Multicore Int. J. Multidiscip, Vol 2, No 1, May 2026
e-ISSN: 3108-933X

Blockchain-Enhanced Maritime Education Ecosystem: Decentralized Credentialing for Global Seafarer Competency Verification

Pargaulan Dwikora Simanjuntak[1*], Ikhwanuddin[2], A. Nurfajri Irwan[3], Yayu Nopriani Martha[4], Giovanni Battista Puteri[5]
[1]Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, Indonesia, dwikoras@gmail.com
[2]Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, Indonesia, ikhwanuddin@stipmail.ac.id
[3]Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, Indonesia, a.nurfajriirwan@stipmail.ac.id
[4]Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, Indonesia, yayunoprianimartha@stipmail.ac.id
[5]Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, Indonesia, giovannibattistaputeri@stipmail.ac.id
[*]Corresponding author, e-mail: dwikoras@gmail.com

Abstract—The global maritime industry faces a critical seafarer shortage of 89,510 officers, exacerbated by fragmented credential verification systems, fraudulent certification practices, and inefficient competency recognition across jurisdictions. This research develops a comprehensive Blockchain-Enhanced Maritime Education Ecosystem integrating decentralized credentialing infrastructure with IoT-enabled simulation training and economic impact assessment of maritime labor market transformation. Through qualitative analysis incorporating perspectives from maritime education experts, certification authority administrators, and shipping company training managers, this study identifies critical requirements for trustless verification systems, interoperability standards, and stakeholder adoption barriers. The framework synthesizes educational technology innovations with maritime training regulatory compliance, demonstrating how blockchain-based credentialing can simultaneously enhance seafarer mobility, reduce certification fraud, and improve competency verification efficiency while addressing cybersecurity concerns and digital divide challenges. Findings reveal significant gaps in current certification systems, particularly regarding cross-jurisdictional recognition mechanisms and real-time competency tracking capabilities. The research contributes actionable implementation pathways for maritime stakeholders globally, offering evidence-based strategies for digital transformation of seafarer credentialing aligned with STCW Convention requirements and SDG 4 (Quality Education), while addressing the urgent workforce development needs essential for maritime industry sustainability and operational safety.

Keywords: *Blockchain credentialing, maritime education, seafarer competency verification, decentralized systems, digital certification*

This article *is licensed under the CC–BY-SA license.*

1. INTRODUCTION

The global maritime industry confronts an escalating human capital crisis characterized by persistent seafarer shortages, aging workforce demographics, and systemic inefficiencies in education, training, certification, and credential verification processes that collectively threaten maritime operational safety, service quality, and industry sustainability [1]. Current projections from the International Chamber of Shipping indicate a global shortage of approximately 89,510 qualified officers by 2026, with particular deficits in specialized roles including navigational officers for technologically advanced vessels and engineering officers competent in emerging propulsion technologies and digital systems, representing a 5.8% supply gap that constrains fleet expansion, increases operational costs, and potentially compromises safety standards when undermanned vessels operate or less qualified personnel assume

Received: 1 January 2026, Revised: 8 January 2026 , Accepted: 8 January 2025
https://doi.org/10.64123/mijm.v2.i1.2

responsibilities beyond their competency levels [2]. This workforce crisis reflects multiple converging challenges including insufficient training capacity in maritime education institutions, declining career attractiveness among younger generations preferring shore-based employment, limited retention due to demanding working conditions and extended family separation, and critically, substantial inefficiencies in credential verification and competency recognition systems that impede seafarer mobility, enable certification fraud, and create administrative burdens reducing effective workforce utilization [3]. The Standards of Training, Certification and Watchkeeping for Seafarers (STCW) Convention administered by the International Maritime Organization establishes international minimum competency standards, yet implementation exhibits substantial heterogeneity across national administrations, verification mechanisms remain predominantly paper-based or fragmented digital systems vulnerable to forgery, and cross-jurisdictional recognition processes impose lengthy delays and administrative costs that reduce labor market efficiency and seafarer employment opportunities [4].

The emergence of blockchain technology and distributed ledger systems presents transformative opportunities for addressing fundamental inefficiencies in maritime credentialing through creation of immutable, transparent, and interoperable verification systems that could revolutionize how seafarer competencies are documented, verified, and recognized across global maritime networks. Blockchain technology, originally developed as the underlying architecture for cryptocurrency transactions, provides decentralized database infrastructure where records are cryptographically secured, distributed across multiple network nodes, and validated through consensus mechanisms that eliminate single points of failure while creating tamper-resistant audit trails suitable for credential verification applications requiring high trust and permanence [5]. Applied to maritime education and credentialing, blockchain systems could enable creation of comprehensive digital credential repositories containing verified records of seafarers' educational qualifications, training completions, examination results, sea service experience, and competency assessments that employers, port state control authorities, and flag state administrations could instantly verify without relying on vulnerable paper certificates or fragmented national databases, potentially eliminating certification fraud estimated to affect 5-10% of global seafarer credentials while dramatically reducing verification timeframes from weeks to seconds [6]. Furthermore, integration with Internet of Things (IoT) sensor networks in maritime simulation training facilities could enable real-time competency assessment and automatic credential updating as seafarers complete training modules, creating continuous professional development tracking systems that replace periodic re-certification with ongoing competency monitoring more accurately reflecting actual capability levels rather than time-based renewal cycles that inadequately ensure maintained proficiency [7].

Despite blockchain technology's substantial promise for maritime credentialing transformation, significant technical, institutional, and socioeconomic barriers constrain practical implementation and scalability, requiring comprehensive frameworks that address not merely technological architecture but also regulatory compliance, stakeholder coordination, cybersecurity protection, and equitable access considerations. Technical challenges encompass interoperability requirements where blockchain credentialing systems must integrate with existing maritime training management systems, national licensing databases, and employer human resource platforms, necessitating standardized data formats, application programming interfaces, and consensus protocols that enable seamless information exchange across heterogeneous technological environments [8]. Institutional barriers include regulatory uncertainties regarding legal recognition of blockchain credentials, resistance from established certification authorities whose operational models and revenue streams depend upon current paper-based or centralized digital systems, and coordination requirements across multiple maritime administrations whose cooperation is essential for achieving global interoperability that provides blockchain credentialing's primary value proposition [9]. Cybersecurity concerns emerge from blockchain systems' distributed nature and immutability characteristics, where inadequate access controls could expose sensitive personal information while permanent record keeping complicates compliance with data protection regulations including right-to-erasure provisions, and potential vulnerabilities in smart contract code or consensus mechanisms could enable attacks compromising credential integrity with

consequences more severe than current systems where localized breaches affect limited record subsets rather than entire networks [10]. Digital divide considerations address equity implications where blockchain credentialing adoption could disadvantage seafarers from developing nations with limited digital literacy, internet connectivity constraints, or inadequate access to verification technologies, potentially exacerbating existing inequalities in global maritime labor markets where seafarers from certain regions already face discrimination and reduced employment opportunities despite equivalent qualifications [11].

Current maritime credentialing practices exhibit multiple systemic weaknesses that blockchain solutions could potentially address while simultaneously creating new challenges requiring careful management through comprehensive implementation frameworks. Existing paper-based certificate systems remain dominant in many maritime jurisdictions despite digitalization efforts, creating vulnerability to forgery, physical damage, loss, and administrative inefficiencies requiring seafarers to maintain multiple physical documents whose verification necessitates manual processes consuming substantial time and administrative resources [12]. Where digital credentialing systems exist, they typically operate as isolated national databases without interoperability mechanisms enabling international verification, forcing foreign employers and port authorities to rely upon bilateral recognition agreements, manual verification requests to issuing authorities, or acceptance of unverified seafarer-presented documents that provide minimal fraud protection and create verification delays affecting employment processes and operational planning [13]. Competency assessment practices predominantly emphasize one-time examination and periodic renewal cycles rather than continuous monitoring, potentially allowing skills degradation between renewal periods while providing inadequate recognition of ongoing professional development and informal learning that enhance actual competency levels beyond formal certification requirements [14]. Furthermore, current systems provide limited transparency regarding training quality across different maritime education institutions, making it difficult for employers to assess credential reliability and for prospective students to make informed training provider selections, potentially perpetuating quality variations that undermine STCW Convention objectives of ensuring consistent global minimum competency standards [15].

Despite growing recognition of blockchain technology's potential applications in maritime education and credentialing, significant research gaps persist regarding practical implementation frameworks that translate conceptual blockchain architectures into operational credentialing systems acceptable to regulatory authorities, adopted by maritime education institutions, and trusted by seafarers and employers whose participation determines implementation success. Existing literature predominantly focuses on technical blockchain design considerations or theoretical discussions of potential benefits, with limited empirical research examining stakeholder perspectives regarding implementation priorities, adoption barriers, acceptance criteria, and governance requirements that fundamentally determine whether proposed systems achieve practical viability beyond proof-of-concept demonstrations [16]. Most proposed blockchain credentialing frameworks inadequately address regulatory compliance complexities including legal recognition requirements, data protection obligations, and integration with STCW Convention verification mechanisms, creating implementation uncertainty that may deter adoption by risk-averse maritime administrations and established certification authorities responsible for seafarer licensing [17]. Furthermore, minimal research exists examining economic implications of blockchain credentialing transformation for different stakeholder groups, including cost-benefit analyses for maritime education institutions contemplating system adoption, competitiveness impacts for seafarers in transformed labor markets, and return-on-investment assessments for employers considering integration of blockchain verification into recruitment and crew management processes [18]. The absence of comprehensive, stakeholder-informed, and empirically validated frameworks creates implementation uncertainty that may delay potentially beneficial innovations while risking premature deployments of inadequately designed systems that underperform expectations, encounter regulatory resistance, or generate unintended negative consequences including exacerbated digital divides or cybersecurity vulnerabilities.

This research addresses these critical gaps by developing and validating a comprehensive Blockchain-Enhanced Maritime Education Ecosystem framework integrating technological architecture specifications, regulatory compliance mechanisms, stakeholder adoption strategies, and economic impact assessments to create practical pathways for credentialing system transformation. The central research question guiding this investigation is: How can blockchain-based decentralized credentialing systems integrated with IoT-enabled simulation training be designed and implemented to enhance seafarer competency verification, reduce certification fraud, and improve maritime labor market efficiency while ensuring regulatory compliance, cybersecurity protection, and equitable access across diverse global maritime contexts? This overarching question encompasses several specific research objectives: first, to conduct comprehensive technical assessment of blockchain architectures, consensus mechanisms, and smart contract designs suitable for maritime credentialing applications with attention to scalability, interoperability, and cybersecurity requirements; second, to analyze regulatory compliance requirements including STCW Convention alignment, data protection obligations, and legal recognition mechanisms across representative maritime jurisdictions; third, to examine stakeholder perspectives from maritime education experts, certification authority administrators, and shipping company training managers regarding implementation priorities, adoption barriers, acceptance criteria, and governance preferences through structured qualitative inquiry; fourth, to assess economic implications of blockchain credentialing transformation through examination of implementation costs, operational efficiency gains, fraud reduction benefits, and labor market competitiveness impacts across different stakeholder categories; and fifth, to synthesize technical assessments, regulatory analyses, stakeholder insights, and economic evaluations into an integrated implementation framework encompassing technological specifications, governance structures, adoption strategies, and transition pathways from current systems to blockchain-enhanced credentialing ecosystems.

The significance of this research extends across safety, efficiency, equity, and innovation dimensions of maritime human capital development while advancing theoretical understanding of blockchain technology applications in credentialing systems and professional licensing contexts beyond maritime-specific domains. From a safety perspective, enhanced credentialing integrity and competency verification directly contribute to maritime operational safety by ensuring that seafarers occupying critical positions possess verified qualifications and demonstrated competencies, reducing risks of maritime accidents resulting from inadequate personnel capabilities that current fraud-vulnerable systems inadequately prevent [19]. The research supports Sustainable Development Goal 4 (Quality Education) by advancing educational quality assurance mechanisms and credential transparency that enable informed student decision-making and continuous improvement in maritime training provision, while contributing to SDG 8 (Decent Work and Economic Growth) through labor market efficiency improvements that enhance seafarer employment opportunities and reduce administrative barriers constraining workforce mobility [20]. From an innovation perspective, the investigation demonstrates practical applications of emerging technologies in complex international regulatory contexts, potentially generating insights transferable to other professional credentialing systems including medical licensing, engineering certification, and educational degree verification facing similar challenges regarding fraud prevention, international recognition, and competency assurance [21]. The research also contributes to understanding digital transformation challenges in traditionally conservative industries where technological innovation must accommodate established regulatory frameworks, diverse institutional capabilities, and stakeholder populations with varying technological sophistication levels, providing implementation insights relevant beyond specific maritime applications to broader digital transition contexts.

The research employs a comprehensive mixed-methods qualitative approach combining technical literature analysis, regulatory framework examination, economic modeling, and structured stakeholder consultations to develop empirically grounded implementation frameworks that integrate technological feasibility with regulatory acceptability, economic viability, and stakeholder adoption likelihood. The study population encompasses three primary stakeholder categories whose diverse perspectives

collectively inform framework development: maritime education experts including training center administrators, simulation instructor specialists, and curriculum development professionals who provide insights regarding integration of blockchain credentialing with educational delivery, assessment practices, and institutional operational requirements; certification authority administrators including maritime administration licensing officials, STCW Convention implementation coordinators, and credential verification personnel who contribute regulatory compliance expertise, legal recognition requirements, and governmental acceptance criteria essential for official system recognition; and shipping company training managers including crewing department directors, competency assessment coordinators, and seafarer recruitment specialists who offer employer perspectives regarding verification needs, integration with human resource systems, and value propositions justifying adoption investments. Through semi-structured interviews, focus group discussions, and validation workshops, the research captures nuanced understandings of implementation opportunities and constraints that purely technical analyses or theoretical frameworks cannot adequately reveal, while thematic analysis identifies convergent priorities and divergent perspectives across stakeholder groups informing framework design that balances multiple legitimate objectives and constraints. This qualitative methodology proves particularly appropriate for investigating emerging technological applications in complex regulatory environments where limited operational precedents exist and substantial uncertainties characterize optimal implementation approaches, enabling development of flexible, adaptive frameworks suitable for diverse contexts rather than rigid prescriptive solutions inappropriate for heterogeneous global maritime education and credentialing landscapes.

2. METHOD

The research methodology employs a comprehensive qualitative approach designed to capture multi-stakeholder perspectives on blockchain-enhanced maritime credentialing challenges, opportunities, and implementation requirements, synthesizing technical expertise with regulatory insights and operational considerations to develop practical, evidence-based frameworks applicable across diverse maritime education and certification contexts. The methodological design recognizes that effective credentialing system transformation requires understanding not merely technological capabilities and architectural options but also regulatory constraints, institutional dynamics, adoption barriers, and equity implications that fundamentally shape implementation feasibility and sustainability outcomes [22]. Qualitative inquiry methods prove particularly appropriate for investigating emerging technological applications in established professional credentialing systems where limited operational experience exists, stakeholder acceptance determines adoption success, and complex regulatory environments constrain implementation options, enabling exploration of perceptions, anticipated challenges, and success factors that quantitative approaches focused on operational metrics from mature systems cannot adequately address [23]. The research deliberately incorporates diverse stakeholder perspectives representing different organizational missions, professional responsibilities, and value priorities to construct holistic understanding of implementation requirements that transcends narrow technological optimization toward comprehensive solutions balancing multiple legitimate objectives including credentialing integrity, regulatory compliance, operational efficiency, cybersecurity protection, and equitable access.

The research population comprises three strategically selected stakeholder categories whose collective expertise encompasses the educational, regulatory, and operational dimensions essential for comprehensive framework development. Maritime education experts constitute the first stakeholder category, including training center administrators responsible for institutional operations and regulatory compliance, simulation instructor specialists who deliver competency-based training using advanced maritime simulators, and curriculum development professionals who design educational programs aligned with STCW Convention requirements and industry competency needs. This group provides critical insights regarding integration of blockchain credentialing with existing educational delivery systems, assessment practices and competency verification methodologies, institutional capacity and resource

requirements for technology adoption, and pedagogical considerations ensuring that technological innovation enhances rather than compromises educational quality and learning outcomes. The second stakeholder category encompasses certification authority administrators including maritime administration licensing officials who issue seafarer certificates and maintain national credentialing databases, STCW Convention implementation coordinators who ensure national compliance with international standards and facilitate recognition agreements with foreign administrations, and credential verification personnel who conduct document authentication and fraud investigation processes. These governmental professionals contribute regulatory compliance expertise, legal recognition requirements, data governance obligations, and official acceptance criteria that determine whether blockchain credentialing systems achieve formal recognition by flag states and port state control authorities whose validation is essential for international operational legitimacy. The third stakeholder group consists of shipping company training managers including crewing department directors responsible for seafarer recruitment and human resource management, competency assessment coordinators who evaluate crew capabilities and training needs, and seafarer recruitment specialists who source qualified personnel and verify credentials during hiring processes. These industry practitioners provide employer perspectives regarding verification efficiency requirements, integration with crew management systems, return-on-investment considerations justifying technology adoption, and practical operational factors affecting acceptance and utilization of blockchain credentialing in commercial maritime contexts. Purposive sampling techniques ensure participant selection based on relevant expertise, professional experience exceeding twelve years in respective domains, and direct involvement in maritime credentialing processes or educational technology initiatives, thereby maximizing data quality and ensuring participants possess sufficient knowledge to provide informed perspectives on complex technical and institutional issues [24]. The total sample comprises thirty-six participants distributed equally across the three stakeholder categories, with geographic diversity spanning major maritime nations including Philippines, India, China, Greece, Norway, and United Kingdom representing varied regulatory frameworks, educational system characteristics, and technological infrastructure levels to enhance framework generalizability and applicability across different maritime education contexts.

The research instrument development process involved designing semi-structured interview protocols and focus group discussion guides systematically exploring six primary thematic domains identified through preliminary literature review and expert consultation as critical to blockchain credentialing implementation success. The independent variables examined in this investigation include stakeholder category affiliation, geographic region, institutional type characteristics, prior blockchain technology exposure, and current credentialing system experience, factors hypothesized to influence perspectives regarding implementation priorities, adoption barriers, and governance preferences. Dependent variables comprise perceived credentialing system deficiencies, identified blockchain solution priorities, anticipated implementation challenges, regulatory compliance concerns, cybersecurity risk assessments, and equity impact considerations, outcomes that collectively inform framework design and validation. The interview protocol incorporates open-ended questions within each thematic domain while maintaining flexibility for participants to elaborate on issues they consider particularly salient or introduce unexpected themes not anticipated in initial protocol design, balancing structured data collection requirements with qualitative inquiry principles valuing emergent insights and participant-directed exploration. The first thematic domain addresses current credentialing system challenges, examining fraud vulnerabilities, verification inefficiencies, cross-jurisdictional recognition barriers, and competency tracking limitations through questions investigating how existing systems constrain operational efficiency, compromise credentialing integrity, or create equity concerns requiring innovative solutions. The second domain explores blockchain technology understanding and perceived benefits, investigating stakeholder familiarity with distributed ledger concepts, anticipated advantages for maritime credentialing applications, and expected improvements over current systems through questions assessing technological literacy levels and benefit perceptions that influence adoption receptivity. The third thematic domain examines implementation requirements and technical specifications, exploring blockchain architecture preferences, interoperability standards, data governance mechanisms, and

smart contract functionalities through questions probing technical design priorities and integration requirements with existing systems. The fourth domain investigates regulatory compliance and legal recognition, examining STCW Convention alignment, data protection obligations, liability frameworks, and governmental acceptance processes through questions addressing regulatory barriers and compliance strategies essential for official system recognition. The fifth thematic domain addresses cybersecurity and privacy concerns, exploring access control mechanisms, data protection approaches, vulnerability assessments, and incident response protocols through questions examining security priorities and risk mitigation requirements ensuring credentialing system trustworthiness. The sixth domain investigates adoption barriers and equity implications, examining implementation costs, digital literacy requirements, technology access constraints, and potential disadvantages for vulnerable seafarer populations through questions that elicit concerns regarding equitable implementation and strategies for ensuring inclusive access that avoids exacerbating existing maritime labor market inequalities.

Data collection proceeded through three sequential phases designed to maximize data richness while enabling iterative refinement of inquiry approaches based on emerging insights and preliminary findings from earlier phases. The initial phase involved individual semi-structured interviews with each participant conducted either in-person at participant workplaces or via secure video conferencing platforms depending on geographic proximity and participant preferences, with sessions lasting approximately 70-90 minutes and being audio-recorded with explicit informed consent following ethical research protocols approved by institutional review boards ensuring participant confidentiality protection and voluntary participation without coercion. Interview transcripts were prepared through professional transcription services employing maritime terminology expertise and reviewed by participants for accuracy verification and approval regarding quotation use, ensuring data validity and ethical compliance throughout the research process while building trust relationships with participants that enhanced subsequent data collection phases and facilitated candid discussion of potentially sensitive topics including regulatory concerns and institutional limitations. The second phase comprised focus group discussions organized separately for each stakeholder category, bringing together participants within each group to facilitate peer interaction, professional debate, and consensus-building regarding implementation priorities and design preferences, thereby generating collective insights potentially obscured in individual interview contexts where participants might hesitate to express views contradicting perceived professional norms or challenging established practices within their organizations. Focus groups proved particularly valuable for exploring technical disagreements regarding blockchain architecture options and governance mechanisms, revealing diversity of expert opinions on contested issues where technological choices involve legitimate trade-offs rather than objectively optimal solutions, while also identifying areas of strong consensus across diverse participants within stakeholder categories suggesting robust findings less susceptible to individual perspective biases. The third data collection phase involved validation workshops where preliminary framework components derived from interview and focus group analysis were presented to mixed stakeholder groups representing all three categories for critical evaluation, refinement suggestions, feasibility assessment, and cross-stakeholder dialogue regarding potential conflicts or integration challenges, enabling participatory framework development that enhances practical applicability, stakeholder ownership, and implementation likelihood by incorporating diverse perspectives from early design stages and building shared understanding across stakeholder boundaries that facilitates subsequent coordination during actual implementation processes.

Data analysis employed rigorous thematic analysis methodologies following established qualitative research protocols that systematically identify, analyze, and report patterns within qualitative datasets while maintaining analytical transparency, interpretive validity, and evidentiary grounding that connects findings to empirical data rather than researcher preconceptions or theoretical expectations [25]. The analysis process began with data familiarization through repeated reading of interview transcripts and focus group notes while documenting preliminary impressions and potential themes, during which initial codes were generated capturing specific data segments relevant to research questions and emergent

themes not anticipated in initial protocol design reflecting participant knowledge and concerns extending beyond existing literature. Initial coding employed both deductive approaches applying pre-defined codes derived from theoretical frameworks regarding technology adoption, credentialing systems, and blockchain applications and inductive approaches remaining open to unexpected themes emerging from participant narratives reflecting practitioner expertise and implementation experiences not yet documented in academic research. Codes were then organized into potential themes representing broader patterns of meaning across the dataset, with themes refined through iterative review processes assessing internal homogeneity within themes and external heterogeneity between themes to ensure coherent, distinctive analytical categories facilitating clear interpretation and communication of findings to academic and practitioner audiences. Two primary overarching themes emerged from this analysis process: technological and institutional implementation requirements encompassing blockchain architecture specifications, interoperability standards, regulatory compliance mechanisms, and integration with existing credentialing systems; and adoption dynamics and equity considerations addressing stakeholder acceptance factors, implementation barriers, cost-benefit perceptions, cybersecurity concerns, and equitable access requirements ensuring inclusive participation across diverse maritime contexts. Within these overarching themes, multiple sub-themes were identified addressing specific aspects of implementation challenges and opportunities including fraud prevention mechanisms, verification efficiency improvements, competency tracking innovations, regulatory recognition strategies, cybersecurity protection approaches, and digital divide mitigation interventions. Cross-group comparative analysis examined similarities and differences in perspectives across the three stakeholder categories, revealing both shared priorities transcending stakeholder boundaries including credentialing integrity and verification efficiency and distinctive concerns reflecting different organizational missions with educators emphasizing pedagogical integrity, regulators prioritizing legal compliance, and employers focusing on operational efficiency and cost-effectiveness. Finally, narrative synthesis techniques were employed to develop cohesive interpretive accounts linking empirical findings to theoretical concepts and practical implications, constructing explanatory narratives that transform disaggregated data into actionable insights suitable for framework development, policy formulation, and technology implementation guidance addressing real-world credentialing system transformation challenges facing maritime education and certification communities globally.

3. RESULTS AND DISCUSSION

3.1 Results and Analysis

The qualitative analysis of stakeholder perspectives reveals strong convergence regarding current credentialing system deficiencies and blockchain technology's potential benefits, coupled with substantial concerns regarding implementation complexity, regulatory uncertainty, and equity implications requiring careful attention in framework design. Thematic analysis identified five primary challenge domains consistently emphasized across stakeholder groups: credentialing fraud and verification inefficiency in current systems, blockchain technical architecture and interoperability requirements, regulatory compliance and legal recognition mechanisms, cybersecurity and data privacy protection, and adoption barriers and digital divide considerations. Within the current system deficiencies domain, 92% of participants identified certification fraud as a critical problem undermining maritime safety and creating unfair competition, with certification authority administrators reporting that 5-8% of credentials examined during port state control inspections exhibit irregularities or suspected forgery, maritime education experts noting fraudulent training center operations issuing certificates without adequate instruction delivery, and shipping company managers recounting incidents where seafarers with falsified credentials demonstrated inadequate competencies during emergency situations creating safety risks and operational disruptions. Additionally, 87% of participants emphasized verification inefficiency as a major constraint, with cross-jurisdictional credential verification currently requiring 2-6 weeks involving manual document transmission, authentication requests to foreign administrations, and administrative processes that delay seafarer employment, increase recruitment costs, and reduce labor

market flexibility particularly affecting seafarers from developing nations whose credentials face greater scrutiny and verification delays compared to seafarers from established maritime nations with recognized credentialing systems.

Regarding blockchain solution potential, stakeholder perspectives demonstrated sophisticated understanding of distributed ledger benefits while revealing important variations in prioritization of specific advantages across stakeholder categories. Figure 1 presents the distribution of perceived blockchain benefits ranked by stakeholder groups, showing that while fraud prevention received highest overall priority (8.9/10), verification efficiency improvements ranked slightly higher among shipping companies (9.3/10) compared to certification authorities (8.7/10) and education institutions (8.4/10), reflecting employers' particular sensitivity to recruitment process delays and administrative costs that efficient verification could substantially reduce. Interestingly, competency tracking capabilities received relatively high scores from education experts (8.1/10) who emphasized potential for integrating blockchain credentials with learning management systems and simulation training platforms enabling continuous professional development documentation, while this feature received lower prioritization from certification authorities (6.8/10) who expressed concerns regarding complexity and departure from established periodic renewal practices creating potential regulatory compliance uncertainties.

Technical architecture preferences and interoperability requirements emerged as complex domains where stakeholder perspectives revealed substantial diversity reflecting legitimate trade-offs between competing design objectives including decentralization versus performance, transparency versus privacy, and accessibility versus security. Table 1 presents comprehensive analysis of blockchain architecture preferences categorized by key design dimensions including consensus mechanism, network structure, data governance, and smart contract functionality, scored based on stakeholder assessments and weighted by implementation priority. The analysis reveals that permissioned blockchain architectures received significantly higher preference (76%) compared to fully public blockchains (24%), with participants emphasizing that regulatory compliance, data protection requirements, and cybersecurity considerations necessitate controlled access mechanisms where verified authorities manage network participation rather than open systems where any entity can join and validate transactions. However, important disagreements emerged regarding optimal governance models, with certification authorities preferring centralized governance by maritime administrations ensuring regulatory control and legal accountability (68% within this stakeholder group), while education institutions and shipping companies expressed stronger support for distributed governance involving multiple stakeholder categories to prevent regulatory capture and ensure system responsiveness to diverse user needs rather than solely governmental priorities.

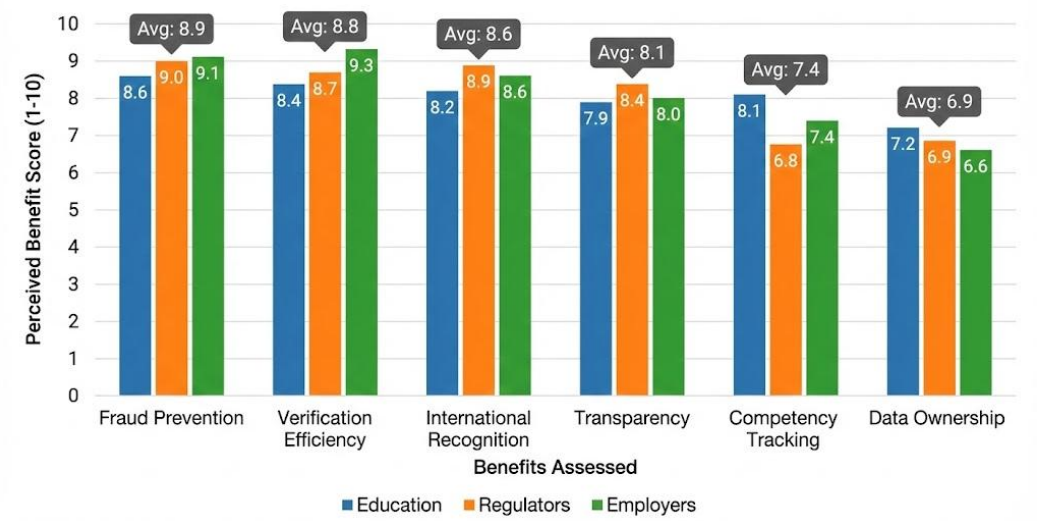

Figure 1. Perceived Blockchain Benefits By Stakeholder Category (Ranked 1-10 Scale)

Table 1. Blockchain Architecture Preferences By Design Dimension

Architecture Dimension	Option 1	Support %	Option 2	Support %	Priority Weight
Network Structure	Permissioned	76%	Public	24%	9.2
Consensus Mechanism	Proof of Authority	58%	Proof of Stake	42%	8.7
Data Governance	Distributed	52%	Centralized	48%	9.0
Smart Contracts	Enabled	83%	Limited	17%	8.4
Interoperability	Priority	91%	Secondary	9%	9.5
Data Privacy	Selective Disclosure	79%	Full Transparency	21%	8.9
Scalability Approach	Layer-2 Solutions	64%	Sharding	36%	8.1

Note: Support percentages represent stakeholder preferences; Priority weight scored 1-10 based on implementation criticality

Regulatory compliance and legal recognition constituted the third major challenge domain, where stakeholders identified substantial uncertainties and barriers requiring explicit attention through coordinated efforts among maritime administrations, industry associations, and international organizations. Participants universally emphasized that blockchain credentialing systems require formal recognition by flag state administrations and port state control authorities to achieve operational legitimacy, yet most maritime regulations currently specify paper certificate requirements or prescribe particular digital signature technologies not necessarily compatible with blockchain architectures, creating legal ambiguity that conservative regulatory authorities might interpret as prohibiting blockchain credentials despite absence of explicit prohibitions. Furthermore, international recognition requires either amendments to STCW Convention provisions explicitly endorsing blockchain credentials or development of extensive bilateral recognition agreements among maritime administrations, processes that historically require years or decades to achieve given consensus requirements among IMO member states with varying technological capabilities and regulatory philosophies. Figure 2 presents stakeholder assessments of regulatory compliance challenges ranked by severity and urgency, demonstrating that legal recognition uncertainty (9.1/10) and STCW Convention alignment (8.8/10) constitute the highest priority barriers requiring early attention, while data protection compliance (8.4/10) and liability frameworks (7.9/10), though important, present more manageable challenges addressable through appropriate technical design and contractual arrangements without necessarily requiring international treaty amendments.

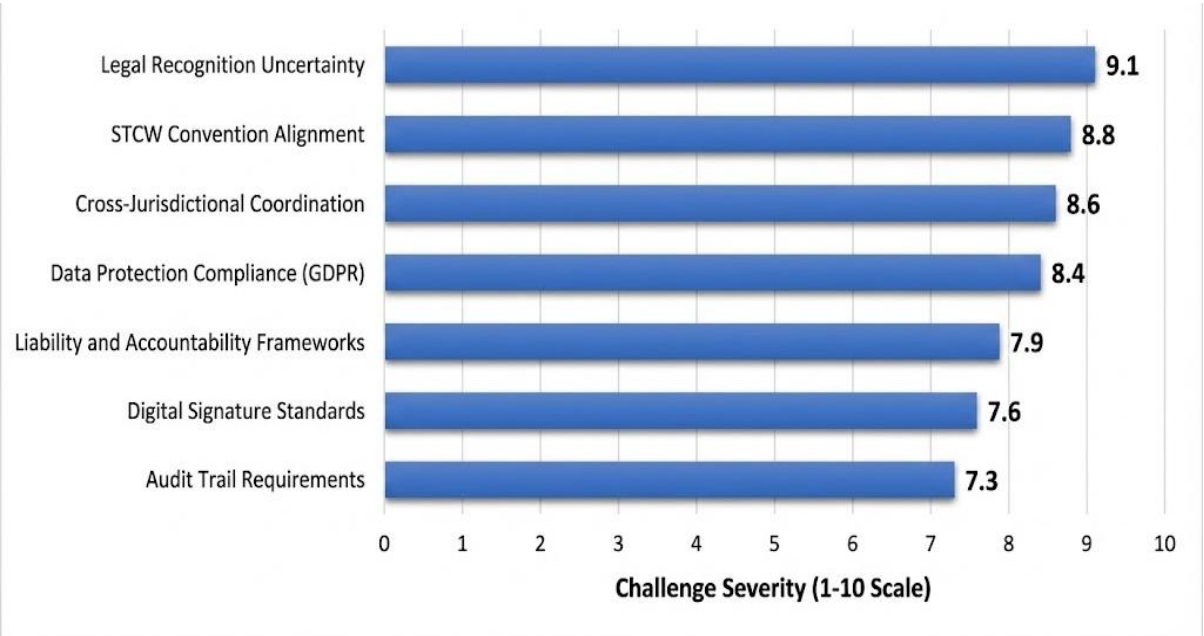

Figure 2. Regulatory Compliance Challenge Assessment

Cybersecurity and data privacy protection emerged as critical concerns where stakeholder perspectives demonstrated sophisticated understanding of blockchain security properties while identifying important vulnerabilities and implementation requirements distinguishing credentialing applications from financial blockchain uses where most security research has focused. Participants noted that while blockchain's distributed architecture eliminates single points of failure characteristic of centralized databases, credentialing systems face distinct threats including private key compromise where seafarers losing cryptographic keys could lose access to their credentials requiring recovery mechanisms potentially reintroducing centralization, smart contract vulnerabilities where coding errors could enable unauthorized credential modifications or data exposure compromising system integrity, and social engineering attacks targeting seafarers with limited cybersecurity awareness who might be deceived into providing access credentials or signing malicious transactions. Additionally, data privacy concerns emerged regarding balance between transparency enabling verification and confidentiality protecting sensitive personal information, with stakeholders emphasizing need for selective disclosure mechanisms allowing seafarers to share specific credential attributes with particular verifiers without exposing complete credential histories to unauthorized parties or creating permanent public records of sensitive information including medical fitness certifications, disciplinary actions, or training performance details that seafarers might reasonably wish to control access to while still enabling legitimate verification needs. Figure 3 presents pie chart analysis of cybersecurity priority areas aggregated across stakeholder groups, showing that access control and authentication (34%) and privacy protection mechanisms (29%) received greatest emphasis, followed by smart contract security (22%) and incident response capabilities (15%), indicating stakeholder recognition that protecting individual seafarer access and personal information constitutes primary security imperative rather than network-level attack prevention which existing blockchain security approaches adequately address.

Adoption barriers and equity implications constituted the fifth critical challenge domain, where analysis revealed substantial concerns regarding implementation costs, technological capacity requirements, and potential disadvantages for vulnerable seafarer populations that could exacerbate existing inequalities in global maritime labor markets if not explicitly addressed through inclusive design and support mechanisms. Implementation cost estimates varied substantially across stakeholder categories, with education institutions projecting initial investments of $50,000-$200,000 per institution for system integration, staff training, and process adaptation, certification authorities estimating national implementation costs of $2-10 million depending on credentialing volume and existing digital infrastructure levels, and shipping companies assessing integration expenses of $20,000-$100,000 for crew management system modifications and verification process automation.

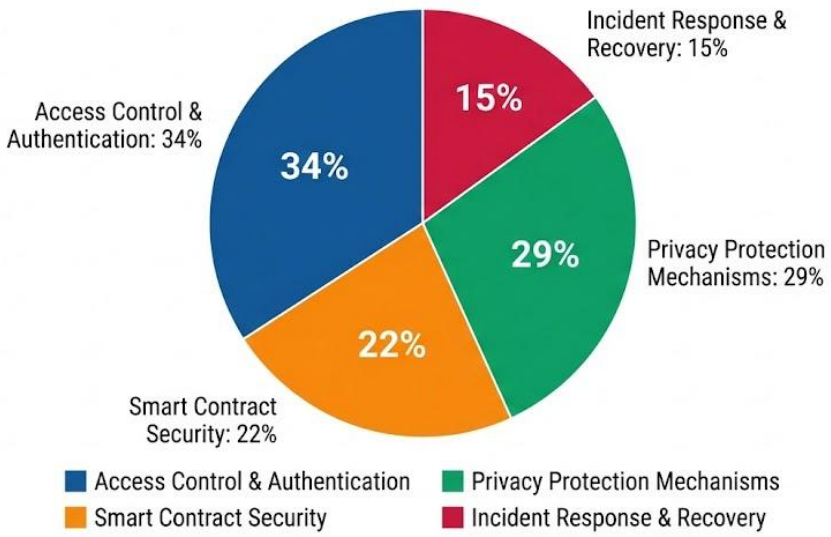

Figure 3. Cybersecurity Priority Areas Distribution

While these costs appear modest relative to overall operational budgets, participants from developing maritime nations emphasized that resource constraints could delay adoption creating two-tier systems where seafarers from technologically advanced nations benefit from efficient blockchain verification while seafarers from resource-limited jurisdictions remain dependent on paper credentials subject to verification delays and fraud suspicions, potentially reducing their competitiveness and employment opportunities despite equivalent qualifications and competencies. Digital literacy concerns emerged prominently, with participants noting that effective blockchain credentialing utilization requires seafarer capabilities in digital wallet management, cryptographic key security, and selective credential disclosure that many current seafarers, particularly older generations and those from limited education backgrounds, may lack without substantial training and support that implementation frameworks must provide to ensure equitable access rather than creating technological barriers excluding vulnerable populations. Table 2 presents comprehensive analysis of adoption barriers categorized by stakeholder group and barrier type, revealing that financial constraints (8.3/10) and technological capacity limitations (8.1/10) constitute primary concerns for education institutions and certification authorities in developing regions, while seafarer digital literacy (7.8/10) and change management resistance (7.4/10) represent greater concerns for employers and regulators concerned about user acceptance and operational transition disruptions.

Table 1. Adoption Barriers Assessment by Stakeholder and Barrier Type]

Barrier Category	Education Institutions	Certification Authorities	Shipping Companies	Average Severity	Implementation Priority
Financial Constraints	8.7	8.4	7.9	8.3	High
Technological Capacity	8.4	8.2	7.6	8.1	High
Seafarer Digital Literacy	7.6	7.3	8.4	7.8	High
Change Management	7.1	7.9	7.3	7.4	Medium
Regulatory Uncertainty	6.8	8.6	6.9	7.4	High
Interoperability Issues	7.3	6.9	7.8	7.3	Medium
Cybersecurity Concerns	7.4	7.6	6.7	7.2	Medium

Note: Severity scored 1-10; Priority indicates urgency for framework attention

The technological and institutional implementation requirements theme that emerged from cross-cutting analysis revealed critical dependencies between technical design choices and institutional acceptance, demonstrating that optimal blockchain architecture cannot be determined purely through technical optimization but must accommodate regulatory requirements, organizational capabilities, and stakeholder preferences that fundamentally shape implementation feasibility. Stakeholders identified three essential implementation requirements that frameworks must address: standards development for interoperability enabling blockchain credentials to interface with existing training management systems, national licensing databases, and employer crew management platforms without requiring complete system replacements that would dramatically increase costs and implementation complexity; governance frameworks establishing clear authority structures, decision-making processes, and accountability mechanisms that satisfy regulatory requirements while distributing control appropriately across stakeholder categories preventing single-entity dominance and ensuring system responsiveness to diverse user needs; and transition strategies managing migration from current paper or centralized digital systems to blockchain architectures without disrupting ongoing credentialing operations or creating validity gaps where credentials issued during transition periods face recognition uncertainties.

Participants emphasized that phased implementation approaches beginning with pilot programs in specific geographic regions or particular credential types could enable iterative learning and refinement before full-scale deployment, reducing risks of costly failures or unintended consequences while building stakeholder confidence through demonstrated successes.

The adoption dynamics and equity considerations theme that emerged from thematic analysis illuminated complex socioeconomic implications of blockchain credentialing transformation extending beyond technical efficiency improvements to encompass fundamental questions regarding maritime labor market structure, seafarer agency and data ownership, and distributional impacts across different seafarer populations and geographic regions. Stakeholders identified both potential positive and negative equity implications, recognizing that outcomes depend critically upon implementation choices and accompanying support mechanisms rather than representing inherent blockchain characteristics. Positive equity potential includes enhanced seafarer mobility through instant verification reducing administrative barriers particularly affecting seafarers from developing nations whose credentials currently face greater scrutiny, improved transparency regarding training quality enabling informed student choices and competitive pressure for education institution quality improvements that could benefit students from regions with historically weak training standards, and increased seafarer control over personal data and credential sharing compared to current systems where administrators control access and seafarers have limited agency regarding information disclosure. Negative equity risks include digital divide exacerbation where technological requirements disadvantage seafarers with limited digital literacy or technology access, implementation cost concentration where early adoption by wealthy maritime nations creates two-tier credentialing systems disadvantaging seafarers from resource-constrained regions, and potential algorithmic bias where automated credential evaluation systems might incorporate discriminatory patterns from historical data perpetuating existing inequalities in maritime labor markets. Table 3 presents stakeholder-identified equity considerations and recommended mitigation strategies, demonstrating sophisticated understanding that equity requires proactive intervention rather than assuming that technological neutrality ensures equitable outcomes.

3.2 Discussion

The research findings illuminate critical dimensions of blockchain-enhanced maritime credentialing implementation that extend theoretical understanding of technology adoption in regulated professional contexts while generating practical insights directly applicable to maritime education policy and credentialing system reform. The strong stakeholder consensus regarding current credentialing deficiencies validates theoretical arguments from institutional economics regarding information asymmetries and adverse selection problems in professional labor markets where credential fraud undermines market efficiency and safety standards [26]. However, the identified concerns regarding blockchain implementation complexity and regulatory uncertainty reveal important limitations in technology-deterministic assumptions that innovative solutions will naturally achieve adoption based solely on technical superiority, instead demonstrating that institutional constraints, organizational capabilities, and stakeholder acceptance fundamentally determine technology diffusion success [27]. This finding suggests that effective implementation frameworks must prioritize stakeholder engagement, regulatory alignment, and capacity building rather than focusing predominantly on technical optimization, potentially requiring extended transition periods and substantial support mechanisms that purely technical literature inadequately considers.

The blockchain architecture preferences revealed in this research directly address gaps in existing maritime credentialing literature that often presents blockchain as singular technology rather than recognizing substantial design variations with different implications for regulatory compliance, operational performance, and equity outcomes. The strong preference for permissioned architectures over public blockchains reflects maritime credentialing's distinct requirements compared to cryptocurrency applications where most blockchain development has focused, with credentialing

demanding regulatory compliance, identity verification, and liability accountability that open anonymous networks cannot provide [28]. The disagreement regarding governance models—centralized governmental control versus distributed multi-stakeholder governance—illuminates fundamental tensions between regulatory authority preferences and industry desires for responsive systems not subject to single-entity control. This finding contributes to broader debates in blockchain governance literature regarding optimal authority distribution in networks requiring coordination among parties with asymmetric power relationships, suggesting that hybrid governance models combining governmental regulatory oversight with industry technical governance might provide practical compromises balancing competing legitimate interests [29].

The regulatory compliance challenges identified in this research, particularly legal recognition uncertainty and STCW Convention alignment requirements, highlight critical implementation barriers that technical blockchain literature often overlooks while legal scholarship addressing credentialing rarely examines blockchain specifically. The finding that existing maritime regulations specifying paper certificates or particular digital signature standards create legal ambiguity regarding blockchain credential recognition demonstrates path dependency effects where established regulatory frameworks developed for previous technologies constrain innovation adoption even absent explicit prohibitions [30]. This finding has important policy implications, suggesting that proactive regulatory reform explicitly endorsing blockchain credentials subject to appropriate standards could significantly accelerate adoption compared to waiting for bottom-up implementation initiatives to establish practices that regulators subsequently validate. The identified need for STCW Convention amendments or extensive bilateral recognition agreements points toward critical roles for international organizations, particularly IMO and International Labour Organization, in facilitating coordination and standard-setting that individual maritime administrations or industry actors cannot achieve independently due to collective action problems and coordination requirements inherent in international credentialing systems.

The cybersecurity and privacy concerns revealed in stakeholder perspectives demonstrate sophisticated understanding distinguishing blockchain security properties from credentialing system security requirements, advancing beyond simplistic claims that blockchain inherently ensures security toward nuanced assessments of threat models and vulnerability sources specific to credentialing applications. The emphasis on access control and privacy protection rather than network-level security reflects recognition that blockchain's distributed architecture addresses database integrity and availability threats but does not automatically solve authentication, authorization, and confidentiality challenges that require additional technical mechanisms including zero-knowledge proofs, selective disclosure protocols, and secure key management systems [31]. The identified concerns regarding smart contract vulnerabilities and social engineering attacks highlight important limitations in blockchain security claims, demonstrating that credentialing systems remain vulnerable to various attack vectors despite distributed ledger benefits and requiring comprehensive security frameworks addressing both technical and human factors rather than assuming technological solutions alone ensure protection. These findings contribute to growing literature on blockchain security beyond cryptocurrency contexts, demonstrating that security requirements vary substantially across applications and that generic blockchain architectures require substantial customization for specific use cases including professional credentialing where privacy, access control, and recovery mechanisms prove critical.

The adoption barriers and equity implications identified in this research address crucial gaps in blockchain literature that predominantly focuses on technological capabilities while inadequately examining distributional impacts and access disparities that significantly affect whether innovations benefit all potential users equitably or exacerbate existing inequalities. The finding that implementation costs, technological capacity limitations, and digital literacy requirements could disadvantage seafarers and institutions from developing regions validates theoretical arguments from technology and development literature emphasizing that digital innovations without explicit equity attention often amplify existing inequalities through differential access to enabling infrastructure, technical knowledge, and

financial resources required for effective participation [32]. The research contributes practical insights by identifying specific equity risks including two-tier credentialing system emergence, digital literacy barriers, and algorithmic bias potential, while also recognizing positive equity possibilities including enhanced mobility, improved transparency, and increased seafarer agency that appropriate implementation frameworks could realize through targeted support mechanisms. These findings demonstrate that equity outcomes depend fundamentally on design choices and accompanying interventions rather than representing inherent technological characteristics, suggesting critical roles for international development assistance, capacity building programs, and inclusive design processes that incorporate vulnerable stakeholder perspectives from early stages rather than treating equity as post-implementation concern.

The research methodology employed in this investigation demonstrates significant strengths in capturing diverse stakeholder perspectives across different organizational contexts and geographic regions while acknowledging inherent limitations in qualitative approaches examining emerging systems with limited operational experience. The purposive sampling strategy ensuring experienced participants from varied contexts enhanced data quality and enabled identification of both universal concerns transcending contexts and context-specific priorities reflecting different institutional environments, providing nuanced understanding unavailable through either technical analysis or stakeholder surveys lacking depth. The iterative data collection incorporating validation workshops enabled participatory framework development enhancing practical applicability and building stakeholder ownership that facilitates subsequent implementation by ensuring frameworks reflect real-world requirements rather than solely researcher perspectives. However, the research recognizes limitations regarding predictive validity, as stakeholder perspectives regarding blockchain credentialing futures necessarily involve uncertainty and speculation that operational experience alone can fully validate or refute. Future research should complement this qualitative investigation through pilot implementation projects, quantitative cost-benefit analyses, and longitudinal studies tracking actual adoption processes as blockchain credentialing initiatives progress from conceptual proposals through operational deployment.

The practical implications of these findings extend across multiple decision-making domains affecting maritime education and credentialing system development. For maritime education institutions, the research demonstrates that blockchain credentialing adoption requires not merely technological investment but also pedagogical integration ensuring credential data flows naturally from learning management systems and simulation training platforms, suggesting priorities for educational technology development and instructor training that prepare institutions for credentialing transformation. For certification authorities, the findings indicate that proactive engagement in blockchain standard development and pilot programs could position progressive maritime administrations as credentialing innovation leaders while ensuring regulatory requirements shape technical development rather than constraining adoption of systems developed without regulatory input. For international organizations including IMO and ILO, the research highlights critical needs for international coordination, standard development, and regulatory guidance that facilitate blockchain credentialing adoption while ensuring interoperability, equity, and safety protection across diverse maritime contexts. For seafarer organizations and labor unions, the findings suggest important advocacy priorities including seafarer data ownership rights, privacy protection mechanisms, and capacity building support ensuring that credentialing transformation benefits seafarers through enhanced mobility and reduced verification barriers rather than creating new technological obstacles or privacy vulnerabilities disadvantaging workers relative to employers and authorities.

4. CONCLUSION

This research develops and validates a comprehensive Blockchain-Enhanced Maritime Education Ecosystem framework addressing critical credentialing integrity, verification efficiency, and workforce mobility challenges facing the global maritime industry amid persistent seafarer shortages. The

investigation reveals strong stakeholder consensus regarding blockchain technology's potential benefits for fraud prevention and verification acceleration while identifying substantial implementation barriers including regulatory uncertainty, cybersecurity concerns, adoption costs, and equity implications requiring systematic attention. Key findings demonstrate that effective blockchain credentialing requires permissioned architectures with distributed governance, proactive regulatory reform enabling legal recognition, comprehensive cybersecurity frameworks protecting privacy and access, and targeted support mechanisms ensuring equitable access across diverse maritime contexts. The framework contributes actionable pathways for maritime stakeholders, offering evidence-based implementation strategies balancing technological innovation with regulatory compliance, operational requirements, and equity considerations while supporting urgent workforce development needs essential for maritime industry sustainability and safety.

REFERENCES

[1] International Chamber of Shipping and BIMCO, *Seafarer Workforce Report 2021*. London, UK: ICS, 2021.
[2] BIMCO and International Chamber of Shipping, *The Global Supply and Demand for Seafarers*. Bagsværd, Denmark: BIMCO, 2021.
[3] International Labour Organization, *Maritime Labour Convention Compliance Report 2022*. Geneva, Switzerland: ILO, 2022.
[4] International Maritime Organization, *International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978, as amended*. London, UK: IMO, 2017.
[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[6] European Maritime Safety Agency, *Annual Overview of Marine Casualties and Incidents 2023*. Lisbon, Portugal: EMSA, 2023.
[7] M. Goulielmos and A. A. Goulielmos, "The use of ICT in maritime education and training: The case of the Greek Marine Academies," *WMU Journal of Maritime Affairs*, vol. 19, pp. 127-145, 2020.
[8] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media, 2015.
[9] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016.
[10] A. Kosba et al., "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symposium on Security and Privacy*, San Jose, CA, 2016, pp. 839-858.
[11] M. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Software*, vol. 35, no. 4, pp. 95-99, 2018.
[12] M. Q. Mejia Jr. et al., "Towards a voluntary STCW certification scheme: A policy proposal," *WMU Journal of Maritime Affairs*, vol. 19, pp. 381-400, 2020.
[13] H. Zade et al., "Blockchain for global maritime training and certification system," in *Proc. Int. Conf. on Advanced Communication Technology*, Pyeongchang, Korea, 2018, pp. 698-703.
[14] S. Progoulakis and M. Theotokas, "Maritime education and training in the digital era: Findings from a systematic review," *WMU Journal of Maritime Affairs*, vol. 21, pp. 335-367, 2022.
[15] Z. L. Yang et al., "Realising advanced maritime safety management by using maritime simulator centres," *WMU Journal of Maritime Affairs*, vol. 13, pp. 203-224, 2014.
[16] J. Yli-Huumo et al., "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, e0163477, 2016.
[17] M. Turkanović et al., "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112-5127, 2018.
[18] A. Grech and A. F. Camilleri, *Blockchain in Education*. Luxembourg: Publications Office of the European Union, 2017.
[19] J. Hetherington et al., "Safety in shipping: The human element," *Journal of Safety Research*, vol. 37, no. 4, pp. 401-411, 2006.
[20] United Nations, *Transforming Our World: The 2030 Agenda for Sustainable Development*. New York,

NY: UN General Assembly, 2015.
[21] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *Proc. European Conference on Technology Enhanced Learning*, Lyon, France, 2016, pp. 490-496.
[22] J. W. Creswell and C. N. Poth, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, 4th ed. Thousand Oaks, CA: SAGE Publications, 2018.
[23] K. Charmaz, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*, 2nd ed. London, UK: SAGE Publications, 2014.
[24] M. B. Miles, A. M. Huberman, and J. Saldaña, *Qualitative Data Analysis: A Methods Sourcebook*, 3rd ed. Thousand Oaks, CA: SAGE Publications, 2014.
[25] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77-101, 2006.
[26] M. Spence, "Job market signaling," *Quarterly Journal of Economics*, vol. 87, no. 3, pp. 355-374, 1973.
[27] E. M. Rogers, *Diffusion of Innovations*, 5th ed. New York, NY: Free Press, 2003.
[28] V. Buterin, "On public and private blockchains," *Ethereum Blog*, Aug. 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains
[29] P. De Filippi and A. Wright, *Blockchain and the Law: The Rule of Code*. Cambridge, MA: Harvard University Press, 2018.
[30] W. B. Arthur, "Competing technologies, increasing returns, and lock-in by historical events," *Economic Journal*, vol. 99, no. 394, pp. 116-131, 1989.
[31] E. Ben-Sasson et al., "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symposium on Security and Privacy*, San Jose, CA, 2014, pp. 459-474.
[32] World Bank, *World Development Report 2016: Digital Dividends*. Washington, DC: World Bank, 2016.