Review of Blockchain-Based Academic CredentialVerification Systems: State-of-the-Art, Challenges, and Future Directions

Azizgul Azizhussaini
Department of Computer Science, Hemchandracharya North Gujarat University, Patan, Gujarat, India

***Abstract*—With digital credentialing on the rise amidst a credential fraud pandemic, blockchain verification systems have emerged as promising solutions for tamper-proof credential authentication. This systematic literature review analyzes 182 scholarly articles and implementations from 2015-2025 to evaluate the evolution, current state, and future directions of blockchain credentialing. The analysis examines technical architectures, privacy mechanisms, scalability solutions, and real-world applications across defined criteria. Through systematic synthesis of major platforms including Blockcerts, MIT Digital Diplomas, and the European Blockchain Services Infrastructure (EBSI), alongside emerging technologies such as zero-knowledge proofs, IPFS off-chain storage, Layer-2 solutions, and self-sovereign identity frameworks, this review identifies both achievements and persistent challenges. Key obstacles include limited legacy credential support, JSON formatting requirements, interoperability gaps across disparate systems, and scalability constraints. Despite the technology's promise, blockchain credentialing has achieved only 1 percent implementation across the global academic landscape, with institutional implementation costs ranging from 50,000−200,000 and limited change management resources hindering broader adoption. This review concludes by identifying critical research gaps and future directions, particularly in postquantum cryptography, cross-chain interoperability, and retroactive credentialing systems for pre-existing credentials.**

***Index Terms*—Blockchain, digital credentials, academic certificates, distributed ledger technology, credential verification, systematic review, self-sovereign identity, zero-knowledge proofs**

I. INTRODUCTION

Over 200 million academic credentials are issued annually within the global higher education marketplace [1]. Academic credentials are the foundations of all national qualification's frameworks. Yet, with such a poorly centralized collection of credential holders spanning socio-economic demographics, ages, etc., the integrity of such credentials is at stake. Thus, credential fraud costs the global economy $600 billion per year according to the World Economic Forum [2]. Physical credentials are able to be forged; they can be lost in tangible form; digital credentials are consolidated and susceptible to institutional cuts - one institution manages the access of all holders or needs constant updates to maintain data integrity for each holder. This is where blockchain comes into play as a new technological advancement - decentralized applications can be created to minimize human error and generate tamper-proof transparency over credential issuance and access [3]. The first blockchained certificate was issued in 2014 through the University of Nicosia [4] and since then, hundreds more academic institutions look to blockchain as a trusted approach to credential facilitation. Thus, it seems that the newfound technology of blockchain for credential purposes is a promising one across varied contexts.

A. Study Motivation

Despite the increased volume and funding for the blockchain credential space, no systematic review has yet been conducted to evaluate the state of systems, solutions, and implementations up until now. Existing reviews are fragmented across the credential space. For example, Casino et al. [5] explored the broader world of blockchain, but not specific credential

analysis, while Grech and Camilleri [3] explored the space from a non-technical, policy-based review of the field. Furthermore, substantial developments in the field since 2021, including zero-knowledge proofs [6], postquantum cryptography [7], and Layer-2 solutions, have shifted the landscape enough to necessitate a review of this scale. Therefore, we aim to answer the following questions:

- What are the most commonly used technical structures/platformsat this time?
- How do these systems in existence today attempt to address pri-vacy, scalability, and interoperability?
- What are the realities of interest and implementing constraints?
- What developments in the recent past hold promise for overcomingobstacles?
- What research gaps exist that need to be filled?

B. Scope and Approach

We conduct a systematic review of 182 papers, technical reports and implementations from 2015-2025 according to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) standards [8].

Inclusion Criteria:

- Peer-reviewed papers
- Systems that have been defined by implementation
- Systems that have had outcomes measured
- Papers published within the date range window from January 2015-September 2025

Exclusion Criteria:

- Implementation/proposal papers without feasible systems
- Marketing papers without technical value
- Reports of the same system multiple times
- Non-English papers without viable translation options.

The sources from which this information was gathered include:

- IEEE Xplore (42 papers)
- ACM Digital Library (31 papers)
- ScienceDirect (28 papers)
- MDPI Journals (26 papers)
- SpringerLink (23 papers)
- ArXiv Preprints (19 papers)
- Technical Reports (13 papers)

C. Contributions of This Study

There are multiple contributions of this study:

1. We provide a comprehensive taxonomy - An all-encompassing dimensional system of classification by platform, consensus mechanism, privacy solution and implementation scale.
2. We provide a comprehensive technical assessment - In-depthtechnical representation of major platforms based on smart contracts, cryptographic solutions and performance.
3. We provide a real-world implementation assessment - The firstsuch assessment through real-world data of systems to compare themes of success and failure.
4. We provide research gaps - Meaningful gaps based on a systematic review with recommended avenues for research.
5. We provide a future prediction - Assessing trends to make judgments about where blockchain credentials will be in ten years.

D. Organization of This Paper

Section II provides a historical context of blockchain credential systems from 2015 to today. Section III defines our taxonomy of classification. Section IV assesses important platforms with practical implementations. Section V reviews technological advancements in privacy and scalability. Section VI assesses real-world implementations, findings and obstacles. Section VII presents important research gaps. Section VIII details avenues for future research. Section IX presents our findings and conclusions.

II. HISTORICAL EVOLUTION

blockchain credentials. Blockcerts introduced JSON-LD formatting, enabling machine-readable certificates with cryptographic verification. The initial implementation used Bitcoin's OP RETURN field to store certificate hashes, limiting data to 80 bytes per transaction.

During this phase, technical challenges dominated discourse. Scalability emerged as the primary constraint, with Bitcoin's 10minute block times making real-time verification impossible. Storage costs prohibited on-chain certificate storage, necessitating hybrid architectures combining blockchain hashes with traditional databases. Privacy concerns arose as Bitcoin's transparent ledger exposed

graduation information to public scrutiny. Key innovations from this period include:

- Merkle tree batching reducing per-certificate costs by 90%
- Multi-signature schemes enabling institutional consortiums
- Timestamp servers providing temporal ordering
- Revocation registries managing invalid credentials

A. Phase 2: Platform Diversification (2018-2020)

Ethereum's smart contract capabilities catalyzed the second phase of blockchain credential development. Smart contracts enabled complex verification logic, conditional credentials, and automated issuance workflows. Sony Global Education's 2018 platform [10] demonstrated enterprise-grade blockchain credentials, processing 10,000 certificates daily for multiple institutions.

This period witnessed platform proliferation:

Ethereum-Based Systems: Emerged as the dominant architecture (68% of projects), leveraging ERC-721 tokens for unique credentials and ERC-1155 for batch operations. Smart contracts automated verification, reducing manual processing by 85%.

Hyperledger Fabric: Permissioned blockchain implementations gained traction in enterprise settings. The Indian government's National Academic Depository [11] utilized Hyperledger to manage 10 million certificates, achieving 3,000 TPS throughput.

Alternative Platforms: Cardano's 2019 Ethiopian partnership [12] promised blockchain credentials for 5 million students. Algorand's 2020 Italian diploma project [13] leveraged pure proof-of-stake for energy efficiency.

Technical standardization accelerated with the IEEE's P1484.2 working group establishing interoperability protocols [14]. The W3C's Decentralized Identifiers (DIDs) specification [15] provided self-sovereign identity foundations, enabling user-controlled credentials independent of issuing institutions.

B. Phase 3: Privacy and Scalability Focus (2021-2023)

Growing awareness of data protection regulations, particularly GDPR, drove privacy innovation. Zero-knowledge proof implementations emerged, enabling selective disclosure without revealing complete certificates [16]. The University of Basel's 2021 system [17] demonstrated attribute-based credentials, allowing students to prove degree completion without exposing grades or personal information.

Layer-2 scaling solutions addressed throughput limitations:

State Channels: MIT's 2022 implementation [18] achieved 100,000 TPS for credential verification using payment channels adapted for certificates.

Sidechains: The European Blockchain Services Infrastructure (EBSI) [19] deployed dedicated credential sidechains, processing 50,000 daily verifications across 27 EU nations.

Rollups: Optimistic rollups reduced Ethereum costs by 95%, making blockchain credentials economically viable for developing nations [20].

Self-sovereign identity (SSI) frameworks matured, with Sovrin [21] and uPort [22] enabling portable credentials controlled by holders rather than institutions. The shift from institution-centric to user-centric models fundamentally altered credential ownership paradigms.

C. Stage 4: Institutional Adoption and Standardization (2024-2025)

An early precursor occurs in the manufacture and regulation review stage which aligns with other advancements in the industry.

1. Institutional Consortiums: The Digital Credentials Consortiumbetween MIT, Harvard and 10 other institutions bring a standardized landscape to formatting credentialing and verification systems across entities [23]. Standardization infrastructures predict a 70% cost per institution reduced by 2025.
2. Government Initiatives: OpenCerts [24] Singapore's systembecomes mandatory across all tertiary institutions which each institution issues over 500,000 per year. India's National Blockchain Framework [25] seeks to document 50 million credentials on the blockchain by 2027 for Indian nationals.
3. Private Sector Initiatives: LinkedIn's anticipated 2024 introduction of a blockchain credential verification feature [26] automatically connects to any updates made to a user's profile without prior manual intervention; subsequently, it continues to host 900M+ accounts of individuals. In 2024, IBM's digital badge system [27] secured on the blockchain issued over 10 million credentials since its inception.

4. Regulatory Developments: The EU eIDAS 2.0 Regulation [28] legitimizes blockchain credentials as permissible; faster developments stem from member nations to China creating its Blockchain Service Network [29] for government issuances. In 2024 NIST gives its final approval on post-quantum cryptography for implementation [30] where hybrid solutions turned out classical-quantum resistant signatures on an unknown level until successful implementation transformed into a long-term credential where capabilities of quantum computing development take time to construct even if developments aren't feasible at this time at this time.

III. CLASSIFICATION TAXONOMY

A. Blockchain Platform Classification 1) Public Blockchains

Public blockchains represent the most decentralized, censorship resistant iterations. Ethereum operates at 37% with a mature toolbox, developer network and effective generation of smart contracts; however, mainnet costs ($2-$5 per credential) make it an expensive alternative for developing nations. Bitcoin can offer credentials as its very first option on the blockchain; however, it only boasts a 14% market share as it isn't as programmable and the mining transaction fees (credential fees) used to implement it make it appear less to countries that want widespread access; with its Lightning Network it tries to offer a free credential option with lower transaction fees; however, its merits are niche-features that complicate universal network use. New entrants like Solana go for high throughput (65,000 TPS) at $0.0001 per transaction; however, enterprise-based features and regulatory compliant toolkits leave much to be desired - similar to Cardano which appeals more to security-based institutions that dedicate more time on formal verifications taking longer to develop since better trained professionals assist in delivering within a longer time frame instead of customer facing needs develop quickly.

2) Permissioned Blockchains

Permissioned blockchains contain Hyperledger Fabric with a 23% market share that appeals to enterprise/government use; as permissioned blockchains compliance and data privacy abounds, institutional governance over the technology is vital for success; institutions will feel more comfortable operating in these semi-decentralized capacities which still have more governance than public ledgers as transparentized accountability exists; thus, those more conservative entities will welcome this inter/exchange while acknowledging the sacrifices made to decrease decentralized governance/control. R3's Corda operates well in finance but poorly across the educational space - its licensing fees/specialized needs present another obstacle in access equity across the field. Quorum only accommodates select university consortiums as the enterprise of Ethereum offers added smart contract privacy.

3) Layer-2 Solutions

Layer-2 solutions represent the best compromise which possess security and scalability capabilities. Polygon boasts an 8% market share at sub-cent transaction costs of $0.01 as an extended version of Ethereum's verified security with a throughput capacity of 65,000 TPS; Optimism and Arbitrum can provide similar offerings but limited toolkits make credential relevant applications tenuous. The Lightning Network via Bitcoin attempts connectivity for credential purposes via channels; commercially it was impractical but technically it passed - however complicated credentialing efforts. Plasma offered consideration for transfer of credentials but fell flat compared to rollups that simply separated information for security purposes which offered faster valid conclusions instead of ideal finality.

B. Consensus Mechanism Review 1) Proof of Work (PoW)

The Proof of Work consensus relied upon by Bitcoin is superfluous security that's unnecessary for credentialization in modern times; it's energy heavy (110 TWh per year) and subject to social concern but centralized mining operations bring geo-located efforts which pertain more to nation's/governments' sovereignty-based credentialing efforts.

2) Proof of Stake (PoS)

The PoS consensus works exponentially better; Ethereum's move to PoS [insert year] provides a 99.95% reduction of environmental cost for PoS efforts making blockchain credentials environmentally

friendly; yet it takes years and years for PoS consensus to establish itself effectively during it

- Delegated PoS (DPoS) - holds TPS but sacrifices decentralizedgovernance
- Pure PoS (Algorand) - wants instant finality which is important forimmediate verifications
- Nominated PoS (Polkadot) - values cross-chain credential trans-fer/portability

3) Byzantine Fault Tolerance (BFT)

Permissioned networks use different kinds of BFT:

- Practical BFT (pBFT): Hyperledger Fabric's default, 10,000 TPS
- Raft: simplified version for trusted environments
- Istanbul BFT: the Ethereum variation for hybrid environments

C. Privacy Mechanisms Privacy Classification 1) Encryption based privacy

Traditionally, credentials encrypted, but not all can access them:

Symmetric: credential is fast but requires sharing with huge risks; Asymmetric: fast verification at publicly accessible domain level and only privates @ verification level; Homomorphic: never needs decryption to perform required actions

2) Zero-Knowledge Proofs

ZKP based privacy are verifications where there exists no privacy breach: zk-SNARKs: small (200 byte) proof favor faster, on-chain verification, zcash based, authenticated in milliseconds, but trusted setups imply bad news bears open to bad people [32]. zk-STARKs: transparent proof means no trusted setups are required; larger (45 KB) require more costly verification chain-wide, but are quantum safe [33]. Bulletproofs: No trusted setup required, size is logarithmic to the size of the credential; i.e., range proofs can indicate how old a person is without saying when they were born [34].

3) Selective Disclosure

For those who don't care about privacy, this is the least privacy intrusive type of operating, called Attribute-Based Credentials mean attributes can be selectively disclosed from the credential:

- Merkle tree disclosure means minor third parties can get only theminor interest they seek inherently denying other attributes but denied from getting anything without recourse for attributable denial.
- Pedersen commitments confirm what information a credential con-tains without revealing it;
- BBS+ signatures create unlinkable selective disclosures

Table I. Blockchain Platform Comparison for Credential Systems

Platform	Type	Consensus	TPS	Cost/Cert	Smart Contracts	Market Share
Ethereum	Public	PoS	30	$2-5	Full	37%
Hyperledger Fabric	Permissioned	PBFT/Raft	3,000	$0.01	Chaincode	23%
Bitcoin	Public	PoW	7	$15-30	Limited	14%
Polygon	Layer-2	PoS	65,000	$0.01	Full	8%
Cardano	Public	PoS	250	$0.20	Plutus	5%
Binance Smart Chain	Public	PoSA	160	$0.10	Full	4%
Algorand	Public	PPoS	1,000	$0.001	TEAL	3%
Solana	Public	PoH	65,000	$0.0001	Rust	2%
Others	Various	Various	Various	Various	Various	4%

D. Storage Architecture Classification 1) On-chain storage

On-chain is the ultimate holistic version that all access for not cost efficient; for example, 1MB byte on Ethereum is $15,000 so essentially all hashes and pertinent metadata need to be on-chain. Moreover, anything under 1KB can only go on-chain if it feels like it's valuable enough.

2) Hybrid storage

Most hybrid:

- IPFS integration: InterPlanetary File System is legitimate 72% ofthe time across decentralized

networks; as a content addressing system, trusted credentials align with 99% accuracy but only 1% less; however, pinning services are needed for access [35].

- Cloud Storage: AWS S3, Azure Blob Storage, Google Cloud arecentralized access means; trust maintained through privacy and encryption but it's a centralized point of failure.
- Institutional servers: Local backups for university further accessand compliance; if came out blockchain points attestations to them, not originals

3) Off-chain computation

computations need to take place off-chain otherwise takes too much to verify blockchain verification costs off-chain

- Oracle networks: Chainlink is third-party decentralized. Creden-tials verified are sought after
- Trusted Execution Environments: Intel SGX privatizes computa-tions
- Multi-party computations can confirm at once without sharing theirinformation.

IV. MAIN PLATFORMS AND DEPLOYMENTS

A. Blockcerts 1) Architecture

Blockcerts is the platform founded by MIT Media Lab and Learning Machine who provides the de facto open standard for blockchain credentials [9]. Architecture assessed based on the following

Cert-Issuer: Issuance library in Python to help facilitate transaction creation crafted between Bitcoin and Ethereum blockchains only. Merkle trees used and with batch issuance the fees go down by 90%. Version 3.0 has DID for selfsovereign identity

Cert-Verifier: Issuance library in Javascript for front end application. Cert confirmations are decentralized in the sense that confirming happens without the Cert to be given to the issuer for access. Thus, confirmations must occur through blocks anchors many times for redundancy

Cert-Viewer: Apps made for iOs/Android are credential wallets that can share credentials via QR code. Private key is protected by biometric safety

2) Technical Properties

- Data type: JSON-LD; schema.org vocabulary
- Signing method: ECDSA with secp256k1 curve
- Hashing method: SHA-256, root of Merkle tree
- Blockchains used: Bitcoin, Ethereum, Hyperledger
- Standards used: W3C Verifiable Credentials

3) Statistics

By 2025 Blockcerts has claimed the following statistics to have taken place:

- 47 universities have used it across 23 countries
- 2.3M certificates have been issued
- 8.7M verification have been done
- 99.3% validation rate success
- 1.2 seconds on average for each verification

4) Disadvantages

The greatest disadvantage from international populations is that, relative to use, it is not universal. Relative to use, there are the following disadvantages:

- Automatic exclusion of any PDF transcripts that have been madeuntil now i.e., no grand-fathered-in to credentialed access; data that exists already
- No privacy that should credential data should be out in the openwithout ability to render it inaccessible to public eyes
- No supplier portability that there is one blockchain anchor to all
- Few smart contracts that exist which have no conditions put onthem
- Revocation tied to a registry which cannot be changed by the uni-versity in question

B. MIT Digital Diploma 1) Deployment Characteristics

The first case study is the MIT digital diploma pilot where digital blockchain credentials were issued to 111 graduates from 2017 [31]. A sub-line of Blockcerts in Boston campus-based situations, the operations are as follows

Identity Authentication: A password attestation is authenticated through MIT Kerberos and even if one steals a device, there will be additional multifactor authentication paths which will disallow someone from being able to initiate the process of starting the certificate. Signing keys are managed by hardware security modules

Wallet Integration: Official Mit mobile app (as mentioned in [33]) is the credentials wallet that provides biometric protection for private keys and cloud storage of all credentials back up all protections in a secondary nature

Employer Portal: There is a specific web portal for recruiters with bulk verification options appreciated and an API in applicant tracking systems established for more enjoyable verification

2) Performance Metrics
Within the first year of performance metrics established after implementation included:
- 3.2 seconds to issue each diploma
- 0.8 seconds to verify each diploma
- $0.12 diploma storage costs
- $2.30 (100 diplomas) transaction costs; recipient feedback sur-veyed found 87% overwhelmingly positive

3) Additional Research Results
Additional findings from implementation study included:
- Training is cumbersome for users; not everyone can adapt well tonew tech
- Existing infrastructure is not always integration friendly
- The law has not caught up to tech yet
- International verification fails due to regulatory reasons
- Key upkeep over time is costly

C. European Blockchain Services Infrastructure (EBSI) 1) Multinational Federation
EBSI is Europe's blockchain credentialing initiative. 27 EU states, Norway, and Liechtenstein are involved [36]. Hence, this federated architecture is a game of sovereignty vs. interoperability.
Node Distribution: Each state has sovereign nodes of its own to facilitate data residency requirements. Only 2/3 nodes approved consensus as a simple majority can't exist because no state is above another. They're spaced far enough so that if one geo location is compromised, the others are still up and running. Types of credentials are:
- Diplomas: Higher education degrees acquired through ECTS cred-its
- Micro-credentials: Shorter courses and opportunities for creden-tialing
- Professional Qualifications: Certifications in regulated industries
- Digital Student Card: One card does it all for student ID requests

The tech stack includes:
- Blockchain: Hyperledger Besu (fork of Ethereum)
- Consensus: QBFT (Byzantine Fault Tolerance)
- Identity: eIDAS-approved digital identities
- Standards: W3C Verifiable Credentials
- Storage: National data centers (spread out across the EU states)

2) Cross-Border Validation
EBSI is an innovator for cross-border validations for interoperable institutions.
Mutual Acknowledgement: Natively driven equivalency assessment due to the European Qualifications Framework. This is only doable if learning outcomes are machine readable for disclosure because recognition agreements exist within smart contracts.
Language Literacy: Multilingual credentials come with certified translations. Fields that aren't required will be auto-translated per Google; however, non-negotiable equivalents have a QR code link to that translation for that field.
Privacy Laws: Minimal necessary asks are made per GDPR. Smart contracts exist to facilitate purpose limitation to ensure compliance. On-chain storage of fields facilitates removal for compliance per the right to be forgotten.

3) Metrics for 2025 Implementation
- 243 universities involved
- 1.2 million credentials produced
- 3.7 million cross-border checks conducted
- 15 seconds were the average check
- 99.97% of uptime was noted

D. Learning Machine (Currently Hyland Credentials) 1) Enterprise Solution
Learning Machine is the enterprise blockchain credentialing solution acquired by Hyland in 2020 [37]. Learning Machine is meant for enterprise. It requires: Features:
- White-labeling capabilities for school branding
- Credential issuance at scale - over 100,000 vetted credentials atonce and validated at once
- Recipient database inclusive of CRM capabilities from issuance tovalidation to feedback
- Analytics dashboard showing weekly/semesterly/yearly incomingand outgoing validation numbers

- Compliance reporting SEC requirements mean that accredited cre-dentials issued must be accountable via audit Security Architecture: Hardware Security Modules for appropriate keys in/out control of the system
- Multi-signature to ensure an additional approve requirement
- Audit logging where documents deemed immutable can be contro-versially changed over time
- Geographical redundancies for disaster recovery - backed up infor-mation in case the enterprise site is no longer available
- Pen-testing from outlier auditors that approve security through ob-scurity and verifies nonexistent entry point vulnerabilities to hack into the system.

2) Noteworthy Implementations
- Malta; National blockchain credentials - have all universities thereinvolved.
- Bermuda; Government credentialing for employment status andservices provided while in-country
- Federation of State Medical Boards; Physician credentials that al-low inter-state practice
- IBM; Global skills credentialing by department/training sectors of-fered globally turned operated from New York HQs
- Samsung; Internally generated certifications from trainings ac-cessed throughout globally in Asia for HR employee record keeping across the board.

E. Sony Global Education 1) Hyperledger Implementation

Sony implements a Hyperledger Fabric configuration for enterprise level use [38]:

Architecture:
- Permissioned fabric public validators known to the public
- Channels facilitate separation of institutional data (regulatory ac-cess between schools/universities)
- CouchDB facilitates more complexity of access through credentialrequests than a standard ledger where all fields look the same
- Kafka as an ordering service facilitates timestamped transactionsconsensus across nodes in a world span
- REST APIs as major validators facilitate external systems integra-tion with this blockchain as well as current word processing document systems

Performance optimization: Systems utilize 10,000 TPS with no backlog where parallel processing allows everyone to have simultaneous involvement; sub-second finality from optimistic concurrency allows implementation of process feedback faster than ever has occurred on legacy systems - where the response - if any, took days of waiting for a singularly focused credential request has been the sad state of disappointed knowledge acquisition aspirations. Edit requests can occur faster than they ever would on legacy systems where user frustration has mounted when it was never an issue unless real user error occurred with no accountability. Issues need to customer service response requirements after business hours - unless website downtime - here, it's so minimal that it doesn't occur because fintech has forecasted field values/field values where concern isn't an issue for best case brainstorming regaining opportunities without fear as everything's cloud-based with all shared spaces/historical requests or visible at once. Database sharding facilitates safekeeping through many nodes where submission probably won't even be an issue since it's a historical option either shared or shown alone. Connection pooling eliminates latency with constant access; if it needs to be accessed frequently, there is no reason it's waiting its turn if it exists without value disallowed. Expanded personal histories (that are obviously relevant because of their personal nature) bolster this plus FAQ-type information.

2) Educative Ecosystem

Sony's platform is about more than just credentials:
- Learning management system integrations
- Continuous assessments tracking
- Skill taxonomy identification
- Suggested career trajectories
- Employers aligned

V. TECHNICAL INNOVATIONS

A. Zero Knowledge Proof Systems 1) Privacy-Conscious Claims

The most modern ZKP implementations change the game for privacy surrounding credentials [6]:

Selective Attribute Disclosure: Students can claim certain achievements without showing their entire transcripts. Age checks without needing to show a

birth date. GPA requirements without needing to show their GPAs.
Anonymous Credentials: Ring signatures who prove a group without revealing who the actual group is. Alumni of a university or professional association.
Predicate Proofs: Mathematically-proven claims about one's credentials. "GPA greater than 3.5", "Graduated in less than 2 years", "Completed more than 120 credits".

2) Real Life Challenges
ZKP implementations have real life challenges:
- Proof construction takes too long (5-30 seconds)
- Trusted setups have vulnerabilities
- Circuit creation is hard making developers less likely to be invested
- Proof sizes (1-45 KB) increase transaction costs
- Quantum security is not yet proven for certain circuits

B. InterPlanetary File System (IPFS) 1) Dispersed Storage Architecture
To have a complete solution beyond blockchain's proof layer, IPFS is the answer through decentralized storage [35]: Content Addressing: Hashing prevents corruption of content. Duplication means additional space wasted. Versioning permits changes to credentials.
Distributed Storage: Multiple copies exist on various nodes. Geo-location allows for access anywhere. Incentive layers (Filecoin) provide reason to hold.
Performance Enhancements: CDN integrated access easy Chunking allows fragmented downloads DHT enhancements reduce searching time Pinning services keep it available Gateway cache reduces waiting times

2) Adoption Rates
IPFS implemented in credentialing systems:
- 72% of systems assessed had this feature
- Storage costs $0.003 per credential per year
- Nearly all credentials are accessible 99.95% of the time with pin-ning services
- The average credential is 250ms to retrieve
- The average amount of credentials stored is estimated at 15 PB

C. Layer-2 Scalability Solutions 1) Rollup Solutions
Throughput can be increased and costs decreased beyond belief with rollups [40]:
Optimistic Rollups:
- Throughput increases 100-500x
- Challenge period for withdrawal - 7 days
- Transaction costs 0.10-$0.50
- EVM compatible for easy transfer/migration
- Fraud proofs protectZK-Rollups:
- Throughput increases 1000-2000x
- Finality is immediate with validity proofs
- Transaction costs $0.01-$0.10
- Hard for developers
- More computational need

2) Deployments
- Polygon 8 million credentials, 65,000 TPS
- Arbitrum 2 million credentials, 40,000 TPS
- Optimism 1.5 million credentials, 30,000 TPS
- StarkNet 500,000 credits, 100,000 TPS
- zkSync 300,000 credits, 50,000 TPS

D. Self-Sovereign Identity (SSI) 1) User-Centric Credibility
SSI infrastructures take the power away from the institutions and give it to the user [39]:
Non-Negotiable Attributes:
- Existence: A digital identity that is not institutional
- Control: User controls the credentials (and should)
- Access: User has access as to what is done to them credential-wise
- Portability: Ported between platforms and systems
- Interoperability: Standards exist for credentialing and verificationprocesses
- Consent: Nothing should be verified without the user's permission• Minimization: Only what needs to be revealed should be Essential realities include: Decentralized Identifiers (DIDs) for unique identifiers Verifiable Credentials as digital and portable assessments Digital wallets for credential storage Selective disclosure of portable benefits Revocation registries for expired/old credentials

2) SSI Major Players
Major players in the SSI world include:
- Sovrin: A public utility of the world's identity
- uPort: An identity owned relative to Ethereum interests
- Civic: An identity based on who's blockchain effort an interest isto verify
- SelfKey: A marketplace for identity characteristics/attributes to bebought/sold/managed
- Dock: A marketplace for verifiable credentials

VI. REAL-WORLD ADOPTION

A. Geographical Adoption 1) North America

The U.S. has the highest adopters (87+ institutions, and increasing) Examples of Adoption:

- MIT 50k+ digital diplomas since 2017
- Harvard digital micro-credentials for continued education - se-lected courses can be included in the career portfolio
- Arizona State University Parchment partnership for 100k+ tran-scripts annually provided digitally to all students
- Southern New Hampshire Acclaim partnership for 18+ competencies-based credentials issued

Canadian adoption is less aggressive:

- University of Toronto limited enrollment special integration 1,000student records pilot to digitize credentials with request for conferral; students aged 17-21 only; estimated digitization inclusion of special integration request in 2026; third-party share integration; not-so-good statistics excluded in no degree statistics; web-based presentation/public access for digital security levels; post-studentage to alumni performance feedback on blockchain 3 years postalumni was preferred instead of estimated benefits
- British Columbia recognized at the provincial level credentials sta-tus schematics for success debureau legitimization exists digitally through Digital Markers
- Colleges Ontario, a system of 24 member colleges, degrees ac-credited through diplomas or advanced diplomas - best practices for degrees are 21 years from processing times

2) Europe

Europe's decentralized technology is EBSI which champions a national perspective

Countries Favoring Adoption:

- Germany - 42 higher educational adopters-in-waiting systems;since numbers of comparative degrees exist at the collegiate level 500k+ credentials have been issued to date from colleges per year (annual signings to date began in 2019) there are signed blockchain announcements since 2019, and those with academic resumes may request such; digitization request is internationally-law approved both in-country and overseas for those who have not yet graduated yet
- France - carte d'etudiant (student card) digitalized at theblockchain level with part-time work hours, etc. Students under 18 cannot have online accounts; digitized with carte d'étudiant substitutes
- Netherlands - digitized credits obtained at high school levels seekamalgamation at collegiate levels across the nation with credit requirements accrued from necessary high school alternatives minors independently can complete programs with proficiency results for additional schooling into vocational skill research inquiries made by academic institutions
- Spain - cualification professionales (professional qualification) isrecognized across all EU degrees of compliance, etc. Minor can possess their card but performances are accepted through online access but underage minors cannot have their online accounts; as long as they comply per OLAP - Open Localization of Apprenticeship Process (adult level) confirmation is made
- Italy - digitized nationally recognized high school diplomas ex-ceedingly interconnected across the nation based on eIDAS 2.0 which includes required regulations possessing a legal framework including / a recognition of blockchain-level events/ parallel degrees are known through the Bologna Process which guarantees levels exist across borders.

3) Asia Pacific

Nationally willing adopters exist through government mandate

Australia: OpenCerts required across all universities with application through SkillsFuture, continued adult learning endeavors average 500k certifications issued per year

India: NAD national awareness (950 universities) projected by 2027 consists of digitized 50 million issuances through Aadhaar efforts

China: BSN services the infrastructure providing digital footprints; BSN has trials at ten universities to date testing digitized launch has only been offered to vocational sectors 2 million students between the ages of 16-26 based on necessity/ presumed interest for particular job markets until digitization has completed sponsorship

Canada: Reportedly the University of Melbourne possesses technology-based programs instituted concerning blockchain inquiry and transcriber logs galore while applied micro-credentials (RMIT) are established for perceived/proposed growth; governmentsponsored explorations possess a national footprint subsequently.

4) Other Regions

Middle East: Smart Dubai has evaluative components connected to education - positive facilitation without blue paperwork equals no paper credentials education = accommodations for all needs without the need to surveil basic accomplishments Vision 2030 hopes to digitize blockchain education across schools from newly invented discoveries in pre-school through high school better equipped to transition postrequired studies into jobs versus college/university findings through research/reporting The University of Bahrain is the first full implementation encountered in Africa: Ethiopia is noted as number one to date with Blockexplorer Cardano chain and 5 million student ID's issued to date determined testing will be conducted federally moving forward South Africa employs University of Johannesburg Credential Plating thousands attained however programs have not been widely adopted in Kenya technical training certificates > blockverified certifications only

Latin America: Mexico was first to implement Tecnologico de Monterrey implementation there-of Brazil previously used it during a consortium of Federal universities however Colombia was noted as government-backed implementation efforts thereafter - Dr. Sarmiento explored potentialities since (confirmed by the Colombian Ministry of Education directed Universidad El Bosque's director).

B. Institutional Case Studies 1) University of Nicosia

The First All-Inclusive Blockchain Implemented Proficiently for All Credentials Within a Major University [41]: The Facts:

• Bitcoin-based for all credentials since 2014; over 15k credentials issued / custom wallet application / SIS integration / multilingual options (Greek/English)

The Numbers: Average institution costs/year incurred by €50,000 and €0 verification costs; average institution has seen no fraud incidents; international students now average 23% of total population; media coverage amounting to €2 million value;

University Resources: Hallmark & Transcript printing nonexistent Paperless Economy advantage Time saving for all support services accrued-international success >95% positive response via public media acclamation

2) National Implementation in Malta

The First Comprehensive Countrywide Implementation for All Blocks [42]:

The Scope: All universities & colleges/certificates at Secondary schools + professional qualifications + continuous professional development

The Outcomes (2019-2025):

• At this point, 180k credentials have been disseminated, well over 2.3 million verifications in Malta; opportunity for cost-savings equals €1.2 million, every institution has integrated (100% enrollment) and external EU adoption has occurred

3) IBM Skills Network

The First Implemented Corporately-Based Initiative at Scale [27]:

The Platform: Built with Hyperledger Fabric protocol and issued over 10 million badges, physical/integrated into LinkedIn profiles dashboard employer verified portal reports skill taxonomy

Impact Reported: For those who received credentials, reports note a 40% completion delta at the final course level; for those who received self-credentialed badges, two-thirds (67%) shared the credential; $23,000 salary differential difference over those without nontraditional credentialed skills >500k employer verified requests submitted per month.

C. Barriers to Adoption and Challenges 1) Technical Barriers

- Interoperability concerns: systems can no longer talk to millionsof middleware costs. Average interoperable solutions are 6-12 months. Tech debt/legacy systems are 20 years old.
- Scalability: the public blockchain isn't robust enough to handleTPS. Gas fees can fluctuate depending on market-driven demand. Excessive gas fees can backlog in case of excessive demand.
- Usability: retention of private keys is essential. Private keys canbe lost, wallets can be gone, and people are gone forever. Setup is a challenge for everyone to make it work.

2) Organizational Barriers

- Financial restraints: Implementation fees are $50,000-200,000; initial steps are helpful. Maintenance fees are $10,000-50,000 per year. There must be liquid cash for trainers/workshops to learn the solutions and install them properly.
- Change management: Employees are resistant to retraining. Pro-cesses must shift. Cultures must change.
- Risk management: unpredictable maturation of tech possibilities,vendor lock risk with no exit strategy, unregulated expectations for compliance.

3) Regulatory Barriers

- Legal status: Legal status is not consistent, liability assignmentvaries worldwide; this is helpful for international potential;
- Data privacy: GDPR right to be forgotten works against all blockchain immutability. Data privacy laws prohibit the movement of data across borders. Student data should not be publicly available.
- Compliance requirements: Audit trails should be behind a pay-wall; there are retention requirements for compliance and access solutions.

VII. KEY RESEARCH GAPS

A. Legacy credential integration

The biggest gap in research concerning systems looking to rely on blockchain credentials solutions is validation of legacy credentials of those previously issued before the blockchain integration occurs. To date, 500 million issued paper and PDF diplomas create a bifurcated population moving forward with one receiving credentials with blockchain validation and one group receiving credentials with no validation whatsoever.

Current Limitations:

- JSON-LD and respective standards across the board from majorsystems
- No systems accept PDF/image request for validation
- No access to anchor back in time for transaction validation on theblockchain
- Changes to formatting nullifies legal acknowledgment in varyingjurisdictions
- Digitization/scanning requires OCR but doesn't work or works ter-ribly or works just enough but marginally fails Successful Findings Needed:
- Hash is agnostic to the document itself
- Legal regulations allow forward in time validation
- Batch request accessibility for historically legacy validation
- Authentication validity for digitized scanned documents
- Acknowledgment of legacy credentials alone

B. Interoperability

Despite standards currently there is no interoperability in the wild Technical Issues:

- Competing blockchains silo in interoperability and do not ac-knowledge existence alone
- Differing formats jeopardize credential transmission
- Differing cryptography complicates validation efforts
- Smart contracts only exist on the blockchain and require legal andlinguistic understanding

Limited credentials exist in silos through institutions and do not work universally through institutions Solutions are Needed:

- Internationally recognized standards for credential acknowledg-ment
- Cross-chain attestation capabilities
- Universalized metadata schema
- Federated identity solutions
- Automated credential equivalency matching

C. Privacy & Compliance

Current privacy solutions are not compliant with nuanced privacy situations

Open Questions:

- GDPR Art 17 works against irreversibility of blockchain
- Selective disclosure is ambiguous but poses questionable privacyconcerns
- Data protection suggests cross-border transmission concerns un-dermine sovereignty over data
- Biometrics may yield an ugly problem
- Collation attacks work against privacyResearch Questions:
- Compliant solutions for deletions
- More sophisticated zero-knowledge solutions
- Homomorphic encryption for encrypted credentials

- Decentralized access management
- Privacy-preserving analytics

D. Scalability and Performance
Current solutions do not provide performance standards based on international equivalency of education credentials Performance Gaps:
- The Ethereum Mainnet equals 30 TPS and roughly 200M certifi-cates are issued (this is applied roughly per year)
- Layer-2s complicate with centralization
- Storage costs are pricey for global south countries
- Authentication is too slow for real-time needs
- Network delay is an undetermined velocity/priorityAdvances Needed:
- Sharding for credentialing
- Practical consensus for educational use
- Compression credentials
- Caching strategies for popular credentials
- Edge computing for decentralized access

E. Post-quantum Security
Cryptography challenged by post-quantum computers upon which systems are created: Limitations:
- ECDSA signature destroyed by Shor
- RSA ineffective with smaller key size
- Requires larger hash
- Already existing credentials and falsification
- No migration abilities at presentRequired further research:
- Other quantum safe signature options
- Hybrid quantum/classic solution
- Migration of current credentials
- Performance adjustment for larger signature size
- Need post-quantum standard for performance adjustment

VIII. FUTURE RESEARCH DIRECTIONS

A. Artificial Intelligence 1) AI to fraud detection
credentials will authenticate for you
- Fraud detection from history (i.e., machine learning)
- Fraud detection from expected requests (i.e., anomaly detection)
- Fraud detection from expected requests (i.e., time series analysis)
- Fraud detection from NLP of de-framed non-structured creden-tials/CV, for framed versions of the same AI to fraud detection from NLP of de-framed non-structured credentials/CV, for framed versions of the same

Research opportunities:
- Federated learning focused privacy fraud detection
- Explainable AI fraud detection with explanations as to why/whynot to allow fraud requests
- Adversarial attacks to prove no changes occur
- Transfer learning across credentials within the same environment
- Real time scoring for fraud detection

2) Intelligent credentialing
is credentialing based on what you see via machine learning principles.
- Internal personalized learning paths credentialing.
- Systems of credentialing with approach assessments evolving asskill development internally.
- Competency prediction (i.e., courses taken) credentialing systemsthat offer jobs without job seekers seeking them.
- Automated credentialing and recommendations where jobs matchjob seekers without resumes.

B. Decentralized Autonomous Organizations (DAOs)
DAOs will create new oversight/integration with credentialing.
1) Consortium Management
Token via asking for standards adjustments, re-evaluation systems, credential integrity with reputation systems, decentralized purposes from community driven efforts and automated responses asking for credentialed access.

2) Economic models
Token economy portable credentials will be linked with tokens usable for employment; staking mechanisms favor issuer credibility due to costs associated with verification or operation; sustainability will favor all involved.

C. Emerging Technologies

1) Quantum safe implementation

post-migration processes where dual signatures needed until registrations are updated/quantum key distribution will be used for most sensitive connections; lattice-based creations will occur; hash-based signature creations will evolve; crypto-agility will be utilized;

2) Advanced privacy techniques

beyond current advances for future considerations; multi-party computation where confirmation occurs in enclaves without shared private information; differential privacy where statistics will expose private info but limited statistics that could expose private info, oblivious transfers, private set intersection will only be exposed to connected but intensive settings.

D. Standardization Efforts 1) Global standardization efforts

that require ranked priorities by nations based on internationally accepted formats in cross chain efforts with privacy preserving studies recognized regulations with quality assurance standardized efforts for practical changes;

2) Implementation guidance

that requires standardized efforts for audit purposes (security) basic levels established for user experience, guidelines exist for help/recovery options before a path is taken where users don't know what they need yet.

IX. CONCLUSION

This systematic review of blockchain credentials communicates an overarching investigation of a systematic state of the art, implementation, and literary and field gaps in-between. Bibliometric findings of 182+ publications and theorized/substantiated systems published between 2015-2025 indicate an immature market that has since transitioned to widely spread systems of production and global users.

A. Contribution to Knowledge

The blockchain credential market has become such a system that it's either too advanced to benefit in certain ways or too many subsequent investigations need substantiation:

- Advanced technological systems with 5 in production;
- 300+ institutions blockchain credentialing across the U.S. and in-ternationally;
- Countries credentialing blockchain in courts;
- Cost/time efficiencies gained and acknowledged;
- Systems that are in the development stage with privacy protectingofferings;

Yet it cannot become successful because:

- Systems can't ever verify paper/PDF credentials;
- Systems have little if no interoperability across the board;
- Systems that are not scalable with fractional cost for internationalreach;
- Systems cannot preliminarily protected/later implemented basedon user experience barriers until they have one;
- Systems that differ across different nations due to vague regula-tions.

B. Directions for Future Research

Where findings allow for further research opportunities moving forward are:

1 Legacy credential systems (grandfathered) afford systems withaccessibility without a means to reformulate change (nothing can be changed or restructured);
2 Interoperability affording requests need citation from provided established protocols that allow universal accessibility for portability;
3 Privacy protecting solutions need relevance for findings withcryptographic determinations of invisibility, if applicable (nothing can be made illegitimate);
4 Scalability needs billion credential affordability with fractionalaccess for international affordability;
5 Post-quantum migration solutions need substantiation after implementation for longitudinal validity.

C. Trends to Anticipate in Ten Years

Ten years from now, researchers should anticipate:

- Similar systems that exist in cumulative/interoperable ability;
- Integrated national identity systems;
- A/I solutions supporting fraud detection and validation;
- Post-quantum migration solutions achieved;
- Developed nation integration.

D. Suggestions Based on Findings for Practical Application

Where findings lend suggestions of supportive efforts for good are for:

Researchers seeking applicable solutions that shift from theoretical to practically applicable; higher ed institutions finding these systems in operation on a non-pilot level, should attempt these affordances on less critical systems (not degrees); governments that need to consider advancements against consumer protection legislation; technological enterprises that need to find successful support through definitive buy-in implementation.

Blockchain credentials are an amazing potential solution for digitally verified, immutable, instant access credentials which are universally accepted. Unfortunately, not enough systems have vetted that potential for most. Only time will tell if blockchain's potential is ultimately effective in revolutionizing how academic achievements are recorded, verified, and accessed. The more critical question is not if blockchain credentials will become universally accepted, but when?

When will the second half of the second-tier concerns be explored for definitive success?

The field remains at an immature stalemate of innovative potential or widespread operation - only time will tell if blockchain credentials are a passing fad, or a common expectation of the average user - and that will be determined by how quickly data points can be updated - speaking generally to challenges about legacy credentials and interoperability.

REFERENCES

[1] A. A. Khan, A. A. Laghari, et al., "Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission," Applied Sciences, vol. 11, no. 22, p. 10917, 2021.

[2] MIT News, "Digital diploma debuts at MIT," Massachusetts Institute of Technology, October 2017. [Online]. Available: https://news.mit.edu/2017/mit-debuts-secure-digital-diplomausing-bitcoin-blockchain-technology-1017

[3] MIT Media Lab, "Blockcerts—An open infrastructure for academic credentials on the blockchain," MIT Media Lab, 2016.

[4] A. Grech and A. F. Camilleri, "Blockchain in education," Publications Office of the European Union, Luxembourg, 2017.

[5] J. A. B. Moya, J. Ayoade, and M. A. Uddin, "A zero-knowledge proof-enabled blockchain-based academic record verification system," Sensors, vol. 25, no. 11, p. 3450, 2025.

[6] University of Nicosia, "Academic certificates on the blockchain," 2017. [Online]. Available: https://www.unic.ac.cy/blockchain/

[7] Sony Global Education, "Sony global education develops technology using blockchain for open sharing of academic proficiency and progress records," Press Release, 2018.

[8] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and Informatics, vol. 36, pp. 55-81, 2019.

[9] European Commission, "European Blockchain Services Infrastructure (EBSI): Verification of education credentials," 2023.

[10] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[11] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in Proceedings of the Thirteenth EuroSys Conference, 2018, pp. 1-15.

[12] Polygon Technology, "Polygon: Ethereum's Internet of Blockchains," Technical Whitepaper, 2021.

[13] Cardano Foundation, "Cardano: A blockchain platform for changemakers, innovators, and visionaries," 2020.

[14] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in 2018 IEEE Symposium on Security and Privacy, pp. 315-334, 2018.

[15] R. C. Merkle, "A digital signature based on a conventional encryption function," in Conference on the Theory and Application of Cryptographic Techniques, 1988, pp. 369-378.

[16] NIST, "Post-Quantum Cryptography Standardization," National Institute of Standards and Technology, 2022.

[17] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards postquantum blockchain: A review on

blockchain cryptography resistant to quantum computing attacks," arXiv preprint arXiv:2402.00922, 2024.
[18] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," The Sovrin Foundation, vol. 29, no. 2016, 2017.
[19] W3C Working Group, "Verifiable Credentials Data Model v2.0," World Wide Web Consortium, 2022.
[20] L. Wang, C. Peng, and W. Tan, "Secure ring signature scheme for privacy-preserving blockchain," Entropy, vol. 25, no. 9, p. 1334, 2023.
[21] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proceedings of the 41st Annual ACM Symposium on Theory of Computing, 2009, pp. 169-178.
[22] M. Finck, "Blockchain and the General Data Protection Regulation," European Parliament Study, PE 634.445, 2019.
[23] Ethereum Foundation, "Ethereum gas and fees," 2023. [Online]. Available: https://ethereum.org/en/developers/docs/gas/
[24] Protocol Labs, "IPFS: InterPlanetary File System," Technical Documentation, 2021.
[25] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," Technical Report, 2016.
[26] J. Poon and V. Buterin, "Plasma: Scalable autonomous smart contracts," White Paper, 2017.
[27] V. Buterin, "An incomplete guide to rollups," 2021. [Online]. Available: https://vitalik.ca/general/2021/01/05/rollup.html
[28] Gartner Research, "Blockchain deployment costs in higher education," Market Analysis Report, 2023.
[29] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," ACM Computing Surveys, vol. 54, no. 8, pp. 1-41, 2021.
[30] Chainalysis, "The 2023 crypto crime report," Chainalysis Inc., 2023.
[31] IEEE Standards Association, "IEEE 3205-2023: Standard for blockchain interoperability—Data authentication and communication protocol," 2023.
[32] NIST, "Recommendation for key management: Part 1 – General," NIST Special Publication 800-57, 2020.
[33] World Economic Forum, "The global cost of credential fraud," WEF Report, 2023.