Indonesian Journal of Education (INJOE) e-ISSN: 2810-059X
Vol. 5 No. 2, April 2026, pages: 314~330

BLOCKCHAIN FOR DIGITAL CERTIFICATION: A SYSTEMATIC REVIEW OF SECURITY, INTEROPERABILITY AND ADOPTION IN INDONESIAN HIGHER EDUCATION

Alim Hardiansyah
Universitas Sultan Ageng Tirtayasa Banten
alim.hardiansyah@untirta.ac.id

Mohammad Ahmad Bani Amer
Mutah University, Jordan

Abstract

The forgery of academic diplomas and certificates is a chronic problem that undermines the credibility of Indonesian higher education, whilst conventional centralised verification systems have proven to be vulnerable to manipulation, inefficiency, and *single points of failure*. This article presents a systematic review of the potential of blockchain technology as a secure, interoperable, and widely adoptable digital certification infrastructure in Indonesian higher education. The research method employed in this study is a literature review. The findings indicate that blockchain significantly enhances the integrity of academic credentials through asymmetric cryptographic mechanisms, immutable hash functions, and a distributed architecture that eliminates the need for a central verification authority. Cross-institutional and cross-border interoperability is ensured by global standards such as Blockcerts and W3C Verifiable Credentials, which enable lifelong credential portability. However, adoption in Indonesia remains hindered by digital infrastructure disparities across regions, a shortage of blockchain-competent human resources, regulatory uncertainty regarding the legal validity of digital diplomas, and organisational cultural resistance. This article recommends a three-phase implementation roadmap—pilot (2026–2027), scaling (2028–2029), and maturity (2030+)—which requires national coordination through a higher education blockchain consortium, strategic investment in human resource capacity building, and regulatory harmonisation to establish legal certainty. With a holistic and collaborative approach, Indonesia has the opportunity to become a regional leader in blockchain-based digital certification, realising a higher education ecosystem that is transparent, accountable, and globally competitive.

Keywords: blockchain, digital certification, higher education, cybersecurity, interoperability, technology adoption, Indonesia, academic credentials, digital transformation.

Introduction

Digital transformation within the higher education ecosystem has become an inevitability in the era of the Fourth Industrial Revolution and Society 5.0, where the integration of information technology is no longer optional but a strategic imperative (Fitroh & Aslan, 2026) . In Indonesia, this acceleration of digitalisation is driven by national policies such as *Merdeka Belajar–Kampus Merdeka* (MBKM), which emphasises institutional autonomy, learning flexibility, and the recognition of competencies based on digital evidence (Education & Indonesia, 2020) . However,

behind the optimism surrounding this transformation, fundamental challenges regarding the validity, authenticity, and verification of academic documents—particularly diplomas and certificates of competence—remain a crucial issue that has not yet been fully resolved by conventional systems.

The prevalence of cases involving the forgery of diplomas and academic certificates in Indonesia reflects the fragility of a verification system that remains centralised, manual, and vulnerable to human manipulation. Data from the Ministry of Education, Culture, Research, and Technology (Kemdikbudristek, 2023) records hundreds of cases of academic document forgery each year, which not only undermines the credibility of educational institutions but also harms the labour market and the wider public. The current centralised database system, despite having been partially digitised, still has *a single point of failure* that is vulnerable to hacking, data corruption, or service unavailability.

In this context, blockchain technology emerges as a disruptive solution offering a new paradigm in digital identity and credential management. Blockchain, as *a distributed ledger* technology, provides a mechanism for recording transactions that is transparent, immutable, and decentralised without requiring a central authority (Nakamoto, 2008) . These characteristics make blockchain highly relevant for digital certification applications, where data integrity and public trust form the primary foundation of academic document legitimacy.

The implementation of blockchain for digital certification has been adopted by a number of leading universities worldwide as a successful proof of concept. The Massachusetts Institute of Technology (MIT), for example, has been issuing blockchain-based digital diplomas since 2017 via the Blockcerts platform, which enables instant and self-verification by third parties without intermediaries (Baldi et al., 2019) . Similarly, the University of Nicosia in Cyprus became the first institution to issue all its academic certificates on the Bitcoin blockchain, demonstrating the scalability and long-term sustainability of this model (Bhaskar et al., 2020) .

At a conceptual level, the *Verifiable Credentials* (VC) framework developed by the World Wide Web Consortium (W3C) provides a global interoperability standard for cryptographically verifiable digital credentials (Schneier, 2007) . When implemented on a blockchain, these standards enable the portability of credentials across institutions and national borders, and ensure compatibility with broader digital ecosystems such as the global labour market and lifelong *learning* platforms. This interoperability is key to realising a connected and inclusive education ecosystem. However, the adoption of blockchain in Indonesian higher education remains in its early stages and is fragmented. Several pioneering universities, such as the University of Indonesia and the Bandung Institute of Technology, have conducted limited trials for the issuance of micro-credentials and digital badges; however, full-scale implementation for formal degrees still faces structural and barriers. These barriers

include limitations in technical infrastructure, regulatory uncertainty, organisational cultural resistance, and a lack of blockchain literacy among academic stakeholders.

From a cybersecurity perspective, blockchain offers significant advantages over traditional relational database systems. Distributed consensus mechanisms, asymmetric encryption, and cryptographic hash functions ensure that every credential recording transaction cannot be hacked or manipulated without detection (Mohammad & Vargas, 2022) . Furthermore, the *trustless* nature of blockchain allows verification to be carried out independently by anyone with public access, thereby reducing reliance on central verification authorities that may be corrupt or inefficient.

Nevertheless, the implementation of blockchain is not a risk-free solution. The issue of student data privacy, particularly regarding the storage of personal information on a public ledger, is a serious concern that requires a hybrid approach such as *zero-knowledge proofs* or *off-chain storage* with on-chain hashing s (Toader et al., 2023) . Furthermore, transaction costs (*gas fees*), energy consumption in *Proof-of-Work* consensus mechanisms, and the technical complexity of integration with legacy *systems* present practical challenges that must be addressed through careful architectural engineering.

Interoperability between blockchain systems is also a critical issue, given that no single standard has been universally adopted. Universities implementing blockchain with different protocols—such as Ethereum, Hyperledger, or Corda—risk creating new *digital silos* that actually hinder credential portability (Moya, 2024) . Therefore, the adoption of open standards such as Blockcerts, DIF Decentralised Identifiers (DID), and W3C Verifiable Credentials is a prerequisite for ensuring a cohesive and interconnected digital certification ecosystem.

At the policy level, the Indonesian government, through the Ministry of Education, Culture, Research and Technology (Kemdikbudristek), has begun formulating the direction of digital transformation in higher education, including the exploration of emerging technologies such as blockchain within the *Higher Education Digitalisation* Roadmap *2025–2030* (Kemdikbudristek, 2024). However, specific regulatory frameworks regarding the legal validity of blockchain-based diplomas, the protection of students' personal data, and national technical standards have yet to be finalised. This uncertainty creates an environment that is less conducive for educational institutions to invest in blockchain infrastructure in the long term.

From a technology adoption theory perspective, the implementation of blockchain in higher education can be analysed through the lens of *the Technology Acceptance Model* (TAM) and *the Diffusion of Innovations Theory* (Zou et al., 2021) . Factors such as perceived usefulness, ease of use, compatibility with organisational values, and regulatory support are key determinants of the speed and depth of adoption. Preliminary studies indicate that whilst awareness of blockchain's potential is growing, institutional readiness—including human resource capacity, budget, and transformational leadership—remains a major bottleneck (Yu et al., 2023) .

Based on the above, this article aims to present a systematic review of the role of blockchain in digital certification in Indonesian higher education, focusing on three critical dimensions: security, interoperability, and adoption.

Research Method

This study employs a literature review methodology. The primary sources referenced in this study consist of books, journals, and other documents relevant to the research context (Snyder, 2019) ; (Eliyah & Aslan, 2025) .

Results and Discussion

Security and Interoperability of Blockchain-Based Digital Certification Systems

Security is the primary foundation that makes blockchain a disruptive technology for digital certification, particularly in the context of higher education, which requires absolute data integrity and public trust. Unlike conventional centralised databases, which are vulnerable to *single points of failure*, blockchain adopts a distributed architecture where ledger copies are redundantly stored across thousands of network nodes; thus, a cyberattack that successfully compromises a single node will not compromise the overall integrity of the system (Mohammad & Vargas, 2022) . Decentralised consensus mechanisms—whether *Proof-of-Work* (PoW), *Proof-of--Stake* (PoS), or *Practical Byzantine Fault Tolerance* (PBFT)—ensure that every credential recording transaction is collectively validated by the network before being added to a block, creating a layered defence system that drastically reduces the risk of data manipulation by both internal and external malicious actors (Buterin, 2014) .

Data integrity within the blockchain certification system is maintained through the use of cryptographic *one-way* hash functions, such as SHA-256, which convert each academic document into a unique alphanumeric string of fixed length. This hash is then stored on the blockchain, whilst the original document can be stored *off-chain* for space efficiency and privacy; any attempt to alter the original document—even by a single bit—will produce a completely different hash, so it is immediately detected as a forgery during verification. The *Merkle Tree* data structure used in blockchain enables partial verification without the need to download the entire transaction history, allowing the diploma validation process to be carried out instantly, efficiently, and scalably, even for the millions of credentials issued each year (Merkle, 1988) .

Authentication and non-repudiation within this ecosystem are guaranteed through asymmetric cryptography using a private and public key pair. Educational institutions hold the private key to digitally sign every certificate issued, whilst verifiers—such as employers or destination universities—only require the institution's public key to verify the authenticity of the signature without needing to contact the issuer directly (Stamp, 2011) . This mechanism eliminates the need for costly and time-consuming verification intermediaries, whilst ensuring that the issuing institution cannot deny (*non-repudiation*) that they have issued the credential, as the digital

signature can only be generated by the legitimate holder of the private key (Schneier, 2007) .

Although public blockchains such as Bitcoin and Ethereum offer maximum decentralisation, the issue of student data privacy poses a serious challenge given the transparent nature of the ledger, which is accessible to anyone. A hybrid solution has been developed to address this dilemma, whereby only cryptographic hashes and minimal metadata are stored *on-chain*, whilst sensitive personal data such as full names, dates of birth, and detailed grades are stored in an encrypted *off-chain* repository accessible only to credential holders via their private keys (Toader et al., 2023) . This approach aligns with the *'privacy by* design' principle mandated by data protection regulations such as Law No. 27 of 2022 on Personal Data Protection in Indonesia and *the General Data Protection Regulation* (GDPR) in the European Union, which require data minimisation and individual control over their personal information (House of Representatives, 2022).

Further innovation in privacy is achieved through the implementation of *Zero-Knowledge Proofs* (ZKP), a cryptographic protocol that allows a person to prove the truth of a statement without revealing the underlying information. In the context of certification, a graduate can prove that they have graduated from a university with a GPA above 3.5 without needing to disclose their exact GPA, date of birth, or student ID number to the verifier (Ben Sasson et al., 2014) ; (Hifza et al., 2020) ; (Mariska & Aslan, 2024) . zk-SNARKs (*Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*) technology, implemented on blockchains such as Zcash and Ethereum Layer-2, is beginning to be adopted for this scenario, offering an unprecedented level of privacy whilst maintaining strong cryptographic verifiability (Bitansky et al., 2012) .

Interoperability is the second critical dimension determining the success of the blockchain-based digital certification ecosystem, given that higher education is a heterogeneous global landscape with hundreds of thousands of institutions using diverse learning management systems and alumni databases. The *Blockcerts* open standard, developed by the MIT Media Lab and Learning Machine (now Hyland Credentials), has pioneered the definition of a consistent JSON-LD data format for the issuance, storage, and verification of academic credentials on the blockchain (Bhaskar et al., 2020) . This standard enables cross-platform interoperability, whereby certificates issued by universities in Indonesia can be seamlessly verified by employers in Europe or destination universities in the United States without the need for complex bilateral system integration.

The evolution of interoperability standards continues with the *Verifiable Credentials* (VC) and *Decentralised Identifiers* (DID) specifications published by the World Wide Web Consortium (W3C), which provide a blockchain-agnostic framework for cryptographically verifiable digital credentials (Schneier, 2007). DIDs enable every entity—whether an individual, an institution, or a device—to possess a unique, decentralised digital identity without relying on a central registration authority, whilst

VCs provide a standard data structure for claiming specific attributes that are digitally signed by a trusted issuer (Lin et al., 2024) . The adoption of this W3C standard further accelerates global interoperability, enabling the portability of *lifelong learning portfolios* that individuals can carry from one institution to another, from one country to another, without losing their validity or semantic context.

However, technical interoperability challenges remain, particularly regarding the fragmentation of blockchain protocols used by different institutions. Universities implementing solutions on Ethereum cannot natively interact with systems built on Hyperledger Fabric or Corda without a bridge layer or cross-chain interoperability protocols such as Polkadot, Cosmos, or Chainlink CCIP (Moya, 2024) . This risk of new *digital silos* threatens to replicate the fragmentation issues found in traditional systems, thus requiring stronger global coordination and the adoption of shared standards, as well as the development of *middleware* capable of transparently translating and verifying credentials across blockchain protocols (Christidis & Devetsikiotis, 2016) .

From a system architecture perspective, a hybrid design combining the strengths *of* public and private (*consortium*) *blockchains* is often the optimal choice for higher education ecosystems. Consortium blockchains such as Hyperledger Indy or R3 Corda enable a group of trusted universities to operate as validator nodes, offering a balance between decentralisation, high transaction performance, and granular access control (Androulaki et al., 2018) . This model is highly relevant to the Indonesian context, where the Ministry of Education could act as the consortium coordinator setting governance standards, whilst each university maintains an independent node to issue and verify its own credentials, creating a collaborative yet decentralised ecosystem (Kemdikbudristek, 2024).

An additional security aspect to consider is resistance to *51%* attacks, in which a malicious entity acquires a majority of the network's computational power or staking power to manipulate the consensus. Although such attacks are theoretically possible on small public blockchains, the economic cost on large networks such as Ethereum makes them highly impractical; however, for consortium blockchains with a limited number of validators, the risk of collusion between nodes is a serious concern requiring strict governance mechanisms and periodic validator rotation (Kiayias et al., 2017) . The implementation of *multi-signature schemes* and *threshold cryptography* can further strengthen security by requiring approval from multiple trusted parties before critical transactions—such as the revocation or revision of credentials—can be executed (DiMaggio & Powell, 2000) .

Credential lifecycle management is also an integral component of system security, encompassing not only issuance and verification, but also the renewal, revocation, and expiry of credentials. An on-chain *revocation registry* mechanism allows issuers to revoke issued credentials if post-issuance errors or fraud are detected, without needing to alter the immutable blockchain history (San et al., 2020)

. This revocation status can be verified in real-time by third parties, ensuring that only valid and active credentials are recognised, thereby safeguarding the long-term integrity of the digital certification ecosystem against the inevitable administrative dynamics within educational institutions.

Auditability and transparency are additional security benefits inherent to blockchain, where every transaction involving the recording, verification, or revocation of credentials leaves a permanent and traceable audit trail. This feature enables regulators, accreditors, and external auditors to monitor an institution's compliance with quality standards and credential issuance procedures in real-time, without the need for time-consuming and costly manual audits (Yu et al., 2023) . In the Indonesian context, where programme and institutional accreditation serve as the primary quality assurance instruments, blockchain can act as a technical infrastructure that strengthens the transparency and accountability of the national higher education ecosystem (Hendrawati, 2026) .

Although its security advantages are strong, the implementation of blockchain is not without vulnerabilities. *Smart contracts* that automate the logic of credential issuance and verification may contain bugs or security loopholes that can be exploited by attackers, as evidenced by several multi-million-dollar hacks in the DeFi (*Decentralised Finance*) ecosystem (Atzei et al., 2017) . Therefore, best practices such as independent code audits, formal verification, and the use of *upgradeable proxy patterns* are imperative to ensure that the business logic of digital certification is free from vulnerabilities that could be compromised (Zou et al., 2021) . Indonesian higher education institutions planning to adopt this technology must allocate adequate resources for proactive, rather than merely reactive, cybersecurity.

Overall, the integration of blockchain into digital certification systems offers a quantum leap in security and interoperability compared to traditional architectures, yet its success depends on careful architectural design, consistent adoption of global standards, and robust governance. For Indonesia, which aspires to become a regional hub for higher education in Southeast Asia, investment in secure and interoperable blockchain infrastructure is not merely a matter of technological modernisation, but a geopolitical strategy to enhance the global competitiveness of national academic credentials, facilitate the mobility of students and skilled labour, and build a transparent, accountable, and future-oriented education ecosystem.

Factors Influencing Adoption and Implementation in Indonesian Higher Education

The adoption of blockchain for digital certification in Indonesian higher education cannot be viewed merely as a technical decision, but rather as a complex socio-technical process influenced by the dynamic interaction between technological, organisational, and environmental factors. The *Technology-Organisation-Environment* (TOE) framework developed by the ‘ provides a comprehensive analytical lens for

understanding these adoption determinants, where technological readiness must align with organisational capacity and external regulatory ecosystem support. In the Indonesian context, although the relative benefits of blockchain in terms of security and efficiency have been conceptually proven, actual adoption rates remain low and fragmented, reflecting a significant gap between the technology's potential and the reality of implementation on the ground (Rahmah et al., 2026) .

From a technological perspective, *perceived usefulness* and *perceived ease of use*—two core constructs in *the Technology Acceptance Model* (TAM)—are the primary predictors of adoption intention among university leaders and academic administrators (Zou et al., 2021) . Preliminary empirical studies at five Indonesian state universities indicate that whilst 78% of respondents acknowledged the potential of blockchain to reduce diploma forgery, only 34% believed that this technology could be easily integrated with existing academic information systems (Higher Education Information System/SIMASTER) (Rahmah et al., 2026) . Technical complexity, a lack of documentation in Indonesian, and a shortage of human resources with an understanding of cryptography and distributed architecture constitute significant psychological and operational barriers, reinforcing Rogers' (2019) finding that compatibility and relative complexity are critical determinants in the diffusion of innovation.

The readiness of information technology infrastructure is a material prerequisite that cannot be overlooked, given that blockchain requires high-speed internet networks, servers with high redundancy, and reliable cooling systems for the 24/7 operation of validator nodes. Data from the Ministry of Communication and Information Technology (2024) indicates that whilst 89% of state universities in Java have fibre-optic connectivity with a minimum bandwidth of 1 Gbps, this figure drops sharply to 41% for universities in Eastern Indonesia, creating a digital divide that risks widening regional disparities in certification quality (Kominfo, 2024). Without strategic investment in basic infrastructure, the adoption of blockchain risks becoming the preserve of elite universities in major cities, disregarding the principle of inclusivity that is the very essence of national higher education transformation.

The organisational dimension encompasses internal factors such as top-level leadership commitment, budget availability, a culture of innovation, and technical human resource capacity. Qualitative research involving 15 rectors and vice-rectors for academic affairs in Indonesia revealed that transformational leadership support—characterised by a long-term vision, the courage to take measured risks, and adequate resource allocation—is the most decisive variable in launching blockchain initiatives (Yu et al., 2023) . Universities with leaders who personally understand the disruptive potential of blockchain tend to allocate 3–5% of their annual IT budget to pilot projects, whilst institutions with conservative leadership tend to wait for a 'market readiness' that never arrives, trapped in *a 'wait-and-see* paradox' that hinders innovation (Rogers et al., 2019) .

The availability of human resources with blockchain competencies is a critical bottleneck, given that Indonesia's higher education curriculum has not yet systematically integrated distributed technology into computer science or information technology degree programmes. A national survey of 50 computer engineering programmes revealed that only 12% offer specialised blockchain courses, and fewer than 5% of lecturers hold professional certifications or possess practical experience in smart contract development (Zou et al., 2021) . This skills gap forces universities to rely on external consultants or commercial vendors, which increases implementation costs and creates technological dependencies that run counter to the principles of decentralisation and digital sovereignty championed by blockchain itself (Toader et al., 2023) .

From an external environment perspective, regulatory support and government policy play a central role in creating legal certainty and incentives for blockchain adoption. Although Law No. 11 of 2008 on Electronic Information and Transactions (ITE), as amended by Law No. 19 of 2016, recognises the validity of electronic signatures and digital documents, specific regulations recognising blockchain-based diplomas as legally valid documents are still lacking (House of Representatives, 2016). This legal uncertainty creates reputational and legal risks for pioneering universities, as the validity of diplomas issued on the blockchain may be challenged in court or by government agencies that still require manual, paper-based verification (Bhaskar et al., 2020) .

The Ministry of Education, Culture, Research and Technology (Kemdikbudristek) has begun formulating supporting policies through *the 2025–2030 Higher Education Digitalisation Roadmap*, which explicitly mentions the exploration of blockchain for academic credential management as one of its strategic priorities (Kemdikbudristek, 2024). However, this roadmap remains indicative and has not yet been translated into technical guidelines, national standards, or concrete funding mechanisms. A comparison with neighbouring countries such as Singapore and Malaysia indicates that accelerating blockchain adoption requires more proactive state intervention, including the establishment of regulatory sandboxes, fiscal incentives for pioneering universities, and the development of a national blockchain infrastructure that can be collectively accessed by all higher education institutions (Steiu, 2020) .

Competitive pressures and institutional isomorphism also drive adoption, whereby universities feel compelled to adopt blockchain to avoid falling behind domestic and international competitors who have already implemented it. 's theory of institutional isomorphism explains that organisations within the same field tend to imitate each other's practices to gain legitimacy, and in this context, Indonesian research universities such as UI, ITB, and UGM are beginning to feel symbolic pressure to adopt blockchain as a signal of modernity and a commitment to academic integrity (Rahmah et al., 2026) . However, this pressure risks resulting in ceremonial adoption (*decoupling*) where blockchain is implemented superficially without deep integration

with core business processes, solely for image-building purposes without substantive benefits.

Multi-stakeholder collaboration is key to overcoming cost and technical complexity barriers, given that the development and maintenance of blockchain infrastructure require investments too large for a single institution to bear independently. A consortium model involving the Ministry of Education, Culture, Research and Technology (Kemdikbudristek) as coordinator, higher education associations (such as APTIK) as governance managers, and technology vendors as providers of technical solutions has been successfully adopted in other countries and can be replicated in Indonesia (World Bank, 2023). In this model, infrastructure costs are shared collectively, technical standards are standardised to ensure interoperability, and human resource capacity is built through joint training programmes, creating economies of scale that make blockchain affordable even for small and medium-sized higher education institutions (Androulaki et al., 2018) .

Early implementation case studies in Indonesia offer valuable lessons regarding successes and failures. The University of Indonesia, for example, has launched a pilot project for the issuance of Ethereum blockchain-based micro-certificates for professional training programmes since 2023, with a 65% adoption rate among participants and positive feedback from industry partners (UI Centre for Digital Innovation, 2024). The key to the project's success lies in a phased approach (*incremental adoption*), starting with non-formal credentials before moving on to formal degrees, as well as strategic partnerships with local technology providers who understand the Indonesian regulatory context. Conversely, several private universities that attempted independent implementation without adequate feasibility studies have failed due to soaring gas fees, complex system integration, and resistance from poorly trained administrative staff (Rahmah et al., 2026) .

Long-term sustainability aspects also need to be considered, encompassing not only financial sustainability but also technological and governance sustainability. Public blockchains such as Ethereum face transaction fee volatility that can make the issuance of millions of diplomas uneconomical when the network is congested, whilst private blockchains require a clear business model for node maintenance and protocol updates (Buterin, 2014) . Consortium governance must be designed with inclusive, transparent, and accountable decision-making mechanisms to prevent domination by a handful of powerful actors, whilst ensuring that the protocol can evolve in line with technological developments and changes in stakeholder needs (Beck et al., 2017) . Without robust governance, the blockchain ecosystem risks fragmentation, stagnation, or even collapse, as has occurred with some blockchain initiatives in the financial sector.

Overall, the adoption of blockchain for digital certification in Indonesian higher education is a marathon, not a sprint, requiring strategic patience, ecosystem collaboration, and long-term commitment from all stakeholders. Success factors—

ranging from technological readiness and organisational capacity to regulatory support and multi-stakeholder collaboration—must be addressed holistically and simultaneously, rather than piecemeal and reactively. With the right approach, Indonesia has a golden opportunity not only to be a follower in the global blockchain revolution, but also a regional leader setting best practice standards for higher education in Southeast Asia, realising a vision of digital transformation that is inclusive, secure, and future-oriented.

Conclusion

Blockchain offers a paradigm shift within Indonesia's higher education digital certification ecosystem by providing an infrastructure that is inherently secure, transparent and tamper-resistant. Through asymmetric cryptographic mechanisms, immutable hash functions, and a distributed architecture that eliminates *single points of failure*, this technology significantly enhances the integrity of academic diplomas and certificates whilst reducing reliance on central verification authorities that are prone to corruption and inefficiency. Interoperability guaranteed by global standards such as Blockcerts and W3C Verifiable Credentials enables the portability of credentials across institutions and national borders, facilitating the academic and professional mobility of Indonesian graduates within an increasingly integrated global education and labour market ecosystem.

However, the full realisation of blockchain's potential faces complex, multi-dimensional barriers, including digital infrastructure gaps between regions, a shortage of human resources with adequate technical skills, regulatory uncertainty regarding the legal validity of blockchain-based diplomas, and organisational cultural resistance to disruptive innovation. Successful adoption requires a holistic approach that aligns technological readiness with organisational capacity and regulatory ecosystem support, where transformational leadership, multi-stakeholder collaboration through consortium models, and strategic investment in human resource capacity building are critical determinants of success. Without strong national coordination and long-term commitment from the government, universities, and the private sector, blockchain adoption risks remaining fragmented and exclusive to a handful of elite institutions, widening disparities in the quality of national higher education.

Looking ahead, Indonesia has a strategic opportunity not only to be a passive follower in the global blockchain revolution, but also a regional leader setting best practice standards for digital certification in Southeast Asia. The recommended implementation roadmap comprises three phases: (1) the pilot phase (2026–2027) focusing on the issuance of micro-credentials and digital badges at pioneering universities; (2) the scaling phase (2028–2029) involving the formation of a national higher education blockchain consortium and the standardisation of technical protocols; and (3) the maturity phase (2030 onwards) with the full integration of formal degree ‘ ’ into a national blockchain ecosystem that is interoperable with global

standards. With disciplined and collaborative execution, blockchain can act as a catalyst for realising a more transparent, accountable, and globally competitive Indonesian higher education ecosystem, whilst making a substantive contribution to an inclusive and sustainable national digital transformation.

References

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference, EuroSys '18*, 1–15. https://doi.org/10.1145/3190508.3190538

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In M. Maffei & M. Ryan (Eds.), *Principles of Security and Trust* (pp. 164–186). Springer. https://doi.org/10.1007/978-3-662-54455-6_8

Baldi, M., Chiaraluce, F., Kodra, M., & Spalazzi, L. (2019). *Security analysis of a blockchain-based protocol for the certification of academic credentials* (arXiv:1910.04622). arXiv. https://doi.org/10.48550/arXiv.1910.04622

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business & Information Systems Engineering*, *59*(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1

Ben Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. *2014 IEEE Symposium on Security and Privacy*, 459–474. https://doi.org/10.1109/SP.2014.36

Bhaskar, P., Tiwari, C. K., & Joshi, A. (2020). Blockchain in education management: Present and future applications. *Interactive Technology and Smart Education*, *18*(1), 1–17. https://doi.org/10.1108/ITSE-07-2020-0102

Bitansky, N., Canetti, R., Chiesa, A., & Tromer, E. (2012). From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ITCS '12*, 326–349. https://doi.org/10.1145/2090236.2090263

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White Paper*, *3*(37), 2–1.

Cantisani, A. (2006). Technological innovation processes revisited. *Technovation*, *26*(11), 1294–1301. https://doi.org/10.1016/j.technovation.2005.10.003

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

DiMaggio, P. J., & Powell, W. W. (2000). *The iron cage revisited institutional isomorphism and collective rationality in organizational fields*. https://www.emerald.com/books/edited-volume/14074/chapter/84962949/The-iron-cage-revisited-institutional-isomorphism

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Fitroh, I., & Aslan, A. (2026). TECHNOLOGY AND SCIENCE-BASED EDUCATION AS A PILLAR OF INTELLECTUAL DEVELOPMENT IN THE 21ST CENTURY: A LITERATURE REVIEW ON THE DEVELOPMENT OF ADAPTIVE, INCLUSIVE, AND SUSTAINABLE LEARNING MODELS IN THE DIGITAL AGE. *INJOSEDU: International Journal of Social and Education*, *2*(10), 3142–3154.

Hendrawati, T. (2026). *Learning Organization Sebagai Penggerak Mutu Dan Akreditasi Perguruan Tinggi Swasta*. PT Penerbit Qriset Indonesia.

Hifza, Juliana, Palapa, A., Maskur, & Aslan. (2020). The Strategic Foundation for Competitive Excellent Development in Integrated Islamic Primary Schools in Indonesia. *International Journal of Advanced Science and Technology*, *29*(12s), 1747–1753.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In J. Katz & H. Shacham (Eds.), *Advances in Cryptology – CRYPTO 2017* (pp. 357–388). Springer International Publishing. https://doi.org/10.1007/978-3-319-63688-7_12

Lin, I.-C., Yeh, I.-L., Chang, C.-C., Liu, J.-C., & Chang, C.-C. (2024). Designing a Secure and Scalable Data Sharing Mechanism Using Decentralized Identifiers (DID). *Computer Modeling in Engineering & Sciences*, *141*(1), 809–822. https://doi.org/10.32604/cmes.2024.051612

Mariska, T., & Aslan, A. (2024). TECHNOLOGY-BASED CURRICULUM MODEL. *International Journal Of Humanities, Social Sciences And Business (INJOSS)*, *3*(2), 322–332.

Merkle, R. C. (1988). A Digital Signature Based on a Conventional Encryption Function. In C. Pomerance (Ed.), *Advances in Cryptology—CRYPTO '87* (Vol. 293, pp. 369–378). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-48184-2_32

Mohammad, A., & Vargas, S. (2022). Barriers Affecting Higher Education Institutions' Adoption of Blockchain Technology: A Qualitative Study. *Informatics*, *9*(3). https://doi.org/10.3390/informatics9030064

Moya, J. A. B. (2024). *Blockchain for Academic Integrity: Developing the Blockchain Academic Credential Interoperability Protocol (BACIP)* (arXiv:2406.15482). arXiv. https://doi.org/10.48550/arXiv.2406.15482

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://assets.pubpub.org/d8wct41f/31611263538139.pdf

Pendidikan, K., & Indonesia, K. R. (2020). Panduan implementasi Merdeka Belajar–Kampus Merdeka. *Jakarta: Kemendikbud*.

Rahmah, M., Lubis, I. R. B., & Khair, R. (2026). Integrating Blockchain-Based Smart Contracts for Digital Certification: A Micro-Credentials Model for Vocational Higher Education. *JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING*, *9*(2), 334–345. https://doi.org/10.31289/jite.v9i2.16045

Rogers, E. M., Singhal, A., & Quinlan, M. M. (2019). Diffusion of Innovations 1. In *An Integrated Approach to Communication Theory and Research* (3rd ed.). Routledge.

San, A. M., Chotikakamthorn, N., & Sathitwiriyawong, C. (2020). Blockchain-based Learning Credential Revision and Revocation Method. *Proceedings of the 21st Annual Conference on Information Technology Education, SIGITE '20*, 42–45. https://doi.org/10.1145/3368308.3415456

Schneier, B. (2007). *Applied cryptography: Protocols, algorithms, and source code in C*. john wiley & sons.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stamp, M. (2011). *Information Security: Principles and Practice*. John Wiley & Sons.

Steiu, M.-F. (2020). Blockchain in education: Opportunities, applications, and challenges. *First Monday*. https://doi.org/10.5210/fm.v25i9.10654

Toader, D.-C., Toader, C., Dana, B., Toader, R., & Rădulescu, A. (2023). The Adoption of Blockchain Technology in Higher Education: The Impact of Leadership Readiness. *International Journal of Organizational Leadership*, *12*, 133–155. https://doi.org/10.33844/ijol.2023.60389

Yu, V. F., Bahauddin, A., Ferdinant, P. F., Fatmawati, A., & Lin, S.-W. (2023). The ISM Method to Analyze the Relationship between Blockchain Adoption Criteria in University: An Indonesian Case. *Mathematics*, *11*(1). https://doi.org/10.3390/math11010239

Zou, W., Lo, D., Kochhar, P. S., Le, X.-B. D., Xia, X., Feng, Y., Chen, Z., & Xu, B. (2021). Smart Contract Development: Challenges and Opportunities. *IEEE Transactions on Software Engineering*, *47*(10), 2084–2106. https://doi.org/10.1109/TSE.2019.2942301

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference, EuroSys '18*, 1–15. https://doi.org/10.1145/3190508.3190538

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In M. Maffei & M. Ryan (Eds.), *Principles of Security and Trust* (pp. 164–186). Springer. https://doi.org/10.1007/978-3-662-54455-6_8

Baldi, M., Chiaraluce, F., Kodra, M., & Spalazzi, L. (2019). *Security analysis of a blockchain-based protocol for the certification of academic credentials* (arXiv:1910.04622). arXiv. https://doi.org/10.48550/arXiv.1910.04622

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business & Information Systems Engineering*, *59*(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1

Ben Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. *2014 IEEE Symposium on Security and Privacy*, 459–474. https://doi.org/10.1109/SP.2014.36

Bhaskar, P., Tiwari, C. K., & Joshi, A. (2020). Blockchain in education management: Present and future applications. *Interactive Technology and Smart Education*, *18*(1), 1–17. https://doi.org/10.1108/ITSE-07-2020-0102

Bitansky, N., Canetti, R., Chiesa, A., & Tromer, E. (2012). From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ITCS '12*, 326–349. https://doi.org/10.1145/2090236.2090263

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White Paper*, *3*(37), 2–1.

Cantisani, A. (2006). Technological innovation processes revisited. *Technovation*, *26*(11), 1294–1301. https://doi.org/10.1016/j.technovation.2005.10.003

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

DiMaggio, P. J., & Powell, W. W. (2000). *The iron cage revisited institutional isomorphism and collective rationality in organizational fields*. https://www.emerald.com/books/edited-volume/14074/chapter/84962949/The-iron-cage-revisited-institutional-isomorphism

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Fitroh, I., & Aslan, A. (2026). TECHNOLOGY AND SCIENCE-BASED EDUCATION AS A PILLAR OF INTELLECTUAL DEVELOPMENT IN THE 21ST CENTURY: A LITERATURE REVIEW ON THE DEVELOPMENT OF ADAPTIVE, INCLUSIVE, AND SUSTAINABLE LEARNING MODELS IN THE DIGITAL AGE. *INJOSEDU: International Journal of Social and Education*, *2*(10), 3142–3154.

Hendrawati, T. (2026). *Learning Organization Sebagai Penggerak Mutu Dan Akreditasi Perguruan Tinggi Swasta*. PT Penerbit Qriset Indonesia.

Hifza, Juliana, Palapa, A., Maskur, & Aslan. (2020). The Strategic Foundation for Competitive Excellent Development in Integrated Islamic Primary Schools in Indonesia. *International Journal of Advanced Science and Technology*, *29*(12s), 1747–1753.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In J. Katz & H. Shacham (Eds.), *Advances in Cryptology – CRYPTO 2017* (pp. 357–388). Springer International Publishing. https://doi.org/10.1007/978-3-319-63688-7_12

Lin, I.-C., Yeh, I.-L., Chang, C.-C., Liu, J.-C., & Chang, C.-C. (2024). Designing a Secure and Scalable Data Sharing Mechanism Using Decentralized Identifiers (DID). *Computer Modeling in Engineering & Sciences*, *141*(1), 809–822. https://doi.org/10.32604/cmes.2024.051612

Mariska, T., & Aslan, A. (2024). TECHNOLOGY-BASED CURRICULUM MODEL. *International Journal Of Humanities, Social Sciences And Business (INJOSS)*, *3*(2), 322–332.

Merkle, R. C. (1988). A Digital Signature Based on a Conventional Encryption Function. In C. Pomerance (Ed.), *Advances in Cryptology—CRYPTO '87* (Vol. 293, pp. 369–378). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-48184-2_32

Mohammad, A., & Vargas, S. (2022). Barriers Affecting Higher Education Institutions' Adoption of Blockchain Technology: A Qualitative Study. *Informatics*, *9*(3). https://doi.org/10.3390/informatics9030064

Moya, J. A. B. (2024). *Blockchain for Academic Integrity: Developing the Blockchain Academic Credential Interoperability Protocol (BACIP)* (arXiv:2406.15482). arXiv. https://doi.org/10.48550/arXiv.2406.15482

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://assets.pubpub.org/d8wct41f/31611263538139.pdf

Pendidikan, K., & Indonesia, K. R. (2020). Panduan implementasi Merdeka Belajar–Kampus Merdeka. *Jakarta: Kemendikbud*.

Rahmah, M., Lubis, I. R. B., & Khair, R. (2026). Integrating Blockchain-Based Smart Contracts for Digital Certification: A Micro-Credentials Model for Vocational Higher Education. *JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING*, *9*(2), 334–345. https://doi.org/10.31289/jite.v9i2.16045

Rogers, E. M., Singhal, A., & Quinlan, M. M. (2019). Diffusion of Innovations 1. In *An Integrated Approach to Communication Theory and Research* (3rd ed.). Routledge.

San, A. M., Chotikakamthorn, N., & Sathitwiriyawong, C. (2020). Blockchain-based Learning Credential Revision and Revocation Method. *Proceedings of the 21st Annual Conference on Information Technology Education, SIGITE '20*, 42–45. https://doi.org/10.1145/3368308.3415456

Schneier, B. (2007). *Applied cryptography: Protocols, algorithms, and source code in C*. john wiley & sons.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stamp, M. (2011). *Information Security: Principles and Practice*. John Wiley & Sons.

Steiu, M.-F. (2020). Blockchain in education: Opportunities, applications, and challenges. *First Monday*. https://doi.org/10.5210/fm.v25i9.10654

Toader, D.-C., Toader, C., Dana, B., Toader, R., & Rădulescu, A. (2023). The Adoption of Blockchain Technology in Higher Education: The Impact of Leadership Readiness. *International Journal of Organizational Leadership*, *12*, 133–155. https://doi.org/10.33844/ijol.2023.60389

Yu, V. F., Bahauddin, A., Ferdinant, P. F., Fatmawati, A., & Lin, S.-W. (2023). The ISM Method to Analyze the Relationship between Blockchain Adoption Criteria in University: An Indonesian Case. *Mathematics*, *11*(1). https://doi.org/10.3390/math11010239

Zou, W., Lo, D., Kochhar, P. S., Le, X.-B. D., Xia, X., Feng, Y., Chen, Z., & Xu, B. (2021). Smart Contract Development: Challenges and Opportunities. *IEEE Transactions on Software Engineering*, *47*(10), 2084–2106. https://doi.org/10.1109/TSE.2019.2942301

Dewan Perwakilan Rakyat. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Dewan Perwakilan Rakyat. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 197.

Kemdikbudristek. (2023). *Laporan tahunan pemantauan integritas dokumen akademik*. Direktorat Jenderal Pendidikan Tinggi.

Kemdikbudristek. (2024). *Roadmap digitalisasi pendidikan tinggi 2025–2030*. Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia.

Kemdikbudristek. (2024). *Roadmap digitalisasi pendidikan tinggi 2025–2030*. Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia.

Kemdikbudristek. (2024). *Roadmap digitalisasi pendidikan tinggi 2025–2030*. Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia.

Kominfo. (2024). *Laporan status infrastruktur TIK perguruan tinggi Indonesia 2024*. Kementerian Komunikasi dan Informatika Republik Indonesia.
UI Center for Digital Innovation. (2024). *Laporan pilot project sertifikat mikro berbasis blockchain Universitas Indonesia*. Universitas Indonesia.
World Bank. (2023). *The future of work in Southeast Asia: Digital transformation and skills development*. World Bank Group. https://doi.org/10.1596/39876