustemi et al. [2], the degree mill industry generates an estimated $7 billion annually through fraudulent diplomas and transcripts. High-profile cases—such as a Philippine court clerk falsifying school records for employment and MIT's former Dean of Admissions misrepresenting her qualifications for nearly three decades—demonstrate that even prestigious institutions are not immune [1]. Career Builder surveys indicate that 33% of job applicants misrepresent their academic qualifications, while 53% of resumes worldwide contain some fraudulent information [1].

The fundamental challenge is that the relationship between forging credentials and verifying them is inversely proportional: forging a paper-based diploma can take mere hours, while authentic verification can take days or weeks [1]. Traditional verification requires contacting the original issuing institution, which then consults centralized or local databases—a process that is slow, expensive, and often infeasible across borders. Digital databases, while faster, introduce their own vulnerabilities: system errors, hacking, and centralized single points of failure [1].

Blockchain technology offers a fundamentally different approach. As a decentralized, cryptographically secured, and immutable distributed ledger, blockchain can record credential transactions in a way that is transparent, tamper-proof, and independently verifiable without relying on any central authority [2]. Early implementations such as

BlockCert, CredenceLedger, Open Certificate, and Gradbase demonstrated the technical feasibility of blockchain-based credential systems [20]. However, a comprehensive systematic review of 1,744 papers from 2018 to 2022 found only 34 studies substantive enough for analysis, revealing how immature the field remains [2].

More critically, a 2025 IEEE Communications Surveys & Tutorials paper on Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) [3] reveals that the evolution of digital identity has progressed well beyond simple blockchain anchoring. The latest paradigm—Self-Sovereign Identity (SSI)— places the credential holder in full control of their digital identity, enabling selective disclosure of credential attributes without revealing unnecessary personal information. This is enabled by technologies such as W3C-standardized DIDs and VCs, BBS+ signature schemes, and protocol standards including OID4VCI and OID4VP. Yet none of these advanced capabilities appear in existing academic credential systems reviewed in the literature.

This survey bridges this gap by systematically analyzing three foundational IEEE papers and their implications for the design of next-generation academic credential systems. We identify the evolution of the field, map critical research gaps, and propose future research directions aligned with the state of the art in decentralized identity.

A. Motivation

India's National Education Policy (NEP) 2020 [15] and the growing emphasis on digital credentials in professional hiring underscore the urgency of reliable, interoperable, and privacy respecting credential systems. The Academic Bank of Credits (ABC) initiative and DigiLocker platform highlight the policy environment, but technical implementations remain inadequate. The convergence of three trends—the standardization of SSI by W3C, the proliferation of online credentials, and increasing privacy regulations including India's DPDP Act 2023—creates both urgency and opportunity for a comprehensive technical solution.

B. Research Questions

This survey is guided by the following research questions:

- **RQ1:** What blockchain architectures and credential management approaches have been proposed for academic credential verification?
- **RQ2:** What privacy mechanisms exist in current systems, and what are their limitations?
- **RQ3:** How do Self-Sovereign Identity principles and W3C standards apply to academic credentials?
- **RQ4:** What critical research gaps remain, and what directions should future systems pursue?

C. Paper Organization

Section II provides background on core technologies. Section III describes the survey methodology. Section IV presents thematic analysis across six themes. Section V provides comparative analysis of existing systems. Section VI identifies research gaps. Section VII concludes with future directions.

II. BACKGROUND AND RELATED TECHNOLOGIES

A. Blockchain Technology

Blockchain is a decentralized, append-only ledger in which records—organized into cryptographically linked "blocks"— are distributed across a peer-to-peer network of nodes. Each block contains a hash of the previous block, a timestamp, a Merkle root summarizing all transactions in the block, and transaction data [1], [2]. This structure ensures immutability: any modification to a historical record changes its hash value, which propagates through all subsequent blocks, making tampering immediately detectable [2].

Blockchain systems are classified into three primary categories. Public blockchains (e.g., Bitcoin [12], Ethereum) allow open, permissionless participation, providing maximum transparency and decentralization but at the cost of scalability, energy consumption, and transaction speed. Private blockchains restrict participation to authorized nodes, offering higher throughput, lower costs, and privacy controls. Consortium or hybrid blockchains combine elements of both, allowing controlled access for defined stakeholder groups—an approach particularly well-suited to multi-institutional academic ecosystems [2].

The evolution of blockchain from purely financial applications (Blockchain 1.0: Bitcoin) through smart contract platforms (Blockchain 2.0: Ethereum) to cross-industry applications (Blockchain 3.0: Hyperledger, Multichain) and Blockchain-as-a-Service (Blockchain 4.0: IBM BaaS, Azure) is documented by Arenas and Fernandez [1], who position academic credentials within this evolution as a Blockchain 3.0 use case.

B. Smart Contracts

Smart contracts are self-executing programs stored on a blockchain that automatically enforce predefined rules when specific conditions are met [2], [3]. In academic credential systems, smart contracts can automate diploma issuance when a student completes all academic and financial obligations, trigger verification checks in real time, and manage access control policies without human intermediaries

[2]. Ethereum's Solidity language [16] and Hyperledger Fabric's chaincode [18] are the most widely used platforms. However, the immutability of smart contracts—a security feature—also complicates credential revocation, since deployed contracts cannot be easily updated [2].

C. Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs)

Self-Sovereign Identity represents the latest paradigm in digital identity management, following centralized, federated, and user-centric identity models [3], [19]. In an SSI system, individuals maintain full control over their digital identities without depending on centralized identity providers. This is achieved through Decentralized Identifiers (DIDs)—globally unique, cryptographic identifiers standardized by the W3C [5]— and Verifiable Credentials (VCs), which carry cryptographically signed claims about the DID subject [3].

A DID consists of three components: a URI scheme (did:), a DID method identifier (e.g., indy, ethr, web), and a method-specific identifier. Each DID resolves to a DID Document stored on a Verifiable Data Registry (VDR), typically a distributed ledger, containing the DID subject's public keys, service endpoints, and authentication parameters [3]. The DID Controller—which may be the DID subject themselves in an SSI system—has the authority to update the DID Document.

Mazzocca et al. [3] identify three types of DIDs: Anywise DIDs (usable with any number of parties, maximizing interoperability), Pairwise DIDs (known only to two parties, minimizing correlation), and N-wise DIDs (for defined groups). For academic credential systems, pairwise DIDs offer significant privacy advantages, as they prevent different verifiers (employers, universities) from correlating a student's credential presentations across contexts.

D. Verifiable Credentials (VCs) and Selective Disclosure

W3C Verifiable Credentials (VCs) provide a standardized, cryptographically verifiable data structure for expressing claims about a DID subject. A VC contains the issuer's DID, the subject's DID, the credential claims (e.g., degree type, institution name, graduation date), validity period, and a cryptographic proof [3]. VCs are stored in the credential holder's digital wallet and presented to verifiers as Verifiable Presentations (VPs), which may include proofs from multiple VCs.

Selective disclosure is a critical privacy feature of VCs that allows holders to reveal only specific attributes without exposing their complete credential or identity [3]. Mazzocca et al. [3] categorize selective disclosure mechanisms into mono claims, hashed values, Zero-Knowledge Proofs (ZKP), and selective disclosure signatures. The current state-of-the-art solution is SD-JWT [10], which replaces plaintext claims with salted digests. More powerful still, BBS+ signatures enable multi-message selective disclosure: a student could prove they hold a valid degree from an accredited institution without revealing their grades, student ID, or graduation date.

E. IPFS and Decentralized Storage

The InterPlanetary File System (IPFS) [17] is a content-addressed, distributed file system where each piece of data is identified by a Content Identifier (CID) derived from a cryptographic hash of its contents [3]. In blockchain-credential systems, IPFS serves as off-chain storage for full credential documents, with only the CID stored on-chain. Any modification to the stored document changes its CID, enabling immediate tamper detection.

F. OID4VCI and OID4VP Protocols

OpenID for Verifiable Credential Issuance (OID4VCI) [7] and OpenID for Verifiable Presentations (OID4VP) [8] are protocol standards developed by the OpenID Foundation for standardized issuance and presentation of W3C VCs [3]. OID4VCI defines a REST API through which credential issuers can issue VCs to credential wallets, while OID4VP defines how holders present credentials to verifiers using standard OAuth 2.0 flows. These protocols are critical for cross-institutional interoperability.

G. Digital Identity Evolution

Mazzocca et al. [3] trace digital identity through four evolutionary eras (Fig. 1): Centralized (IANA, ICANN, user names/passwords), Federated (Microsoft Passport, Liberty Alliance, SAML, OpenID), User-Centric (OpenID Connect, OAuth 2.0, FIDO), and Self-Sovereign Identity (2012–present, based on DIDs and VCs). Each era addressed limitations of the previous: federated identity reduced fragmentation but concentrated trust; user-centric identity gave individuals more control but still depended on centralized providers. SSI, the current frontier, eliminates centralized intermediaries entirely. Academic credential systems reviewed in the literature are mostly stuck in the Centralized or at best Federated era, missing the significant advances of the SSI paradigm.

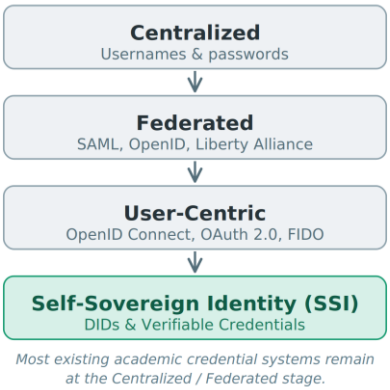

Fig. 1. Evolution of digital identity management models, from centralized to Self-Sovereign Identity.

III. SURVEY METHODOLOGY

A. Research Approach

This survey employs a structured thematic analysis approach, building upon the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework [14] used by Rustemi et al. [2]. Rather than conducting an independent search from scratch, this survey synthesizes findings from three comprehensive primary sources covering the state of the art from multiple perspectives: system implementation (CredenceLedger [1]), systematic literature review of blockchain-based credential systems [2], and the broader decentralized identity landscape [3].

TABLE I
PRIMARY SOURCES USED IN THIS SURVEY

Paper	Type	Scope	Year
Arenas & Fernandez [1]	System Paper	Permissioned blockchain using Multichain	2018
Rustemi et al. [2]	SLR	34 papers, PRISMA, 2018–2022	2023
Mazzocca et al. [3]	Survey	DIDs, VCs, SSI, implementations, regulations	2025

B. Primary Source Overview

Table I presents an overview of the three primary sources used in this survey.

C. Scope and Limitations

This survey covers academic credential systems published between 2018 and 2025. We focus specifically on technical systems for credential issuance, storage, and verification—not broader blockchain-in-education applications such as payment systems or learning management. We include both peer-reviewed academic papers and standardization documents (W3C, IETF, OpenID Foundation) where relevant to understanding the technology landscape.

IV. THEMATIC ANALYSIS

Drawing from all three primary sources, we identify six major themes (Fig. 2) that collectively characterize the research landscape in blockchain-based academic credential systems.

Fig. 2. Taxonomy of the six research themes identified across the surveyed literature.

A. Theme 1: Blockchain Architecture and Classification

The choice of blockchain architecture fundamentally determines a system's properties of scalability, privacy, access control, and cost. Rustemi et al. [2] identify three blockchain categories applied in academic credential systems: public (permissionless), private (permissioned), and consortium (hybrid).

Public blockchain systems dominate the literature (approximately 65% of reviewed implementations). Bitcoin-based systems like BlockCert and Gradbase anchor credential hashes in Bitcoin transactions, providing maximum transparency and trustlessness. Ethereum-based systems such as Open Certificate and BCDIPLOMA use smart contracts for automatic credential generation and management. However, public blockchain systems face significant challenges: high and volatile transaction costs, limited throughput (15–20 TPS for Ethereum), energy consumption, and the paradox of transparency conflicting with privacy requirements [2].

CredenceLedger [1] represents the permissioned approach, using the open-source Multichain platform [13] with stream-based data management. Permissioned blockchain nodes are added by invitation only, restricting participation to authorized educational stakeholders. This approach offers higher throughput, lower costs, smaller chain size, and no need for cryptocurrency. The mining

diversity scheme set at 0.75 keeps technical failures and malicious collusion below 0.001%.

Mazzocca et al. [3] add further nuance by documenting how the Verifiable Data Registry (VDR)—the infrastructure storing DID Documents—relates to blockchain choice. While most VDR implementations use blockchains, alternatives like IOTA's Tangle (a DAG-based DLT) offer feeless DID registration, which could be transformative for developing country educational contexts.

B. Theme 2: Credential Issuance and Lifecycle Management

Academic credential systems must support the full credential lifecycle: issuance, storage, verification, and revocation. Each stage presents distinct technical challenges.

Credential issuance through smart contracts is the dominant approach in the literature. Smart contracts automatically issue credentials when predefined conditions are met—course completion, examination pass rates, payment confirmation [2]. However, the immutability of smart contracts complicates updating credential formats or correcting errors.

The W3C VC model documented by Mazzocca et al. [3] offers a more structured approach to credential issuance. In the W3C model, an Issuer (university) creates a VC containing structured claims about a Holder (student), signs it with the issuer's private key, and delivers it to the holder's wallet. The holder can then present the VC as a Verifiable Presentation (VP) to a Verifier (employer). This three-party Issuer-Holder-Verifier model (Fig. 3) is well-established in digital identity theory but has not been implemented in any existing academic credential system reviewed by Rustemi et al. [2].

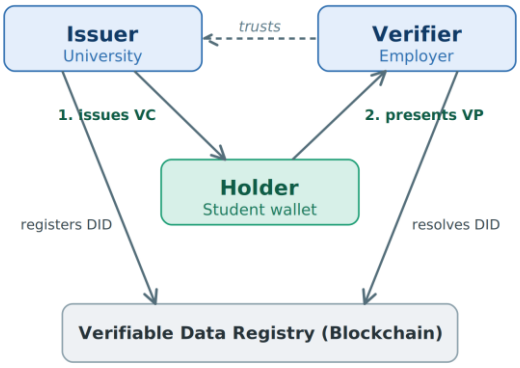

Fig. 3. The W3C Issuer–Holder–Verifier trust model for verifiable credentials.

Credential revocation is identified by both Rustemi et al. [2] and Mazzocca et al. [3] as a critical unsolved problem. Blockchain immutability means that once a credential is issued, the blockchain record cannot be deleted. Existing solutions include revocation registries, the W3C Revocation List 2020, and cryptographic accumulator-based approaches

C. Theme 3: Privacy Preservation and Selective Disclosure

Privacy is the most critically underdeveloped dimension of existing academic credential systems. The fundamental tension is that blockchain's core value proposition—transparency and immutability—directly conflicts with privacy requirements in educational contexts.

GDPR compliance is a significant challenge for European deployments. The GDPR's "right to be forgotten" (Article 17) is structurally incompatible with blockchain immutability [2]. Rustemi et al. [2] document several partial solutions: off-chain storage with on-chain hashes, encryption of data before on-chain storage, and permissioned architectures that restrict data visibility.

The selective disclosure gap is most significant. All existing academic credential systems identified by Rustemi et al. [2] operate on an all-or-nothing disclosure model. Mazzocca et al. [3] document how selective disclosure mechanisms—particularly SD-JWT and BBS+ signatures—address this limitation. With BBS+ signatures, a student could prove to an employer that they hold a degree from an accredited institution without revealing their specific grades, student ID number, thesis title, or graduation date. No reviewed system implements this capability.

Mazzocca et al. [3] document specific privacy threats in DID/VC systems including credential validity attacks, credential correlation, and man-in-the-middle attacks. Pairwise DIDs provide strong unlinkability guarantees. Combining pairwise DIDs with BBS+ selective disclosure creates a system where even the same credential can be presented differently to different verifiers without enabling correlation.

D. Theme 4: Enabling Technologies and Implementation Stack

The technology stack of blockchain-based credential systems has significant implications for adoption, cost, security, and interoperability. Smart contract development platforms— primarily Solidity on Ethereum—dominate the literature [2].

Digital wallet implementations are critical but often neglected in academic credential research. Mazzocca et al. [3] provide a comprehensive comparison of DID/VC implementations including Hyperledger Aries (open-source, most enterprise grade, supports BBS+ signatures), DIDKit (Rust-based, multi-platform, supports SD-JWT), IOTA Identity (IoT-optimized, feeless), and Veramo (JavaScript, plugin-

based). Among these, Hyperledger Aries' ACA-Py [9] is the most relevant for academic credential systems, providing production-ready DID management, VC issuance/verification, and BBS+ selective disclosure support.

The Hyperledger Indy blockchain, purpose-built for identity management, provides specific advantages for academic credential systems: built-in DID method (did:indy), support for BBS+ signatures natively, revocation registry support, and a permissioned consortium model suitable for consortiums of universities [3].

E. Theme 5: Standards Compliance and Interoperability

Standards compliance is critical for cross-institutional interoperability but is almost entirely absent from existing academic credential systems. Rustemi et al. [2] find that no reviewed system implements W3C VCDM [4], Open Badges 3.0 [6], CLR 2.0, or any OID4VC protocols. This means credentials from one blockchain system cannot be verified by another—creating a fragmented landscape of incompatible silos.

Mazzocca et al. [3] document the European EBSI (European Blockchain Services Infrastructure) [11] initiative, which uses DIDs and VCs for cross-border educational credential verification between EU universities. The ELMO2EDS project converts existing EMREX digital credentials into EBSI-compatible SSI format. These European initiatives provide concrete implementation blueprints for academic credential interoperability.

OID4VCI and OID4VP protocols enable standardized credential exchange flows compatible with existing OAuth 2.0 infrastructure [3]. An academic institution supporting OID4VCI can issue VCs to any compatible wallet, while any OID4VP compatible verifier can request and verify credentials. This protocol layer is the key to ecosystem-level interoperability and is completely absent from existing academic credential systems in the literature.

F. Theme 6: Security Threats and Mitigation

Mazzocca et al. [3] provide the most systematic threat analysis for DID/VC systems, identifying four threat categories with specific mitigations relevant to academic credential security.

Key and Credential Compromise: An adversary may compromise a student's private key or steal a valid credential, enabling impersonation. Mitigations include key rotation, Hardware Security Modules (HSMs) for secure key storage, multi-factor authentication for wallet access, and binding the credential to a biometric or FIDO authenticator.

Credential Validity Attacks: A revoked credential may still be presented if the verifier does not check the revocation registry. The W3C Revocation List 2020 provides a scalable solution using a bitstring where each credential is assigned an index.

Privacy Threats: Credential correlation is addressed through pairwise DIDs and BBS+ unlinkable presentations. Mazzocca et al. [3] note that even SD-JWT discloses the number of claims in a credential, enabling inference attacks. BBS+ signatures eliminate this vulnerability by generating independent, unlinkable proofs for each presentation.

Man-in-the-Middle Attacks: Communications between credential holders and verifiers can be secured through DIDComm—a secure, end-to-end encrypted messaging protocol built on DID-based authentication [3].

V. COMPARATIVE ANALYSIS OF EXISTING SYSTEMS

Table II presents a comprehensive comparative analysis of key academic credential systems against dimensions critical for a privacy-preserving decentralized system. The comparative analysis reveals a stark pattern: existing systems prioritize immutability and basic hash-based verification while consistently neglecting privacy, SSI integration, and standards compliance.

The EBSI initiative in Europe, documented by Mazzocca et al. [3], represents the closest approach to the proposed direction, implementing W3C VCDM and partial OID4VC support. However, EBSI's use of Hyperledger Fabric rather than Hyperledger Indy means it lacks native BBS+ support for full selective disclosure. The proposed research direction addresses all identified gaps simultaneously, representing a significant advancement over the state of the art.

VI. RESEARCH GAPS AND OPEN CHALLENGES

Based on systematic analysis of all three primary sources,

we identify six critical research gaps that collectively define the frontier for next-generation academic credential systems.

A. Gap 1: Absence of Self-Sovereign Identity Architecture

No existing academic credential system implements SSI principles. All reviewed systems maintain institution-centric architectures where credential validity depends on institutional databases or blockchain records controlled by issuing institutions. True SSI requires that credential holders fully own their credentials—stored in their wallets, presented without institutional mediation, and verifiable by

anyone with the issuer's public key. Rustemi et al. [2] explicitly identify SSI as a research direction, while Mazzocca et al. [3] provide comprehensive implementation blueprints through Hyperledger Aries and related frameworks.

B. Gap 2: No Implementation of Selective Disclosure with BBS+ Signatures

The all-or-nothing disclosure model of existing systems violates the data minimization principle central to both GDPR and SSI design philosophy. Mazzocca et al. [3] document multiple selective disclosure mechanisms including SD-JWT, ZKSD (Zero-Knowledge Selective Disclosure), ZKP, and BBS+ signatures. ZKP allows a prover to demonstrate knowledge of certain credential attributes to a verifier without revealing the actual underlying data. BBS+ signatures extend this further by enabling multi-message selective disclosure: a student can prove a subset of their credential claims without revealing others, and each such proof is cryptographically unlinkable across different presentations, preventing verifier correlation. SD-JWT offers a simpler but less privacy-preserving alternative, with the limitation that it still discloses the total number of claims—a limitation that BBS+ eliminates entirely. No reviewed academic credential system implements any form of selective disclosure, ZKP, or BBS+ signatures.

C. Gap 3: Incomplete and Inconsistent Revocation Mechanisms

Credential revocation is consistently identified by both Rustemi et al. [2] and Mazzocca et al. [3] as a major unsolved problem. Existing systems either lack revocation entirely or implement ad-hoc solutions incompatible with blockchain immutability. The W3C Revocation List 2020, OCSP-inspired revocation registries, and cryptographic accumulator-based approaches each offer viable solutions with different tradeoffs between privacy, performance, and complexity. A comprehensive revocation framework addressing all these scenarios—while preserving privacy and maintaining blockchain compatibility— is absent from the literature.

D. Gap 4: Absence of Modern Credential Standards Compliance

W3C VCDM, Open Badges 3.0, Comprehensive Learner Records (CLR 2.0), and OID4VCI/OID4VP protocols constitute the current standards ecosystem for digital credentials. Rustemi et al. [2] confirm that no reviewed system from 2018–2022 implements any of these standards. This creates severe interoperability limitations: credentials from one system cannot be verified by another, students cannot port their credentials across institutions, and employers cannot use standard tools to verify credentials.

TABLE II
COMPREHENSIVE COMPARISON OF BLOCKCHAIN-BASED ACADEMIC CREDENTIAL SYSTEMS

System	Blockchain	SSI/DID	Sel. Disc.	ZKP/BBS+	W3C Std.	Revoc.	IPFS	OID4VC
CredenceLedger [1]	Multichain	No	No	No	None	No	No	No
BlockCert (MIT)	Bitcoin	No	No	No	None	Partial	No	No
Open Certificate	Ethereum	No	No	No	None	No	Yes	No
Gradbase	Bitcoin	No	No	No	None	No	No	No
Sony Global Edu.	Hyperledger	No	No	No	None	No	No	No
CVSS	Ethereum	No	No	No	None	No	No	No
BCDIPLOMA	Ethereum	No	No	No	None	No	No	No
CERBERUS	Ethereum	No	No	No	None	No	No	No
BLOCKCERTS	Hyperledger	No	Partial	No	None	Partial	No	No
BCERT	Ethereum	No	No	No	None	No	Yes	No
Polygon Evidence	Polygon L2	No	No	No	None	No	Yes	No
EBSI (EU) [3]	Hyperledger	Yes	Partial	No	VCDM	Yes	No	Partial
Proposed Dir.	**Hyp. Indy**	**Yes**	**Yes**	**Yes (BBS+)**	**VCDM+OB3.0**	**Yes**	**Yes**	**Yes**

E. Gap 5: GDPR and Privacy Regulation Compliance

Privacy regulation compliance requires proactive design rather than retrofitting. The GDPR's right to erasure, data minimization requirements, and purpose limitation principles all create tensions with blockchain's immutability. Mazzocca et al. [3] document how SSI's selective disclosure mechanisms— particularly BBS+ and SD-JWT—support GDPR compliance through data minimization. Additionally, off-chain storage of credential content with on-chain CID references ensures that personal data can be deleted from IPFS while maintaining the blockchain's integrity record. India's Digital Personal Data Protection (DPDP) Act 2023 introduces analogous requirements in the Indian context.

F. Gap 6: Interoperability and Cross-Institutional Verification

Academic credential systems are currently institution-specific silos. Mazzocca et al. [3] document how DID and VC standardization, combined with cross-chain interoperability protocols like DIDComm, can enable ecosystem-level interoperability. The W3C Universal Resolver—which can resolve DIDs from multiple DID methods—is a key enabling infrastructure.

For India's academic ecosystem, where credentials may need to move between state boards, central universities, professional councils, and international employers, cross-institutional interoperability is not optional but essential.

VII. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This survey has systematically reviewed the state of the art in blockchain-based academic credential verification through three complementary IEEE sources, spanning from early permissioned blockchain systems (2018), through comprehensive systematic literature reviews (2023), to the latest standards in decentralized identity (2025).

The findings are unambiguous: the field has made significant progress in demonstrating technical feasibility but has failed to keep pace with advances in digital identity standards and privacy-preserving cryptography.

The comparative analysis of 12 existing systems against eight critical dimensions—SSI/DID, selective disclosure, ZKP/BBS+, W3C standards, revocation, IPFS, and OID4VC—reveals that no existing system addresses all dimensions simultaneously. The gap between what is technically achievable (as documented by Mazzocca et al. [3]) and what has been implemented in academic credential systems (as documented by Rustemi et al. [2]) is substantial and represents a significant research opportunity.

Future systems should be designed from first principles around SSI architecture using Hyperledger Indy (or equivalent DID-supporting blockchains), implementing BBS+ signatures for full selective disclosure, and achieving compliance with W3C Verifiable Credentials Data Model (VCDM) and Open Badges 3.0. They should also support OID4VCI/OID4VP for standardized credential exchange, implement robust revocation via W3C Revocation List or cryptographic accumulators, and use IPFS for privacy-respecting off-chain storage. Such a system would represent a definitive advance over the state of the art, enabling truly portable, privacy-preserving, and interoperable academic credentials—meeting both technical requirements and regulatory obligations in the global digital credential ecosystem.

REFERENCES

[1] R. Arenas and P. Fernandez, "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials," in *Proc. 2018 IEEE Int. Conf. on Engineering, Technology and Innovation (ICE/ITMC)*, Stuttgart, Germany, 2018. DOI: 10.1109/ICE.2018.8436324.

[2] 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.

[3] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A Survey on Decentralized Identifiers and Verifiable Credentials," *IEEE Communications Surveys & Tutorials*, 2025. DOI: 10.1109/COMST.2025.3543197.

[4] World Wide Web Consortium, "Verifiable Credentials Data Model 1.1," W3C Recommendation, Mar. 2022. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[5] World Wide Web Consortium, "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, Jul. 2022. [Online]. Available: https://www.w3.org/TR/did-core/

[6] IMS Global Learning Consortium, "Open Badges 3.0 Specification," 2022. [Online]. Available: https://openbadges.org/

[7] OpenID Foundation, "OpenID for Verifiable Credential Issuance (OID4VCI)," Draft Specification, 2023.

[8] OpenID Foundation, "OpenID for Verifiable Presentations (OID4VP)," Draft Specification, 2023.

[9] Hyperledger Foundation, "Hyperledger Aries Cloud Agent Python (ACA-Py) Documentation," 2024. [Online]. Available: https://aca-py.org

[10] D. Fett, K. Yasuda, and B. Campbell, "Selective Disclosure for JWTs (SD-JWT)," IETF Draft, 2023.
[11] European Commission, "European Blockchain Services Infrastructure (EBSI)," 2024. [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI
[12] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[13] Gideon Greenspan, "MultiChain Private Blockchain — White Paper," 2018. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf
[14] David Moher, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," *Annals of Internal Medicine*, vol. 151, no. 4, p. 264, 2009. DOI: 10.7326/0003-4819-151-4-200908180-00135.
[15] Ministry of Education India, "National Education Policy 2020," Government of India, 2020. Available: https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf
[16] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," White Paper, 2014.
[17] J. Benet, "IPFS — Content Addressed, Versioned, P2P File System," *arXiv preprint arXiv:1407.3561*, 2014.
[18] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proc. 13th EuroSys Conf. (EuroSys '18)*, Porto, Portugal, 2018, Art. no. 30.
[19] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.
[20] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review," *Applied Sciences*, vol. 9, no. 12, Art. no. 2400, 2019.