



RESEARCH ARTICLE

A conceptual framework for legal-responsive permissioned blockchain deployment in port communities

Dang Thuy Long Chau^{1,*}, Pham Thai Hoang¹, Nguyen Phuong Ngan¹, Nguyen Cao Thuc¹, Le Thanh Tung¹, Le Hoang Dung²

¹ Logistics Center, Ho Chi Minh City University of Transport, Ho Chi Minh City, Vietnam

² Department of Import–Export, Vietnam National Coffee Corporation, Ho Chi Minh City, Vietnam

ARTICLE INFO

Received: 07/11/2025

Revised: 05/08/2026

Accepted: 07/09/2026

Published online: 15/09/2026

KEYWORDS

Permissioned blockchain
Legal-responsive design
Necessity-and-viability screening
Port community systems
Electronic trade records
Competition compliance

ABSTRACT

Permissioned blockchain promises port communities better traceability, document integrity, and coordination, yet deployment is constrained where data-protection, cybersecurity, electronic-transactions, contract, and competition law diverge across jurisdictions. This study develops a legal-responsive framework that translates regulatory requirements into governance and architectural choices for permissioned blockchain systems in port ecosystems. Combining doctrinal legal analysis, functional comparative synthesis, and design-science modeling, legal materials were coded against five analytical dimensions — data governance, contractual and evidentiary validity, accountability and liability, operational security, and competitive conduct — and compared across Singapore, the Netherlands and the European Union, and Vietnam. The framework places a Layer 0 necessity-and-viability screen (S1–S4) ahead of four coupled design layers. The necessity question is inherited from the do-you-need-a-blockchain decision frameworks; Layer 0 tightens it against the strongest non-replicated alternatives — a threshold-signed multi-party log and a sector interoperability standard — and adds institutional, economic, and legal tiers, so the screen can return the answer not to deploy. A bounded pilot scenario for release-order and gate-event coordination at Cat Lai Port translates the framework into measurable indicators and an ex-ante cost model, reported as design assumptions. Formative ex-post probes against nine real platforms, a Monte Carlo analysis of the cost rule, and a benchmark spanning both prior-art families returned one negative result: the necessity questions predict adopted designs but not survival. This forced a disclosed repair — the S4 viability question, stated in binding-commitment form — leaving the Cat Lai verdict conditional on those commitments. Naturalistic validation through deployment remains necessary.

1. Introduction

Within port clusters — defined as geographical concentrations of interconnected maritime businesses and their supporting infrastructures — the adoption of permissioned blockchain networks holds a disruptive promise of facilitating real-time stakeholder collaboration by optimizing transparency, security, and efficiency in a diverse array of operational processes [1]. Singapore's TradeTrust, for example, issues electronic trade documents as blockchain-based tokens whose legal status rests on the Electronic Transactions Act as amended in 2021 [2], while several European ports have pursued standardized data exchange for port-call optimization through platforms such as PortXchange, which is a data-sharing service rather than a distributed-ledger system [3]. Generated benefits are, however, substantially constrained by the multiple legal systems that regulate these areas [4].

The global landscape of legal systems, each possessing distinct approaches to data privacy, contract law, and regulatory compliance, creates a complex web of requirements

that blockchain implementations must navigate. Furthermore, the inherent characteristics of blockchain technology, such as its decentralized nature and cryptographic security, present unique challenges to conventional legal concepts, necessitating careful consideration and adaptation of existing legal frameworks [5]. The long-term ability of decentralized blockchain systems to evolve and sustain depends critically on how governance structures are designed to absorb these legal pressures [6].

Two considerations sharpen the problem. First, the most consequential evidence available to the field is a failure rather than a success: TradeLens, the largest maritime blockchain platform yet attempted, was announced for discontinuation in late 2022 because, in the operators' own words, "the need for full global industry collaboration has not been achieved" and the platform had not reached commercial viability [7]. Subsequent analysis attributes the outcome to weak stakeholder engagement, unclear governance, and confidentiality concerns rather than to any legal prohibition [8], [9]. Legal compli-

* Corresponding author: Dang Thuy Long Chau. Email: chaudtl@ut.edu.vn

DOI: <https://doi.org/10.55228/j.uth.150510>

ance is therefore necessary but not sufficient, and a design framework that optimises only for lawfulness may be solving the wrong constraint. Second, port-community data sharing is conducted among firms that compete with one another, which places these arrangements within the scope of competition law — a body of rules examined in competition-law commentary but not yet operationalized as a design dimension in existing blockchain deployment frameworks [10], [11]. Both considerations are incorporated into the framework developed below. For transport research, they relocate the object of study: the binding constraints on port-community coordination platforms turn out to be operator neutrality and reachable adoption volume — properties of the port ecosystem’s market and institutional structure — rather than properties of the ledger technology itself, and the framework is accordingly as much an instrument for deciding *against* replication as for configuring it.

Yet the specific implications of legal variation for blockchain system design and deployment remain insufficiently addressed in current research — particularly in port ecosystems where multiple jurisdictions, institutional mandates, and data governance regimes intersect simultaneously. This paper contributes to filling this research gap by proposing a conceptual framework that systematically maps legal considerations to the technical and governance design of permissioned blockchain systems within the multi-jurisdictional context of port operations [12].

Three research questions guide the inquiry:

RQ1. How do jurisdictional legal differences influence permissioned blockchain architecture and operations in port communities?

RQ2. What design strategies can mitigate legal-technical trade-offs in permissioned environments?

RQ3. Under what conditions is a permissioned blockchain the appropriate instrument at all, as against a signed append-only database with interoperability interfaces?

RQ3 is posed first in the framework, as a screening gate, so that the analysis does not presuppose the conclusion that blockchain should be deployed.

The remainder of the paper is organized as follows. Section 2 reviews the legal, governance, competition, and stakeholder literature relevant to the problem domain, examines the evidence from failed consortia, positions the study against the established law-and-architecture tradition, and consolidates the design requirements the framework must satisfy. Section 3 describes the research methodology and the coding protocol. Section 4 presents the proposed framework, including the Layer 0 necessity-and-viability screen and an explicit statement of the framework’s claims and the evidence that would disconfirm them. Section 5 applies the framework to Singapore and to the Netherlands and the European Union as reference jurisdictions, then to Vietnam, develops a bounded pilot scenario for Cat Lai Port, and subjects the framework to formative ex-post probes (Sections 5.4–5.7). Section 6 discusses theoretical and practical implications. Section 7 concludes and states limitations and directions for future research.

2. Literature Review

Permissioned blockchain deployment in port communities intersects the five analytical dimensions defined in Section 3.1 (Table 2): data governance, contractual and evidentiary validity, accountability and liability, operational security, and competitive conduct. The following subsections review the literature on each in turn, then examine the stakeholder ecosystem, the evidence from failed consortia, and the position of this study relative to prior law-and-architecture scholarship.

2.1. Data Protection and the Immutability Conflict

The inherent characteristics of blockchain technology — particularly its cryptographic immutability — render the direct modification or deletion of recorded data technically infeasible [13], presenting significant compliance hurdles under stringent regulations such as the General Data Protection Regulation, which mandates the “right to be forgotten” and data accuracy [14]. Blockchain systems designed for multi-stakeholder environments must therefore implement hybrid architectures that balance on-chain immutability with off-chain data management solutions to address these privacy concerns [15]. Typically, these solutions involve storing sensitive or personally identifiable information off-chain in encrypted databases, with only cryptographic hashes or proofs of existence recorded on the distributed ledger [16], [17], [18], [19].

This architectural response, however, is weaker than the literature has generally assumed, and this paper treats that weakness as a design constraint rather than a solved problem. The European Data Protection Board has issued guidance addressed specifically to blockchain, which states that where personal data is stored off-chain “it is important to recall that the GDPR will still apply to that processing activity and that the hash will also be considered personal data,” and that verifiability can be restricted only where the hash is produced with “a randomly generated secret key or salt of a sufficient size” [20]. The French data protection authority had earlier reached a comparable position [21]. Three consequences follow for design. First, an unsalted hash of a container number, a consignee name, or a driver identifier is not an anonymization measure. Second, the off-chain store is itself a distinct processing operation requiring its own controller allocation, retention schedule, and data protection impact assessment. Third, erasure is effected not by deleting an on-chain record — which cannot be done — but by destroying the salt and the off-chain pre-image such that the residual on-chain state no longer permits direct or indirect identification. Custody, rotation, and destruction authority over salts and keys therefore becomes a governance question, not merely a cryptographic one. A distinct branch of the literature pursues the opposite route — redactable or mutable ledgers that use chameleon hashes or committee-controlled rewriting to make on-chain data editable for erasure [22] — but this paper does not adopt it, because it relocates trust into a redaction authority and unsettles the evidentiary status of the record; the salted-hash-plus-off-chain design is preferred precisely because it keeps the ledger append-only while confining erasure to the governance of secrets.

In practice, jurisdiction-specific responses differ. Archipels, a French consortium founded in 2019 by Caisse des Dépôts, EDF, ENGIE, and La Poste to provide blockchain-based document authentication, became the subject of the first merger-control assessment of a private blockchain consortium in Europe [23], while China's Blockchain-based Service Network includes localized data storage protocols to comply with restrictions on cross-border data flow under the Personal Information Protection Law [24]. The architectural compromise introduces complexity, necessitating robust access control mechanisms and governance protocols to manage the interplay between on-chain and off-chain data components effectively [25]. Solutions such as zero-knowledge proofs or homomorphic encryption have emerged to enable verification without exposing personal data [26]. Furthermore, the global nature of blockchain transactions often leads to jurisdictional conflicts, where data originating in one regulatory domain may be processed or stored in another with differing legal requirements [27]. Self-sovereign identity solutions coupled with robust consent mechanisms have been proposed to let data subjects control personal data while facilitating verifiable exchange [28], [29]. The high cost of on-chain storage and scalability limitations further incentivize off-chain solutions for large volumes of data, which must then be reconciled with immutability guarantees through careful architectural design [30].

2.2. Smart Contracts and Contract Law

Smart contract enforceability varies widely across legal systems. The UK Jurisdiction Taskforce of the LawTech Delivery Panel concluded that smart contracts are capable of giving rise to binding legal obligations under English law and that a contract may be formed and evidenced by code [31], a position summarized for practitioners by Makarova and Maughan [32]. Conversely, civil law jurisdictions often require express legislative recognition or specific legal interpretations to fully integrate smart contracts into their existing contractual frameworks, particularly concerning consumer protection and liability allocation [33]. The 2016 DAO exploit illustrates these tensions: although technically correct in execution, the event raised crucial concerns about consent and intent — highlighting that “code is law” may not override traditional equitable principles [34]. The OConsent protocol offers one response, providing a privacy- and consent-aware architecture that integrates smart contracts with off-chain legal documentation and governance [35]. In cross-border contexts such as maritime logistics, Singapore's adoption of the Model Law on Electronic Transferable Records is a notable step forward — granting legal status to blockchain-based instruments such as digital bills of lading [36], [37] — yet as of 2026 only thirteen States and territories had enacted legislation based on or influenced by that Model Law, and Vietnam was not among them [38]. The challenge of achieving global harmonization of smart contract enforceability therefore remains, as differing legal interpretations of contract formation, dispute resolution, and governance persist [34]. Where deterministic execution cannot accommodate unforeseen contingencies, the practical remedy adopted in this paper is a hybrid instrument:

machine-executable logic bounded by a human-readable master agreement that specifies governing law, evidentiary status, and fallback procedures.

2.3. Governance, Jurisdictional Ambiguity, and Integration Risk

Decentralized governance models prevalent in blockchain networks frequently conflict with centralized legal and regulatory frameworks, generating jurisdictional ambiguity over accountability, liability, and enforcement in multi-stakeholder permissioned systems. The Tezos initial coin offering litigation (*In re Tezos*) illustrates this concretely: courts asserted jurisdiction over a foundation using a globally distributed blockchain even though the underlying smart contract and assets were coded and held abroad [39]. This case underscores the complex interplay between technological decentralization and traditional jurisdictional principles, highlighting the persistent challenge of reconciling immutable, distributed ledgers with established legal concepts of territoriality and control [40]. Similarly, the increasing prevalence of Decentralized Autonomous Organizations further complicates legal accountability, as collective decision-making blurs traditional lines of participant liability and governance [41], [42], [43]. The Liechtenstein Blockchain Act (2020) provides one approach by offering legal recognition for token holders and blockchain-based entities [44]. This jurisdictional dilemma is intensified by the “code is law” paradigm often espoused in blockchain communities, which clashes with established legal systems that rely on human interpretation and judicial discretion [45]. Sector-specific studies confirm that the value of on-chain evidence in dispute resolution depends on prior agreement about its evidentiary status rather than on the ledger itself [46].

Integration into legacy systems and convergence with other emerging technologies introduce layered legal and technical risks that existing frameworks struggle to address. Adaptive legal frameworks capable of addressing the rapid pace of technological innovation are therefore needed [47]. Integration with Artificial Intelligence and the Internet of Things escalates these risks by expanding the attack surface [48]. Comparable tensions have been documented in other regulated sectors: privacy-preserving blockchain designs in healthcare illustrate the same trade-off between verifiability and confidentiality [49], [50], while systematic reviews of the GDPR–blockchain tension confirm that the conflict is structural rather than implementation-specific [51]. Risk-management studies in regulated industries reach the same conclusion about the need for explicit governance of residual risk [52], [53]. These considerations are treated here not as an independent research theme but as inputs to the operational layer of the framework, where monitoring, incident response, and periodic review are specified.

2.4. Competitive Conduct: A Design Dimension Not Yet Operationalized in Existing Frameworks

A port community system is, by construction, an arrangement in which competing undertakings exchange operational information. Carriers that compete on the same trade lanes, terminal operators that compete for the same calls, and freight

forwarders that compete for the same shippers are asked to write to and read from a shared ledger. In European Union law this places the arrangement within the scope of Article 101 of the Treaty on the Functioning of the European Union, and the Commission's horizontal cooperation guidelines set out when information exchange between competitors becomes a restriction of competition [11]. The regulatory environment has recently become stricter rather than more permissive: the Consortia Block Exemption Regulation, which had provided a safe harbor for liner shipping consortia, expired on 25 April 2024 after the Commission decided not to renew it, with the consequence that operators must now self-assess each cooperation arrangement against Article 101 [54]. That block exemption covered vessel-sharing liner consortia rather than port-community data platforms, so its lapse illustrates a stricter enforcement climate rather than the removal of a safe harbor this class of arrangement ever enjoyed. The Archipels merger-control assessment shows that competition authorities examine precisely whether a permissioned-blockchain joint venture creates a channel for information exchange among rivals [23]. A body of scholarship has already examined blockchain under competition law — Munari showing that the cargo-data visibility of TradeLens could generate anti-competitive effects by making commercially sensitive information available among competitors [10], alongside broader analyses of anti-competitive agreements and abuse of dominance in decentralized and permissioned systems [55], [56], [57]. That work diagnoses the risk at the level of doctrine and enforcement; what it does not do — and what this paper contributes — is to operationalize competitive conduct as a generative design dimension inside a deployment framework, on the same footing as data protection and evidentiary validity.

Vietnamese law contains a functionally comparable constraint. The Law on Competition prohibits agreements between enterprises on the same relevant market that fix prices, divide markets or customers, or restrict output, and additionally prohibits other agreements where they cause or may cause a significant anti-competitive effect [58]. Neither regime prohibits port-community data sharing as such; both require that the design of the sharing arrangement be justified. This has direct architectural consequences — minimization by competitive sensitivity, aggregation and delay of commercially sensitive fields, tiered access, and neutrality of the operating entity — and it is therefore incorporated into the Legal Layer as a fifth dimension rather than left as a compliance afterthought.

2.5. Stakeholder Ecology in Port Communities

2.5.1. Participatory design and legal sensitivity

Permissioned blockchain deployment in multi-stakeholder port communities requires participatory design that integrates legal sensitivities from the outset, involving port authorities, shipping companies, customs agencies, and technology providers in an iterative co-design process. This iterative process helps to build consensus among stakeholders, which is crucial for the long-term viability and successful adoption of complex distributed ledger technologies in a highly

regulated environment [13]. The active involvement of legal experts throughout the design and implementation phases is paramount to translate regulatory requirements, such as data protection principles and smart contract enforceability, into concrete technical specifications and operational protocols [59].

2.5.2. Trust, transparency, and interoperability

Successful deployment in port communities depends not only on cryptographic assurance but also on institutionally credible governance arrangements through which participants can understand who validates transactions, who can access data, and how disputes are escalated. Trust must therefore be designed simultaneously at the technical level — identity, logging, access control — and at the collaborative-governance level — participation rules, transparency commitments, and shared procedures for exception handling [60], [61], [62]. In practice, interoperability requires common data models, API-based integration with legacy port systems, and legal agreements clarifying the evidentiary status of shared records across organizational boundaries [63], [64]. Standardized information exchange has been examined as a route to environmental and efficiency objectives in maritime transport, which broadens the set of beneficiaries beyond the immediate transacting parties [65] and connects port-community design to the wider literature on shared industrial infrastructure [66].

2.5.3. Legal enablement and cross-sectoral coordination

Legal enablement strategies for permissioned blockchain systems in port communities must focus on developing adaptable regulatory sandboxes and industry-specific guidelines that bridge the gap between existing legal frameworks and novel technological capabilities. Cross-sectoral coordination is paramount, bringing together legal professionals, technology developers, and maritime industry experts to co-create solutions that are both legally compliant and technologically innovative [64]. This collaborative effort facilitates the harmonization of diverse legal interpretations and technical standards across jurisdictions [67], and can lead to industry-led consortia that define best practices and self-regulatory mechanisms [68], [69], [70]. Table 1 sets out the roles of fourteen stakeholder groups in permissioned blockchain ecosystems within port communities. The list is constructed from the question “who is affected by the system” rather than “who operates it,” which brings in trade-finance and insurance interests, foreign customs authorities, small shippers, and port labor. The addition is not cosmetic: a bill of lading is a transferable instrument with financing value, so banks issuing letters of credit and protection-and-indemnity insurers determine in practice whether an electronic instrument is acceptable, irrespective of whether the consortium considers it valid.

2.6. Evidence from Consortium Failures

The literature reviewed above is drawn almost entirely from platforms that were operating at the time of writing, which introduces a survivorship bias into the design requirements the field has derived. The single most informative case in maritime blockchain is a discontinued one. TradeLens, developed by A.P. Moller – Maersk and IBM and at its peak

the largest platform of its kind, was announced for discontinuation on 29 November 2022 and taken offline in the first quarter of 2023. The stated reasons were that “the need for full global industry collaboration has not been achieved” and that the platform “has not reached the level of commercial viability necessary to continue” [7]. A case analysis conducted through the lens of commons theory attributes the failure to a lack of stakeholder engagement, unclear governance, and confidentiality concerns [8]; a broader study of blockchain technology providers identifies founder power concentration and centralized decision-making as recurring failure mechanisms [9]. Reviews of the maritime landscape reach a similar conclusion about the gap between technical feasibility and institutional adoption [73]. Broader adoption research corroborates the diagnosis: a study of blockchain adoption in the maritime supply chain identifies operator neutrality, stakeholder salience, and reachable critical mass as decisive barriers [74], and a critical review of adoption models prompted by the TradeLens discontinuation, together with a case reconstruction of the platform, reaches the same conclusion about the need for industry-wide collaboration and adaptive governance [75], [76].

Two design requirements follow, and neither is derivable from the legal literature alone. First, the neutrality of the operating entity is a precondition rather than a governance preference: competitors will not write commercially sensitive events to a ledger controlled by one of their number, however lawful the arrangement. Second, participation reaches a critical mass or the network produces no coordination benefit, which means that onboarding cost for the smallest participants is a design variable of the same order as cryptographic assurance. The framework in Section 4 accommodates both: Section 4.2 (S4) states the critical-mass condition as an explicit gate, and Section 4.6 states the neutrality boundary condition.

2.7. Positioning Against Prior Law-and-Architecture Scholarship

The proposition that legal requirements should be embedded in technical architecture rather than appended to it is not new, and this paper engages the scholarship in which it originates. Lessig argued that law, architecture, norms, and markets operate as interacting modalities of regulation and that law frequently regulates indirectly by regulating architecture [77]. Hildebrandt developed the distinction between “legal by design,” where compliance is hard-coded, and “legal protection by design,” where the architecture preserves the contestability that legal protection requires [78], [79]. Finck examined the co-production of European Union law and blockchain architecture and separated the governance of blockchain from governance by blockchain [80]. De Filippi and Wright advanced a parallel argument about the rule of code [81]. Within blockchain governance specifically, van Pelt and colleagues developed a multi-layer governance framework with six dimensions [82], and systematic reviews have mapped governance across architectural and process layers [42], [83]. Closest to the present design are two recent frameworks: a pattern-oriented, four-layer reference

architecture for governance-driven blockchain systems [84], and a framework that aligns stakeholder interests, governance requirements, and blockchain design “control points” in business–government information sharing [85]; a parallel strand in the data-protection literature proposes compliance-by-design combinations of off-chain storage, keyed hashing, redactable ledgers, and consortium governance [86]. A further body of prior art must be named, because it anticipates the *form* of Layer 0 directly: the “do-you-need-a-blockchain” decision frameworks of the late 2010s. Wüst and Gervais’s widely used decision tree asks whether multiple writers exist and whether an always-online trusted third party can be used, and returns “don’t use blockchain” for most paths [87]; the NIST blockchain overview reproduces a flowchart of the same logic [88]; and Pedersen, Risius, and Beck offer a ten-step decision path for managers [89]. The conclusion that most candidate applications do not need a blockchain has therefore been the consensus of that literature since 2018, and this paper does not claim it as a discovery.

Against that background, the contribution claimed here is deliberately narrow. The layered form is inherited, not invented. What this paper adds is threefold, and each element is stated as a *residual* over the prior art just named. First, it makes jurisdiction-specific legal obligation the input to the layering, rather than treating law as an undifferentiated constraint; the comparative reading in Section 5 shows that the same framework produces materially different design postures across three legal environments — a dimension no decision tree in the 2018 family carries. Second, relative to that family, Layer 0 is not the invention of the necessity question but a *tightening and extension* of it in three specific respects: (i) where the 2018 trees test necessity against a weak null alternative — a conventional centralized database — S3 tests it against the strongest non-replicated designs — a mutually notarized threshold-signed log, and a sector interoperability standard — so the region in which blockchain survives the screen is deliberately narrower; (ii) where the trees ask abstractly whether a trusted third party “can be used,” S1 requires the question to be answered institutionally, against a list of named candidate keepers with their mandates examined (Section 5.3.1 does this for three candidates at Cat Lai); and (iii) the trees contain no economic gate at all, whereas S4 conditions deployment on the participation economics of Equations (2)–(3). Third, and most substantively, the paper provides an article-level reading of the Vietnamese instruments and derives from it a design posture that the comparative literature cannot currently express, because that literature operates with a binary distinction between jurisdictions that have enacted the Model Law on Electronic Transferable Records and those that have not, and Vietnam occupies a third position: electronic transactions are broadly enabled, while transferable trade documents remain governed by sector-specific rules. Relative to the governance architectures and the decision-tree family alike, the distinguishing combination is therefore the strongest-null necessity test, the institutional and economic gates, the jurisdiction-specific generative input, and the explicit competition dimension — rather than either the layered form or the necessity question itself.

Table 1. Stakeholder roles and legal-technical contributions in permissioned blockchain design

Stakeholder	Primary role	Legal contribution	Technical contribution
Port authorities	System oversight, regulatory enforcement	Ensure compliance with port regulations, customs law, maritime codes	Define node architecture, access levels, audit trails
Shipping companies	Data providers and users	Align smart contract terms with commercial shipping agreements	Provide operational data, integrate with cargo management systems
Customs agencies	Regulatory enforcement, border control	Enforce compliance with import/export laws, validate data retention and disclosure standards	Validate documents, interface with national customs systems
Technology providers	System developers and integrators	Translate legal requirements into system design	Develop infrastructure, implement cryptographic features, identity management
Legal experts / law firms	Legal advisory and compliance verification	Interpret jurisdictional laws, draft binding contract frameworks, ensure data sovereignty	Collaborate on smart contract enforceability, provide audit guidelines
Logistics operators / freight forwarders	Supply chain orchestrators	Ensure documentation matches regulatory requirements	Integrate IoT and tracking data, trigger smart contract events
Government bodies / legislators	Policy shaping, standard setting	Define regulatory sandboxes, cross-border legal alignment, dispute resolution mechanisms	Enable API-level access for national legal registries or digital ID validation
Consortia / industry alliances	Cross-sector coordination and standardization	Develop model legal agreements, governance templates	Define interoperability standards, test cross-platform operability
Academia / research institutions	Knowledge support, testing and evaluation	Propose new governance models, assess legal risks in design phase	Prototype systems, assess scalability, support pilot testing
Shippers and small import-export firms	Data subjects and cost bearers	Bear consent, disclosure, and onboarding obligations without in-house legal capacity	Require low-cost, low-integration access channels
Trade-finance banks	Financiers of the underlying transaction	Determine whether an electronic instrument satisfies documentary credit requirements	Require verifiable presentation and title-transfer evidence
Insurers and P&I clubs	Risk carriers	Determine insurability of electronic title documents and allocate loss	Require auditable provenance and non-repudiation evidence
Foreign customs authorities	Recognition gatekeepers at destination	Decide admissibility of consortium-issued documents in their own procedures	Require interoperable formats and verifiable signatures
Port labor and hauliers	Affected operators of the physical process	Hold collective-bargaining and employment interests in process automation	Determine feasibility of gate-event capture at the point of work

Source: authors' synthesis from [59], [60], [62], [64], [67], [68], [71], [72].

2.8. Summary and Research Gap

The literature reveals substantial progress in addressing individual dimensions of blockchain deployment in port communities. Technical frameworks for blockchain applications in maritime supply chains have established the architectural possibilities available to system designers [62], [64]. Privacy-preserving design studies have elaborated GDPR-compliant techniques — including off-chain storage, cryptographic hashing, and zero-knowledge proofs — that partially reconcile blockchain immutability with data subject rights [16], [19], [26]. Blockchain governance scholarship has identified the institutional accountability structures and role-allocation mechanisms that permissioned networks require [42], [71], [72], [82], [83]. Studies on stakeholder coordination in port communities have further demonstrated that trust and interoperability cannot be achieved through technical design alone but depend equally on institutional governance arrangements [59], [60], [64].

However, these contributions remain partial and disconnected in four respects. First, existing frameworks treat legal compliance as a downstream checklist rather than an upstream design variable — legal requirements are mapped onto architectural choices after the system has been conceptualized, rather than driving those choices from the outset. Sec-

ond, no existing study provides a cross-jurisdictional integration mechanism: the literature addresses GDPR compliance, or smart contract enforceability, or governance accountability, but not their interaction under conditions of jurisdictional divergence — the defining condition of multi-stakeholder port ecosystems. Third, the literature lacks a structured adaptation mechanism for responding to legal change over time; existing models are static snapshots rather than adaptive governance instruments. Fourth, although competitive conduct has been examined in competition-law commentary [10], [55], it has not been operationalized as a design dimension in existing deployment frameworks, even though every port-community arrangement is an information exchange among rivals and the European safe harbor for shipping consortia has now lapsed [54]. These gaps collectively point to the need for an integrated framework that begins with jurisdiction-specific legal obligations, translates those obligations systematically into governance and architectural design choices, and embeds a feedback mechanism for adapting to regulatory change — all calibrated to the particular multi-stakeholder ecology of port communities.

3. Methodology

This study adopts a qualitative multi-method design that combines doctrinal legal analysis, functional comparative synthesis, and design science-inspired conceptual modeling to examine how legal frameworks shape the design of permissioned blockchain systems in multi-stakeholder port communities. The methodological logic follows design science research in that the study builds an artifact — a legal-responsive framework — from a clearly specified problem domain [90], [91]. Design science distinguishes the construction of an artifact from its evaluation. The present paper completes construction and then subjects the artifact to a set of *formative*, *artificial*, *ex-post* robustness probes in the sense of Venable, Pries-Heje, and Baskerville: multi-case comparison against independent real-world platforms, simulation of its cost logic, and a benchmark of competing frameworks, each scored against criteria fixed in advance (Section 5.4) [92], [93]. Two qualifications bound what these probes can show. First, in the FEDS framework artificial evaluation is the weakest evidential tier — Venable and colleagues note that to the extent an artificial setting is unreal, results may not correspond to real use — so the probes test coherence, external consistency, and robustness, not efficacy; they do not change the paper’s evidential class. Second, the probes are reported with their failures: the multi-case episode returned a negative result against one of the pre-stated criteria, which prompted a disclosed repair to the artifact (Section 4.2, S4). Naturalistic evaluation with intended users remains the outstanding step and is specified in Section 7.2. Section 5 is therefore an application (Sections 5.1–5.3) followed by formative artificial probes (Sections 5.4–5.7), not an empirical case study.

3.1. Unit of Analysis and Analytical Dimensions

The unit of analysis is the legal-technical design decision. Legal materials were selected using three criteria: (i) direct relevance to electronic trade documents, data protection, cybersecurity, smart contracts, competitive conduct, or port-community data exchange; (ii) current normative force or authoritative guidance in the jurisdiction examined; and (iii) operational significance for permissioned blockchain deployment.

A single set of five dimensions is defined in Table 2 and used throughout the paper, from the abstract to the comparative application. Each dimension carries sub-codes, which are the units actually applied to the text of each instrument. The comparative tables in Section 5 additionally report three context descriptors — institutional coordination model, legacy-system integration, and indicative design posture — which are not legal dimensions but describe the environment in which the legal dimensions operate, and are labeled as such.

Table 2. Analytical dimensions, sub-codes, and design relevance

Dimension	Sub-codes applied to each instrument	Primary design determinant affected
D1. Data governance and cross-border transfer	Lawful basis; purpose limitation; minimization; data-subject rights; controller / processor / joint-controller allocation; localization duties; outbound-transfer conditions	Lawful data location and transfer
D2. Contractual and evidentiary validity	Validity of data messages; electronic signature status; transferable-record recognition; smart-contract recognition; sector-specific carve-outs	Evidentiary and contractual validity of records
D3. Accountability and liability	Role allocation; liability apportionment; forum selection and governing law; audit and reporting duties	Liability, audit, and reporting obligations
D4. Operational security	Authentication duties; log retention; incident reporting; cooperation with competent authorities; critical-infrastructure classification	Hosting, logging, and incident-response design
D5. Competitive conduct	Prohibited agreements between undertakings on the same relevant market; <i>abuse of a dominant position and essential-facility access</i> ; information-exchange assessment; block-exemption availability; merger-control exposure of joint ventures; <i>data-portability and interoperability duties</i>	Data granularity, latency, access tiering, operator neutrality, and open-access obligations

Source: authors’ construction. The full instrument-by-dimension coding matrix is given in Appendix A.

3.2. Comparative Logic

For the comparative phase, the *tertium comparationis* is the functional question of how each jurisdiction enables or constrains legally reliable digital transactions among port-community actors [94]. The comparison is framed as a social problem posed identically to each jurisdiction: on what conditions can party B rely on an electronic record originated by party A, and what must the system do to make that reliance lawful? Functional equivalents are then sought in each system irrespective of the doctrinal label under which they appear.

The reference jurisdictions are Singapore and the Netherlands within the European Union legal order; Rotterdam and Cat Lai appear as port-level illustrations within their respective jurisdictions, not as comparators, since a port has no legislative competence in data protection.

3.3. Coding Protocol

The coding protocol is stated explicitly so that the analysis can be reproduced. A codebook was constructed from the sub-codes in Table 2, with a decision rule for each sub-code specifying what textual evidence counts as a positive coding. Each instrument was read in full and coded provision by provision against the codebook; the resulting instrument-by-dimension matrix is reported in Appendix A. Coding was

carried out by the two authors responsible for legal-source compilation and for comparative legal design, working from the primary text in each case, with disagreements resolved by joint re-reading of the provision. Because this was consensus coding rather than independent double-coding, an inter-coder reliability coefficient cannot meaningfully be computed; we state this plainly rather than report a spurious statistic. Reproducibility rests instead on two artifacts made available with the paper: the full codebook, with a decision rule for each sub-code, provided as supplementary material, and the instrument-by-dimension matrix in Appendix A. Where an instrument was silent on a sub-code, silence was coded as such rather than inferred, and this is visible in Appendix A.

3.4. Research Phases

1. Phase 1 – Doctrinal legal analysis. Relevant statutes, regulations, model laws, and institutional guidance — including the GDPR, the EDPB blockchain guidelines, the PIPL, eIDAS, the UNCITRAL Model Law on Electronic Transferable Records, the horizontal cooperation guidelines under Article 101 TFEU, and selected Vietnamese legal instruments — were interpreted to identify binding obligations, permitted design space, and legally sensitive failure points for blockchain deployment in port ecosystems.

2. Phase 2 – Comparative synthesis. The coded legal materials were compared across jurisdictions to identify functional convergence and divergence. This step translates doctrinal variation into comparable design problems.

3. Phase 3 – Conceptual modeling. The comparative findings — recorded in full in the instrument-by-dimension matrix of Appendix A — were used to populate an inherited layered form: a screening gate placed ahead of four coupled layers linking legal requirements to governance structures, system architecture, and operational controls. The layered form itself is taken from prior blockchain-governance scholarship (Section 2.7); the contribution of this phase is the population of that form from jurisdiction-specific coded material and the addition of the screening gate, not the invention of layering. The resulting model is prescriptive rather than predictive.

4. Phase 4 – Claim specification and disconfirmation design. The framework’s substantive claims are stated as propositions with boundary conditions, together with the designs the framework excludes and the observations that would disconfirm it (Section 4.6), so that the framework is a theory testable against evidence rather than a taxonomy that no observation can contradict.

To demonstrate contextual relevance, the framework is applied to Singapore and to the Netherlands and the European Union as reference jurisdictions and then to Vietnam through a scenario-based policy and architecture assessment. These applications are analytical rather than empirical case studies, and are evaluated ex-post in Sections 5.4–5.7. [Figure 1](#) presents the workflow, which is iterative rather than purely linear: scenario application refines the framework, while the framework in turn structures subsequent legal comparison and design revision.

4. Conceptual Framework Development

4.1. Theoretical Anchoring

The proposed framework is grounded in three complementary literatures: design science research, which justifies the construction of a normative artifact for solving a class of design problems [90], [91]; functional comparative law, which supports comparison on the basis of equivalent regulatory problems rather than formal doctrinal labels [94]; and blockchain governance studies, which show that institutional rules, technical architecture, and operational controls are co-produced rather than independent [42], [62], [82]. Its normative premise — that legal protection must be inscribed in architecture rather than appended to it — is inherited from Lessig and from Hildebrandt, and the layered form from blockchain-governance scholarship. What this framework adds to that tradition is not anticipated by the law-and-architecture works it builds on: a screening gate whose necessity core descends from the decision-tree family and is tightened here (Section 2.7), and the treatment of provision-level legal obligation as a generative design input rather than a downstream constraint. It is therefore an operationalization of legal protection by design for one class of systems, but a non-trivial one [77], [78], [80].

4.2. Layer 0: Necessity and Viability Screening

The framework begins by asking whether a permissioned blockchain is the appropriate instrument at all — a question worth posing because every substantive recommendation the framework produces has the effect of moving data off the chain. Personal data is held off-chain; authoritative documents are held off-chain; contractual fallbacks are held off-chain; existing customs and terminal systems are not replaced. What remains on-chain is a timestamped, access-controlled log of hashes and status events. A signed append-only database with interoperability interfaces can produce the same artifact at materially lower cost, and a framework that never tests this is at risk of rationalizing a technology choice rather than evaluating it.

Layer 0 therefore poses four screening questions in sequence:

S1. Is there an institutionally available third party that all intended participants would in fact accept as the sole keeper of the authoritative record? Availability here means more than legal possibility: the candidate must be reachable at acceptable cost, be free of a commercial stake in the transactions it records, and be acceptable to every participant. Where such a party exists, a conventional shared system administered by it is the lower-cost design and the screen is not passed.

S2. Does the process require multiple organizations to write to a shared record with non-repudiation, such that no single participant can be trusted to maintain the authoritative sequence of events? If writing is effectively single-sourced, replication adds cost without adding assurance.

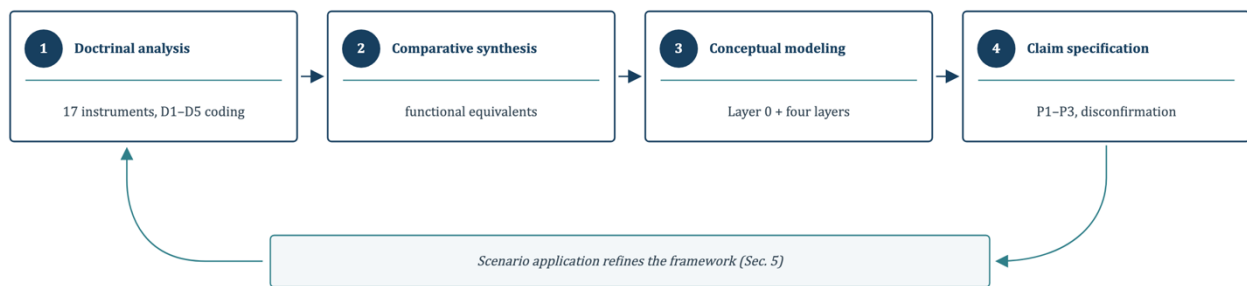


Figure 1. Iterative methodological workflow for framework development and scenario-based refinement

Source: authors' synthesis based on design science research and the functional comparative-law method [90], [91], [94].

S3. Would a non-replicated alternative satisfy the same evidentiary and coordination requirements? The alternative must be taken in its strongest available form, of which there are two: a mutually notarized, threshold-signed, append-only log administered by a neutral convener, delivering multi-party non-repudiation and tamper-evidence without a replicated consensus machine; and a sector-wide interoperability standard with competing conformant platforms — the path container shipping has taken for the electronic bill of lading through the DCSA standards, which requires neither a single keeper nor a shared ledger [95]. If either form suffices, that design should be preferred, because it supplies the coordination assurance at lower cost than replication.

S4. Do the binding routing commitments of the essential participant classes — take-or-pay minima or equivalent charter obligations, not statements of intent — sum to at least the break-even volume $Q(\text{be})$ of Equation (2), and is the participation condition of Equation (3) satisfiable for every essential participant? The commitment form of this question is deliberate. Demand forecasts for infrastructure are both systematically optimistic — transport demand forecasts err by on the order of a factor of two, with strategic misrepresentation a documented mechanism [96] — and strategically gameable in this setting, since Section 5.3.3 identifies the incumbent platform provider as the participant most likely to violate Equation (3): a gate keyed to a forecast would let an incumbent kill a pilot with a low number or a promoter inflate one with a high number. Commitments are costly signals that neither party can issue insincerely without consequence, and where commitments are not yet obtainable, the fallback is a reference-class forecast in Flyvbjerg's sense — anchored on the realized volumes of comparable consortia (Table 7), adjustable upward only against binding commitments — never an unanchored participant forecast. The reference class must match the adoption regime: for a voluntary-usage workflow the anchor is the realized volumes of Table 7; for a workflow whose channel an authority or operator can mandate, the anchor is the realized volume of the incumbent channel itself — at Cat Lai, the ePort delivery-order volume. Because the sample contains no port-coordination failure (Section 7.1), a voluntary-regime port forecast has no domain-matched reference class, which is a further reason commitments, not forecasts, are the primary ad-

missible evidence at S4, and the forecast route is a bridge only, never a substitute. Two further disciplines bound this question. First, because $Q(\text{be})$ itself depends on the participant set, the datasets, and the transfer routes (Section 5.3.3), S4 is an existence condition for a joint fixed point of commitments and cost, not a comparison against a fixed threshold. Second, a stopping rule for the screen as a whole: Layer 0 comprises the inherited necessity core S1–S3 — each a cost-dominance test against a non-replicated design delivering the same assurance — and admits *additions* only where they are derivable a priori from the participation constraints of Equations (2)–(3); S4 itself is Equation (3) promoted from the cost model to the gate — a procedural reordering of machinery the framework already contained, not a new theoretical element — and the same rule is what prevents the screen from accreting an S5, S6, and so on as new failure modes are observed: a failure cause that cannot be expressed as a violation of the participation constraints is recorded as a scope limit, not absorbed as a new gate. One further discipline closes a loop the framework itself opened: the commitment round is an arrangement among competing undertakings and therefore falls within dimension D5 before it can serve as a gate input. Individual take-or-pay levels are commercially sensitive forward-looking information, so commitments are collected bilaterally by the participant-independent operating entity and disclosed horizontally only as the aggregate sum tested against $Q(\text{be})$, never as individual figures; and the commitments' compatibility with Article 101(3) TFEU and Articles 11–12 of the Law on Competition is documented as an ancillary-restraint self-assessment in the competition-compliance charter. That the framework's own viability gate is disciplined by its own competition dimension is a consistency requirement, not an afterthought. S4 was not part of the screen as originally constructed; it was added when the multi-case evaluation of Section 5.5 showed that S1–S3 predict the design real platforms adopt but not whether they survive. The provenance is disclosed deliberately, and Section 7.2 specifies the prospective test the repair still owes.

A permissioned blockchain is indicated only where S1 is answered negatively, S2 affirmatively, S3 negatively, and S4 affirmatively. This gate is what allows the framework to return the answer “do not deploy,” and it is the reason the frame-

work can be described as prescriptive rather than merely descriptive. Applied to the Vietnamese scenario in Section 5.3, S1–S3 are passed for release-order and gate-event coordination — where carriers, terminals, and hauliers each dispute the others' record of what was authorized and when — and are not passed for document storage, which is accordingly kept off-chain; S4 remains undetermined for Cat Lai until binding routing commitments exist, so the screen's answer there is conditional, not an endorsement.

Because S3 is tested against a threshold-signed multi-party log and a sector interoperability standard, and not merely against a single-administrator database, the region in which the screen's answers jointly indicate a blockchain is narrow. It is the case in which a neutral convener is acceptable enough to the participants to coordinate the consortium at all, yet not trusted enough by competing participants to be the sole keeper of one signed log even under independent attestation, so that assurance must be placed in a replicated consensus protocol rather than in any single administrator's process — the condition the TradeLens experience documents. Where the assurance margin between a threshold-signed log and a replicated ledger is too small to justify the additional cost, the framework's default is to return the multi-party log and to treat the blockchain as an exception that must be affirmatively earned. A screen that defaults against replication rather than toward it is the strongest form of the necessity claim, and it is what distinguishes a framework that evaluates the technology from one that presupposes it.

4.3. Framework Architecture: The Four Design Layers

The choice of four layers follows the logic of how compliance constraints travel through a permissioned blockchain system in port ecosystems. The Legal Layer defines the binding normative environment; the Governance Layer translates those norms into decision rights, accountability, and dispute processes; the Architectural Layer encodes those choices into data location, identity, consensus, and interface design; and the Operational Layer governs day-to-day execution, auditing, exception handling, and inter-organizational interoperability [71], [72].

1. Legal Layer – captures data-protection, electronic-transactions, contract, cybersecurity, jurisdictional, competitive-conduct (both anti-competitive agreements and abuse of a dominant position), and data-portability requirements, following dimensions D1–D5 of Table 2.

2. Governance Layer – allocates roles, validation authority, liability, escalation rules, salt and key custody, and change-management responsibilities.

3. Architectural Layer – defines on-chain/off-chain data placement, salting and selective disclosure, identity and access controls, node design, and middleware integration.

4. Operational Layer – specifies audit routines, exception handling, monitoring, interoperability processes, data protection impact assessment review, and compliance review cycles.

The layers are analytically distinct but operationally coupled. Legal change can trigger governance redesign; governance rules constrain architectural options; architectural

choices determine what can be monitored operationally; and operational feedback — such as audit findings, incidents, or interoperability failures — feeds back into governance review and, when necessary, legal reassessment. Figure 2 visualizes the screening gate, these vertical dependencies, and the feedback loops that connect them.

4.4. Legal-to-Design Mapping

To operationalize the framework, this section maps key legal requirements to their corresponding technical design implications. Each legal mandate is analyzed for its impact on system architecture and is paired with feasible design solutions or mitigation strategies. Table 3 summarizes these relationships. The first row is worth emphasising: off-chain storage is not a solution to the right to erasure but a reallocation of that obligation onto key-lifecycle management, developed in Section 4.4.1.

4.4.1. Secret Lifecycle: Reconciling Erasure, Verification, and Mandatory Retention

The salted-hash architecture creates a tension that the mapping in Table 3 states but does not resolve, and that this subsection addresses directly. The same salt that a controller must destroy to effect erasure is the value a counterparty needs in order to verify an on-chain commitment; a design must therefore decide, per field, whether verifiability or erasability is the governing requirement. Three rules follow. First, salts are scoped per data subject and per record, not shared across a batch, so that destroying one subject's salt to satisfy an erasure request does not disable the proofs on which other parties in the same transaction rely. Second, verification is granted to a counterparty by disclosing the pre-image and salt through a governed off-chain channel for the duration of the verification, not by embedding the salt on-chain; the on-chain commitment remains a bare salted hash. Third, and most consequentially for Vietnam, the erasure duty must be reconciled with mandatory-retention duties that point the other way — Decree 53/2022 requires local retention of specified data for at least twenty-four months once triggered and of logs for at least twelve months, and customs records are retained for years — so the governance layer maintains, per dataset, a retention-versus-erasure precedence table that records which duty prevails and until when. Because destruction of a secret is a negative fact that cannot be audited by inspecting the ledger, the framework treats proof of destruction as a governance obligation discharged through logged, witnessed key-destruction procedures and periodic third-party attestation, not as a cryptographic guarantee. A further consequence must be stated plainly: concentrating both erasure and re-identification power in the salt store makes that store a single point of privacy failure, since compromise of the salts enables re-identification across every record they cover; threshold secret-sharing of salt custody among independent governance holders reduces this exposure but does not remove it. These are limitations rather than solutions, and they are recorded as such in Section 7.1.

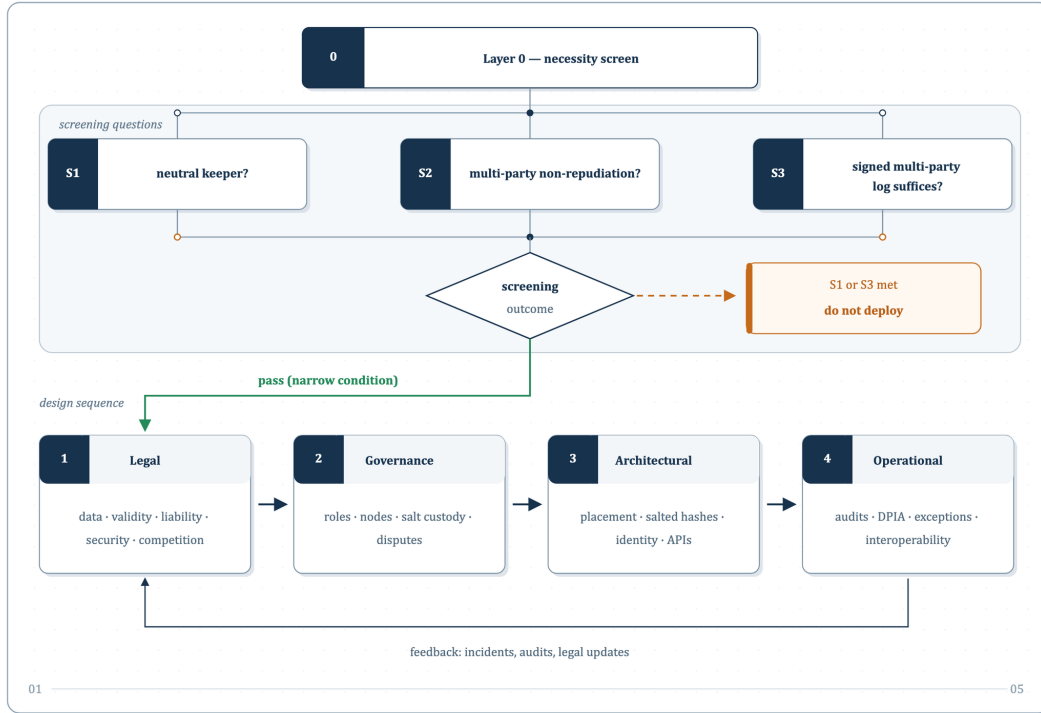


Figure 2. Layer 0 screening (S1–S4, with the S4 viability question supplied by Equations (2)–(3)) and the four-layer legal-responsive framework with vertical dependencies and feedback loops

Source: authors’ synthesis informed by blockchain-governance and port-community-system literature [42], [62], [71], [72], [82].

4.5. Adaptive Governance and the Materiality Workflow

Permissioned blockchains operating within legally diverse port ecosystems require governance structures that are flexible, context-sensitive, and capable of evolving with the regulatory environment. Unlike fully decentralized systems, they require explicit role assignments, decision-making processes, and conflict-resolution mechanisms that are legally grounded enough to withstand scrutiny under contract law, administrative regulation, and applicable liability frameworks. In multi-stakeholder environments such as port communities, governance must additionally address asymmetrical power dynamics, cross-border collaboration, and sector-specific constraints [62]. Adaptable governance requires role-based permissions; jurisdiction-aware policy enforcement; multi-tiered dispute resolution combining automated on-chain procedures with human oversight; periodic governance audits and legal reviews; a competition-compliance review on the same cycle; and modular governance templates that can be repurposed across analogous deployments.

In Figure 3, a legal change is treated as material when it changes at least one of four design determinants: (i) lawful data location or transfer, (ii) consent and identity requirements, (iii) evidentiary or contractual validity of electronic records, or (iv) liability, audit, or reporting obligations. Where no material change is identified, the workflow returns to a scheduled periodic review cycle; where material change exists, the model proceeds to impact assessment, governance approval, technical reconfiguration, and post-change compliance testing.

Three clarifications are added here. First, the four determinants broadly track dimensions D1–D4 of Table 2; a change

touching dimension D5, competitive conduct, is treated as material by the same test, since it alters permissible data granularity and access tiering. Second, a potential tension between the reconfiguration step and the treatment of immutability as binding is resolved by distinguishing the ledger record from the executing logic. Historical state is never rewritten. Reconfiguration proceeds by deploying revised logic behind a stable interface, with the prior contract retained in a terminal state and a governance-approved migration record committed on-chain so that the audit trail remains continuous across the change. Upgrade authority is a governance-layer allocation and must not rest with a single commercial participant; where an upgradeable pattern is used, the identity of the upgrade authority and the approval record become part of the evidentiary package, because a ledger whose logic one party can rewrite unilaterally cannot support a non-repudiation claim against that party. Third, monitoring scans not only instruments in force but also published drafts and bills: the replacement of Decree 13/2023 by the Law on Personal Data Protection 91/2025 — enacted through a public legislative process more than a year before this manuscript’s cut-off — is a change the workflow should have flagged at draft stage. Horizon-scanning of drafts is therefore added to the monitoring step, and Section 7.1 reports this omission as the framework’s first negative test result.

4.6. Framework Claims and Disconfirming Evidence

A framework that excludes no design and can be contradicted by no observation is a classification scheme rather than a theory. This section therefore states the framework’s substantive claims, the designs it rules out, and the observations that would disconfirm it.

Table 3. Legal-to-design mapping for permissioned blockchain compliance

Legal requirement	Technical implication	Design solution / strategy
Right to erasure (GDPR Art. 17; Vietnamese personal-data regime)	Conflict with blockchain immutability; an on-chain hash of personal data is itself personal data	Personal data off-chain; on-chain commitment only as a salted hash; erasure effected by destroying the salt and the off-chain pre-image so that residual on-chain state permits no direct or indirect identification [16], [19], [20], [21]
Salt and key custody	Erasure capability and re-identification risk both depend on secret lifecycle, not on ledger design	Governance-layer allocation of salt generation, custody, rotation, and destruction authority; separation of duties between operator and participants; documented key-compromise procedure [20], [25]
Impact assessment duties (GDPR Art. 35; Vietnamese impact-dossier requirements)	High-risk processing and outbound transfer require documented assessment before deployment	Impact dossiers per dataset and per transfer route maintained in the operational layer and re-run on material change [20], [97], [98]
Information exchange among competitors; abuse of a dominant position	Shared operational ledger can restrict competition between undertakings on the same relevant market; a dominant operator can additionally face abuse-of-dominance and essential-facility-access duties	Minimization by competitive sensitivity; aggregation and delayed release of sensitive fields; clean-team access tiers; competition-compliance charter; neutrality of the operating entity; published fair-access and data-portability terms where a dominance or sector open-access duty applies [11], [23], [54], [58]
Transfer of core and important data (Vietnamese Law on Data)	Categories of non-personal data also attract outbound-transfer conditions	Dataset classification distinguishing personal, core, and important data; per-category transfer rules encoded in access policy [99]
Smart contract enforceability	Variation in legal recognition across jurisdictions	Human-readable master agreement plus legally reviewed smart-contract logic, with governing-law and fallback clauses outside chain code [31], [32], [34]
Cross-border data transfer restrictions	Jurisdictional conflicts in data storage and processing	Data localization, permissioned nodes, and geo-fenced access controls [24], [27], [39]
Data subject consent requirements	Need for explicit, purpose-bound, revocable consent before data use	Consent-management modules and self-sovereign identity controls, with consent records reproducible on request [29], [35], [61]
Jurisdictional ambiguity in disputes	Unclear applicable law and forum in transnational systems	Governance rules on forum, governing law, and dispute escalation; preserved human override [34], [39], [45], [46]
Auditability and legal accountability	Requirement for traceability and non-repudiation	Tamper-evident logs and cryptographic proof of origin and modification, with continuity of the audit trail preserved across reconfiguration [25], [63]
Data minimization principle	Limit on amount and type of personal data processed	Pseudonymization, selective disclosure, and zero-knowledge proofs [19], [26]
Liability allocation in multi-stakeholder systems	Ambiguity in role and responsibility in failure or breach scenarios	Defined node roles, liability clauses, and shared-risk governance models [42], [62]

Source: authors' synthesis.

4.6.1. Propositions

P1 (asymmetric retrofit cost). A defined subset of legal obligations — erasure, localization, evidentiary status of records, controller and processor allocation, and liability apportionment — maps onto architectural primitives that are frozen at the moment the consortium charter, data schema, and node topology are settled. The cost of satisfying these obligations is therefore strongly asymmetric across that point: addressing them earlier is a specification task, addressing them later is a redesign task.

P2 (dimensional sufficiency, bounded). Within the legal envelope, the five dimensions of Table 2 are sufficient to derive the *set of admissible design postures* for a jurisdiction; selection among admissible postures additionally requires the institutional-coordination and legacy-integration descriptors, which are reported separately in Table 4 and are not claimed to be derivable from law alone. P2 therefore concerns the admissible set, not the posture ultimately selected — a distinction made because

the comparative application in Section 5 derives Vietnam's selected posture partly from a non-legal descriptor.

P3 (reversible-event automation). In a jurisdiction where transferable trade documents remain governed by sector-specific rules, automating only reversible, well-defined events — release authorization, handover confirmation, gate status — while keeping authoritative documents and exception handling under human control yields a lower rate of legally unresolvable exceptions than automating title transfer.

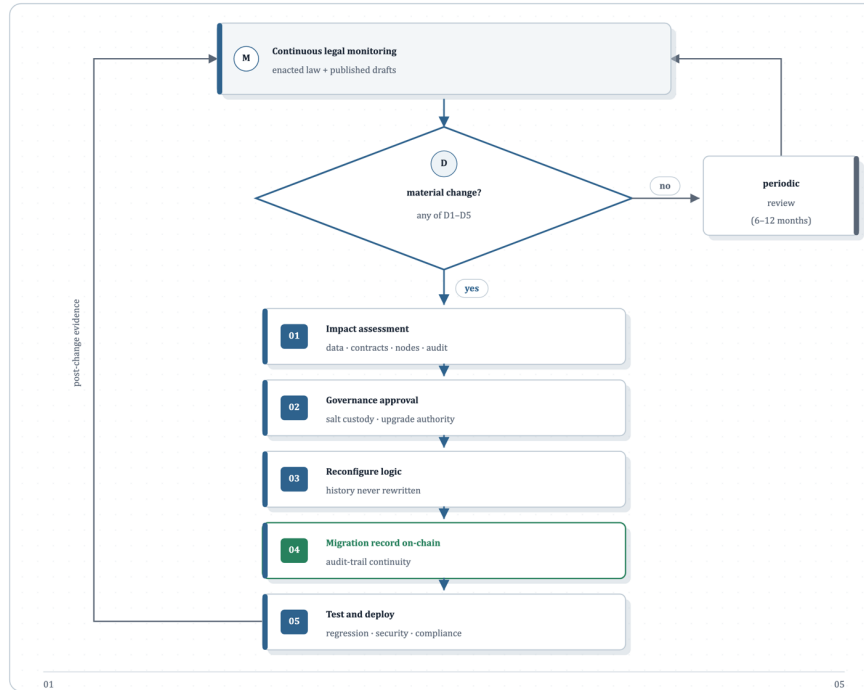


Figure 3. Materiality-based legal adaptation workflow with periodic review cycle

Source: authors' synthesis.

4.6.2. What the framework rules out

- Any design that places signed bills of lading, consignee identity, or commercially sensitive rate information on-chain as plaintext or as an unsalted hash.
- Any upgradeable-contract design in which upgrade authority rests with a single commercial participant, or in which no governance approval record is committed alongside the upgrade.
- Any consortium whose node and permission structure gives one commercial competitor unilateral write or veto authority over another participant's operational events, or whose operating entity is controlled by a participant that competes with other members.
- Any deployment that proceeds to the Legal Layer without passing the Layer 0 screen, including deployments whose only justification is document storage or traceability obtainable from a signed append-only database.

4.6.3. Observations that would disconfirm the framework

1. P2 is disconfirmed by any instrument that alters the *admissible set* of design postures — not merely the posture ultimately selected — without engaging a sub-code of Table 2. To be probative the worked candidate must lie outside all five dimensions, since a duty that D5 already registers cannot falsify a claim about the sufficiency of D1–D5. A mandatory environmental-disclosure or carbon-data-sharing duty imposed on port-community platforms — for example an obligation to collect and share verified vessel- or cargo-emissions data across participants for regulatory reporting — is such a candidate: it would compel a data-collection, retention, and sharing posture that none of D1–D5 registers, and its emergence would require a sixth, sustainability-reporting di-

mension. Interoperability, open-access, and data-portability duties are deliberately *not* used as the worked falsifier, because dimension D5 now registers them explicitly (Table 2, D5); counting them would render P2 unfalsifiable by construction.

2. A deployment in which architecture demonstrably shaped the applicable legal requirement — for instance through a regulatory sandbox in which the design informed the rule — and in which compliance outcomes were better than under the prescribed upstream sequence, would disconfirm the directionality claim of Figure 2.

3. A measured ratio of retrofit cost to design-ahead cost close to unity across operating port community systems would disconfirm P1. This is a feasible measurement and is proposed as the first empirical test of the framework in Section 7.2.

4. A consortium automating irreversible events that recorded no higher rate of legally unresolvable exceptions than a comparable consortium automating only reversible events would disconfirm P3.

5. Application and Evaluation in Port Ecosystems

This section demonstrates the applicability of the framework across three legal environments representing contrasting positions on the legal-technical spectrum: Singapore as a centralized, MLETR-mature digital-trade environment; the Netherlands within the European Union legal order, illustrated at port level by Rotterdam's consortium-based ecosystem; and Vietnam as an emerging context characterized by a fragmented digital infrastructure and a rapidly consolidating legal framework. The purpose is not to claim completed empirical case studies, but to show how the framework sup-

ports structured translation of jurisdiction-specific legal conditions into governance and architectural design choices. Consistently with Section 3.2, the comparators are States and legal orders; ports appear as illustrations within them. Singapore and the Netherlands serve as reference jurisdictions against which the framework's analytical range can be established; Vietnam constitutes the primary original application, drawing on article-level analysis of domestic legal instruments not previously integrated into the blockchain-port community literature. Sections 5.1–5.3 are the application; Sections 5.4–5.7 then subject the framework to formative ex-post probes — against nine real platforms, including four failed neutral consortia selected because they stress the screen, a simulation of its cost rule, and its nearest competing frameworks — using criteria fixed in advance, and report the criterion that failed as well as those that held.

5.1. Comparative Application Across Three Legal Environments

Table 4 applies the five analytical dimensions of Table 2 to the three legal environments and states the resulting design implication in each case. The three rows below the dividing line are context descriptors rather than legal dimensions, and are labeled accordingly.

5.2. Applying the Framework to Vietnam's Port Sector

Vietnam's practical baseline for blockchain deployment is not a paper-only environment but a fragmented digital stack: import and export processing relies on VNACCS/VCIS and the National Single Window at the border-management layer, while large terminal operators such as Saigon Newport have deployed ePort-type platforms for booking, payment, and electronic delivery-order authentication — yet these solutions remain operator-centric rather than port-community-wide, and further information systems have been added alongside VNACCS/VCIS with weak interlinkage across workflows [71], [72], [108], [109], [110]. A further consideration is that VNACCS/VCIS has been in operation since 2014 and a successor digital-customs system is under development; a design that hard-wires integration to the current platform therefore carries obsolescence risk, and the integration layer should be specified as platform-neutral.

The first legal constraint set arises from cybersecurity law. The Law on Cybersecurity 2018 identifies the transport sector as one of the sectors that may contain information systems important to national security (Article 10), and Article 26 imposes duties on relevant service providers concerning user authentication, account security, cooperation with competent authorities, and removal of unlawful content [105]. Decree 53/2022 operationalizes the storage regime by specifying three data categories with localization relevance and by prescribing at least twenty-four months of local storage once a request is triggered, as well as at least twelve months of logs for investigating cybersecurity violations [106]. For port-community blockchain design, the implication is not that every port consortium will automatically be classified as a critical-information system; rather, any internet-facing service layer that processes Vietnamese-user data or depends on foreign-hosted infrastructure should be architected so

domestic storage, lawful-access logging, and cybersecurity-cooperation workflows can be implemented without structural redesign.

The second constraint set concerns personal-data protection. Decree 13/2023/ND-CP ceased to have effect on 31 December 2025; the governing instruments are now the Law on Personal Data Protection No. 91/2025/QH15, adopted on 26 June 2025 and effective from 1 January 2026, together with its implementing Decree No. 356/2025/ND-CP of 31 December 2025 [97], [98]. The statutory regime retains and elevates the features that matter for consortium design: differentiated roles among controller, processor, controller-cum-processor, and third party; purpose limitation and collection proportionate to the stated purpose; data-subject rights of access, correction, withdrawal of consent, deletion, restriction, and objection; consent that must be explicit, purpose-bound, and reproducible; and documented assessment of processing impact and of outbound transfer, with the implementing decree specifying the impact-assessment and transfer-dossier procedures and the data-protection personnel requirements. A viable consortium therefore needs a dataset-by-dataset role matrix, a clear retention schedule, auditable consent and notice records, and an architecture in which personally identifiable information and sensitive commercial data remain editable or deletable off-chain while only salted hashes, timestamps, or status proofs are committed on-chain.

A third constraint set arises from the Law on Data No. 60/2024/QH15, effective 1 July 2025, which regulates data that is not personal data. The Law establishes the national integrated database and, in Article 23, subjects the outbound transfer of core data and important data to conditions relating to national defense, security, and the public interest [99]. This matters for port applications because much of the relevant payload — vessel schedules, cargo manifests, aggregate throughput — is not personal data and therefore falls outside the personal-data regime entirely, yet may fall within these categories. Dataset classification must accordingly distinguish three regimes rather than two.

The fourth and partly enabling rule set comes from the Law on Electronic Transactions 2023. Articles 8–11 confirm that data messages cannot be denied legal validity solely because they are electronic and may satisfy documentary, original, and evidentiary requirements when accessibility and integrity conditions are met; Articles 22–23 recognize electronic signatures and grant secure specialized electronic signatures and digital signatures legal value equivalent to wet-ink signatures. At the same time, Article 1 makes clear that sector-specific legislation still prevails wherever electronic form is restricted or specially regulated [107]. Vietnam is therefore legally more enabling for digital port documentation than under its earlier electronic-transactions regime, but not yet functionally equivalent to a fully MLETR-mature environment across all maritime instruments — and, as the UNCITRAL status record confirms, Vietnam is not among the thirteen States and territories that had enacted MLETR-based legislation as of 2026 [38].

Table 4. Application of the legal-responsive framework across three legal environments

Dimension	Singapore	Netherlands / EU (illustrated at Rotterdam)	Vietnam	Implication for framework
D1. Data governance and cross-border transfer	PDPA emphasises purpose limitation, accountability, and transfer-limitation safeguards for overseas disclosures [100].	GDPR [101] imposes stricter lawful basis, minimization, purpose limitation, and data-subject rights; EDPB blockchain guidance requires salting and impact assessment.	Law on Personal Data Protection 91/2025 and Decree 356/2025 require role allocation, purpose-bound consent, and impact dossiers; Law on Data 60/2024 adds transfer conditions for core and important data.	Keep personal data off-chain; commit only salted hashes; maintain consent and transfer logs; allocate controller and processor roles per dataset; classify datasets as personal, core, or important.
D2. Contractual and evidentiary validity	ETA as amended in 2021 adopts MLETR-style recognition of electronic transferable records [102]; smart contracts sit within ordinary contract law.	Electronic records and signatures are recognized under eIDAS [103], but transferable trade-document practice still depends substantially on platform rules and contractual structuring.	Law on Electronic Transactions 2023 gives data messages documentary, original, and evidentiary value where integrity and accessibility conditions are met; Article 1 preserves sector-specific rules, and Vietnam has not enacted MLETR.	Use a hybrid contract architecture: machine-executable logic plus human-readable master terms, governing-law clauses, and evidentiary provisions; do not use the chain as a title-transfer rail where sector rules prevail.
D3. Accountability and liability	PDPA imposes an accountability obligation on organizations for personal data under their control, including data processed by intermediaries on their behalf [100].	GDPR Articles 24, 26, and 28 allocate controller, joint-controller, and processor duties, with Article 82 governing compensation; shared governance across multiple operators makes this allocation contested rather than given.	The controller / processor / joint-controller taxonomy means participant roles must be allocated dataset by dataset rather than assumed collectively.	Define RACI-style decision rights, escalation paths, legal-review forums, and auditable responsibility matrices in the governance layer; attach processor agreements and change-control procedures.
D4. Operational security	Digital-trade initiatives operate within a comparatively centralized regulatory environment with strong incident-response oversight.	Cyber risk is managed through EU-style risk management, reporting duties, and distributed community operators.	Law on Cybersecurity 2018 and Decree 53/2022 make user-data handling, domestic storage, cooperation duties, and long-form logging operationally salient for internet-facing services.	Prefer domestic hosting for sensitive layers; segment sensitive nodes; preserve investigation logs and regulator audit access; build incident-response routines into the operational layer.
D5. Competitive conduct	Competition rules apply to information exchange, but centrally steered initiatives reduce the risk of participant-controlled gatekeeping.	Article 101 TFEU applies directly; the consortia block exemption [104] lapsed on 25 April 2024, so each arrangement must be self-assessed against the horizontal guidelines.	Law on Competition 2018 prohibits agreements between undertakings on the same relevant market that fix prices, divide markets, or restrict output, and other agreements causing significant anti-competitive effect.	Minimize by competitive sensitivity; aggregate and delay sensitive fields; apply clean-team access tiers; adopt a competition-compliance charter; ensure the operating entity is not controlled by a competing participant.
Context: institutional coordination model	Central public steering supports tighter permissioning and faster policy alignment.	Neutral community coordination relies on multi-actor service integration and shared governance.	Hybrid: customs and ministries anchor compliance interfaces, while terminals, carriers, brokers, and hauliers control operational data.	Adopt a consortium charter with a public-law compliance forum and a private operational steering group.
Context: legacy-system integration	Nationally coordinated digital-trade infrastructure provides integration momentum.	Port-community services support broad information exchange across many operators.	VNACCS/VCIS and the National Single Window digitize filing and status exchange, but customs runs many parallel systems and terminals rely on operator-specific ePort tools; a successor customs system is under development.	Use API middleware and a canonical event schema; overlay fragmented systems rather than replace them; keep the integration layer neutral with respect to the customs platform generation.
Context: indicative design posture	A compliance-oriented consortium can scale faster once institutional approval is secured.	An interoperable consortium should remain open to neutral interfaces and federated identity services.	Best near-term posture is a bounded permissioned pilot for release-order, handover, and gate-event coordination, with documents off-chain and salted hashes on-chain.	Scale only after legal practice stabilises and customs and terminal links operate reliably.

Source: authors' synthesis from [2], [11], [19], [20], [36], [38], [54], [58], [62], [71], [72], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110].

Restated as testable claims, the Vietnamese application yields three propositions that the international literature currently lacks the vocabulary to express:

PV1 (conditional localization). Vietnamese law imposes localization on a triggered rather than a default basis: the obligation crystallises on request and for a defined retention period. The design consequence is a localization-ready architecture — domestic storage capability provisioned and switchable without re-design — which is distinct both from the transfer-restriction model of the GDPR and from full-scope localization regimes.

PV2 (dataset-level role allocation). Because the personal-data regime differentiates four legal capacities, role allocation in a Vietnamese consortium is a matrix over datasets rather than an attribute of the consortium. Two participants

may hold different capacities in respect of the same workflow.

PV3 (coordination rail, not title rail). Because the Law on Electronic Transactions preserves the priority of sector-specific rules, a permissioned blockchain in a Vietnamese port cannot serve as the rail for transferring title in trade documents; it can serve as a rail for coordination, provenance, and status. This is a third position, not reducible to the binary of MLETR-enacted and not-enacted, and distinct from a mere pre-enactment default: the Netherlands has not enacted the Model Law either, yet Vietnam's position is a positive configuration — electronic transactions broadly enabled by the 2023 Law while a sector-specific carve-out is expressly preserved — rather than a legislative silence awaiting reform.

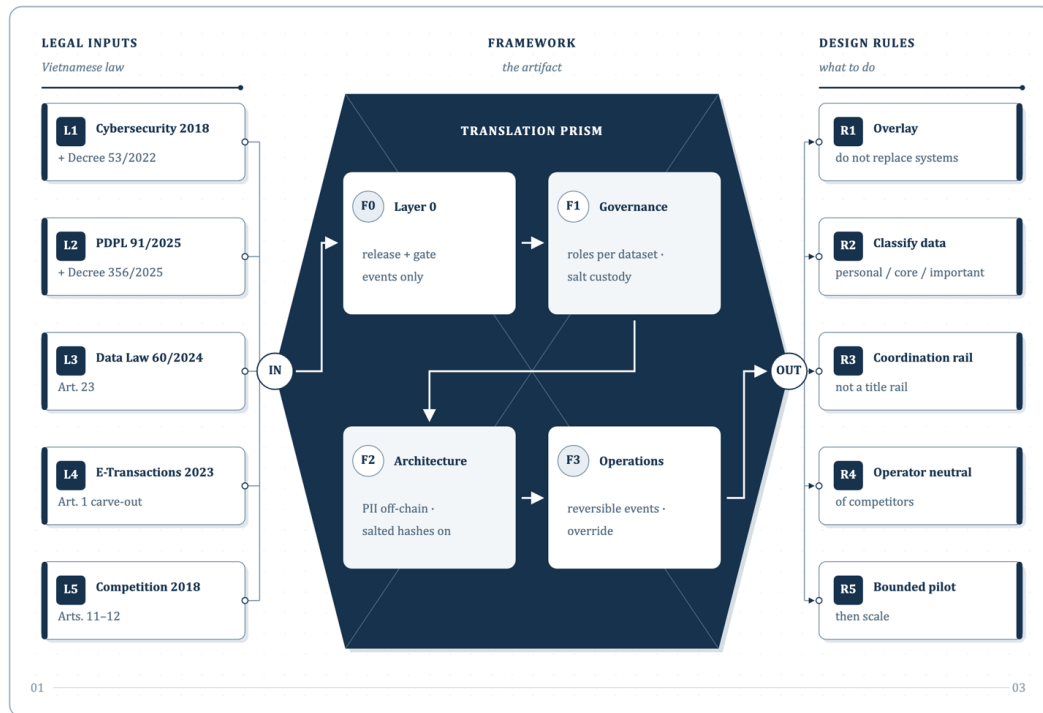


Figure 4. Vietnam-specific legal-technical mapping for permitted blockchain deployment in port operations

Source: authors' synthesis based on Vietnamese legal instruments and current port digital infrastructure [97], [98], [99], [105], [106], [107], [108], [109], [110]. The personal-data input is the Law on Personal Data Protection 91/2025 and Decree 356/2025, superseding Decree 13/2023 [111] from 1 January 2026; the Law on Data 60/2024 and the Law on Competition 2018 are included, the Layer 0 screening outcome is shown, and on-chain commitments are salted hashes.

PV1–PV3 are the Vietnam-specific instances of the general propositions, and are disconfirmable on the same terms as their parents. PV1 and PV2 instantiate P2 on dimensions D1 and D3 respectively: PV1 is disconfirmed if a Vietnamese deployment meets the localization duty without a switchable domestic-storage capability, and PV2 is disconfirmed if a single consortium-wide controller/processor assignment satisfies Decree 356/2025 across all datasets. PV3 instantiates P3 and is disconfirmed if a Vietnamese port lawfully transfers document title on-chain despite the Article 1 carve-out.

The appropriate design response is a bounded permissioned consortium overlay: the governance layer should allocate controller and processor roles explicitly and allocate salt custody; the architecture layer should connect VNACCS/VCIS, the National Single Window, and terminal ePort systems through APIs and a common event schema; and the operational layer should automate only reversible, well-defined events such as release authorization, handover confirmation, and gate status, while keeping legally authoritative documents and exception handling under human oversight. Figure 4 summarizes the Vietnam-specific translation of legal inputs into governance, architectural, and operational controls.

5.3. A Bounded Pilot Scenario at Cat Lai Port

This section specifies the bounded pilot that the framework implies for the Vietnamese context. It is a design specification, not a report of results: no deployment has taken place, and every figure below is an ex-ante target or a parameter to be measured, not an observation.

5.3.1. Scope and the Layer 0 outcome

The pilot scope is deliberately narrow: coordination of the electronic release order and the associated gate events for laden import containers at a single terminal, together with the handover confirmation between terminal and haulier. This coordination is not hypothetical: at Cat Lai, Saigon Newport already issues electronic delivery orders through its ePort service [109], so the pilot's question is not whether release coordination can be digitized — it already is — but whether the authoritative release-and-gate sequence can be placed under neutral custody when the incumbent platform provider is itself a terminal operator competing with other participants. Three considerations set this boundary. First, the S1 test of Layer 0 is applied to named third-party candidates rather than assumed. Three present themselves. (i) The customs authority holds statutory powers over declarations but has no mandate over the commercial release authority exchanged between carrier, terminal, and haulier; it can sit as a read-and-audit node but cannot be the keeper of that private sequence. (ii) The National Single Window is a filing and status-exchange channel for regulatory submissions, not a register of private release authorizations. (iii) A port-authority or industry-association vehicle is legally conceivable but is not at present constituted, funded, or mandated for this function; the maritime port authority holds public-regulatory competence over safety, security, and vessel procedures under the Maritime Code [112] but, like the customs authority, holds no mandate over the commercial release sequence, so it too could sit only as an audit node. On the current institutional facts no available third party is accepted by all participants as the sole keeper of

the release-and-gate sequence, and carriers, terminals, and hauliers each maintain their own conflicting record; S1 is therefore answered negatively. The conditional is stated deliberately: were such a neutral vehicle to be constituted — for instance by the port authority under public mandate — S1 would be answered affirmatively and the framework would return “do not deploy a blockchain” for this workflow. The screen is meant to be capable of excluding the present pilot, not merely of endorsing it. Second, the workflow is composed entirely of reversible events — the condition of P3 — so no transfer of title is implicated; the coordination-rail rather than title-rail posture of PV3 therefore applies and the sector-specific carve-out in Article 1 of the Law on Electronic Transactions is not engaged. Third, the payload can be reduced to non-identifying references, so the personal-data surface is small enough to be managed by salting and off-chain storage.

The S3 test requires an explicit answer, and must be applied against the strongest non-replicated alternative rather than a weak one. That alternative is not a single-participant database — which fails S3 for the same reason S1 fails, since whichever participant hosts it acquires unilateral control over the authoritative sequence — but a mutually notarized, threshold-signed, append-only log administered by a neutral convener, which would deliver multi-party non-repudiation and tamper-evidence without replication. The second strongest-null branch of Section 4.2 — a sector interoperability standard with competing conformant platforms — does not reach this workflow either: a standard harmonizes formats across platforms but supplies no custody of a single authoritative release-and-gate sequence among parties who each maintain conflicting records; the question here is who keeps the sequence, not how it is formatted. The release-and-gate workflow therefore turns S3 on the availability of that convener, and the answer is tightly coupled to S1. If a neutral party existed that all competing participants accepted as administrator of a threshold-signed log, that same party would in most cases be acceptable as the sole keeper contemplated in S1; S1 would then be answered affirmatively and the framework would return “do not deploy.” S3 is answered in the negative here only because, on the current institutional facts, no such neutral administrator is available: a threshold-signed log would have to be administered by one of the competing participants, reintroducing the unilateral-control problem, whereas a replicated permissioned ledger distributes that control across the participant set by construction. This distribution is partial rather than absolute — a permissioned ledger still requires a membership and certificate authority and an agreed ordering service, so the trust otherwise placed in a single keeper is redistributed and constrained rather than eliminated — which is why the assurance margin over a threshold-signed log is narrow and must be earned workflow by workflow rather than assumed. The pilot thus sits close to the screen’s boundary — a boundary Section 6.3 states explicitly — and the answer would flip the moment a mandated neutral vehicle were constituted. Document storage, by contrast, fails S2 — writing is effectively single-sourced by the document issuer — and is therefore excluded from scope: authoritative documents remain in the systems of record, with only

salted hashes and status transitions committed on-chain. Customs declaration processing is also excluded; the pilot overlays the existing customs interface rather than substituting for it, consistently with the platform-neutrality requirement noted in Section 5.2.

The participant and node structure follows from Section 2.6 and from dimension D5. Four participant classes are envisaged: the terminal operator, two or more shipping lines or their agents, licensed hauliers, and a compliance observer node for the customs authority with read and audit rights but no write authority over commercial events. Two participation facts remain to be established rather than assumed. The customs authority’s own participation constraint has not been computed: its integration cost against its supervisory benefit is an open term in Equation (3), so the observer role is an assumption about incentives that pilot design must verify, not a settled fact. And the physical keying of gate events is labor: who records an event, on what device, under what incentive to record promptly and truthfully is a workflow-design question that indicator K8’s independent-confirmation rate monitors but does not solve — the haulier community’s device and digital-skills reality must be surveyed before the event schema is fixed. The operating entity must not be controlled by any participant that competes with another; where, as at Cat Lai, the terminal operator is also the incumbent platform provider, the pilot must either place the operating entity under a separate governance vehicle with participant-independent control or restrict the pilot to workflows in which the terminal operator is not a competitor of the other participants. This is a precondition, not a preference: it is the condition whose absence is most strongly implicated in the TradeLens outcome [7], [8], and it is the point at which the exclusive-versus-sharing trade-off becomes decisive. Wang and colleagues frame precisely this choice — whether a port deploys blockchain capability exclusively or shares it — as a strategic decision governed by the competitive relationship between the parties rather than by the technology, which is why the identity and control of the operating entity must be settled before the data schema [59]. Node replication is bounded to domestic infrastructure, because the ledger — the accumulated record of release-and-gate events — may itself constitute important data under Article 23 of the Law on Data and is in any case subject to local-retention duties. This bound is a design constraint on the consensus topology rather than a free choice: the localization duty and the number of independent validating nodes pull against each other, since confining nodes to one jurisdiction reduces the pool across which write control is distributed, and the tension is recorded as a limitation in Section 7.1.

A caveat specific to Cat Lai must be verified before the governance vehicle is fixed: the incumbent terminal operator is a state-linked enterprise, which may bear on both the competition analysis of dimension D5 and the classification of operational data as important data under the Law on Data. Whether the notion of competitor imported from European law applies to a state-linked operator is a question of Vietnamese law that this conceptual treatment flags rather than resolves.

The charter must also specify the consortium lifecycle, which the design treats as a first-class governance question.

Three events need pre-agreed rules: a participant leaving (its node is decommissioned, but the historical commitments and the salts needed to honor outstanding verification and retention duties are escrowed under the secret-lifecycle rules of Section 4.4.1, not destroyed); a participant being expelled for cause (as above, plus revocation of write authority); and the pilot itself ending. Because release-and-gate records retain evidentiary and regulatory value for years after a pilot concludes, dissolution does not mean deletion: the charter names a successor custodian for the ledger and for the secret-lifecycle obligations, and fixes the retention horizon against the longest applicable duty. A pilot without an exit clause silently assumes perpetuity, which neither the participants nor the retention law supports.

5.3.2. Indicators

Table 5 specifies the indicators the pilot must measure. Each is given a formal definition so that it can be computed identically before and after deployment. The baseline column deliberately contains no values: baselines are to be established from terminal and carrier records during a measurement window preceding go-live, and publishing invented baselines would defeat the purpose of the exercise. Targets are stated as ex-ante design targets, meaning the improvement the design is intended to achieve and against which it should be judged, not a prediction. One indicator (K8) addresses the oracle limit: the ledger secures who asserted what and when, but a gate event is keyed by an operator at the point of work, so on-chain integrity is necessary but does not by itself establish that the physical event occurred; K8 measures the share of events corroborated by an independent, non-manual source.

5.3.3. Ex-ante cost model

A cost-benefit statement for a system that does not yet exist can be honest only as a model with named parameters, not as a table of currency amounts. Let k index the in-scope event types, $Q(k)$ the annual volume of events of type k , $\Delta T(k)$ the time saved per event, and $v(k)$ the value of the time of the party that saves it. Let $C(\text{node})$ denote annual node hosting, operation, and domestic-storage provisioning; $C(\text{int})$ the amortized integration cost across participant systems; $C(\text{gov})$ the annual cost of governance, legal review, impact assessment, and competition-compliance review; and $C(\text{on})$ the aggregate onboarding cost borne by participants. Annual net benefit is then:

$$NB = \sum_k [\Delta T(k) \cdot v(k) \cdot Q(k)] + S(\text{disp}) - [C(\text{node}) + C(\text{int}) + C(\text{gov}) + C(\text{on})] \quad (1)$$

where $S(\text{disp})$ is the annual saving from avoided disputes, computed as the reduction in the K3 dispute rate multiplied by the mean administrative and demurrage cost per dispute. Setting $NB = 0$ and assuming a single dominant event type gives the break-even annual event volume $Q(\text{be})$:

$$Q(\text{be}) = [C(\text{node}) + C(\text{int}) + C(\text{gov}) + C(\text{on}) - S(\text{disp})] / [\Delta T \cdot v] \quad (2)$$

Equation (2) is the operative decision rule and makes the framework's cost logic falsifiable in a specific way. The four cost terms are largely fixed with respect to volume, while the benefit term scales with it; a pilot confined to a workflow whose annual event volume falls below $Q(\text{be})$ cannot be justified on efficiency grounds regardless of how well it satisfies the legal dimensions. Two implications follow. First, $C(\text{gov})$ is not a residual: the framework's own compliance apparatus — impact dossiers, role matrices, competition review, salt custody procedures — enters the denominator of the deployment decision, and a framework that ignored this would understate the cost of its own prescriptions. Second, $C(\text{on})$ determines whether critical mass is reachable, which is why K7 is reported separately rather than folded into an aggregate. Parameter values must be obtained from vendor quotations and participant records before a deployment decision; they are not supplied here, and any figure presented in their absence would be fabricated rather than estimated.

Two refinements are required, because Equation (1) as written is the objective of a single social planner whereas participation in a port-community consortium is decentralized — the mechanism the TradeLens evidence in Section 2.6 identifies. First, aggregate net benefit is necessary but not sufficient. Let N be the set of participants without whom the coordination benefit does not exist and $NB(i)$ the net benefit accruing to participant i after any transfer or subsidy agreed in the consortium charter — transfers being a charter matter rather than a discretion of the operating entity, since side-payments set unilaterally by a dominant participant would entrench control rather than share benefit. For the coordination rationale to hold, N must contain at least two participants that compete on the same relevant market; where it does not, writing is effectively single-sourced and the workflow fails S2 rather than reaching this condition. Deployment is viable only where:

$$NB \geq 0 \quad \text{and} \quad NB(i) \geq 0 \quad \text{for all } i \in N \quad (3)$$

The second condition is the one the aggregate hides: a positive NB is fully compatible with no participant joining, which is precisely how a socially beneficial platform can fail to form. Indicator K7 reports the binding case, the smallest participant class. The other binding case is the largest: for an incumbent platform provider — at Cat Lai, the terminal operator whose ePort service currently mediates release — $NB(i)$ must be computed net of the platform rents the incumbent forgoes when the authoritative sequence moves to neutral custody, including the revenue and the gatekeeping control it currently derives from that position. On that accounting the incumbent is the participant most likely to violate Equation (3) even when aggregate NB is large, which is why the operator-neutrality precondition of Section 5.3.1 is also an economic condition, not only a competition-law one. Second, the cost terms are not strictly constant. $C(\text{gov}) = c_0 + c_d D + c_r R$ rises with the number of datasets D and transfer routes R , since each adds an impact dossier and a role assignment under Table 3, and $C(\text{on}) = \sum(i) C(\text{on},i)$ is a sum over participants. The break-even volume $Q(\text{be})$ is therefore a function of $(|N|, D, R)$ rather than a constant, and the cost claim is disconfirmed if an operating port community system exhibits $\partial C(\text{gov})/\partial D \approx 0$.

Table 5. Pilot indicators, definitions, and ex-ante design targets

Code	Indicator	Definition	Baseline source	Ex-ante design target
K1	Release-order turnaround time	$K1 = (1/N) \sum_i [t(\text{auth}, i) - t(\text{instruct}, i)]$ over the N laden import containers i handled in the period, in minutes	Terminal and carrier timestamps, 4-week pre-go-live window	Reduction against measured baseline; direction of change is the test, magnitude to be agreed with participants before go-live
K2	Duplicate data-entry events	$K2 = \sum(f) [n(f) - 1]$ per declaration, where n(f) is the number of participant systems into which field f is separately keyed	Process observation and system logs, same window	Elimination of duplicate entry for fields carried by the common event schema
K3	Document-dispute rate	$K3 = 1000 \cdot D / C$, where D is disputes raised over release authority or gate timing and C is containers handled	Terminal exception register and carrier claims log, 12 months prior	Reduction against measured baseline
K4	Time to evidence retrieval	$K4 = \text{median over sampled queries of } [t(\text{pack complete}) - t(\text{query received})]$, where a complete pack includes any translation or notarization an administrative use requires	Sample of historical queries, same period	Digital pack retrieved within one working hour without manual reconciliation; translation and legalization, where a proceeding requires them, timed and reported as a separate component
K5	Verifiable provenance coverage	$K5 = E(\text{verifiable}) / E(\text{in scope})$	Nil at baseline by construction	Full coverage of in-scope event types
K6	Exception rate requiring human override	$K6 = E(\text{escalated}) / E(\text{in scope})$, reported separately for the legally unresolvable subset	Terminal exception register	Monitored, not minimized; a rising legally unresolvable share is the disconfirming signal for PV3
K7	Smallest-participant onboarding cost	$K7 = C(\text{one-off}) + C(\text{annual})$ for the smallest participant class, per participant	Vendor quotations and participant reporting	Bounded at a level the smallest class of participant can absorb without subsidy; reported explicitly because critical mass is a design variable
K8	Independent event-confirmation rate	$K8 = E(\text{confirmed}) / E(\text{in scope})$, where confirmation is a second, non-manual source (gate OCR, weighbridge, or terminal operating system) for the same event	Terminal sensor and TOS logs, same window	High coverage for gate events; the residual is the oracle limit — on-chain integrity does not establish physical occurrence

Source: authors' construction. All entries are design specifications; no values are reported because no deployment has taken place. K6 and K7 are included as disconfirming and feasibility indicators respectively.

Proposition P1 of Section 4.6 also becomes measurable in this setting. If the pilot is instrumented to record the cost of accommodating a legal requirement identified before charter settlement against the cost of accommodating one identified afterwards, the ratio provides the first direct test of the asymmetric-retrofit claim.

5.4. Evaluation Strategy and Criteria

Sections 5.1–5.3 demonstrate the artifact: they show that it can be applied and that it yields coherent, jurisdiction-specific design consequences. Demonstration is not evaluation. An artifact assessed only by its designers, against no criterion fixed in advance, has not been evaluated in the design-science sense [90], [91]. This section adds a set of probes that are explicitly *formative*, *artificial*, and *ex-post* in the terms of the FEDS framework of Venable, Pries-Heje, and Baskerville: the artifact is checked against independent real-world cases and modelled data rather than through a live deployment, which remains future work; Section 3 states the evidential tier of such probes and its limits once, and that statement governs everything below [92]. Three complementary methods drawn from the evaluation taxonomy of Prat, Comyn-Wattiau, and Akoka are used — comparison of the artifact's output with real-world outcomes, simulation of its internal logic, and comparison with competing artifacts [93]. To keep the exercise honest rather than self-serving, the success criteria are stated here, before any result is presented, and the results below include one criterion that *failed*: the failure is reported in full

in Section 5.5, and the repair it forced is disclosed in Section 4.2.

Four criteria are fixed in advance. **CE1 (discriminant efficacy)**. The necessity screen must produce different verdicts for different inputs and, in particular, must be capable of returning “do not deploy”; a screen that only ever endorses blockchain is a rationalization, not a decision procedure. **CE2 (external consistency)**. Applied to independent real platforms, the screen's verdicts must agree with those platforms' observed design and survival. **CE3 (economic robustness)**. The break-even decision rule of Equation (2) must keep the correct sign — break-even below realistic event volume — across the full plausible parameter range, and must reveal which parameters govern the result. **CE4 (comparative distinctiveness)**. The framework must address design concerns that the nearest existing frameworks leave implicit. The three methods map onto these criteria: multi-case analysis tests CE1 and CE2 (Section 5.5), cost simulation tests CE3 (Section 5.6), and benchmarking tests CE4 (Section 5.7).

5.5. Multi-Case Analytical Evaluation

The necessity screen makes a claim that independent evidence can contradict: that whether a replicated permissioned ledger is the right instrument turns on operator neutrality and the availability of a trusted neutral keeper, not on the technology's merits. Section 6.3 applies the screen retrospectively to the single case of TradeLens. This section generalizes that check in two deliberately different directions. Table 6 codes

five port- and trade-document platforms whose structures and outcomes are publicly documented; Table 7 then extends the sample *adversarially*, with four platforms selected precisely because they should stress the screen — neutral consortia that deployed replicated ledgers and nonetheless failed. Before any case is coded, the coding rule must be fixed, because a neutrality judgement inferred from a platform's fate would make the exercise circular. Operator neutrality is therefore coded from *ex-ante structural facts only*: the ownership and control of the operating entity, whether any participant that competes with another holds board control or a veto, and who appoints the membership and certificate authority and the ordering service. On that rule TradeLens codes as non-neutral without reference to its outcome — the operating venture was co-owned by Maersk, a carrier competing with the carriers it needed to enroll [7], [8] — and GSBN codes as neutral because no single competitor controls the incorporated non-profit [113].

Two features of Table 6 bear on criteria CE1 and CE2. On CE1, the screen is discriminating rather than permissive: it returns “do not deploy a replicated ledger” in three of the five cases and “deploy” in two, so its endorsement carries information. The two deploy verdicts fall exactly on the neutral-consortium structures — GSBN among competitors, Archipels among non-rivals, whose certification function does not require competitor co-writing and is therefore screened by S1 and S3 alone, and the three negative verdicts fall on the case with a structurally non-neutral operator (TradeLens) and the two cases where a trusted neutral keeper already exists (TradeTrust, Portbase) — and in those last two the surviving real design is indeed not a replicated coordination ledger but a minimal-trust or centralized one. On CE2 as stated — agreement with observed design *and survival* — the five cases of Table 6 are consistent. Table 6 alone, however, contains only one failure, and it is of the confirming kind. A screen tested only on cases it should pass has not been stressed. Table 7 supplies the stress.

Table 7 is a negative result against criterion CE2, and it is reported as one. All four platforms satisfied the structural conditions the screen tests — competing participants, no trusted neutral keeper, genuine multi-party writing — and all four failed anyway. Across the nine cases the screen's verdict agrees with the *design the market adopted or converged on* in nine of nine, which is evidence that S1–S3 capture the instrument choice; but it agrees with *survival* in only five of nine. The variable that separates the survivors from the graveyard is not one the screen tested: realized adoption volume. Contour's reported volumes — of the order of hundreds of transactions per year — sit roughly two orders of magnitude below the break-even volume that the cost model of Section 5.3.3 implies for even a modest deployment, and Section 5.6 shows this quantitatively. The diagnosis is that S1–S3 test whether replication is the right instrument, not whether the consortium is viable; lawfulness and instrument-fit are necessary, and neither is sufficient. That diagnosis is what forced the repair disclosed in Section 4.2: a fourth screening question, S4, supplied by Equations (2)–(3). Two disciplines gov-

ern how the repair may be read against these cases. First, an honest distinction between quantities: what Table 7 records is *realized* volume, known only after the fact, whereas a gate must operate on information available before deployment — and the two can diverge sharply. Applied in forecast form to we.trade at its 2017 design point, S4 would in all likelihood have *passed*: the founding banks' adoption forecasts were optimistic and credible by every contemporary standard. This is precisely why Section 4.2 states S4 in *commitment* form — the founding banks forecast volume but never bound themselves to route it, and a commitment-form gate would have returned exactly the answer the outcome vindicates. Second, the repair's provenance: it was made *after* the evidence that motivated it, so the ex-post consistency of the nine cases with the repaired screen is a hypothesis the repair must survive prospectively, not a confirmation it has already earned.

A domain-transfer caveat must also be argued rather than assumed, because the four failures of Table 7 are trade-finance and insurance platforms — voluntary-usage networks competing against entrenched free rails, with volume dependent on thousands of dispersed decisions — whereas gate and release coordination at a single terminal is a setting in which the channel can be made quasi-mandatory by the operator, as Cat Lai's own ePort delivery-order service illustrates. What transfers across domains is therefore not the surface pattern (“consortia die of low adoption”) but the mechanism: violation of the Equation (3) participation constraint by an essential participant. The mechanism takes different visible forms — dispersed users declining to switch in trade finance; an incumbent declining to surrender gatekeeping rents at a terminal — but the violated inequality is the same, and Table 7's source note now records the mechanism for each case. The wider case record supports reading *mandatability of the channel* as the regime variable: GSBN survives with volume routed by its carrier-shareholders; Egypt's CargoX gateway operates because ACI filing through it is a legal obligation [120]; TradeWaltz, a neutral consortium of competing Japanese trading houses, operates in production [121] — a boundary case for the regime reading, since its volume appears to be routed substantially by its own trading-house shareholders, as at GSBN, though its routing mechanism is not publicly documented in the detail the other cases are — while the fully voluntary-usage consortia died. Two further cases bound the screen's jurisdiction honestly: ShipChain was shut down by securities enforcement [122] — a failure cause outside the participation constraints, which under the stopping rule of Section 4.2 is recorded as a scope limit, not absorbed as a new gate — and the DCSA electronic bill-of-lading programme shows competing carriers choosing a third instrument entirely, interoperability standards without keeper or ledger [95], which S3 now names. The sample still contains no port-coordination case that died of adoption; the transfer of the S4 lesson to the port domain is therefore a flagged assumption, testable by the pilot itself, and recorded as such in Section 7.1.

Table 6. Retrospective application of the Layer 0 necessity screen to five real platforms

Platform	Neutrality condition (what the screen keys on)	Screen verdict	Observed design and status	Consistent?
TradeLens (Maersk–IBM)	Operating entity co-controlled by the carrier Maersk; not neutral toward rival carriers.	Operator-neutrality precondition fails — do not deploy a competitor-controlled ledger.	Competitor-controlled replicated ledger on Hyperledger Fabric; rivals withheld participation; discontinued Q1 2023 for want of commercial viability [7], [8].	Yes
GSBN	Incorporated non-profit co-owned by competing carriers (COSCO, Hapag-Lloyd, OOCL) and terminal operators; no single competitor controls it and no external neutral keeper of the shared record exists.	Replication distributes write control across competitors — deploy a neutral-consortium ledger.	Non-profit consortium permissioned ledger on Hyperledger Fabric; incorporated 2021 and operating since [113].	Yes
TradeTrust (Singapore, IMDA)	A trusted neutral keeper — a government agency — is available for the document-notarization function (S1 satisfied).	S1 answered affirmatively — do not deploy a replicated coordination ledger; a minimal-trust design suffices.	Blockchain used only for document integrity and notarization under an MLETR-aligned standard, not as a replicated coordination ledger; live [2].	Yes
Portbase (Netherlands)	A trusted neutral keeper — a port-authority-owned not-for-profit — is available (S1 satisfied).	S1 answered affirmatively — do not deploy a replicated ledger.	Centralized Port Community System. Portbase did integrate the TradeLens blockchain in 2020 [114]; after TradeLens was discontinued, the surviving design is the centralized PCS [115] — the market converged on the keeper design the screen indicates.	Yes*
Archipels (France)	Public-consortium keeper (Caisse des Dépôts, La Poste, and others), neutral among its users; no single user controls it.	Neutral consortium of non-rivals — deploy a permissioned ledger for the certification function.	Public-consortium permissioned ledger for document certification; live, and cleared EU merger control [23].	Yes

Source: authors' coding from public records under the ex-ante structural rule stated in the text. Cases were selected for documentation quality, not sampled systematically; outcomes were known when the cases were chosen. *Portbase's verdict is coded "Yes" with a qualification: the port community briefly ran a replicated ledger (the TradeLens integration, 2020–2022) before converging on the design the screen indicates. TradeLens and GSBN are best read as a natural pair — same technology, opposite control structure, opposite outcome — rather than as two independent confirmations.

Table 7. Adversarial extension: neutral consortia that deployed replicated ledgers and failed

Platform (sector)	Ex-ante structure	S1–S3 verdict	Outcome	Consistent with survival?
we.trade (trade finance)	Joint venture of competing banks (HSBC, Santander, Société Générale, UBS and others) with IBM; no single competitor in control.	Neutral consortium, no trusted keeper — deploy a consortium ledger.	Deployed on Hyperledger Fabric; filed for insolvency June 2022 after shareholders declined further funding [116].	No — failed despite passing S1–S3
Marco Polo (trade finance)	Network of some thirty banks on a common platform; no participant bank in control.	Neutral consortium — deploy.	Deployed on Corda; entered insolvency February 2023 with unfunded liabilities [117].	No
Contour (trade finance)	Owned by eight competing banks; operator independent of any one of them.	Neutral consortium — deploy.	Deployed on Corda; wound down late 2023 as shareholders withdrew; reported volumes of the order of hundreds of transactions per year [118].	No
B3i (insurance)	Consortium of major insurers and reinsurers; no single-member control.	Neutral consortium — deploy.	Ceased trading July 2022 after a failed funding round [119].	No

Source: authors' coding from public records under the same ex-ante structural rule. These four cases were selected adversarially — because they should stress the screen — and they do. Mechanism of failure, coded per case: in all four, violation of the Equation (3) participation constraint under voluntary adoption — dispersed users and shareholder banks declined to route volume — rather than any structural defect the necessity questions test. All four are trade-finance or insurance platforms; the domain-transfer argument and its limits are stated in the text.

This relocates the Cat Lai pilot honestly. On the structural facts, Cat Lai resembles GSBN's position — competing participants, no accepted neutral keeper — but it *equally* resembles we.trade's position, and what separated those two outcomes was adoption, not structure. The screen's answer for Cat Lai is therefore conditional: S1–S3 are passed on current institutional facts, and S4 is undetermined until binding routing commitments exist for each essential participant class, a reference-class forecast being admissible only as a

bridge (Section 4.2). The framework accordingly withholds the deploy verdict rather than issuing it — which is the behavior a screen “willing to reject its own object” should exhibit at exactly this point. Were a mandated neutral vehicle to be constituted, the pilot would move to the TradeTrust–Portbase branch and the screen would return “do not deploy” at S1; were the commitment round — or its reference-class bridge — to fall short of Q(be), it would return “do not deploy” at S4.

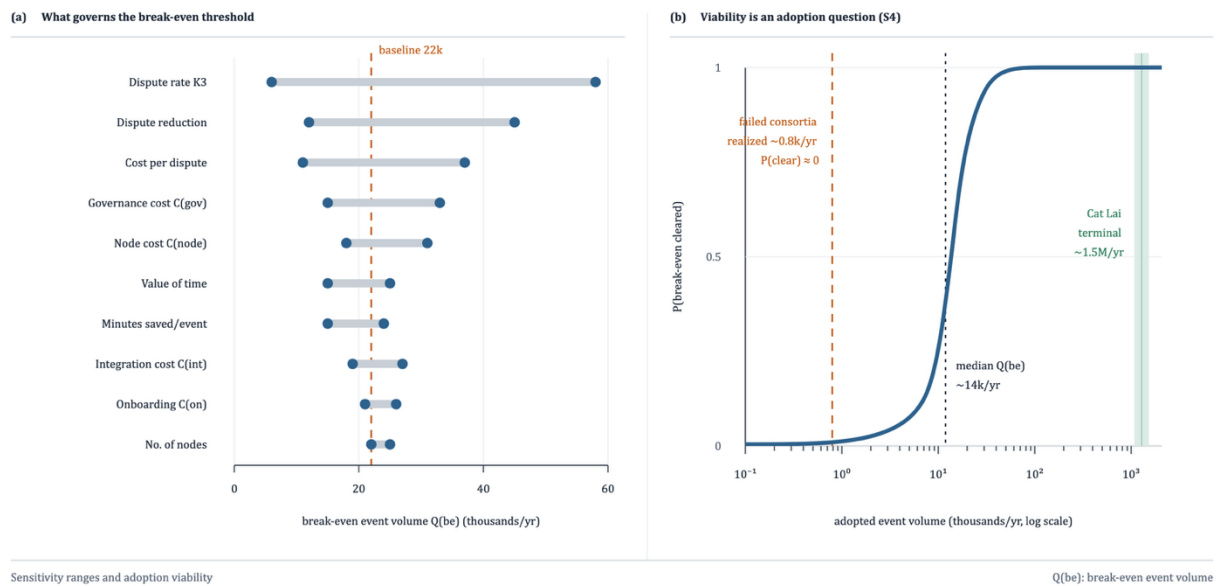


Figure 5. Monte Carlo evaluation of the break-even rule of Equation (2): (a) sensitivity of the break-even event volume to each parameter; (b) probability of clearing break-even as a function of adopted event volume — the S4 question — with the realized scale of the failed consortia of Table 7 and the Cat Lai terminal volume marked

Source: authors' simulation (60,000 draws, fixed seed). Ranges are illustrative and sourced, not measured at Cat Lai; minutes saved per event and value of time are estimates. The simulation evaluates the robustness of the decision rule, not the profitability of an actual deployment.

The limitations of this evaluation must be stated as plainly as its results. All nine cases are retrospective and their outcomes were known when they were chosen; the coding, although fixed by an ex-ante structural rule, was performed by the authors rather than by independent coders; borderline judgements remain — whether the Archipels consortium is fully neutral among its members is arguable; and the S4 repair owes the prospective test committed to in Section 7.2. Multi-case checking of this kind is formative, artificial, ex-post work in the sense of Venable and colleagues; it has raised one genuine negative result and forced one disclosed repair, but it does not substitute for the naturalistic evaluation specified in Section 7.2.

5.6. Cost-Model Sensitivity Evaluation

Criterion CE3 concerns the cost rule, not the cost figures. Because no deployment exists, no parameter can be measured; what can be evaluated is whether the decision rule of Equation (2) is robust, which parameters govern it, and — the question Table 7 forces — what the rule says when adoption, rather than capacity, is treated as the uncertain quantity. Each cost and benefit parameter was assigned a triangular distribution over a sourced range (node hosting, integration, governance, and onboarding costs from vendor and compliance price points; dispute cost from demurrage-and-detention figures; the two benefit-side timing quantities — minutes saved per event and the value of time — flagged as estimates). Adopted volume was then modelled two ways: conditional on full terminal adoption, as a triangular distribution around Cat Lai's laden-import volume; and under an adoption-agnostic prior, log-uniform from 500 events per year — the order of magnitude the failed consortia of Table 7 actually realized — up to full terminal volume. 60,000 Monte Carlo draws were taken under a fixed seed. Figure 5 reports the result.

Four findings follow, and none of them is a currency amount. First, the rule itself is robust in the conditional sense: the break-even volume (median approximately 14,000 events per year, interquartile range 9,000–20,000) amounts to roughly one percent of Cat Lai's laden-import volume (median 0.9%, interquartile range 0.6–1.4%), so *conditional on adoption at terminal scale* net benefit is positive across the sampled parameter space. Second — and this is the finding Table 7 makes decisive — the conditional result is not the decision-relevant one, and the decision-relevant quantity turns out to be a *regime*, not a number. Under the voluntary-adoption prior the probability of *negative* net benefit is 0.41 — but this figure must be read for what it is: a property of the prior, not of Cat Lai. It moves with the prior's lower bound (0.51, 0.41, and 0.29 for lower bounds of 100, 500, and 2,000 events per year respectively), which is exactly the behavior of a statement of ignorance about adoption. Under a mandated-channel regime — the operator designates the channel and volume approaches terminal throughput, as Cat Lai's ePort already does for the electronic delivery order — the probability of negative net benefit is zero to four decimal places. Mandatability, however, is not a free lever but an endogenous variable: at Cat Lai the party able to mandate the channel is either the incumbent — the participant most likely to violate Equation (3) — or a public vehicle whose constitution would flip S1 and return “do not deploy”; the mandated-regime result therefore describes a boundary of the analysis, not a design option available to a screen-passing consortium. The economically decisive variable is therefore *which regime obtains*: mandatability of the channel, together with the binding commitments S4 now requires. At volumes of the order Contour reported for the consortia of Table 7 — hundreds of events per year [118] — the probability of clearing break-even is zero to

four decimal places; the S-curve of panel (b) shows the transition, with its midpoint at the ~14,000-event median. Third, the tornado in panel (a) shows that break-even is governed by the dispute-side parameters — the dispute rate, the fractional dispute reduction, and the cost per dispute — far more than by node, onboarding, or integration cost; the economic case rests on dispute avoidance, which sharpens indicator K3 into the quantity a real pilot must measure first. Fourth, the number of nodes and the onboarding cost are near-irrelevant to the break-even *threshold* — but this must not be read as license to enlarge the consortium freely, because onboarding cost operates on the other side of the S4 question, through each participant’s willingness to route volume at all (Equation (3)).

The evaluation cuts against a naive reading of the framework as well as for it — in both directions. Against the technology-first reading: a workflow can need distributed control and still destroy value if adoption stalls, which is how four structurally sound consortia died. Against this paper’s own first instinct: the conditional result — net benefit positive in every draw — is the number a designer is tempted to report as the finding, yet treating capacity as if it were adoption is precisely the error the graveyard exposes, which is why the adoption-agnostic analysis is reported alongside it. The falsifier of Section 5.3.3 stands and gains a companion: an operating port community system whose governance cost does not rise with the number of datasets would disconfirm the cost structure, and a deployment that clears break-even from a volume forecast that S4 rejected would disconfirm the viability gate. Like the multi-case analysis, this is a formative probe on modelled inputs; it cannot stand in for the instrumented pilot of Section 7.2, whose first task is to replace these ranges with measured values.

5.7. Benchmarking Against Alternative Frameworks

Criterion CE4 asks what the framework adds. It is evaluated by structured comparison with the nearest reference works in *both* relevant families: the do-you-need-a-blockchain decision trees, which are the direct prior art of Layer 0 [87], [88], [89], and the three nearest design frameworks — the governance-driven blockchain reference architecture (BGRA) of Liu and colleagues [84], the stakeholder-aligned design method of van Engelenburg and colleagues for business-and-government information sharing [85], and Kumar’s analysis of GDPR-compliance challenges for blockchain systems [86] — across the design concerns this paper claims as distinctive. Two scope limits on this comparison are structural rather than incidental: the concerns compared are selected by the authors from their own paper, and the scoring is the authors’ own — so the table can show *coverage* of the claimed concerns, never a neutral quality ranking; and, as noted after the table, each comparator is stronger than the present framework on the axis for which it was built, including the one axis a design-science reviewer weighs most — van Engelenburg and colleagues validate their method in use, which this paper has not.

Read fairly, Table 8 shows the framework’s contribution to be integrative scope rather than depth, and the comparison would mislead if the comparators’ strengths went unstated.

The decision trees are simpler, more general, and far more widely used than Layer 0, and they established the necessity question this paper inherits — what they lack is precisely and only the strongest-null test, the institutional examination of the keeper, and the economic and legal tiers added here. The BGRA offers a far richer catalogue of reusable architectural patterns and a formal reference architecture that this framework does not attempt; van Engelenburg and colleagues ground their method in empirical government-industry data-sharing cases and validate it in use, whereas the present evaluation is artificial; Kumar treats specific GDPR mechanisms in more doctrinal detail than the data-governance dimension here. The framework does not replace these works — it inherits their architectural and stakeholder machinery and adds what they leave implicit: a necessity gate that can decline blockchain, provision-level legal responsiveness across jurisdictions including a non-EU emerging one, a competition dimension, and a cost rule that prices the framework’s own compliance apparatus. That combination, rather than any single column, is the distinctive claim.

Taken together, the three episodes give a mixed and therefore credible verdict on the criteria fixed in Section 5.4: the multi-case analysis supports CE1 on nine platforms, supports the design half of CE2 in nine of nine cases, and *fails* the survival half of CE2 in four of nine — the negative result that forced the S4 repair; the simulation supports CE3 for the decision rule while showing that the binding uncertainty is adoption rather than cost; and the benchmark supports CE4 on the authors’ own selected concerns, with the self-scoring caveat stated above. These are formative, artificial, ex-post probes at the weakest tier of the FEDS hierarchy. They leave the framework better tested than a demonstration would — one criterion failed, one repair was forced and disclosed — but they neither require nor supply the naturalistic evaluation that Section 7.2 sets out, and the two should not be conflated.

6. Discussion

6.1. Theoretical Implications

The framework’s theoretical contribution should be stated at the level the evidence supports. The layered form is inherited from the law-and-architecture tradition and the claim to novelty does not rest on it. What the analysis adds is that legal variation, when read at the level of individual provisions rather than of regimes, is a *generative* input to design rather than a constraint on it: the same five dimensions applied to three legal environments produce three materially different design postures, and the differences are not reducible to strictness. Singapore is more enabling on evidentiary validity but no less demanding on accountability; the European Union is more demanding on data governance and, since the lapse of the consortia block exemption, on competitive conduct; Vietnam is enabling on electronic transactions while preserving sector-specific priority, which produces a design posture that neither of the other two implies.

Table 8. Coverage of distinctive design concerns across the framework and its nearest alternatives

Design concern	Decision trees (Wüst–Gervais; NIST; Pedersen)	BGRA (Liu et al.)	van Engelenburg et al.	Kumar (GDPR)	This framework
Necessity gate that can reject blockchain (Layer 0)	Yes — the family’s defining feature; null alternative is a conventional database	No — presupposes a blockchain is to be built	Partial — assesses stakeholder fit but has no reject gate	No	Yes — necessity against the strongest null (S3), institutional S1, economic S4
Provision-level legal responsiveness across jurisdictions	No	No — governance patterns, jurisdiction-agnostic	Partial — requirements from stakeholders, not legal provisions	Single regime (GDPR)	Yes — five dimensions coded across three legal orders
Competition / antitrust dimension	No	No	No	No	Yes — Article 101 TFEU and the Law on Competition (D5)
Operator neutrality as an architectural precondition	Partial — asks whether a TTP “can be used,” in the abstract	Implicit in decentralization patterns	Partial — stakeholder alignment	No	Yes — examined against named candidate keepers with mandates
Cost / viability decision rule	No	No	No	No	Yes — Equations (1)–(3); S4 in commitment form
Emerging (non-EU) jurisdiction application	No	No — generic	No — EU e-government	No — EU / GDPR	Yes — article-level Vietnamese instruments

Source: authors’ analysis. Coverage is judged for the distinctive concerns of this paper; it is not a measure of overall quality (see text).

The second implication concerns the boundary of the framework’s own explanatory ambit. Adding a competitive-conduct dimension and a necessity screen makes explicit that lawfulness is only one of the constraints binding on a port-community consortium; the TradeLens evidence, tested across nine platforms in Section 5.5 — including four neutral consortia that satisfied every structural condition and failed for want of adoption — indicates that neutrality of the operating entity and reachable adoption volume bind earlier, and the second of these is now screened explicitly at S4. A legal-responsive framework is therefore best understood as necessary infrastructure for a viability argument rather than as a viability argument in itself, and Section 4.6 states the boundary conditions under which it applies.

6.2. Practical Implications

For practitioners, the framework yields four operative rules. First, run the Layer 0 screen and be willing to accept its negative answer; the cost asymmetry identified in P1 applies to the technology choice itself, not only to compliance features. Second, treat salt and key custody as a governance appointment with named holders and a documented destruction procedure, because in a salted-hash architecture the erasure obligation is discharged there and nowhere else. Third, settle operator neutrality and the smallest participant’s onboarding cost before settling the data schema, since both are effectively frozen with the charter. Fourth, automate only reversible events until the evidentiary status of consortium-issued documents in administrative proceedings has been tested in practice.

For policymakers in emerging jurisdictions, the single most actionable implication is institutional rather than technological, and it deserves to be stated first: constituting a mandated neutral convener for port-community coordination — a port-authority or public-mandate vehicle accepted by all competing participants — would simultaneously close the

S1 window (making a blockchain unnecessary) and deliver most of the coordination benefit this paper analyzes, at a fraction of the cost. The framework’s highest-value output for Vietnam is thus a specification of the institution worth building, not the technology. Beyond this, the analysis suggests a sequencing point: enacting MLETR-based legislation is often presented as the decisive step for digital trade, but the Vietnamese case shows that the binding constraint may lie elsewhere — with electronic transactions already broadly enabled, the marginal gain from further general enabling legislation is smaller than the gain from clarifying the admissibility of consortium-issued records in administrative and customs proceedings, and from providing a competition-law safe harbor or guidance for neutral port-community data-sharing arrangements.

6.3. Why Legal Compliance is Necessary but Not Sufficient

It is worth stating plainly what the failure evidence implies for a paper of this kind. TradeLens was not stopped by a regulator. It was stopped because competitors would not join a platform controlled by one of their number and because the resulting participation never reached commercial viability [7], [8], [9]. A framework that produced a fully compliant design for such a platform would have produced a compliant failure. The response adopted here is not to abandon the legal-design program but to bound it: the framework specifies what lawfulness requires, states in Section 4.6 the conditions outside its scope that must independently hold, and incorporates the two that are architecturally expressible — operator neutrality and bounded onboarding cost — as design constraints rather than as contextual observations.

This leaves a narrow boundary condition, which the framework states rather than conceals — and it should be acknowledged that the boundary is, at bottom, a single institutional

variable viewed from two sides: S1 and S3 both turn on whether a neutral party trusted by all competing participants exists, so the screen's necessity questions collapse into one institutional fact plus the multi-party-writing test of S2. A permissioned blockchain is indicated only where a neutral convener is acceptable enough to the participants to coordinate the consortium, yet not trusted enough — by those same competing participants — to keep a single threshold-signed log even under independent attestation; where a fully trusted neutral keeper can be constituted, the screen is satisfied at S1 and returns “do not deploy”; where no convener is acceptable even to coordinate, the consortium does not form at all. The window in which replication is the correct answer is thus real but bounded on three sides — bounded above by institutional maturity (a trusted keeper closes it), bounded below by coordination failure (no consortium forms), and bounded economically by adoption (S4 withholds deployment where committed volume cannot clear break-even, the side on which the four consortia of Table 7 perished). The claim that follows must be stated in its falsifiable form rather than as a slogan: the window requires the *conjunction* of four conditions — no trusted keeper constitutable, genuine multi-party writing, insufficiency of both a threshold-signed log and an interoperability standard, and committed volume above break-even — each individually uncommon; how large a share of workflows at any given port falls outside the conjunction is an empirical question, and the pilot's first phase should include the workflow census that answers it. A census finding that a majority of workflows at a surveyed port satisfy all four conditions would disconfirm the rarity claim. That the window is bounded in this structural sense is not a defect of the framework; it is the framework's central structural finding, and it is the respect in which the framework tightens rather than repeats the 2018 decision-tree consensus. We take a framework whose screen can return a negative verdict against a live pilot to be more useful than one built only to endorse deployment: the contribution is a decision procedure willing to reject its own object, and the Cat Lai analysis is offered as much as a demonstration of that willingness as an endorsement of any particular deployment. Applied retrospectively to the very platform that motivates this paper, the screen yields a negative result that the historical record supports: TradeLens fails S1, because no keeper neutral to its competitors was available, so the framework would have counselled against a competitor-controlled ledger before any compliance work began. That the screen returns “do not deploy” on the best-documented failure in the field is a first analytical check that it discriminates rather than rationalizes; Section 5.5 generalizes that check to nine real platforms, and the naturalistic evaluation specified in Section 7.2 remains the necessary next step.

7. Conclusion

This paper has developed a legal-responsive framework, comprising a necessity-and-viability screen (S1–S4) and four coupled design layers, for permissioned blockchain deployment in port communities, grounded in design science research, functional comparative law, and blockchain governance theory. The framework treats legal compliance as an upstream

design variable rather than a late-stage overlay, makes explicit the vertical dependencies among the Legal, Governance, Architectural, and Operational layers, and embeds a materiality-based adaptation mechanism for responding to regulatory change over time. The comparative application across Singapore, the Netherlands and the European Union, and Vietnam demonstrates that the same analytical instrument produces different but structured design consequences across legal environments — reflecting differences in data protection regimes, electronic trade law maturity, cybersecurity obligations, competition-law exposure, and institutional coordination models.

The principal theoretical contribution is narrow and correspondingly well supported: the premise that legal protection must be inscribed in architecture is inherited from Lessig and Hildebrandt and the layered form from blockchain-governance scholarship, and what is added is the treatment of provision-level legal variation as a generative design input, a screening gate that permits the framework to reject blockchain deployment, and an article-level reading of the Vietnamese instruments that yields three propositions — conditional localization, dataset-level role allocation, and coordination-rail rather than title-rail deployment — which the existing comparative literature cannot express. The comparative application further shows that frameworks developed primarily for mature port ecosystems require substantive adaptation when applied to emerging contexts.

The three research questions can now be answered directly. On RQ1, jurisdictional legal differences influence architecture and operations through the five dimensions of Table 2, which the comparative application shows to generate materially different — not merely stricter — design postures. On RQ2, the legal-technical trade-offs are mitigated by the mappings of Table 3, by the salted-hash and secret-lifecycle discipline of Section 4.4.1, and by confining automation to reversible events. On RQ3, a permissioned blockchain is the appropriate instrument only where the Layer 0 screen is passed; for the Cat Lai workflow, S1–S3 are passed on the current institutional facts while S4 — the viability question the multi-case evaluation forced into the screen — remains undetermined until binding routing commitments exist, so the framework's answer is conditional rather than an endorsement, and a change in the institutional facts or a failing commitment round would each withdraw it. Two implications deserve emphasis beyond the framework itself: for emerging jurisdictions, the binding constraint on digital trade may be the admissibility of consortium-issued records and a competition-law safe harbor rather than the enactment of further enabling legislation; and, methodologically, because the governance cost $C(\text{gov})$ enters the denominator of the deployment decision, the framework prices its own prescriptions rather than treating compliance as free.

Amid the conditionals that honesty requires, what this paper asserts *unconditionally* should be listed plainly: (i) the article-level reading of Vietnam's 2018–2025 instruments and the three propositions it yields — conditional localization, dataset-level role allocation, coordination-rail rather than title-rail — stand on the public texts of the instruments

and on nothing else in this paper; (ii) the necessity question is inherited from the 2018 decision-tree literature, and Layer 0's tightening of it — strongest-null S3, institutionally examined S1, commitment-form economic S4 — is a specific, named extension of that prior art; (iii) the deploy window is bounded on three sides by the stated institutional and economic conditions, a structural claim independent of any census result; and (iv) competitive conduct is operationalized as a design dimension, which no compared framework or decision tree provides. Everything else in the paper is conditional, and is labeled as such where it appears.

7.1. Limitations

Several limitations bound the scope and validity of the findings. First, the framework is conceptual and has not been validated naturalistically through deployment or observational data from operating port community systems. It has, however, been subjected to formative artificial ex-post probes — multi-case analysis against nine independent platforms, Monte Carlo simulation of its cost rule, and benchmarking against competing frameworks, each scored on criteria fixed in advance (Sections 5.4–5.7). These probes establish internal coherence, external consistency of the necessity questions with adopted designs, and comparative distinctiveness; they also produced one negative result — the screen as originally constructed did not predict survival, four neutral consortia having failed for want of adoption — which forced the S4 repair disclosed in Section 4.2. Because S4 was added after the evidence that motivated it, its ex-post consistency is a hypothesis awaiting a prospective test, not a confirmation; and none of this establishes efficacy in a live socio-technical setting. Naturalistic evaluation therefore remains the outstanding validation step. Second, the legal analysis reflects instruments and authoritative guidance in force as of 15 July 2026; blockchain-relevant regulation is evolving rapidly in all three jurisdictions, and the framework's own materiality workflow did not anticipate the replacement of Decree 13/2023 by the Law on Personal Data Protection 91/2025, although that law was enacted through a public legislative process more than a year before this manuscript's cut-off. We report this as the framework's first negative test result rather than conceal it: it shows that monitoring instruments in force is insufficient and that horizon-scanning of published drafts and bills is required — a step now added to the monitoring stage of Figure 3 — and it is a further reason to state the legal cut-off date explicitly in any application of the framework. Third, the comparative application relies on publicly available legal and institutional sources; primary data from port operators, customs agencies, or consortium participants was not collected, and practitioner perspectives on feasibility and implementation constraints are therefore absent. Fourth, the framework addresses permissioned blockchain specifically and does not extend to public or hybrid chain architectures. Fifth, no parameter values measured at Cat Lai are supplied for the cost model of Section 5.3.3; the Monte Carlo of Section 5.6 exercises Equation (2) on illustrative sourced ranges, not site measurements. Sixth, the competitive-conduct dimension is developed at the level of the prohibitions and guidance iden-

tified; it is not a full competition-law analysis, and no formal assessment under Article 101 TFEU or the Law on Competition is offered. Seventh, the requirement to localize ledger data constrains the consensus topology: confining validating nodes to domestic infrastructure to satisfy the Law on Data reduces the pool across which write authority is distributed, so data sovereignty and Byzantine-fault resilience trade off against each other in a way this conceptual treatment identifies but does not quantify. Eighth, the salted-hash architecture concentrates erasure and re-identification power in salt custody, which is therefore a single point of privacy failure; the mitigation is procedural — threshold secret-sharing among independent holders and witnessed destruction — and the residual re-identification risk is a hard limitation rather than a solved problem. Ninth, the operator-neutrality precondition presumes a market of competing private operators of the kind European competition law contemplates; where the incumbent operator is a state-linked enterprise, as at Cat Lai, whether the imported notion of “competitor” applies is a question of Vietnamese law and industrial organization that this framework flags but cannot resolve, so its applicability to state-dominated port sectors is a scope condition, not an assumption that may be silently carried over — and the state-directed scenario compounds it: a state that can both constitute the keeper (flipping S1) and mandate adoption (satisfying S4 by fiat) collapses the voluntary-market logic on which the screen's discriminations rest, a branch this paper flags but does not analyze. Tenth, the legal analysis throughout is of law on the books; enforcement practice — how consistently the data-protection, cybersecurity, and competition regimes are applied to port-sector incumbents in practice — is not observed, and a compliance-heavy design posture is justified only to the extent that enforcement is real, which is itself an empirical premise the pilot should record. Eleventh, the multi-case sample contains no port-coordination platform that failed for want of adoption; the transfer of the S4 lesson from voluntary-usage trade-finance networks to the port domain rests on the mechanism argument of Section 5.5 and is a flagged assumption, testable by the pilot itself.

7.2. Future Research Directions

Five research directions follow directly from these limitations, and the first is now specified in enough detail to be executed.

1. Naturalistic evaluation of the artifact, with a commitment that prevents indefinite deferral. The formative probes of Sections 5.4–5.7 should be complemented by naturalistic evaluation: a two-round Delphi or expert-panel assessment involving carrier and terminal legal counsel, customs officials, trade-finance bankers, and competition practitioners, scoring the framework against criteria fixed before the assessment begins, followed by the instrumented pilot below. So that this step is not deferred indefinitely — the standing risk of any conceptual artifact whose only decisive test requires a deployment — the S4 gate is bound to a concrete default: the first act of pilot design must be to seek binding routing commitments from each essential participant class, and if commitments satisfying S4 cannot be obtained during pilot design — with a reference-class forecast in Flyvbjerg's

sense [96] admissible only as a bridge, never as a substitute — the framework's own verdict for Cat Lai becomes “do not deploy,” recorded as such. An incumbent's refusal to commit is itself a datum: it is observable evidence on the Equation (3) constraint, not a gap in the record. This is the step that would move the framework from artificial to naturalistic evaluation in the sense of Peffers and of Venable [91], [92].

2. Instrumented pilot studies. Pilot studies should test the framework with observed workflow data from port community systems, customs interfaces, and carrier platforms, using the indicators specified in Table 5 and reporting the retrofit-cost ratio that tests Proposition P1.

3. Standardized contractual instruments. Future work should develop standardized clauses for smart-contract fallback, governing law, evidence retention, and liability allocation in cross-border port operations, together with model salt-custody and competition-compliance provisions, translating the governance layer into reusable legal instruments.

4. Quantitative evaluation models. Quantitative models are needed to compare compliance costs, interoperability gains, and security trade-offs across alternative node and data-storage designs, providing the parameter estimates that Equations (1) and (2) require.

5. Vietnam-specific implementation studies. Implementation studies should examine how the Law on Electronic Transactions 2023, the Law on Personal Data Protection 91/2025 and Decree 356/2025, the Law on Data 60/2024, and cybersecurity enforcement practice interact in real port operations — particularly regarding data localization requirements, consent management workflows, the treatment of port-community data sharing under the Law on Competition, and the admissibility of blockchain-based port documents in administrative and legal proceedings.

Author contributions

Dang Thuy Long Chau: Conceptualization; Methodology; Comparative legal design and case selection (Singapore – Netherlands/EU – Vietnam); Instrument coding and multi-case platform coding (ex-ante rule, with N. P. Ngan); Formal analysis (framework, screen S1–S4, and cost model, Equations (1)–(3)); Validation; Writing – original draft; Writing – review and editing; Supervision; Funding acquisition; Project administration; Response to peer review. Pham Thai Hoang: Overall consistency checking; Writing – review and editing. Nguyen Phuong Ngan: Legal-source compilation; Comparative synthesis; Instrument coding and multi-case platform coding (with D. T. L. Chau); Investigation; Visualization (tables); Writing – original draft. Nguyen Cao Thuc: Investigation; Verification of sources and case records; Resources. Le Thanh Tung: Software (simulation code); Formal analysis (Monte Carlo evaluation of the cost rule, Section 5.6, and adoption-regime analysis); Data curation (platform and cost-parameter evidence base, Tables 6–7); Visualization (Figures 1–5); Writing – review and editing. Le Hoang Dung: Investigation (industry practice at the import–export interface); Verification; Resources; Overall checking.

Declaration of competing interest

The authors declare no conflict of interest. The authors confirm that this manuscript is original, has not been published elsewhere, and is not under consideration by another journal. Generative artificial-intelligence tools were used to assist in language editing and in checking the completeness of the reference list; all legal interpreta-

tion, analysis, and conclusions are the authors' own, and all sources were verified against their primary texts.

Data availability

All legal instruments and institutional documents analysed in this study are publicly available; the full instrument-by-dimension coding matrix is provided in Appendix A. No primary or personal data was collected.

Acknowledgements

The authors thank the reviewers and the editorial board of the Journal of Transportation Science and Technology for comments that substantially improved this manuscript, particularly on the currency of the legal analysis, the treatment of competitive conduct, and the specification of the pilot scenario.

Appendix A. Instrument-by-Dimension Coding Matrix

Table A1 reports the corpus of legal materials coded in Phase 1 and the provisions coded against each analytical dimension of Table 2. Entries give the operative provisions where the instrument speaks to the dimension; “silent” records that the instrument does not address the dimension, and is reported rather than inferred. This appendix makes the coding described in the methodology checkable provision by provision, rather than leaving it as a described but unexhibited protocol.

References

- [1] D. K. Boison and A. Antwi-Boampong, “Blockchain Ready Port Supply Chain Using Distributed Ledger,” *Nordic and Baltic Journal of Information and Communications Technologies*, Jan. 2020, doi: 10.13052/nbjict1902-097x.2020.001.
- [2] Infocomm Media Development Authority of Singapore, “Trade-Trust: Legality Guide.” [Online]. Available: <https://www.tradetrust.io/about/legality-guide/>.
- [3] Port of Rotterdam Authority, “PortXchange: standardised data exchange for port call optimisation.” [Online]. Available: <https://www.portofrotterdam.com/en/services/online-tools/portxchange>.
- [4] C. Clott, B. C. Hartman, and B. Beidler, “Sustainable blockchain technology in the maritime shipping industry,” in *Elsevier eBooks*, Elsevier BV, 2020, p. 207, doi: 10.1016/b978-0-12-818421-9.00011-2.
- [5] N. G. Kilbride, “Distributed Ledgers, Cryptography, and Smart Contracts,” in *Cambridge University Press eBooks*, Cambridge University Press, 2021, p. 239, doi: 10.1017/9781316529683.019.
- [6] L. Schädler, M. Lustenberger, and F. Spychiger, “Analyzing decision-making in blockchain governance,” *Frontiers in Blockchain*, vol. 6, Aug. 2023, doi: 10.3389/fbloc.2023.1256651.
- [7] A.P. Moller – Maersk, “A.P. Moller – Maersk and IBM to discontinue TradeLens, a blockchain-enabled global trade platform,” Press release, Nov. 29, 2022.
- [8] I. Najati, “Exploring the failure factors of blockchain adopting projects: A case study of TradeLens through the lens of commons theory,” *Frontiers in Blockchain*, vol. 8, art. no. 1503595, 2025, doi: 10.3389/fbloc.2025.1503595.
- [9] Y. Zhan, A. C. L. Yeung, K. H. Tan, Y. Xiong, X. Xing, and F. Ye, “Success and failure of blockchain technology providers: Founders' power, beyond-blockchain exploration and centralized decision-making,” *Journal of Operations Management*, vol. 71, no. 7, pp. 893–916, 2025, doi: 10.1002/joom.1364.

Table A1. Legal instruments coded, by analytical dimension

Instrument	D1 Data governance	D2 Contractual / evidentiary	D3 Accountability / liability	D4 Operational security	D5 Competitive conduct
GDPR (EU) 2016/679	Arts. 5, 6, 17, 25, 44–49	silent	Arts. 24, 26, 28, 82	Art. 32	silent
EDPB Guidelines 02/2025 (blockchain)	Hashing, salting, off-chain storage, erasure	silent	Controller allocation in DLT	Security of processing	silent
eIDAS Regulation (EU) 910/2014	Data processing by trust-service providers (Art. 5)	Electronic signatures, seals, timestamps	Trust-service liability	Trust-service security duties	silent
Art. 101 TFEU and Horizontal Guidelines (2023)	silent	silent	silent	silent	Information exchange between competitors
Consortia Block Exemption Reg. 906/2009	silent	silent	silent	silent	Expired 25 Apr. 2024; no safe harbor
PDPA (Singapore)	Purpose limitation, accountability, transfer limitation	silent	Accountability obligation	Protection obligation	silent
Electronic Transactions Act (Singapore, as amended 2021)	silent	Electronic transferable records; MLETR alignment	silent	silent	silent
UNCITRAL MLETR (2017)	silent	Functional equivalence of transferable records	silent	Integrity and reliability requirements	silent
PIPL (China)	Cross-border transfer, localization	silent	Processor obligations	Security assessment	silent
Law on Cybersecurity 2018 (Vietnam)	Art. 26 user-data duties	silent	Cooperation duties	Art. 10 important systems; Art. 26	silent
Decree 53/2022/ND-CP (Vietnam)	Data categories; local storage on request	silent	silent	Log retention; lawful access	silent
Law on Personal Data Protection 91/2025/QH15	Roles; purpose limitation; subject rights; transfer	Consent records as evidence of lawful basis	Controller / processor / third-party duties	Protection measures	silent
Decree 356/2025/ND-CP (Vietnam)	Impact assessment; outbound-transfer dossier	silent	Data-protection personnel duties	Procedural safeguards	silent
Law on Data 60/2024/QH15 (Vietnam)	Art. 23 transfer of core and important data	silent	National integrated database duties	Data-security duties	silent
Law on Electronic Transactions 2023 (Vietnam)	silent	Arts. 8–11 data messages; Arts. 22–23 signatures; Art. 1 carve-out	silent	Integrity and accessibility conditions	silent
Law on Competition 23/2018/QH14 (Vietnam)	silent	silent	silent	silent	Arts. 11–12 prohibited agreements
Decree 85/2019/ND-CP (Vietnam, NSW)	Data exchange via National Single Window	Electronic administrative dossiers	Agency responsibilities	silent	silent

Source: authors' coding of the primary texts [2], [11], [20], [21], [24], [38], [54], [58], [97], [98], [99], [100], [102], [103], [104], [105], [106], [107], [108]. The codebook, with a decision rule for each sub-code, is provided as supplementary material.

- [10] F. Munari, "Blockchain and smart contracts in shipping and transport," in *New Technologies, Artificial Intelligence and Shipping Law in the 21st Century*, B. Soyer and A. Tettenborn, Eds. Abingdon, U.K.: Routledge, 2019, doi: [10.4324/9780429029172-1](https://doi.org/10.4324/9780429029172-1).
- [11] European Commission, "Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements," *Official Journal of the European Union*, C 259, pp. 1–125, July 21, 2023.
- [12] K. Lockett-Yeung, "Regulation by blockchain: the emerging battle for supremacy between the code of law and code as law," *Modern Law Review*, Jun. 2018.
- [13] E. Esener, "Adaptive Governance for Blockchain Networks," *SSRN Electronic Journal*, Jan. 2023, doi: [10.2139/ssrn.4500961](https://doi.org/10.2139/ssrn.4500961).
- [14] A. Zhuk, "Beyond the blockchain hype: addressing legal and regulatory challenges," *SN Social Sciences*, vol. 5, no. 2, Jan. 2025, doi: [10.1007/s43545-024-01044-y](https://doi.org/10.1007/s43545-024-01044-y).
- [15] S. S. M. Abdul, "Navigating Blockchain's Twin Challenges: Scalability and Regulatory Compliance," *Blockchains*, vol. 2, no. 3, p. 265, Jul. 2024, doi: [10.3390/blockchains2030013](https://doi.org/10.3390/blockchains2030013).
- [16] M. Godyn, M. Kędziora, Y. Ren, Y. Liu, and H. Song, "Analysis of solutions for a blockchain compliance with GDPR," *Scientific Reports*, vol. 12, no. 1, Sep. 2022, doi: [10.1038/s41598-022-19341-y](https://doi.org/10.1038/s41598-022-19341-y).
- [17] S. Castell, "Slaying the Crypto Dragons: Towards a Crypto-Sure Trust Model for Crypto-economics," in *Smart Innovation, Systems and Technologies*, Springer Nature, 2021, p. 49, doi: [10.1007/978-981-33-6470-7_4](https://doi.org/10.1007/978-981-33-6470-7_4).

- [18] S. Han and S. Park, "A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review," *IEEE Access*, vol. 10, p. 103888, Jan. 2022, doi: [10.1109/access.2022.3210110](https://doi.org/10.1109/access.2022.3210110).
- [19] A. B. Haque, A. K. M. N. Islam, S. Hyrynsalmi, B. Naqvi, and K. Smolander, "GDPR Compliant Blockchains — A Systematic Literature Review," *IEEE Access*, vol. 9, p. 50593, Jan. 2021, doi: [10.1109/access.2021.3069877](https://doi.org/10.1109/access.2021.3069877).
- [20] European Data Protection Board, *Guidelines 02/2025 on Processing of Personal Data through Blockchain Technologies*, Version 2.0, adopted July 7, 2026. [Online]. Available: https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202502_blockchain_v2_en.pdf.
- [21] Commission Nationale de l'Informatique et des Libertés, *Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*. Paris, France, Oct. 2018.
- [22] E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain Mutability: Challenges and Proposed Solutions," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1972–1986, 2021, doi: [10.1109/tetc.2019.2949510](https://doi.org/10.1109/tetc.2019.2949510).
- [23] A. Babinet and D. Dubois, "Archipels' Case: EU's First Merger Control Analysis of a Private Blockchain Consortium," *Journal of European Competition Law & Practice*, vol. 12, no. 8, pp. 630–632, Oct. 2021, doi: [10.1093/jecclap/lpab032](https://doi.org/10.1093/jecclap/lpab032).
- [24] Z. Tan and C. Zhang, "China's PIPL and DSL: Is China following the EU's approach to data protection?," *Journal of Data Protection & Privacy*, vol. 5, no. 1, p. 7, Dec. 2021, doi: [10.69554/natu8989](https://doi.org/10.69554/natu8989).
- [25] M. Karpinski, A. Kuznetsov, and R. Oliynykov, "Security, Privacy, Confidentiality, and Trust in the Blockchain: From Theory to Applications," *Electronics*, vol. 14, no. 3, p. 581, Feb. 2025, doi: [10.3390/electronics14030581](https://doi.org/10.3390/electronics14030581).
- [26] S. Bansod and L. Ragha, "Challenges in making blockchain privacy compliant for the digital world: some measures," *Sādhanā*, vol. 47, no. 3, Aug. 2022, doi: [10.1007/s12046-022-01931-1](https://doi.org/10.1007/s12046-022-01931-1).
- [27] P. De Filippi, M. Mannan, and W. Reijers, "The alegality of blockchain technology," *Policy and Society*, vol. 41, no. 3, p. 358, Feb. 2022, doi: [10.1093/polsoc/puac006](https://doi.org/10.1093/polsoc/puac006).
- [28] F. Molina, G. Betarte, and C. M. Luna, "A Blockchain based and GDPR-compliant design of a system for digital education certificates," *arXiv*, Jan. 2020, doi: [10.48550/arxiv.2010.12980](https://doi.org/10.48550/arxiv.2010.12980).
- [29] R. D. Garcia et al., "A Survey of Blockchain-Based Privacy Applications: An Analysis of Consent Management and Self-Sovereign Identity Approaches," *arXiv*, Nov. 2024, doi: [10.48550/arxiv.2411.16404](https://doi.org/10.48550/arxiv.2411.16404).
- [30] H. Eren, O. Karaduman, and M. T. Gençoglu, "Security Challenges and Performance Trade-Offs in On-Chain and Off-Chain Blockchain Storage: A Comprehensive Review," *Applied Sciences*, vol. 15, no. 6, p. 3225, Mar. 2025, doi: [10.3390/app15063225](https://doi.org/10.3390/app15063225).
- [31] UK Jurisdiction Taskforce, LawTech Delivery Panel, *Legal Statement on Cryptoassets and Smart Contracts*. London, U.K., Nov. 2019.
- [32] Y. Makarova and A. Maughan, "Legal Statement on Cryptoassets and Smart Contracts: A Step in the Right Direction," *The Computer & Internet Lawyer*, vol. 37, no. 5, pp. 17–18, May 2020.
- [33] J. Madir, "Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks?," *SSRN Electronic Journal*, Jan. 2018, doi: [10.2139/ssrn.3301463](https://doi.org/10.2139/ssrn.3301463).
- [34] D. Drummer and D. Neumann, "Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts," *Journal of Information Technology*, vol. 35, no. 4, p. 337, Aug. 2020, doi: [10.1177/0268396220924669](https://doi.org/10.1177/0268396220924669).
- [35] S. Mitra, "OConsent — Open Consent Protocol for Privacy and Consent Management with Blockchain," *arXiv*, Jan. 2022, doi: [10.48550/arXiv.2201.01326](https://doi.org/10.48550/arXiv.2201.01326).
- [36] N.-P. Abdellatif, "An Ethereum bill of lading under the UNCITRAL MLETR," *Maastricht Journal of European and Comparative Law*, vol. 27, no. 2, p. 250, Apr. 2020, doi: [10.1177/1023263x20904316](https://doi.org/10.1177/1023263x20904316).
- [37] M. Goldby, *Electronic Documents in Maritime Trade: Law and Practice*, 2nd ed. Oxford, U.K.: Oxford University Press, 2019, doi: [10.1093/law/9780198811978.001.0001](https://doi.org/10.1093/law/9780198811978.001.0001).
- [38] United Nations Commission on International Trade Law, "Status: UNCITRAL Model Law on Electronic Transferable Records (2017)." [Online]. Available: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records/status.
- [39] A. Y.-P. Yang, "When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?," *SSRN Electronic Journal*, Jan. 2022, doi: [10.2139/ssrn.4027692](https://doi.org/10.2139/ssrn.4027692).
- [40] A. Ma, "Emerging Legal Issues in Blockchain for Construction Supply Chains," Dec. 2020, doi: [10.1145/3448823.3448880](https://doi.org/10.1145/3448823.3448880).
- [41] A. Napieralska and P. Kępczyński, "Redefining Accountability: Navigating Legal Challenges of Participant Liability in Decentralized Autonomous Organizations," 2024, doi: [10.48550/ARXIV.2408.04717](https://doi.org/10.48550/ARXIV.2408.04717).
- [42] Y. Liu, Q. Lu, G. Yu, H.-Y. Paik, and L. Zhu, "Defining Blockchain Governance Principles: A Comprehensive Framework," *arXiv*, Jan. 2021, doi: [10.48550/arxiv.2110.13374](https://doi.org/10.48550/arxiv.2110.13374).
- [43] J. Z. L. Covarrubias and I. N. L. Covarrubias, "Different types of government and governance in the blockchain," *Journal of Governance and Regulation*, vol. 10, no. 1, p. 8, Jan. 2021, doi: [10.22495/jgrv10i1art1](https://doi.org/10.22495/jgrv10i1art1).
- [44] A. Ferreira, "Emerging regulatory approaches to blockchain based token economy," *The Journal of the British Blockchain Association*, vol. 3, no. 1, p. 1, Mar. 2020, doi: [10.31585/jbba-3-1-\(6\)2020](https://doi.org/10.31585/jbba-3-1-(6)2020).
- [45] Y. Aouidef, F. Ast, and B. Deffains, "Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects," *Frontiers in Blockchain*, vol. 4, Mar. 2021, doi: [10.3389/fbloc.2021.564551](https://doi.org/10.3389/fbloc.2021.564551).
- [46] D. Adam, D. B. Matellini, and A. Kaparaki, "Benefits for the bunker industry in adopting blockchain technology for dispute resolution," *Blockchain: Research and Applications*, vol. 4, no. 2, p. 100128, Jan. 2023, doi: [10.1016/j.bcr.2023.100128](https://doi.org/10.1016/j.bcr.2023.100128).
- [47] O. Akpobome, "The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation," *International Journal of Research Publication and Reviews*, vol. 5, no. 10, p. 5046, Oct. 2024, doi: [10.55248/gengpi.5.1024.3012](https://doi.org/10.55248/gengpi.5.1024.3012).
- [48] M. N. Yaacob, S. Z. S. Idrus, and M. Idris, "Managing Cybersecurity Risks in Emerging Technologies," *International Journal of Business and Technopreneurship*, vol. 13, no. 3, p. 253, Oct. 2023, doi: [10.58915/ijbt.v13i3.297](https://doi.org/10.58915/ijbt.v13i3.297).
- [49] B. P. Pokharel, N. Kshetri, S. R. Sharma, and S. Paudel, "block-HealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems," *Information*, vol. 16, no. 2, p. 133, Feb. 2025, doi: [10.3390/info16020133](https://doi.org/10.3390/info16020133).
- [50] M. Hiwale, R. Walambe, V. Potdar, and K. Kotecha, "A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine," *Healthcare Analytics*, vol. 3, p. 100192, May 2023, doi: [10.1016/j.health.2023.100192](https://doi.org/10.1016/j.health.2023.100192).
- [51] R. Belen-Saglam, E. Altuncu, Y. Lu, and S. Li, "A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems," *arXiv*, Jan. 2022, doi: [10.48550/arxiv.2210.04541](https://doi.org/10.48550/arxiv.2210.04541).
- [52] S. Dewi, A. Firasati, L. Sitoayu, and D. Bennet, "Risk Management Strategies in Blockchain Adoption within Financial Institutions: Analyzing Challenges and Opportunities," *Aptisi Transactions on Management*, vol. 9, no. 1, p. 20, Jan. 2025, doi: [10.33050/atm.v9i1.2393](https://doi.org/10.33050/atm.v9i1.2393).
- [53] O. Reis, N. E. Eneh, B. Ehimuan, A. Anyanwu, T. Olorunsogo, and T. O. Abrahams, "Privacy law challenges in the digital age:

- a global review of legislation and enforcement,” *International Journal of Applied Research in Social Sciences*, vol. 6, no. 1, p. 73, Jan. 2024, doi: [10.51594/ijarss.v6i1.733](https://doi.org/10.51594/ijarss.v6i1.733).
- [54] European Commission, “Commission decides not to extend antitrust block exemption for liner shipping consortia,” Press release IP/23/4742, Brussels, Belgium, Oct. 10, 2023.
- [55] K. Stylianou, *Antitrust in the Decentralized Economy*. Oxford, U.K.: Oxford University Press, 2025, doi: [10.1093/9780191925504.001.0001](https://doi.org/10.1093/9780191925504.001.0001).
- [56] C. Hutchinson and M. Egorova, “Potential Legal Challenges for Blockchain Technology in Competition Law,” *Baltic Journal of Law & Politics*, vol. 13, no. 1, pp. 74–91, 2020, doi: [10.2478/bjlp-2020-0004](https://doi.org/10.2478/bjlp-2020-0004).
- [57] C. Pike, “Antitrust and the Trust Machine,” OECD Blockchain Policy Series, Paris, France, 2020. [Online]. Available: <https://ssrn.com/abstract=3940527>.
- [58] National Assembly of Vietnam, *Law on Competition*, Law No. 23/2018/QH14, June 12, 2018 (effective July 1, 2019).
- [59] J. Wang, J. Liu, F. Wang, and X. Yue, “Blockchain technology for port logistics capability: Exclusive or sharing,” *Transportation Research Part B: Methodological*, vol. 149, p. 347, May 2021, doi: [10.1016/j.trb.2021.05.010](https://doi.org/10.1016/j.trb.2021.05.010).
- [60] C. Ansell and A. Gash, “Collaborative Governance in Theory and Practice,” *Journal of Public Administration Research and Theory*, vol. 18, no. 4, pp. 543–571, 2008, doi: [10.1093/jopart/mum032](https://doi.org/10.1093/jopart/mum032).
- [61] B. C. Ghosh et al., “Decentralized Cross-Network Identity Management for Blockchain Interoperation,” in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, May 2021, doi: [10.1109/icbc51069.2021.9461064](https://doi.org/10.1109/icbc51069.2021.9461064).
- [62] R. W. Ahmad, H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar, “Blockchain applications and architectures for port operations and logistics management,” *Research in Transportation Business & Management*, vol. 41, p. 100620, Feb. 2021, doi: [10.1016/j.rtbm.2021.100620](https://doi.org/10.1016/j.rtbm.2021.100620).
- [63] E. Marangone, C. Di Ciccio, D. Friolo, E. N. Nemmi, D. Venturi, and I. Weber, “Enabling Data Confidentiality with Public Blockchains,” *arXiv*, Jan. 2023, doi: [10.48550/arxiv.2308.03791](https://doi.org/10.48550/arxiv.2308.03791).
- [64] J. Liu, H. Zhang, and L. Zhen, “Blockchain technology in maritime supply chains: applications, architecture and challenges,” *International Journal of Production Research*, vol. 61, no. 11, p. 3547, May 2021, doi: [10.1080/00207543.2021.1930239](https://doi.org/10.1080/00207543.2021.1930239).
- [65] M. Jović, E. Tijan, D. Žgaljić, and S. Aksentijević, “Improving Maritime Transport Sustainability Using Blockchain-Based Information Exchange,” *Sustainability*, vol. 12, no. 21, p. 8866, Oct. 2020, doi: [10.3390/su12218866](https://doi.org/10.3390/su12218866).
- [66] S. N. A. A. Termizi, S. R. W. Alwi, Z. A. Manan, and P. S. Varbanov, “Potential Application of Blockchain Technology in Eco-Industrial Park Development,” *Sustainability*, vol. 15, no. 1, p. 52, Dec. 2022, doi: [10.3390/su15010052](https://doi.org/10.3390/su15010052).
- [67] C. Durán, A. K. Yazdi, I. Dérpich, and Y. Tan, “Leveraging Blockchain for Maritime Port Supply Chain Management through Multicriteria Decision Making,” *Mathematics*, vol. 12, no. 10, p. 1511, May 2024, doi: [10.3390/math12101511](https://doi.org/10.3390/math12101511).
- [68] Harshvardhan and S. Y. Teoh, “Improving Shipping Efficiency: Industry-Led Consortium Blockchain Smart Contract,” *Journal of Global Information Management*, vol. 30, no. 1, p. 1, Nov. 2022, doi: [10.4018/jgim.313035](https://doi.org/10.4018/jgim.313035).
- [69] I. Peronja, K. Lenac, and R. Glavinović, “Blockchain technology in maritime industry,” *Pomorstvo*, vol. 34, no. 1, p. 178, Jun. 2020, doi: [10.31217/p.34.1.19](https://doi.org/10.31217/p.34.1.19).
- [70] X. Xin, M. Liu, X. Wang, H. Chen, and K. Chen, “Investment strategy for blockchain technology in a shipping supply chain,” *Ocean & Coastal Management*, vol. 226, p. 106263, Jun. 2022, doi: [10.1016/j.ocecoaman.2022.106263](https://doi.org/10.1016/j.ocecoaman.2022.106263).
- [71] M. A. B. Farah et al., “A survey on blockchain technology in the maritime industry: Challenges and future perspectives,” *Future Generation Computer Systems*, vol. 157, p. 618, Apr. 2024, doi: [10.1016/j.future.2024.03.046](https://doi.org/10.1016/j.future.2024.03.046).
- [72] E. Irannezhad, “The Architectural Design Requirements of a Blockchain-Based Port Community System,” *Logistics*, vol. 4, no. 4, p. 30, Nov. 2020, doi: [10.3390/logistics4040030](https://doi.org/10.3390/logistics4040030).
- [73] H. J. 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*, vol. 16, no. 12, p. 454, Dec. 2024, doi: [10.3390/fi16120454](https://doi.org/10.3390/fi16120454).
- [74] G. Balci and E. Surucu-Balci, “Blockchain adoption in the maritime supply chain: Examining barriers and salient stakeholders in containerized international trade,” *Transportation Research Part E: Logistics and Transportation Review*, vol. 156, art. no. 102539, Dec. 2021, doi: [10.1016/j.tre.2021.102539](https://doi.org/10.1016/j.tre.2021.102539).
- [75] S. Wong, J. K.-W. Yeung, Y.-Y. Lau, T. Kawasaki, and R. Kwong, “A Critical Literature Review on Blockchain Technology Adoption in Supply Chains,” *Sustainability*, vol. 16, no. 12, art. no. 5174, 2024, doi: [10.3390/su16125174](https://doi.org/10.3390/su16125174).
- [76] B. George, “Blockchain in logistics: Critical insights for next-generation digital supply chains,” *Sustainable Social Development*, vol. 3, no. 4, 2025, doi: [10.54517/ssd3481](https://doi.org/10.54517/ssd3481).
- [77] L. Lessig, *Code: Version 2.0*. New York, NY, USA: Basic Books, 2006.
- [78] M. Hildebrandt, “Legal protection by design: Objections and refutations,” *Legisprudence*, vol. 5, no. 2, pp. 223–248, 2011, doi: [10.5235/175214611797885693](https://doi.org/10.5235/175214611797885693).
- [79] M. Hildebrandt, *Law for Computer Scientists and Other Folk*. Oxford, U.K.: Oxford University Press, 2020, doi: [10.1093/oso/9780198860877.001.0001](https://doi.org/10.1093/oso/9780198860877.001.0001).
- [80] M. Finck, *Blockchain Regulation and Governance in Europe*. Cambridge, U.K.: Cambridge University Press, 2018, doi: [10.1017/9781108609708](https://doi.org/10.1017/9781108609708).
- [81] P. De Filippi and A. Wright, *Blockchain and the Law: The Rule of Code*. Cambridge, MA, USA: Harvard University Press, 2018.
- [82] R. van Pelt, S. Jansen, D. Baars, and S. Overbeek, “Defining blockchain governance: A framework for analysis and comparison,” *Information Systems Management*, vol. 38, no. 1, pp. 21–41, 2021, doi: [10.1080/10580530.2020.1720046](https://doi.org/10.1080/10580530.2020.1720046).
- [83] Y. Liu, Q. Lu, L. Zhu, H.-Y. Paik, and M. Staples, “A Systematic Literature Review on Blockchain Governance,” *arXiv*, Jan. 2021, doi: [10.48550/arxiv.2105.05460](https://doi.org/10.48550/arxiv.2105.05460).
- [84] Y. Liu, Q. Lu, G. Yu, H.-Y. Paik, and L. Zhu, “A Pattern-Oriented Reference Architecture for Governance-Driven Blockchain Systems,” in *Proc. IEEE Int. Conf. Software Architecture (ICSA)*, 2023, pp. 23–34, doi: [10.1109/ICSA56044.2023.00011](https://doi.org/10.1109/ICSA56044.2023.00011).
- [85] S. van Engelenburg, B. Rukanova, W. Hofman, J. Ubacht, Y.-H. Tan, and M. Janssen, “Aligning Stakeholder Interests, Governance Requirements and Blockchain Design in Business and Government Information Sharing,” in *Electronic Government (EGOV 2020)*, LNCS 12219. Cham, Switzerland: Springer, 2020, pp. 197–209, doi: [10.1007/978-3-030-57599-1_15](https://doi.org/10.1007/978-3-030-57599-1_15).
- [86] D. Kumar, “GDPR Compliance Challenges in Blockchain-Based Systems,” *Scientific Journal of Artificial Intelligence and Blockchain Technologies*, vol. 1, no. 3, 2024, doi: [10.63345/sjaibt.v1.i3.104](https://doi.org/10.63345/sjaibt.v1.i3.104).
- [87] K. Wüst and A. Gervais, “Do you Need a Blockchain?,” in *Proc. 2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, 2018, pp. 45–54, doi: [10.1109/CVCBT.2018.00011](https://doi.org/10.1109/CVCBT.2018.00011).
- [88] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview,” National Institute of Standards and Technology, NISTIR 8202, Oct. 2018, doi: [10.6028/NIST.IR.8202](https://doi.org/10.6028/NIST.IR.8202).
- [89] A. B. Pedersen, M. Risius, and R. Beck, “A Ten-Step Decision Path to Determine When to Use Blockchain Technologies,” *MIS Quarterly Executive*, vol. 18, no. 2, pp. 99–115, 2019. [Online]. Available: <https://aisel.aisnet.org/misqe/vol18/iss2/3/>.

- [90] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004, doi: [10.2307/25148625](https://doi.org/10.2307/25148625).
- [91] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007, doi: [10.2753/MIS0742-122240302](https://doi.org/10.2753/MIS0742-122240302).
- [92] J. Venable, J. Pries-Heje, and R. Baskerville, "FEDS: a Framework for Evaluation in Design Science Research," *European Journal of Information Systems*, vol. 25, no. 1, pp. 77–89, 2016, doi: [10.1057/ejis.2014.36](https://doi.org/10.1057/ejis.2014.36).
- [93] N. Prat, I. Comyn-Wattiau, and J. Akoka, "A Taxonomy of Evaluation Methods for Information Systems Artifacts," *Journal of Management Information Systems*, vol. 32, no. 3, pp. 229–267, 2015, doi: [10.1080/07421222.2015.1099390](https://doi.org/10.1080/07421222.2015.1099390).
- [94] R. Michaels, "The Functional Method of Comparative Law," in *The Oxford Handbook of Comparative Law*, M. Reimann and R. Zimmermann, Eds. Oxford, U.K.: Oxford University Press, 2006, pp. 339–382, doi: [10.1093/oxfordhb/9780199296064.013.0011](https://doi.org/10.1093/oxfordhb/9780199296064.013.0011).
- [95] Digital Container Shipping Association, "DCSA's member carriers commit to a fully standardised electronic bill of lading by 2030," Feb. 2023. [Online]. Available: <https://dcsa.org/newsroom/dcsas-member-carriers-commit-to-a-fully-standardised-electronic-bill-of-lading-by-2030>.
- [96] B. Flyvbjerg, M. K. Skamris Holm, and S. L. Buhl, "How (In)accurate Are Demand Forecasts in Public Works Projects? The Case of Transportation," *Journal of the American Planning Association*, vol. 71, no. 2, pp. 131–146, 2005, doi: [10.1080/01944360508976688](https://doi.org/10.1080/01944360508976688).
- [97] National Assembly of Vietnam, *Law on Personal Data Protection*, Law No. 91/2025/QH15, June 26, 2025 (effective January 1, 2026).
- [98] Government of Vietnam, *Decree No. 356/2025/ND-CP Detailing a Number of Articles and Measures for the Implementation of the Law on Personal Data Protection*, December 31, 2025.
- [99] National Assembly of Vietnam, *Law on Data*, Law No. 60/2024/QH15, November 30, 2024 (effective July 1, 2025).
- [100] Parliament of Singapore, *Personal Data Protection Act 2012*, Act 26 of 2012, as amended.
- [101] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), *Official Journal of the European Union*, L 119, May 4, 2016.
- [102] Parliament of Singapore, *Electronic Transactions Act 2010*, as amended by the Electronic Transactions (Amendment) Act 2021.
- [103] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *Official Journal of the European Union*, L 257, Aug. 28, 2014.
- [104] Commission Regulation (EC) No 906/2009 of 28 September 2009 on the application of Article 81(3) of the Treaty to certain categories of agreements, decisions and concerted practices between liner shipping companies (consortia), *Official Journal of the European Union*, L 256, Sept. 29, 2009; extended by Commission Regulation (EU) 2020/436 and expired April 25, 2024.
- [105] National Assembly of Vietnam, *Law on Cybersecurity*, Law No. 24/2018/QH14, June 12, 2018.
- [106] Government of Vietnam, *Decree No. 53/2022/ND-CP Detailing a Number of Articles of the Law on Cybersecurity*, August 15, 2022.
- [107] National Assembly of Vietnam, *Law on Electronic Transactions*, Law No. 20/2023/QH15, June 22, 2023.
- [108] Government of Vietnam, *Decree No. 85/2019/ND-CP on the Implementation of Administrative Procedures under the National Single Window, ASEAN Single Window and Specialized Inspection for Imported and Exported Goods*, November 14, 2019.
- [109] Saigon Newport Corporation, "Officially Launching SNP ePort Mobile App of Saigon Newport Corporation," Aug. 15, 2022.
- [110] General Department of Vietnam Customs, "Summary Report of Scientific Research Project TCHQ/ĐT/2022-18: Applying Artificial Intelligence (AI) to Collect, Aggregate, and Analyze Information Serving Customs Leadership Direction and Administration," Hanoi, Vietnam, 2023.
- [111] Government of Vietnam, *Decree No. 13/2023/ND-CP on Personal Data Protection*, April 17, 2023 (expired December 31, 2025).
- [112] National Assembly of Vietnam, *Maritime Code of Vietnam*, Law No. 95/2015/QH13, November 25, 2015 (effective July 1, 2017).
- [113] Global Shipping Business Network, "Global Shipping Business Network Successfully Incorporated to Accelerate the Digital Transformation of Global Shipping and Trade," Press release, Hong Kong, Mar. 17, 2021. [Online]. Available: <https://www.prnewswire.com/news-releases/global-shipping-business-network-successfully-incorporated-to-accelerate-the-digital-transformation-of-global-shipping-and-trade-301248048.html>.
- [114] Smart Maritime Network, "Portbase brings TradeLens blockchain to Dutch ports," Aug. 31, 2020. [Online]. Available: <https://smartmaritimelens.com/2020/08/31/portbase-brings-tradelens-blockchain-to-dutch-ports/>.
- [115] Portbase, "About us: the Port Community System of the Dutch ports." [Online]. Available: <https://www.portbase.com/en/about-us/>.
- [116] Finextra, "Bank-backed blockchain consortium we.trade files for insolvency," Jun. 2022. [Online]. Available: <https://www.finextra.com/newsarticle/40408/bank-backed-blockchain-consortium-we.trade-files-for-insolvency>.
- [117] Global Trade Review, "Marco Polo brings in liquidators as funds run dry," Feb. 2023. [Online]. Available: <https://www.gtreview.com/news/top-stories/marco-polo-brings-in-liquidators-as-funds-run-dry/>.
- [118] Global Trade Review, "Contour to shut down as bank shareholders pull funding," Oct. 2023. [Online]. Available: <https://www.gtreview.com/news/fintech/exclusive-contour-to-shut-down-as-bank-shareholders-pull-funding/>.
- [119] Insurance Journal, "Industry's Blockchain Project, B3i, Ceases to Trade After Filing for Insolvency," Jul. 29, 2022. [Online]. Available: <https://www.insurancejournal.com/news/international/2022/07/29/677926.htm>.
- [120] Trade Finance Global, "CargoX authorized by the Egyptian government as blockchain provider for ACI declaration," 2021. [Online]. Available: <https://www.tradefinanceglobal.com/posts/cargox-authorized-by-the-egyptian-government-as-blockchain-provider-for-aci-declaration/>.
- [121] Ledger Insights, "Japan's trade blockchain TradeWaltz goes into production," 2021. [Online]. Available: <https://www.ledgerinsights.com/japans-trade-blockchain-trade-waltz-goes-into-production-this-week/>.
- [122] FreightWaves, "Logistics provider ShipChain, which built on blockchain, shutting down after big payment to SEC," 2021. [Online]. Available: <https://www.freightwaves.com/news/logistics-provider-shipchain-which-built-on-blockchain-shutting-down-after-big-payment-to-sec>.