IET Intelligent Transport Systems

WILEY

The Institution of Engineering and Technology

ORIGINAL RESEARCH OPEN ACCESS

Investigation of Blockchain for Cybersecurity in Maritime Autonomous Surface Ships

Ian Hamilton | Dante Ben Matellini | Chia-Hsun Chang

Liverpool Logistics, Offshore and Marine Research Institute (LOOM) and School of Engineering, Liverpool John Moores University, Liverpool, UK

Correspondence: Chia-Hsun Chang (c.chang@ljmu.ac.uk)

Received: 13 August 2025 | **Revised:** 4 January 2026 | **Accepted:** 18 January 2026

ABSTRACT

As Maritime Autonomous Surface Ships (MASS) become increasingly prevalent, cybersecurity emerges as a critical challenge due to the reliance on interconnected digital systems. Blockchain technology offers promising solutions to enhance data security, transparency and operational resilience. However, the high energy consumption of blockchain creates a dilemma for the maritime sector to meet low-carbon and sustainability targets. Identifying strategies balancing energy consumption with the security benefits brought by blockchain is therefore essential. This research aims to examine the integration of blockchain to improve cybersecurity, operational efficiency and data integrity in MASS. The study contributes to an integration of a literature review, strengths, weaknesses, opportunities, threats (SWOT), threats, opportunities, weaknesses, strengths (TOWS) analysis with a practitioner survey, providing strategic insights into blockchain to strengthen cybersecurity frameworks for MASS. Findings of SWOT-TOWS highlight blockchain's potential to improve cybersecurity and automate functions through smart contracts, while identifying significant barriers such as scalability, energy consumption, etc. Survey results show strong industry support for blockchain's role in enhancing cybersecurity, particularly in communication and automation systems. Respondents emphasised the importance of protocols and transaction speed. The study concludes with strategic recommendations and policy considerations to guide effective blockchain integration in MASS.

1 | Introduction

Interest in the development and deployment of Maritime Autonomous Surface Ships (MASS) is rapidly growing, with these vessels operating under varying levels of autonomy. Numerous studies have highlighted the potential of MASS to enhance operational efficiency, productivity and safety [1, 2]. For example, Tao et al. [3] conducted a systematic review of hazard identification and risk analysis methodologies, emphasising the safety challenges that must be addressed alongside the operational benefits.

At the same time, blockchain technology holds significant potential to transform the maritime industry, with early successes already evident in maritime logistics. Blockchain technology is a decentralised digital ledger system that records transactions securely across a network of computers. Each record, or 'block,' is linked to the previous one in a way that makes the chain of data tamper-resistant and highly transparent [4]. One of the key advantages of blockchain in the context of MASS lies in its ability to facilitate secure and transparent communication and data exchange [5]. By maintaining tamper-proof records through an immutable ledger, blockchain ensures data integrity

Abbreviations: AHP, Analytic Hierarchy Process; AI, Artificial Intelligence; BIMCO, Baltic and International Maritime Council; COLREGS, Convention on the International Regulations for Preventing Collisions at Sea; DPoS, Delegated Proof of Stake (consensus algorithm); IACS, International Association of Classification Societies; IMO, International Maritime Organisation; IoT, Internet of Things; KMO, Kaiser-Meyer-Olkin (test for validity); LiDAR, Light Detection and Ranging; MASS, Maritime Autonomous Surface Ships; MET, Maritime Education and Training; OT, Operational Technology; PoS, Proof of Stake (blockchain consensus algorithm); PoW, Proof of Work (blockchain consensus algorithm); SMS, Safety Management Systems; SVM, Support Vector Machine; SWOT, Strengths, Weaknesses, Opportunities, Threats; TOPSIS, Technique for Order Preference by Similarity to Ideal Solution; TOWS, Threats, Opportunities, Weaknesses, Strengths.

and authenticity. Both of these factors are critical to the safety and efficiency of maritime operations [6]. Blockchain also enables secure interaction among autonomous ships using smart contracts, self-executing agreements embedded with predefined rules such as those derived from the Convention on the International Regulations for Preventing Collisions at Sea (COLREGS). This facilitates coordinated decision-making between vessels, reducing the need for human intervention and enhancing both safety and operational efficiency [7].

A notable example is provided by Chen et al. [8], who demonstrated how smart contracts can be applied to validate collision data and generate avoidance strategies, supporting safe navigation in complex maritime environments. Blockchain also enhances traceability and transparency across operations by recording all activities on an immutable ledger. Furthermore, Adam et al. [9] demonstrate that there are benefits in using blockchain for dispute resolution within the bunker industry. All these applications show that blockchains can provide a reliable audit trail, which is valuable for accident investigations, cargo management and overall maritime governance. [6].

Despite these promising developments, several challenges hinder the broader adoption of blockchain in autonomous maritime systems. These include the immaturity of the technology, lack of standardisation, scalability concerns and the high energy consumption of blockchain platforms—all of which are particularly problematic for the lightweight systems required in MASS [4, 10, 11]. Although there are successful blockchain applications in maritime domains such as port logistics, supply chains, marine insurance and classification societies, research specifically focused on MASS remains limited. Given the growing importance of autonomy in maritime operations, this represents a significant research gap.

To address this, further investigation is needed into the potential benefits, challenges and practical applications of integrating blockchain technology into MASS, particularly concerning economic, environmental and social sustainability [12]. Such research will not only advance academic understanding but also contribute to the development of safer, more efficient and more sustainable maritime transport systems. Accordingly, this study aims to evaluate the feasibility and advantages of employing blockchain technology to enhance the integrity, reliability and resilience of cybersecurity systems within the context of MASS.

2 | Critical Literature Review

This review evaluates the technological, security and environmental aspects of blockchain implementation in MASS using current academic and regulatory sources. The discussion is organised into four thematic areas: autonomous vessel systems, cybersecurity risks, blockchain applications and sustainability.

2.1 | Maritime Autonomous Surface Ships

Maritime Autonomous Surface Ships (MASS) are expected to significantly influence maritime operations. Research into the integration of emerging technologies, such as artificial intelligence (AI), deep learning and blockchain, is accelerating the advancement and success of related projects. MASS refers to vessels that can navigate and operate autonomously with varying degrees of human intervention. Their adoption is driven by the promise of enhanced safety, improved operational efficiency and increased environmental sustainability [13].

The International Maritime Organisation (IMO) has outlined four distinct levels of autonomy for MASS in Circular MSC.1/Circ.1638:

- Degree 1 features ships with automated processes and decision support, where some operations are automated, but a crew remains onboard for supervision.
- Degree 2 involves remotely controlled ships, which require a crew on board for operational support but can be controlled remotely.
- Degree 3 represents remotely controlled ships without a crew onboard, where all operations are controlled remotely.
- Degree 4 describes fully autonomous ships, capable of making decisions and performing actions independently, with no onboard crew.

This classification is non-hierarchical, meaning a single vessel may shift between different autonomy levels during a voyage, depending on operational needs.

Global attention has focused on the development of MASS, with substantial efforts underway to address technical challenges and maximise its benefits. For instance, Chang et al. [1] addressed MASS risk assessment by identifying and prioritising the potential operational hazards, other risk assessment related studies can be found in a review work by Yuzui and Kaneko [14]. From the maritime education and training (MET) perspective, Belabyad et al. [15] reviewed the research related to MASS MET and further identified a list of skills and competencies for operating MASS. In addition, Belabyad et al. [16] further ranked the importance of the identified skills and competencies.

One of the primary advantages of MASS is enhanced safety. By removing or reducing the crew from a ship, the inherent risks associated with human error are reduced. MASS utilises advanced technologies such as AI-powered collision avoidance systems, real-time monitoring and predictive maintenance informed by deep learning and prognostics [17]. For instance, LiDAR-based systems have been used for ship detection and tracking, supporting safe navigation and collision avoidance (Xie, Nanlal and Liu [18]). Situation-aware tools, such as knowledge maps, can be integrated with decision-making models. This enables MASS to autonomously assess navigational hazards. As a result, vessels can perform avoidance manoeuvres in real time [19]. Risk-based path planning algorithms also play a key role in minimising the risk of accidents, including collisions and groundings [20].

In addition to safety, MASS can also improve operational efficiency. Autonomous ships use advanced algorithms to analyse real-time data. This lets them optimise routes, speed and fuel use. These improvements lead to cost savings, reduced emissions and better performance. Such optimisation translates into cost savings, lower emissions, and enhanced performance [21]. Blockchain technology in MASS strengthens transparency and traceability, particularly in supply chain management [6]. By securely recording transactions and cargo data on a tamper-proof ledger, blockchain minimises the risk of fraud or data tampering [4]. However, despite these advantages, the widespread adoption of MASS faces several challenges. Establishing robust legal and regulatory frameworks is critical to ensuring that MASS complies with international maritime laws while addressing emerging risks and technological demands [2]. Current efforts focus on developing standards tailored to MASS, particularly in areas such as cybersecurity, safety protocols and emergency response procedures [22]. As autonomous shipping evolves, public administration for autonomous shipping is evolving to accommodate the unique requirements of MASS, emphasising the need for agile responses to new threats and operational changes [23]. Understanding the potential risks associated with MASS operations is vital for creating effective safety regulations and hazard mitigation strategies [3].

2.2 | Cybersecurity Challenges in MASS

As the technical capabilities of MASS continue to evolve, their increasing reliance on interconnected digital systems introduces significant cybersecurity vulnerabilities. These risks are further amplified by internet connectivity, which exposes MASS to a wider range of cyber threats [24]. Various studies have examined the cybersecurity risks associated with MASS and have proposed frameworks to evaluate and mitigate them. One notable example is the Model-based Framework for Maritime Cyber-Risk Assessment (MaCRA) proposed by Tam and Jones [25]. Model-based approaches such as the MaCRA framework and emerging blockchain-enabled risk assessment models provide comprehensive methodologies for assessing maritime cyber risks by considering system configurations, user interactions and evolving operational environments [26]. However, vulnerabilities persist due to ineffective policies and company procedures, outdated software, insufficient cybersecurity protections in legacy operational technology (OT) systems, lack or limited monitoring and a lack of specialised expertise among maritime staff [27–29]. DNV's 'Maritime Cyber Priority 2024/25' report highlights increased cyber risk appetite within the industry and emphasises the integration of OT security barriers, a trend echoed by recent blockchain-based anomaly detection frameworks for autonomous ships [26].

The critical nature of MASS within the broader maritime infrastructure means that their safety and security are the most important issue. Recognising this, the European Directive 'EU 2016–679' recognises the vulnerability of cyber-enabled autonomous ships and emphasises the need for their protection against cyber threats [30, 31]. One increasingly significant threat involves deception attacks such as GPS spoofing, which manipulates navigational or communication signals, disrupting vessel control and compromising safety [32].

Addressing these threats requires the development of advanced control schemes and detection mechanisms. Recent research has proposed several solutions, including self-triggered neural network controllers and event-triggered adaptive control frameworks [33], and recent blockchain-driven protocols for anomaly management and secure identity authentication [26]. However, many of these approaches primarily focus on maintaining closed-loop stability and often neglect spatial and communication security. To overcome these limitations, integrating finite-time stability techniques, fuzzy logic and resilient communication protocols is essential for strengthening cybersecurity in MASS [34]. Updated IMO guidelines (MSC-FAL.1/Circ.3/Rev.3), IACS requirements (E26, E27) and the latest LR and DNV trends now require cyber risk management as a core operating principle [35].

The need to adapt existing risk models to reflect the unique characteristics of maritime autonomous systems is increasingly recognised. Cybersecurity protocols must evolve alongside emerging threats, incorporating frequent risk assessments and aligning with global trends. In this regard, the IMO has played a key role by issuing interim guidelines on maritime cyber risk management, while Lloyd's Register's 'Global Maritime Trends 2025 Barometer' stresses the importance of harmonised legislative standards to facilitate industry-wide digital transformation [36]. The IMO guidance is further supported by industry standards such as the BIMCO cybersecurity guidelines [37], which highlight 8 core areas of concern in MASS systems: (1) Cargo and loading management systems, (2) Bridge systems, (3) Propulsion and machinery management and power control systems, (4) Access control systems, (5) Passenger servicing and management systems, (6) Passenger facing public networks, (7) Administrative and crew welfare systems and (8) Communication systems. Tusher et al. [38] further explored the threats to autonomous ships, proposing a framework for risk assessment but offering limited practical recommendations for mitigation. Wang et al. [10] identified the root causes of MASS vulnerabilities and categorised them into three main types: lack of identity authentication, message authentication and trust censorship. These vulnerabilities can potentially be addressed by introducing blockchain into communication systems.

Blockchain technology has gained increasing attention as a potential cybersecurity safeguard for MASS. However, Ghosh et al. [39] highlight the challenges of cross-network blockchain interoperability, particularly with regard to establishing trust across chains. Their study proposes the use of a third-party distributed identity registry but warns that this approach could increase reliance on external communication networks, adding further vulnerability and latency to the process. Instead, a standardised blockchain communication protocol within the maritime sector could significantly reduce these risks.

Given these cybersecurity risks, more interest has been shown in blockchain technology as a potential safeguard [40]. The following section explores how blockchain can address these vulnerabilities and enhance trust, transparency and resilience in MASS operations.

2.3 | The Potential of Blockchain Technology in MASS

Blockchain technology has gained significant attention and has shown promising application prospects across various sectors, including the maritime industry. Blockchain provides a decentralised, immutable ledger and transparent data handling, making it particularly suitable for enhancing the integrity, trust and resilience of MASS.

The distributed nature of blockchain eliminates the need for a central authority, thus reducing the risk of single points of failure and security breaches [41, 42]. Each transaction or data update is recorded in a block, which is linked to the previous blocks through cryptographic hashes, creating a secure, tamper-evident chain. This ensures that any unauthorised modification would require altering all subsequent blocks, a virtually impossible task, thereby safeguarding data integrity [43].

Blockchain technology offers several benefits in the context of autonomous maritime vehicles. Notably, it enhances the security and integrity of critical operational data such as sensor readings, performance metrics and software updates by ensuring these records remain tamper-proof and authentic across interconnected systems [6, 44]. In addition, blockchain supports decentralised decision-making processes through smart contracts, enabling autonomous systems to respond reliably and transparently to complex operational scenarios. Secure, decentralised communication is another crucial advantage, as blockchain facilitates peer-to-peer authentication and trust-building among autonomous vessels and their IoT devices capabilities that are increasingly essential for safe and coordinated maritime operations [6, 44].

Blockchain's utility extends beyond vessel-to-vessel interactions to broader maritime logistics. For instance, smart contracts can automate secure transactions between MASS and other entities, such as ports, shipping companies and regulatory authorities [45]. Smart contracts can ensure that all parties involved in a transaction adhere to the agreed-upon terms and conditions, reducing the risk of fraud or malicious activities [46].

Blockchain technology significantly enhances the traceability and provenance of data in MASS operations. Its transparent and immutable ledger creates a verifiable record of all data exchanges and transactions, which is crucial for tracking cargo, vessel movements and ensuring compliance with international regulations. These tamper-proof records foster accountability, support reliable audit trails and build trust among industry participants [6].

Beyond operational benefits, blockchain can also contribute to maritime sustainability. By reducing reliance on paper-based processes and enabling real-time visibility across logistics chains, blockchain can streamline workflows, reduce administrative costs and lower environmental impact. It can also facilitate the implementation of sustainable practices such as carbon footprint tracking and emission reduction initiatives, by providing a transparent and auditable platform for data collection and verification [12].

Despite these advantages, several challenges remain that may hinder blockchain's widespread adoption in MASS. The scalability challenge arises from the massive volume of data generated by MASS and the need for efficient consensus algorithms to validate transactions [43]. Security concerns include vulnerability to 51% attacks, double-spending and vulnerabilities in poorly designed smart contracts [47].

Although recent studies have explored the technical performance and theoretical characteristics of blockchain systems, much of this literature remains generalised and sector-agnostic. Limited attention has been paid to the specific cybersecurity requirements, operational constraints and regulatory context of MASS. In particular, there is a lack of research that integrates blockchain's technical capabilities with industry-driven strategic assessment frameworks. This study addresses this gap by examining blockchain adoption explicitly within the MASS cybersecurity context and by incorporating practitioner perspectives to support real-world applicability.

2.4 | Environmental Implications and Adoption Challenges of Blockchain in MASS

While blockchain offers significant benefits for enhancing the security, transparency and efficiency of MASS, its deployment carries important environmental and operational implications. The decentralised nature of blockchain increases trust and privacy in autonomous systems, but it also comes with considerable energy demands, particularly in systems reliant on consensus mechanisms such as Proof of Work (PoW). The computational power required to validate transactions and maintain blockchain operations contributes to increased energy consumption and, consequently, a larger carbon footprint [48].

Not all blockchain technologies are created equal. While PoW is widely criticised for its inefficiency and environmental impact, emerging consensus models such as Proof of Stake (PoS) and other energy-efficient protocols offer promising alternatives. Bada et al. [49] highlight that newer models can significantly reduce energy usage compared to traditional approaches. As the industry evolves, the selection of appropriate consensus mechanisms will be key to balancing blockchain's security benefits with environmental sustainability.

To ensure alignment with global sustainability objectives, it is essential to develop and enforce environmental standards and regulations governing the use of blockchain in autonomous vehicles. Such frameworks can guide the responsible deployment of blockchain technologies in line with green goals.

The maritime industry, like many other sectors, is undergoing a broader transition toward greener, more sustainable practices. This includes a shift to low-emission power sources and efforts to improve energy efficiency. Blockchain, if thoughtfully implemented, can support these efforts by streamlining operations, reducing administrative overhead and enhancing security [50]. Truby [51] notes the challenges of regulating blockchain's energy use in sectors like cryptocurrency; however, the maritime domain may be better equipped to manage these concerns with its structured regulatory environment [11].

Operationally, blockchain presents both opportunities and risks for the maritime sector. As a service-based industry primarily focused on transport, maritime operations could benefit from blockchain's potential to reduce paperwork, improve data

TABLE 1 | SWOT-TOWS analysis.

		External	
Internal		**Opportunities (positive)**	**Threats (negative)**
	Strengths (positive)	**SO strategies** Leverage internal strengths to capitalise on external opportunities identified in the environment.	**ST strategies** Apply existing strengths to defend against or reduce the impact of external threats.
	Weaknesses (negative)	**WO strategies** Address internal weaknesses by taking advantage of external opportunities.	**WT strategies** Minimise weaknesses to avoid vulnerability to external threats.

integrity and increase overall transparency [11]. However, successful adoption depends heavily on the level of integration across the supply chain. If key stakeholders such as suppliers or customers are not part of the blockchain network, implementation could disrupt coordination and logistics rather than enhance them.

The success of blockchain adoption in maritime also hinges on several critical success factors (CSFs), including adequate financial investment, specialised staff training, regulatory flexibility, community and management support and industry-specific expertise [11]. Historically, the maritime sector has been cautious in adopting transformative digital technologies, partly due to the complexity of its operations and the significant cultural change required. Nonetheless, as blockchain matures, it may play a pivotal role in advancing the digitalisation and sustainability of maritime logistics.

Brothwell [52] offers an apt analogy, comparing blockchain networks to trains that consume the same energy regardless of passenger count. By standardising practices and increasing the number of transactions per block, the industry can optimise blockchain's efficiency and reduce unnecessary energy waste.

While the environmental implications of blockchain have been widely discussed in the literature, existing studies predominantly approach energy consumption from a technical optimisation or policy perspective. Less attention has been given to how industry stakeholders perceive and prioritise energy efficiency during early-stage adoption of blockchain-enabled systems, particularly in safety-critical and emerging domains such as MASS. This distinction is important, as operational decision-making may prioritise cybersecurity performance and system reliability over environmental considerations in the initial deployment phases. The present study explicitly examines this perception gap by combining strategic analysis with stakeholder survey evidence.

3 | Methodology

To evaluate the feasibility of using blockchain technology in enhancing cybersecurity for MASS, this study employs a hybrid methodological approach, combining SWOT and TOWS analyses, and further validates the results with a questionnaire.

The SWOT framework provides a structured approach to categorise internal capabilities (strengths and weaknesses) and external influences (opportunities and threats) related to blockchain deployment within autonomous maritime systems. This evaluation provides a holistic understanding of blockchain's potential to enhance cybersecurity, operational efficiency and data integrity in the context of MASS. A critical literature review underpins the SWOT analysis. Scholarly and technical sources are systematically collected from the Web of Science and Scopus databases using targeted keywords such as MASS, Blockchain, IMO and International Association of Classification Societies (IACS). The search strategy remains adaptive, allowing for the inclusion of emerging studies and technologies identified throughout the review process. The selected literature focuses on cybersecurity frameworks, maritime regulations, autonomous vessel systems and blockchain innovations to ensure a balanced and current evidence base.

Based on the SWOT findings, the TOWS matrix is applied to develop strategic responses (see Table 1). This includes leveraging strengths to capitalise on external opportunities, addressing or converting weaknesses and developing defensive strategies to counter external threats. Particular attention is given to known implementation barriers such as blockchain's scalability limitations and energy demands, which are analysed in the context of recent advancements in consensus algorithms and green blockchain technologies.

To complement the secondary data, a structured questionnaire was developed and disseminated to maritime industry professionals via professional networking platforms. Professionals in ship management, cybersecurity, and maritime operations were sampled to create a target population that was directly involved in the operational and technical aspects of shipping. A combination of seagoing engineers, cybersecurity experts and operational managers made up the survey's sample size of 41 respondents. The Cronbach's alpha coefficient was calculated at 0.742, which showed strong internal consistency and exceeded the recognised threshold of 0.7, verifying the questionnaire's reliability. The Kaiser-Meyer-Olkin (KMO) measure and Bartlett's test of sphericity were used to confirm validity; the KMO value was 0.650, which is higher than the suggested 0.6 threshold and Bartlett's test was statistically significant, indicating that the data was appropriate for factor analysis. These results show that, in accordance with accepted research practices, both validity and reliability criteria were satisfied. The survey will incorporate an importance-ranking scale, allowing respondents to assess the relative weight of SWOT elements and proposed TOWS strategies. This primary data collection aims to validate

S Strengths	W Weaknesses	O Opportunities	T Threats
• High data integrity and security • Transparent and auditable • Decentralised Architecture • Smart Contracts	• Scalability limitations • High energy consumption • Complex and costly integration • Regulatory ambiguity	• Enhanced Cybersecurity • Improved transactional efficiency • Increased automation capabilities • Promotes sustainability	• Regulatory uncertainty • Technological immaturity • Privacy concerns • Industry resistance

FIGURE 1 | Results of SWOT analysis.

literature-based findings and offer practitioner insights into real-world applicability.

The integration of SWOT/TOWS analyses with both literature-based and empirical data ensures a methodologically rigorous and contextually grounded investigation. This hybrid approach enables a dual-layered evaluation: it not only maps the strategic viability of blockchain adoption in MASS but also generates actionable recommendations that align with current industry practices and evolving regulatory expectations. By engaging both academic research and stakeholder perspectives, the methodology ensures that the study's outcomes are analytically robust and strategically sound.

4 | Results of SWOT Analysis

The SWOT analysis of the key findings from the literature review is presented in Figure 1. This analysis is then further elaborated, and validated; its implications on the subject matter are explained in the text below.

4.1 | Strengths

Blockchain technology offers a high degree of data integrity and security due to its decentralised and immutable nature. The tamper-proof recording system of blockchain serves as a robust safeguard against unauthorised data manipulation in the context of MASS. Reliability of navigation, control and communication systems is mission-critical on these vessels. This enhances the trustworthiness of operational data essential for safe vessel performance.

Another major advantage is the transparency and traceability. Blockchain maintains a permanent and verifiable audit trail of all recorded activities. This feature is highly beneficial in the maritime sector for post-incident investigations, regulatory reporting and ensuring compliance with international safety and environmental standards. The immutability of recorded data ensures accountability and reduces opportunities for falsification or error.

Furthermore, blockchain's decentralised structure eliminates reliance on a single point of control, significantly increasing system resilience. This distributed model enhances fault tolerance and system availability, which are two critical factors for MASS operations, where continuous and reliable functionality is highly desirable [53].

Incorporating smart contracts further strengthens blockchain's utility in MASS. These programmable protocols can automate processes such as ship-to-ship coordination, real-time compliance verification and cargo documentation. By reducing the need for human intervention, smart contracts contribute to increased efficiency, reduced administrative burden and lower risk of human error [45].

4.2 | Weaknesses

Despite the many positives, blockchain does face several limitations when applied to MASS. One of the key challenges is scalability, particularly in the PoW consensus mechanism. PoW struggles to efficiently manage high transaction volumes, making it ill-suited for environments where real-time data processing and rapid consensus are required, such as autonomous navigation, collision avoidance and situational awareness in MASS operations [53].

Another significant drawback is the high energy consumption associated with PoW-based blockchain systems. This contradicts the maritime industry's sustainability objectives and contributes to a larger environmental footprint. As international regulations increasingly demand reductions in emissions and promote energy efficiency, the environmental cost of blockchain may hinder its acceptability in shipping operations [4, 49].

System integration also poses substantial difficulties. Existing maritime infrastructures are often based on legacy systems that lack compatibility with decentralised technologies. Retrofitting these infrastructures to accommodate blockchain requires major investments, both in terms of financial resources and technical expertise. This results in high implementation costs, prolonged adaptation timelines and potential disruption during the transition phase [31].

Moreover, regulatory uncertainty represents a considerable barrier to adoption. The absence of clear and consistent international guidelines or standards creates ambiguity around the legal status and compliance requirements for blockchain in critical maritime operations, particularly from key governing bodies such as the IMO. This is especially problematic in safety-sensitive contexts, where regulatory approval is a prerequisite for implementation [5, 11].

4.3 | Opportunities

A key opportunity lies in strengthening cybersecurity. The cryptographic security mechanisms inherent to blockchain can effectively mitigate critical vulnerabilities in MASS communication and data exchange systems, including spoofing, data tampering and unauthorised access. By offering tamper-resistant data integrity and secure authentication protocols, blockchain significantly enhances trust in autonomous maritime operations [54, 55].

Blockchain also enables substantial operational streamlining. Its decentralised ledger allows for faster, more transparent transaction processing and record-keeping. This can reduce administrative burdens, enhance supply chain visibility and support the maritime industry's broader digital transformation agenda, particularly in port operations and logistics coordination [11].

The integration of smart contracts introduces further opportunities for automation and optimisation. These self-executing protocols facilitate condition-based decision-making without human intervention, enabling MASS to autonomously perform tasks such as compliance verification, cargo documentation, or navigational adjustments. This not only improves responsiveness and reduces latency, but also ensures regulatory adherence in real time [46].

In addition, blockchain can be leveraged to support the maritime industry's sustainability goals. By improving operational efficiency and reducing reliance on paper-based documentation, blockchain can contribute to lower fuel consumption and emissions. Its ability to provide transparent, immutable tracking also enables verifiable carbon footprint monitoring, supporting environmentally responsible shipping practices and alignment with global decarbonisation targets [56].

4.4 | Threats

A primary concern is regulatory uncertainty. The slow pace of consensus among international maritime bodies, such as the IMO and the IACS, has resulted in a lack of clear guidelines for blockchain integration in autonomous systems. Current regulations, such as IMO MSC.1/Circ.1526, offer limited direction on blockchain-specific applications, leading to stakeholder hesitation, compliance ambiguity and constrained long-term strategic planning and investment.

The immaturity of the technology also poses a critical risk. While blockchain is evolving rapidly, it remains an emerging solution with unresolved challenges related to scalability, interoperability and security vulnerabilities. These technical limitations may hinder its deployment in complex, real-time environments such as MASS operations, where system reliability and responsiveness are extremely important [34].

Increased data transparency, a core feature of blockchain, may paradoxically introduce privacy concerns. Without the implementation of robust privacy-preserving mechanisms, such as zero-knowledge proofs or differential privacy techniques, there is a risk of inadvertently disclosing commercially or operationally sensitive information. This poses a legal and reputational risk, especially in competitive or security-sensitive contexts [57].

Finally, institutional resistance remains a significant barrier. The maritime industry has traditionally been risk-averse and conservative in adopting disruptive technologies. Coupled with the high capital investment and technical expertise required for blockchain integration, this cultural inertia may delay implementation and lead to missed opportunities for innovation and competitiveness [11].

5 | TOWS Analysis

Building on the insights from the SWOT framework, this section presents four strategic responses that align internal factors (strengths and weaknesses) with external conditions (opportunities and threats). The aim is to provide practical and forward-looking recommendations for blockchain integration into MASS.

5.1 | SO (Strengths-Opportunities) Strategies

To capitalise on blockchain's core strengths, such as transparency, immutability and decentralisation, while leveraging emerging opportunities in the maritime domain, the following two strategies are proposed:

Enhance regulatory compliance through smart contract automation. Blockchain's transparent and secure ledger can be utilised to automate compliance processes with IMO regulations. Smart contracts can streamline routine audits, validation procedures and reporting activities, thus reducing human error and administrative overhead and further making MASS more economical and efficient. [4, 45].

Optimise autonomous operations using smart contracts and permissioned blockchain: Self-executing smart contracts can facilitate critical autonomous maritime functions (e.g., ship-to-ship communications, navigation protocols and safety verification) without the need for a central authority, reducing reliance on centralised systems and improving both efficiency and safety in autonomous maritime operations [46]. As Gai et al. [58] argue, permissioned blockchains also enable secure sharing of position and performance data while maintaining data confidentiality, significantly reducing vulnerability to cyber threats.

5.2 | WO (Weaknesses-Opportunities) Strategies

To overcome current limitations while seizing growth opportunities, two strategies are proposed as follows:

Adopt next-generation consensus protocols: Transitioning from energy-intensive PoW to more sustainable mechanisms such as PoS or Delegated Proof-of-Stake (DPoS) can drastically reduce the environmental footprint of blockchain systems. These newer protocols improve energy efficiency, reduce latency and are more scalable, making them better suited for real-time MASS applications [49].

Collaborate on regulatory frameworks and technical standards. Proactive engagement with regulators and international bodies such as the IMO and IACS can support the development of harmonised standards and legal frameworks tailored to blockchain use in autonomous shipping. These frameworks can facilitate legal certainty, improve cross-platform interoperability and foster industry-wide adoption [11].

5.3 | ST (Strengths-Threats) Strategies

The following two strategies are proposed to use internal strengths to mitigate external threats:

Utilise decentralised infrastructure to counter cybersecurity threats. One of blockchain's defining strengths, its decentralised architecture, directly counters the threat of single-point-of-failure vulnerabilities in centralised maritime systems. By distributing control across the network, blockchain improves system resilience against cyberattacks and technical disruptions [59].

Integrate privacy-preserving technologies. To mitigate concerns about data exposure while preserving transparency, blockchain systems should incorporate cryptographic techniques such as zero-knowledge proofs, homomorphic encryption, or selective disclosure protocols. These technologies enable verifiable data sharing without revealing the underlying content, striking a balance between transparency and confidentiality [60].

5.4 | WT (Weaknesses-Threats) Strategies

Implement permissioned blockchain systems. Rather than relying on public, open-access blockchain networks, the use of permissioned (private or consortium-based) blockchains can address scalability, privacy and regulatory compliance concerns. These systems offer more controlled access, enhanced transaction throughput and alignment with operational and legal requirements specific to the maritime sector [12].

Conduct pilot studies to facilitate adoption and risk mitigation. Pilot projects and controlled testbeds allow stakeholders to observe the tangible benefits of blockchain integration in MASS environments. These trials can help de-risk implementation by evaluating technical feasibility, identifying potential integration challenges and building trust among industry actors before large-scale deployment (Pu and Lam, 2020).

6 | Survey Results

To ensure the reliability and validity of the survey instrument, several statistical tests were conducted. A Cronbach's Alpha score of 0.744 exceeded the commonly accepted threshold of 0.7, indicating a satisfactory level of internal consistency among the items. Validity was supported by a Kaiser-Meyer-Olkin (KMO) measure of 0.650, which is acceptable for proceeding with factor analysis. Furthermore, Bartlett's Test of Sphericity yielded a statistically significant result ($p < 0.001$), confirming the adequacy of inter-item correlations for further analysis.

6.1 | Respondent Background

Table 2 summarises the background characteristics of the survey respondents ($n = 41$), including their professional domain, education and years of work experience. Figure 2 illustrates the distribution of respondents by occupation. Regarding their professional domain, a substantial portion of participants (78.1%) reported working in operational or management roles. Although these professionals may not hold direct policymaking authority, they are commonly responsible for implementing cybersecurity risk assessments, operational protocols and Safety Management Systems (SMS) within their organisations. In terms of level of education, around 76% of respondents have obtained a degree of undergraduate or above, suggesting a generally well-educated sample with the capacity to understand and evaluate technical innovations such as blockchain and MASS cybersecurity. For work experience, over 50% of respondents had more than 10 years of work experience in the maritime sector. This indicates that the responses were informed by considerable industry exposure and practical insight, lending robustness to the findings.

To gain a clearer understanding of the respondents' professional roles, Figure 2 presents the specific job titles reported in the survey. A significant proportion of participants identified as chief engineers, reflecting the composition of the sample pool, as previously noted. Chief engineers on sea-going vessels typically possess extensive knowledge of maritime legislation and are often well-versed in emerging technological developments.

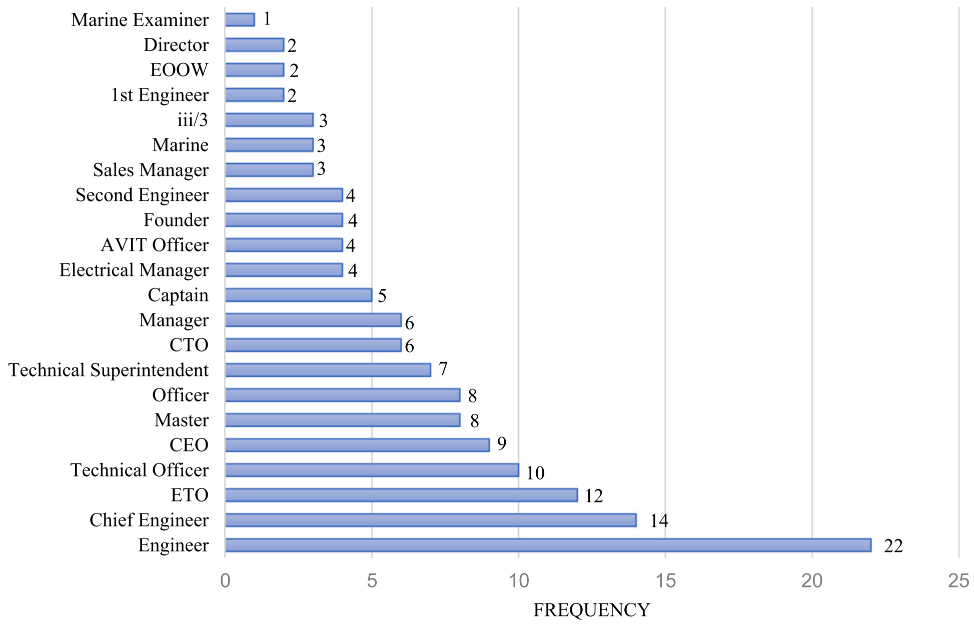

FIGURE 2 | Occupations of respondents.

TABLE 2 | Respondent background.

	Frequency	Percentage (%)
Type of business		
Shipping operational	23	56.1%
Shipping management	9	22.0%
Survey/regulatory/ legislative professional	3	7.3%
Cybersecurity professional	3	7.3%
Not answered	3	7.3%
Level of education		
High school	7	17.1%
Undergraduate	16	39.0%
Postgraduate	15	36.6%
Not Answered	3	7.3%
Work experience		
0–10 years	7	17.1%
11–20 years	10	24.4%
21–30 years	8	19.5%
31–40 years	2	4.9%
41–50 years	1	2.4%
Not answered	13	31.7%

Additionally, as heads of their respective departments (often including responsibility for onboard IT systems), they are uniquely positioned to provide informed insights into the practical challenges of managing cybersecurity within operational maritime environments.

TABLE 3 | Vulnerability of MASS systems.

	Mean	S.D.
About MASS systems		
Bridge systems	3.98	1.012
Propulsion and machinery systems	3.68	0.986
Communication systems	4.00	1.025
About cyberterrorism on MASS systems		
Ship identification systems	3.63	0.942
Ship to ship collision avoidance systems	3.76	0.860
Global positioning systems	3.85	1.062
Ship to infrastructure system (vessel routing information)	3.93	0.787
Automation communications	3.98	0.880

6.2 | Vulnerability of Systems and Cyber Terrorism Attacks

Table 3 presents respondents' perceptions of vulnerabilities across various systems in MASS, rated on a scale from 1 (not vulnerable) to 5 (very vulnerable). Communication systems were identified as the most vulnerable, with the highest mean score of 4.00, reflecting their critical role in maintaining operational safety and continuous connectivity. Bridge systems followed closely with a mean of 3.98, indicating general confidence in their robustness, though concerns remain due to their centrality in navigation and control. Propulsion and machinery systems were considered the least vulnerable (mean 3.68), although this may stem from a lack of awareness about the remote control and monitoring of these systems in autonomous vessels.

TABLE 4 | Agreement for blockchain to enhance cybersecurity in MASS.

	Mean	S.D.
Current cybersecurity safeguards for MASS are adequate	2.39	1.022
Blockchain can enhance cybersecurity	4.02	0.865
Blockchain would enhance the security for identifications, communication and automation of MASS	3.12	0.954

In terms of respondents' perceptions of cyberterrorism on MASS systems, the mean values indicate a moderate to high likelihood across all systems. The perceived threat is more significant for systems involving communication, automation and ship-to-infrastructure connections, where constant data exchange and remote accessibility increase exposure to cyber risks. The elevated concern regarding GPS and automated communication systems aligns with broader industry awareness of their vulnerability to spoofing, jamming and data manipulation. In contrast, systems such as ship identification scored lower, likely due to their relatively isolated operation and limited digital interface, particularly in traditional tools like RADAR or manual identification methods, which are perceived as less susceptible to cyber intrusion. Overall, while the responses highlight significant areas of concern, the moderate mean values across systems suggest a level of confidence in the effectiveness of existing cybersecurity frameworks within the maritime domain.

6.3 | Perception of Blockchain's Role in Enhancing Cybersecurity in MASS

Table 4 shows the respondents' agreement (rated from 1: Strongly disagree to 5: Strongly agree) with the statements regarding the use of blockchain to enhance cybersecurity in MASS operations. The statement 'Current cybersecurity safeguards for MASS are adequate' received a low mean score of 2.39, indicating general dissatisfaction. Only 12.2% of respondents agreed or strongly agreed, while 61% disagreed or strongly disagreed. This result highlights a significant perceived gap in current cybersecurity measures, suggesting that existing safeguards may not sufficiently address the unique vulnerabilities of autonomous systems. Although a minority expressed confidence, possibly reflecting specialised knowledge or involvement in cybersecurity initiatives, the prevailing sentiment underscores the urgent need for improved protection.

By contrast, the statement 'Blockchain can enhance cybersecurity in general' received a high mean score of 4.02, with 68.3% of respondents agreeing or strongly agreeing. This finding is consistent with increasing industry interest in blockchain as a solution for securing digital operations, particularly due to its decentralised architecture and tamper-resistant ledger capabilities.

When evaluating the more specific statement 'Blockchain would enhance the security of identification, communication and automation systems in MASS', the mean score was 3.12, suggesting a more cautious optimism. Here, 29.3% of respondents agreed, while 17.1% disagreed. This mixed response may reflect uncertainty about practical implementation, particularly in light of the current scalability and integration challenges highlighted in the SWOT analysis. In essence, while blockchain's potential to enhance cybersecurity is broadly recognised, the maritime community remains tentative about its immediate applicability to MASS due to unresolved technical and operational barriers.

TABLE 5 | Importance of blockchain in MASS.

	Mean	S.D.
Well established and proven Protocol	4.41	0.865
Speed of the transaction	4.32	0.907
Energy efficiency of transactions	3.46	1.206

6.4 | Perceived Importance of Key Blockchain Attributes for MASS

Table 5 presents respondents' views on the importance (rated from 1: Not important to 5: Very important) of various blockchain attributes relevant to MASS. The importance of having proven and reliable blockchain protocols received a high mean score of 4.41, with 87.8% of respondents rating it as important or very important. This highlights a strong consensus that robust and standardised protocols are essential for ensuring the security, efficiency and interoperability of blockchain systems in autonomous maritime operations.

Similarly, transaction speed was also rated highly, with a mean score of 4.32 and 83% of respondents considering it important or very important. This suggests that real-time or near-real-time data processing is regarded as vital for maintaining the responsiveness and security of MASS systems, particularly in safety-critical functions such as navigation, communication and collision avoidance.

In contrast, energy efficiency in blockchain transactions received a more moderate mean score of 3.46, with 46.4% viewing it as important or very important. While this indicates a growing awareness of the environmental impact of blockchain, particularly relevant in light of the maritime industry's decarbonisation goals, it is currently seen as secondary to security and performance-related attributes. The relatively lower prioritisation of energy efficiency by survey respondents does not necessarily indicate a lack of concern for sustainability, but rather reflects the operational context in which MASS technologies are currently being evaluated. Many respondents occupy technical or operational roles, where immediate priorities include cybersecurity robustness, system reliability and real-time performance in safety-critical environments. At this early stage of blockchain adoption in MASS, energy consumption may be perceived as a secondary issue, particularly given expectations that implementations will rely on permissioned blockchains or energy-efficient consensus mechanisms rather than energy-intensive public proof-of-work systems.

7 | Conclusion, Research Limitations and Future Directions

7.1 | Conclusion

This research has examined the current landscape of international guidance and legislation relevant to MASS, highlighting that while regulatory frameworks remain in their formative stages, key stakeholders are actively working toward more comprehensive and standardised guidelines. The level of engagement among classification societies appears uneven, likely reflecting the extent of their collaboration with major technology developers driving autonomous innovations.

The findings show that blockchain technology presents several core strengths, such as interoperability, data integrity, transparency and security, which offer significant potential to address cybersecurity and operational challenges in MASS. Secondly, the findings of the SWOT–TOWS analyses demonstrate strong alignment with insights obtained from the stakeholder survey. Both strands of evidence emphasise the importance of robust blockchain protocols and high transaction speed, which are viewed as critical for supporting real-time operational effectiveness in autonomous maritime systems. Thirdly, communication systems were consistently identified as the most vulnerable component of MASS, reflecting their centrality in ensuring navigational safety and secure vessel-to-vessel and vessel-to-infrastructure interactions. Fourthly, some divergences were also observed. While energy efficiency appeared as a major concern in the strategic analysis, industry respondents were more ambivalent, suggesting a gap between theoretical assessments and frontline operational priorities. Similarly, regulatory engagement was highlighted as urgent in the TOWS analysis, but did not resonate as strongly with practitioners, indicating potential disconnects in stakeholder awareness. Finally, the study confirms that blockchain is not a universal solution but can significantly enhance cybersecurity and operational resilience in MASS, provided certain enabling factors are met.

Based on the results, this study proposes several policy recommendations below:

- Adopt energy-efficient, scalable consensus mechanisms (such as PoS in permissioned ship-to-shore networks) so that real-time functions such as secure remote control, software update validation and encrypted telemetry can run continuously without impacting energy and decarbonisation goals.
- Create and standardise interoperable blockchain protocols (for example, sharing of voyage data information for emission regulation compliance, compliance record information between flag states and cargo status information) to enable the maritime sector to facilitate cross-platform and cross-system collaboration.
- Strengthen international guidance and standardisation by further engaging bodies such as the IMO, Lloyd's Register and DNV to recognise blockchain-secured logs, create standardised secured certificate verification and identity registers to simplify compliance, risk management and digital transformation.
- Implement pilot projects on non-critical systems to build trust, such as using blockchain to secure software and firmware updates, tamper-proof voyage and event reporting or track access to remote control interfaces, to demonstrate technical feasibility, quantify risk reduction before extending to safety-critical MASS functions.

From a practical perspective, the findings of this study highlight several concrete application pathways for blockchain in MASS cybersecurity. These include securing ship-to-ship and ship-to-infrastructure communications, ensuring the integrity and traceability of operational data and supporting automated compliance and audit processes through smart contracts. For ship operators, such applications can enhance operational reliability and reduce cyber-related risks in autonomous navigation. For regulators and classification societies, blockchain-enabled systems offer improved transparency, traceability and efficiency in certification, monitoring and compliance verification. Together, these applications demonstrate the tangible value of blockchain as an enabling technology for the safe, secure, and scalable deployment of MASS.

7.2 | Research Limitations and Future Directions

This study has several research limitations as follows:

First, the scope of this study was confined to the maritime industry, which limited broader cross-sectoral comparisons of blockchain applications in cybersecurity. Although focusing on recent maritime-specific literature was justified by its rapid growth, this approach restricted opportunities to benchmark maritime use cases against innovations in other sectors, such as finance or healthcare. Future work could broaden the analysis by incorporating cross-industry comparative studies. Examining blockchain-enabled cybersecurity in sectors outside maritime may reveal transferable best practices and help contextualise MASS-specific findings.

Secondly, the study concentrated on blockchain as a stand-alone cybersecurity solution. Less attention was paid to the integration between blockchain and other digital technologies, such as IoT and AI, which could offer more comprehensive cyber-resilience frameworks for MASS. Further research should explore how blockchain interacts with complementary technologies (e.g., IoT, AI, or advanced control systems) to strengthen cybersecurity in MASS, ideally through empirical investigations into integrated or hybrid cyber-resilience solutions.

Thirdly, while the SWOT-TOWS analysis was effective in identifying factors influencing blockchain adoption, the method does not provide a systematic means to prioritise these factors. Additional studies could apply quantitative multi-criteria evaluation techniques, such as Analytic Hierarchy Process (AHP) or Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS), to assess the relative importance of these factors for structured decision-making in technology adoption.

Fourthly, although a mixed-methods approach offered valuable insights, the survey component was based on a relatively small sample size ($n = 41$), potentially limiting the representativeness and generalisability of the findings. For further research, larger-scale surveys, including more diverse respondent groups from multiple geographic and operational backgrounds, should be conducted to validate and extend the results. Qualitative approaches, such as in-depth interviews or focus groups with experts and stakeholders, could further enrich the contextual understanding of cybersecurity perceptions and operational challenges.

Finally, the environmental impact of blockchain, particularly its energy consumption, was only briefly addressed, despite being a significant industry concern. For future research, investigating the practical viability of adopting energy-efficient, 'green' blockchain solutions such as Proof-of-Stake within MASS and associated infrastructures is recommended. This could involve pilot projects to quantify energy savings, assess scalability and validate operational reliability, thereby supporting industry sustainability goals.

Author Contributions

Ian Hamilton: conceptualisation, data curation, formal analysis, investigation, methodology, visualisation, writing – original draft. **Dante Ben Matellini**: validation, writing – review and editing. **Chia-Hsun Chang**: formal analysis, funding acquisition, investigation, methodology, supervision, validation, visualisation, writing – review and editing.

Funding

This paper is partially financially supported by the Royal Society (IEC\NSFC\223196)

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

1. C.-H. Chang, C. Kontovas, Q. Yu, and Z. Yang, "Risk Assessment of the Operations of Maritime Autonomous Surface Ships," *Reliability Engineering & System Safety* 207 (2021): 107324.

2. C.-H. Chang, C.-C. Lin, Z. Yang, and C. Kontovas, "Evaluating the Social Acceptance of Autonomous Ferries: An Observation from Passengers' Boarding Willingness," *Transport Policy* 159 (2024): 83–94.

3. J. Tao, Z. Liu, X. Wang, et al., "Hazard Identification and Risk Analysis of Maritime Autonomous Surface Ships: A Systematic Review and Future Directions," *Ocean Engineering* 307 (2024): 118174.

4. M. B. Farah, Y. Ahmed, H. Mahmoud, et al., "A Survey on Blockchain Technology in the Maritime Industry: Challenges and Future Perspectives," *Future Generation Computer Systems* 157 (2024): 618–637.

5. H. Kim, Z. Xiao, X. Zhang, X. Fu, and Z. Qin, "Rethinking Blockchain Technologies for the Maritime Industry: An Overview of the Current Landscape," *Future Internet* 16, no. 12 (2024): 454.

6. K. Li, J.-Y. Lee, and A. Gharehgozli, "Blockchain Implementation in the Maritime Industry: A Literature Review and Synthesis Analysis of Benefits and Challenges," *Maritime Economics & Logistics* 26, no. 4 (2024): 630–657.

7. J. Pokorny, K. Ma, S. Saafi, et al., "Prototype Design and Experimental Evaluation of Autonomous Collaborative Communication System for Emerging Maritime Use Cases," *Sensors* 21, no. 11 (2021): 3871.

8. Y. Chen, T. Wang, Y. Xiao, Y. Wang, and G. Yan, "An Approach of Consensus-Based Double-Layer Blockchain System for Multi-Ship Collision Risk Mitigation Considering COLREGs," *Applied Sciences* 13, no. 20 (2023): 11178.

9. D. Adam, D. B. Matellini, and A. Kaparaki, "Benefits for the Bunker Industry in Adopting Blockchain Technology for Dispute Resolution," *Blockchain: Research and Applications* 4, no. 2 (2023): 100128.

10. Y. Wang, P. Chen, B. Wu, C. Wan, and Z. Yang, "A Trustable Architecture Over Blockchain to Facilitate Maritime Administration for Mass Systems," *Reliability Engineering & System Safety* 219 (2022): 108246.

11. Y. S. Zhou, Y. H. Soh, H. S. Loh, and K. F. Yuen, "The Key Challenges and Critical Success Factors of Blockchain Implementation: Policy Implications for Singapore's Maritime Industry," *Marine Policy* 122 (2020): 104265.

12. M. Jović, E. Tijan, D. Žgaljić, and S. Aksentijević, "Improving Maritime Transport Sustainability Using Blockchain-Based Information Exchange," *Sustainability* 12, no. 21 (2020): 8866.

13. J. Xu and L. Zhang, "Privacy-Preserving Techniques for Blockchain in Maritime Applications," *IEEE Transactions on Information Forensics and Security* 19 (2024): 1234–1245.

14. T. Yuzui and F. Kaneko, "Toward a Hybrid Approach for the Risk Analysis of Maritime Autonomous Surface Ships: A Systematic Review," *Journal of Marine Science and Technology* 30, no. 1 (2025): 153–176.

15. M. Belabyad, C. Kontovas, R. Pyne, and C. H. Chang, "Skills and Competencies for Operating Maritime Autonomous Surface Ships (MASS): A Systematic Review and Bibliometric Analysis," *Maritime Policy & Management* 53 (2025a): 1–26.

16. M. Belabyad, C. Kontovas, R. Pyne, et al., "The Human Element in Autonomous Shipping: A Study on Skills and Competency Requirements," *WMU Journal of Maritime Affairs* 24 (2025b): 575–605.

17. M. Petković and I. Vujović, "Blockchain Security of Autonomous Maritime Transport," *Journal of Applied Engineering Science* 17, no. 3 (2019): 333–337.

18. Y. Xie, C. Nanlal, and Y. Liu, "Reliable LiDAR-Based Ship Detection and Tracking for Autonomous Surface Vehicles in Busy Maritime Environments," *Ocean Engineering* 312 (2024): 119288.

19. R. Song, E. Papadimitriou, R. R. Negenborn, and P. V. Gelder, "Integrating Situation-Aware Knowledge Maps and Dynamic Window Approach for Safe Path Planning by Maritime Autonomous Surface Ships," *Ocean Engineering* 311 (2024): 118882.

20. R. G. Maidana, S. D. Kristensen, I. B. Utne, and A. J. Sørensen, "Risk-Based Path Planning for Preventing Collisions and Groundings of Maritime Autonomous Surface Ships," *Ocean Engineering* 290 (2023): 116417.

21. J. Liu, A. W.-K. Law, and O. Duru, "Reducing Emissions of Atmospheric Pollutants Along Major Dry Bulk and Tanker Routes Through Autonomous Shipping," *Journal of Environmental Management* 302 (2022): 114080.

22. Y. A. Ahmed, G. Theotokatos, I. Maslov, L. A. L. Wennersberg, and D. A. Nesheim, "Regulatory and Legal Frameworks Recommendations for Short Sea Shipping Maritime Autonomous Surface Ships," *Marine Policy* 166 (2024): 106226.

23. D. Luchenko, I. Georgiievskyi, and M. Bielikova, "Challenges and Developments in the Public Administration of Autonomous Shipping," *Lex Portus* 9 (2023): 20.

24. R. Zagan, G. Raicu, and A. Sabau, "Studies and Research Regarding Vulnerabilities of Marine Autonomous Surface Systems (Mass) and Remotely Operated Vessels (Rovs) From Point of View of Cybersecurity," *International Journal of Modern Manufacturing Technologies* 14 (2022): 310–318.

25. K. Tam and K. Jones, “MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment,” *WMU Journal of Maritime Affairs* 18, no. 1 (2019): 129–163.

26. A. Farao, A. Zarras, A. Voudouris, G. Paparis, and C. Xenakis, “B2SAPP: Blockchain Based Solution for Maritime Security Applications,” *Frontiers in Computer Science* 7 (2025): 1572009.

27. C. Park, C. Kontovas, Z. Yang, and C. H. Chang, “A BN Driven FMEA Approach to Assess Maritime Cybersecurity Risks,” *Ocean & Coastal Management* 235 (2023): 106480.

28. C. Park, C. Kontovas, Z. Yang, and C. H. Chang, “Building Cyber-Resilience in Maritime Transport: A Stakeholders’ Perspective on Mitigation Measures,” *Journal of International Maritime Safety, Environmental Affairs, and Shipping* 9 (2025): 2594832.

29. K. Kanwal, W. Shi, C. Kontovas, Z. Yang, and C. H. Chang, “Maritime Cybersecurity: Are Onboard Systems Ready?,” *Maritime Policy & Management* 51, no. 3 (2024): 484–502.

30. F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, “Cybersecurity Challenges in the Maritime Sector,” *Network (Bristol, England)* 2, no. 1 (2022): 123–138.

31. S. Nguyen, P. S.-L. Chen, and Y. Du, *Blockchain Adoption in Container Shipping: An Empirical Study on Barriers, Approaches, and Recommendations* (Marine Policy, 2023), 105724.

32. G. Loukas, D. Gan, and T. Vuong, “A Review of Cyber Threats and Defence Approaches in Emergency Management,” *Future Internet* 5 (2013): 205–236.

33. G. Zhang, X. Dong, Q. Shan, and W. Zhang, “Event-Triggered Robust Adaptive Control for Unmanned Surface Vehicle in Presence of Deception Attacks,” *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering* 237, no. 7 (2023): 1266–1280.

34. S. Z. Jiang and H. Zhang, “Research on Communication Network Security of Unmanned Surface Vehicle Based on Blockchain,” *Image Processing, Electronics and Computers* 57 (2024): 589–596.

35. DNV, "Maritime Cyber Priority 2024/25: Managing Cyber Risk to Enable Innovation," accessed October 17, 2025, https://www.dnv.com/maritime/maritime-cyber-priority/.

36. LR, Lloyds Register of Shipping, "Global Maritime Trends 2025 Barometer," accessed November 10, 2025, https://www.lr.org/en/insights/global-maritime-trends-barometer-2025/.

37. BIMCO, "The Guidelines on Cyber-Security Onboard Ships," accessed August 5, 2025, https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

38. H. M. Tusher, Z. H. Munim, T. E. Notteboom, T.-E. Kim, and S. Nazir, “Cyber Security Risk Assessment in Autonomous Shipping,” *Maritime Economics & Logistics* 24, no. 2 (2022): 208–227.

39. B. C. Ghosh, V. Ramakrishna, and C. Govindarajan, “Decentralized Cross-Network Identity Management for Blockchain Interoperation,” in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (IEEE, 2021), 1–9.

40. M. A. Azad, W. Meng, and X. Du, *Towards Blockchain-Enabled Cybersecurity Risk Assessment for Cyber-Ship Systems* (Data Security and Privacy Protection, 2025).

41. S. Pu and J. S. L. Lam, “Blockchain Adoptions in the Maritime Industry: A Conceptual Framework,” *Maritime Policy & Management* 48, no. 6 (2021): 777–794.

42. N. Tabish and T. Chaur-Luh, “Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives,” *IEEE Access* 12 (2024): 17114–17136.

43. D. Patil and V. Bhosale, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *International Journal of Advanced Research in Science Communication and Technology* 3, no. 3 (2023): 293–298, https://doi.org/10.48175/IJARSCT-8158.

44. P. E. Leonis, K. Ntouros, A. I. Mazilu, S. Brotsis, and N. Kolokotronis, “SEAGuard: A Blockchain-Based Security Framework for IoT Maritime Transportation Systems,” in *2024 IEEE International Conference on Cyber Security and Resilience (CSR)* (IEEE, 2024), 421–426.

45. P. Serra, G. Fancello, R. Tonelli, and L. Marchesi, “Application Prospects of Blockchain Technology to Support the Development of Interport Communities,” *Computers* 11, no. 5 (2022): 60.

46. T. Shanthi, M. Ramprasath, A. Kavitha, and T. Muruganantham, “Deep Learning Based Autonomous Transport System for Secure Vehicle and Cargo Matching,” *Intelligent Automation & Soft Computing* 35, no. 1 (2023): 957.

47. X. Li, P. Jiang, T. Chen, X. Luo, and Q.-Y. Wen, “A Survey on the Security of Blockchain Systems,” *Future Generation Computer Systems* 107 (2020): 841–853.

48. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,” *Future Generation Computer Systems* 29, no. 7 (2013): 1645–1660.

49. A. O. Bada, A. Damianou, C. M. Angelopoulos, and V. Katos, “Towards a Green Blockchain: A Review of Consensus Mechanisms and Their Energy Consumption,” in *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (IEEE, 2021), 503–511.

50. L. Lei, L. Song, and J. Wan, “Improved Method of Blockchain Cross-Chain Consensus Algorithm Based on Weighted PBFT,” *Computational Intelligence and Neuroscience* 2022, no. 1 (2022): 5169259.

51. J. Truby, “Decarbonizing Bitcoin: Law and Policy Choices for Reducing the Energy Consumption of Blockchain Technologies and Digital Currencies,” *Energy Research & Social Science* 44 (2018): 399–410.

52. R. Brothwell, "Contextualising Blockchain’s Energy Use and Exploring the Green Blockchain," accessed August 8, 2025, https://bsvblockchain.org/news/contextualising-blockchain-energy-use-and-exploring-the-green-blockchain/.

53. W. P. Freire, W. S. Melo, V. D. do Nascimento, P. R. Nascimento, and A. O. de Sá, “Towards a Secure and Scalable Maritime Monitoring System Using Blockchain and Low-Cost IoT Technology,” *Sensors* 22, no. 13 (2022): 4895.

54. A. Jain and R. Tiwari, “Blockchain for Cybersecurity in Maritime Autonomous Systems: A Review,” *Journal of Maritime Research* 20, no. 2 (2023): 30–45.

55. S. Jain, N. J. Ahuja, P. Srikanth, et al., “Blockchain and Autonomous Vehicles: Recent Advances and Future Directions,” *IEEE Access* 9 (2021): 130264–130328.

56. J. Truby, “Blockchain for Sustainable Shipping: Enhancing Traceability and Reducing Emissions,” *Journal of Cleaner Production* 400 (2024): 130–145.

57. H. Xu and N. Zhang, “Privacy Implications of Blockchain Systems: A Data Management Perspective,” *Organizational Cybersecurity Journal Practice Process and People* 3, no. 1 (2023): 71–79.

58. K. Gai, H. Tang, G. Li, et al., “Blockchain-Based Privacy-Preserving Positioning Data Sharing for IoT-Enabled Maritime Transportation Systems,” *IEEE Transactions on Intelligent Transportation Systems* 24, no. 2 (2023b): 2344–2358.

59. J. Liu, H. Zhang, and L. Zhen, “Blockchain Technology in Maritime Supply Chains: Applications, Architecture and Challenges,” *International Journal of Production Research* 61, no. 11 (2021): 3547–3563.

60. K. Gai, M. Qiu, and H. Zhao, “Addressing Scalability Challenges in Maritime Logistics Using Blockchain Technology,” *Future Generation Computer Systems* 135 (2023a): 45–56.