# Blockchain Technology and Maritime Shipping: A Primer

Submitted to
U.S. Maritime Administration

Prepared by

Erin H. Green
Edward W. Carr, Ph.D.
James J. Winebrake, Ph.D. (Co-PI)
James J. Corbett, Ph.D. (Co-PI)

June 2020

## Table of Contents

# Acknowledgements

We would like to thank Dan Yuska and the U.S. Department of Transportation Maritime Administration for supporting this work. We would also like to thank various reviewers for their helpful comments on earlier drafts of this work. Lastly, we thank the many members of the blockchain business and non-profit community who spoke with us and provided valuable insights into the potential opportunities and challenges for blockchain technology implementation in the maritime sector.

# Acronyms and Abbreviations

| | |
|---|---|
| AIS | Automatic Identification System |
| ARPA | Automatic Radar Plotting Aid |
| AWS | Amazon Web Services |
| B/L | Bill of Lading. Also, eB/L, electronic Bill of Lading |
| BIMCO | Baltic and International Maritime Council |
| BLOC | Blockchain Labs for Open Collaboration |
| CINS | Cargo Incident Notification System |
| CO2 | Carbon dioxide, a greenhouse gas |
| COLREG | Convention on the International Regulations for Preventing Collisions at Sea, 1972 |
| DNA | Deoxyribonucleic acid |
| DoS | Denial of Service, a type of cyber-attack. Also, DDoS, distributed denial of service |
| ECDIS | Electronic Chart Display and Information System |
| EDI | Electronic Data Exchange |
| EEDI | Energy Efficiency Design Index |
| EU | European Union |
| EWF | Energy Web Foundation |
| GB | Gigabyte |
| GDPR | General Data Protection Regulation |
| GHG | Greenhouse Gas |
| GMDSS | Global Maritime Distress and Safety System |
| GPS | Global Positioning System |
| GSBN | Global Shipping Business Network |
| IBM | International Business Machines, a large technology company |
| ICO | Initial Coin Offering |
| ICT | Information and Communication Technology |
| IEA | International Energy Agency |
| IMO | International Maritime Organisation |
| IoT | Internet of Things |
| IPCC | Intergovernmental Panel on Climate Change |
| ISM | International Safety Management |
| ISO | International Organization for Standards |
| ISPS | The International Ship and Port Facility Security Code, 2002 |
| kWh | Kilowatt-hour a measure of energy consumption. Also, TWh, terawatt-hour |
| MARAD | United States Maritime Administration |

| | |
|---|---|
| MARPOL | International Convention for the Prevention of Pollution from Ships |
| MBL | Marine Blockchain Labs |
| MEPC | Marine Environment Protection Committee |
| MIT | Massachusetts Institute of Technology |
| MRV | Shipping Emissions Monitoring Verification and Reporting, developed by BLOC |
| MTI | Maritime Transport International |
| NASA | National Aeronautics and Space Administration |
| PoA | Proof of Authority, a blockchain validation algorithm |
| PoS | Proof of Stake, a blockchain validation algorithm |
| PoW | Proof of Work, a blockchain validation algorithm |
| PSF | Prime Shipping Foundation |
| SEEMP | Ship Energy Efficiency Management Plans |
| SMS | Safety Management System |
| SOLAS | Safety of Life at Sea Convention |
| STCW | International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978/1995/2010 |
| TB | Terabyte |
| TEU | Twenty-foot Equivalent Unit |
| VGM | IMO Verified-Gross-Mass (VGM) regulation, part of the SOLAS treaty |

# 1 Introduction to Blockchain Technology

## 1.1 Blockchain Technology Overview

A blockchain is a digital ledger made up of linked entries, referred to as blocks, that, depending on the application, store some form of data. Cryptocurrencies, for instance, are designed to record information regarding financial transactions. To decentralize the technology, copies of a blockchain are shared and stored on all computers in a common network rather than on a central server alone. No copy is considered more credible than another, and all changes must be mutually verified, usually using a proof-of-work or proof-of-stake system. Collaboration between computers to maintain the blockchain eliminates need for a centralized authority. By design, this structure resists unauthorized modifications and allows for verification of transactions between parties due to its immutable nature. Although these features hold for most instances of blockchain, it is important to note that there are various implementations of the technology, each having unique advantages and disadvantages. The issues discussed in the sections of this report are in the context of the maritime sector, but are relevant to any agency from the local, state, and federal level when considering blockchains for energy and transportation issues (Winebrake et al., 2019)[1].

## 1.2 Transactions on Centralized Systems

Many of the transactions we make on a daily basis require a central agent, whether it be a bank, email platform, or ridesharing app. These central agents or organizations often charge fees for their services and slow down the exchange process. The user is required to trust these central agents. In the case of a financial transfer, for instance, we trust banks to not only complete the exchange without fraudulent interference, but to also keep a record of the transfer including pertinent details. There is little work required from the sender's or the receiver's end; rather, the onus is on the bank to successfully complete the task. Although this system has traditionally

[1] Some of the material in this report draws on research conducted by the authors of this report, in previous work conducted for the New York State Energy Research & Development Authority on a similar topic (Winebrake et al., 2019).

worked well, its concentration of workload on a single entity is inefficient and increases security risks.

## 1.3 Decentralized Networks and Distributed Ledgers

### 1.3.1 Decentralized Networks

In a decentralized network, peers or “nodes” (computers) communicate with one another without a central server. Rather than having a single entity control all the data in a system, in decentralized networks information is directly available to all participants, with each node storing equally valid copies of files and documents, thus avoiding the need for trusted third parties. Having no point of central storage also makes information on networks less vulnerable to being tampered with and guarantees that systems will remain operational if certain nodes malfunction.

If there are too many nodes in a decentralized network, there may be a need for high performance nodes called “supernodes” that are better equipped to handle data flow. These nodes facilitate communication similar to servers in a centralized model and increase speed. Rather than a true distributed network, decentralized networks that use supernodes tend to follow a small world model, wherein all nodes are not neighbors or connected directly to one another, but most nodes can be reached by other nodes through a few hops or steps  (Hui et al., 2004).

### 1.3.2 Distributed Ledger

A distributed ledger is a record of transactions that can be accessed anywhere across a decentralized network. Information on the ledger is stored securely, with each entry having a unique cryptographic hash, digital signature, and timestamp values. All participants in the network have the ability to make additions to the record, which are then copied and distributed to the network once validated. All nodes hold a copy of the distributed ledger.

## 1.4 Mechanics of Blockchain

### 1.4.1 Transactions

As the name suggests, blockchain technology involves producing an unbroken “chain” of “blocks”.  Each block contains:

- **Data**, which depends on the type of blockchain. Cryptocurrencies, for example, store information about sender, receiver, amount of currency sent and received, etc.;

- **Hash**: the unique ID of the block; clock/modular arithmetic is used to create it, so the hash cannot be replicated or reversed; and,
- **Hash of previous block**: Including the hash of the previous block creates a chain of blocks, which increases security, because this means to tamper with one block, it is necessary to change hashes of all following blocks).

The nature of a transaction is one of the key concepts to understand in blockchain technology. A transaction may be conceptualized as a transfer of value from one party to another. In the context of blockchain, a transaction also includes additional information documenting the exchange details. Transactions may take many forms, including the trading of goods and services for monetary compensation, the exchange of knowledge and information, or the trading of assets. Transactions need not be financial, but the transfer of information, and the subsequent ownership of that information must be clearly defined.

### 1.4.2 Creating Blocks

New transactions on the blockchain network are timestamped and broadcast to each node in the network. Transactions are digitally signed by the seller and the buyer using a public key and a private key, both of which are unique digital signatures, and so ensure identity and validity. Public keys are known by all participants, while private keys are only known by the owner. Information can be sent from one node to another using the node's public key, but only the owner of that node can access that information using a private key. After verifying the transaction, new transactions are collected into blocks of transactions (Figure 1).

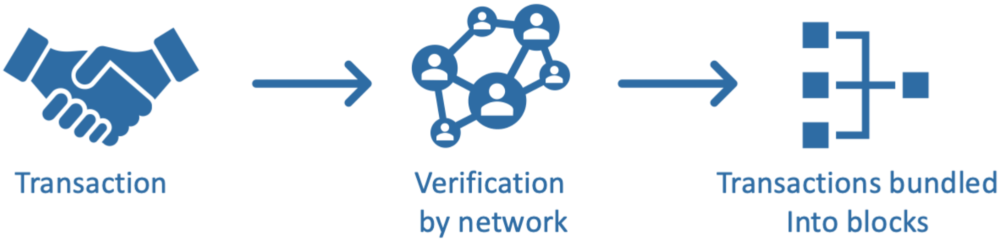
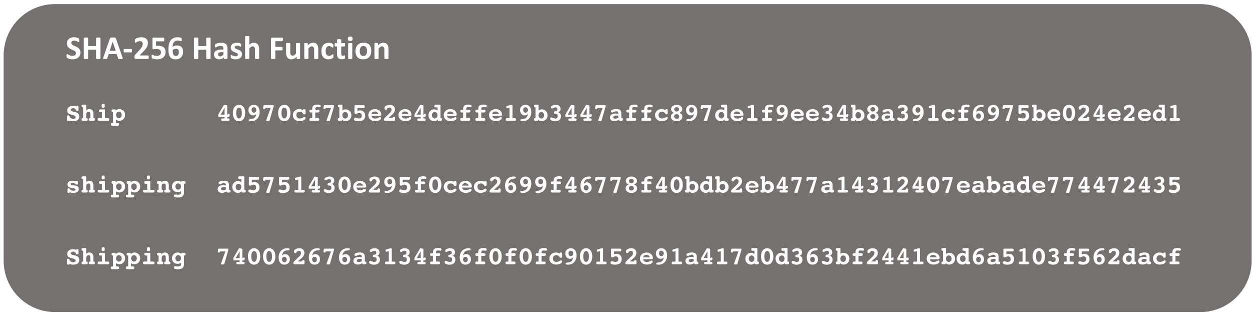


Figure 1: Transactions are verified by nodes and then bundled into blocks (Source: Winebrake et al., 2019)

### 1.4.3 Hashing

Hashing involves converting information into a unique digital fingerprint using hash functions. Regardless of the size or type of the input data, hash functions transform information into a unique fixed-length output string called a hash value or hash number. Though identical inputs produce identical hash values, small changes in inputs result in very different hash values. For example, the hash values in Figure 2 for "Shipping" and "shipping" share no similarities with each other, nor do they with the hash value for "Ship." Similarly, if a single character in a document were changed, and the document were re-hashed, a completely different and unique string of output characters would result. Hash functions are uni-directional and pseudorandom, meaning that someone would not be able to decipher (or reverse engineer) the original input data by knowing the hash values, as hash values do not relay any information about the original input data. Reversing hash functions requires a very large amount of computing power, to the point that doing so is infeasible.



SHA-256 Hash Function

```
Ship      40970cf7b5e2e4deffe19b3447affc897de1f9ee34b8a391cf6975be024e2ed1

shipping  ad5751430e295f0cec2699f46778f40bdb2eb477a14312407eabade774472435

Shipping  740062676a3134f36f0f0fc90152e91a417d0d363bf2441ebd6a5103f562dacf
```

Figure 2: Hash output for similar input data; this particular hash function (SHA-256) generates a string of 64 characters for each input string of characters, no matter what the size of the input string.

### 1.4.4 Adding Blocks to the Blockchain

Hashing condenses transaction information into a string of characters, which can then be incorporated into "blocks" of transactions. Creating a block of transactions is the first step of creating a blockchain. Next, nodes need to agree on the validity of the transactions in that block, and then post those transactions to the ledger by adding that block to the chain of existing blocks—creating the blockchain. Nodes come to agreement, or "consensus," by employing consensus algorithms, described in Section 1.5.

The node that first completes the required computational puzzle shares the new block with all other nodes in the network, which in turn accept the block only if the block's transactions are valid, as agreed upon by consensus. The accepted block is then added to the chain, chained together using the hash of the previous block to create the next block in the chain. Any changes to the blockchain are easily identifiable as changes to the hash values.

Each of the nodes in the network have a copy of all of the blocks that have been validated (i.e., a distributed ledger). The system relies on “honest” nodes to correctly validate the chain of transactions. Honest nodes are computers on the network that operate without attempting to maliciously or otherwise alter the transactions. The blockchain system is robust as long as honest nodes control more computing power than any dishonest nodes.

If more than 51% of nodes, or computing power, are operating in a coordinated manner, then the distributed nature of the blockchain is jeopardized, and the nodes in the majority may manipulate the system. This is called the 51% problem. In large networks, the distribution of validated information across the network achieves the same goals as independent institutional review and certification; however, networks with fewer nodes are more susceptible to manipulation.

### 1.4.5 Timestamp Server

Timestamps are included with any block ID information and are applied to blocks by the validating node when the blocks are successfully added to the chain. Timestamps are vital to the function of blockchain, as a timestamp proves that the transaction data included in the block existed, and also serves to describe and record the chronological order of transactions, preventing double-spending. A block’s hash function includes the previous timestamp in its hash, thus creating a chain with each subsequent timestamp reinforcing the timestamps before it.

### 1.4.6 The Double Spend Problem

Double-spending is a potential problem with digital currencies that occurs when the same set of resources is spent on different transactions. A race attack would occur if a user were to spend money on two or more transactions simultaneously (or near simultaneously). Normally, the network would be able to distinguish between the transactions and mark them as invalid. However, if the verification processes also occur at the same time, multiple versions of the blockchain (one for each transaction) exist. This would initiate a race between each version of the chain, with the one to achieve the next successful verified block as the winner. The other chains are then rejected despite the sender benefitting from all original transactions. It is therefore good practice to wait for multiple subsequent blocks to be verified before deeming a transaction complete.

## 1.5 Validation Algorithms

### 1.5.1 Proof-of-Work

Blockchain networks use consensus mechanisms to check the validity of transactions before adding them to new blocks. The consensus procedure must be robust to ensure security, especially when there is little trust between participant nodes. There are several consensus algorithms used in blockchain technology; Proof-of-Work, Proof-of-Stake, and Proof-of-Authority are currently among the most common validation algorithms.

In Proof-of-Work (PoW), “miners” in the network race to solve a computational puzzle, often by trial and error, which is to find a value, called the nonce, which when included in the block yields a hash with a specified number of leading zeroes. The network can adjust the difficulty of the verification puzzle to moderate or speed up validation.. Once a solution is found, other nodes will verify the validity of the outcome. If there is a consensus, the corresponding block is broadcasted to the entire network. The successful miner is also rewarded. Despite being difficult to find, hashes are designed to be easy for all nodes in the system to check. The process of finding a valid hash is straight forward, but repetitive and time-consuming, often using brute force methods.

Mining also requires sophisticated computer hardware and consumes a large amount of power, making the proof-of-work mechanism both financially and environmentally costly. As of late August 2019, the Bitcoin network was estimated to consume 624 kWh of electricity per transaction (the equivalent of the daily consumption of 20 U.S. households)—over 73 TWh annually, producing an estimated carbon footprint equivalent to that of the entire nation of Denmark (de Vries 2019b).

Proof-of-Work rewards those with better equipment and greater computing power, which provides and incentive for replacing computing equipment; as a result, the Bitcoin network is estimated to produce a quantity of e-waste equivalent to that produced by Luxemburg annually (de Vries 2019b). Rewards for better equipment and greater computing power also incentivize people to team up and create mining pools, increasing centralization of the network, and results in a situation where “the rich get richer”.

### 1.5.2 Proof-of-Stake:

In a Proof-of-Stake (PoS) consensus system the network elects a random node to validate a transaction, rather than having nodes compete against each other to mine blocks. Nodes are expected to stake some amount of currency to be chosen as a validator (and lose part of their stakes for approving fraudulent blocks); it is assumed that those who hold a stake in the network have an incentive to work in the interest of the network. The larger the stake offered by a node, the more likely the node will be selected as a validator. The PoS system deals with the same "the rich get richer" problem as Proof-of-Work, however the linear cost-to-benefit function makes it impossible for the rich to benefit from economies of scale under PoS. Under a delegated PoS mechanism, stakeholders vote on who to select as validators of the network. Proof-of-Stake consensus is more energy and cost efficient than Proof-of-Work; the Ethereum network (which supports many applications in the energy sector) this year announced plans to shift from Proof-of-Work to Proof-of-Stake consensus.

### 1.5.3 Proof-of-Authority

Proof-of-Authority is a modified version of Proof-of-Stake, where instead of placing monetary or financial resources at stake, the potential validator places their reputation at stake. Proof-of-Authority requires that validators' identity be publicly known and verified, in contrast to Proof-of-Work and Proof-of-Stake systems, in which nodes and validators are anonymous. Validators in Proof-of-Authority may be required to obtain a license or pass an exam to maintain their standing. Proof of Authority is used in centralized systems.

### 1.5.4 Additional Consensus Algorithms

Recognizing the challenges and weaknesses associated with the more common consensus algorithms, additional consensus algorithms have been developed. These include: Delegated Proof-of-Stake, in which validators are elected by the pool of stakeholders; Proof-of-Weight, in which validators are selected based on relative weights of relevant attributes (such as the quantity of data being stored, or reputation of the validator); Byzantine Fault Tolerance methods including Practical Byzantine Fault Tolerance, where, in centralized systems, "generals" are pre-selected as generals (validators), and Federated Byzantine Agreement, where in some systems generals (validators) are pre-selected, and in others participants are allowed to select which generals/validators to trust (Witherspoon, 2017).

## 1.6 Public vs. Private Blockchains

### 1.6.1 Public Blockchains

There are two main types of blockchain systems: public (open-source or permissionless), and private (permissioned). Much of the ongoing conversation around blockchain technology, including structure, strengths, and weaknesses, is in the context of public blockchains. Yet many applications—especially those run by private entities and organizations or consortiums—use private blockchain platforms. There are key differences between public and private blockchain systems, and important tradeoffs to consider in understanding the potential implications of using each.

In public blockchains, no user is given unique privileges or decision-making powers; the high level of decentralization makes public blockchains more secure. Most public blockchains are permissionless, but they can be made permissioned. Bitcoin and Ethereum are all examples of public blockchains. Compared to centralized systems, public blockchains offer several potential advantages. These include, reduced centralized authority, immutable data storage, reduced transaction costs, increased transparency and traceability, and security (See Section 1.8 for further discussion). However, these advantages come with tradeoffs. First, validation requires extremely high energy consumption (which comes at a significant financial and environmental cost). Second, Public blockchains are often unable to quickly handle large numbers of transactions. Bitcoin, for instance, has a theoretical limit of 4,000, but a realized (real-world) average of 7 transactions per second. Visa credit cards, on the other hand, has an average of 2,000, and can process up to 56,000 transactions per second (Ganne, 2018).

### 1.6.2 Private Blockchains

Private blockchains are managed by single or small groups of organizations. Transactions are verified and processed by certain nodes, increasing the network efficiency and speed of transactions. Restrictions in a private blockchain network can be customized (ex: In a network of four users (A, B, C, D), B could decide to only exchange information with D and C).

The centralized nature of private blockchains, however, mean that data are not immutable (administrators can make changes to the ledger), and can make them more susceptible to external interference. Private blockchains also lose the advantage of decentralization, as relatively few participants or administrators have the power to hold, and make changes to, the ledger.

Additional challenges and limitations of blockchain technology are presented in Section 4.

## 1.7 Smart Contracts in Blockchain Technology

Smart contracts are one of the more intriguing aspects of blockchain technology for many organizations, given their potential to increase efficiency of transactions through digitization and automation.

A smart contract is written as a program between two or more contracting parties (who can remain anonymous) that can be accessed on the public ledger for others to view; a trigger event causes the smart contract to execute automatically without needing a third-party to monitor or function as an intermediary. Smart contracts inherit the properties of blockchain (i.e. immutability, traceability, transparency), yet offer more flexibility than standard blockchain. The use of smart contracts requires "oracles", which provide necessary data on real world events and conditions relevant to the contract (such as prices or air temperature or whether a physical barrier has been crossed, etc.). The Ethereum platform, which is widely used, including in the maritime sector, offers smart contracts as a feature in their implementation of blockchain.

Smart contracts are not as flexible as traditional contracts in accounting for non-quantifiable clauses and conditions, nor are they as accommodating to unforeseen events. Additional limitations and challenges of smart contracts, including those which may be of particular concern to the maritime sector, are presented in Section 4.3.2.

## 1.8 Potential Benefits/Strengths of Blockchain

### 1.8.1 Reduced Centralized Authority

The decentralized nature of blockchain technology leads to reduced centralized authority and open communication and data sharing among participants, or "nodes". Systems are not reliant on one party for decision-making authority, transaction approval, and data storage and validation. Reduced centralized authority also means that systems are not as susceptible in terms of a single point of failure. The level of decentralization (and thus reduced reliance upon a central authority, and related potential strengths) varies considerably depending upon the type and specifics of a given blockchain platform, with public, permissionless systems being more decentralized, and private, permissioned systems being less so.

### 1.8.2 Immutable Data Storage

Blockchain systems involve storage on multiple distributed ledgers, which means that multiple copies of data records are held on multiple nodes often across multiple geographies. As data stored on paper can degrade, and digital data storage systems can be corrupted, blockchain offers a potential improvement in terms of avoiding degradation of data. Blockchain is also often described as being inherently immutable in terms of its structure, as hashing and creating blocks present significant barriers to deliberately (or accidentally) changing data records in ledgers. The immutable nature of blockchain records, however, is a characteristic of public, permission-less platforms or systems, and is not an attribute of private or permissioned systems. Further, experience with blockchain platforms in recent years has shown that in practice, blockchain ledgers may not be as immutable as originally imagined. Concerns surrounding manipulation of data and security of data, etc., are discussed further in Section 4.3.4.

### 1.8.3 Reduced Transaction Costs (or Information Sharing Costs)

Transactions in existing centralized systems typically require an intermediary to verify and complete the transaction (e.g. a bank for a financial transaction; banks, lawyers and agents for a real estate transaction). These intermediaries often charge fees, which can increase the total cost of the transaction substantially. This is particularly the case in the maritime industry, where brokers, couriers and documentation add substantial transaction costs to shipments. Blockchain systems (public, permissioned in particular) reduce or remove the need for such intermediaries, and typically do not charge high per-transaction fees. The use of blockchain platforms and systems come with their own associated costs, however, including start-up costs, equipment and technology costs, per-transaction fees, and data storage costs. These are discussed in greater detail in Section 4.3.4.

### 1.8.4 Increased Transparency and Traceability

A major concern with centralized systems today is the lack of transparency with respect to parties providing data, and with respect to the holders of the data in centralized systems. Blockchains can improve transparency by recording all stages of a transaction (or all relevant data points), and by allowing the data to be recorded in a distributed fashion, so that all participants may access, view and verify transactions. Of potentially particular interest to the maritime industry is blockchain’s ability to increase traceability of linked actions and transactions, in one record shared among all relevant parties (participants).

### 1.8.5 Facilitation of Payments

Blockchain provides a way to facilitate payments without the need or use of fiat currency. Blockchain platforms or systems often use “tokens” or “coins”, or other so-called cryptocurrencies, which allow for electronic payments outside of banks or traditional intermediaries. Payments may be made automatically with smart contracts (e.g. once a shipment is received, a payment is automatically made). The facilitation of payments outside of fiat currency may be of particular use for the maritime industry, given that international shipments typically involve many parties from various countries (all of which make use of different fiat currencies). Where blockchain systems offer this potential advantage or strength, however, they also face a related limitation; blockchain systems are not able to process transactions involving fiat currency. Blockchain systems can report that a transaction involving fiat currency took place or that it was supposed to take place), but they cannot within themselves transfer fiat currency—blockchain systems can only transfer currencies that are native to that blockchain (e.g. Bitcoins in Bitcoin, Ether in Ethereum, or TEU tokens in 300Cubits (as of October 2019, 300Cubits TEU token is defunct).

### 1.8.6 Security

Blockchain is often described as improving data security compared to centralized and legacy systems, as the distributed nature of blockchain ledgers leaves the network less vulnerable to a single-point attack, and also due to the structure of blockchain systems. Consensus mechanisms; hashing, validating and creating blocks; and distributed ledgers all make the system resistant to changes. For several years, blockchain was touted as being “unhackable’. However, experience in recent history (2018 to 2019 in particular) has shown that blockchain systems can be hacked and continue to be hacked; see Section 4.3.1 for further discussion.

# 2 Potential Role of Blockchain Technology in Maritime Sector

## 2.1 Key Drivers and Issues in the Maritime Sector

A number of issues and trends in the maritime sector serve as drivers to exploration of, or potential use of, blockchain technology in shipping. These drivers, which include the current inefficient nature of transactions, ISO standards and codes, cold chain requirements, data flows and movement toward internet of things, cybersecurity threats, fraud, environmental and efficiency standards, and regional, national, and international regulations.

## 2.2 Current Inefficient Nature of Transactions with Minimal Transparency

Transactions in the maritime sector are currently slow, time-consuming, and expensive. An estimated 20% of operational budgets are due to poor information management (Czachorowski et al., 2019). Many parties and intermediaries are involved in transactions (i.e. exporters, importers, port and customs authorities and officials, financiers, surveyors, valuators, agents etc.), none of whom have access to data and information on all necessary parts of the supply chain. Paper documentation is required, and transactions often require physical inspection of documents resulting in high transaction costs for shipments. Brokers also increase costs substantially. There is little-to-no accountability for inefficiency, fraud, or cargo theft. Additionally, it is difficult for small-to-midsize agents to find reasonable terms for financing, which is skewed in support of larger entities (Botton, 2018; Joseph, 2018).

The paperless exchange of documents has the potential to address some of the current challenges of transactions in the maritime sector. According to IBM, out of a total cost of $2,000 to move a container of avocados from Mombasa to Rotterdam, paperwork costs approximately $300, or 15%. IBM estimates that complete digitalization of the shipping process could save shipping carriers up to $38 billion per year (Ganne, 2018). Blockchain presents one way in which paperwork could be digitized in the maritime sector and could improve the cost-effectiveness of transactions; cost has been identified as a main driver to digital innovation (and potentially use of blockchain) in the maritime industry (Gausdal et al., 2019).

In the maritime sector, the application of blockchain (and smart contracts) for paperless exchange of documents contracts might involve, as described by Joseph (2018), a computer program which would engage all involved parties (exporters, export and port authorities and officials, importers, financiers, surveyors, and valuators), and which would involve uploading of various documents to a system, "publishing" the relevant contract on blockchain, and allowing parties to negotiate on the network; once documents were approved and signed by parties, a program would then approve and move on to the next phase of the transaction. Finally, the contract would be automatically executed by network consensus, and all relevant information would be uploaded information for all interested parties. (Joseph, 2018).

As described in Botton (2018), using blockchain for paperless documentation in shipping could:

> …provide a firm with the infrastructure necessary to remove the need to secure each transaction or step in the supply-chain through intermediaries via registration, tracking and certification. Information on any shipment– whether it be a proof of purchase, a clearance form, a bill of lading, insurance – can be made part of a block, a transparent chain of custody, and be accessible to suppliers, transporters, buyers, regulators and auditors…
>
> Used in customs handling, exporters could upload all the documents onto a customs office blockchain and instantly prove their abidance with all the import rules – for example, qualification for preferential rates through rules of origin, sanitary and phytosanitary (SPS) rules, or compliance with embargoes (e.g. against conflict minerals). The technology could also facilitate…border tax adjustments for carbon or corporate taxes.

The ability to have all of this information is one place, accessible to all relevant parties, would lower transaction costs, as well as reducing auditing and accounting costs (Botton, 2018).

Estimates show that savings from paperless trade would be most impactful for smaller shipments and perishable goods, both of which are of interest for transitioning economies; a shift to paperless exchange could decrease barriers to entry, potentially benefitting smaller nations and shipping companies (UN, 2006)

On the other hand, the transition to, and implementation of, paperless trade will be costly up front, and might actually present barriers to smaller companies engaging in the marketplace. Likewise, developing countries may not have access to adequate infrastructure to implement paperless trade, and thus could be excluded. Further, until a robust and widely used paperless system is developed, companies will likely not be able to reap the full benefits.

The transition to paperless documentation will not be simple. Companies will choose to adopt the system if they see a clear benefit. Initial implementation and maintenance costs may prevent them from switching. Paperless trade will also be most useful when all or most parties in the supply chain have access to the blockchain. This would require the entire shipping and related industries to make the switch to a common paperless system, which, if even possible, will take time to manage and coordinate.

### 2.2.1 ISM and ISO Standards and Codes

Implementation of International Safety Management (ISM) code and International Organization for Standards (ISO) requirements related to quality management have complicated the reporting and management of documents in the shipping industry. Outside of safety and quality requirements, documentation requirements for exports also commonly include documents related to export, transportation, compliance, certificates of origin and other certificates, among others. These regulatory requirements are expected to become more stringent over time, in response to the breakdown of trade unions between major economic powers, further increasing the complexity of transactions and required documentation. (DiGregorio & Nustad 2017). Similar to the discussion of inefficient transactions, blockchain has the potential to reduce the administrative burden faced by those in the shipping industry, by allowing the streamlining, digitization and automation of certain documents and reporting requirements through the use of smart contracts (DiGregorio & Nustad 2017).

### 2.2.2 Cold Chain Requirements

Many products, from food to pharmaceuticals, require climate- or temperature-controlled conditions to ensure product safety or efficacy (Sykes, 2018). According to the World Health Organization, 40% of vaccines degrade from temperature variation during transport. The pharmaceutical industry spent $13.4 billion on transporting temperature-sensitive products in 2017 and as of 2018 approximately 20% of pharmaceutical payloads were shipped on ocean-going vessels. This is estimated to increase to roughly 75% of pharmaceutical payloads sent by marine freight within ten years (Muspratt, 2018).

Blockchain-enabled shipping containers that regulate temperature have been developed and could be useful in transporting temperature-sensitive goods such as food and pharmaceuticals. Currently these blockchain-enabled containers have been developed for use in air freight (over 1,000 were in circulation as of 2018), but similar containers could feasibly be used in sea shipments in the future (Hampstead, 2018). The containers are cooled with a rechargeable passive cooling technology and include sensors to monitor temperature and location among other variables. The "blockchain-like" ledger used with these containers records documents such as bills of lading and customs forms (Hampstead, 2018).

### 2.2.3 Data Flows

The data flow of the shipping industry is ever increasing.  A typical supply chain manages about 100 gigabytes of data per day—and is expected to increase substantially in the near future—with some sources estimating that supply chains will produce zettabytes of data by 2020 (Czachorowski et al., 2019; Gausdal et al., 2018). In most cases the data are not shared among relevant parties and stakeholders. There is increasing recognition for the need to connect stakeholders and share relevant data flows—for instance, the port of Hamburg has required that all parties share data on a single connected system (Czachorowski et al., 2019).

### 2.2.4 Internet of Things

The Internet of Things (IoT) involves the use of sensors and other devices which are interconnected to networks and allow for monitoring and related management of devices, machines, equipment or other "things". IoT is predicted to play an increasing role in the maritime sector, potentially allowing for asset tracking, improved route optimization, and reduced maintenance costs (DiGregorio & Nustad, 2017). Current application of IoT in the shipping industry includes GPS tagging of containers to facilitate movement through transit nodes and allowing for real-time tracking of cargo and vessels (Czachorowski et al., 2019).

In the refrigerated shipping containers example above, asset tracking with IoT could involve the use of sensors on the containers, a processing unit, and a transmitter which would allow for real-time monitoring of temperature, which in turn could allow for immediate response or management in the case that temperature approached designated thresholds (DiGregorio & Nustad, 2017).

There are many concerns and challenges surrounding the use of IoT. Users of the system must trust that the data received from IoT devices have not been altered in any way. IoT devices have relatively limited computing power with internet (often wi-fi) connectivity, and their firmware is typically not updated frequently, making them subject to cyber-attack. Nineteen distinct categories of security issues associated with IoT were highlighted in a 2018 review article; these included jamming adversaries, Sybil and spoofing attacks, sinkhole and wormhole attacks, authentication and secure communication, privacy violation, and insecure interfaces, software or firmware (Khan & Salah 2018)[2]

Blockchain is complementary with IoT technologies, in its potential to improve security and provide for storage of data collected from IoT uses. Blockchain itself does not enable the use of sensors, monitoring or management, or data collection—these are all aspects of the use of IoT and associated data-collection systems. Blockchain could, however, allow for the documentation and storage of recorded data on a ledger, and also has the potential (in conjunction with oracles) to allow the use of smart contracts in managing devices in real-time (DiGregorio & Nustad 2017). Blockchain could eliminate the need for a centralized broker or authority, serving as an autonomous clearinghouse when appropriately integrated with IoT devices.

### 2.2.5 Cybersecurity Threats

In addition to security concerns with IoT outlined above, the shipping industry increasingly faces cybersecurity threats, such as the NotPetya ransomware attack that affected Maersk in 2017, at a cost of over $200 million to the shipping company (Mathews, 2017; DiGregorio & Nustad, 2017).

Cybersecurity is an increasing concern in the maritime sector, given the potential impacts on, and implications for critical areas of the maritime sector, including cargo handling and management, passenger servicing and management, welfare of crew and administration,

[2] Remaining security issue categories reported in Khan and Salah (2018) include: insecure initialization, insecure physical interface, sleep deprivation attack, replay or duplication attacks due to fragmentation; insecure neighbor discovery, buffer reservation attack, RPL routing attacks, transport level end-to-end security, session establishment and resumption, CoAP security with internet, and middleware security. An in-depth discussion of these security threats is beyond the scope of this report, but the reader is directed to Khan and Salah (2018) for details and elaboration.

management and control of machinery and power, access control systems, and communication systems, among others. Intentional (e.g. cyber-attacks), or unintentional errors such as loss, corruption, or compromising of data have the potential to result in operational, safety or security failures, or in failures to protect the marine environment (IMO 2017).

The maritime sector relies upon computerized, integrated and automated systems, while information and operational technology systems onboard vessels are increasingly connected. These technological changes can open the door for unauthorized or malicious access, both by parties outside the ship or network, or by onboard personnel (ICS n.d.).

Modern vessels have advanced systems that rely on computers and communications to operate. These include ECDIS (Electronic Chart Display and Information System), AIS (Automatic Identification System), Radar/ARPA (Automatic Radar Plotting Aid), compass, steering, and GMDSS (Global Maritime Distress and Safety System) (DiRenzo et al 2015). Demonstrations have shown that vessels can be hacked into and navigated remotely by taking over the ship's GPS system; signal jammers can interfere with several onboard systems used for communication and navigation; and, port and cargo systems can be hacked, with data trails erased (DiRenzo et al 2015).

The ECDIS system (a marine navigational chart and information system), required by IMO as of 2018, is considered vulnerable to cyberattacks as it relies on internet connected software. Flaws in ECDIS systems potentially allow attackers to access and modify files and charts; demonstration attempts to penetrate ECDIS systems have identified several weaknesses including the ability to access, download, read, delete or replace any file stored on the machine hosting the ECDIS, which could allow attackers to interact with the shipboard network and all connections, potentially causing serious financial or environmental damages and safety and security risks including loss of life (DiRenzo et al 2015).

As more technological innovations and internet-connected devices and control systems are used in shipping, more cybersecurity risks will need to be identified and minimized. In seeking to minimize cybersecurity risks, in 2017 the IMO adopted MSC.428(98), on Maritime Cyber Risk Management in Safety Management System (SMS), which encourages administrations to appropriately address cyber risks in safety management by January 2021. In

2017, IMO also developed guidelines and high-level recommendations in minimizing cybersecurity threats and vulnerabilities in the maritime sector (ICSb n.d.; IMO 2017).

Blockchain is envisioned as a way to address or alleviate cybersecurity threats of centralized systems, as it may assist in blocking identify theft, preventing tampering with data, and resisting denial-of-service (DoS) attacks (ransomware attacks are considered DoS attacks that use malware or executable files to impede business services); blockchain systems cannot be exploited with malware in the same way that centralized systems can, and are largely considered much safer than centralized systems (DiGregorio & Nustad 2017).

### 2.2.6 Fraud

Fraud is a major problem in shipping, and both incidents and methods of fraud have increased recently. Examples of fraud in the maritime sector include: falsification of Bills of Lading, including under-invoicing to avoid taxes; bribes and illicit payments to obtain contracts, influence inspections or enable port operations; and defrauding importers or exporters with illegally purchased letters of credit. Such fraudulent activities are estimated to increase the cost of shipping operations by 10%, according to the World Economic Forum (DiGregorio & Nustad, 2017).

Blockchain could improve protection against fraud while also facilitating the identification of fraud, as it could be used to assist in authentication and verification of valid transactions, and to store the information on a transparent, distributed and tamper-resistant ledger, which all relevant parties in the supply chain could view. Government and customs officials are particularly interested in blockchain to combat fraudulent activities, as it may allow for automation of many controls now handled by these authorities (DiGregorio & Nustad, 2017).

### 2.2.7 Environmental Standards and Efficiency Requirements

The maritime industry is subject to increasingly stringent environmental rules and regulations, with the intention of protecting public health and marine and coastal environments. Key rules enacted through the International Maritime Organization (IMO) and the European Union involve clean fuel standards and efficiency and emissions standards. IMO 2020 requires that ships burn fuel with an effective sulfur content of less than 0.5%, compared to the current limit of 3.5% sulfur content. This will require shifts to low-sulfur fuels such as LNG or alternative fuels, or if using higher-sulfur-content fuel, vessels can opt to use scrubbers (IMO

2019; Saul 2019). The “carriage ban”, adopted in 2018, prohibits ships without installed scrubbers from carrying or transporting fuel with a fuel sulfur content higher than 0.5%. IMO 2020 is estimated to prevent over 570,000 premature deaths between 2020 and 2025 (Sofiev et al 2018). Implementation, tracking and enforcement of the standard presents substantial challenges, however, as IMO does not have the authority to enforce the standards; authority for monitoring, tracking, and enforcement resides with Flag States and port states (IMO 2019). Estimates of deliberate non-compliance (cheating) have ranged from 10% to 30% of total marine fuel consumption (Grimmer, 2018).

IMO has also adopted legally binding energy efficiency requirements for vessels under MARPOL Annex VI. These requirements, termed the Energy Efficiency Design Index (EEDI), which apply globally, set baselines for fuel consumed for a given cargo capacity; the baselines become progressively more stringent, with a 30% improvement required by ships built in 2025, compared to those built in 2014 (MEPC 62/24/Add.1 Annex 19, page 12 ). The energy efficiency regulations require Ship Energy Efficiency Management Plans (SEEMP) and require cleaning or replacement of inefficient parts of the ship, among others.

As of 2016 the IMO requires that ships of 5,000 gross tonnage and above collect fuel consumption data by fuel type, and other transport-related data. The Marine Environment Protection Committee (MEPC) has also developed an initial strategy, to reduce greenhouse gas emissions (GHGs) from ships. The initial strategy, which according to a Roadmap approved in 2016, will be updated in 2023, has a goal of reducing GHG emissions from shipping 50% by 2050 (IMO 2018, IMO n.d.).

### 2.2.8 Other Regulations and Initiatives

Additional regulations faced by the shipping industry include: the IMO Safety of Life at Sea Convention (SOLAS) requirement for shippers to provide a Verified Gross Mass (VGM) for every packed container as a condition for vessel loading, which took effect in 2016, and additional SOLAS requirements; MARPOL (International Convention for the Prevention of Pollution from Ships) requirements to prevent pollution from routine operation or in the case of accidents; COLREG (Convention on the International Regulations for Preventing Collisions at Sea, 1972) regulations to prevent collisions; ISPS (The International Ship and Port Facility Security Code, 2002) requirements to ensure the security of ships and port facilities; and STCW

(International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978/1995/2010), which establishes competence standards and certification requirements for seafarers; among other regulations and initiatives requiring documentation, or monitoring, tracking, and enforcement (ICSa, n.d.).

# 3 Current Examples and Potential Applications of Blockchain in the Maritime Sector

Potential applications of blockchain technology in the maritime sector include: tracking and tracing shipments and cargo from start to end; electronic sharing and transferring of “smart” Bills of Lading; storing and managing documents, digitalizing and decentralizing shipping logistics, declaration and handling of hazardous goods, payments for shipping services, connecting stakeholders to enable collaboration, fuel provenance, a system for emissions credits or certificates, certification, marine insurance, and registering ships into class. Each of these potential applications of blockchain, in fact, is being tested in the maritime industry, although platforms are generally in introductory or pilot phase. In this section we highlight the current examples of pilot projects and initiatives involving the use of blockchain in these areas.

## 3.1 Paperless Trade, Tracking, Logistics, and Facilitating Stakeholders Communication/Data Sharing

### 3.1.1 TradeLens

IBM and Maersk have partnered to create a blockchain-based platform to increase transparency in the shipping supply chain. The platform is designed to be accessible to all in the supply chain ecosystem (shipowners/brokers, land transportation providers, customs/government agencies, port regulators, insurance companies, etc.), and tracks shipments from start to end with process statuses visible to all in the network. Documents can be digitized and electronically signed. As of August 2019, over 100 organizations were involved in the TradeLens early adopter program (MI News Network, 2019).

### 3.1.2 CargoX – Bill of Lading

A Bill of Lading (B/L), a contract of carriage which serves as a document of ownership and receipt, is required by Maritime Law. B/L are often delayed due to banks and other intermediaries, leading cargo to arrive at ports ahead of the B/L. Fraud is also a concern with B/L, including forged signatures and inaccurate descriptions of cargo (Czachorowski et al, 2019)

CargoX has created a blockchain-based platform for sharing smart B/L. The system is paperless and is reported to cut transfer time from several days to minutes or seconds. In addition to improving transaction transfer speed, paperless B/L are also anticipated to reduce transportation costs, eliminate emissions from courier services to transport traditional bills of lading, and reduce chances of loss, theft, or damage to the bill-of-lading. The first container processed using CargoX's technology was shipped from Shanghai, China and released in Port of Koper, Slovenia in August 2018; the B/L was issued and transferred electronically "in just minutes instead of days or weeks". The electronic Bill of Lading (eB/L) cost $15, approximately 15% of the estimated typical cost for a document to be delivered such long-distance using courier services. (MI News Network, 2018a; MI News Network, 2019)

### 3.1.3 Global Shipping Business Network (GSBN)

The Global Shipping Business Network (GSBN), based on distributed ledger technology, is the product of a consortium of nine leading ocean carriers and terminal operators, including CMA CGM, COSCO SHIPPING Lines, Evergreen Marine, OOCL, Yang Ming, DP World, Hutchison Ports, PSA International Pte Ltd, Shanghai International Port, and CargoSmart, a software provider. GSBN has the intention of connecting stakeholders in the shipping community, including carriers, shippers, terminal operators, customs, shippers, and logistics service providers, to allow collaboration and communication. (MI News Network, 2019).

### 3.1.4 Abu Dhabi Ports—Silsal

In 2018 Maqta Gateway, an Abu Dhabi Ports subsidiary, launched the blockchain technology Silsal. Silsal has the objective of securely linking stakeholders in the shipping and trade industries, using blockchain and unique digital user identities. (MI News Network, 2019).

### 3.1.5 Pacific International Lines Ltd, PSA International and IBM Singapore

Pacific International Lines Ltd, PSA International and IBM Singapore are collaborating on a venture to use blockchain in tracking and tracing cargo movements. The blockchain supply-chain platform, is being tested and applied in tracing and tracking shipments from Chongqing to Singapore via the Southern Transport Corridor (MI News Network, 2019).

### 3.1.6 AMRO, Samsung SDS And Port Of Rotterdam

ABN AMRO, the Port of Rotterdam Authority and Samsung SDS (which involves logistics and IT) are collaborating on a blockchain-based pilot project with the goal of integrating a paperless network of physical, administrative and financial streams within international shipping and distribution.

### 3.1.7 ShipChain

ShipChain, based on the Ethereum platform, is a blockchain-enabled end-to-end shipping logistics company with the goal of tracking shipments from the production facility through final delivery to a customer. ShipChain's initial coin offering (ICO)—essentially an opportunity to invest in the company—has been met with a great deal of public scrutiny, as after raising over $30 million, the value of ShipCoins plummeted to about 1% of the initial value, and the price now stands at a fraction of a penny.

## 3.2 Payments for Shipping Services: 300Cubits

300Cubits makes use of smart contracts on the Ethereum platform and allows for TEU tokens to be used as booking deposits on shipments. A trial shipment consisting of two 40-foot containers shipped from Malaysia to Brazil was completed in early 2018; the TEU tokens were returned to users upon receiving a port Electronic Data Exchange (EDI) message confirming receipt of the shipment (MI News Network 2019). 300Cubits TEU tokens are now defunct, as of October 2019 (Meyer, 2019).

## 3.3 Environmental/Efficiency Standards

### 3.3.1 Marine Blockchain Labs (MBL) Fuel Provenance

Marine Blockchain Labs is a partnership set up between Lloyd's Register Foundation and Blockchain Labs for Open Collaboration (BLOC). One project is a fuel provenance register for the maritime sector, which aims to provide trusted information about fuel origin, journey and characteristics to improve traceability and transparency; a demonstration project traced a batch of biofuels through creation, processing, blending, and delivery to the bulk cargo carrier Frontier Sky. The BLOC MBL consortium includes Lloyd's Register, Precious Shipping, Bostomar, BIMCO, International Bunker Industry Association and GoodFuels. (Cleaner Seas, 2018a).

### 3.3.2 BLOC Shipping Emissions Monitoring Verification and Reporting (MRV)

BLOC also developed the Shipping Emissions Monitoring Verification and Reporting (MRV) solution, which build upon the Marine Fuel Assurance prototype. The MRV project, which seeks to allow tracing of shipping emissions and ultimately improve public health, won the Massachusetts Institute of Technology (MIT) Solve's Coastal Communities Challenge. BLOC, through the MRV tool, seeks to create a chain of custody for fuels, and provide a decision support system to assist stakeholders in the shipping industry in compliance with the IMO 2020 Sulphur cap and other such regulations (Cleaner Seas, 2018b).

## 3.4 Safety

### 3.4.1 BLOC, Lloyds Register, and Rainmaking—Hazardous and Dangerous Goods

Shipping containers do not often carry indication of their specific contents; though a product code may be scanned or traced in some data systems, these data systems rarely share or interoperate with other stakeholders' systems. This can present a serious safety issue in the case of hazardous or otherwise dangerous goods (which make up between 5 and 10% of a typical containership's cargo); misdeclaration of cargo can lead financial losses, ship damages, injuries and loss of life. The Cargo Incident Notification System (CINS) estimates that almost one-quarter of serious incidents onboard containerships were due to cargo being mis-declared. (Cleaner Seas 2019).

Marine Blockchain Labs and Rainmaking are partnering to build and test a prototype of a blockchain-based tool to allow traceability, transparency and accountability in tracking hazardous and dangerous goods. The project, funded by the Lloyd's Register Foundation, involves a consortium of stakeholders in the shipping industry, including ports, carriers, and technology and service providers. The demonstration project was set to run through September 2019 (Cleaner Seas, 2019).

### 3.4.2 Marine Transport International Limited (MTI) and SOLAS VGM

The IMO Verified-Gross-Mass (VGM) regulation, part of the SOLAS treaty (International Convention for the Safety of Life at Sea) requires that shippers report the VGM of containers to the appropriate terminal or carrier prior to loading onto a vessel. In response, Maritime Transport International (MTI) has been using SOLAS VGM, a blockchain-based digital ledger technology for processing information required under the VGM regulation, which will allow for information and records to be available for port officials, shippers, cargo owners, and other interested parties. (Czachorowski et al., 2019; DiGregorio & Nustad, 2017)

## 3.5 Certification

### 3.5.1 Maritime Blockchain Labs (MBL) Seafarer Certification

Maritime Blockchain Labs (MBL) and the Lloyd's Register Foundation established a consortium to pilot a seafarer certification system based on blockchain, which has the goal of streamlining and expediting the certification process through improved verification and access to seafarer certification documentation. The consortium involves many stakeholders with an interest in crew certification, including shipping companies such as Maersk, Heidmar, and PTC Holdings Corp, as well as technology and platform providers, and the international seafarer welfare organization The Mission to Seafarers. A demonstration will focus on end-to-end documentation of digital certification, as well as a repository for crew documentation, training logs, and approval (MI News Network, 2019; World Maritime News, 2018).

### 3.5.2 Port of Antwerp

The Port of Antwerp has partnered with Belfruco, Enzafruit, PortApp, 1-Stop and T&G Global to develop a blockchain application that will allow the transferring of documents such as certificates of origin and phytosanitary certificates, using smart contracts. A pilot project involves fruit shipped to the European market from New Zealand; using blockchain, digital phytosanitary certificates are transferred to the Belgian importer (Enzafruit), to the partner freight forwarder (Belfruco), and to the Belgian authorities before the cargo is released. Typically, these certificates are sent by mail via courier, which is far more costly both financially and in terms of time (MI News Network, 2018b).

## 3.6 Other Initiatives

### 3.6.1 Marine Insurance—EY, Guardtime, Maersk, Microsoft

Blockchain and smart contracts have been an area of interest for insurance companies to help improve customer experience, reduce operating costs, verify identification, etc. The marine insurance industry relies heavily on paper, and by exchanging documents electronically and automatically via blockchain and smart contracts, rather than processing manually, companies could reduce costs (Ganne, 2018). Oracles that collect real world data could be used for more complex cases (ex: weather could be treated as a trigger). In a distributed blockchain network, internal departments and third parties that need to review information could easily be given access to the documents. Sensitive customer data could be more secure on a blockchain, and insurance payments could be managed through cryptocurrencies or blockchain "wallets" (Gatteschi, 2018).

EY, Guardtime, Maersk and Microsoft, together with several insurance companies (ACORD, MS Amlin, Willis Towers Watson and XL Catlin), co-launched a blockchain platform for marine insurance. The platform, which was launched after a 20-week proof-of concept period, will support more than half a million automated ledger transactions and manage risk for over 1,000 commercial vessels in first year (MI News Network, 2019).

### 3.6.2 Shipbuilding and Registration—LR and Hyundai Heavy Industries (HHI)

Lloyd's Register and Hyundai Heavy Industries (HHI) are collaborating on a project to explore how blockchain may be applied to shipbuilding. LR also developed a prototype of a blockchain-enabled Class Register, which allows the registration of ships into Class.

### 3.6.3 Emissions Offsets

Though not specific to the maritime sector, several companies/initiatives such as Veridium Labs (partnered with IBM), CarbonX, Climatecoin, and Nori are introducing coins or certificates for carbon emissions offsets using blockchain technology.

# 4 Challenges for Blockchain in the Maritime Sector

The challenges discussed here are specific to the maritime sector, but are relevant to any agency from the local, state, and federal level when considering blockchains for energy and transportation issues (Winebrake et al., 2019).

## 4.1 Overview

Amidst the potential and promise of blockchain, and numerous small-scale or pilot-phase initiatives in the maritime sector, there are significant barriers to, and challenges surrounding, large-scale adoption in shipping. Barriers largely relate to the maritime culture, technological capabilities of stakeholders, and implementation costs. Challenges include energy use and security concerns, and the technological limitations and costs of blockchain technology and related system requirements.

## 4.2 Barriers to Adoption of Blockchain Technology Shipping

A 2018 study examined the barriers to digital innovation and the potential use of blockchain technology in the maritime industry, using a case study approach involving interviews with operators and suppliers and secondary research including company, industry, and media reports. The main barriers identified in the study included the high cost of implementation of blockchain technology, low quality of offshore internet access, the older age of decisionmakers, the culture, a lack of investment initiatives, the currently low use of blockchain in the supply chain, and aversion to risk (Gausdal et al 2018).

Others have noted that the transparency of blockchain systems, while offering potential benefits in the form of improved efficiency, may also serve as a barrier to the use of blockchain in shipping and trade, as some parties may view the transparency into their supply chain as undesirable, due to the desire to keep trade secrets, or to avoid criticism (e.g. the ability to view, on blockchain ledgers, details of specific factories where clothing is sourced may place firms under public scrutiny) (Botton, 2018).

## 4.3 Challenges Surrounding Adoption of Blockchain Technology in the Maritime Sector

Though blockchain offers potential benefits in several areas of shipping, there are also a number of significant challenges and concerns. These challenges include: security and reliability of data; energy consumption and resource use and associated emissions; storage, transaction speeds, and scalability; legal and regulatory (use of smart contracts); integration of data communications; and, “transaction” costs. (Reyna et al., 2018; Andoni et al., 2019).

We present these challenges and concerns to provide context and a balanced perspective surrounding blockchain initiatives in the maritime sector, and as a precursor to use cases and a more in-depth exploration of challenges and concerns, which will follow in a companion report.

### 4.3.1 Security and Reliability Concerns

Security concerns and vulnerabilities of the maritime sector have called for solutions to protect and secure data. Blockchain is often identified as improving security and reliability of data over traditional centralized databases, if not resolving or eliminating security and reliability concerns entirely (e.g. blockchain is presented as "trustless" and "immutable"). Recent real-world experiences, however, have shown system vulnerabilities and other concerns which demonstrate that systems relying upon blockchain face their own—sometimes significant—security and reliability challenges and consequences.

Theoretically, once validated and entered into open-source blockchain, data are immutable, which prevents against tampering with stored data. Blockchain systems, however, cannot ensure that data has not been tampered with or corrupted prior to being validated in the network. For example, if system sensors or networked devices fail, are faulty, or are tampered with—or if data are corrupted or incorrect for a number of other reasons—this incorrect data will then be stored in the blockchain (Reyna et al 2018). In the case of public permissionless blockchains, the flawed data or records would be immutable for practical purposes; in the case of private, permissioned blockchains, data are not immutable, and so can be changed—errors may be more easily corrected, but the at the expense of the confidence that any or all (correct) data have not been altered. These vulnerabilities may allow opportunities for fraud.

Blockchain systems are also more vulnerable to attacks and security risks than is typically imagined. Blockchains were largely considered to be "unhackable" but are now being hacked at an increasing rate (Orcutt 2019). In the first nine months of 2018, hackers stole nearly $1 billion from blockchain cryptocurrencies (Khatri, 2018); in the first quarter of 2019, over $1.2 billion was reportedly stolen (NewsBTC, 2019). Security concerns for open-source or public blockchains include the majority attack (or 51% attack), where a participant is able to control consensus by gaining more than half of computing power; such an attack reportedly took place on Ethereum Classic in January 2019, in which an estimated $270,000 to $1.1 million was stolen (Huillet, 2019; Orcutt 2019). Blockchain security vulnerabilities may also stem from code errors—an error in one line of code in Ethereum, for instance, led to the theft of $55 million in Ether currency, and eventually to the "hard fork" that split into Ethereum and Ethereum Classic (Leising, 2017).

Public blockchains are susceptible to additional security issues such as DoS attacks, or eclipse attacks where attackers isolate a node by monopolizing its connections, changing how the node sees the network (Reyna et al., 2018). Computing advancements could allow hackers to decipher digital signatures (Reyna et al., 2018); such attacks seem to be occurring in the Ethereum network, where certain accounts or wallets are being emptied almost as soon as money is deposited (Greenberg, 2019).

A computerized and distributed ledger is susceptible to vulnerabilities and bugs in particular if all participants do not install necessary software updates and security upgrades. In May 2019 more than half of all Bitcoin nodes were estimated to be vulnerable to the "inflation bug," while an estimated one third of Ethereum nodes were unpatched with a necessary security update, making the network more susceptible to a 51% attack (Avan-Nomayo, 2019; Palmer, 2019). As with traditional, centralized systems, security vulnerabilities of blockchain are constantly evolving, as are the responses and proposed solutions and patches to address these concerns; malicious efforts, in turn, are evolving to override these fixes. The cybercurrency firm BitPoint Japan, for instance, recently admitted: "We encoded our secret keys to make them unusable if they are stolen, but they were decoded" (NewsBTC, 2019).

### 4.3.2 Legal or Regulatory Concerns and Limitations of Smart Contracts

Smart contracts on blockchain have been suggested as one way to minimize or eliminate the current challenges and limitations to streamlined, efficient and effective transactions in the maritime sector, while also allowing for accessible records for all relevant parties. As envisioned, such smart contracts could offer an opportunity to streamline, and improve the efficiency and transparency of shipping transactions and contractual agreements, while reducing costs.

Smart contracts may therefore have the potential to facilitate progress in support of U.S. maritime capabilities, and innovation. Yet, if improperly implemented, smart contracts may also present challenges related to (or possibly counteract) these goals, given some of the limitations and challenges.

Blockchains cannot pull real world data from outside their network, so data must be provided by entities referred to as "oracles". Oracles are third-party services that feed required information onto the network. Types of oracles include: software oracles which provide information from an online source such as a website (e.g. weather conditions); hardware oracles which provide readouts from the physical world (e.g. when a vessel or container crosses a barrier); inbound oracles which introduce data from the external world (e.g. prices); outbound oracles, which have the ability to send data to the outside world (e.g. to unlock a smart lock once a payment has been received); and consensus oracles, where to improve security, a combination of a majority of oracles (e.g. 3 out of 5) are used (Blockchainhub 2019).

The practical application of smart contracts using oracles is not as simple as it may appear. Oracles must “sign” smart contracts in order for them to be executed/validated. To trust the validity of the smart contract, the oracle itself must be trusted, and so must be authenticated; the channel for data communication must also be secure. In order to manage the feeds by oracles and other interactions between the outside world and the blockchain, a trusted third-party entity is required; the addition of third-party oversight, however, diminishes decentralization. Smart contracts may also be overloaded in accessing several data sources (Reyna et al., 2018).

A smart contract may also be activated by blockchain transactions. For the smart contract to be executed in response to blockchain transactions, the necessary funds (e.g. currency, credits or tokens) must be stored on the blockchain. That is, a payment involving a cryptocurrency or credit (e.g. Bitcoin or tokens) can be executed if that currency or credit is native to that blockchain, and the blockchain can verify that the quantity of currency or credits are in the account; otherwise blockchain can neither guarantee nor enforce payment. Blockchain cannot execute terms of financial transactions involving fiat currency or other such payments— though blockchain can report and record that a transaction reportedly took place (Greenspan, 2016).

Blockchain cannot enforce smart contracts or any transactions involving resources outside of the blockchain (Reyna et al 2018); enforcement, if any, would require legal or regulatory intervention, or intervention by another such third-party authority. That is, while blockchains can show transfers or obligations of ownership or transactions, some sort of enforcement is required to ensure transfers of possession: “Blockchains can record obligations. Punishing those who default on their obligations is another matter.” (Abadi and Brunnermeier, 2019).

Traditional legal contracts (e.g. on paper, outside of code) often include clauses and conditions that aren’t readily quantifiable, and thus cannot be executed by smart contracts (Reyna et al., 2018). This is particularly the case in the maritime sector, where contracts tend to be unique and specific to the shipment or transaction, special contractual terms are often used, and certain aspects of transactions are typically handled commercially; maritime norms and features would need to be recognized and accounted for in blockchain (Joseph 2018). Currently no government or jurisdiction has implemented the use of blockchain for legal contracts in the maritime sector (Joseph, 2018). If and when governments decide to enforce blockchain contracts, a potential legal issue could arise: if a given blockchain splits through a hard fork (such as the hard fork of Ethereum that resulted in Ethereum and Ethereum Classic) and the forks disagree on the validity of contracts and transactions, then which contracts and transactions are enforceable? (Abadi and Brunnermeier, 2019).

Given some of the complexities of, and challenges with smart contracts, as of 2018 smart contracts had not been fully implemented outside of cryptocurrency transactions, and many proposed use cases of blockchain (e.g. in the energy sector) have been found to be infeasible in the near-to-mid-term.

Regulatory oversight (or lack thereof) presents a challenge in the maritime sector, both due to the potential legal implications and also in that it presents barriers to the adoption of blockchain. Parties justifiably perceive the use of blockchain as risky in the absence of regulatory oversight, and regulatory bodies see little impetus to engage or develop guidelines or standards, etc. when there is so little use of blockchain in the maritime sector (Botton, 2018).

### 4.3.3 Energy Consumption and Environmental Impacts of Blockchain

Blockchain may offer the potential to collect and store data on vessel fuel type, efficiency, and various other environmental attributes, which could enable measurement of progress toward goals of improved efficiency and reduced emissions in shipping, as well as facilitating enforcement of standards and regulations in these areas. Data collection and storage using blockchain technology, however, may come at a significant energy and environmental cost when considered on a lifecycle basis. The energy consumption of certain blockchain platforms and systems, and the associated emissions, therefore, have the potential to counteract strategic goals of minimizing environmental impacts in the maritime sector.

As of late August 2019, the Ethereum network, was estimated to consume 28 kWh per transaction (the equivalent of ~0.95 typical U.S. households' daily electricity consumption), with the entire network consuming 7.18 TWh annually (equivalent to the annual consumption of over 664,700 U.S. households) (de Vries 2019a). The Bitcoin network is estimated to consume 73 TWh of energy annually, producing an estimated carbon footprint equivalent to that of the entire nation of Denmark (de Vries, 2019b). Ethereum's energy use may be of particular interest as certain blockchain applications in the maritime sector currently use Ethereum. Additionally, energy consumption and emissions for certain applications in the maritime sector may be substantially higher than that of an average or typical Ethereum transaction, as complex transactions (such as those involving smart contracts) require far more computing power, or "gas" (Skvorc, 2018).

Private, permissioned blockchain platforms are far more efficient than open-source, public platforms, but come at the cost of decentralization, transparency, immutability, verification, and other attributes offered by public blockchain.

### 4.3.4 "Transaction" Costs

Blockchains have the potential to reduce or avoid transaction costs in the form of intermediary fees, time and processes, or other transactions costs associated with the status quo. But blockchains—and the equipment, devices, and other system elements required to use Blockchain—come with their own costs. These costs are highly variable, and in some cases quite significant. Blockchains themselves are currently expensive to develop: it is unclear whether the savings in transaction costs promised by blockchain will not be mostly offset—if not exceeded by—the cost of implementing blockchain in practice (Andoni et al., 2019).

Blockchain system costs include hardware, software, devices and equipment, training, and services and fees (such as smart contracts fees, the fee for the given application/service, blockchain platform transaction fees, or blockchain-as-a-service—where members pay for the use of blockchain nodes, writing data, storage, and which charge by the hour on an ongoing basis). Upfront costs and ongoing fees can reach hundreds to thousands of dollars per month for a relatively modest number of contracts and small amounts of data storage (e.g. $500/month for 25 users and 900 smart contracts annually; cost to store 1 kb of text on blockchain: $2.88; cost of blockchain network membership with 500 GB storage $1.93 per hour, indefinitely) (AWS, 2019; Monax, 2019; BitInfoCharts, 2019; Skvorc, 2018).

These costs, which do not include the costs of establishing a blockchain platform, or the devices and equipment necessary to do so, may be prohibitive in many applications, especially those involving large amounts of data. This was recently the case with a group of several organizations who were involved in funding and verifying carbon credit activities, and realized that the data storage requirements would be too expensive using blockchain; the groups opted to use blockchain for storage of key data elements only (which needed to be immutable), and used databases and other tools for other data. These costs may be particularly prohibitive for smaller companies and developing countries who may not have access to infrastructure or financial capital necessary to make these investments; yet, these are the very parties that blockchain is foreseen to help through reducing traditional transaction costs.

Then there is the issue of increased scale, which is typically assumed to lead to per-unit cost reductions with technological and computing advancements.  This may not apply with the use of blockchain technology, however—though certain devices or equipment may decline in cost, the overall costs of the system (and cost per transaction, etc.) may continue to increase, given that computing requirements, bandwidth, and energy requirements increase as the blockchain network size and processing requirements expand (Reyna et al., 2018; Andoni et al., 2019). So, the more that the network is used, the more expensive it could be.

The costs of establishing, using and maintaining a blockchain-based system are highly variable and depend upon the type of platform, the data and storage needs, the number of participants, and a number of other factors that would depend upon the application and use. Though they cannot be estimated on a broad, general, basis, these costs are important to consider in context, for each use case and application.

## 4.4 Technical Limitations of Blockchain

This section details challenges in applying blockchain technology which may limit its usefulness or feasibility in many potential or envisioned applications in the maritime sector.

### 4.4.1 Storage, Transaction Speeds, and Scalability

Blockchain is not designed to store large amounts of data, yet many of the proposed applications in the maritime sector—especially those related to the Internet of Things (IoT) will produce vast amounts of data and will require processing and storing that data on a continual basis, and over the long term.  This will require a great deal of processing speed and storage space, yet these are areas where blockchain technology (and public, permission-less blockchain in particular) is lacking. While IoT devices can generate GB of data in real-time, in 2018 an Ethereum full node (the entire copy of the ledger containing the history of transactions) was 46 GB in size (Reyna et al., 2018).

Blockchain processing speed is also much slower than traditional databases. Public, permission-less blockchains currently process a small number of transactions per second, compared to thousands of transactions processed per second by centralized databases. Ethereum processes an estimated ~15 transactions per second, with more complex transactions such as smart contracts processed at ~7 per second (Kasireddy, 2017). Queues also develop in response to a high number of pending transactions (MacManus, 2018), with Ethereum's pending transactions queue averaging several thousand transactions at an estimated wait time of 5 to 43 minutes, depending on transaction complexity (Etherscan, 2019);  Wait time per transaction for Bitcoin ranges from 10 minutes to several days (MacManus, 2018).

### 4.4.2 Integration of Data Communications.

The way data are currently communicated in energy systems also presents a challenge for integration with blockchain, as many energy systems currently rely on security protocols that are complex and require centralized authority of infrastructure (Reyna et al., 2018). Another challenge is the disparity between blockchain architecture requirements and IoT/smart devices or other systems, as blockchain requires powerful computers and capabilities of significant data storage far beyond those available in IoT or smart devices (Reyna et al., 2018).

# 5 Conclusion

Blockchains have been deployed across a range of including in maritime. The strengths and weaknesses of blockchains lie in their fundamental mechanics. Validation algorithms, immutable distributed ledgers, and automated smart contracts are appealing for many use cases, but security concerns around connecting blockchains to IoT and other applications, as well as high latency and poor storage can hamper blockchain applications.

It is impractical to make definitive recommendations as to whether blockchains represent an opportunity for maritime users as the technology is relatively nascent, and the array of possibilities and vulnerabilities is not yet fully understood. Interested parties should consider that given the uncertainties in costs, benefits, energy and resource use, security and privacy, and other key variables and potential consequences blockchains may not be appropriate in all applications.

A deeper understanding of the challenges and concerns and related potential ramifications and consequences of blockchain will be important for maritime stakeholders and partners to pursue in the context of each use case. The Use Case companion document to this report provides a deeper dive into specific use cases, and the benefits and challenges of employing blockchain to solve existing problems. Maritime stakeholders may benefit most understanding the risks and benefits included with integrating blockchains into existing regulatory frameworks; examining the extent of energy and environmental impacts of blockchain platforms; examining and better understanding the costs associated with blockchain; and, minimizing security risks of blockchain.

The possibilities blockchains offer are great, and the range of use cases is potentially broad, but it is important that stakeholders and interested parties consider the full suite of costs and benefits of blockchains before committing to the technology. An improved understanding of the potential benefits and pitfalls of blockchains will help stakeholders work towards optimal solutions to meet shared energy, environment and economic goals in the maritime sector.

# 6 References

Abadi, J. and Brunnermeier. M. (2019) Blockchain Economics. February 5, 2019. Princeton University Dept. of Economics. https://scholar.princeton.edu/sites/default/files/markus/files/blockchain_paper_v6j.pdf

Andoni, M., Robu, V. Flynn, D., Abram, S. Geach, D., Jenkins, D., McCallum, P. Peacock, A. (2019) Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews, Vol. 100, Pages 143-174, ISSN 1364-0321, https://doi.org/10.1016/j.rser.2018.10.014.

Avan-Nomayo, O. (2019, May 19). Inflation Bug Still a Danger to More Than Half of All Bitcoin Full Nodes. CoinTelegraph. https://cointelegraph.com/news/inflation-bug-still-a-danger-to-more-than-half-of-all-bitcoin-full-nodes

AWS (2019) Amazon Managed Blockchain pricing https://aws.amazon.com/managed-blockchain/pricing/ Accessed June 2019.

BitInfoCharts (2019) Ethereum Avg. Transaction Fee historical chart. BitInfoCharts. June 2019. https://bitinfocharts.com/comparison/ethereum-transactionfees.html

BlockchainHub (2019) Types of Oracles. https://blockchainhub.net/blockchain-oracles/ Accessed May 20, 2019.

Botton, Nicolas (2018) : Blockchain and trade: Not a fix for Brexit, but could revolutionise global value chains (if governments let it), ECIPE Policy Brief, No. 1/2018, European Centre for International Political Economy (ECIPE), Brussels https://www.econstor.eu/handle/10419/174812

Czachorowski, K., Solesvik, M. and Kondratenko, Y. in The Application of Blockchain Technology in the Maritime Industry, in V. Kharchenko et al. (eds.), Green IT Engineering: Social, Business and Industrial Applications, Studies in Systems, Decision and Control 171, https://doi.org/10.1007/978-3-030-00253-4_24

Cleaner Seas (2018a) BLOC and GoodFuels Marine Announce World's First Bunker Delivery Using Blockchain Tech. Cleaner Seas. September 19, 2018.

https://www.cleanerseas.com/bloc-and-goodfuels-marine-announce-worlds-first-bunker-delivery-using-blockchain-tech/

Cleaner Seas (2018b) Blockchain Has Won MIT Solve's Communities Challenge With Blockchain Shipping Emissions MRV Solutions. Cleaner Seas. October 13, 2018 https://www.cleanerseas.com/blockchain-has-won-mit-solves-communities-challenge-with-blockchain-shipping-emissions-mrv-solutions/

Cleaner Seas (2019) Blockchain Consortium Launched by Maritime Blockchain Labs and Rainmaking. Cleaner Seas. July 8, 2019. https://www.cleanerseas.com/blockchain-blockchain-consortium-launched-by-maritime-blockchain-labs-and-rainmaking-to-tackle-mis-declaration-of-dangerous-goods/

De Vries, A. (2019a) Ethereum Energy Consumption Index (beta). https://digiconomist.net/ethereum-energy-consumption. Accessed August 28, 2019.

De Vries, A. (2019b) Bitcoin Energy Consumption Index (beta). https://digiconomist.net/ethereum-energy-consumption. Accessed August 28, 2019.

Di Gregorio, R. & Nustad, S. (2017). Blockchain adoption in the shipping industry: A study of adoption likelihood and scenario-based opportunities and risks for IT service providers. M.S. Thesis, Copenhagen International Business School. https://www.researchgate.net/publication/323292747_Blockchain_Adoption_in_the_Shipping_Industry_A_study_of_adoption_likelihood_and_scenario-based_opportunities_and_risks_for_IT_service_providers

DiRenzo, J. Goward, D., Roberts, F. (2015) The Little-known Challenge of Maritime Cyber Security. Command, Control, and Interoperability Center for Advanced Data Analysis. http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberSecurityCorfu7-5-15.pptx.pdf

Etherscan (2019) Ethereum Pending Transactions Queue https://etherscan.io/chart/pendingtx

Ganne, E. (2018). Can Blockchain revolutionize international trade? World Trade Organization.

https://www.wto.org/english/res_e/booksp_e/blockchainrev18_e.pdf ISBN 978-92-870-4761-8

Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? Future Internet 2018, 10, 20. https://www.mdpi.com/1999-5903/10/2/20

Gausdal, A.H., Czachorowski, K.V, Solesvik, M. V. (2018) Applying Blockchain Technology: Evidence from Norwegian Companies. Sustainability. 10, 1985; doi:10.3390/su10061985

Greenberg, A. (2019) A 'Blockchain Bandit' Is Guessing Private Keys and Scoring Millions. Wired. April 23, 2019. https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys/

Greenspan, G. (2016, April 17) Why Many Smart Contract Use Cases Are Simply Impossible. Coindesk. https://www.coindesk.com/three-smart-contract-misconceptions Accessed May 2019.

Grimmer (2018). IMO 2020 Part 5: Enforcement. Stillwater Associates. https://stillwaterassociates.com/imo-2020-part-5-enforcement/

Hampstead, J.P. (2018) Swiss firm brings blockchain to the biopharmaceutical cold chain. FreightWaves. https://www.freightwaves.com/news/blockchain/skycellblockchaincoldchain

Hofer, L. (2019) Interview with Simone Accornero, CEO of FlexiDao. The BlockchainLand. https://theblockchainland.com/2019/02/18/interview-simone-accornero-ceo-flexidao/

Hui, K.Y.K. & Lui, John C.s & Yau, D.K.Y.. (2004). Small world overlay P2P networks. 201 - 210. 10.1109/IWQOS.2004.1309383. https://www.cse.cuhk.edu.hk/~cslui/PUBLICATION/small_world.pdf

Huillet, M.  (2019) Crypto Exchange Gate.io Confirms 51% Attack on Ethereum Classic, Promises Refunds. January 9, 2019. Cointelegraph. https://cointelegraph.com/news/crypto-exchange-gateio-confirms-51-attack-on-ethereum-classic-promises-refunds

ICSa (n.d.) The Principal Regulations Governing Maritime Safety International Chamber of Shipping

https://www.ics-shipping.org/shipping-facts/safety-and-regulation/the-principal-regulations-governing-maritime-safety

ICSb (n.d.) The Guidelines on Cyber Security Onboard Ships. International Chamber of Shipping.

http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

IMO (2017) MSC-FAL.1/Circ. Guidelines on Maritime Cyber Risk Management 35 July 2017

http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

IMO (2018) UN body adopts climate change strategy for shipping. International Maritime Organization.

http://www.imo.org/en/MediaCentre/PressBriefings/Pages/06GHGinitialstrategy.aspx

IMO (2019) Sulphur 2020 – cutting sulphur oxide emissions. International Maritime Organization,

http://www.imo.org/en/MediaCentre/HotTopics/Pages/Sulphur-2020.aspx

IMO (n.d.) Low carbon shipping and air pollution control. International Maritime Organization.

http://www.imo.org/en/MediaCentre/HotTopics/GHG/Pages/default.aspx

Joseph, N. (2018).Blockchain and the Maritime Industry: An introduction. Stephenson Harwood. March 2018. https://www.marinemoney.com/system/files/media/2018-03/Mr.%20Nijoe%20Joseph.PDF

Kasireddy, P. (2017) Blockchains don't scale. Not today, at least. But there's hope. Hackernoon. August 23, 2017. https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

Khan, M. A. & Salah, K. (2018). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems. Vol 82 pp. 395-411. https://doi.org/10.1016/j.future.2017.11.022

Khatri, Y. (2018) Nearly $1 Billion Stolen In Crypto Hacks So Far This Year: Research. Coindesk. https://www.coindesk.com/nearly-1-billion-stolen-in-crypto-hacks-so-far-this-year-research

Leising, M. (2017, June 13) The Ether Thief. Bloomberg. https://www.bloomberg.com/features/2017-the-ether-thief/

MacManus, R. (2018, February 28) Blockchain speeds & the scalability debate. Blocksplain. https://blocksplain.com/2018/02/28/transaction-speeds/

MARAD (2017) Maritime Administration Strategic Plan: Navigating the Future. 2017-2021. https://www.maritime.dot.gov/outreach/policy-papers-and-fact-sheets/2017-marad-strategic-plan

Mathews, L. (2017) NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million. Forbes.

https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#22a726a64f9a

Meyer, R. (2019) 300cubits, a Blockchain Shipping Pioneer, Gives up on its TEU Token. CoinDesk, October 4, 2019.

MI News Network (2018b) First Ever Blockchain-Based CargoX Smart B/l Successfully Completed Its Historic Mission. Updated August 24, 2018. https://www.marineinsight.com/shipping-news/first-ever-blockchain-based-cargox-smart-b-l-successfully-completed-its-historic-mission/

MI News Network (2018b) Port Of Antwerp Confirms Pioneering Role In The Field Of Innovation With Blockchain Based Document Workflow. MI News Network.

https://www.marineinsight.com/shipping-news/port-of-antwerp-confirms-pioneering-role-in-the-field-of-innovation-with-blockchain-based-document-workflow/

MI News Network (2019) 7 Major Blockchain Technology Developments In Maritime Industry In 2018. MI News Network. https://www.marineinsight.com/know-more/7-major-blockchain-technology-developments-in-maritime-industry-in-2018/ Updated on June 26, 2019

Monax (2019) How much does MONAX cost? https://monax.io/pricing/ Accessed June, 2019.

Muspratt, A. (2018) Guide to Temperature Controlled Logistics. PharmaLogisticsIQ August 23, 2018. https://www.pharmalogisticsiq.com/packaging-shipping-systems/articles/guide-to-temperature-controlled-logistics

NewsBTC (2019) Crypto Asset Thefts Top $1.2 Billion in Q1 2019, Report States.

https://www.newsbtc.com/2019/07/23/crypto-asset-thefts-top-1-2-billion-in-q1-2019-report-states/

Orcutt, M. (2019) Once hailed as unhackable, blockchains are now getting hacked. MIT Technology Review.https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

Palmer, D. (2019) Unpatched Ethereum Clients Pose 51% Attack Risk, Says Report. Coindesk. https://www.coindesk.com/unpatched-ethereum-clients-pose-51-attack-risk-says-report

Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M. (2018) On blockchain and its integration with IoT. Challenges and opportunities, Future Generation Computer Systems, Vol. 88, 2018, pp.173-190, ISSN 0167-739X, https://doi.org/10.1016/j.future.2018.05.046.

Saul, J. (2019) Factbox: IMO 2020 - a major shake-up for oil and shipping. Reuters. https://www.reuters.com/article/us-imo-shipping-factbox/factbox-imo-2020-a-major-shake-up-for-oil-and-shipping-idUSKCN1SN2BX

Skvorc (2018, May 24). Ethereum: How Transaction Costs are Calculated. SitePoint. https://www.sitepoint.com/ethereum-transaction-costs/ Accessed June 2019.

Sykes C. (2018). Time- and Temperature-Controlled Transport: Supply Chain Challenges and Solutions. P & T : a peer-reviewed journal for formulary management, 43(3), 154–170. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5821242/

Sofiev, M., Winebrake, J.J., Johansson, L. et al. (2018) Cleaner fuels for ships provide public health benefits with climate tradeoffs. Nat Commun 9, 406 (2018) doi:10.1038/s41467-017-02774-9

U.N. (2006) A Roadmap towards Paperless Trade. United Nations Economic Commission for Europe. ECE/TRADE/371.https://www.unece.org/fileadmin/DAM/cefact/publica/ece_trd_371e.pdf

Witherspoon, Z. (2017). A Hitchhiker's Guide to Consensus Algorithms. HackerNoon.

Winebrake, J., Carr, E., Green, E.. 2019. “Blockchain Technology: Opportunities and Challenges for New York’s Energy Sector: Part I – Blockchain Overview,” NYSERDA Report Number [draft submitted]. Prepared by Energy and Environmental Research Associates, LLC, Pittsford, NY. nyserda.ny.gov/publications

World Maritime News (2018). Maritime Industry Eyes Blockchain for Seafarer Certification. World Maritime News. December, 2018. https://worldmaritimenews.com/archives/266538/maritime-industry-eyes-blockchain-for-seafarer-certification/