Trends and Reviews of Technological Engineering in Education
Vol. 2, No. 2 (2026) | ISSN 3071-2211 | Open Access

REVIEW ARTICLE

Smart Contract-Enabled Micro-Credentialing for Competency-Based E-Learning: Architecture, Empirical Analysis, and Design Guidelines

Shuaihua Li [1,*], Dong Deng [2]
[1] School of Architecture, Jiangxi University of Applied Science and Technology, Nanchang, China 330100
[2] Research Direction of Student Management and Student Satisfaction, Jiangxi University of Applied Science and Technology, Nanchang, China 330100
* Correspondence: 664520851@qq.com

Received 14 December 2025 · Accepted 22 April 2026 · Published 30 June 2026

Abstract

Competency-based education requires credentials that specify the learning outcome, the assessment and the issuer. A learning management system can issue a portable credential. A smart contract can enforce award rules and record evidence for a verifier. This review examines smart contracts for educational micro-credentials. The reported publication window covers January 2018 to March 2025. The review reports 76 included studies, with 28 selected for detailed analysis. The stage totals reconcile, but the available records give no study-by-study list for either set. We propose a five-layer reference architecture integrating Hyperledger Fabric chaincode, W3C Verifiable Credentials, Decentralised Identifiers (DIDs), and IPFS-based hybrid storage. Published performance evidence distinguishes the timing of a ledger operation from the time required to issue or verify a credential. In a Hyperledger Fabric experiment using Fabcoin, mean end-to-end latency was 371 ms for minting and 542 ms for spending. A common educational workload would be required to rank the platforms for credential services. The review compares seven design considerations, including security, scalability, privacy and interoperability. It examines oracle security, regulatory requirements, contract auditing and access for learners, and proposes a five-phase roadmap for institutional implementation.

Keywords: Smart Contracts; Micro-Credentialing; Competency-Based Education; Blockchain; Hyperledger Fabric; W3C Verifiable Credentials; Decentralised Identity; GDPR.

How to cite: Shuaihua Li & Dong Deng (2026). Smart Contract-Enabled Micro-Credentialing for Competency-Based E-Learning: Architecture, Empirical Analysis, and Design Guidelines. TRTEE, 2(2), 1–28.
https://doi.org/10.63646/VDGR2954

1. Introduction

Competency-based education asks what a learner can demonstrate. For a small unit of learning, a recipient needs to know the outcome, the assessment and the institution that stands behind the award. The Council of the European Union's 2022 recommendation on micro-credentials identifies standard elements that issuers can record, including learning outcomes, notional workload and the type of assessment [72]. A learner applying for a job or further study may need to share that information across institutions. The receiving organisation can use it to interpret the scope of an award and decide how much weight to give it. Reviews of blockchain applications in higher education describe the management and verification of academic records among the proposed uses [5], [64]. This raises a practical question for credential design. What evidence should travel with the record so that another institution can verify it?

A verifier checking a diploma has two distinct tasks. One is to establish whether the document matches the record the issuer released. The other is to establish whether that issuer had the authority to award the qualification. In one implementation, a QR code lets a verifier check a doctoral certificate against an Ethereum record [3]. Lutfiani et al. discuss signatures and time-stamping for detecting certificate fraud [10]. Alam et al. propose a framework for managing student records securely [11]. Research on diploma forgery also identifies challenges for higher education institutions that adopt these systems [23]. A digital signature can protect a PDF, and a registry can provide a separate record against which to check it [13], [43]. Neither check alone shows how well a learner met the requirements of an award.

In proposals for blockchain-based educational certificates, the issuer registers a credential so that others can later check it [7]. A smart contract can apply issuance rules to an approved assessment record [12], [18], [48]. A separate mechanism protects the integrity of the record. Haber and Stornetta described how to time-stamp digital documents [68]. Bitcoin later linked timestamped blocks through proof of work [9]. A university can record a digest of a credential and let a verifier compare it with the digest of the document presented. That comparison can detect a change to the document. The verifier still needs to identify the issuer, check the relevant proof and decide whether to accept the issuer's claim [43], [46]. This distinction is important when a university outsources its record storage or participates in a ledger shared with other institutions.

The literature addresses different parts of this problem. Casino et al. classify blockchain applications across sectors [30]. In education, Choi et al. review uses for student records and document transactions [8], while Mihus examines uses in educational management [17]. Rasheed and Mimirinis use social impact assessment to examine how integration with a university graduation system could affect graduates and other stakeholders [14]. These studies ask different questions from a technical verification study. An employer may be able to check the signature on a credential yet still need the issuing university to explain what counted as evidence of mastery. This article brings the two questions together by considering the credential format alongside the process for issuing and interpreting academic claims.

This article brings together four contributions. The review reports 76 studies on smart contracts and educational credentials between 2018 and March 2025. A five-layer reference architecture combines Hyperledger Fabric, W3C Verifiable Credentials, decentralised identifiers and off-chain storage. The performance analysis compares what published sources actually measured and uses a documented Fabric experiment to show how transaction type affects latency. This makes it possible to distinguish a protocol setting, a measured ledger transaction and a completed university service. The final contribution is a five-phase roadmap for institutions considering credential issuance, governance,

© 2026 TRTEE. Open Access under CC BY 4.0

privacy and learner access. Sections 2 and 3 describe the background and review methods. Section 4 presents the architecture, Section 5 examines the evidence and Section 6 discusses implications for implementation. Section 7 summarises the findings and identifies questions for further research.

2. Background

2.1. Competency-Based Education and Micro-Credentialing

Competency-based education (CBE) organises learning around explicit competencies and their assessment. It need not eliminate time-based measures of progress. U.S. Department of Education guidance distinguishes credit- or clock-hour CBE from direct assessment, where progress is measured by demonstrated competencies [85]. For the architecture proposed here, an institution would specify the outcome, assessment rule and authorised decision required before issuing a credential. Recognition by an employer or another institution requires criteria for interpreting that evidence and deciding whether it meets a particular requirement.

A micro-credential records assessed outcomes from a small learning activity. Under the Council of the European Union's recommendation of 16 June 2022, assessment uses explicit criteria and the credential may stand alone or be combined with others [72]. This does not make every micro-credential a digital certificate, a single competency or a component of a CBE programme. Annex I lists eleven standard descriptive elements, including the issuer, learning outcomes, assessment type and notional workload. Annex II sets out principles for design and issuance. Recording these elements supports interpretation but does not itself confer official recognition. A receiving institution decides which credentials it accepts or combines; accumulating them does not automatically confer a degree [72].

Verification can involve several issuers and credential formats. The proposed service would measure response time and availability for its own workload before claiming that it can support a university's demand. Open Badges v2.0 defines hosted and signed assertions [47]. A verifier retrieves a hosted assertion from the issuer, while a signed assertion is checked using an authorised issuer key. Both approaches require access to the relevant credential and verification information. A ledger may record a digest for comparison with a document, but a digest match alone does not identify a trustworthy issuer or establish the truth of an assessment [43]. The institution still needs a process for correcting a record and communicating its current status.

2.2. Smart Contracts: Technical Foundations

Smart contracts are programs that execute according to rules defined for a blockchain platform [61]. Ethereum, for example, specifies how transactions change account and contract state [48], [55]. Educational designs can use a contract to check who may register a document or to record a change in its status. One study describes an Ethereum document-verification contract for the Moodle learning management system [18]. Latha et al. likewise present a framework for document verification [24]. These uses illustrate a boundary of the proposed design. A program can check a recorded prerequisite or an authorised signature. The awarding institution must determine who can assess a learner and what counts as mastery.

Hyperledger Fabric separates endorsement, ordering and validation. Endorsing peers simulate a proposed transaction. The ordering service arranges transactions into blocks, and peers validate them before applying updates to the ledger [49]. A channel limits the distribution of its ledger to participating organisations [49], [60]. Androulaki et al. report throughput above 3,500 transactions per second in particular configurations [49]. An institutional deployment would need its own workload and measurements. The choice of consensus protocol also changes

© 2026 TRTEE. Open Access under CC BY 4.0

the assumptions behind confirmation. Studies of Bitcoin relate confirmation security to block production, network conditions and competing chains [50], [63]. In permissioned systems, Byzantine fault tolerance addresses a different failure mode, including a participant that sends conflicting messages [62], [69]. The consortium must identify which failures its ordering protocol can tolerate, which organisations can write records and whom they must trust [51].

2.3. Decentralised Identity and W3C Verifiable Credentials

The W3C Verifiable Credentials (VC) Data Model describes how an issuer expresses claims about a subject and how a holder can present a credential to a verifier [43]. A university can issue a signed credential to a learner, who can store it in a digital wallet and share it with an employer. A decentralised identifier (DID) can identify the university. The DID method determines how the verifier resolves the identifier and obtains verification material [46]. A distributed ledger is one possible registry. The verifier checks the proof and decides whether to trust the university for the particular claim. Privacy also depends on how the system processes data. Even when the credential is stored off-chain, an identifier or hash may be linkable to an individual. That possibility matters when assessing the processing under the GDPR [45].

Figure 1 groups the proposed system into five functional layers. It is a reference design, with interfaces between the application, identity, contract, ledger and storage components. A deployment would need to specify those interfaces and test its credential and transaction flows. Upgrading one component would also require compatibility checks for the components that use it; the diagram does not establish independent upgradeability or production readiness.

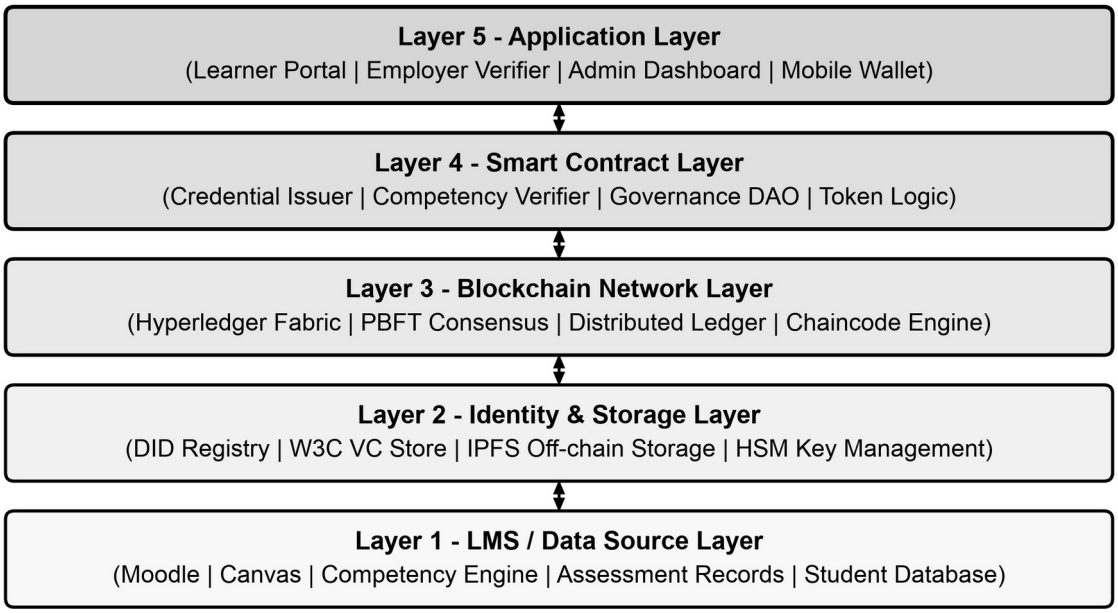


Figure 1. Five-Layer Reference Architecture for Smart Contract-Enabled Micro-Credentialing System

Layer 5 separates learner, verifier and administrator interfaces. In a Fabric deployment, an application could use Fabric Gateway to evaluate queries and submit transactions; the gateway coordinates endorsement, ordering submission and commit-status checks [54]. The design must also specify who may request each operation and how the application and chaincode validate its inputs. An authenticated REST or gRPC connection does not, by itself, ensure that a credential request is authorised or correct.

Table 1. Comparison of Credential System Approaches: Features and Trade-offs

Feature	Paper/PDF Diploma	Open Badges (Centralised)	Public Blockchain	Permissioned Blockchain	SSI + W3C VC

© 2026 TRTEE. Open Access under CC BY 4.0

Feature	Paper / PDF	Open Badges	Ethereum	Fabric	SSI + W3C VC
Tamper evidence	Issuer copy	Proof or record	Ledger digest	Ledger record	Securing proof
Verification method	Varies by file	Host/signature	Ledger check	Ledger check	Credential proof
Privacy review	Access rights	Shared fields	Persistent identifiers	Channel access	Disclosed attributes
Capacity factor	File handling	Host capacity	Load and gas limits	Workload and configuration	Proof checks
Exchange format	Paper or PDF	Open Badges profile	App-defined	App-defined schema	VC data model
Issuer check	Issuer contact	Issuer profile	Key binding	Member roles	Verify issuer authority
Cost drivers	Staff time	Hosting	Network fees	Nodes and operations	Wallet support
Version to record	File format	Badge version	Contract code	Fabric release	VC model version

Table 1 gives examples at different layers. A ledger can record a digest while a W3C credential carries the issuer's proof. The verifier must establish who controls the signing key and whether to trust that issuer for the claim [43], [73]. A privacy review follows who can link, access or retain the data [45]. Institutions may exchange records using a common format [58] and still apply different rules for recognising a qualification [72].

2.4. Related Work and Positioning of This Study

Chen et al. discuss ways to use blockchains for academic certificates, learning records and the recognition of achievement [34]. A subsequent review examines blockchain solutions specific to higher education [53]. Skiba discusses educational credentials [42]; Park examines blockchain in education [64]. A paper may propose a record format, implement a prototype or observe its use by an institution. Each supports a different conclusion. For example, a verifier can test whether an altered document is detected in a prototype. Evidence about the time staff spend handling exceptions or how employers interpret an award requires observation in the setting where people use it. This distinction guides the comparison with earlier reviews.

Delgado-von-Eitzen et al. searched eleven databases and included 28 articles in their final review of blockchain applications in education [4]. Ocheja et al. combined bibliometric analysis with a qualitative component. They selected 44 papers for full reading to examine applications and their integration with educational tools [6]. Rustemi et al. reviewed 34 primary studies specifically on academic certificate verification [13]. These counts refer to different questions and stages of selection. Silaghi and Popescu compared blockchain initiatives with established practices in higher education [25]. Their review appeared on 8 April 2025, after the March cutoff stated below, and is cited here as later context. This article focuses on how an assessment record can support a competency claim, how the claim can be verified and how institutions might implement the process.

3. Methodology

3.1. Systematic Literature Review Protocol

The review reports its selection process using PRISMA 2020 [29], which updates the 2009 statement [56]. PRISMA-P addresses review protocols [65]. Three questions guided the review. RQ1 asks which smart contract architectures have been proposed or deployed for educational credentials. RQ2 asks which benchmarks and security properties have been reported and how the alternatives compare. RQ3

© 2026 TRTEE. Open Access under CC BY 4.0

asks which technical, regulatory and institutional barriers affect adoption and which design choices address them. The search covered IEEE Xplore, Scopus, Web of Science, ACM Digital Library and SpringerLink using the search string: ("Smart Contract" OR "Chaincode" OR "Blockchain") AND ("Micro-credential" OR "Competency-Based" OR "Digital Badge" OR "Verifiable Credential" OR "Academic Certificate") AND ("Education" OR "E-Learning" OR "Higher Education"). The temporal scope was January 2018 to March 2025 [29], [38], [39].

Eligibility required English-language, peer-reviewed work proposing or deploying a blockchain mechanism in education, with enough detail for technical replication. The protocol excluded purely theoretical work without implementation, non-educational applications and grey literature. The authors report independent screening by two reviewers, with a third helping resolve disagreements. They report Cohen's kappa of 0.87. Recalculation requires the screening stage and the reviewers' paired decisions before consensus [66].

Figure 2 gives the reported totals. Removing 93 duplicates from 487 search records left 394 to screen. Excluding 271 by title and abstract left 123 full texts. The 47 full-text exclusions comprised 18 off topic, 12 without peer review, 10 published before 2018 and 7 with insufficient methods. This left 76 for synthesis, including 28 for detailed analysis. The totals reconcile. The available records do not link individual reports to the 76 studies or identify the 28 selected for architectural completeness and empirical rigour.

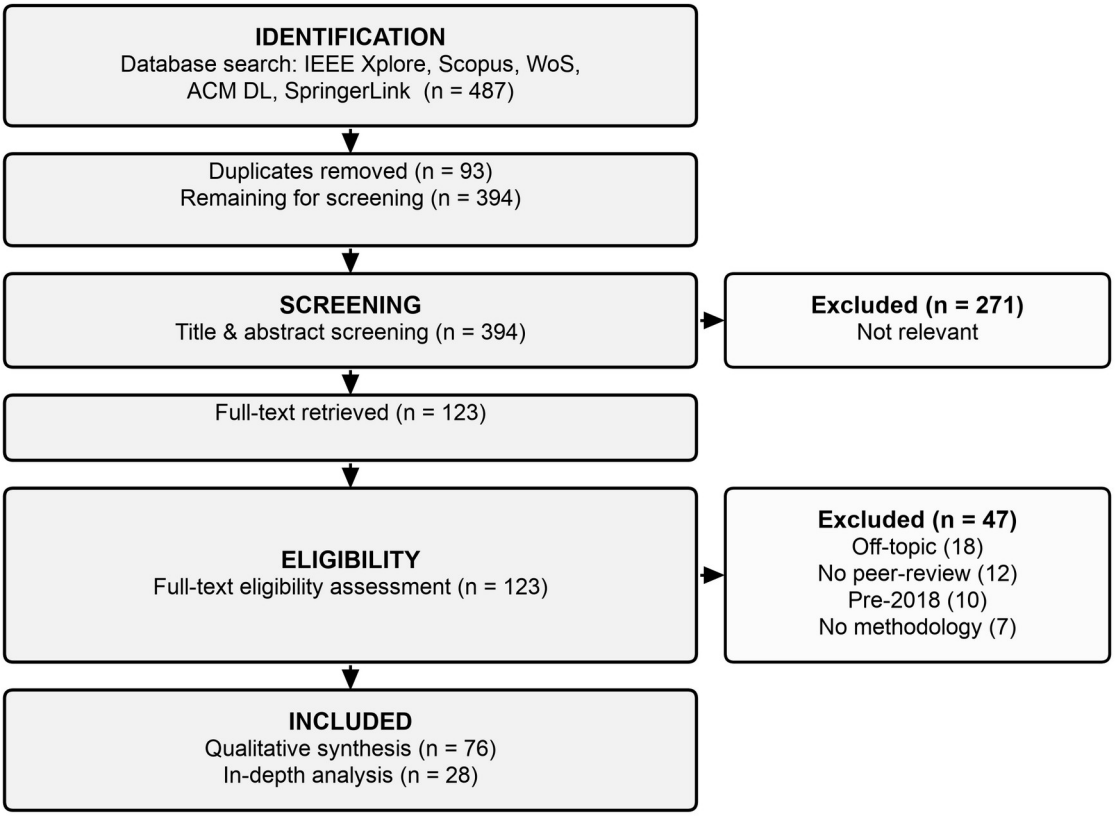


Figure 2. Reported selection totals. The 28 detailed studies are a subset of the 76.

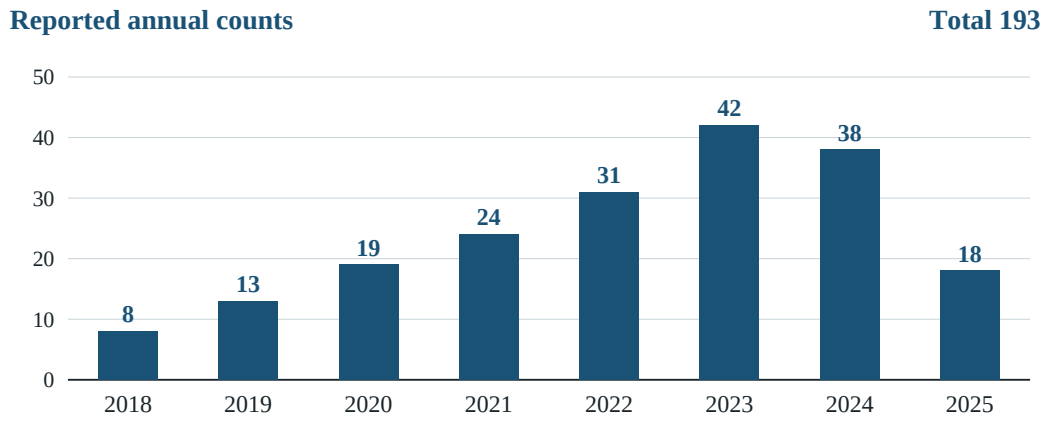
Basilaia and Kvavadze describe the move to remote teaching in Georgia [40]. Cheriguene et al. discuss online learning during pandemics [19]. Neither source establishes the geographic distribution of this review. The original Asia-Pacific share was 31%. With 76 studies and one region per study, 23/76 is 30.3% and 24/76 is 31.6%.

© 2026 TRTEE. Open Access under CC BY 4.0

Neither rounds to 31%. Establishing regional shares requires the location recorded for each study and the rule for studies spanning several regions.

3.2. Interpreting the Reported Publication Counts

Figure 3 reproduces the annual counts in the manuscript. From 2018 through 2025 the values are 8, 13, 19, 24, 31, 42, 38 and 18. They sum to 193. Assigning each of the 76 included studies a single publication year would instead yield a total of 76. The source records for the plotted series were unavailable. Its rise from 8 in 2018 to 42 in 2023 gives annualised growth of 39.3% over five intervals for that series alone. The eligibility window ends in March 2025. The last bar has no documented cutoff. W3C published its first VC Recommendation in November 2019 [43]. The EU recommendation on micro-credentials followed in June 2022 [72].



The eight bars sum to 193. Their link to the 76 included studies is undocumented.

Figure 3. Annual counts transcribed from the manuscript. Study membership is unverified.

The named and anonymised versions of the submission share the same 112 references. Of these, 39 are dated before 2018. At most 73 entries remain before further eligibility checks. The bibliography also cites standards and methods. It does not map reports to the included studies or the detailed subset. A reproducible record would identify each included study, cite its reports, and give the publication year used in the analysis [29], [66]. One report can describe several studies, and one study can produce several reports.

3.3. Data Extraction Framework

The stated extraction framework covers nine fields. These are ledger platform and version, contract language and execution environment, credential standard, identity management, storage design, performance, security analysis, regulatory strategy and deployment context. To reproduce the detailed analysis, each of the 28 study records would need a citation, a source location and the values extracted. A study may describe several implementations. Each benchmark needs its own workload, unit and test conditions [38], [39]. Published reviews provide context for the comparison [13], [25].

4. Proposed Reference Architecture

4.1. Architectural Design Principles

The five-layer architecture uses six design principles. Separation of concerns gives the assessment record, the issued credential and the verification information distinct roles. For each item, the issuer can specify who creates it, who can read it and how it can be corrected. Privacy by design calls for

© 2026 TRTEE. Open Access under CC BY 4.0

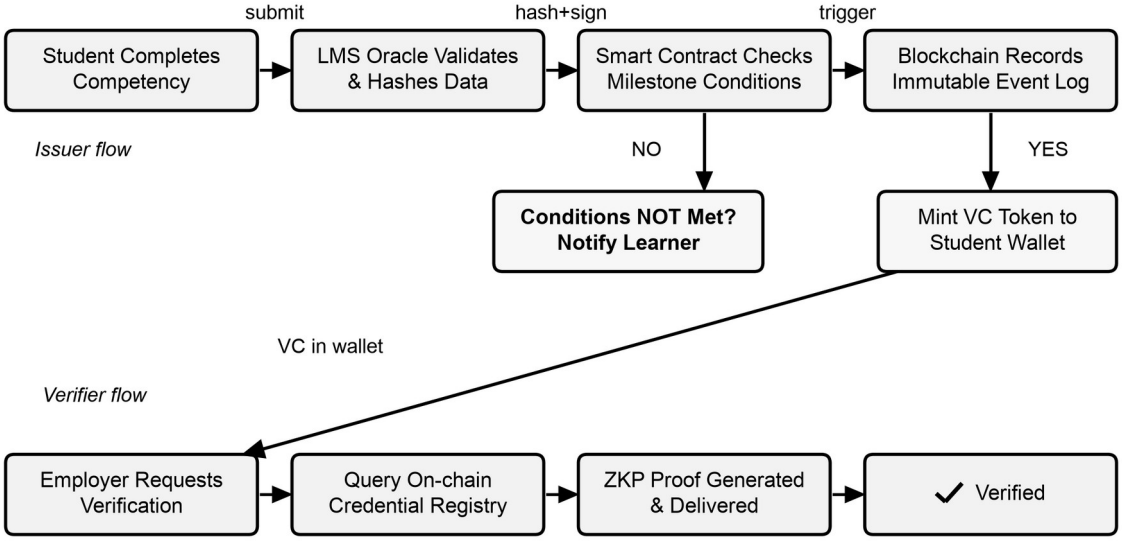
documenting the personal data and identifiers that each participant can link to a learner [27], [45]. For interoperability, the issuer and verifier need to agree on a credential format, a proof mechanism and the way they resolve issuer information [43], [46], [47]. Defence in depth calls for separate checks on the authority of the assessor, access to the issuing contract and the status of the credential. A check at one of these boundaries answers a different question from a check at another [28], [57].

Governance transparency requires a record of who can admit a member, approve a contract upgrade or change a retention rule. Consortium members need access to the rules that apply to them and a way to challenge decisions [2], [22]. For economic sustainability, an institution can estimate fixed operating costs and the additional cost of each type of activity. Issuing a credential, looking up its status and processing an appeal use different resources. The cost comparison in Section 5.5 therefore distinguishes the number of issuances from the number of verification requests.

4.2. Smart Contract Design Patterns

Three patterns organise the proposed credential service. The Credential Registry Pattern (CRP) records a document digest and issuer identifier, building on document-verification designs [18]. It would also need a status check and a rule for trusting the issuer. The Competency Gate Pattern (CGP) checks recorded prerequisites against an institution's stated award rule. Such a check cannot establish that an assessment was valid or that another institution recognises the credential. The Consortium Governance Pattern (CGovP) records approvals required by an agreement between institutions. Fabric's endorsement policies can require designated organisations to endorse a transaction [54]; those signatures must be distinguished from an academic decision to recognise credit. These are design proposals whose implementation and educational validity require separate tests.

Figure 4 starts at the interface between the learning management system (LMS) and the ledger. Related work examines blockchain integration with an LMS [20] and proposes a model to protect online examination results [21]. In the design shown here, the LMS sends an approved assessment result to the oracle. The oracle checks who authorised the record, computes the credential digest and submits the issuance transaction. A later digest check can detect changes to the recorded document. If the original grade was entered in error, the same check will still pass. A process for correcting the source grade is therefore part of the issuance workflow.



© 2026 TRTEE. Open Access under CC BY 4.0

Figure 4. End-to-End Smart Contract Workflow for Micro-Credential Issuance and Verification

In the verifier flow, the learner presents a credential from a wallet. The verifier checks the proof, obtains the issuer's verification information and checks status when a status mechanism is specified [43], [46], [73]. Some systems use a zero-knowledge proof to demonstrate a defined statement while keeping its inputs private [67]. Whether a credential can be presented this way depends on its securing mechanism [73]. Figure 4 illustrates one such design. To measure verification time, an implementation would need to specify the proof, the status check, the network conditions and where timing begins and ends.

4.3. Storage Architecture: Hybrid On-Chain / Off-Chain Model

In a hybrid credential system, the issuer can keep the certificate off-chain and put a cryptographic commitment to it on the ledger. A verifier with the certificate can recompute the commitment and check it against the published value. The issuer must specify which bytes are covered, how the verifier establishes the issuer's identity and how it checks whether the certificate is still valid. IPFS is one possible store for an off-chain document. Its content identifier addresses content, while access over time depends on somebody retaining and serving it [44]. An institution also needs to identify who holds copies and which records can still be linked to a learner. Under the GDPR, identifiability depends on the means reasonably likely to be used. Article 17 sets out grounds for erasure and exceptions [45]. Deleting a file from one service addresses only the copy held there.

Table 2. Storage designs and checks when a credential changes

Storage design	Where the evidence is kept	Checks after a change
Full on-chain	Credential data are replicated by ledger nodes.	Check the current award and its status. Earlier entries can remain on replicas.
Off-chain database	The institution keeps the credential in its database.	Check the authorised issuer record. Track exports and backups separately.
IPFS with a ledger	A CID addresses the file. A commitment is recorded on the ledger.	Check the commitment and new version. Other nodes may retain an unpinned file.
Encrypted on-chain	Ledger nodes hold ciphertext. Decryption keys are kept separately.	Account for key backups and previously decrypted copies when retiring a key.
Cloud with notarisation	The cloud holds the file. A separate service can timestamp its digest.	Verify the timestamp and digest. Ask the credential issuer for current status.

The four shares in the original Table 2 totalled 112%. The submission leaves their denominator and possible overlaps unspecified. A timestamp can establish that a digest existed by a given time [68]. The TU Delft pilot gave the learner an OpenCert file and published a certificate hash [80]. In December 2018, KAUST announced plans to issue Blockcerts to that month's graduates [81].

4.4. Consortium Governance Framework

An educational consortium needs to assign responsibility for decisions that affect more than one institution. Six questions help define the agreement. Who may operate a node or attest to a learner's result? Who may propose, test and approve a contract upgrade? Which party handles retention, access and

© 2026 TRTEE. Open Access under CC BY 4.0

correction requests for the records it controls? How can a receiving institution or a learner dispute a credential? How will the members share operating and support costs? Who will track changes to credential formats and tell members which versions their verifiers accept? The answers can differ for an issuing university and a verification provider [2], [22], [59]. An agreement can identify a decision maker, a record of the decision and an appeal route for each responsibility. A comparison across consortia would require evidence of these arrangements for each participating service.

Hassan and De Filippi describe DAOs as arrangements for coordination through blockchain rules and decentralised governance [52]. This does not make token-weighted voting a requirement for every DAO or determine whether an educational credential will be recognised. The proposed consortium would allocate specific decisions to named institutional roles. A steering committee could authorise protocol changes, while contracts could record approvals and apply agreed membership rules. The agreement would need to define representation, voting rights, conflicts of interest, correction procedures and accountability for each decision. It should also identify the institution responsible for assessment and credit recognition, including cases that require human review. A recorded vote would show that a configured procedure was followed; it would not by itself establish the educational validity or regulatory acceptability of the result.

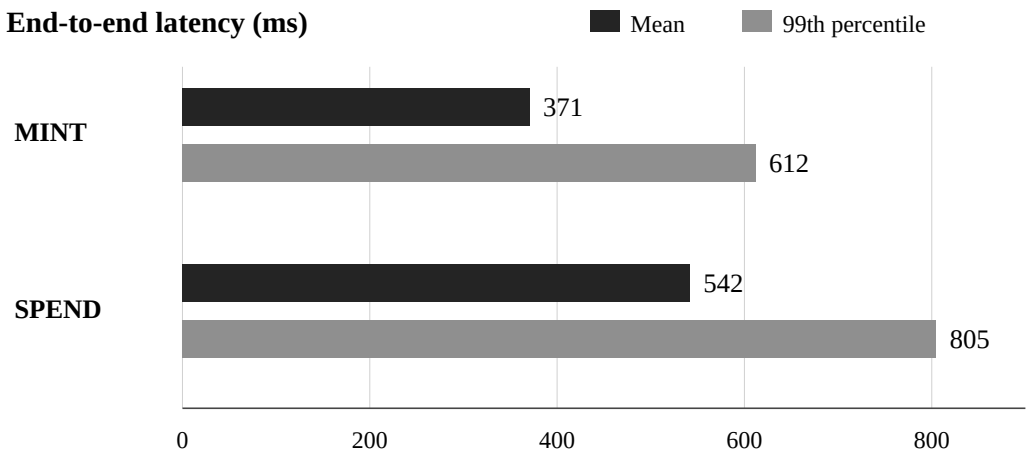
The EduCTX prototype used ECTX tokens to represent credits earned for completed courses. Its authors built the first implementation on ARK [59]. A later report describes an implementation on Ethereum using smart contracts for digital credentials [89]. The two reports document a change in implementation. Neither establishes a market price for credits or measures the financial viability of a university consortium. A separate trial at TU Delft assigned different roles to the university and its partner, Accredify. The university identified an eligible volunteer and agreed how the learner's information would be used. Accredify provided the issuance and verification service [80]. These arrangements illustrate which responsibilities partners must allocate. Comparing fees or long-term funding would require their agreements and operating accounts.

5. Empirical Analysis and Results

5.1. Platform Performance Benchmarks

The consensus and architecture literature describes differences among blockchain designs [15], [16], [31], [32]. Among the five sources cited here, Androulaki et al. report controlled measurements on Hyperledger Fabric using Fabcoin [49]. Figure 5 compares the two transaction types in that experiment. In an educational example, a Moodle document-verification contract was tested on the Ropsten test network [18]. A test of that application and a payment benchmark answer different questions. A comparison of campus issuance, verification and revocation would need the same payloads, operations, hardware, network conditions and definition of completion for each platform.

© 2026 TRTEE. Open Access under CC BY 4.0



End-to-end time includes endorsement, ordering and validation.

Figure 5. Fabcoin end-to-end transaction latency on Hyperledger Fabric 32-vCPU peer and 2 MB blocks, from Table 1 of Androulaki et al.

Androulaki et al. measured Fabcoin on Fabric v1.1.0-preview. With a 32-vCPU peer and 2 MB blocks, mean end-to-end latency was 371 ms for MINT and 542 ms for SPEND. At the 99th percentile the corresponding values were 612 and 805 ms. The same experiment reported average throughput above 3,420 MINT and 3,560 SPEND transactions per second [49]. It used a Kafka ordering service. These observations concern the execution of Fabcoin transactions. A registrar timing credential issuance would also have to define when assessment approval, delivery or confirmation counted as complete. For a separate capacity example, suppose 40,000 students each need one issuance transaction and the service sustains 100 transactions per second. The estimated batch time is 40,000 / 100 = 400 seconds. This rate is an assumption for the calculation. Queuing, retries and the required level of finality would affect the elapsed time.

Table 3. Published timings and protocol settings for five blockchain configurations
Block intervals, transaction latency and confirmation time have different endpoints.

Platform	Source or setting	Reported quantity	What it describes
Ethereum (proof of work)	Mainnet before the 2022 Merge [86]	About 13.3 s	Target time between successive blocks
Ethereum (proof of stake)	Mainnet after the 2022 Merge [86]	12 s per slot	Opportunity to propose a block
Hyperledger Fabric	Fabcoin, 32-vCPU peer, 2 MB blocks [49]	371 ms (MINT) 542 ms (SPEND)	Mean end-to-end transaction latency
IOTA (legacy Tangle)	Historical mainnet study, 2020 [87]	Around 10 min for a majority of transactions	Time to transaction confirmation
Custom EduChain (Clique-style PoA)	Clique specification EIP-225 [88]	Configurable minimum block period	Minimum interval between timestamps

Custom EduChain denotes a class of networks. The Clique specification sets a minimum block interval [88]. MIT used Bitcoin anchoring for its diploma pilot [78]. To compare energy per 1,000 transactions, divide metered kilowatt-hours by completed transactions and multiply by 1,000. A fee comparison also needs a date, currency and fee model.

5.2. Security and Attack Surface Analysis

© 2026 TRTEE. Open Access under CC BY 4.0

The security analysis distinguishes three operations. A verifier can compare a credential digest with a trusted reference. A secure transport channel can protect the message between the assessment system and the issuer. The issuer still needs to establish that the assessment was approved by the person authorised to award credit [28], [35], [43]. For example, a correctly signed message can carry an obsolete grade. Reviewing this case requires the source record, its version, the person or service permitted to submit it and the policy for handling a later correction. The assessment record supplies that approval history.

Table 4 presents seven failure modes and tests that an institution can adapt to its credential workflow. Each row describes a possible failure and an expected result to check. Comparing the frequency of a defect across platforms would require the identity and version of each implementation, the number examined on each platform, the tests applied and the number with a confirmed finding. An unreported test must be coded separately from a completed test that found no defect. The review reports 28 studies selected for in-depth analysis. A study can describe several contracts, and several papers can describe one implementation. A contract-level rate therefore needs a documented link from each paper to the implementations it describes.

Table 4. Security checks for educational credential systems

Failure mode	Example in a credential service	Proposed test and expected behaviour
Reentrancy	A callback re-enters issuance before the award is recorded.	Call back into the issuance function. One approved award should produce at most one credential.
Integer overflow or underflow	A counter wraps and reuses a credential identifier.	Try values at both bounds. An invalid update should fail without changing the credential record.
Access-control bypass	A caller without the issuer role issues or revokes a credential.	Exercise each role, including a former issuer. Unauthorised calls should leave the credential state intact.
Time-dependent release	A time check releases an award before an assessment deadline.	Test immediately before, at and after the cutoff. Compare each outcome with the stated release rule.
Oracle input manipulation	A stale or unauthorised assessment changes a learner's award.	Reject stale or wrongly signed inputs. Replaying an accepted result must not issue a second award. Test an authorised correction.
Consensus fault assumptions	A validator outage or collusion disrupts agreement on a record.	State the quorum and fault model. Test a partition and recovery. Check for conflicting commits and record when progress resumes.
Transaction ordering	Competing updates arrive in a different order from the one expected.	Run issuance, revocation and replay in different orders. Check the final status against the specified credential lifecycle.

For an oracle test, start with an approved assessment, record the credential identifier and replay the same message. Then submit a corrected assessment through the institution's authorised procedure. Check whether the original award was duplicated and whether the verifier can see the intended status after correction. Record the inputs and observed states for the tested version. Slither can help identify Solidity code paths for inspection [91]. Fabric endorsement policies govern which parties must endorse a transaction [49], [60]. Assessing the accuracy of the grade still requires the assessment record.

5.3. Evidence for Evaluating Credential Systems

Figure 6 sets out seven questions an institution can use to evaluate a credential service. First specify the issuer, the learner, the verifier and the operation under

© 2026 TRTEE. Open Access under CC BY 4.0

test. A learning management system can issue a W3C credential. The institution can separately decide whether to record a digest on a public or permissioned ledger [43], [73]. The credential format, the application and the ledger can therefore be evaluated within the same deployment.

Dimension	Evaluation question	Evidence to collect
Security and privacy	Can a former issuer change an award? What data are disclosed?	Rejected or accepted request and the fields visible to each role.
Scalability	Can the service finish an end-of-term batch on time?	Completed awards per second and 95th-percentile latency at a stated load.
Data protection	How is a valid erasure request handled across copies?	Decision, action dates and the basis for retaining any copies.
Operating cost	What does it cost to issue and maintain a defined batch?	Costs over the stated period and the number of completed awards.
Interoperability	Can a second system read the claim and check its proof?	Formats and versions used, plus the result of each check.
Learner experience	Can a learner recover access and present an award?	Task completion, time taken and assistance requested.
Standards maturity	Which published profile does each implementation support?	Dated specification, conformance tests run and their results.

Figure 6. Seven questions for evaluating a credential service

The original radar plot illustrates a limit of numerical comparison. Its seven Fabric values sum to 53. Their equal-weight mean rounds to 7.6 out of 10, whereas the submitted text reported 7.1. The submission omits the study-level inputs and rules needed to reproduce those scores. For an institutional evaluation, define the workload and timing boundary before measuring latency. The Fabcoin measurements in Figure 5 describe transactions under one Fabric configuration [49]. For privacy, identify the learner records, who can access them and how long copies are kept [45]. For learner access and recognition, observe a learner presenting a credential and a receiving institution deciding whether to accept it [25], [27]. Those observations answer different questions from a transaction benchmark.

5.4. Competency Ecosystem Mapping

Figure 7 organises six proposed component clusters around micro-credential exchange. Competency frameworks define the skills and evidence to be recorded; mappings to qualifications or sector taxonomies require review rather than an assumption that shared labels mean equivalent competence [1], [34], [47]. A rule engine may check versioned prerequisites and co-requisites approved by the awarding institution. A credential in a portfolio provides evidence for review; it does not automatically award credit or waive a requirement. Applicable equivalencies, missing evidence and disputes need institutional decisions.

© 2026 TRTEE. Open Access under CC BY 4.0

Certificate verification alone does not establish educational equivalence [12], [71].

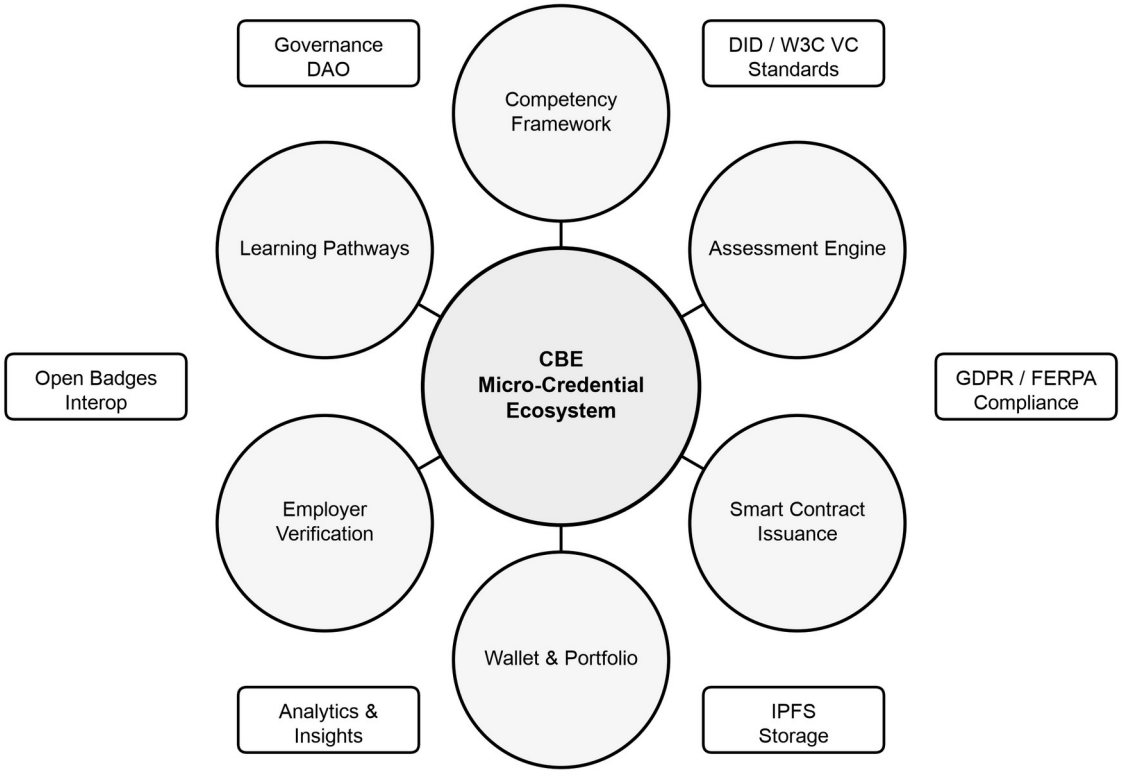


Figure 7. Competency-Based Micro-Credentialing Ecosystem: Components and Interdependencies

A DAO-inspired component could record proposals and votes on the consortium's network rules [52]. The design would specify who may propose a change, how votes are counted and how learners participate. Decisions about assessment and recognition would remain assigned to identified institutional roles. Course credits and governance votes represent different rights: the EduCTX prototype assigned ECTX tokens for completed coursework [59]. To evaluate participation, a study would need records of voting rights, proposals, turnout and how decisions were implemented. A ledger of earned credits alone would not provide that evidence.

5.5. Economic Analysis: Transaction Costs and Total Cost of Ownership

Consider a five-year cost scenario for a university with 20,000 students and 5,000 credential issuances per year. The amounts below are inputs to the calculation, expressed in US dollars. The model counts setup costs once and recurring costs in each of five years. It assumes that annual volumes and unit costs stay constant, with no adjustment for inflation or discounting. The five-year cost per student uses 20,000 as its denominator. The cost per credential uses all 25,000 issuances.

The one-time Fabric costs are USD 80,000–120,000 for setup, 60,000–90,000 for chaincode development and audit, 40,000–70,000 for LMS integration and 15,000–25,000 for legal review. Together they total USD 195,000–305,000. The annual inputs are USD 18,000–36,000 for three cloud nodes, 20,000–30,000 for maintenance and 10,000–15,000 for standards and wallet updates. These sum to USD 48,000–81,000 per year. Adding five years of recurring costs to the initial investment gives USD 435,000–710,000 over five years. With the stated denominators, this is USD 21.75–35.50 per student over the full period, or USD 17.40–28.40 per credential issued.

© 2026 TRTEE. Open Access under CC BY 4.0

An issuance and a verification request are different services. A break-even calculation would need the number and cost of verification requests actually avoided, together with the operating costs that the institution would continue to incur.

For a public Ethereum scenario, assume that each issuance requires one transaction and that the fee is USD 0.05–0.80 per transaction. At 5,000 issuances annually, transaction fees would total USD 250–4,000 per year, or USD 1,250–20,000 across five years at the same rates. This calculation covers only transaction fees. An institution comparing platforms would also need development, integration, key management, hosting, support and compliance costs on a consistent basis. The volume of credential issuance and the volume of verification requests must be specified separately. A verifier may be able to check a signed credential without submitting a new ledger transaction [43].

5.6. Geographic Adoption Patterns and Institutional Readiness

Publication geography and the location of a working credential service measure different things. A paper can report a design without naming an issuing institution. A single pilot may also involve universities in several countries. For example, the European Commission describes a July 2021 EBSI pilot in which two alliances brought together eleven universities from eleven countries to test six cross-border scenarios [82]. Its unit of observation was the scenario. Counting each university as a separate rollout would give a different impression of the programme. In the United States, MIT's 2017 diploma pilot gives earlier context for recipient-held records [78]. The date places it before the review's 2018 start. A regional comparison of deployment maturity needs dated evidence for each service and one rule for counting sites that participate together.

In Singapore, OpenCerts allows an institution to issue a digital certificate with a cryptographic proof. A verifier can check the file against its proof and the record on the blockchain [83]. In a cross-border example, TU Delft and Accredify tested this route with a Singapore-based professional learner who had completed a TU Delft course [80]. In Japan, Tohoku University made Open Badges available to eligible learners completing its online courses from fiscal year 2022 [84]. The notice describes the learner's completion requirement and how the learner receives the award. In Saudi Arabia, KAUST announced in December 2018 that it planned to issue digital credentials to its graduates using Blockcerts [81]. A programme announcement, a single-learner trial and an offer to eligible course completers establish different facts. Comparing uptake across regions would require the number eligible, the number issued and a common observation period.

For an institution planning a rollout, a practical starting point is to assign a person or team to each part of the service. The registrar can identify which record authorises issuance and who can correct it. The technology team can test what happens when a learner loses access or an external verification service is unavailable. Learner support can record how many people need assistance and at which step. MIT's pilot, for example, offered the digital diploma option to 111 graduates [78]. To estimate uptake, the next measure would be how many accepted that offer. To estimate routine support needs, it would also help to know how many activated their wallets, shared a credential or requested help during a specified period. A university budgeting a rollout can use these quantities to separate one-time integration work from recurring support. Comparing actual costs across institutions would also require their approved budgets, expenditures and reporting periods.

© 2026 TRTEE. Open Access under CC BY 4.0

6. Critical Discussion

6.1. The Oracle Security Gap: Priority Research Agenda

An oracle carries information from an assessment system to the credential contract. Even a valid ledger transaction can record an incorrect, incomplete or outdated educational claim [28], [35]. Table 4 gives examples of the inputs and outcomes to test. For each source, identify who may submit a result, how the service recognises a repeated message and how a disputed grade can be corrected. A useful test record includes the source event, the authorised approval, the contract version and the credential state before and after processing. These records let an auditor trace a particular award to its assessment.

Multiple feeds may help identify discrepancies when their sources and failure modes are sufficiently independent; agreement alone does not establish that the assessment is correct. Threshold signatures can require approval by a specified number of authorised parties, but confirm signatures rather than educational validity. Slither applies static analysis to Solidity contracts [91]. Formal methods can establish specified properties under a defined model and assumptions; neither a clean tool report nor a proof of a limited property establishes that the whole credential service is secure. Evaluations should record the code, tool versions, threat model, coverage and how identified issues and disputed assessment inputs are handled.

6.2. Regulatory Architecture: GDPR, FERPA, and Global Compliance

Legal obligations depend on the jurisdiction, the parties and their roles. Where the GDPR applies, controllers must assess the purposes, data minimisation and the conditions for erasure [45]. Under FERPA, a parent or eligible student may inspect education records and request amendment of information believed to be inaccurate, misleading or in violation of privacy rights [90]. A ledger does not remove these obligations. Cross-border operations require an assessment of the disclosure, transfer and data protection rules that apply to each institution and transaction. Institutions should document how those rules are implemented and reviewed.

Keeping credentials off-chain and anchoring proofs or identifiers may reduce some exposure, but a hash or identifier can still be personal data if it can be linked to an identifiable individual [45]. Selective disclosure and zero-knowledge proofs can limit the information presented; their effects depend on the proof mechanism and the implementation [43], [45]. A correction pointer can direct a verifier to an updated record, but does not itself erase a prior record or establish legal compliance. The institution must define how it handles access and amendment requests, corrections and retention for the records it controls. It should also test whether verifiers use the current credential and whether earlier records remain accessible. The relevant legal requirements depend on the applicable rules and on the details of the deployment [45], [90].

6.3. Digital Equity and Inclusion Imperatives

A learner may need to install a wallet, retrieve a credential, recover access and present it to a verifier. Each step places different demands on the user [2], [41]. In MIT's pilot, the offer of a digital diploma establishes who had the opportunity to participate [78]. A usability study would need to observe a defined task, record how many people attempted it and distinguish independent completion from completion with help. Initial uptake and successful presentation should be measured separately. To compare learners with different prior experience, the study would also need the size

© 2026 TRTEE. Open Access under CC BY 4.0

of each group and the support available during the task. Readiness for blockchain use in assessment is a related but distinct research question [26].

Connectivity, equipment and staffing can limit participation, so readiness needs local assessment rather than inference from a country's income category [2], [41]. Proposed options include assisted or custodial wallets and participation without a full node; privacy, access recovery and support still need review [2], [59]. Offline checks depend on the verification material available. A stored proof does not establish current issuer trust or current revocation status. The verifier should record the profile, evidence and time checked, apply its status-freshness policy, and defer a decision if a required check cannot be completed [43], [73].

6.4. Implementation Evidence: Case Study Synthesis

Table 5 traces five dated milestones in four credential initiatives. The two university reports from 2017 supply historical context before the review period. EduCTX appears twice because the developers reported two different platforms. Each row identifies the scope of the original account and what it demonstrates.

Table 5. Documented milestones in academic credential initiatives

Initiative and year	Platform	Credential or record	Scope	Evidence type	Reported use
MIT Blockcerts (2017) [78]	Bitcoin anchoring	Digital diploma	111 offered the option	University pilot	Receive, share and verify a digital diploma
University of Melbourne (2017) [79]	Learning Machine	Teaching Certificate	Teaching programme	University issuance report	Issue a recipient-held Blockcerts record
EduCTX (2018) [59]	ARK	ECTX tokens	Course credits	Prototype paper	Record credits earned for completed courses
EduCTX (2018) [89]	Ethereum	Digital micro-credentials	Learner skills	Developers' technical report	Issue and verify digital credentials
TU Delft and Accredify (2021) [80]	Ethereum	OpenCert file	One volunteer	Cross-border pilot with a learner in Singapore	Check a shared certificate in the verifier portal

MIT counted students offered a digital diploma. TU Delft described one learner who completed a course and agreed to a verification trial [78], [80]. A comparison of uptake would require counts of offers and acceptances at both institutions. Melbourne documented the issue of its Teaching Certificate but supplied no recipient count or service timings [79]. The two EduCTX papers describe how credits or credentials were represented on successive platforms [59], [89]. They provide no basis for estimating a token price or consortium revenue. To compare service performance, each institution would need to report the same operation, the observation period and the number of attempts. For wallet uptake, the denominator would be eligible learners offered a wallet.

6.5. Research Gaps and Future Directions

© 2026 TRTEE. Open Access under CC BY 4.0

Five questions guide further evaluation. First, can an institution detect a false or stale assessment input and recover the intended credential state? A threat model should identify which parties are trusted and which failures it covers [28], [35]. Second, can the service handle an end-of-term batch at the required rate? A comparison of layer-2 or other scaling designs needs the same operations, load and definition of completion [32], [36]. Third, can participating institutions carry out the access, disclosure and correction procedures that apply to their records? A review should trace the actual data flows and responsibilities in each jurisdiction [27], [45], [90]. Fourth, how do learners and employers use a credential over time? An evaluation can follow a defined cohort and record eligible learners, offers, acceptances, subsequent use and staff support. Finally, who encounters barriers when obtaining or presenting a credential? Researchers can observe the same task under different access conditions, including limited connectivity, loss of access to a device or the need for assistance [2], [41]. Each question requires evidence from the activity being studied.

Table 6. Evidence and proposed studies for institutional credential systems

Research Gap	Evidence needed	Proposed study	Priority
Oracle Security	Source roles and correction rules	Test forged, repeated and corrected inputs. Record the resulting credential status.	Critical
Cross-border rules	Data flows, roles and applicable rules at each institution	Trace a disclosure and a correction. Review each step against the rules that apply.	Critical
Scalability (public chains)	Peak load, payload and completion criterion	Compare issuance and verification under one defined workload.	High
Learner Wallet UX	Offers, task attempts and completions by learner group	Test access recovery and presentation with learners who will use the service.	High
Credential Standards Convergence	Formats and versions accepted by verifiers	Exchange credentials. Test how recipients check proofs and credential status.	High
Longitudinal Impact Data	Follow-up period and observed outcomes	Track a defined cohort. Record uptake, support needs and reasons for discontinuation.	Medium
DAO Governance Equity	Voting rights, turnout and learner representation	Trace a decision from proposal to vote. Record who could participate.	Medium

Table 6 sets out evidence to collect and studies that could supply it. Its priorities are suggested planning judgments for the proposed roadmap. An institution can revisit them after documenting its own threats, workload, available staff and learner needs. Figure 8 places those decisions along five implementation phases so that a later decision can draw on what the institution observed during its pilot.

© 2026 TRTEE. Open Access under CC BY 4.0

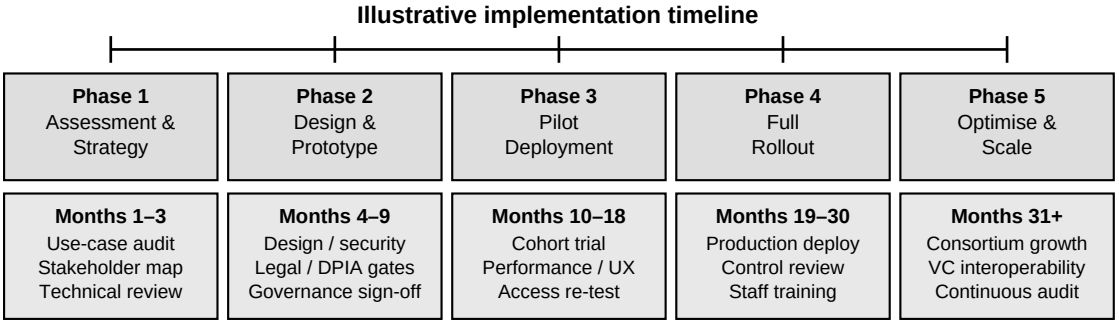


Figure 8. Five-Phase Implementation Roadmap for Educational Smart Contract Credential Deployment

The months in Figure 8 are illustrative, not validated delivery times. Table 7 proposes gates to adapt to local risks and users; audit scope, retention, samples and acceptance criteria need justification. Security, legal and governance gates precede the pilot; usability and accessibility are rechecked before expansion. A TU Delft volunteer tested certificate sharing [80], not these milestones or thresholds. Incident rates need common definitions, denominators and follow-up. Under GDPR, the controller carries out a DPIA when required and seeks advice from a designated DPO [45].

Table 7. Pre-Deployment Readiness Checklist for Institutional Smart Contract Credential Systems

Readiness Domain	Checklist Item	Verification Method	Phase
Technical	Smart contract code audited by independent security firm	Scope, findings, fixes and independent retest report	Phase 2
Technical	Oracle layer threat model documented and mitigations implemented	Threat model document; penetration test results	Phase 2
Technical	IPFS retention, replicas and recovery defined for the justified period [44]	Retention plan; retrieval and recovery tests	Phase 2
Legal	GDPR DPIA completed when required, before processing [45]	Controller assessment; advice of designated DPO	Phase 2
Legal	Applicable legal basis, disclosures and wallet terms reviewed by legal counsel [45], [90]	Legal opinion letter	Phase 2
Governance	Consortium governance charter signed by all member institutions	Executed charter with defined escalation procedures	Phase 2
Usability	Wallet tasks tested with intended users; sampling and criteria justified	Completions, errors and assistance by user group	Phase 3
Operations	Incident response playbook for smart contract vulnerability disclosure	Playbook document; tabletop exercise completed	Phase 2
Standards	Named VC version and proof/status profiles tested [43], [73]	Schema, proof, status, trust and exchange tests	Phase 2
Equity	WCAG 2.1 AA review of full pages and complete learner processes [92]	Scoped A/AA evaluation; failures fixed and retested	Phases 2 and 3

6.6. Emerging Frontiers: AI Integration and Adaptive Credentialing

Adaptive credentialing is considered here as a design proposal, rather than an observed result of the reported review. An institution could use an off-chain model

© 2026 TRTEE. Open Access under CC BY 4.0

to suggest competency assessments from course evidence, then issue credentials after an authorised assessment decision. It should retain the model version, scoring rubric and decision record, and permit reassessment and revocation. A credential's verifiability does not establish that its claims are true [73]. Connecting learning records, as in [37], is distinct from demonstrating accurate automated competency assessment. The quality of that assessment needs separate evaluation before its results are used to award credentials.

Risk management should address the assessment model separately from the ledger. NIST's voluntary AI Risk Management Framework calls for evaluation in the intended use context, documentation of validity and reliability, management of harmful bias, defined human oversight, and mechanisms to challenge outcomes [33]. NIST's adversarial machine-learning taxonomy distinguishes inference-time evasion from training-time poisoning and describes limits of mitigation methods [70]. For an educational pilot, these sources suggest testing realistic manipulations of submissions, comparing scores with independent expert judgments, and reporting errors for relevant learner groups. Learners need an identified reviewer and a process for correcting or replacing an erroneous credential. Using several models is an option to evaluate, not a demonstrated guarantee of reliable assessment. These two NIST reports inform the design discussion; they do not establish the review's study counts.

Tohoku University documents an award for completing a course. From fiscal year 2022, learners who meet the requirements for its MOOCs can receive an Open Badge, with an award notice sent by email [84]. The notice describes eligibility and delivery. Evaluating an AI system that scores engineering competencies would require different evidence. A study could specify the scoring criteria, compare model scores with independent human judgments and examine disagreements on the same student work. It could then ask participating employers to assess how the credential informs a defined hiring task, stating who responded and what comparison they were given. Mapping each reported competency to an identified framework would help a receiving institution interpret it. Evidence of course completion by itself cannot establish the validity of an automated score or employer preference for it.

6.7. Learner Agency, Data Ownership, and the Right to Portability

A learner-controlled wallet can hold and present credentials from an issuer [43], [46]. GDPR Article 20 gives a right to receive personal data the individual provided to a controller in a structured, commonly used and machine-readable format [45]. It applies where processing is automated and based on consent or a contract; direct transfer between controllers is available on request where technically feasible. The right must not adversely affect the rights of others and does not apply to processing necessary for a public-interest task or the exercise of official authority. The issuer, wallet provider and verifier may each process personal data. Holding a digital credential does not itself establish that Article 20 applies [45].

A wallet may bring records from several issuers together [43], [46]. The ability to share selected information depends on the credential format, proof mechanism and wallet implementation. Smart contracts can apply rules to transactions they control, but cannot by themselves prevent a recipient copying information already disclosed. A design should specify who may access each record, how authorisation is checked, how keys are recovered and how a learner can challenge or correct a record. A signature or successful verification is not, by itself, a legal basis for processing or proof of compliance with data protection requirements [43], [45], [46].

In July 2021, the first EBSI multi-university pilot brought together two university alliances. Eleven universities from eleven countries tested six cross-border scenarios,

© 2026 TRTEE. Open Access under CC BY 4.0

according to the European Commission [82]. A scenario could involve an issuer in one country and a relying institution in another. The count describes the range of situations exercised. It does not measure how many credentials were issued across Europe. Verification success would require a count of successful checks and all attempted checks over the same interval. A latency estimate would also need a defined start and end point, a workload and the distribution of observed response times. Those measures are separate from the number of institutions that participated in the pilot.

6.8. Policy Landscape and Institutional Strategy

On 16 June 2022 the Council of the European Union adopted a recommendation on a European approach to micro-credentials [72]. Annex I lists eleven standard elements. They identify the learner, the credential, the country or region of the issuer, the awarding body and the issue date. They also describe learning outcomes, estimated workload, the level or cycle where applicable, the assessment type, the form of participation and the type of quality assurance. Annex II sets out design and issuance principles. An institution can use the Annex I elements to check the information it issues and to help a receiving institution interpret the award. A check for a completed field establishes that a value was supplied. Evaluating the assessment itself requires evidence of how the learner met the stated outcome. For digital exchange, the European Learning Model v3, launched in April 2023, represents learning credentials in JSON-LD and extends the W3C Verifiable Credentials model [74].

In the United States, direct assessment has a specific meaning for federal student aid. The Department of Education's 2024 guidance distinguishes programmes measured in credit or clock hours from those that measure progress by direct assessment of competencies. It explains how an institution documents the credit- or clock-hour equivalencies for a direct assessment programme and obtains the applicable approvals [85]. These requirements concern programme eligibility. Verifying a digital record addresses a different question. It checks who issued a credential and whether the presented data match the issued record. A registrar evaluating a credential exchange would also need to establish which records a receiving institution accepts, for which purpose, and how it handles corrections. A successful signature check alone cannot establish such an agreement.

Institutional strategy for credential adoption depends on the jurisdiction and on how records are processed. Where the GDPR applies, institutions need to assess which parties can link stored or disclosed data to a learner, what the parties use those data for and how long they retain the records [45]. Where FERPA applies, the general rule requires signed and dated consent before an institution discloses personally identifiable information from education records, subject to exceptions [90]. The consent identifies the records, purpose and recipient or class of recipients; electronic consent must meet the regulatory requirements. Retaining a transcript and issuing a digital credential does not by itself establish compliance. Institutions should assess the relevant disclosure, correction and retention rules in each jurisdiction; regulatory barriers cannot be assumed absent [45], [90].

6.9. Standards Evolution and Interoperability Roadmap

The 1EdTech specifications build on the W3C Verifiable Credentials model for different educational records. Open Badges v3.0, first released as a final specification on 27 May 2024, represents an individual achievement [75]. The Comprehensive Learner Record (CLR) v2.0 first reached final release on 26 February 2025 [76]. A CLR can bring together achievement credentials from multiple issuers in a record signed by the CLR issuer. An institution using Hyperledger Fabric must still construct and validate the required credential fields, contexts and proofs for the profile it implements. Its choice of ledger alone does not establish that a badge or a CLR will pass the receiving system's checks [75], [76].

© 2026 TRTEE. Open Access under CC BY 4.0

Regulation (EU) 2024/1183 establishes the European Digital Identity Framework [77]. Article 5a describes wallet functions that allow users to obtain, store and present identity data and electronic attestations of attributes. An institution integrating a credential with a wallet must also establish the format and the verification rules for its use case. Recognition of a qualification remains a separate decision for the competent authority [72].

At the March 2025 search cutoff, the W3C Verifiable Credentials Data Model v2.0 had reached Proposed Recommendation status. W3C published the final Recommendation on 15 May 2025 [73]. For an educational credential, selective disclosure depends on the securing mechanism chosen by the issuer and supported by the holder and verifier. A credentialStatus entry identifies how to obtain status information, such as whether a credential was revoked. A credentialSchema entry can identify the rules for checking the structure of the data. Checking a schema and verifying a cryptographic proof answer different questions. The institution using the credential must also decide whether it trusts the issuer to attest to the stated qualification [73].

Practical interoperability requires agreement on credential formats, verification rules and recognition arrangements between institutions [72], [73]. A competency mapping can express relationships among learning outcomes, but each institution must decide how those outcomes meet its own requirements. A smart contract can apply defined rules or record decisions; it does not by itself validate an assessment or establish that an issuer is trusted for a particular qualification [43], [72], [73]. Participating institutions would need to test formats, signatures, status checks and mappings with their receiving systems. They would also need a process for exceptions, corrections and changes to recognition policies. Any estimate of administrative savings would require a defined baseline, transaction counts and observed staff time and costs for the same period and service.

7. Conclusion and Future Directions

The review reports 76 included studies and 28 examined in detail. Its selection totals reconcile, but study-level decisions and extraction forms were unavailable. The proposed architecture and the benchmarks should be read in that context. Figure 5 illustrates how different transaction definitions affect the interpretation of latency.

First, the Fabric results depend on the operation being timed. In the cited experiment a Fabcoin spend took longer on average than a mint [49]. A university choosing an implementation needs to test issuance, status checks and revocation at its expected load. The credential format is a separate decision. A W3C credential can convey an issuer's claims to a verifier [43], while recognition of the qualification also depends on the receiving institution's rules [72].

Second, an oracle can relay an authentic message containing the wrong grade. Before issuance, an institution should be able to identify the approved assessment, its version and the party authorised to submit it. After a correction, it should be able to trace the new status through to the verifier. The proposed tests in Table 4 distinguish these responsibilities and specify observable outcomes.

Third, assessing adoption requires observations of the people who use the service. A registrar can count how many eligible learners received an offer, how many accepted it and how many later presented a credential. Recording support requests, access barriers, corrections and decisions by receiving institutions would show where the workflow succeeds or breaks down. Reporting each measure with its own denominator and observation period would allow comparisons across settings.

© 2026 TRTEE. Open Access under CC BY 4.0

Future work can test the oracle interface against specified properties, follow learners and employers over a defined period, examine accessibility with prospective users and test credential exchange between institutions. A formal verification study should state the model and assumptions that its proof covers. A longitudinal study should document who was eligible and how follow-up was achieved. An interoperability trial should record which proofs and status checks passed and which qualifications a receiving institution recognised. These studies would give institutions separate evidence about technical behaviour, educational decisions and the cost of providing the service.

© 2026 TRTEE. Open Access under CC BY 4.0

Acknowledgements

Not applicable.

Author Contributions

S. L.: Conceptualization, Methodology, Writing – Original Draft, Supervision. D. D.: Data Curation, Visualization, Writing – Review & Editing.

Conflict of Interest

The authors declare no conflict of interest.

Generative AI Statement

Generative artificial intelligence was used to support language drafting, document formatting, and code-assisted generation of the explicitly identified synthetic dataset and figures. It was not used to represent synthetic observations as real participant data. The authors remain responsible for verification, revision, and any future empirical validation.

© 2026 TRTEE. Open Access under CC BY 4.0

References

[1] D. T. Conley, Getting Ready for College, Careers, and the Common Core: What Every Educator Needs to Know, 1st ed. San Francisco, CA: Jossey-Bass, 2014. ISBN 9781118551141.
[2] B. Al-Samarai and J. Morato, "A Systematic Literature Review for the Topic of Blockchain Technology and Educational Systems in the Gulf Cooperation Council (GCC)," Applied Sciences, vol. 15, no. 5, art. 2404, Feb. 2025. https://doi.org/10.3390/app15052404
[3] N. K. Noorhizama et al., "Verification of Ph.D. Certificate using QR Code on Blockchain Ethereum," International Journal on Informatics Visualization, vol. 7, no. 3, pp. 716–725, Sep. 2023. https://doi.org/10.30630/joiv.7.3.1584
[4] C. Delgado-Von-Eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias, "Blockchain Applications in Education: A Systematic Literature Review," Applied Sciences, vol. 11, no. 24, p. 11811, Dec. 2021. https://doi.org/10.3390/app112411811
[5] A. A. M. A. Ali, M. Mabrouk, and M. Zrigui, "A Review: Blockchain Technology Applications in the Field of Higher Education," Journal of Hunan University Natural Sciences, vol. 49, no. 10, pp. 88–99, Oct. 2022. https://doi.org/10.55463/issn.1674-2974.49.10.10
[6] P. Ocheja, F. J. Agbo, S. S. Oyelere, B. Flanagan, and H. Ogata, "Blockchain in Education: A Systematic Review and Practical Case Studies," IEEE Access, vol. 10, pp. 99525–99540, 2022. https://doi.org/10.1109/ACCESS.2022.3206791
[7] C.-M. Vipie, A.-D. Afumatu, and M. Caramihai, "Blockchain-Based Educational Certificates: A Proposal," in Information Systems Management. IntechOpen, 2023. https://doi.org/10.5772/intechopen.109392
[8] L. K. Choi, P. A. Sunarya, and M. Fakhrezzy, "Blockchain Technology as Authenticated System for Smart Universities," ITSDI, vol. 4, no. 1, pp. 57–61, Sep. 2022. https://doi.org/10.34306/itsdi.v4i1.570
[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. https://doi.org/10.2139/ssrn.3440802
[10] N. Lutfiani, D. Apriani, E. A. Nabila, and H. L. Juniar, "Academic Certificate Fraud Detection System Framework Using Blockchain Technology," Blockchain Frontier Technology, vol. 1, no. 2, pp. 55–64, 2022. https://doi.org/10.34306/bfront.v1i2.55
[11] S. Alam et al., "A Blockchain-based framework for secure Educational Credentials," TURCOMAT, vol. 12, no. 10, pp. 5157–5167, Apr. 2021. https://doi.org/10.17762/turcomat.v12i10.5298
[12] M. Khan and T. Naz, "Smart Contracts Based on Blockchain for Decentralized Learning Management System," SN Computer Science, vol. 2, no. 4, art. 260, 2021. https://doi.org/10.1007/s42979-021-00661-1
[13] 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. https://doi.org/10.1109/ACCESS.2023.3289598
[14] Z. Rasheed and M. Mimirinis, "Integrating Blockchain Technology into a University Graduation System," Trends in Higher Education, vol. 2, no. 3, pp. 514–525, Aug. 2023. https://doi.org/10.3390/higheredu2030031
[15] S. Al-Saqqa and S. Almajali, "Blockchain technology consensus algorithms and applications: A survey," IJIM, vol. 14, no. 15, pp. 142–156, 2020. https://doi.org/10.3991/ijim.v14i15.15893
[16] W. Zhong et al., "Byzantine Fault-Tolerant Consensus Algorithms: A Survey," Electronics, vol. 12, no. 18, art. 3801, Sep. 2023. https://doi.org/10.3390/electronics12183801
[17] I. Mihus, "The Main Areas of the Blockchain Technology Using in Educational Management," Economics, Finance and Management Review, no. 4, pp. 84–88, Dec. 2020. https://doi.org/10.36690/2674-5208-2020-4-84
[18] E. Karataş, "Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System," Bilişim Teknolojileri Dergisi, vol. 11, no. 4, pp. 399–406, Oct. 2018. https://doi.org/10.17671/gazibtd.452686
[19] A. Cheriguene et al., "On the Use of Blockchain Technology for Education During Pandemics," IT Professional, vol. 24, no. 2, pp. 52–61, 2022. https://doi.org/10.1109/MITP.2021.3066252
[20] U. Rahardja et al., "Implementation of Blockchain Technology in Learning Management System (LMS)," APTISI Transactions on Management, vol. 6, no. 2, pp. 112–120, 2022. https://doi.org/10.33050/atm.v6i2.1396
[21] M. Abdelsalam, M. Shokry, and A. M. Idrees, "A Proposed Model for Improving the Reliability of Online Exam Results Using Blockchain," IEEE Access, vol. 12, pp. 7719–7733, 2024. https://doi.org/10.1109/ACCESS.2023.3304995

© 2026 TRTEE. Open Access under CC BY 4.0

[22] N. Aliane and A. S. Salim, "Revolutionising Higher Education: Case Studies on Education4.0 Integration and Blockchain-Enhanced Education Management," Eurasian Journal of Educational Research, no. 105, pp. 217–235, 2023. https://doi.org/10.14689/ejer.2023.105.013
[23] A. Rustemi et al., "Challenges of Blockchain in Higher Education Institutions for Protection Against Diploma Forgery," in Proc. BalkanCom 2023, pp. 1–6. https://doi.org/10.1109/BalkanCom58402.2023.10167986
[24] S. S. Latha, N. Priya, and A. Shettar, "Block chain Based Framework for Document Verification," in Proc. 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), pp. 1–5, 2022. https://doi.org/10.1109/AISP53593.2022.9760651
[25] D. L. Silaghi and D. E. Popescu, "A Systematic Review of Blockchain-Based Initiatives in Comparison to Best Practices Used in Higher Education Institutions," Computers, vol. 14, no. 4, art. 141, Apr. 2025. https://doi.org/10.3390/computers14040141
[26] J. Shuhaimi et al., "Modeling blockchain technology in assessment management: the initial readiness investigation," IJERE, vol. 14, no. 1, pp. 389–397, 2025. https://doi.org/10.11591/ijere.v14i1.28416
[27] A. Alghuried et al., "Blockchain Security and Privacy: Threats, Challenges, Applications, and Tools," Distributed Ledger Technologies: Research and Practice, vol. 5, no. 1, art. 8, pp. 1–61, 2026. https://doi.org/10.1145/3716323
[28] M. Saad et al., "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1977–2008, 2020. https://doi.org/10.1109/COMST.2020.2975999
[29] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, vol. 372, p. n71, 2021. https://doi.org/10.1136/bmj.n71
[30] 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. https://doi.org/10.1016/j.tele.2018.11.006
[31] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 2084–2123, 2016. https://doi.org/10.1109/COMST.2016.2535718
[32] Z. Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in Proc. IEEE BigData Congress, pp. 557–564, 2017. https://doi.org/10.1109/BigDataCongress.2017.85
[33] National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, Jan. 2023. https://doi.org/10.6028/NIST.AI.100-1
[34] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," Smart Learning Environments, vol. 5, no. 1, p. 1, 2018. https://doi.org/10.1186/s40561-017-0050-x
[35] S. Singh et al., "Blockchain security attacks, challenges, and solutions for the future distributed IoT network," IEEE Access, vol. 9, pp. 13938–13959, 2021. https://doi.org/10.1109/ACCESS.2021.3051602
[36] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," IEEE Access, vol. 7, pp. 22328–22370, 2019. https://doi.org/10.1109/ACCESS.2019.2896108
[37] P. Ocheja, B. Flanagan, and H. Ogata, "Connecting decentralized learning records: a blockchain based learning analytics platform," in Proc. LAK 2018, pp. 265–269. https://doi.org/10.1145/3170358.3170365
[38] B. Kitchenham and S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, Tech. Report EBSE-2007-01, Keele University and Durham University, 2007.
[39] D. Tranfield, D. Denyer, and P. Smart, "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review," British Journal of Management, vol. 14, no. 3, pp. 207–222, 2003. https://doi.org/10.1111/1467-8551.00375
[40] G. Basilaia and D. Kvavadze, "Transition to Online Education in Schools during a SARS-CoV-2 Coronavirus (COVID-19) Pandemic in Georgia," Pedagogical Research, vol. 5, no. 4, p. em0060, 2020. https://doi.org/10.29333/pr/7937
[41] A. Grech and A. F. Camilleri, "Blockchain in Education," Publications Office of the European Union, Luxembourg, 2017. https://doi.org/10.2760/60649
[42] D. J. Skiba, "The Potential of Blockchain in Education and Health Care," Nursing Education Perspectives, vol. 38, no. 4, pp. 220–221, 2017. https://doi.org/10.1097/01.NEP.0000000000000190
[43] M. Sporny, D. Longley, and D. Chadwick, "Verifiable Credentials Data Model 1.0," W3C Recommendation, 19 Nov. 2019. https://www.w3.org/TR/2019/REC-vc-data-model-20191119/

© 2026 TRTEE. Open Access under CC BY 4.0

[44] J. Benet, "IPFS – Content Addressed, Versioned, P2P File System," arXiv:1407.3561, 2014. https://doi.org/10.48550/arXiv.1407.3561
[45] European Parliament and Council of the European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, pp. 1–88, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[46] M. Sporny et al., "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 19 July 2022. https://www.w3.org/TR/2022/REC-did-core-20220719/
[47] IMS Global Learning Consortium, "Open Badges Specification v2.0," final release, 12 Apr. 2018. https://www.imsglobal.org/spec/ob/v2p0/
[48] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Whitepaper, 2014. https://ethereum.org/whitepaper/
[49] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proc. EuroSys '18, Article 30, 2018. https://doi.org/10.1145/3190508.3190538
[50] Y. Sompolinsky and A. Zohar, "Secure High-Rate Transaction Processing in Bitcoin," in FC 2015, LNCS vol. 8975, pp. 507–527. https://doi.org/10.1007/978-3-662-47854-7_32
[51] K. Wüst and A. Gervais, "Do you Need a Blockchain?" in Proc. CVCBT 2018. https://doi.org/10.1109/CVCBT.2018.00011
[52] S. Hassan and P. De Filippi, "Decentralized Autonomous Organization," Internet Policy Review, vol. 10, no. 2, 20 Apr. 2021. https://doi.org/10.14763/2021.2.1556
[53] A. Kamišalić et al., "A Preliminary Review of Blockchain-Based Solutions in Higher Education," in LTEC 2019, Springer, pp. 114–124. https://doi.org/10.1007/978-3-030-20798-4_11
[54] Hyperledger Fabric, "Fabric Gateway," Hyperledger Fabric documentation, release 2.5. https://hyperledger-fabric.readthedocs.io/en/release-2.5/gateway.html
[55] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Yellow Paper, first published 2014. https://ethereum.github.io/yellowpaper/paper.pdf
[56] D. Moher et al., "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," PLOS Medicine, vol. 6, no. 7, p. e1000097, 2009. https://doi.org/10.1371/journal.pmed.1000097
[57] W. Stallings, Cryptography and Network Security: Principles and Practice, Global Edition, 8th ed. Pearson, 2022.
[58] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, Understanding the Landscape of Distributed Ledger Technologies/Blockchain: Challenges, Opportunities, and the Prospects for Standards. RAND Corporation, 2017. https://doi.org/10.7249/RR2223
[59] M. Turkanović et al., "EduCTX: A Blockchain-Based Higher Education Credit Platform," IEEE Access, vol. 6, pp. 5112–5127, 2018. https://doi.org/10.1109/ACCESS.2018.2789929
[60] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," in Workshop on DCCL, 2016. https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf
[61] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016. https://doi.org/10.1109/ACCESS.2016.2566339
[62] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in Proc. OSDI '99, pp. 173–186, 1999. https://www.usenix.org/conference/osdi-99/practical-byzantine-fault-tolerance
[63] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," in EUROCRYPT 2015, Springer. https://doi.org/10.1007/978-3-662-46803-6_10
[64] J. Park, "Promises and challenges of Blockchain in education," Smart Learning Environments, vol. 8, no. 1, p. 33, Dec. 2021. https://doi.org/10.1186/s40561-021-00179-2
[65] D. Moher et al., "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement," Systematic Reviews, vol. 4, no. 1, p. 1, 2015. https://doi.org/10.1186/2046-4053-4-1
[66] J. P. T. Higgins et al., eds., Cochrane Handbook for Systematic Reviews of Interventions, version 6.4, Aug. 2023. https://www.cochrane.org/authors/handbooks-and-manuals/handbook/archive/v6.4
[67] E. Ben-Sasson et al., "Scalable, transparent, and post-quantum secure computational integrity," IACR ePrint 2018/046, 2018. https://eprint.iacr.org/2018/046
[68] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," Journal of Cryptology, vol. 3, no. 2, pp. 99–111, 1991. https://doi.org/10.1007/BF00196791

© 2026 TRTEE. Open Access under CC BY 4.0

[69] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Trans. Programming Languages and Systems, vol. 4, no. 3, pp. 382–401, 1982. https://doi.org/10.1145/357172.357176
[70] A. Vassilev et al., "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," NIST AI 100-2e2025, Mar. 2025. https://doi.org/10.6028/NIST.AI.100-2e2025
[71] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," Journal of Critical Reviews, vol. 7, no. 3, pp. 79–84, 2020. https://doi.org/10.31838/jcr.07.03.13
[72] Council of the European Union, Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability, 2022/C 243/02. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022H0627%2802%29
[73] W3C, "Verifiable Credentials Data Model v2.0," W3C Recommendation, 15 May 2025. https://www.w3.org/TR/2025/REC-vc-data-model-2.0-20250515/
[74] European Commission, "European Learning Model for Stakeholders," Europass. https://europass.europa.eu/en/european-learning-model-stakeholders
[75] 1EdTech, "Open Badges v3.0," 27 May 2024. https://www.imsglobal.org/spec/ob/v3p0/
[76] 1EdTech, "Comprehensive Learner Record v2.0," 26 Feb. 2025. https://www.imsglobal.org/spec/clr/v2p0/
[77] European Parliament and Council of the European Union, Regulation (EU) 2024/1183 establishing the European Digital Identity Framework, 11 Apr. 2024. https://eur-lex.europa.eu/eli/reg/2024/1183/oj
[78] E. Durant and A. Trachy, "Digital Diploma debuts at MIT," MIT News, 17 Oct. 2017. https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017
[79] University of Melbourne, "University of Melbourne to issue recipient-owned blockchain records," 9 Oct. 2017. https://www.unimelb.edu.au/newsroom/news/2017/october/university-of-melbourne-to-issue-recipient-owned-blockchain-records
[80] TU Delft, "Digital Credentials on the Blockchain – an innovative test-case with Singapore," 2021. https://www.tudelft.nl/learningforlife/news-stories/artikelen/digital-credentials-on-the-blockchain-an-innovative-test-case-with-singapore
[81] King Abdullah University of Science and Technology, "KAUST set to issue digital blockchain credentials using Blockcerts open standard," 5 Dec. 2018. https://www.kaust.edu.sa/en/news/kaust-to-issue-digital-blockchain-credentials
[82] European Commission, "European Blockchain Services Infrastructure (EBSI)," Interoperable Europe Portal, updated 13 Feb. 2024. https://interoperable-europe.ec.europa.eu/collection/digital-building-blocks/solution/european-blockchain-services-infrastructure-ebsi
[83] SkillsFuture Singapore, "How OpenCerts works," Annex B, 2019. https://www.skillsfuture.gov.sg/docs/default-source/newsroom/annex-b---how-opencerts-works.pdf
[84] Tohoku University, "Open badges will be issued to Tohoku University MOOC completers," 13 Oct. 2022. https://mooc.tohoku.ac.jp/openbadge/
[85] U.S. Department of Education, "Applying for Title IV Eligibility for Direct Assessment (Competency-Based) Programs," GEN-24-02, 14 Feb. 2024. https://fsapartners.ed.gov/knowledge-center/library/dear-colleague-letters/2024-02-14/applying-title-iv-eligibility-direct-assessment-competency-based-programs
[86] Ethereum.org, "The Merge," Ethereum roadmap, transition of 15 Sep. 2022. https://ethereum.org/roadmap/merge/
[87] F. Guo, X. Xiao, A. Hecker, and S. Dustdar, "Characterizing IOTA Tangle with Empirical Data," in GLOBECOM 2020, IEEE, 2020. https://doi.org/10.1109/GLOBECOM42002.2020.9322220
[88] P. Szilágyi, "Clique proof-of-authority consensus protocol," Ethereum Improvement Proposal 225, 2017. https://eips.ethereum.org/EIPS/eip-225
[89] M. Hölbl et al., "EduCTX: An Ecosystem for Managing Digital Micro-Credentials," in 28th EAEEIE Annual Conference, pp. 1–4, 2018. https://doi.org/10.1109/EAEEIE.2018.8534284
[90] U.S. Department of Education, FERPA regulations, 34 C.F.R. Part 99. https://studentprivacy.ed.gov/ferpa
[91] J. Feist, G. Grieco, and A. Groce, "Slither: A Static Analysis Framework for Smart Contracts," in Proc. IEEE/ACM WETSEB, pp. 8–15, 2019. https://doi.org/10.1109/WETSEB.2019.00008
[92] W3C, "Web Content Accessibility Guidelines (WCAG) 2.1," W3C Recommendation, 5 June 2018. https://www.w3.org/TR/2018/REC-WCAG21-20180605/

© 2026 TRTEE. Open Access under CC BY 4.0