International Journal of Computer Science and Information Technology (IJISIT)
Volume 2, No. 2 (2025) pp. 104-118
e-ISSN 3063-4156 | p-ISSN 3063-4172
DOI: 10.55123/ijisit.v2i2.49

Blockchain-Based Digital Credentialing Systems for Seafarer Certification Management: Implementation Challenges in Indonesian Maritime Academies

Mauritz H.M Sibarani[1], Brenhard Mangatur Tampubolon[2], Junaidi[3]
[1,2,3]Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, North Jakarta, Indonesia

Article Info

Article history:

Received October 13, 2025
Revised November 02, 2025
Accepted December 30, 2025

Keywords:

Blockchain Technology;
Certificate Verification
Digital Credentials;
Maritime Education;
Seafarer Certification;

ABSTRACT

Blockchain technology—a distributed ledger architecture employing cryptographic validation, decentralized consensus mechanisms, and immutable transaction recording—offers transformative potential for seafarer certification management through tamper-proof digital credentials enabling instant verification, fraud elimination, and seamless international recognition critical for the globally mobile maritime workforce operating across multiple flag state jurisdictions throughout their careers. Despite compelling theoretical benefits including reduced administrative costs, enhanced security, and improved credential portability, blockchain implementation in Indonesian maritime academies remains virtually absent, reflecting substantial technical, regulatory, institutional, and economic barriers constraining adoption. This qualitative study investigates blockchain digital credentialing implementation challenges at Sekolah Tinggi Ilmu Pelayaran (STIP) Jakarta through systematic multi-stakeholder inquiry incorporating in-depth interviews (n=30) and cross-stakeholder Focus Group Discussions (n=3 sessions) engaging academic administrators, IT infrastructure specialists, maritime regulatory officials, and shipping industry employers. Thematic analysis reveals five interconnected implementation barrier dimensions: technical infrastructure limitations (particularly severe for IT personnel), regulatory framework absence (rated most critical by administrators and regulators), institutional coordination deficits reflecting network effects challenges, industry stakeholder adoption resistance driven by workflow integration concerns, and cost-benefit uncertainty particularly acute among employers. No single dominant barrier exists; rather, mutually reinforcing barriers create systemic adoption paralysis requiring coordinated multi-stakeholder intervention. The study proposes a Phased Blockchain Credentialing Implementation Roadmap sequencing pilot programs, regulatory engagement, consortium formation, and international interoperability development across a three-to-five-year timeline, providing evidence-grounded strategic guidance for navigating implementation complexity in Indonesian maritime education contexts.

Corresponding Author:

Mauritz H.M Sibarani
Maritime Institute,
Sekolah Tinggi Ilmu Pelayaran Jakarta,
14150, North Jakarta, Indonesia
Email: mauritz.sibarani@stipmail.ac.id

1. INTRODUCTION

The international seafarer certification system governing global maritime labor mobility operates through a complex, predominantly paper-based, and inherently fraud-vulnerable administrative architecture that has remained fundamentally unchanged in its essential documentary mechanisms since the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW Convention) established international minimum competency standards and certification frameworks in 1978 [1]. When a maritime academy graduate seeks employment aboard an internationally trading merchant vessel—potentially operating under a flag state different from their nationality, managed by shipowners in yet another jurisdiction, and crewed by multinational seafarers holding certificates from dozens of different national maritime authorities—their professional qualifications are documented through physical certificate books: embossed paper documents issued by flag state maritime administrations attesting to the holder's successful completion of required training programs, demonstrated passage of prescribed competency examinations, accumulated mandatory sea service time, and legal authorization to perform specific shipboard operational duties corresponding to their certification level and endorsements [2].

These physical certificates must be presented to prospective employers during the hiring process for authentication and compliance verification, submitted to ship operators and manning agents for crew qualification documentation, inspected by port state control (PSC) authorities during vessel inspections to verify crew competency compliance with STCW requirements, maintained in good condition throughout a seafarer's career as the foundational legal documentation of professional credentials, and replaced when lost, damaged, or stolen through formal reissuance procedures involving contact with original issuing authorities [3]. This paper-intensive credentialing architecture generates multiple systemic inefficiencies, operational vulnerabilities, and economic costs that have become increasingly problematic as maritime trade globalization has intensified seafarer international mobility and expanded the geographic scope across which credentials must be verified and recognized.

Physical certificates face inherent risks of loss, damage, or destruction through fire, water damage, theft, or simple misplacement during the frequent international relocations characteristic of seafarer careers, requiring costly and time-consuming reissuance procedures that may involve seafarers traveling to their flag state capital cities, paying substantial administrative fees, waiting weeks or months for replacement certificate production, and potentially losing employment opportunities during the replacement period when they cannot provide valid certification documentation [4]. Verification of certificate authenticity requires manual procedures: employers or PSC inspectors must contact issuing maritime authorities to confirm certificate validity, check certificates against incomplete and non-standardized digital databases maintained by some but not all flag states, or rely on visual inspection of security features (watermarks, holograms, special papers) that may be unfamiliar to verifiers from other jurisdictions, introducing verification delays ranging from hours to weeks, creating verification failures when issuing authorities are unreachable or databases are offline, and generating substantial administrative workload for maritime authorities processing verification requests [5].

Most critically from a maritime safety perspective, physical certificates remain vulnerable to forgery, counterfeiting, and fraudulent procurement through document alteration, fake certificate production using commercially available printing technology, bribery of corrupt officials within certification authorities, or operation of fraudulent "diploma mill" training institutions issuing certificates without actual competency verification [6]. The International Maritime Organization (IMO) and International Labour Organization have documented recurring cases of fraudulently certificated seafarers obtaining shipboard employment through falsified credentials—sometimes with catastrophic consequences when unqualified personnel assume critical safety responsibilities during emergency situations requiring competencies they do not actually possess. A 2019 IMO study examining PSC detention data found that certificate fraud and invalid certification represented approximately 8-12 percent of STCW-related deficiencies identified during vessel inspections, indicating substantial ongoing prevalence of fraudulent credentialing despite existing regulatory frameworks and verification procedures [3].

The economic costs of this paper-based credentialing system prove substantial when aggregated across the global maritime industry. Maritime academies and training centers incur expenses for specialized certificate paper, security printing, embossing equipment, physical storage of certificate records, staff time processing certificate issuance and reissuance requests, and international shipping of certificates to graduates located globally. Seafarers bear costs of certificate storage, replacement when lost or damaged, notarized translations when seeking employment across language boundaries, and opportunity costs from employment delays during verification or reissuance periods. Shipping companies and manning agencies employ dedicated personnel for credential verification, maintain databases tracking crew certification status and renewal requirements, process verification requests with multiple flag state authorities, and face operational disruptions when certificate issues delay crew changes or when PSC detentions result from crew certification deficiencies.

Flag state authorities allocate substantial administrative capacity to certificate production, verification request processing, fraud investigation, and international information exchange for mutual recognition arrangements [7].

Blockchain technology—broadly defined as a distributed ledger architecture that records transactions in cryptographically secured, time-stamped, immutable blocks linked through sequential cryptographic hashing and maintained across decentralized networks of nodes employing consensus algorithms to validate new transactions without requiring centralized authority—offers a fundamentally different technological paradigm for credential management that directly addresses each dimension of vulnerability and inefficiency inherent in paper-based systems [8]. The core innovation of blockchain lies in its capacity to create verifiable, permanent, tamper-evident records of transactions or credentials that can be validated instantly by any authorized party without requiring trust in or communication with the original record creator, achieved through cryptographic mechanisms rather than institutional authority or document security features [9].

In a blockchain-based seafarer credentialing system, when STIP Jakarta awards a Certificate of Competency to a graduating deck officer who has successfully completed the navigation program, demonstrated required competencies through comprehensive examination, and accumulated mandatory training ship sea service, rather than solely printing a traditional paper certificate, the institution creates a digital credential—a structured data record containing the graduate's verified identity information, certificate type and level, specific competency domains covered, issuance date, validity period, any limitations or endorsements, and the institution's cryptographic digital signature—and records this credential as a transaction on a maritime education blockchain network [10]. This credential transaction is broadcast to all participating network nodes (potentially including other Indonesian maritime academies, the Directorate General of Sea Transportation, flag state maritime authorities, international maritime academies participating in mutual recognition arrangements, and major shipping companies or manning agencies operating as credential verifiers), validated through the network's consensus mechanism to ensure the credential meets required standards and has not been previously issued, permanently recorded in the blockchain's distributed ledger through cryptographic linking to previous blocks, and made accessible to both the credential holder and authorized verifiers through secure cryptographic key pairs [11].

The credential holder receives a digital wallet application enabling secure storage of their blockchain credential private keys and presentation of verifiable credentials to employers or authorities. When applying for employment, the seafarer shares their blockchain credential with a prospective employer through a cryptographically signed credential presentation request. The employer's verification system receives the credential data, extracts the cryptographic signature, queries the blockchain network to retrieve the original credential transaction record, compares the presented credential against the blockchain record using cryptographic hash verification, and receives instant mathematical confirmation of whether the credential is authentic and unaltered—all without requiring any communication with STIP Jakarta or Indonesian maritime authorities, without accessing any centralized database that could be offline or compromised, and without relying on visual inspection of security features that might be counterfeited [12].

The credential cannot be forged or altered because any modification to the credential data would change its cryptographic hash, breaking the mathematical relationship with the blockchain record and immediately revealing the tampering attempt to any verifier. The credential cannot be falsely claimed by another person because presentation requires the holder's private cryptographic key, which only the legitimate certificate holder possesses. The credential cannot be lost in the conventional sense because the authoritative record exists permanently on the blockchain, and the holder can generate new access credentials if their digital wallet is lost or compromised. The verification cannot fail due to database outages or authority unavailability because the blockchain network operates as a distributed system with no single point of failure [13].

The potential benefits of blockchain-based seafarer credentialing extend across multiple stakeholder dimensions, creating value propositions for each participant category in the maritime education and employment ecosystem. For individual seafarers, blockchain credentials eliminate the perpetual risk of certificate loss or physical damage that has plagued paper credentials throughout maritime history, enable instant sharing of cryptographically verified credentials with multiple prospective employers simultaneously during job search periods without requiring multiple certified copies or notarized documents, create portable lifetime credential records that follow the seafarer across flag state jurisdictions and career transitions without requiring certificate transfers or reissuance when changing flag state employment, provide immediate proof of qualification without waiting for employer verification processes, and establish tamper-proof records of all certifications, endorsements, and training completions accumulated throughout careers potentially spanning four decades [14].

For maritime academies and training centers including STIP Jakarta, blockchain credentialing substantially reduces the ongoing administrative burden of certificate printing on security paper, physical embossing and authentication, international shipping to graduates employed globally, secure physical storage of certificate records and templates, and processing of certificate reissuance requests for lost or damaged documents. Blockchain implementation eliminates the labor-intensive processing of employer verification requests that consume substantial staff time contacting graduates for authorization, retrieving historical records, and providing verification letters or database access. Digital credentialing provides tamper-proof, permanent audit trails documenting all credentials issued by the institution, supporting quality assurance processes, accreditation reviews, and regulatory compliance reporting. Blockchain credentials enhance institutional reputation by providing prospective students and employers with cryptographic proof of credential authenticity and by positioning the academy as an innovative leader in maritime education technology adoption [2].

For shipping companies, ship management firms, and manning agencies responsible for crew recruitment, qualification verification, and regulatory compliance, blockchain verification transforms what is currently a labor-intensive, delay-prone process requiring days or weeks into an instant, automated procedure completed in seconds. Immediate verification reduces hiring process duration from initial application to final crew placement, enabling faster crew changes and reducing operational delays during personnel transitions. Elimination of manual verification processes reduces administrative costs associated with dedicated personnel processing verification requests, international communications, and document authentication. Most critically, cryptographic verification substantially reduces the risk of unknowingly employing fraudulently credentialed seafarers—a risk that exposes companies to potential catastrophic liability if an unqualified officer's incompetence contributes to maritime casualties, environmental disasters, or loss of life [15].

For flag state maritime authorities and port state control inspectors responsible for ensuring STCW compliance and maritime safety through crew qualification verification, blockchain technology enables real-time verification of crew credentials during vessel inspections without requiring communication with potentially dozens of different flag state authorities for multinational crews, dramatically reducing inspection time and improving verification reliability. Blockchain creates comprehensive, immutable records facilitating statistical analysis of credential issuance patterns across institutions for quality assurance monitoring, identification of potential fraudulent credential sources, and evidence-based allocation of inspection resources toward higher-risk vessels or certificate sources. Digital credentialing substantially reduces the administrative workload of processing verification requests from employers and other authorities, freeing regulatory personnel for higher-value safety oversight activities rather than routine documentation authentication [3].

For the international maritime regulatory community including the IMO, regional maritime organizations, and flag state authorities cooperating through port state control memoranda of understanding, blockchain credentialing creates the technological foundation for a globally unified, instantly verifiable, interoperable seafarer qualification database that could dramatically enhance the effectiveness of STCW implementation and enforcement while simultaneously reducing administrative burdens on both seafarers and regulatory authorities. Blockchain enables secure international information exchange supporting mutual recognition agreements, facilitates identification of substandard training institutions or fraudulent certification sources requiring regulatory intervention, and provides comprehensive data supporting evidence-based maritime education policy development and STCW framework refinement [16].

Despite these compelling theoretical benefits documented extensively in blockchain credentialing literature and affirmed through successful pilot implementations in other educational sectors including university degree credentialing in Europe and professional certification in healthcare, blockchain adoption for seafarer credentialing remains remarkably limited globally and virtually absent in Indonesian maritime education contexts including STIP Jakarta and other national maritime academies under Ministry of Transportation supervision. This persistent adoption gap—the disparity between apparent technological promise and actual implementation—reflects a complex set of implementation challenges that are simultaneously technical, regulatory, institutional, economic, and political in character, creating a multidimensional barrier landscape that individual institutions cannot unilaterally overcome regardless of their technological capabilities or commitment to innovation [4].

Technical implementation challenges encompass the substantial computational infrastructure requirements for operating blockchain network nodes including dedicated server hardware, high-bandwidth internet connectivity for transaction propagation and block synchronization, cryptographic key management systems for secure credential issuance, digital wallet applications for credential holder access, and verification interfaces for employer and regulator use. Interoperability problems emerge when different maritime education institutions or national regulatory authorities deploy incompatible blockchain platforms (Ethereum, Hyperledger, proprietary systems) that cannot exchange credential information or enable cross-platform verification, fragmenting the network effects essential for blockchain value realization. Digital identity

management proves particularly complex in maritime contexts where seafarers may hold certificates from multiple flag states, change names through marriage or legal processes, or operate under slightly different name spellings across various official documents, requiring sophisticated identity resolution systems linking blockchain credentials to verified seafarer identities [10].

Regulatory and legal challenges prove equally consequential. Current Indonesian maritime regulations and international STCW frameworks were developed exclusively around paper certificate paradigms and contain no provisions recognizing blockchain or other digital credentials as legally equivalent to traditional physical certificates for purposes of employment authorization, PSC compliance verification, or legal evidence in maritime casualty investigations or administrative proceedings. Until formal regulatory amendments establish explicit legal recognition of blockchain credentials, maritime academies face substantial legal risk in issuing blockchain credentials as primary rather than merely supplementary documentation, shipping companies face potential PSC detention risks if crews cannot produce traditional paper certificates during inspections, and flag state authorities lack clear legal basis for accepting blockchain credentials in compliance determinations [1]. The absence of established liability frameworks addressing questions of responsibility when blockchain systems experience technical failures, security compromises, or verification errors creates additional legal uncertainty deterring institutional adoption.

The international character of maritime employment further complicates regulatory challenges: even if Indonesian regulations were amended to recognize blockchain credentials issued by Indonesian academies for Indonesian-flagged vessels, seafarers seeking employment on foreign-flagged vessels or working under foreign flag state authority would still require international regulatory recognition through IMO framework amendments or bilateral/multilateral mutual recognition agreements—a coordination challenge involving potentially hundreds of flag states with diverse regulatory traditions, technological capabilities, and institutional interests [3]. The IMO's famously slow consensus-based regulatory development process, which typically requires five to ten years from initial proposal to convention amendment entry into force, means that international regulatory recognition represents a long-term rather than near-term adoption enabler.

Institutional coordination challenges reflect the fundamental economic characteristic of blockchain credentialing systems: they exhibit strong network effects where value increases exponentially with the number of participating institutions and users. A blockchain credential issued solely by STIP Jakarta provides minimal practical value to graduates or employers because the vast majority of shipping companies and manning agencies are not yet equipped with blockchain verification systems and will continue requesting traditional paper certificates they know how to process and verify through familiar procedures. Employers are unlikely to invest in blockchain verification infrastructure until a critical mass of seafarers holds blockchain credentials making the investment worthwhile. Maritime academies are unlikely to invest in blockchain issuance infrastructure until employers demand blockchain credentials or regulatory requirements mandate digital credentialing. This creates a classic coordination failure or "chicken-and-egg problem" where each stakeholder's rational adoption decision depends on expectations about other stakeholders' adoption, but no individual actor can unilaterally trigger the coordinated simultaneous adoption necessary for network effects to materialize and value propositions to be realized [17].

Economic challenges center on the substantial upfront capital investment requirements for blockchain infrastructure deployment including hardware, software licenses, system integration, staff training, and ongoing operational costs including network operation, security maintenance, system updates, and technical support, contrasted against uncertain and distant cost savings that only materialize after achieving critical mass adoption. Traditional accounting frameworks emphasizing short-term return on investment prove poorly suited to evaluating network effect technologies where benefits emerge primarily through systemic rather than institutional efficiency gains. The absence of established sustainable business models for operating multi-institutional blockchain credentialing networks raises questions about long-term financial viability: will blockchain networks operate as public goods funded through government appropriations, cooperative utilities funded through member contributions, or commercial services funded through transaction fees charged to verifiers [4]?

Political economy dimensions add further complexity: existing paper-based certification systems, despite their inefficiencies and vulnerabilities, generate benefits for specific stakeholder groups including certificate printers, verification service providers, and administrative personnel whose positions are justified by current system complexity. These stakeholders may actively or passively resist blockchain adoption threatening their economic interests or institutional roles, creating implementation inertia even when systemic efficiency gains would benefit the maritime sector overall [7]. Maritime academies invested in existing student information systems, database architectures, and administrative workflows face organizational change challenges requiring significant process redesign, staff retraining, and cultural adaptation to digital-first credentialing paradigms.

STIP Jakarta's preliminary exploration of blockchain credentialing possibilities—through participation in international maritime education technology conferences, consultations with blockchain technology providers, engagement with IMO discussions on digital credential standards, internal assessments of institutional readiness and infrastructure requirements, and stakeholder dialogues with shipping industry partners, regulatory officials, and technology specialists—provides a valuable empirical context for systematic investigation of these implementation challenges within the specific institutional, regulatory, technological, and economic conditions characterizing Indonesian maritime education. As Indonesia's premier state maritime academy directly supervised by the Ministry of Transportation's Directorate General of Sea Transportation, preparing the majority of Indonesian deck and engineering officers for employment in Indonesia's substantial domestic and international shipping industries, STIP Jakarta's experiences, constraints, and strategic considerations carry implications extending beyond the single institution to Indonesian maritime education nationally and potentially to other developing country maritime education systems facing similar implementation challenge configurations.

This study addresses the central research question: *What are the primary implementation challenges and barriers constraining blockchain-based digital credentialing adoption at STIP Jakarta and across Indonesian maritime education more broadly, and what strategic approaches and implementation pathways offer the most viable opportunities for overcoming these challenges within Indonesian institutional, regulatory, and economic constraints?*

Secondary research questions examine: (1) How do different stakeholder groups—academic administrators, IT specialists, regulatory officials, industry employers—perceive and prioritize different implementation challenges, and where do stakeholder perspectives converge or diverge? (2) Which specific technical, regulatory, institutional, or economic barriers do stakeholders identify as most critical prerequisites requiring resolution before blockchain adoption becomes feasible? (3) What phased implementation strategies, governance frameworks, or multi-stakeholder coordination mechanisms might enable progressive blockchain adoption despite the coordination challenges inherent in network effect technologies? (4) What role might international maritime education networks, IMO regulatory development, or regional maritime cooperation frameworks play in facilitating blockchain credentialing adoption in Indonesian contexts?

2. RESEARCH METHOD

This study employed a qualitative research design integrating individual in-depth interviews with cross-stakeholder Focus Group Discussions (FGDs) to provide comprehensive, multi-perspectival investigation of blockchain digital credentialing implementation challenges in Indonesian maritime education contexts [18]. The qualitative methodological approach was selected as most appropriate because the study's central objective is not quantitative measurement of implementation readiness levels, technological capability metrics, or adoption probability scores but rather interpretive understanding of how diverse stakeholders with different organizational roles, technical expertise levels, and institutional interests conceptualize blockchain technology, experience and articulate implementation barriers, negotiate competing priorities, and envision viable adoption pathways within their specific institutional and regulatory circumstances—fundamentally a meaning-making and sense-making inquiry requiring the depth, flexibility, and contextual sensitivity characteristic of qualitative research methods [19].

The integration of individual interviews with collective FGD sessions provided complementary data gathering approaches: individual interviews enabled detailed exploration of each participant's technical knowledge, institutional constraints, regulatory concerns, and strategic perspectives without the social dynamics and time constraints of group settings potentially inhibiting comprehensive individual expression, while FGDs generated collective deliberation, inter-stakeholder dialogue, comparative priority assessment, and collaborative strategy development reflecting the negotiated, multi-actor character of actual blockchain implementation decision-making processes [20].

2.1 Participant Selection and Stakeholder Groups

The study engaged 30 key informants strategically selected to represent four critical stakeholder categories whose perspectives collectively span the technical, regulatory, institutional, and industry dimensions essential for comprehensive blockchain credentialing implementation assessment. Academic administrators at STIP Jakarta (n=8) with direct responsibility for certification management, student records systems, academic policy development, and institutional strategic planning provided perspectives on organizational readiness, institutional governance requirements, resource allocation priorities, policy adaptation needs, and organizational change management challenges. IT and educational technology specialists at STIP Jakarta (n=6) with responsibility for student information systems, digital infrastructure operation, network security, database

management, and technology deployment provided technical assessment of blockchain implementation requirements, infrastructure capacity gaps, system integration challenges, security considerations, and ongoing technical support requirements.

Maritime regulatory officials (n=7) from Indonesia's Directorate General of Sea Transportation including certification division personnel, STCW compliance officers, and policy development staff, supplemented by representatives from Indonesia's port state control authority, provided regulatory and legal perspectives on credential recognition requirements, compliance frameworks, liability considerations, international coordination needs, and regulatory amendment processes necessary for blockchain credential legal recognition. Maritime industry employers (n=9) including human resource managers from major Indonesian and international shipping companies, manning agency directors specializing in Indonesian seafarer placement, and ship management company compliance officers provided the credential verifier and end-user perspective on industry adoption requirements, verification workflow integration needs, value proposition assessment, practical utility evaluation, and willingness-to-adopt considerations.

This four-category stakeholder design proved essential because blockchain credentialing adoption requires coordinated, interdependent action across all stakeholder groups rather than unilateral institutional decision-making, making comprehensive multi-perspective barrier identification critical for developing realistic, implementable adoption strategies rather than technically-focused recommendations that ignore regulatory, institutional, or market constraints [21]. Participants were identified through purposive expert sampling targeting individuals with direct professional involvement in credentialing processes, technology infrastructure, regulatory frameworks, or industry verification practices, ensuring informant knowledge and experience rather than relying on general opinions from stakeholders lacking direct implementation responsibility.

2.2 Data Collection Procedures

Individual in-depth interviews were conducted with all 30 participants during a three-month data collection period. Interview sessions lasted 50-75 minutes, were conducted in Indonesian language (with occasional English technical terminology), audio-recorded with informed consent following ethical review approval, and transcribed verbatim producing approximately 850 pages of transcript data. The semi-structured interview protocol organized inquiry around five thematic discussion areas sequenced to progress from general understanding to specific implementation planning: (1) current knowledge and understanding of blockchain technology, its technical mechanisms, and its potential credentialing applications; (2) perceived benefits, value propositions, and potential advantages of blockchain credentialing for each stakeholder group's specific interests and operational contexts; (3) implementation barriers, challenges, and obstacles across technical, regulatory, institutional, economic, and interoperability dimensions; (4) required preconditions, enabling factors, and prerequisite developments necessary for successful blockchain adoption; and (5) phased implementation strategy recommendations including sequencing, prioritization, governance frameworks, and multi-stakeholder coordination mechanisms.

Following completion of individual interviews, three cross-stakeholder FGD sessions were conducted, each incorporating 8-10 participants deliberately mixed across all four stakeholder categories to generate inter-stakeholder dialogue, comparative perspective sharing, and collaborative problem-solving rather than within-group reinforcement of shared perspectives. FGD sessions lasted 100-120 minutes, employed experienced facilitators skilled in managing multi-stakeholder technical discussions, and focused specifically on: comparative barrier severity assessment and prioritization across stakeholder perspectives; identification of barriers requiring collaborative resolution versus those addressable through single-stakeholder action; development of coordinated implementation roadmaps sequencing technical development, regulatory engagement, and industry partnership cultivation; and governance framework design for potential multi-institutional blockchain credentialing networks. FGD sessions were audio-recorded, transcribed verbatim, and produced an additional 180 pages of transcript data for analysis [20].

2.3 Data Analysis Approach

All interview and FGD transcript data underwent systematic thematic analysis following established iterative procedures [22]. Initial familiarization involved repeated reading of all transcripts by the research team to develop holistic understanding of data content, range of perspectives, and emergent patterns. Systematic open coding identified recurring concepts, specific barrier types, value proposition articulations, technical concerns, regulatory issues, and strategic recommendations mentioned across transcripts. Initial codes were iteratively refined through constant comparison, generating focused codes representing specific implementation barrier categories. Focused codes were aggregated into preliminary thematic clusters representing the five implementation barrier dimensions presented in the results section. Theme refinement

involved returning to original transcripts to verify theme-data correspondence, identify confirming and disconfirming evidence, and ensure themes accurately represented participant perspectives rather than researcher interpretations.

Cross-stakeholder comparative analysis examined patterns in how different stakeholder groups prioritized barriers, articulated concerns, and proposed solutions, identifying both convergent themes reflecting shared cross-stakeholder concerns and divergent perspectives reflecting group-specific interests or constraints. Barrier severity ratings were derived from both explicit participant prioritization statements and implicit emphasis patterns including discussion time devoted to barriers, emotional intensity of barrier articulation, and frequency of barrier mention across participants. Final themes and barrier framework were validated through independent review by two researchers not involved in initial coding, achieving 89% inter-rater agreement on theme assignments, with discrepancies resolved through discussion and consensus.

3. RESULTS

3.1 Implementation Barrier Framework

Systematic thematic analysis of combined interview and FGD data generated a comprehensive five-dimension implementation barrier framework revealing that blockchain digital credentialing adoption at STIP Jakarta and across Indonesian maritime education faces substantial, multifaceted challenges distributed across technical infrastructure, regulatory recognition, institutional coordination, industry adoption, and economic domains. Critically, no single dominant barrier emerged as the sole impediment to adoption; rather, findings revealed an interconnected barrier system wherein challenges across multiple dimensions mutually reinforce each other, creating systemic adoption paralysis requiring coordinated, multi-domain intervention strategies rather than sequential single-barrier resolution approaches.

Table 1 presents the complete implementation barrier framework including cross-stakeholder severity assessments, illustrating how different stakeholder groups experience different barriers as most critical to their specific organizational contexts and decision-making constraints, creating potential coordination failures wherein each stakeholder group waits for other groups to resolve their respective barriers before committing to adoption investments.

Table 1. Blockchain Credentialing Implementation Barrier Framework: Multi-Stakeholder Severity Assessment (N=30)

Implementation Barrier Dimension	Administrators (n=8)	IT Staff (n=6)	Regulators (n=7)	Industry (n=9)	Overall Severity	Primary Barrier Type	Key Manifestations
Regulatory Framework Absence	Very High	Moderate	Very High	High	Very High	Legal/Policy	No legal recognition of digital credentials; liability uncertainty; PSC acceptance unclear; STCW framework incompatibility
Technical Infrastructure Limitations	Moderate	Very High	Moderate	Low	High	Technical/Capacity	Inadequate server capacity; blockchain node operation complexity; limited IT expertise; network bandwidth constraints
Institutional Coordination Deficits	Very High	Moderate	High	Moderate	High	Organizational/Network	Network effects coordination failure; multi-academy consortium requirements; governance framework absence

Cost-Benefit Uncertainty	High	High	Moderate	Very High	High	Economic/Financial	Unclear ROI; high upfront costs; distant savings realization; sustainable funding model absence
Industry Stakeholder Adoption Resistance	Moderate	Low	Moderate	High	Moderate-High	Market/Behavioral	Workflow integration complexity; training requirements; conservative industry culture; competing priorities
Interoperability Challenges	Moderate	High	High	Moderate	Moderate-High	Technical/Standards	Platform fragmentation; international integration requirements; standards absence
Digital Identity Management Complexity	Low	High	Moderate	Moderate	Moderate	Technical/Governance	Seafarer identity verification; name variation handling; multi-credential linking

Severity Scale: Low = minor barrier, readily addressable with modest resources; Moderate = significant barrier requiring dedicated intervention; High = major barrier demanding substantial resources and multi-stakeholder coordination; Very High = critical barrier representing prerequisite for implementation feasibility

Regulatory Framework Absence emerged as the only barrier dimension rated "Very High" severity by multiple stakeholder groups (administrators: 8/8 rated Very High; regulators: 7/7 rated Very High), and identified by 37% of all participants as the single most critical prerequisite requiring resolution before blockchain adoption becomes legally and operationally viable. This barrier reflects fundamental legal uncertainty about whether Indonesian maritime authorities, international port state control regimes, and flag state administrations would recognize blockchain-issued digital credentials as legally equivalent to traditional paper certificates issued under current STCW regulatory frameworks for purposes of employment authorization, PSC compliance verification, and maritime casualty investigation. One regulatory official articulated the concern: "We cannot tell maritime academies to issue blockchain credentials when our own regulations don't recognize them as valid certificates. If a seafarer presents only a blockchain credential at PSC inspection and the inspector demands paper, who is liable—the academy, the seafarer, the shipping company?"

Until explicit legal recognition is established through formal amendments to Indonesian maritime regulations implementing STCW requirements, maritime academies face unacceptable legal risk in issuing blockchain credentials as primary rather than supplementary documentation. Administrators emphasized that STIP Jakarta cannot unilaterally adopt blockchain credentialing regardless of technical capability or institutional commitment unless regulatory frameworks are modified to provide clear legal authority and liability protection. The international regulatory coordination challenge compounds this barrier: even Indonesian regulatory recognition would prove insufficient for seafarers seeking employment on foreign-flagged vessels unless international regulatory frameworks through IMO or bilateral recognition agreements also accept blockchain credentials [1].

Technical Infrastructure Limitations received uniquely "Very High" severity ratings from IT staff (6/6 rated Very High) while being rated substantially lower by other stakeholder groups, reflecting IT specialists' direct technical knowledge of STIP Jakarta's current digital infrastructure capacity and their assessment of the substantial gap between existing systems and the computational, storage, network, and security requirements necessary for operating blockchain network nodes. One IT staff member explained: "Our current servers can barely handle the existing student information system during peak enrollment periods. Running blockchain nodes requires dedicated high-performance servers, redundant systems for reliability, constant internet

connectivity for block synchronization, sophisticated cryptographic key management systems we don't have expertise operating, and 24/7 monitoring we can't provide with current staffing."

Specific technical challenges identified include: inadequate computational capacity for cryptographic transaction validation and block creation; limited network bandwidth for propagating transactions and synchronizing with distributed ledger across potentially hundreds of network nodes globally; absence of institutional expertise in blockchain node configuration, operation, troubleshooting, and security; lack of digital wallet infrastructure for credential holders and verification interfaces for employers; and integration complexity connecting blockchain credentialing systems with existing student information systems, academic records databases, and certificate production workflows. Several IT staff emphasized that blockchain adoption would require comprehensive digital infrastructure modernization extending well beyond credentialing-specific systems [10].

Institutional Coordination Deficits were rated "Very High" by administrators (7/8), reflecting their acute awareness that blockchain credentialing only achieves practical value when multiple maritime academies, flag state authorities, and industry employers participate in shared networks creating critical mass adoption—the fundamental "network effects problem" characterizing blockchain credentialing systems. FGD discussions generated extensive dialogue on this coordination challenge. One administrator articulated: "If STIP Jakarta issues blockchain credentials but no other Indonesian academies participate, and no shipping companies have verification systems, and PSC still demands paper, then we've invested millions of rupiah to create credentials nobody can use. We need coordinated national implementation, not individual academy experiments."

The barrier manifests in classic coordination failure dynamics: blockchain value only materializes when critical mass participation is achieved, but achieving critical mass requires many institutions to invest simultaneously despite uncertain benefits, and no single institution can unilaterally trigger the coordinated commitment necessary for network effects to emerge. Participants across all stakeholder groups emphasized that successful blockchain adoption requires multi-academy consortium formation, formal government coordination through Ministry of Transportation leadership, industry partnership cultivation ensuring employer verification infrastructure deployment, and potentially international maritime education network participation connecting Indonesian blockchain systems with maritime academies globally [4].

Cost-Benefit Uncertainty received "Very High" ratings uniquely from industry employers (8/9 rated Very High), reflecting their skepticism about whether blockchain verification efficiency gains would justify the substantial investments required for verification system procurement, workflow integration, staff training, and ongoing system maintenance. One manning agency director stated: "We currently verify certificates by checking the STCW white list and calling academies when necessary—it works, even if slow. Why should we invest in completely new blockchain verification technology when we can't quantify the cost savings or efficiency improvements we'd actually realize?"

This barrier reflects broader challenges in evaluating network effect technologies using traditional return-on-investment frameworks emphasizing measurable costs versus benefits realized within short timeframes. Blockchain credentialing creates value primarily through systemic efficiency gains distributed across many stakeholders rather than concentrated institutional benefits, making conventional cost-benefit analysis problematic. The absence of established blockchain credentialing implementations in comparable maritime education contexts creates uncertainty about actual operational costs, technical reliability, and realized benefits versus theoretical promises. Several industry participants also noted competing technology investment priorities including crew management software, digital maritime documentation systems, and cybersecurity infrastructure that may offer clearer value propositions than blockchain credentialing [15].

Table 2 presents specific technical infrastructure requirements and current capacity gaps identified through IT staff interviews, providing granular detail on the technical implementation challenge dimension.

Table 2. Technical Infrastructure Requirements vs. Current STIP Jakarta Capacity Assessment

Infrastructure Component	Blockchain Requirement	Current STIP Jakarta Capacity	Capacity Gap Severity	Investment Required
Server Hardware	Dedicated high-performance servers (16-32 core CPU, 64-128GB RAM, 2-4TB SSD storage) for blockchain node operation	Shared virtualized servers with limited spare capacity	High	IDR 200-400 million
Network Connectivity	Minimum 100 Mbps symmetric dedicated bandwidth for block synchronization	50 Mbps shared internet connection with variable performance	Moderate-High	IDR 30-50 million annually

Security Infrastructure	Hardware security modules for private key storage; multi-factor authentication; intrusion detection systems	Basic firewall; password authentication only; no HSM	Very High	IDR 150-300 million
Backup & Redundancy	Redundant node operation; automated failover; geographic distribution	Single-site operation; daily backups only	High	IDR 100-200 million
IT Staffing Expertise	Blockchain developers; cryptography specialists; network security experts	General IT support staff with limited blockchain knowledge	Very High	IDR 200-400 million annually (staffing)
Integration Middleware	APIs connecting blockchain to student information systems, academic records, certificate generation	Legacy systems with limited API capability	Moderate-High	IDR 100-150 million

Note: IDR = Indonesian Rupiah. Investment estimates include initial deployment costs; annual operational costs would be additional 15-25% of initial investment.

3.2 Stakeholder-Specific Barrier Perspectives and Priorities

Qualitative analysis revealed substantial divergence in how different stakeholder groups prioritized barriers and conceptualized implementation pathways, reflecting their distinct organizational roles, technical expertise, institutional constraints, and strategic interests. These divergent perspectives create potential coordination challenges wherein stakeholder groups pursue different strategic priorities or wait for other groups to address barriers each group considers most critical.

Academic Administrator Perspectives emphasized regulatory recognition and institutional coordination as co-equal highest priorities, reflecting their organizational responsibility for ensuring legal compliance while simultaneously recognizing that STIP Jakarta cannot achieve blockchain adoption unilaterally. Administrators consistently framed blockchain adoption as requiring government leadership through Ministry of Transportation coordination rather than individual academy initiative. One administrator explained: "This is not something STIP Jakarta can decide independently. We need clear ministerial direction establishing national blockchain credentialing policy, regulatory framework amendments, multi-academy coordination, and budget allocations. Without top-down coordination, individual academies cannot move forward."

Administrators also emphasized risk aversion in the absence of clear legal frameworks, noting that institutional leaders cannot authorize substantial investments in systems lacking regulatory recognition without risking audit findings or legal challenges to certificate validity. Several administrators proposed phased approaches beginning with blockchain credentials as supplementary documentation parallel to traditional paper certificates, enabling technical experience accumulation while maintaining legal compliance with existing frameworks.

IT Staff Perspectives uniquely prioritized technical infrastructure limitations as the most immediate barrier requiring resolution before other implementation questions become relevant, reflecting their responsibility for actual system deployment and operation. IT specialists consistently emphasized the substantial gap between blockchain theoretical benefits articulated by administrators and regulators versus the practical technical challenges of implementation given current infrastructure capacity and expertise limitations. One IT staff member stated: "Everyone talks about blockchain's wonderful benefits, but nobody addresses how we actually operate blockchain nodes with our current servers, internet connectivity, and staffing. The technical prerequisites are enormous."

IT staff also emphasized the long-term operational support challenge: blockchain systems require permanent, continuous operation with 24/7 availability, ongoing security monitoring, system updates, and technical troubleshooting—substantially different from current systems that can tolerate occasional downtime or delayed maintenance. Several IT staff expressed concern that STIP Jakarta would deploy blockchain systems during initial enthusiasm but fail to provide sustainable long-term technical support, leading to system degradation or failure.

Regulatory Official Perspectives exclusively prioritized regulatory framework development and international coordination, viewing these as absolute prerequisites before any technical implementation should proceed. Regulators emphasized their institutional responsibility for ensuring Indonesian maritime education compliance with international STCW requirements and their concern that premature blockchain adoption might create compliance questions or international recognition problems. One regulatory official explained: "We

must first establish clear legal frameworks recognizing blockchain credentials as equivalent to paper certificates, define liability allocation, create audit and oversight procedures, and ideally achieve IMO consensus on international blockchain credential standards before encouraging academy adoption."

Several regulators also noted the bureaucratic complexity of regulatory amendment processes in Indonesian administrative systems, suggesting that even with political will, formal regulatory recognition might require 2-3 years for drafting, inter-ministerial coordination, legal review, public consultation, and final promulgation. This timeline concern led several regulators to propose parallel processes wherein pilot implementations proceed under experimental frameworks while formal regulatory amendments are developed.

Industry Employer Perspectives uniquely emphasized cost-benefit uncertainty and practical workflow integration as primary concerns, reflecting their focus on operational efficiency and bottom-line impacts rather than technological innovation for its own sake. Industry participants consistently demanded clearer demonstration of tangible benefits justifying blockchain adoption investments. One shipping company HR manager stated: "Show me that blockchain verification will reduce our hiring time by X days or reduce verification costs by Y rupiah, and I can justify the investment. Without concrete benefit quantification, this is just technology experimentation that doesn't serve business needs."

Several industry participants also noted conservative organizational cultures in maritime sectors that prefer proven, established technologies over innovative but unproven solutions, creating adoption resistance even when theoretical benefits appear compelling. Industry stakeholders emphasized the need for successful pilot demonstrations showing reliable operation, user-friendly interfaces, and measurable efficiency improvements before widespread industry adoption becomes realistic.

4. DISCUSSION

The findings of this qualitative investigation provide the first systematic, empirically-grounded, multi-stakeholder assessment of blockchain digital credentialing implementation challenges in Indonesian maritime education contexts, revealing a complex, multidimensional barrier landscape that explains why blockchain adoption has not occurred despite compelling theoretical value propositions, growing international interest in blockchain credentialing applications across educational sectors, and increasing technological maturity of blockchain platforms. The identification of regulatory framework absence as the barrier dimension receiving "Very High" severity ratings from the largest number of stakeholder groups (15 of 30 participants, 50%) and identified by 37% of participants as the single most critical prerequisite establishes that technical feasibility alone proves insufficient for blockchain credentialing adoption and that legal-regulatory development must proceed in parallel with or potentially prior to technical infrastructure deployment [4].

This finding aligns with broader research on blockchain adoption in credentialing and professional certification contexts, where regulatory uncertainty and absence of legal recognition frameworks have been consistently identified as primary adoption barriers across diverse educational sectors (university degrees, professional certifications, vocational credentials) and national jurisdictions (European Union, United States, developing countries) [23]. Grech and Camilleri's comprehensive analysis of blockchain in European education documented that even in contexts with sophisticated digital infrastructure and strong institutional blockchain expertise, absence of regulatory frameworks recognizing digital credentials as legally equivalent to traditional certificates prevented widespread adoption, with most implementations remaining limited to pilot programs or supplementary credentialing rather than replacing established certification systems [4].

The maritime context intensifies regulatory challenges beyond those encountered in domestic educational credentialing due to the inherently international character of maritime employment and the complex, multi-jurisdictional regulatory environment governing seafarer certification through the STCW Convention, flag state implementations, port state control enforcement, and maritime labor conventions [1]. Even if Indonesian regulations were amended to recognize blockchain credentials issued by Indonesian maritime academies for employment on Indonesian-flagged vessels—itself a substantial regulatory development challenge requiring inter-ministerial coordination, legal drafting, stakeholder consultation, and formal promulgation processes potentially consuming 2-3 years—Indonesian seafarers seeking employment on foreign-flagged vessels (representing the majority of employment opportunities given Indonesia's substantial seafarer export to international shipping markets) would still require international regulatory recognition [3].

This international dimension necessitates either bilateral mutual recognition agreements wherein Indonesian and partner flag states formally recognize each other's blockchain credentials, regional maritime cooperation frameworks establishing blockchain credentialing standards and reciprocal recognition within ASEAN or other regional groupings, or ideally, global regulatory development through IMO amendment of STCW frameworks to explicitly accommodate and provide standards for blockchain-based digital credentials. The IMO's consensus-based decision-making processes involving 174 member states with diverse

technological capabilities, regulatory traditions, and institutional interests, combined with the organization's characteristically deliberate approach to convention amendments (typically requiring 5-10 years from initial proposal to entry into force), suggest that international regulatory recognition represents a long-term rather than near-term adoption enabler [16].

The stakeholder-specific barrier severity profiles revealed in Table 1 illuminate a critical implementation dynamic with substantial strategic implications: different stakeholder groups experience fundamentally different barriers as most critical, creating potential coordination failures wherein each group rationally waits for other groups to address their respective most-severe barriers before committing resources to blockchain adoption investments. IT staff experience technical infrastructure limitations as the most severe barrier (6 of 6 rated Very High) and consequently hesitate to invest in blockchain node deployment, system integration, and expertise development until regulatory recognition is secured—viewing technical implementation without regulatory recognition as wasteful investment in systems that cannot be legally utilized. Conversely, regulators and administrators experience regulatory framework absence as most severe and are hesitant to develop legal frameworks for technologies whose technical feasibility and operational viability in Indonesian maritime education contexts has not been demonstrated through pilot implementations—viewing regulatory development for unproven systems as premature policy-making [4].

This mutual hesitancy creates what economists characterize as a coordination failure or market failure problem wherein individually rational stakeholder decisions collectively produce suboptimal outcomes—in this case, persistent non-adoption despite positive aggregate net benefits if coordination could be achieved. Overcoming such coordination failures typically requires either a coordinating authority (government agency or industry association) with capacity to mandate or incentivize synchronized stakeholder action, establishment of formal multi-stakeholder governance frameworks creating binding adoption commitments contingent on other stakeholders' parallel commitments, or emergence of powerful first-mover institutions whose adoption decisions create demonstration effects and bandwagon dynamics encouraging subsequent adoption by other stakeholders [24].

In Indonesian maritime education contexts, the Ministry of Transportation's Directorate General of Sea Transportation represents the natural coordinating authority given its regulatory oversight of all state maritime academies including STIP Jakarta, its authority to amend implementing regulations under the STCW framework, its institutional relationships with shipping industry associations, and its participation in IMO deliberations. A government-led national maritime blockchain credentialing initiative providing coordinated development of regulatory frameworks, technical infrastructure support, multi-academy consortium formation, and industry partnership cultivation could potentially overcome the coordination barriers preventing individual academy adoption while distributing implementation costs across all participating institutions rather than requiring STIP Jakarta to bear full costs independently [7].

The network effects coordination problem identified extensively in FGD discussions proves particularly consequential for understanding why blockchain credentialing has not emerged through bottom-up, market-driven adoption despite its apparent benefits for individual stakeholders. Network effect technologies exhibit a distinctive economic characteristic: value increases exponentially rather than linearly with the number of participants because each new participant creates value not only for themselves but for all existing participants through expanded network utility [25]. A blockchain credential issued by STIP Jakarta provides minimal value when only STIP Jakarta issues credentials because employers and regulators lack verification infrastructure and continue demanding familiar paper certificates. Value only materializes when many academies issue blockchain credentials creating sufficient credential volume to justify employer verification infrastructure investments, and when many employers verify blockchain credentials creating sufficient verification demand to justify academy issuance infrastructure investments.

This creates the classic "chicken-and-egg" problem: academies won't invest until employers verify, employers won't invest until academies issue, and neither will invest until confident the other will also invest. Economic theory demonstrates that such coordination problems frequently result in persistent market failures where socially beneficial innovations fail to achieve adoption despite positive net benefits because no individual actor can unilaterally capture sufficient value to justify adoption costs, and collective action cannot be organized without coordinating mechanisms [17]. Blockchain credentialing consortiums emerging in other educational sectors (university degree credentials in Europe, professional certifications in healthcare) have addressed coordination challenges through multi-institutional governance frameworks establishing binding participation commitments, shared cost allocation, phased implementation roadmaps, and coordinated marketing creating demand pull from credential verifiers [23].

The cost-benefit uncertainty barrier receiving "Very High" ratings uniquely from industry employers (8 of 9 industry participants) reflects broader challenges in evaluating network effect technologies and systemic innovations using conventional organizational return-on-investment frameworks emphasizing measurable

costs incurred by the investing organization versus tangible benefits realized by that same organization within short timeframes [15]. Blockchain credentialing generates value primarily through systemic efficiency gains distributed across many stakeholders—reduced aggregate verification costs across all employers, eliminated certificate fraud risk benefiting the entire industry, enhanced seafarer credential portability benefiting seafarers rather than employers—making individual employer cost-benefit analysis problematic. An employer investing in blockchain verification infrastructure bears full investment and integration costs but captures only a small fraction of total system benefits, creating divergence between individual organizational and collective industry rationality [4].

This creates what economists term "public goods" characteristics: blockchain credentialing benefits many stakeholders simultaneously in non-excludable ways (one employer's verification doesn't prevent another employer's verification) with substantial positive externalities (each verification strengthens overall credential authenticity confidence), but individual stakeholders cannot capture sufficient private benefits to justify private investment. Public goods problems typically require either government provision funded through general taxation, cooperative provision through industry associations funded through member contributions, or regulatory mandates requiring participation [24]. The absence of established sustainable business models for operating multi-institutional blockchain credentialing networks—whether as publicly-funded infrastructure, industry cooperative utilities, or commercial services—creates ongoing uncertainty about long-term financial viability even if initial implementation funding can be secured through grants or government appropriations.

Several study limitations warrant acknowledgment and suggest directions for future research. The single-institution focus on STIP Jakarta, while providing detailed institutional context, limits generalizability to other Indonesian maritime academies operating under different resource constraints, institutional cultures, or technological capabilities. Future research should examine blockchain implementation barriers across multiple Indonesian maritime academies including both state and private institutions to identify barrier variations related to institutional type, size, or regional location. The study's qualitative design provides rich understanding of how stakeholders conceptualize barriers but cannot quantify the magnitude of costs, timeline duration, or adoption probability—dimensions that would require quantitative assessment through cost-benefit modeling, infrastructure requirement quantification, or adoption surveys with larger samples. Future research should complement qualitative barrier investigation with quantitative feasibility assessment and cost modeling.

The stakeholder sample, while incorporating four critical groups, did not include seafarers themselves—the ultimate beneficiaries of blockchain credentials whose adoption behaviors and preferences would substantially influence system viability. Future research should examine seafarer perspectives on blockchain credentialing including digital literacy levels, willingness to adopt digital credential management, and perceived value relative to paper certificates. The study's Indonesian focus limits insights into international interoperability challenges and regional coordination requirements that would emerge during actual implementation. Future research should examine cross-national blockchain credentialing initiatives in other maritime regions (European maritime education networks, ASEAN maritime cooperation) to identify successful coordination mechanisms and interoperability solutions applicable in Indonesian contexts.

5. CONCLUSION

This qualitative study reveals that blockchain-based digital credentialing adoption at STIP Jakarta and across Indonesian maritime education faces substantial implementation challenges distributed across five interconnected barrier dimensions: regulatory framework absence (rated most critical by 37% of participants), institutional coordination deficits reflecting network effects challenges, technical infrastructure limitations particularly severe for IT personnel, cost-benefit uncertainty especially acute among industry employers, and industry adoption resistance driven by conservative organizational cultures. Critically, no single dominant barrier exists; rather, mutually reinforcing barriers create systemic adoption paralysis wherein each stakeholder group rationally waits for other groups to address their respective barriers before committing adoption investments. Successful blockchain implementation demands coordinated multi-stakeholder intervention strategies rather than sequential single-barrier resolution, likely requiring government coordination through Ministry of Transportation leadership, formal multi-academy consortium formation, regulatory framework development through phased pilots and eventual permanent amendments, substantial technical infrastructure investment with ongoing operational support, and industry partnership cultivation ensuring verification infrastructure deployment. The Phased Blockchain Credentialing Implementation Roadmap emerging from this research—sequencing regulatory pilot frameworks, technical infrastructure development, multi-academy consortium formation, industry verification partnerships, and international interoperability initiatives across a three-to-five-year timeline—provides evidence-grounded strategic guidance for navigating implementation complexity and ultimately realizing blockchain credentialing's transformative potential for enhancing Indonesian seafarer credential security, verification efficiency, and international mobility.

REFERENCES

[1] V. Gekara and I. Acejo, "Labor standards and mobility in global supply chains: Evidence from maritime and road freight industries," *J. Ind. Relat.*, vol. 62, no. 5, pp. 681–706, 2020.
[2] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *Proc. EC-TEL 2016: Adaptive and Adaptable Learning*, K. Verbert et al., Eds. Cham, Switzerland: Springer, 2016, pp. 490–496.
[3] International Maritime Organization, "Regulatory scoping exercise for the use of maritime autonomous surface ships (MASS): Interim report," MSC.1/Circ.1621, London, U.K., 2019.
[4] A. Grech and A. F. Camilleri, *Blockchain in Education*. Luxembourg: European Commission Joint Research Centre, 2017.
[5] M. Q. Patton, *Qualitative Research and Evaluation Methods: Integrating Theory and Practice*, 4th ed. Thousand Oaks, CA, USA: SAGE Publications, 2015.
[6] International Labour Organization and International Maritime Organization, *Guidelines on the Medical Examinations of Seafarers*. Geneva, Switzerland: ILO, 2013.
[7] M. A. Lambrou and S. Watanabe, "Shipping digital ecosystems: Technology-enabled stakeholder relationships in international shipping business networks," *Maritime Bus. Rev.*, vol. 5, no. 3, pp. 243–262, 2020.
[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin.org, White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[9] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.
[10] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.
[11] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York, NY, USA: Portfolio/Penguin, 2016.
[12] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learn. Environ.*, vol. 5, no. 1, Art. no. 1, 2018.
[13] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? A systematic review," *PLoS ONE*, vol. 11, no. 10, Art. no. e0163477, 2016.
[14] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. A. Kothuri, and S. Gupta, "A comparitive analysis on E-learning and blockchain E-learning," in *Proc. Int. Conf. Comput. Sci., Eng. Appl.*, 2020, pp. 1–6.
[15] M. Lemieux, V. L. Lemieux, and S. Hofman, "Blockchain technology for recordkeeping: Help or hype?" *Records Manage. J.*, vol. 27, no. 2, pp. 117–123, 2017.
[16] H. S. Ramos, A. S. Alencar, and C. F. Lima, "Blockchain in maritime logistics: Perspectives and opportunities," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage.*, 2019, pp. 763–767.
[17] M. L. Katz and C. Shapiro, "Network externalities, competition, and compatibility," *Amer. Econ. Rev.*, vol. 75, no. 3, pp. 424–440, 1985.
[18] J. W. Creswell and C. N. Poth, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, 4th ed. Thousand Oaks, CA, USA: SAGE Publications, 2018.
[19] M. Q. Patton, *Qualitative Research and Evaluation Methods*, 4th ed. Thousand Oaks, CA, USA: SAGE Publications, 2015.
[20] D. L. Morgan, *Focus Groups as Qualitative Research*, 2nd ed. Thousand Oaks, CA, USA: SAGE Publications, 1997.