Irannezhad, Elnaz

Article

The architectural design requirements of a blockchain-based Port Community System

Logistics

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Irannezhad, Elnaz (2020) : The architectural design requirements of a blockchain-based Port Community System, Logistics, ISSN 2305-6290, MDPI, Basel, Vol. 4, Iss. 4, pp. 1-31, https://doi.org/10.3390/logistics4040030

This Version is available at:
https://hdl.handle.net/10419/310120

logistics

MDPI

Article

The Architectural Design Requirements of a Blockchain-Based Port Community System

Elnaz Irannezhad

The Australian Road Research Board, Brisbane, QLD 4006, Australia; elnaz.irannezhad@arrb.com.au

Received: 18 September 2020; Accepted: 12 October 2020; Published: 20 November 2020

Abstract: This paper presents the value proposition of blockchain for Port Community Systems (PCS) by dissecting the business processes in port logistics and unfolding functionalities of blockchain in lowering the transaction cost. This paper contributes to the research by a detailed technical assessment of the plethora of currently available blockchain platforms and consensus mechanisms, against the identified requirements in this specific use case. The results of this technical assessment highlight the central value proposition of blockchain for landlord ports, which is independency from a central authority as the controlling agent. Bridging between two research domains of Information Technology and Logistics, this paper proposes the preferred architectural design requirements of a blockchain-based PCS, including provisioning private sidechains, modular design with inter-chain interoperability, and encrypted off-chain data storage. Availability—the readiness for correct service, and reliability—the continuity of correct service, are heavily reliant on the right choice being made for blockchain design for such a complex use case. A preliminary comparative analysis among different decentralisation levels in this paper suggests that a permissioned public blockchain offers the best trade-off in performance measures for this use case. This technical review identifies six research agenda from a design perspective.

Keywords: supply chain; logistics; freight transportation; distributed ledger technology; maritime transportation; international trade

1. Introduction

The international trade and supply chain, deluged by a growing complexity of information and physical transactions, face critical challenges such as compliance, traceability, governance, higher transaction costs, and security [1]. Despite the high monetary valuation of the transactions and the regulatory scrutiny, the core data infrastructure in the maritime logistics is currently unable to keep pace with digitisation trends [1].

Increasing the efficiency and productivity of supply chain as the primary driver of competitiveness among adjacent ports has led to developing integrated information exchange platforms or so-called Port Community Systems (PCS) in a number of modern ports. PCS development has gone through various transformation waves and the ongoing latest wave, started in 2018, concerns the PCS evolution by new concepts like blockchain and Artificial Intelligence [2]. There is extensive research on PCS and the impacts of information exchange platforms on the port performance [2–8]. However, despite the strong practical potential of these new trends, the integration of blockchain and PCS has not been explored in the academic literature [2].

In the absence of PCS, a significant number of transactions can be impacted by data discrepancies and disputes due to lots of paperwork, multiple stakeholders, and human mistakes. While PCS reduces these costs, similar to any centralised platform, additional charges emerge for maintaining the security and immutability of data in the platform. Furthermore, implementing a centralised PCS

does not seem a viable solution since the logistics operators are less likely to share their business information with the port authorities, particularly in landlord ports [9]. This is where blockchain technology can circumvent the PCS adoption barriers and pave the road for horizontal and vertical industry integration.

Blockchain is an open-source and distributed platform that allows a more efficient, transparent, and trustworthy flow of transactions between companies and individuals by removing the middleman and cutting out the costs, time-lapses, and inter-parties lack of trust issues, while also maintaining the privacy, immutability, and business data confidentiality [10]. Blockchain technology has been identified globally as a potential tool to disrupt many industries, including the supply chain and logistics industry. It is worth mentioning that the complex multi-level permissioning schemes and the distributed feature of blockchain are something that can be achieved with existing databases. What makes blockchain stand out compared to centralised digital enterprise solutions is the capacity to build trust without relying on a single authority to provide administrative control over the system or business rules. In other words, what differentiates a blockchain-based PCS from a centralised PCS is solving the "who" problem, such as the following questions: Who owns the data? Who is allowed to edit/change/delete the data? Who creates the database and maintains it? Who ensures the validity of data and verifies the transactions and claims?

Accordingly, a number of international ports have committed to delivering a pilot blockchain-based platform, including the Port of Antwerp, Port of Rotterdam, Port of Valencia, Associated British Ports (ABP), Port of Abu Dhabi, Port of Montreal, and Port of Busan in South Korea. TradeLens, a product of a partnership between IBM (multinational technology and consulting company) and Maersk shipping line, is keeping ahead in a race with other products such as CargoX [11]. More recently, nine shipping lines and terminal operators also announced their 'declaration of intent' to form a blockchain consortium as the Global Shipping Business Network (GSBN) and shareholders of CargoSmart Limited—a blockchain-based logistics initiative (https://www.maritime-executive.com/article/nine-companies-sign-up-for-global-shipping-business-network).

Notably, these pilot projects have deployed various blockchain platforms with different architectural designs. Given the competitive nature of these businesses, the criteria for choosing the specific design and benchmarking the performance of these pilot projects have not been reported in detail. For example, one of the critical decisions is the level of decentralisation, which defines if a blockchain architecture is public, private, or permissioned (consortium). The literature of Information Technology provides flowcharts and general guidelines about the suitability of public, private, permissioned, or hybrid blockchains [12,13]. However, to the best of our knowledge, these criteria have not been systematically fine-tuned for a blockchain-based PCS platform, at least in the academic literature.

Integration of blockchain and supply chain are expected to become new research hotspots in the supply chain and logistics domain, particularly with the digital supply chain innovations, advances of enterprise blockchain solutions, Internet of Things (IoT), and implementation of national strategies [14]. In the academic literature, the interest in blockchain and its business applications has been steadily growing over the last few years [15]. The literature on the application of blockchain in the supply chain can be grouped into five categories as: (i) business model and business process implications [16–19], (ii) descriptive assessment of potentials and challenges [20–26], (iii) simulation models [27–30], (iv) single or multiple case study approach [31–36], and (v) survey-based methodology to analyse the adoption behaviours [37–42].

In the maritime supply chain domain, Yang [11] explored the factors affecting intentions to use blockchain on a sample of 38 shipping experts in Taiwan. The results of interviews reconfirmed that intention of using blockchain positively associates with three factors as: (i) digitalising and easing paperwork, (ii) customs clearance management, and (iii) standardisation and platform developments.

Notably, the differences of blockchain architectures have been overlooked in the scientific literature of blockchain in the supply chain domain, which affects the generalisability of the findings. Even more surprisingly, there exists confusion and often generalisation of different types of blockchain

and consensus algorithms in the literature. For example, many blockchain technology assessments have been made based on the assumption that all blockchain projects utilise the same consensus mechanism, such as Bitcoin—Proof of Work (PoW). Notably, there is no assessment of the various consensus mechanisms in the supply chain and logistics domain. A thorough investigation into the existing platforms, properties, and challenges would be valuable to future investment decision making by practitioners. Hence, the critical research gap concerns architectural design choices for this specific use case. This paper aims to fill this gap by a thorough investigation of the existing blockchain platforms, particularly reviewing the technical properties and challenges in the port logistics. This review aims to answer the following questions:

- What is the value proposition of blockchain in the port logistics?
- What is the preferred architectural design of a blockchain-based PCS platform?

Contributions of this paper are as follows. First, the value propositions of blockchain for port logistics are dissected based on the Transaction Cost Economics (TCE) theory. From a socio-economic perspective, the first step to understand the necessary conditions for the adoption of blockchain is studying the transaction cost and value attribution in this specific setting. Second, a critical review is undertaken on the blockchain components, quality attributes, and the main existing platforms, namely Enterprise Ethereum solutions and Hyperledger solutions. The third contribution involves cross-validating the system attributes of these platforms with the business requirements in the port logistics. Based upon this cross-validation, recommendations of the architectural design requirements are made with the aim of lowering transaction costs. Lastly, six new research agenda are specified.

The remainder of the paper is comprised of the following sections. Section 2 presents an overview of blockchain components, and reviews two market-ready blockchain platforms. Section 3 presents an overview of the port logistics process. Section 4 presents the value creation of the blockchain. Section 5 presents the suggestive findings of a blockchain-based PCS platform design requirements. Section 6 discusses possible areas for future research, and Section 7 draws conclusions from this study and provides closing remarks.

2. Overview of Blockchain

This section unfolds the main blockchain components, the performance measures, and reviews the most applicable blockchain platforms in the supply chain and logistics use-cases.

2.1. Blockchain Components

Blockchain platforms are categorised into three types, namely, public, private, and permissioned blockchains. The permissioned blockchain is defined as a system where one or more authorities act as a gate for the participation of other members. Permissioning in blockchain can be done at multiple levels, for example, permission to join the network (and thus read information from the blockchain network), permission to initiate transactions, or permission to validate ledgers.

As depicted in Table 1, public permission-less networks currently suffer from a number of challenges that make them problematic for enterprises. They are notoriously unscalable and expensive to use. Generally, private blockchain platforms do not suffer from the throughput, latency, and scalability problems as much as public blockchains do. Nevertheless, private blockchains are subject to debates and critics since they create another form of power-broking middleman and defeat the whole purpose of the blockchain.

Table 1. The level of decentralisation and blockchain properties (adopted from Reference [43]).

		Throughput, Latency, and Scalability Efficiency	Integrity and Security Efficiency	Transaction Cost-Efficiency
Public blockchain	Permission-less	+	+++	+
	Permissioned	++	++	++
Private blockchain	Permission-less	+++	+	+++
	Permissioned	+++	+	+++

By and large, however, all these blockchain platforms consist of common features, namely, a sequence of blocks of distributed ledgers across peers (client nodes), validation algorithm, cryptography (hashing system), data storage layer, communication channels, and smart contracts (Figure 1). The following subsections explain the blockchain components in more detail.

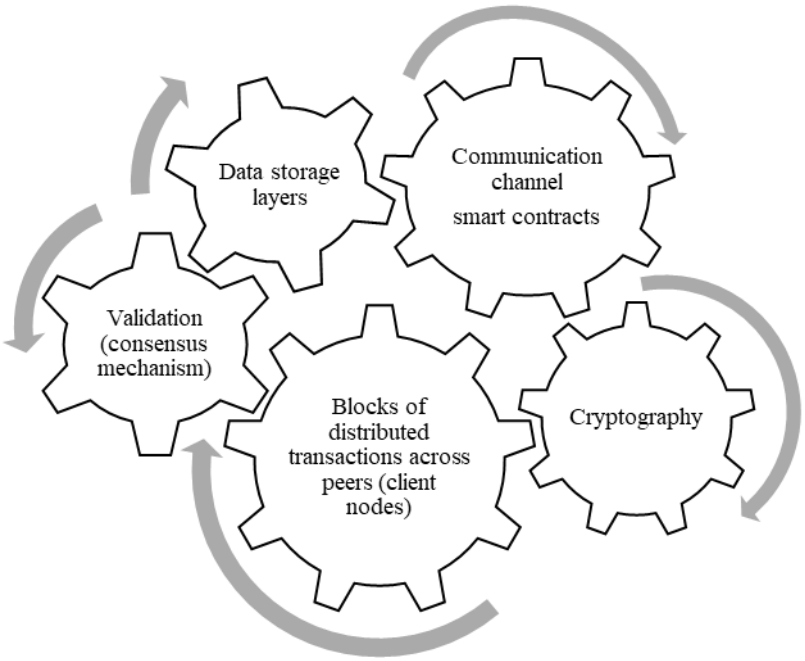

Figure 1. Blockchain features.

2.1.1. Cryptography

Cryptographic mechanisms or so-called hashing algorithms provide the security of a blockchain network by encrypting the transaction data. There are various cryptographic hash functions, but all are common in having an 'avalanche effect', which means even a small change in the input will be drastically reflected in the hash. Interested readers are referred to [44], who describes the various cryptography algorithms in detail.

2.1.2. Blocks of Distributed Transactions

Following the notations of Ethereum [45], the blockchain data structure is defined as a transaction-based state machine where ledgers of transactions link two states, as follows:

$$\sigma_{t+1} \equiv \gamma(\sigma_t\ ,\ T) \tag{1}$$

where γ is a state transition function. Transaction T is an encrypted instruction constructed by a blockchain node (user) and can represent either a message call or a new autonomous object (used for

contract creation). This instruction roughly consists of a transaction proposal and a transaction receipt. Transaction proposal is sent by a client node to the validating nodes and contains information about the transaction, such as sender, the account whose code is to be executed, value, and computational costs. Transaction receipt contains the results after the execution of the transaction, namely the validator's signature and timestamp of execution. Accordingly, transaction T is presented as:

$$T \equiv \begin{cases} \left(T_n,\ T_p,\ T_g,\ T_t,\ T_v,\ T_i,\ T_w,\ T_r,\ T_s\right) & \text{for contract creation} \\ \left(T_n,\ T_p,\ T_g,\ T_t,\ T_v,\ T_d,\ T_w,\ T_r,\ T_s\right) & \text{for message calls} \end{cases} \tag{2}$$

where T_n is the number of transactions, T_p is the computational costs of transaction execution, T_g is the maximum amount of computational costs, T_t is the address of the recipient, and T_v is the amount of transferred value. The combination of T_w, T_r, and T_s represents the signature of the sender, including the chain identifier, private key, and timestamp, respectively. T_i and T_d specify the account initialisation and input data of the message call, respectively. Transactions $(T_0, T_1, \dots)$ are then collated into blocks using a cryptographic hash as a mean of reference. Accordingly, the block-level state transition function can be re-written as:

$$\sigma_{t+1} \equiv \Pi(\sigma_t\ ,\ B) \tag{3}$$

Accordingly, blockchains attain immutability from the hashing algorithm and creating a block of ledgers. Block B is constructed of:

$$B \equiv (H,\ T,\ U) \tag{4}$$

where H is the block header, T is the information corresponding to the list of compromised transactions, and U is the block metadata that contains information about this block such as the set of other block headers that have the same parent or so-called Ommer blocks. Figure 2 presents a simplified schematic of blocks and transactions.

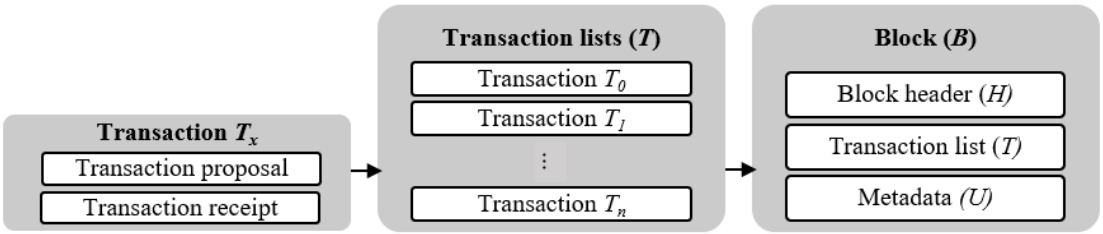

Figure 2. Simplified illustration of blocks and transactions.

Block header itself compromises of the hash of several other pieces of information which are useful for serialisation of blocks, such as a hash of the parent's block H_P, a hash of the Ommer list of this block H_o, timestamp, and a number of other information. The ledger structure varies across various blockchain platforms. For example, Bitcoin ledgers are presented in a list, while in others, are either as a directed acyclic graph of blocks (e.g., Hedra Hashgraph, which is an enterprise public blockchain), or the abstract logical view of the transaction history of a global graph of transactions (e.g., R3 Corda, which is an enterprise public blockchain).

In public blockchain protocols, a transaction passes through consecutive phases before being considered as committed (shown in Figure 3). First, after the transaction submission, it is announced in a pool. If the previous transactions (so-called parents) are yet unknown, the transaction inclusion will be delayed, waiting for the parent transactions to arrive. However, validators might decide to drop the transaction from the pool, which in that case, it is called an 'orphan' transaction. A transaction may also contain a parameter, so-called 'lock time', declaring it as invalid until the block with a certain sequence number has been validated. Lock time enables setting an 'execution date'. Waiting for a higher number of confirmation blocks may increase confidence in integrity and durability of transactions but will harm the latency and the throughput of the system.

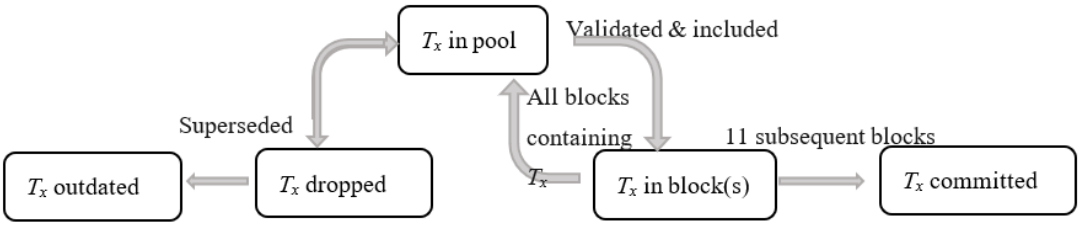

Figure 3. Transaction inclusion in Ethereum (adopted from Reference [46]).

2.1.3. Validation

The block finalisation is achieved through a validation process, which is bolstering a block over any other potential competitor blocks. Block-finalisation state transition function is defined as:

$$\Pi(\sigma_t\ ,\ B) \equiv \Omega(\ B,\ \gamma(\gamma(\sigma_t\ ,\ T_0),\ \ T_1\ ),\ldots) \tag{5}$$

where Ω is the block finalisation state transition function which commonly compromises of four actions: (i) validating transaction, (ii) validating Ommer transactions, (iii) verifying state and mapping a block to its initiation state, and (iv) applying rewards.

Accordingly, block finality is an essential blockchain property which affirms that once the confirmed blocks are committed, they cannot be revoked, arbitrarily changed, or reversed. In the literature, two types of finality are defined, namely probabilistic and absolute finality. Probabilistic finality refers to public blockchains such as Ethereum, in which the probability of transaction finality increases as the block length increases. Absolute finality is mostly achieved in permissioned or private protocols such as Hyperledger, in which the finality is immediately obtained once it is validated. Notably, the finality of public blockchains can be affected by transaction reordering. Hence, in order to keep the integrity (i.e., time ordering) of transactions, it is essential that a suitable transaction lock time is set up, and also, high-speed links between certain nodes in public blockchains are provided [46].

A set of rules and validation procedures is called a consensus algorithm, which maintains the coherency between multiple participating nodes. The consensus mechanism is one of the blockchain pillars, even in permissioned and private blockchains. The role of the consensus mechanism becomes more important where there are untrusted and unknown nodes in the network. The choice of consensus protocol impacts performance measures such as security and scalability.

Proof of Work (PoW) is the most common consensus mechanism used in public blockchains such as Bitcoin and Ethereum, which is notorious for its computationally heavy and energy-consuming mining process. However, this is intentional, and the reason is that it prevents anyone from easily taking over the network (explained in the Appendix A). Thus, PoW is very suitable for high levels of decentralisation where anyone (including attackers) can participate in the network. In permissioned public blockchains, nodes are intrinsically more trusted than those in the permission-less public blockchains. As such, the PoW consensus mechanism may be overly burdensome, and other mechanisms may provide 'enough' trust to run a distributed system [47]. Hence, several consensus algorithms have been developed. Notably, there is no perfect consensus mechanism, and there is always a trade-off between these mechanisms in terms of throughput, latency, security, and scalability [48].

Fault tolerance, as another important aspect of blockchain, refers to the possibility that consensus agreement occurs. Higher fault tolerance translates into higher reliability. Notably, these consensus mechanisms can be combined for a greater outcome. For example, the hybrid PoW and Proof of Stake (PoS) deployed in Neo and Zililiqa blockchains requires much lower amounts of energy than PoW, while it provides higher integrity compared to PoS.

A comparison of the leading consensus algorithms is depicted in Table 2, which is summarised based upon an extensive review of various platforms in the IT literature [43,47–50]. This comparison includes the relative performance measures, transaction costs, fault tolerance, and block finality.

Table 2. Comparison of consensus algorithms (developed by the author from the studies in References [43,47–50]).

Consensus Algorithm	Description	Applications	Advantages	Challenges
Proof of Work (PoW)	Based on the information of the previous block, the different nodes calculate the specific solution of a mathematical problem. Computational power is required to solve the math problem. The first node that solves this math problem can create the next block and get a certain amount of reward in terms of Ether, or any other kind of token.	Suitable for public permission-less blockchains, e.g., Bitcoin and Ethereum	Good scalability, 50% Byzantine fault tolerance	High computation and power consumption, probabilistic finality
Proof of stake (Pos)	In PoS, those who hold tokens can "stake" their tokens (staking means to temporarily place the tokens in a locked smart contract—until staking is over) and in exchange, confirm transactions and receive rewards based on the relative number of tokens held. PoS does not need relative computing power required in PoW but needs at least the same held stake of the transaction cost.	Suitable for public permission-less blockchains, e.g., Hedra Hashgraph, EOS, Qtum, and Nano	Less consumption and computation power compared to PoW, good scalability, 50% Byzantine fault tolerance	Inequality since wealthier stakeholders are more likely rewarded, probabilistic finality
Zero Proof of Knowledge (ZPK)	In ZKP, there are two key actors, namely prover and validator. The prover gets some authenticated secret knowledge. The validator request on prover's data. The prover computes the response and constructs the proof of correct computation. The validator applies ZKP algorithm to ensure the answer is correct. Cryptography is complex and computationally expensive. However, the third version, released in 2020, combines up to 20 transactions together, thereby reducing costs.	Suitable for public permission-less blockchains, e.g., EY Ops Chain, EY Blockchain Analyzer, Blocknet	Computational efficiency due to no encryption, good scalability, protecting the privacy	Probabilistic finality
Proof of Importance (PoI)	POI not only rewards nodes with a large account balance (similar to PoS) but also takes into account how much they transact to others and who they transact with and give them a score. In PoI, a participant with a higher score has an increased possibility of being selected as a validator.	Suitable for public permission-less blockchains, e.g., NEM	Less consumption and computation power compared to PoW and PoS, good scalability, 50% Byzantine fault tolerance	Major supply chain actors and more prominent companies get rewarded more, probabilistic finality
Proof of Authority (PoA)	PoA is a modified form of PoS where instead of stake with the monetary value, a validator's identity performs the role of stake. PoA uses a Byzantine Fault Tolerance algorithm which relies on a set of trusted validators.	Suitable for permissioned blockchains, e.g., Parity	Negligible power consumption, high performance in terms of throughput and latency, absolute finality	Need for trusted validators, 33% Byzantine fault tolerance

Table 2. *Cont.*

Consensus Algorithm	Description	Applications	Advantages	Challenges
RAFT	Raft uses a crash fault tolerance consensus mechanism, developed by researchers at Stanford University. It generally contains five server nodes. Up to two nodes are allowed to crash at the same time. The server node has three states: leader, follower, and candidate. There is only one leader in a term, and the leader is responsible for handling all clients' requests. Raft followers blindly trust their leader.	Suitable for permissioned blockchains, e.g., Quorum	Absolute finality, efficient storage saving, faster block time compared to other consensus algorithms, 50% crash fault tolerance.	Poor scalability, integrity issue since the leader is always assumed to act honestly.
Practical Byzantine fault tolerance (PBFT)	A validator verifies the proposed block just like PoW in an untrusted environment. Each node in the network publishes a public key. Then, when messages come through a node, it is signed by the node to verify the message as being the correct format. Once enough identical responses to the message are reached, the consensus that the message is a valid transaction is met. The list of validators that get involved in voting for each block can be dynamically expanded or reduced by asking existing validators to vote.	Suitable for permissioned blockchains, e.g., Hyperledger and Cosmos	Negligible power consumption, high performance in terms of throughput and latency, absolute finality, reduced time between blocks	Poor scalability, no guarantee on the anonymity, need for trusted validators, 33% Byzantine fault tolerance
Istanbul Byzantine fault tolerance (IBFT)	IBFT is similar to PoA and modification of PBFT. Each block requires multiple rounds of voting by the set of validators to arrive at a mutual agreement. Agreements are recorded as a collection of signatures on the block content.	Suitable for permissioned blockchains, e.g., Enterprise Ethereum solutions, Pantheons and Quorum	Negligible power consumption, high performance in terms of throughput and latency, absolute finality, reduced time between blocks	Poor scalability, no guarantee on the anonymity, need for trusted validators, 33% Byzantine fault tolerance

2.1.4. Data Storage

A data management strategy in order to increase the performance in blockchain-based projects is to store raw data off-chain and to store the metadata, hashes, and small-size critical data on the main chain. Many kinds of data are also better stored off-chain, for scalability reasons, for confidentiality reasons (private data), or for dealing with legacy databases. Therefore, another important architectural choice concerns the off-chain data storage.

2.1.5. Communication Channels and Smart Contracts

Transactions can be created through a smart contract, which is an automatic and self-executing contracting application. The idea of smart contracts was first proposed by [51], which combined computer protocols with user interfaces to execute the terms of a contract. Many blockchain platforms enable smart contracts. Reduction in payment reconciliation time and cost is the most important advantage of smart contracts in supply chain use-cases. Additionally, transactions which are sent from unauthorised agents, or in a wrong point of the process, can be automatically rejected, which prevents double-spending and human mistakes [52]. Interested readers are referred to a study by the authors of Reference [53], who provide a comprehensive review of various smart contracts.

Transactions in different blockchain platforms can be structured in different ways. In permissioned blockchain, transactions are only distributed to parties of interest via communication channels, to limit the distribution of transactions further while attesting to the integrity of unseen parts

of the transaction graph. Furthermore, state channel or sidechain is a technique for performing transactions and other state updates between different blockchains off-chain. Notably, things that happen "inside" of a state channel retain a very high degree of security and protection of off-chain data. Sidechain allows transactions of one blockchain/channel to be securely transferred and used in another blockchain/channel, while the integrity of blocks is still kept in the original chain or so-called main chain. Sidechains can be private chains which are linked to a public blockchain. Main chain can protect the transactions on the sidechains and prevent the forking issue. Sidechaining prevents overloading the main chain, reduces the latency, and increases the performance.

There are two ways of sidechaining, unilaterally and bilaterally linked. For a unilateral (or one-way) sidechain, the interaction is only from the main chain to the sidechain. For a bilateral sidechain, the communication is bidirectional. One mechanism to secure bilateral linked sidechains is essentially a voting system where a group of pre-specified peers vote to make decisions about a transaction [54,55]. While the private sidechain is pinned to the main chain, it only allows the permissioned members to interact with the data on the main chain. The pinning needs to be done in such a way that the list of participants in one sidechain is not revealed on the main chain as part of the pinning process. The rate of transactions needs to be masked such that participants on the main chain cannot infer the activity level on the sidechain [55].

2.2. Blockchain Performance Measures

Interaction of the abovementioned features affects the performance of a blockchain network, which can be measured in terms of throughput, latency, scalability, and transaction cost.

2.2.1. Throughput

Throughput is defined as the number of transactions that can be processed within a time period and depends on the decentralisation level, ledger, and block configuration [46].

2.2.2. Latency

Read and write latency is defined as the speed that the system responds to a request for reading or writing a transaction. Read and write latency is affected by demand, resource bottlenecks, smart contract, and architectural mechanisms used for scalability (e.g., load balancing) [46]. Read latency is often low in the blockchain platforms because peers can have a local copy of the blockchain. However, write latency is typically high because updates of transactions must be propagated across a global network. Validation latency is also defined as the time between the transaction submission and confirmation and is affected by the consensus protocol [46]. For example, latency in a public Ethereum network is around 3 min (consisting of 14 s block intervals with 12 block confirmation).

2.2.3. Scalability

Blockchain scalability also refers to the number of nodes and communication channels and is affected by the data storage and communication channels strategy.

2.2.4. Transaction Cost

Transaction cost is another critical concern in the design of a software system and particularly for the collaborative business processes. While the cost of the initial platform set up and on-going maintenance costs of private blockchains are high, these costs are very minimum for public blockchains [50]. Nevertheless, the cost of basic computation and storage on public blockchains has a different cost structure than conventional cloud infrastructure [56]. Public blockchain (e.g., Ethereum) costs orders of magnitude more than cloud services (e.g., Amazon Web Services) for practical uses for business process execution on a large-scale dataset [56]. This is basically the cost of distrust and distributed power that blockchain users have to pay. There is a cost (although not necessarily in

private blockchains) for new transactions, computation, and data storage on blockchain platforms. The costs of running and hosting applications can also be high. For example, in Ethereum, there is a fixed cost of 21,000 gas—the fee, or pricing value, required to successfully conduct a transaction or execute a contract on the Ethereum blockchain platform—in addition to variable costs concerning the transaction's complexity. If the arbitrary data is stored in a smart contract, the cost of storing data depends on the number of operations, which starts at 20,000 gas. Alternatively, arbitrary data can be excluded from the smart contract, and instead a subsequent transaction can be executed to update the variables, which in that case, it incurs 5000 gas instead of 20,000 gas. The third option is storing arbitrary data as a log event which costs 375 gas and an extra 8 gas for every byte of data. Interested readers are referred to References [44,46], who reviewed the cost models of public blockchains and smart contracts.

2.3. Most Common Blockchain Platforms

There is a plethora of blockchain platforms, some of which are more popular such as Ethereum, Hyperledger, R3 Corda, Cardano, Parity, Quorum, and Ops Chain. A review of the blockchain-based supply chain projects suggested that the majority are built on top of Ethereum and Hyperledger Fabric (10 and 9 out of 30 projects, respectively), and others are platform agnostic [10,57]. This is expected since, among a plethora of platforms and projects, these enterprise blockchain platforms are the only ones that meet the business goals in supply chain use cases. In the port logistics, freight companies are collaborating to streamline shared business processes, such as data management, transactions, and asset tracking. Hence, the focus of this paper is also based upon these two platforms. It should be noted that there is no single product called "Enterprise Ethereum", and what this term basically covers is the modified Ethereum platforms such as Quorum, Parity, and Pantheon that provide permissioning on top of the public Ethereum network. The following subsections provide an overview of these two blockchain solutions.

2.3.1. Ethereum

Undoubtedly, Ethereum is currently the most common platform used by over 2000 Decentralised applications (Dapps). Ethereum is an open-source collaborative project, proposed by Vitalik Buterin in 2014, which supports a modified version of Nakamoto consensus (i.e., consensus mechanism used in Bitcoin) via transaction-based state transitions. Ethereum enables smart contracts via the Ethereum Virtual Machine (EVM) and deploys Solidity programming language. The amount of computational cost in Ethereum is expressed as 'gas' which is used to calculate the fees that need to be paid to the network in order to execute an operation, such as running a smart contract or executing a transaction. Ethereum can currently process roughly 15 transactions per second. The reason for this slow throughput is that Ethereum public blockchains require every transaction to be processed by every single node in the network.

Hence, several advances have been made to overcome the performance inefficiencies, as shown in Figure 4. In the so-called Layer 1 protocol, Sharding architecture has been deployed to increase throughput and reduce latency in the Layer one protocol by splitting the network into different sections called shards, each of which can independently process transactions. In this way, the throughput can be increased by orders of magnitude. These shards can be presented as separate blockchains that connect to each other to share consensus agreement.

So-called Layer 2 solutions address the specific needs of an enterprise such as increased privacy, performance, and scalability, as well as permission and governance controls. Despite the Layer 1 protocol, the Layer 2 solutions solve the scalability issue by better utilizing the current capacity instead of increasing it. Layer 2 solutions provide better throughput by creating off-chains (or child-chains) and adjusting gas limits and block sizes, making it competitive with other enterprise solutions. State channels [58], Plasma [59], and Raiden [60] are examples of such solutions in the permission-less public blockchain applications.

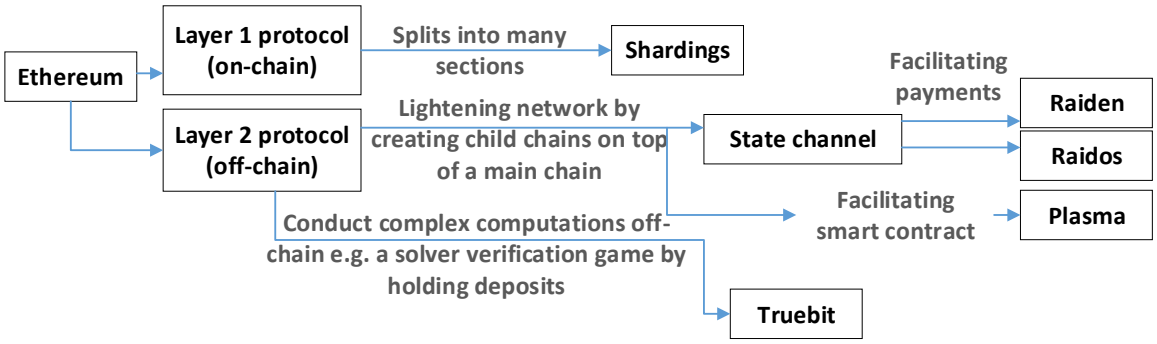

Figure 4. Public Ethereum protocols (developed by the author).

Notably, off-chains can also have their own consensus mechanism such as PoA or IBFT algorithm, while the main chain still deploys the PoW mechanism. Quorum (developed by JP Morgan) and Parity are examples of this solution. In these solutions, the capacity of the main chain remains the same, but many more transactions are performed in off-chains. In these Enterprise Ethereum solutions, nodes interact with various platforms through Application Programming Interfaces (APIs) and have full access to shared raw data, while also allowing for independent verifications.

In some of these solutions, however, the privacy settings are not suitable for an industry with high data confidentiality concerns. For example, while Quorum allows for transaction details to be made visible only to the parties specified in the contract, this feature is only available at the level of nodes, rather than between individual addresses. Consequently, in an industry with a high number of stakeholders, requiring each participant to run their own node is not feasible. Additionally, Quorum does not encrypt off-chain transactions [55]. Quorum has been used in supply chain applications such as AgriDigital, a food supply chain pilot project in Australia. Compared with the existing solutions, Quorum was evaluated as the best solution in 2016 based on throughput and privacy. The throughput of Quorum was sufficient for the AgriDigital use-case, producing sub-second transaction times for the exchange of digital currency and digital title. At a rate of four transactions per second, this settlement method was scalable to satisfy the throughput and latency requirements of the Australian grains industry. However, there were industry concerns in terms of transparency of transactions and scalability [46,61]. Newer Layer 2 solutions, such as Pantheon—the latest release of the Enterprise Ethereum collections—has addressed the privacy issue by encrypting the off-chain data, permissioning, and providing interoperability [62].

2.3.2. Hyperledger

Hyperledger is an open-source collaborative project, hosted by the Linux Foundation, which supports private and permissioned blockchain projects. Hyperledger developers have aimed to enable organisations to launch their own individual blockchain network. Hence, it has attracted over 200 organisations to develop their private or permissioned blockchain networks. In Hyperledger, all nodes of a network need to enrol through a trusted membership service provider. Despite Ethereum, nodes (users) of Hyperledger have known identities, and public keys are tied to the organisations and end-users. A channel allows a group of participants to create a separate ledger of transactions, shared only between themselves. The concept of a channel is similar to the off-chain in the Layer 2 solutions of the Ethereum, where the privacy and data confidentiality is guaranteed only between channel members, and no others can see the transactions on the associated ledger for that channel. Similar to traditional multi-layer database architectures, members in Hyperledger who are connected to one channel may be unaware of the existence of other channels.

Similar to the Ethereum Layer 2 solutions, nodes of the Hyperledger network have a pre-defined hierarchical role. There are three types of nodes within a Hyperledger system: client (end users), peer, and orderer (validators or miners). Peers commit transactions and maintain the state of the ledger.

Some of the peers can take a special role as the endorser. Each Chaincode might identify an endorsement policy to define the necessary and sufficient conditions for valid transaction endorsement. Such endorsement might involve single or multiple endorsers. Hyperledger deploys container technology for smart contracts (so-called Chaincode) execution. Container technology is a method to package an application so it can be run, with its dependencies, isolated from other processes.

The consensus mechanism used in Hyperledger is currently Practical Byzantine Fault Tolerance (PBFT), while it is claimed that various consensus mechanisms can be deployed in individual channels. In PBFT, each node in the network publishes a public key. Then, when messages come through a node, it is signed by the node to verify the message as being of the correct format. Once enough identical responses to the message are reached, a consensus that the message is a valid transaction is met. The PBFT consensus mechanism does not require any hashing power to validate transactions within a blockchain [63]. A transaction should be approved in three stages, including endorsement (done by peers), ordering (done by orderers), and validation. Validation checks the correctness of a set of ordered transactions within a block, considering the endorsement policy, and versioning checks for data integrity. Thakkar [64] provide six guidelines on configuring Hyperledger parameters (e.g., block size, endorsement policy, channels, resource allocation, and state database choices) based on an empirical study, and also identified three major performance bottlenecks and three simple optimisation methods to overcome those bottlenecks (for further details, see References [65,66]).

There are five major blockchain projects under the Hyperledger umbrella, namely Fabric, Sawtooth Lake, Iroha, Burrow, and Indy. Under modules, there are the Hyperledger Cello, Hyperledger Composer, Hyperledger Explorer, and Hyperledger Quilt. Fabric proposed by IBM is the most common project used by Hyperledger users. Fabric, developed by IBM, has addressed several problems of the public blockchain by providing permission, privacy, reduced read/write latency, and increased throughput. For the overview of Fabric architecture, interested readers are referred to a work by Bashir [44]. Table 3 summarises a comparative analysis of Ethereum and Hyperledger platforms.

Table 3. Comparative analysis of the two most common blockchain platforms (developed by author).

	Advantages	Limitations
Enterprise Ethereum solutions	Providing optional access to public Ethereum, which is the most used platform in the world so far. The capability of linking to a public network provides public enforcement for dispute resolution and arbitration while still maintains the full benefits of a privately controlled network. Tokenising or digitising of assets/transactions are enabled, which can be useful for incentivisation and removing international exchange rates. Negligible maintenance and deployment costs [50]. Encryption of the off-chain transactions is supported in the latest version. Adding a new participant is easier by merely executing a smart contract or so-called Ethereum Registration Authorities [67].	Lack of storage protocol since all private transactions need to be reprocessed each time an Enterprise Ethereum node restarted [55]. Lower performance measures compared to Hyperledger.
Hyperledger	Deployed by the dominant players in the maritime freight transportation and supply chain. Solving the performance scalability and privacy issues by permission mode of operation, using a IBFT algorithm and fine-grained access control. Supporting storage of data privately, by utilizing communication channels to provide a separation between different supply chain actors. Maintaining the existing business process and relationships by pre-specifying the roles of participants. Such as Access Control Lists (ACL) and data access rights. Encrypting of the off-chain transactions is supported in the latest version.	Hyperledger's assumption that all nodes (participants) are trusted cannot be fully supported in many applications, such as PCS. Ledgers are split in channels and even may lead to scalability issues because it becomes complicated to maintain a large number of encrypted channels at the same time and also maintaining a unified ledger structure on the entire network. The lack of bootstrapping method, which means adding new participants (e.g., a new importer, exporter, transport company, etc.) to a network is a complex and time-consuming process [55]. High initial setup costs, deployment costs, and maintenance costs [50].

3. Port Supply Chain

Maritime transportation is an example of a fragmented supply chain market where multiple parties interact with each other over one shipment, as shown in Figure 5. The interactions are in two layers of physical and administrative. Four types of transaction are identified within and across these two layers, namely information, financial, physical, and liability transaction [68]. Transaction cost is defined as the coordination cost incurred in a transaction, which consists of the costs of searching for agents or information, establishing a contract, governing, monitoring, settling disputes, or enforcing the implementation of contract. Coordination failures in transactions lead to higher logistics costs and losses of efficiency and productivity. In the context of port logistics, transaction costs include contract establishment costs (e.g., freight forwarder or customs broker fees), administrative fees (e.g., pre-receival permit and booking fees), transport service rates (e.g., terminal handling, storage and inland transport charges), governance costs (e.g., customs and auditing fees), and other costs for settling disputes and uncertainties.

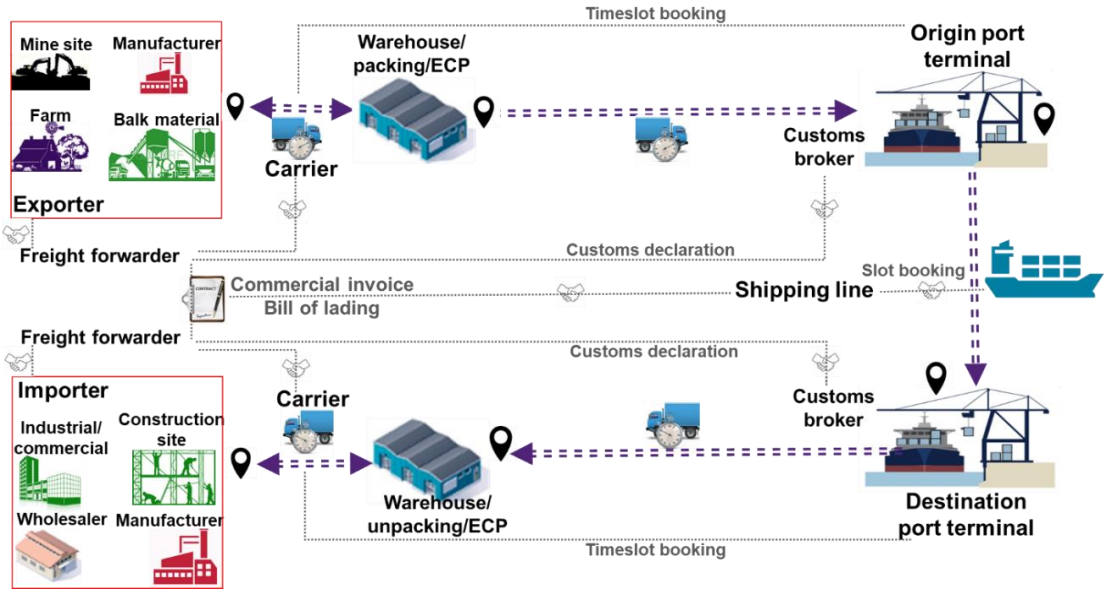

Figure 5. The fragmented market of international freight transportation.

Import/export trade starts with a bill of lading, which is a trade contract between consignor (seller or exporter) and consignee (buyer or importer) where the terms of sale and payments are identified. Importers and exporters may have in-house freight forwarder and customs broker, or they may contract these agents separately. Freight forwarders negotiate and contract with shipping lines and in-land carriers to manage the carriage stage. It is estimated that of total freight forwarder fee for administering of a container, 63% is the regular activities costs, 25% is the administrative costs related to customs checks, and 12% is the logistics preparation for scanning and inspections [69].

Customs brokers are responsible for submitting a summary document to the customs at least 3.5 days before the ship arrival, and releasing the container at maximum three days after the ship arrival [70]. The anecdotal evidence suggests that the freight forwarder should provide the customs broker with a list of relevant documents five days before the ship arrival. This suggests that all the necessary contracts and agreements should be finalised a few days in advance. Port terminals refer to businesses that engage in loading and unloading a ship's cargo. They are responsible for checking and releasing the discharged/charged cargo against manifest, customs declaration, and notifying the importer/exporter.

Shipping lines are responsible for carrying the containers and/or cargo, from the loading port to discharge at the destination port. Shipping lines may sign long-term contracts with in-land carriers

and offer door-to-door service. They may also operate, own, or share vessels, and may own or rent containers. They are also responsible for notifying the importer/exporter about the estimated arrival/departure date and the name of port terminal to/from which the cargo is discharged/charged. Freight forwarders submit a booking order to a shipping line that includes an approximate volume/number of containers and the preferred time window for shipping. Freight booking order allows the shipping line to pre-plan the probable demands with respect to vessel capacities and schedules. Final booking is confirmed by the shipping line when the details of the cargo and the cut-off dates are finalised. The cut-off date is the deadline for the exporter that determines whether the full container should be in port terminal and is determined based on ship schedule. Final booking triggers assigning an empty container number which is simultaneously announced to the empty container park (ECP) and the freight forwarder.

Notably, only full containers generate revenue for shipping lines. Shipping lines impose restrictive time windows for importers and exporters in order to afford enough time in balancing the empty and full containers and optimise their revenue. Exceeding the time window incurs demurrage and detention fees which are borne by importers and exporters. Demurrage refers to the delay in picking up the full container, and detention is the delay in delivering an empty container. While these rates vary across shipping lines, they also have different demurrage and detention regimes across various customers, ports, and in-land carrier modes (rail or road). These regimes tend to favour trucking as the hinterland transport mode [69]. The time windows and fees are negotiable and are not transparent.

Port terminals also charge the importers and exporters if the storage exceeds the free days, and the daily storage rate increases exponentially the longer the container is left on the terminal's yard. The reasons causing storage include inconsistency between the documents, delay in customs release, missing the ship, unpaid duty and/or Goods and Services Tax (GST) invoice, and missing permits.

In export supply chain, freight forwarders are required to prepare a mandatory document called Export Receival Advice (ERA), or an electronic version called a Pre-Advice Export Receival Advice (PRA). The ERA/PRA includes details of the packed container such as the contents, booking number, container number, and booking timeslot at the stevedore. The valid ERA/PRAs are manifested to the truck registration number and are entered in the timeslot booking at the port terminals. If for any reason there is an inconsistency in the information in the ERA/PRA, the freight forwarder must submit an amendment and pay an amendment fee. Additionally, ERA/PRA adjustments often incur the 'missing timeslot fee', and/or 'truck waiting time fee', which is imposed when waiting more than 1–2 free hours at the wharf gate.

As shown in Tables 4 and 5, port logistics is subject to too many uncertainties, inefficiencies, and coordination failures. Direct costs are resulted from booking cancellations, timeslot missing, double-spending, re-packing costs, and penalty fees. Indirect costs are also incurred as a result of inefficient planning of resources, fleets, and drivers. For example, due to a lack of empty containers at ECP, invalid permits, or "re-direction", trucks are being turned away, causing futile truck trips, vastly inflated costs, and inefficient job allocation for truck drivers.

Table 4. Overview of transactions in pre-carriage logistics in the status quo (developed by the author).

Transaction	Main Actor	Documents/Key Events	Uncertainty/Inefficiency Causes
Freight forwarder contract	Exporter/Importer	Cargo information and transport instructions	Paper-based contracts, communications by email/phone, middleman involvement
Freight booking order	Freight forwarder	Negotiation with the shipping line, cargo information and instruction	Communications by email/phone between freight forwarder and shipping line.
Final booking	Shipping line	Vessel allocation, determining the cut-off date and empty container number issuance, notifying the freight forwarder and ECP operator	Missing cut-off dates and cancellation from the exporter side, since customer often books more container slots or book multiple times through various shipping lines to guarantee enough space for their cargo or just comparing the prices, hence lower ship utilisation and shipping line revenue loss. Unavailability of the released empty container leads to renting the container from a third-party.
Arrangements with warehouse, packing, unpacking	Freight forwarder	Cargo information and instructions	Paper-based contracts, communications by email/phone
Submission the documents to the customs broker	Exporter/Importer	Bill of Lading, commercial invoice, packing list, packing declaration, cargo manifest, other documents (e.g., phytosanitary certificate, manufacturer's declarations, lot codes and batch numbers, fumigation certificates, costings and assist sheets, permits, certificate of origin, certificate of Analysis)	Paper-based contract, communications by email/phone, middleman involvement
Pre-departure customs declaration/ Pre-arrival delivery order	Customs broker	Submission of a summary document to Customs	Manual data entry, lack of collaboration between freight forwarders and customs broker, double data entry
Customs release	Customs broker	Digital scanning, physical inspection (1–2% of containers)	Demurrages, detention fees, missing timeslots at the wharf, the futile trips to the wharf, ECP or depot storage, unpacking or packing areas
Inland haulage contract	Freight forwarder	Transport instruction, transport charge, liability	
Port call	Ship captain	Ship schedule, port charge payment including navigation, berth hire, and cargo charges, ship berthing permit including a list of personnel on board, all non-commercial goods on board, technical certificate	Surveillance, the increasing trend of port charges

Table 5. Overview of transactions in inland haulage logistics in the status quo (developed by the author).

Transaction	Main Actor	Documents/Key Events	Uncertainty/Inefficiency Causes
Terminal timeslot booking	Trucking company	PRA number for export, and pickup container number in import, truck registration number	Multiple-spending due to bulk bookings, costs of missing timeslots (A$100–250 per slot), due to unexpected congestion/delay in haulage, wrong container packing, PRA adjustments, or long queues at the terminal gates
ERA/PRA submission	Freight forwarder	Documents informing the container arrival at the port terminal including cargo information, container number, booking number, booking timeslot	Multiple adjustments (A$125 per each amendment)
Empty container pickup arrangement	ECP operator	Daily monitoring and notifying shipping lines about stocks, notifying forklift drivers, gate out receipt issuance and emailing to carrier	Cancellations, re-keying manual entries of the container number by the truck driver, no availability of container with the specified PIN, picking up the wrong container by the transport carrier
Container release at port terminals	Port terminal inspector	Checking the container against manifest and customs declaration, notifying importer and exporter	Delay which incurs truck waiting fee, storage fee (A$100–350 per container per day), and demurrage rates
Container pickup/delivery by carrier	Trucking company	Picking or delivering the container, entering the container number in the terminal system	Re-keying manual entry of container number at the terminal gate, wrong container pick-up or the wrong container number entered in the terminal system, counterfeiting container number data and risk of security breaches with container numbers being manipulated

This is mostly the result of incompatible interfaces between actors, reliance on manual transactions, and lack of interoperability between siloed systems. For example, bilateral communication between parties occurs mostly with email communication, and only on some occasions with dedicated user interfaces. These interfaces are privately owned and managed. Accordingly, data are not often shared with governments, let alone other businesses, due to data confidentiality issues and lack of data sharing protocols. While all parties are in favour of linking up one single interface to reduce their manual work and human errors, a new trusted third party is not a viable solution in many ports, particularly in landlord ports. Landlord ports suffer from a lack of authority over freight operators which is a big challenge for integration or perhaps reengineering the logistics business processes [9]. Accordingly, freight operators have no incentive or obligation in sharing information with the port authorities. As a result, there is no efficient monitoring mechanism over the whole supply chain and logistics operations. Where there is a lack of transparency, trust, and coordination, inefficiencies hardly can be quantified and be highlighted to the involved parties. For example, as suggested in Reference [71], while it is a general knowledge that ships often operate in 90% of their capacity due to container slot cancellations, and despite the industry attention to the slot cancellation, the factors leading to cancellations have not been investigated, mainly due to lack of real data.

The Transaction Cost Economics (TCE) theory explains the governance structure of agents to attain organisational efficiency, such as transaction cost minimisation through vertical integration [72]. In TCE, a transaction is defined as the ultimate unit of activity transferring across technologically separable interfaces, possessing three dimensions of uncertainty, frequency, and asset specificity [73]. Uncertainty is defined as an event that cannot be predicted. There are various types of uncertainty, including environmental, behavioural, relational, competitive, and strategic uncertainty [74]. The concept of

asset specificity is also defined as the extent to which a party is tied in in a mutual business relationship. For example, physical asset specificity refers to the degree to which a specialised tool or IT equipment is designed for a single transaction, and human specificity refers to knowledge and experience that is required for a specific transaction. Clearly, the fragmented logistics processes and centralised IT platforms lead to higher specificity, and hence higher transaction cost. Williamson argued that asset specificity becomes an issue because of opportunism, and hence a high specificity leads to a higher transaction cost [73]. The intermediaries in the port supply chain such as customs brokers or freight forwarders increase the potential for opportunistic behaviour.

The unexpected costs such as demurrage/detention fee or terminal storage fees are often a source of many disputes over which party is ultimately liable since culpability for the delay is often unclear. Exporters and importers not only are liable for any of these unexpected costs but also must either invest in in-house specificity or contract with third parties such as freight forwarder or customs broker. Human specificity plays a vital role in the success of these industries. For example, the customs broker has a specialty in free trade agreements, concessions, duties, taxes, and GST. It is also a common knowledge that negotiation about the costs or free days is the key in this market. Hence, the information about arrangements and contracts are considered as an invaluable asset. The impact of a negotiable market and information asymmetry is ultimately borne by exporters, importers, and producers. For example, the infrastructure charges are levied by port terminals in Australia in order to recover their scaling costs, such as port rents, taxes, and council rates. However, the infrastructure charge has shown its impact to significant growth in towage rate (12.9% increase from 2018 to 2019), which is borne by exporters and importers, indicating the negotiation power of shipping lines [75].

Additionally, untruthful activities such as masquerading the information on the contracts or double spending incur extra costs of auditing and monitoring, resulting in higher transaction costs. Notably, the lack of visibility results in a lack of surveillance and compliance. On some occasions, the contents of containers are not declared correctly, either due to last-minute changes, to avoid duty, or to pay less insurance liability. For example, an accident investigation by the Marine Accident Investigation Branch in 2008 reported that about 20% of containers' manifests had less weight from the actual weight (in total 312 tonnes), and 7% had a wrong position than the declared position by the port terminals [69]. Another example is in excess of 31 million AUD of duty evasion in 2019 for smuggling tobacco and cigarettes in Australia [76].

4. The Value Proposition of Blockchain for Port Supply Chain

By and large, the issues above can be resolved by digitising, integration, and inter-organisational transaction governance. While digitalisation and integration via Electronic Data Interchange (EDI) protocols might be a solution for many of these issues, cyber-attacks always threaten the shipping and logistics industries given their vital and central role in the supply chain. Cyber-attacks to the centralised databases and IT systems paralyse the operations and cause irretrievable loss of sensitive information and financial damages to all supply chain actors. A cyber-attack on Maersk in 2017 crippled the IT infrastructures of this company for a few days, which led to 300 million USD costs to the company [76]. Another cyber-attack in 2018 on COSCO (China Ocean Shipping Company Limited) paralysed the communications between vessels, customers, and port terminals in the USA [76]. The comparison of costs and risks between blockchain, EDI, and service-oriented architectures is studied in Reference [18] for the food supply chain. The authors reiterated the advantage of blockchain in terms of reducing cyberattack threads, and the need for trust among parties and intermediaries. While in EDI, for example, one actor dominates the others and forces adoption, which ultimately leads to higher specificity and higher transaction cost.

Taking the discussions in the previous section into account, it was possible to summarise the following implications:

- Port logistics is a multi-party industry, where not all parties are trusted.
- Landlord port authorities are not trusted, and a new trusted third party is not viable.

- Several intermediaries are involved in the logistics process and hence incur higher specificity and results in higher transaction costs.
- Significant time and resources are spent in reconciling data that has been entered into multiple systems and databases.
- Tamper-proof digital recording of events and their evidences are required for monitoring, supervision, governance, and compliance analysis by the regulatory bodies.
- Transparency is partially required while immutability and encryption are essential for maintaining the confidentiality of businesses information.
- Supply chain actors are more likely geared towards technologies with lower entry barriers such as lower set up and maintaining costs.
- While the storage of data on the main network is not required, providing the visibility of transactions for all certified actors is crucial.
- Seamless administrative and financial transactions are required.
- A centralised platform not only creates another intermediary but also is subject to cybersecurity attacks.

The blockchain value proposition for port logistics is realised through the aforementioned unique specifications. Amongst many other potential drivers of value, blockchain resolves coordination failures that arise as a consequence of asymmetric information in such a fragmented and untrusted market. The distributed structure and the complex cryptographic verification make it nearly impossible to alter the state of the transaction fraudulently. Hence, some of the shortcomings of the current IT systems could be overcome by effectively digitising all transactions and providing sharing, accessibility, and readability protocols. For example, the Port of Antwerp tested a blockchain pilot project for the container release, whereby container PINs are generated and saved on a blockchain network, making it impossible to counterfeit.

Blockchain can also overcome disputes over unexpected costs and business complexities by achieving true tamper resistance of data, guaranteeing no collusion between business partners, no tampering with data or transactions, and no capacity to unilaterally alter business rules. As such, smart contracts can be securely executed if pre-specified conditions are met. Not only can a smart contract solve the inter-agent lack of trust, but it also reduces human error. Accordingly, operators see the advantages of an integrated marketplace, compared with dealing with multiple parties with different platforms and business structures. It not only removes the dependency on the other authorities and intermediaries by the disintermediation but also reduces the likelihood of hacking threats and cyberattacks [18].

Following the conceptualisation suggested in Reference [77], the value proposition of a blockchain-based PCS platform is assessed within four central dimensions: the Who, the What, the How, and the Value (Table 6). The first dimension 'Who' identifies the target customer or stakeholder. This dimension consists of all agents involved in the maritime supply chain either directly or indirectly. The 'What' dimension describes the value proposition, or in other words, what is offered via blockchain. The 'How' represents how several processes and activities must be mastered to generate and distribute the value proposition. The 'Value' dimension explains why blockchain is financially viable and how it relates to the revenue model.

Table 6. Implications of blockchain-based PCS business models, developed by the author based on the St. Gallen conceptual model [77].

What: Value Proposition	How: Potential Opportunity with Blockchain	Value: Implications
Track and traceability: Lack of traceability of contracts, carriers (trucks and containers), and shipments in the status quo results in manipulation and masquerading of crucial information, leading to higher monitoring and auditing costs.	Blockchain keeps track of all business events (transactions executed) and the associated details in the event's lifecycle such as timestamp, new asset creation, and asset state modification.	Provenance
Visibility and transparency: Lack of transparency adds complexity to the management where freight actors have no monitoring power over their resources when they are outside their premises. It is one of the key drivers of coordination failures and lower productivity due to lack of an accurate, real-time picture of container/truck, demand signals and supplier inventory levels (e.g., idle truck fleets, drivers, empty containers, storage capacity). Inefficiencies and uncertainties impose extra costs, and in the status quo, the supply chain actors consider these costs as "the cost of doing business" such as low truck utilisation, idle fleets, slots cancellation, and empty running of trucks.	The unimpeded flow of information provided by blockchain contributes to more efficient functionality and liability. All information on pricing and other aspects are continuously and instantaneously updated, hence facilitating pre-planning and creating a transparent market. The dynamic planning capabilities of the logistics service providers will be enhanced. Turnaround times, on-time delivery failures, and the costs of doing business will be reduced.	Efficiency and productivity at firm-level
Interoperability, coordination, and integration: In the status quo, every freight operator has its own management platform and dataset, with the limited interconnection capability. Freight operators are operating as silos with a limited sense of common purpose and impacts of each element on the overall performance of the supply chain. Container supply chain information is dispersed and needs to be able to be coalesced to facilitate planning and operations. Due to a lack of understanding of the capacity of the entire maritime supply chain, it is extremely difficult to know where the capacity constraints are likely to emerge and how they should be addressed.	Freight actors can securely share their information with their business partners across the supply chain to drive productivity through a trusted and possibly a multi-level data access architecture. Data on interoperability will enhance the ability of policymakers to coordinate across the system and relieve the points of highest friction in the system. The integration also enables providing optimised logistics solution (e.g., truck-sharing, back-loading, and empty container repositioning).	Efficiency and productivity at the system level
Disintermediation and reduced payment reconciliation time and cost: The majority of transactions in the port logistics are performed manually either by email or phone calls, resulting in human errors, double-booking, double-spending or pick up/delivery of a wrong shipment. There are several intermediaries (e.g., customs broker and freight forwarding company) involved in the process which incur extra costs.	The validation mechanism of blockchain prevents data discrepancies because transaction metadata should match to the previous linked block when passing through multiple supply chain actors. Smart contracts, instantaneous settlement and real-time processing reduce settlement, penalty fees, and human mistakes. History of immutable transactions removes the cost of settling disputes over co-ordination failures and unexpected delays and expenses. By tokenising, payments can be seamlessly transferred across the international trade parties without incurring an exchange rate.	Lowering business costs

Table 6. *Cont.*

What: Value Proposition	How: Potential Opportunity with Blockchain	Value: Implications
Risk mitigation in contractual, legal, and regulatory aspects of the trade: In the status quo, lack of information sharing protocol is the main barrier for compliance directives related to trade practices, environmental mandates, customs, legal and regulatory purposes. Cybersecurity attacks to granular IT infrastructure, data manipulation, masquerading the real information on the contracts, bill of lading, and customs declaration documents are common problems in the status quo.	The blockchain contains a complete history of every data manipulation and transactions. The transactions also contain metadata essential for compliance analysis and audit such as the identity of node, the identity of validator, the timestamp and exchanged monetary values. The distributed structure of database minimises the risk of cyberattacks.	Compliance, governance, and increasing security
Enabling trust: In the status quo, revealing sensitive business information is the main barrier for data sharing. Additionally, lack of a trustable and unique source of proof often leads to disputes over the accountability of freight actors for unexpected costs, losses, and delays.	Distributed confidentiality mechanism of blockchain enables data integration without a need for trust. Timely detection of any attempt to manipulate or compromise the booking system will reinforce trust in the platforms. Encryption of transaction metadata and secure identity management protocols remove entry barriers and lead to a greater willingness to use, compared to centralised systems.	Lowering auditing and monitoring costs Creating Co-innovation (Co-innovation refers to activities to build new knowledge and create opportunities for cooperation among participants [8]).

5. Architectural Design Requirements of a Blockchain-Based PCS Platform

An industry stakeholder consultation, involving various trade parties, was undertaken to outline the most important platform requirements, including minimum performance requirements for a PCS in terms of read/write latency and throughput. The results of the industry stakeholder engagement and the review of blockchain design components in Section 2 outlined five suggestive architectural design requirements in the context of PCS architecture, as follows:

5.1. Requirement 1: Lowering Entry Barrier, Creating Trust among Fragmented and Untrusted Actors

The supply chain actors are more likely geared towards technologies with lower entry barriers such as lower set up and maintaining costs. Using a private blockchain instead of a public blockchain may allow greater control over the admittance of processing nodes and transactions into the system but also increases entry barriers and thus partly reduces some of the benefits of using a blockchain. Particularly, it is risky when it is predicted that the public blockchains will provide connectivity in the future similar to the internet these days. It is believed that the future of public blockchain is similar to the Internet where all blockchain applications will be connected. Accordingly, the capability of public chain compatibility will be of utmost importance.

It seems that a permissioned public blockchain is preferred in the PCS architecture, where better performance is required while the core functionality of blockchains is also maintained, including creating trust among untrusted parties, less asset specificity, and removing middlemen. Accordingly, data in the platform will be deemed to be owned by its creator and the data owner can define who will be able to access to their data, but simultaneously, users should have access to proof that the base data they are relying on has not been altered since its source.

➢ Suggestion 1: Deploying permissioned public blockchain, in which transactions are fully transparent to the pre-specified parties and partially transparent to all involved actors, yet fully traceable on the public network.

5.2. Requirement 2: Enabling Interoperability

The inter-chain interoperability is a key criterion for PCS platforms. Interoperability relates to communication between various blockchain platforms, or between two instances of the same platform, or between two sidechains within the same platform. The interoperability is an important specification for ensuring the viability of the product, mainly because it is expected that some freight actors develop their own blockchain.

Private sidechain channels are also foreseen in the architecture of the platform to provide privacy for specific subsets of network members. In a private sidechain, the data for transactions on that channel is invisible to members that are not granted access. Due to the dynamic nature of the international trade market, there is also a need to provide a flexible platform that provides easy access for the new trade participants. The bootstrapping method, such as the mechanism suggested in Reference [67], enables adding a new participant to the network without a need for setting up a new channel by a third-party. A blockchain-based PCS should augment (via APIs) rather than replace the existing operational systems developed by different supply chain actors.

➢ Suggestion 2: Enabling private sidechain interoperability, employing bootstrapping method and API interaction with the existing non-blockchain operating systems to lower the entry barrier (e.g., Ethereum Layer 2 protocols).

5.3. Requirement 3: Near Seamless Administrative and Financial Transactions and Validation

Undoubtedly, a PCS architecture should be capable of handling thousands of concurrent transactions per hour, which are submitted from multiple participants. The preliminary consultation with different trade parties outlined 10 s and 30 min for read and write latency on the public network, respectively. In the private sidechains, these values are expected to be 1 and 5 s for the read and write latency, respectively.

In order to increase the throughput and read and write latency, computationally heavy validation algorithms will not be applicable for this specific use-case. The initial assessment of consensus mechanisms suggests that the ZPK and IBFT seem to be the most preferred protocols. However, no inevitable conclusion can be made until there is a more detailed comparative analysis, at least in a simulation setting.

➢ Suggestion 3: Permissioned public blockchain with an IBFT or ZPK consensus mechanism can support the latency and throughput requirements of a PCS.

5.4. Requirement 4: Vast Range of Roles and Responsibilities

In the envisaged platform, any organisation with a verifiable role in the maritime transportation and supply chain should be able to participate. However, transactions and participants could be treated differently. For example, an account which is permitted to submit a transaction to update the state of a contract should not necessarily be able to submit a transaction which deploys a new contract.

➢ Suggestion 4: Pre-identified roles of each node.

5.5. Requirement 5: Large-Scale Nature of Transaction Data

Currently, in most public blockchain protocols, each node stores all states (i.e., account balances or contract code) and processes all transactions. This mechanism provides a high level of security but greatly limits scalability. Considering the massive number of transactions for supply chain and logistics application, and the fact that transactions in blockchain will stay forever, after a while, the network will experience congestion at times, and the scaling problem may arise. This necessitates deploying new methods to overcome the scalability limitations, such as artificially aborting transactions by superseding them with an idempotent or counteracting transaction [78]. Clearly, due to the limited size of the data store provided by blockchain, an off-chain data storage is necessary for a PCS platform.

Furthermore, encrypting data before storing it on a blockchain may increase confidentiality, but will reduce performance, and may harm transparency or independent auditing processes. On the other hand, storing only a hash of data on-chain and keeping the contents off-chain will improve confidentiality and may improve performance, but partly undermines the distinctive benefit of blockchains in providing distributed trust. This may create a single point of failure, reducing system availability and reliability. Hence, support for the level of encryption must be specifically investigated ahead of time.

➢ Suggestion 5: *Enabling off-chain data storage and off-chain data encryption*.

6. Future Research Agenda

In this paper, many of the research questions raised by Tönnissen and Teuteberg [36] were answered in the context of port logistics. There are a few other studies that have outlined a number of research propositions. Saberi et al. [25] identified seven post-implementation research agenda focusing on the potential outcomes from blockchain implementation in the supply chain, which are still understudied. Wang et al. [10] suggested six future research agenda, some of which are still unexplored. Our survey of existing research on blockchain application and maritime supply chain also identifies a research agenda in six primary directions, as follows.

6.1. Model-Driven Engineering

Model-driven engineering is translating the business process into the design and testing the platform at various abstraction levels and different stages of platform development. Model-driven engineering is not only independent of a specified platform but is also easier to understand and verify than codes. This can be particularly useful for communicating with industry partners about smart contracts and strengthening confidence in that code from all stakeholders. Many studies have presented model-driven engineering for blockchain platforms in general [78–82]. To the best of the author's knowledge, there are only two qualitative studies looking at the reengineering of the business process of blockchain in the supply chain [17,19]. Hence, a more detailed analysis is required to identify and define the corresponding limitations and trade-offs. A simulation would need to be set up at the real-size scale taking the nature of freight actors, the database, and market structure into account. This simulation will cast light upon specification requirements, including throughput (of transactions), scalability, transaction cost, and interoperability. The outcome can progress the assessment of new and improved platforms and be tailored to meet the identified requirements of the PCS.

6.2. Benchmarking the Blockchain Performance

Generally, an inability to predict overall performance is one of the main challenges of blockchain technology [46]. However, architectural models can be employed to benchmark the performance of blockchain before and during development stages. The majority of performance metrics presented in the academic literature are limited to running laboratory experiments on proof of concept projects [57]. Future research is required to focus on the performance benchmarking of port logistics by developing architectural models.

Architectural models are either developed by analytical solvers or simulation engines. These models are two-fold including analytical performance models (e.g., Petri Nets Queueing networks and layered queueing networks), and architecture-level performance models that can be either simulated or converted to analytical models (e.g., Palladio Component model, UML profile, and Descartes modelling language). Virtual machines such as go-Ethereum (Geth) can also be deployed to mimic practical deployment to some degree. The importance of testing read/write latency is that a wide range of architectural alternatives can be analysed. Some of these decisions are about blockchain-specific issues, such as inter-block time or the number of confirmation blocks. Other design

decisions, such as possible business process changes, are system-level design options but are impacted by latency arising from the blockchain-related factors [46].

6.3. Building Standards and Interoperability Protocols

A protocol is a standard language that lets a group of people work together on a specific problem. The first IT protocol was created in 1973 when different intranet networks realised that they could adopt a unified internetwork protocol to expand their service. Later, other protocols were developed such as Hypertext Transfer Protocol (HTTP) (i.e., protocol defining how information is transmitted over the web), Simple Mail Transfer Protocol (SMTP) (i.e., protocol for email app for sending and receiving email), and Secure Sockets Layer (SSL) (i.e., protocol of a browser for a secure data transfer). Interoperability is a protocol's capacity to interact and cooperate with different blockchains and to facilitate smart contracts between one protocol and another. Currently, blockchain suffers from a lack of standard protocols to link different blockchains, instead of creating a new larger blockchain. This lack of open standards and protocols may encourage companies to develop their own blockchain system without being designed for interoperability and positioning it among a myriad of systems involved in the port supply chain. Currently, various ports, shipping lines, and container terminals are currently developing their own blockchain platforms. Hence, it is expected that standards and interoperability protocols are required to leave everyone on their blockchain and just connect them to the rest of the ecosystem. These standards and protocols allow supply chain actors to minimise the disclosure of proprietary information while providing interoperability among other blockchain-based systems, such as another international ports. A combined desktop and interview study in Reference [83] revealed the importance of standardisation and regulations. Another area to investigate is the indicative level of standardisation needed to support the use of blockchain in port logistics. Consideration could be made of work underway in the international context to enabling interoperability among various blockchain platforms.

6.4. Blockchain Technology Adoption in the Port Supply Chain Industry

The adoption of new technology is often curtailed by a lack of appropriate IT capabilities within the traditional freight companies, and also lack of interoperability between supply chain actors. The literature is not devoid of technology adoption studies. There are a few studies reporting the expert opinions and providing first-hand insights into the blockchain adoption in the port logistics industry (see, e.g., References [35,37]). These studies indicate some of the barriers of blockchain adoption, such as privacy of information, lack of digitalisation in logistics companies, and lack of blockchain technology readiness [35].

There are also a handful of papers experimenting the technology adoption theories on case studies. Johnson [38] studied the theoretical relationship between organisational learning and blockchain through a qualitative case study approach and semi-structured interviews. Francisco and Swanson [37] used the technology innovation adoption concept or so-called the Unified Theory of Acceptance and Use of Technology to study the application of blockchain for supply chain traceability. Dobrovnik et al. [16] categorised blockchain applications based on multiple transformation phases and identified the potential blockchain applications in logistics based on the Diffusion of Innovation theory and the associated attributes of innovation framework which comprises relative advantage, compatibility, complexity, trialability, and observability. Verhoeven et al. [31] undertook a multiple case study approach on five applications selected based on five organisation objectives, namely smart contracts, business-to-business traceability, business-to-customer traceability, data transfer, and payment. Each selected case was reviewed according to five technology adoption principles, namely 'engagement with the technology', 'technological novelty-seeking', 'awareness of local context', 'cognisance of alternative technologies', and 'anticipation of technology alteration'.

Nevertheless, one future research inquiry concerns investigating the duration of the adoption cycle, and the degree to which blockchain is effectively integrated into the freight operator's systems.

These are dependent upon the experience gained from the adoption of like technologies such as Electronic Data Interchange (EDI) with particular reference to the frequency of these experiences and the complexity of the technology—indicating their technology readiness. As blockchain seeks to communicate and integrate across organisational boundaries, the complexity of the adoption process and the associated coordination costs and potential for opportunistic behaviour that can damage the adoption process are heightened.

6.5. Usability

Usability is defined as the ability of the platform to be easily usable by end-users as well as developers. Ease-of-use is extremely important for freight actors who do not necessarily possess IT skills. If properly designed, the end-users might not even get to know that they are using blockchain. Usability is supplied by a few other components working alongside the blockchain network, as depicted in Figure 6.

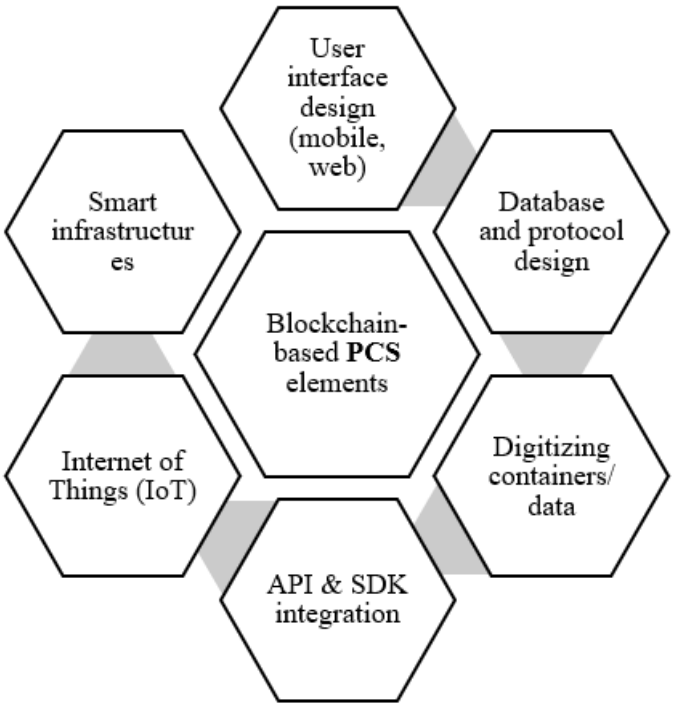

Figure 6. Blockchain-based PCS design components.

User interface design includes designing a mobile app or web portal to enable freight agents to transact and track their asset and data. Database design, similar to any Enterprise Resource Planning (ERP) system, allows interacting with APIs and smart contracts of external organisations. IoT design concerns automatic tracking of the physical movements of assets and containers across the supply chain and updating the chain of custody and other complementary decisions based on real-time sensor data (e.g., tracking shipment conditions such as geospatial data, temperature, humidity, etc.). APIs allow clients and applications to interact with the blockchain, and Software Development Kits (SDKs) provide mechanisms to deploy and execute transactions, query blocks, and monitor events on the blockchain. As the blockchain technology progress, platform providers develop data visualisation and analytics tools for on-chain data [84,85]. Nevertheless, usability and the ability to use analytic tools on blockchain transactions are understudied in the literature.

6.6. Regulatory Challenges

The emergence and application of blockchain technology clearly challenge existing public regulatory frameworks [10]. Future research should examine how blockchain minimises transactional

legal risk in both national and international shipping law. It is particularly important to investigate how shipping law could be made amenable to incorporation into smart contracts. Since blockchain is codifying already extant rules and norms, it should be capable of working with different rule-based systems. However, there are debates on how smart contracts are interpreted by arbitrators and courts. Most blockchain legal activity has taken place around the cryptocurrency aspects, rather than contracts themselves. Immutable and unchangeable smart contracts could create problems where there is mistake, fraud, negligence, misrepresentation, and the like. Could smart contracts be made voidable, how would rescission operate? As yet, these questions are relatively untested in maritime logistics.

7. Conclusions

Blockchain characteristics are believed to assist a business structure such as port supply chain that involves many parties requiring trust, transparency, as well as efficiency in inter-party transactions, contracting, and data management. The emergence of this technology as the next generation of PCS platforms is predicted to transform business operations dramatically. Therefore, it is important to consider the rationale for embracing it as there are many questions that need to be answered as this technology progresses. Most importantly, while most articles are talking solely in favour of this technology, the barriers and challenges, either financial or technical, should not be underestimated.

In this paper, the value propositions of blockchain technology were assessed. The results of this assessment reconfirmed the potential of blockchain to lower the transaction costs, boost the service quality and transaction governance, and consequently improve the organisation and the entire supply chain competitiveness. The distributed and encrypted data structure of blockchain, provision of smart contract without human intervention, and no need for a central authority as the controlling agent are advantages of a blockchain-based PCS in landlord ports.

An essential aspect of this research was to investigate the existing blockchain platforms at a technical level and to cut through the 'marketing hype' which often makes unrealistic and unsubstantiated claims regarding the features and functionality of some of the available and emerging blockchain platforms. Confirmed also by the previous studies [2,83], despite the importance of blockchain on the maritime shipping and port logistics, the published papers are limited to discussing generalities of this technology, and the practical details are far from being clarified. The literature in the domain of logistics is also devoid of technical review of the architectural design of blockchain-based platforms. As suggested in Reference [83], the industry sources also suffer from a polarizing issue, where Tradelens—a Maersk–IBM joint venture—is introduced as the industry leader.

This paper addresses this gap by taking the first step to analyse the extant currently available blockchain platforms against the identified requirements for the port logistics use-case by answering two salient research questions. A detailed survey was conducted among currently available blockchain platforms suitable for the port logistics to address these research questions.

This paper offered a thorough survey of the advantages and limitations of a wide range of available consensus algorithms and various architectural choices. The results of this technical review highlight that there are considerations that should be taken into account to custom design a platform to PCS specifications. Availability—the readiness for correct service, and reliability—the continuity of correct service, are heavily reliant on the right choice being made for blockchain design for such a complex use case. A preliminary comparative analysis among different decentralisation level in this paper suggested that a permissioned public blockchain offers the best trade-off in performance measures for this use-case.

As a result of this survey, a number of necessary platform requirements were outlined for a blockchain-based PCS, including private sidechains, modular design with inter-chain interoperability, and encrypted off-chain data storage mechanisms. The results of this critical review reiterate that these properties are not summed up in one platform [48]. Hence, an uncritical adoption of an existing platform is not advised. This conclusion highlights the importance of close collaboration between the port authorities, freight operators, and blockchain platform developers to drive forward

standards and protocols which will, in turn, maximise value propositions of this technology for this specific use-case.

Notably, the performance measures of various blockchain pilot projects in port supply chain have not been officially reported yet. Hence, it imposes a limitation on comparing the performance of these different platforms. This research can be extended by simulating and benchmarking the key performance measures, as well as a multi-disciplinary perspective in the design of a platform. Accordingly, a few research agenda were outlined for the future extension of this work. More importantly, there remained several unanswered critical questions that may even change the suggestive design requirements proposed in this paper. The author suspects these questions are fundamental barriers that have lagged the development of a blockchain-based PCS in practice, and perhaps should be answered in designing national and international roadmaps. These questions are as follows:

- Should a blockchain-based PCS be developed from bottom-up by individual ports or from the top by a multinational and a third-party entity?
- How will the costs of developing a platform be incurred by ports or companies?
- If each port has its PCS with a specific architecture, will this not constitute a barrier of costs to the entry of new companies in the supply chain and to free competition?
- Each PCS and public entity in port logistics has different information requirements in the ship and cargo processes. How will the integration task take place at the international level, to allow a true integration of the PCS in blockchain logistics chains, without losing the independence of each country and the possibility of requiring the documentation they want?
- Given that the future of integrated trade market is envisaged via interoperable blockchain-based PCSs, how can each individual solution be accepted by multinational companies?

Funding: This research received no external funding.

Acknowledgments: The author acknowledges the support provided by the Port of Brisbane Ltd. Pty., as part of the University of Queensland–Port of Brisbane Research Partnership.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Using the notations of Ethereum [45], this appendix explains the PoW consensus mechanism and clarifies the reasons that this algorithm is computationally heavy. PoW involves choosing pseudo-random slices of the dataset, d, and cryptographically hashing them together, or so-called mix-hash, H_m. These slices, however, are selected only based on the block header, H, and the number of transactions (without the mix-hash). Accordingly, PoW evaluates to an array of $(n, m) = \text{PoW}(H, d)$. The block finalisation, therefore, should satisfy the following conditions:

$$n \leq \frac{2^{256}}{H_d} \quad \wedge \quad m = H_m \quad \wedge \quad H_s > P(H)_{H_s} \quad \wedge \quad H_i = P(H)_{H_i} + 1 \tag{A1}$$

where H_s is a scalar value corresponding to the timestamp, $P(H)_{H_s}$ is a scalar value corresponding to the timestamp of parent's block, H_i is the number of ancestor blocks (for the genesis block $H_i = 0$), and n is the number of transactions sent from a given address, or so-called nonce, and is increasing by one at every time the sender sends a transaction. The nonce is used to enforce the valid transactions and therefore is dependent on block header difficulty, H_d.

This mechanism of block validity is the foundation of security and integrity of a public blockchain, because the nonce, n, must meet the conditions and conditions depend on the block's contents, which itself is made from a collated list of transactions. In PoW, the difficulty of finding a solution to

Equation (A1) is proportional to the difficulty of block H_d. Accordingly, the difficulty of a block header, H_d, is defined as:

$$H_d \equiv \max\left(H_{d_0}, \left(P(H)_{H_d} + \left[\frac{P(H)_{H_d}}{2048}\right] \times \varsigma + \varepsilon\right)\right) \tag{A2}$$

where H_{d_0} is the difficulty of the genesis block, defined as 131,072. $P(H)_{H_d}$ is a scalar value corresponding to the difficulty of the parent's block. The parameter ς is used to affect dynamic homeostasis of time between blocks, as shown in Equation (A3):

$$\varsigma \equiv \max\left(\left[y - \frac{H_s - P(H)_{H_s}}{9}\right], -99\right) \text{ where } y \equiv \begin{cases} 1 & \text{for the sec ond block} \\ 2 & \text{otherwise} \end{cases} \tag{A3}$$

The difficulty exponentially increases by adding the parameter ε and as a result, the block time difference will be increased, as shown in Equation (A4). However, to avoid freezing up the network, the difficulty is scaled down by subtracting a big number (e.g., three million) from the ancestor block number H_i. As ε decreases, the time differences between blocks are reduced.

$$\varepsilon \equiv 2^{[\max(H_i - 3{,}000{,}000, \quad 0)/100{,}000] - 2} \tag{A4}$$

This mechanism enforces an increase in the difficulty level for the smaller period between the last two blocks, which avoid forking of blocks.

References

1. Babica, V.; Sceulovs, D.; Rustenova, E. Digitalization in Maritime Industry: Prospects and Pitfalls. In *ICTE in Transportation and Logistics 2019*; Ginteres, E., Ruiz, E.M., Piera, E.M., Eds.; Springer: Cham, Switzerland, 2019; pp. 20–27.
2. Moros-Daza, A.; Amaya-Mier, R.; Paternina-Arboleda, C. Port Community Systems: A structured literature review. *Transp. Res. Part A Policy Pract.* **2020**, *133*, 27–46. [CrossRef]
3. Carlan, V.; Sys, C.; Vanelslander, T. How port community systems can contribute to port competitiveness: Developing a cost–benefit framework. *Res. Transp. Bus. Manag.* **2016**, *19*, 51–64. [CrossRef]
4. Irannezhad, E.; Prato, C.G.; Hickman, M. An intelligent decision support system prototype for hinterland port logistics. *Decis. Support Syst.* **2020**, *130*, 113227. [CrossRef]
5. Caldeirinha, V.; Felício, J.A.; Salvador, A.S.; Nabais, J.L.; Pinho, T. The impact of port community systems (PCS) characteristics on performance. *Res. Transp. Econ.* **2020**, *80*, 100818. [CrossRef]
6. Irannezhad, E.; Hickman, M.; Prato, C.G. Modeling the Efficiency of a Port Community System as an Agent-based Process. *Procedia Comput. Sci.* **2017**, *109*, 917–922. [CrossRef]
7. Jacobsson, S.; Arnäs, P.O.; Stefansson, G. Automatic information exchange between interoperable information systems: Potential improvement of access management in a seaport terminal. *Res. Transp. Bus. Manag.* **2020**, 100429. [CrossRef]
8. Carlan, V.; Sys, C.; Calatayud, A.; Vanelslander, T. *Digital Innovation in Maritime Supply Chains*; IDB Inter-American Development Bank: Washington, DC, USA, 2018.
9. Verhoeven, P. A review of port authority functions: Towards a renaissance? *Marit. Policy Manag.* **2010**, *37*, 247–270. [CrossRef]
10. Wang, Y.; Han, J.H.; Beynon-Davies, P. Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Manag. Int. J.* **2019**, *24*, 62–84. [CrossRef]
11. Yang, C.-S. Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use. *Transp. Res. Part E Logist. Transp. Rev.* **2019**, *131*, 108–117. [CrossRef]
12. Greenspan, G. Avoiding the Pointless Blockchain Project 2015. Available online: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/ (accessed on 22 November 2015).
13. Suichies, B. Why Blockchain Must Die in 2016. Available online: https://medium.com/@bsuichies/why-blockchain-must-die-in-2016-e992774c03b4 (accessed on 22 December 2015).

14. Li, X.; Wang, F.; Zou, X. Current Situation and Trend of Research on Application of Blockchain Technology in Logistics Field. In Proceedings of the 5th International Conference on Economics, Business, Finance, and Management (ICEBFM 2019), Shenzhen, China, 6–8 June 2019.
15. Miau, S.; Yang, J.-M. Bibliometrics-based evaluation of the Blockchain research trend: 2008–March 2017. *Technol. Anal. Strat. Manag.* **2018**, *30*, 1029–1045. [CrossRef]
16. Dobrovnik, M.; Herold, D.M.; Fürst, E.W.M.; Kummer, S. Blockchain for and in Logistics: What to Adopt and Where to Start. *Logistics* **2018**, *2*, 18. [CrossRef]
17. Chang, S.E.; Chen, Y.-C.; Lu, M.-F. Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technol. Forecast. Soc. Chang.* **2019**, *144*, 1–11. [CrossRef]
18. Kumar, A.; Liu, R.; Shan, Z. Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities. *Decis. Sci.* **2019**, *51*, 8–37. [CrossRef]
19. Pundir, A.K.; Jagannath, J.D.; Chakraborty, M.; Ganpathy, L. Technology Integration for Improved Performance: A Case Study in Digitization of Supply Chain with Integration of Internet of Things and Blockchain Technology. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 0170–0176.
20. Chen, S.; Yan, J.; Tan, B.; Liu, X.; Li, Y. Processes and challenges for the adoption of blockchain technology in food supply chains: A thematic analysis. In Proceedings of the iConference 2019, Washington, DC, USA, 31 March–3 April 2019.
21. Choi, T.-M.; Wen, X.; Sun, X.; Chung, S.-H. The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era. *Transp. Res. Part E Logist. Transp. Rev.* **2019**, *127*, 178–191. [CrossRef]
22. Hughes, L.; Dwivedi, Y.K.; Misra, S.K.; Rana, N.P.; Raghavan, V.; Akella, V. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *Int. J. Inf. Manag.* **2019**, *49*, 114–129. [CrossRef]
23. Min, H. Blockchain technology for enhancing supply chain resilience. *Bus. Horiz.* **2019**, *62*, 35–45. [CrossRef]
24. Morkunas, V.J.; Paschen, J.; Boon, E. How blockchain technologies impact your business model. *Bus. Horiz.* **2019**, *62*, 295–306. [CrossRef]
25. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2018**, *57*, 2117–2135. [CrossRef]
26. Tijan, E.; Aksentijević, S.; Ivanić, K.; Jardas, M. Blockchain Technology Implementation in Logistics. *Sustainability* **2019**, *11*, 1185. [CrossRef]
27. Dolgui, A.; Ivanov, D.; Potryasaev, S.; Sokolov, B.; Ivanova, M.; Werner, F. Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *Int. J. Prod. Res.* **2019**, *58*, 2184–2199. [CrossRef]
28. Hofman, W.; Brewster, C. The Applicability of Blockchain Technology in the Mobility and Logistics Domain. In *Towards User-Centric Transport in Europe: Challenges, Solutions and Collaborations*; Müller, B., Meyer, G., Eds.; Springer International Publishing: Cham, Switzerland, 2019.
29. Longo, F.; Nicoletti, L.; Padovano, A.; D'Atri, G.; Forte, M. Blockchain-enabled supply chain: An experimental study. *Comput. Ind. Eng.* **2019**, *136*, 57–69. [CrossRef]
30. Wen, Q.; Gao, Y.; Chen, Z.; Wu, D. A Blockchain-based Data Sharing Scheme in The Supply Chain by IIoT. In Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, 6–9 May 2019; pp. 695–700.
31. Verhoeven, P.; Sinn, F.; Herden, T.T. Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology. *Logistics* **2018**, *2*, 20. [CrossRef]
32. Azzi, R.; Chamoun, R.K.; Sokhn, M. The power of a blockchain-based supply chain. *Comput. Ind. Eng.* **2019**, *135*, 582–592. [CrossRef]
33. Behnke, K.; Janssen, M. Boundary conditions for traceability in food supply chains using blockchain technology. *Int. J. Inf. Manag.* **2020**, *52*, 101969. [CrossRef]
34. Blossey, G.; Eisenhardt, J.; Hahn, G. Blockchain Technology in Supply Chain Management: An Application Perspective. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA, 8–11 January 2019.
35. Hackius, N.; Reimers, S.; Kersten, W. *The Privacy Barrier for Blockchain in Logistics: First Lessons from the Port of Hamburg; Logistics Management*; Springer: Cham, Switzerland, 2019.

36. Tönnissen, S.; Teuteberg, F. Analysing the impact of blockchain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies. *Int. J. Inf. Manag.* **2020**, *52*, 101953. [CrossRef]
37. Francisco, K.; Swanson, D. The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. *Logistics* **2018**, *2*, 2. [CrossRef]
38. Johnson, V. Organizational Learning through Disruptive Digital Innovation. A Blockchain Implementation. Master's Thesis, Georgia State University, Atlanta, GA, USA, May 2019.
39. Kamble, S.S.; Gunasekaran, A.; Sharma, R. Modeling the blockchain enabled traceability in agriculture supply chain. *Int. J. Inf. Manag.* **2020**, *52*, 101967. [CrossRef]
40. Queiroz, M.M.; Wamba, S.F. Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *Int. J. Inf. Manag.* **2019**, *46*, 70–82. [CrossRef]
41. Saberi, S.; Kouhizadeh, M.; Sarkis, J. Blockchains and the Supply Chain: Findings from a Broad Study of Practitioners. *IEEE Eng. Manag. Rev.* **2019**, *47*, 95–103. [CrossRef]
42. Wang, Y.; Singgih, M.; Wang, J.; Rit, M. Making sense of blockchain technology: How will it transform supply chains? *Int. J. Prod. Econ.* **2019**, *211*, 221–236. [CrossRef]
43. Xu, X.; Weber, I.; Staples, M.; Zhu, L.; Bosch, J.; Bass, L.; Pautasso, C.; Rimba, P. A Taxonomy of Blockchain-Based Systems for Architecture Design. In Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3–7 April 2017; pp. 243–252.
44. Bashir, I. *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*; Packt Publishing Ltd.: Birmingham, UK, 2018.
45. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger; Ethereum Project Yellow Paper. 2019. Available online: https://scholar.google.com.hk/scholar?hl=zh-CN&as_sdt=0%2C5&q=Ethereum%3A+A+Secure+Decentralised+Generalised+Transaction+Ledger&btnG= (accessed on 12 October 2020).
46. Xu, X.; Weber, I.; Staples, M. *Architecture for Blockchain Applications*; Springer Science and Business Media LLC: Cham, Switzerland, 2019.
47. Mingxiao, D.; Xiaofeng, M.; Zhe, Z.; Xiangwei, W.; Qijun, C. A review on consensus algorithm of blockchain. In Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 2567–2572.
48. Zhang, S.; Lee, J.-H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2020**, *6*, 93–97. [CrossRef]
49. Bach, L.M.; Mihaljevic, B.; Zagar, M. Comparative analysis of blockchain consensus algorithms. In Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; pp. 1545–1550.
50. Ernst & Young. Total Cost of Ownership for Blockchain Solutions. 2019. Available online: https://github.com/EYBlockchain/fundamental-cost-of-ownership/blob/master/EY%20Total%20Cost%20of%20Ownership%20for%20Blockchain%20Solutions.pdf (accessed on 8 November 2020).
51. Szabo, N. Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*. [CrossRef]
52. Staples, M.; Chen, S.; Falamaki, S.; Ponomarev, A.; Rimba, P.; Tran, A.; Weber, I.; Xu, X.; Zhu, J. *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*; Csiro: Sydney, Australia, 2017.
53. Pinna, A.; Ibba, S.; Baralla, G.; Tonelli, R.; Marchesi, M. A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics. *IEEE Access* **2019**, *7*, 78194–78213. [CrossRef]
54. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. Available online: https://pdfs.semanticscholar.org/1b23/cd2050d5000c05e1da3c9997b308ad5b7903.pdf?_ga=2.40853538.1220751227.1604802457-1483863585.1604802457 (accessed on 8 November 2020).
55. Robinson, P. Requirements for Ethereum Private Sidechains. Available online: https://arxiv.org/abs/1806.09834 (accessed on 8 November 2020).
56. Rimba, P.; Tran, A.B.; Weber, I.; Staples, M.; Ponomarev, A.; Xu, X. Comparing Blockchain and Cloud Services for Business Process Execution. In Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA), Goethenburg, Sweden, 3–7 April 2017; pp. 257–260.
57. Gonczol, P.; Katsikouli, P.; Herskind, L.; Dragoni, N. Blockchain Implementations and Use Cases for Supply Chains-A Survey. *IEEE Access* **2020**, *8*, 11856–11871. [CrossRef]

58. Warren, W.; Bandeali, A. 0x: An Open Protocol for Decentralized Exchange on the Ethereum Blockchain. 2017. Available online: https://0x.org/pdfs/0x_white_paper.pdf (accessed on 8 November 2020).
59. Poon, J.; Buterin, V. Plasma: Scalable Autonomous Smart Contracts. *White Pap.* **2017**, *206*, 1–47.
60. Khalil, R.; Gervais, A. Revive: Rebalancing Off-Blockchain Payment Networks. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 439–453.
61. CBH Group Agridigital. Solving for Supply Chain Inefficiencies and Risks with Blockchain in Agriculture. Available online: https://assets.website-files.com/5acb6c048451816da066ad80/5af2a0068f5865bb84d047ff_AgriDigital%20CBH%20Blockchain%20White%20Paper%20Final.pdf (accessed on 8 November 2020).
62. Gleim, B.; Bertani, T.; Cabelguen, J.-C.; Towne, B.; Von Kohorn, D.; Polzer, G. Enterprise Ethereum Alliance Off-Chain Trusted Compute Specification V1.0. *Enterp. Ethereum Alliance* **2019**. Available online: https://entethalliance.org/wp-content/uploads/2019/05/EEA_Off_Chain_Trusted_Compute_Specification_V0_5.pdf (accessed on 8 November 2020).
63. Sousa, J.; Bessani, A.; Vukolic, M. A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. In Proceedings of the 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Luxembourg, 25–28 June 2018; pp. 51–58.
64. Thakkar, P.; Nathan, S.; Viswanathan, B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. In Proceedings of the 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Milwaukee, WI, USA, 25–28 September 2018; pp. 264–276.
65. Cachin, C. Architecture of the Hyperledger Blockchain Fabric. In Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, USA, 25 July 2016; Volume 310.
66. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; p. 30.
67. Robinson, P. Using Ethereum Registration Authorities to establish Trust for Ethereum Private Sidechains. *J. Br. Blockchain Assoc.* **2018**, *1*, 1–7. [CrossRef]
68. Reis, V. A new theoretical framework for integration in freight transport chains. *Transp. Rev.* **2019**, *39*, 589–610. [CrossRef]
69. Chung-Yee, L.; Qiang, M. *Handbook of Ocean Container Transport Logistics: Making Global Supply Chains Effective*; Springer International Publishing: Cham, Switzerland, 2015.
70. Commonwealth Australia. *Time Release Study 2016*; Australian Government: Canberra, Australia, 2018.
71. Zhao, H.; Meng, Q.; Wang, Y. Exploratory data analysis for the cancellation of slot booking in intercontinental container liner shipping: A case study of Asia to US West Coast Service. *Transp. Res. Part C: Emerg. Technol.* **2019**, *106*, 243–263. [CrossRef]
72. Williamson, O.E. Outsourcing: Transaction cost economics and supply chain management. *J. Supply Chain Manag.* **2008**, *44*, 5–16. [CrossRef]
73. Williamson, O.E. The Economics of Organization: The Transaction Cost Approach. *Am. J. Sociol.* **1981**, *87*, 548–577. [CrossRef]
74. Sawant, R.J. Asset Specificity and Corporate Political Activity in Regulated Industries. *Acad. Manag. Rev.* **2012**, *37*, 194–210. [CrossRef]
75. Australian Competition and Consumer Commission. Container Stevedoring Monitoring Report 2018–2019. 2019. Available online: https://www.accc.gov.au/publications/container-stevedoring-monitoring-report/container-stevedoring-monitoring-report-2018-19 (accessed on 1 January 2020).
76. Shipping Australia Limited. Annual Review. 2019. Available online: https://shippingaustralia.com.au/wp-content/uploads/2020/01/SAL_Annual_Review_2019_WEB-1.pdf (accessed on 8 November 2020).
77. Gassmann, O.; Frankenberger, K.; Csik, M. *The Business Model Navigator: 55 Models That Will Revolutionise Your Business*; Pearson: Edinburgh, UK, 2014.
78. Weber, I.; Gramoli, V.; Ponomarev, A.; Staples, M.; Holz, R.; Tran, A.B.; Rimba, P. On Availability for Blockchain-Based Systems. In Proceedings of the 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Hong Kong, 26–29 September 2017; pp. 64–73.

79. García-Bañuelos, L.; Ponomarev, A.; Dumas, M.; Weber, I. Optimized Execution of Business Processes on Blockchain. In *Business Process Management*; Carmona, J., Engels, G., Kumar, A., Eds.; Springer: Cham, Switzerland, 2017; pp. 130–146.
80. López-Pintado, O.; García-Bañuelos, L.; Dumas, M.; Weber, I. Caterpillar: A Blockchain-Based Business Process Management System. In Proceedings of the Business Process Management, Barcelona, Spain, 10–15 September 2017.
81. Tran, A.B.; Xu, X.; Weber, I.; Staples, M.; Rimba, P. Regerator: A Registry Generator for Blockchain. In Proceedings of the CAiSE-Forum-DC 2017, Essen, Germany, 12–16 June 2017; pp. 81–88.
82. Tran, A.B.; Lu, Q.; Weber, I. Lorikeet: A Model-Driven Engineering Tool for Blockchain-Based Business Process Execution and Asset Management. In Proceedings of the BPM 2018: International Conference on Business Process Management—Demonstration Track, Sydney, Australia, 9–14 September 2018.
83. Bavassano, G.; Ferrari, C.; Tei, A. Blockchain: How shipping industry is dealing with the ultimate technological leap. *Res. Transp. Bus. Manag.* **2020**, *34*, 100428. [CrossRef]
84. Balaskas, A.; Franqueira, V.N.L. Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges. In Proceedings of the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Glasgow, UK, 3–4 June 2018; pp. 1–8.
85. Dillenberger, D.N.; Novotny, P.; Zhang, Q.; Jayachandran, P.; Gupta, H.; Hans, S.; Verma, D.; Chakraborty, S.; Thomas, J.J.; Walli, M.M.; et al. Blockchain analytics and artificial intelligence. *IBM J. Res. Dev.* **2019**, *63*, 5:1–5:14. [CrossRef]