sustainability

MDPI

Article

A Blockchain Prototype for Improving Electronic Seals on Container Shipping Operations

Wei Le [1], Adriana Moros-Daza [2], Maria Jubiz-Diaz [2,*] and Stefan Voß [1]

[1] Faculty of Business Administration, Institute of Information Systems, University of Hamburg, 20146 Hamburg, Germany; rakuraku1201@gmail.com (W.L.); stefan.voss@uni-hamburg.de (S.V.)
[2] Department of Industrial Engineering, Universidad del Norte, Km 5 Via Puerto Colombia, Barranquilla 081007, Colombia; amoros@uninorte.edu.co
* Correspondence: jubizm@uninorte.edu.co

Abstract: With the widespread use of electronic seals (e-seals), their traceability and security have attracted more and more attention. Moreover, the complexity of shipping operations and container handling justifies the use of technologies to ensure information security in the face of attacks. This work contributes a blockchain-based solution with a simulated prototype for improving electronic seals for containers on terminals in ports. An electronic seal was designed, and a blockchain prototype was constructed for a container data flow. The obtained results from the prototype were evaluated using performance tests. The security issues in the blockchain were also discussed from a strategic perspective based on game theory. Finally, the simulation concluded that the blockchain improves transaction efficiency. No studies were found that integrated blockchain technology with electronic seals. Therefore, this work intends to combine blockchain technology with e-seal to improve the security of transferred data due to its immutable nature.

Keywords: blockchain; electronic seal; game theory; container terminal; prototype simulation

Citation: Le, W.; Moros-Daza, A.; Jubiz-Diaz, M.; Voß, S. A Blockchain Prototype for Improving Electronic Seals on Container Shipping Operations. *Sustainability* **2023**, *15*, 11341. https://doi.org/10.3390/su151411341

Academic Editors: Jian Li, Zhou He, Yongwu Li and Bing Xia

Received: 28 March 2023
Revised: 5 May 2023
Accepted: 16 May 2023
Published: 21 July 2023

1. Introduction

Maritime transport has become a critical operation in supply chains, given its development and globalisation, especially for international trade. Containers handle approximately 90% of world commerce, which makes shipping operations affect the coordination among the actors involved in this industry [1]. Moreover, its low-cost and high-efficient service makes maritime transport very attractive. However, shipping engages many complex transactions with confidential information, and the operation intensity on container terminals is increasing. Therefore, the container shipping industry is usually threatened under high-risk conditions because of the lack of a central system for organising the whole transport chain [2]. This leads to the need for stricter requirements to achieve efficiency, speed, and safety of data transmission on container terminals. Several leading worldwide ports have implemented different technologies to improve their core competency. Mobile devices (apps), real-time monitoring, sensors, and electronic seal technology are applied to enhance handling processes and security issues.

An electronic seal (hereafter called e-seal) is most widely used for indicating tamper activities during container transport. E-seals serve as transponders to track shipments, ensure their integrity, and provide information about status, location, container content, and interactions. Therefore, they are electronic alternatives to mechanical container seals where a physical lock with an electronic device is located on the container's back door to communicate with the tracking system [3]. In other words, e-seals show potential benefits in streamlining container logistics within supply chains and automating certain decision-making processes at specific stages of the logistics process [4]. Although e-seals greatly support the detection of unauthorised attempts from malicious entities during container transport, they cannot resist unauthorised access but only prove and record the existence of

illegal intrusions that have occurred when e-seals are damaged or destroyed [5]. Therefore, sometimes it is hard to attribute an accurate time to when the tampering activity happened. For this reason, the traceability of the e-seal is a characteristic that should be strengthened for better data security.

Blockchain technology has been proposed as a solution to these concerns. It is a decentralised ledger system that can record and track transactions in a secure and transparent manner. Moreover, it is possible to create a tamper-proof record of the container's movements and status throughout the shipping process using blockchain to record the data from e-seals. Despite the great benefits of blockchain implementation, this technology has been mostly explored in theory for shipping operations. There is barely any structural simulation in real scenarios, and it is rarely addressed in the literature [6].

Hasan et al. [7] proposed a blockchain-based solution integrated with smart contracts to manage shipped containers of pharmaceutical goods. The smart containers were equipped with Internet of Things (IoT) sensors for tracking shipping conditions. The blockchain handles transactions among the stakeholders. Ref. [8] implemented IoT sensors with blockchain technology and smart contracts for transporting medical products. Komathy [9] proposed a framework to integrate blockchain in cargo shipping operations aiming to connect users with smart transactions and reduce delays. In addition, the transactions were validated to guarantee security and authenticity. Bauk [10] developed a conceptual framework of a blockchain for shipping management jointly with cryptocurrency payments, smart contracts, and cargo tracing using Radio Frequency Identification (RFID) technology.

The literature shows that blockchain implementation to maintain security in maritime operations and container handling is still in its infancy. Moreover, no studies have integrated blockchain technology with electronic seals. Therefore, this work intends to combine blockchain technology with e-seals to optimise the security of transferred data due to its immutable nature. The main contribution of this research is a novel blockchain prototype designed to enhance the performance of e-seals and improve security issues at container terminals. Furthermore, the following contributions are made:

- The assessment of the blockchain's impact on the performance of e-seals and the benefits of using blockchain technology for enhancing data transmission and overall efficiency.
- A detailed analysis of cyber-attack behaviours through different game theory scenarios, considering non-cooperative and cooperative games.
- Identify the insights on the potential implications of the blockchain prototype for the container terminal industry.

This paper is organised as follows. Section 2 outlines relevant research on improving security using blockchain and its differences from other technologies. Section 3 introduces the methodology for designing the e-seal and the blockchain prototype. Section 4 presents a test to analyse the prototype's performance, while Section 5 conducts a strategic analysis of security issues of the proposed blockchain based on game theory. Section 6 discusses the main findings and, finally, Section 7 concludes the study.

2. Related Background

Blockchain is becoming a technology that supports different methods for solving problems in various fields. For instance, blockchain reduces the high cost of transactions by preventing wilful fraud or theft in real-time monitoring [8,11]. Moreover, it protects digital copyright from plagiarism by offering decentralised validation authority and a piracy tracing system [12]. However, there are many other applications of blockchain, as summarised in Table 1 based on the literature review by Sunny et al. [13].

Table 1. Applications of blockchain technology.

Industry	Area
Transportation	Traffic conditions [14,15], payment systems [16], energy [17], data distribution [18–21]
IoT	Smart cities [22–24], industrial operations [25], supply chain operations [26,27], agriculture [28–32], smart contracts [33,34]
Finance	Banking [35], tourism [36], product traceability [32], trading [37,38], data administration [39]
Security	Healthcare [40], finance [41,42], Apps [43,44], automobile industry [45,46]
Government	Land property [47,48], certification and registration [49,50], voting [51–53]

For shipping operations, blockchain technology substantially improves all logistical processes from storage to payment, increases security and transparency, and speeds up the flow of goods [54,55]. In addition, blockchain involves different mechanisms to decrease the impact of cyber-attacks [1]. Jović et al. [1] provided the leading blockchain applications in the shipping industry. Maersk and IBM developed "Tradelens", a solution focused on improving provenance and transparency [56]. The platform aimed to reduce the cost and complexity of trading and the need for documentation [57]. In addition, it allowed the safe sending and signing of contracts, while the blockchain-based smart contract led to faster approvals and information processing. Another example is the platform for containerisation in shipping called "Global Shared Container Platform", developed by the company Blockshipping [58]. This technology is focused on providing transparency in operations that involve a large number of stakeholders. Further, CargoX introduced a Blockchain Documentation Transaction System to store encrypted data and exchange documents using smart contracts [59].

2.1. Comparative Analysis between RFID and Blockchain Technology

RFID technology has been widely adopted for improving the security of e-seals in container terminals [60,61]. However, it has limitations on security, as it is vulnerable to hacking and cloning. This highlights the need for a more secure and efficient solution, such as blockchain technology. While some authors may argue that using RFID on e-seals is comparable to using blockchain technology, it is suitable to note that there are significant differences between them. Table 2 outlines the differences between RFID and blockchain on e-seals.

Table 2. RFID vs. blockchain for e-seals.

Feature	RFID	Blockchain	References
Encryption	To secure data transmissions	To secure data transmissions	[60,61]
Authentication	Relies on access control based on a tag	Uses digital signatures for authentication	[60,62]
Physical security	Limited	High level of robustness	[63]
Vulnerability management	Very vulnerable to hackers	Relatively secure against hacks	[62,64]
Access controls	Limited to those with RFID readers	Flexible access controls	[61,63]
Audit trails	Limited audit trail capabilities	Robust audit trail capabilities	[62,64]
Physical environment	Susceptible to physical attacks and interference	Can be accessed from anywhere with an internet connection	[65]

RFID and blockchain have their strengths and weaknesses regarding the security of electronic seals of containers. Both RFID and blockchain technology use encryption to secure data transmissions. However, blockchain technology also uses digital signatures for authentication for an extra layer of security. Physical security is an important factor for electronic seals of containers. Blockchain technology offers a higher level of security compared to RFID. While RFID tags can be physically compromised, blockchain provides a distributed and decentralised system that is more difficult to tamper with.

Moreover, Table 2 shows that the two technologies must be updated with the latest security patches and firmware updates. Blockchain is relatively secure against hacks, whereas RFID is vulnerable to hacking and other security issues. On the other hand, RFID access is limited to those with RFID readers, while blockchain technology allows for flexible access controls, which can be beneficial in certain situations. Audit trails are essential for keeping track of all activities related to electronic seals, and blockchain technology provides robust audit trail capabilities, while RFID offers limited capabilities in this regard. The physical environment is also a factor, and while RFID can be susceptible to physical attacks and interference, blockchain can be accessed from anywhere with an internet connection, which can be a significant advantage in certain situations.

2.2. Comparative Analysis of Blockchain Developed Methods for E-Seal Prototypes

In recent years, the implementation of blockchain technology has gained significant attention in different industries, including logistics [18–21] . With its potential to enhance security, transparency, and efficiency in data management, blockchain technology has been explored in numerous logistics applications. Implementing an e-seal in containers requires a secure and reliable system that protects data transmission, ensures identity verification, and provides a robust solution for complex logistics operations. Therefore, the method used in this study for developing a blockchain prototype for an e-seal emphasises security, identity verification, and robustness, which are essential in the container logistics industry. Table 3 shows that, compared to other methods, blockchain stands out due to its emphasis on security, identity verification, and robustness.

Table 3. Advantages and disadvantages of blockchain development methods for e-seal prototypes.

Method	Description	Advantages	Disadvantages
Smart Contract Development	A programmable blockchain protocol that executes automated actions based on predefined conditions	Flexibility, transparency, automation	Complexity in developing and testing the smart contract code
Permissioned Blockchain	A blockchain network where access is restricted to authorised parties	Improved privacy, scalability, and performance	Lack of decentralisation, less secure than public blockchain
Tokenization	Physical or virtual assets as digital tokens on a blockchain	Improved liquidity, faster transactions, fractional ownership	Regulatory uncertainty, potential for fraud and hacking
Proof of Authority (PoA) Consensus Algorithm	A consensus algorithm where validators are selected based on their identity and reputation	Faster consensus, lower energy consumption	Centralisation and lack of resilience compared to Proof of Work (PoW)
Interoperability	A feature that allows different blockchains to communicate and share data with each other	Improved scalability, more efficient data sharing	Complexity in implementation, potential for security risks
This paper	Consortium-based blockchain with elliptic-curve (ECC) based e-seal scheme and PoW consensus algorithm	High security level, identity verification, robust e-seal scheme	Inefficiency and high energy consumption of PoW

While Smart Contract Development offers flexibility and automation, it is a complex way of developing/testing smart contract coding. Permissioned Blockchain provides improved privacy, scalability, and performance. However, it lacks decentralisation and is less secure than public blockchains. Tokenization offers improved liquidity and faster transactions but may face regulatory uncertainty and potential security risks. PoA consensus algorithm provides a faster consensus and lower energy consumption, but it is centralised

and less resilient. Finally, interoperability offers improved scalability and data sharing but can be complex to implement and may also pose security risks.

3. Methodology

Typically, an e-seal is installed on a container at the origin, and the seal's data is transmitted to a central system via a wireless connection. As the container moves through the supply chain, the e-seal's status is updated, and any attempts to tamper with or remove the seal are immediately detected and reported [3]. This information ensures that the container's contents remain within safe parameters and are undamaged during transit. However, it is usually threatened under high conditions because of the lack of security regarding hacking operations. Therefore, a blockchain prototype is designed to improve the security of e-seals. For developing this prototype, a methodology composed of four phases is proposed: (1) the design of the e-seal for the container transportation process; (2) prototype modelling based on Petri Net; (3) prototype simulation; and (4) analysis of performance tests.

3.1. Designing the E-Seal

The literature on container transport has shown different approaches for designing e-seals, from a physical device attached to the container door to an information protection method based on cryptography for sealing shipping documents. This study considers the implementation of an e-seal as a unique form of electronic signature based on cryptographic systems for securing data transmission. The potential impacts of implementing an e-seal are improved security for data transmission, faster processing of documents, cost and time savings, compliance with regulations, and improved transparency using real-time tracking [1,55,57]. A consortium platform with relevant stakeholders for handling the container operation on a terminal is determined. All the participating nodes are strictly required for identity verification when proceeding with their process. Therefore, each move of container transition on the terminal is considered a "transaction" under the blockchain. The transaction is protected by an asymmetric encryption system. Thus, every stakeholder of the blockchain consortium owns a pair of keys from a common protocol. Public keys are open to the public, while private keys are secret. Figure 1 shows a blockchain-based asymmetric encryption scheme.

Figure 1 shows that a digital digest from original container data using a hash function is generated and encrypted with the member's private key to create an electronically sealed document. The encrypted data is then packed into block data (note that a hash tree may also be called Merkle tree). The data can be obtained from the corresponding block in the blockchain, and the authenticity can be verified by decrypting with the pairing public key. In addition, it shows that the original data is hashed to obtain another digest and compared with the two digest sources to determine whether consistency could be reached. When conformity is achieved, the data are stated as not being interfered with.

3.2. Modelling the Prototype with Petri Nets

A container operation procedure can be modelled as a Petri net with a 4-tuple (P, T, I, O), where $P = (p_1, \ldots, p_m)$ is the set of m places and $T = (t_1, \ldots, t_n)$ is the set of n transactions on the seaport and container terminal. Each transaction t_i is a bridge linking two places (p_i, p_{i+1}). It is formulated from input I and output O functions, where $I \leftarrow P \times T$, $O \leftarrow T \times P$, and $P \cap T = \varnothing$. Figure 2 introduces a Petri net model with eight places ($m = 8$) and seven transactions ($n = 7$), i.e., $P = (p_1, \ldots, p_8)$ and $T = (t_1, \ldots, t_7)$.

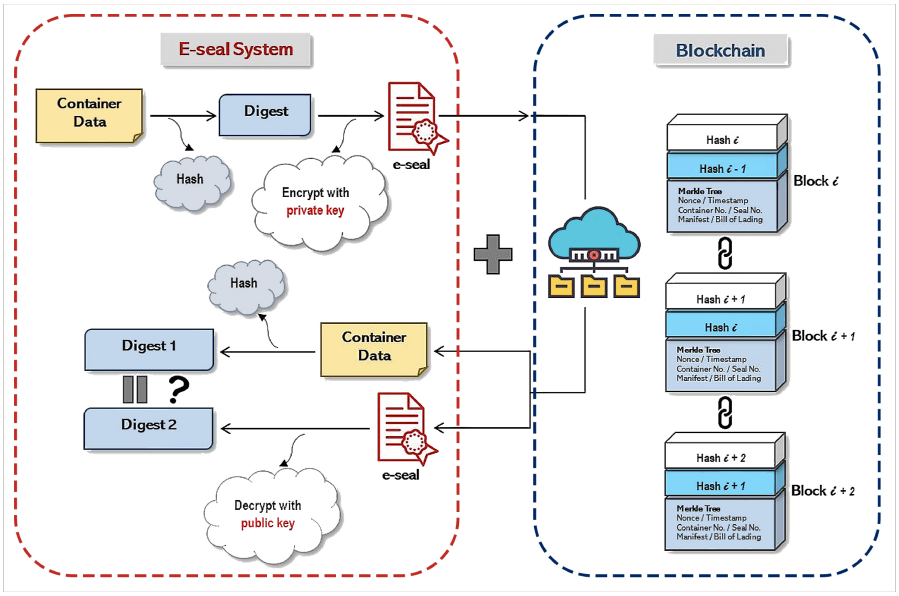


Figure 1. Description of the e-seal.

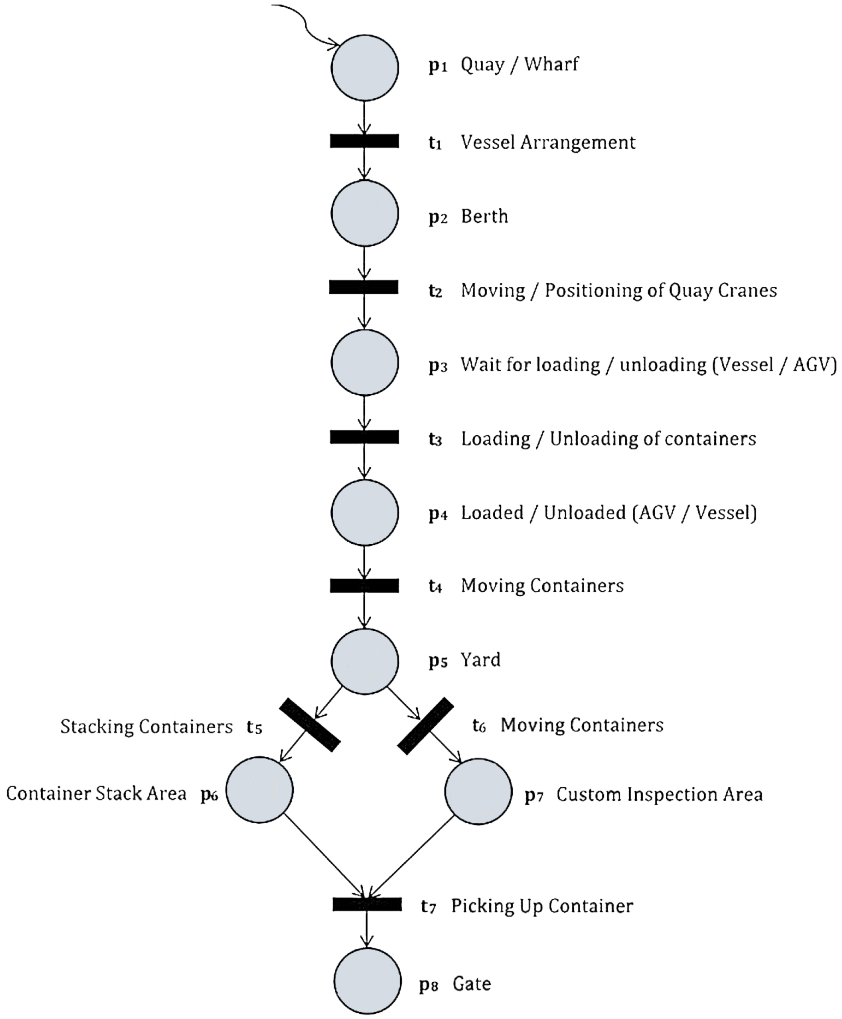


Figure 2. Flow chart of places and transitions on a terminal.

Each circle represents the location of the seaport or container terminal, i.e., the position where the container is in a stationary condition. The black bars between the circles are transactions, that is, the dynamic states of the container between two positions, such as handling, moving, or operating. As there is no extra third-party agency for issuing trustworthy credentials, the blockchain verifies the correctness and identification of the e-seals with the help of a decentralised organisational structure. Therefore, a standard operating procedure (SOP) is established for each following stakeholder to authenticate e-seals from the previous ones before proceeding current transaction with handling containers. Figure 3 presents the flow chart of the SOP for container handling on a terminal.

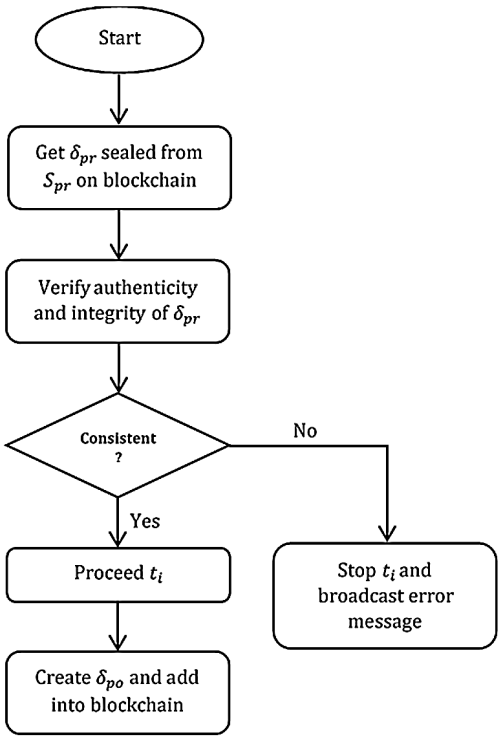


Figure 3. Flow chart of the SOP on a container terminal.

Let $t_i \in T$ be the current transaction, $S_{pr} \in S$ the previous stakeholder (referenced for current transaction t_i), $S_{po} \in S$ the following stakeholder (responsible for the current transaction t_i), δ_{pr} the sealed data from S_{pr}, and δ_{po} the sealed data from S_{po}. In this way, the integrity of the e-seals must be checked for all previous party(s) S_{pr} before proceeding to the next transaction for each following stakeholder S_{po}. The following transactions are organised after ensuring that the e-seals are functioning properly. Consequently, the necessary condition for implementing the next transaction is $I(t_{po}) = O(t_{pr})$, where $t_{pr} \in T$ is the previous transaction and $t_{po} \in T$ is the following one.

Then, a scenario under the framework of a container terminal was designed jointly with the Petri net and SOP. Table 4 defines eight relevant stakeholders related to container handling processes on a terminal. Every time the container moves, each transition t_i has two statuses—input/output (IN/OUT)—for describing the dynamic container transport and operation between stakeholders.

First, a vessel is approaching the destination port in a time, so t_1—ship's arrangement—is used as an example for a detailed analysis. For t_1, the previous stakeholder is the carrier (s_4) because the container is still loading onto the board. Therefore, the stakeholder behind t_1 is only s_4. In the next phase, the vessel arrives at the destination port and is ready to berth. The port authority (s_1) has to deal with the arriving ship, so s_1 is classified into the following parts. When s_1 starts to organise the ship's berthing, it sends instructions and communicates with the personnel on board. Therefore, the responsibility of t_2 must be

"the carrier" and "the port authority". With the analysis of the above two states, it is clear that the inbound and outbound stakeholders for t_1 are s_4 and s_1, s_4. Each location and its associated stakeholder can be assembled and organised. Due to the characteristics of the consortium blockchain, not all nodes are allowed to add new blocks or stakeholders, such as service providers or direct customers. For example, the stakeholder node s_5 does not allow adding new data to the blockchain without permission when t_4 "moves the container". However, it notifies the authorised node of s_2 to add its new sealed data.

Table 4. List of stakeholders and transactions.

	Stakeholder	t_1		t_2		t_3		t_4	
s_1	Seaport authority	IN	OUT	IN	OUT	IN	OUT	IN	OUT
s_2	Container terminal authority	s_4	s_1	s_1	s_2	s_2	s_2	s_2	s_5
s_3	Custom		s_4	s_4	s_7	s_7	s_5	s_5	
s_4	Carrier								
s_5	AGV service provider	t_5		t_6		t_7		t_8	
s_6	Trailer service provider	IN	OUT	IN	OUT	IN	OUT	IN	OUT
s_7	Quay crane service provider	s_5	s_2	s_5	s_3	s_2	s_2	s_3	s_2
s_8	Yard crane service provider		s_8		s_6	s_8	s_6	s_6	s_6

3.3. Prototype Simulation

Depending on the SOP of container handling on the terminal, a protocol was designed based on a combination of the e-seal system and blockchain fundamental elements. The prototype is divided into two segments: transaction (Algorithms 1 and 2) and block (Algorithm 3). Algorithm 1 defines the process for restricting and regulating the behaviour of stakeholders by transaction rules (i.e., smart contracts). The basic algorithm is described between two stakeholders that are handling a transaction. The KeyCreator generates a public–private key, which creates and verifies the e-seals.

Algorithm 1 Transaction (smart contract)

1: Let M be the container shipping data
2: $(pk, sk) \leftarrow$ KeyCreator (1^λ): a pair of public–private keys owned by each stakeholder and generated by KeyCreator with a security parameter (1^λ), $\lambda \in \mathbb{N}^*$
3: $\delta \leftarrow$ Hash(M): a digest generated from container data M using a hash function
4: $\sigma \leftarrow$ Seal(sk,δ): a randomised algorithm for sealing digest δ with sk and producing an e-seal σ
5: $b \leftarrow$ Verify(pk,σ,δ): a deterministic algorithm for verifying an e-seal σ with pk and comparing with digest δ. If $(\sigma, pk) = \delta$, $b = 1$; otherwise, $b = 0$
6: **if** $b = 1$ **then**
7: Proof [Verify(pk,Hash(M),Seal(sk,δ)) = 1] = 1
8: **else**
9: Consistency is not proved, stop process and broadcast error message
10: **end if**

Algorithm 2 is an extension of Algorithm 1, considering a transaction under multiple stakeholders by adding several sharing functionalities. That is, one of the parts of the transaction is composed of two or more stakeholders. The relevant stakeholders share a public key by holding their partial keys. Creating and verifying the e-seals should only be executed when the keys of all stakeholders are complete.

Algorithm 2 Transaction among multi stakeholders (smart contract)

1: Let M the container shipping data
2: $(pk, VK, SK) \leftarrow$ KeyCreator($params$,1^{λ}): an interactive protocol including up to p stakeholders $(s_1, s_2, \ldots, s_p)$ and $(p \in P)$ that generates a public verification key pk, a vector of partial verification keys $VK = (vk_1, vk_2, \ldots, vk_p)$, and a vector of partial secret keys $SK = (sk_1, sk_2, \ldots, sk_p)$ for each stakeholder with inputs of common public parameters $params$ and security parameter (1^{λ}), $\lambda \in \mathbb{N}^*$
3: $\delta_p \leftarrow$ Hash(M_i,p): a digest generated from container data (M_i) created from each stakeholder S_i with hash function. P is a set of up to p parties $\delta_P = \{\delta_i | \text{Hash}(M_i), i \in P\}$
4: $\sigma_i \leftarrow$ Share-Seal(sk_i,δ_P): a randomised algorithm for sealing hash digest δ_P with a secret key sk_i from each stakeholder S_i,$(i \in P)$ to produce a share-seal σ_i
5: $b_i \leftarrow$ Share-Verify(pk,VK,δ_P,σ_i): a deterministic algorithm for verifying each partial e-seal σ_i from each stakeholder S_i with his own verification seal vk_i and the public key pk. Comparing with digest δ_P, if $\prod_{i=1}^{p}(\sigma_i, pk) = \delta_P$, $i \in P$, $b = 1$; otherwise, $b = 0$
6: $\delta_P^{'} \leftarrow$ Hash(M_i,P): a digest generated from set of container data M_i from stakeholder S_i with a hash function, then $\delta_P^{'} = \text{Hash}\left(\sum_{i=1}^{p} M_i,\ i \in P\right)$
7: $(\sigma_p \cup \perp) \leftarrow$ Combine(pk,VK,σ_i,p): a full e-seal σ_P is generated from up to p stakeholders with their partial verification keys $VK = (vk_1, vk_2, \ldots, vk_p)$, share-seals σ_i and public keys pk. Otherwise, any of σ_i is ill-formed
8: $b_P \leftarrow$ Verify(pk,σ_P,$\delta_P^{'}$): a deterministic algorithm for verifying a full e-seal σ_P up to p stakeholders with public keys pk. Comparing with digest $\delta_P^{'}$, if $(\sigma_P$,$pk) = \delta_P^{'}$, $b = 1$; otherwise, $b = 0$
9: **if** $b_i = 1$ and $b_P = 1$ **then**
10: Proof [Share-Verify(pk,VK,Hash(M_i,p), Share-Seal(sk_i,δ_P)) = 1] = 1
11: Proof [Verify(pk,Combine(pk,VK,Hash(M_i,P))) = 1] = 1
12: **else**
13: Consistency is not proved, stop process and broadcast error message
14: **end if**

Algorithm 2 constructs the block data and blockchain configuration using Python as the programming language for the blockchain prototype. According to the hierarchical data structure, a set of parameters has been defined to characterise the fundamental construction of the block data and connect the created blocks into a chain-forming composition, namely "blockchain", as shown in Algorithm 3.

Algorithm 3 Block and blockchain

1: Class Block parameters: Block number (*block_num*), previous hash (*prev_hash*), original container data M (*data*), a number added to a hashed block used once (*nonce*), real time when block is created (*timestamps*), hash function used to generate digest (*hash*), public key from stakeholder that creates the block (*public_key*)
2: Use the hash function *get_hash* to generate digest from original data
3: Forage new block by executing the function loop once more until the process stops and a permitted hash digest (starts with '0000') with its corresponding *nonce* is generated
4: Class Blockchain - configuration
5: *_init_*: Initialisation of Class Blockchain
6: *add_block*: Add new block to blockchain
7: *block_dict*: Wrap the block data into container format that fits the output presentation (e.g., JSON)

Based on the above algorithms, the blockchain prototype can be implemented with the following steps:

1. Prepare the container's original data.

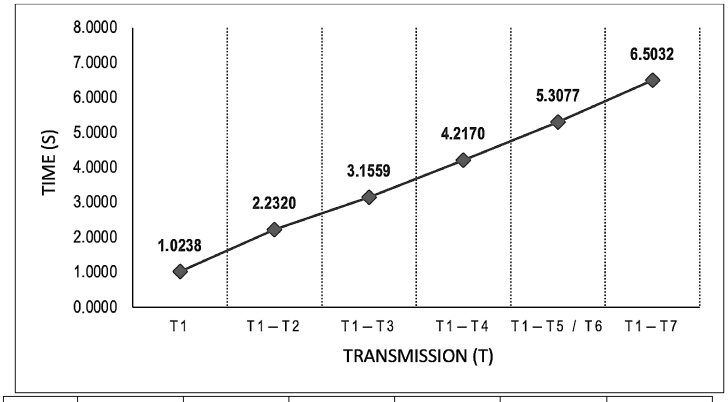
2. Construct the smart contract. Define a standard form for a transaction. For each operation (such as creating or verifying a transaction), all the structured data inside the transaction should be checked for validation. A transaction is composed of four elements:
    - The public key from the previous stakeholder to clarify the transaction or block creator.
    - Private key from the previous stakeholder to generate the e-seal for each transaction.
    - The public key from the following stakeholder to clarify the transaction data recipient.
    - Data package.
3. Generate public–private key pair with ECC encryption. Use a random function to create a private key and then generate a public key based on the private one. Save both keys as Privacy Enhanced Mail (PEM) files. The key length for applied encryption algorithms can be changed as needed.
4. Use the private key from the relevant stakeholders to generate a unique e-seal. The e-seal is composed of original data + hash digest and encrypted with the private key.
5. Verify the data for each transaction, taking the e-seal, original data, and a copy of the public key from relevant stakeholders. Then, use the public key to decrypt the e-seal, obtain the digest and compare it with another digest generated from the original data to see if they match up.
6. Define the basic block structure with the stated parameters.
7. Use the hash function to generate a digest from the original data, keeping rehashing until an allowed digest (starts with '0000') appears and stopping the process.
8. Wrap all the data into container format (JSON) for presenting results.
9. Define chain-formed configuration to extend the sequence of the following blocks, i.e., creating and chaining new blocks continuously. The main blockchain structure starts with an empty list, and it is filled with new foraged blocks later.
10. Establish the back-end web Application Programming Interface (API) and front-end client-server for running the prototype.

The results of the full implementation of the prototype are presented in Appendix A.

4. Performance Test

The prototype efficiency was tested by estimating the transmission time for each transaction (t_1 to t_7) and the whole process. The parameters for the simulation were the transmission time, number of stakeholders involved in the transaction, and key length for encryption. A number of Q transactions were conducted. The time per transaction corresponds to the time to complete each transaction, and the time for the process was calculated by adding up the transmission time per transaction (t_1 to t_7). The latter determines the efficiency of the blockchain prototype and identifies any areas that could be improved to optimise the performance.

It should be noted that the transmission time increases by about one second once the data is passed to the next stakeholder. Therefore, the time needed for each transaction is approximately one second. Consequently, the total transmission time throughout the container handling procedure at the terminal with blockchain technology in data transactions is $t_{NIST521p} \approx 6.5$ s for each container. With the NIST-256p or NIST-384p curves, the required transmission time is shortened, approximately $t_{NIST256p} \approx 2.5$ s and $t_{NIST384p} \approx 4.5$ s. The transmission time between all the transactions is shown in Figure 4.



T	T1	T1—T2	T2—T3	T3—T4	T4—T5/T6	T5/T6—T7
Δt (s)	1.0238	1.2082	0.9240	1.0611	1.0907	1.1955

Figure 4. Transmission time.

The findings show that blockchain technology significantly improves transaction efficiency compared to traditional systems. The estimated transmission time per transaction in the blockchain prototype is lower than the total transmission time for e-seal transaction systems with RFID technology for traditional container terminal systems. According to [3], the total transmission time for e-seal transaction systems with RFID technology is 6 min. Therefore, the simulation concludes that blockchain technology improves transaction efficiency.

5. Analysis of Scenarios

This section considers different scenarios based on game theory for analysing the security issues of the proposed blockchain. From a strategic perspective, it is assumed that the blockchain can provide a natural and appropriate environment to obtain Pareto optimality under the Nash equilibrium condition due to its specific features [66]. To prove the hypothesis, a non-cooperative game is introduced in Scenario 1 to illustrate the problems that can occur applying Proof of Work (PoW) as a consensus algorithm. By modelling the players' behaviour in a non-cooperative game, it is possible to identify the conditions that could lead to a suboptimal outcome, such as a double-spending attack. Then, a cooperative game is described in Scenario 2 to solve the issues of Scenario 1 because it is possible to achieve Pareto optimality with a game where the players have a shared goal. Moreover, no player can improve their outcome without making another player worse. Scenario 3 presents the Gambler's ruin theory as the theoretical basis for analysing the double-spending attacks that have occurred repeatedly in reality. Moreover, the relationship between the attacker's computing power and the probability that the attack could happen is studied. Then, it is possible to determine the minimum requirements needed to ensure blockchain security.

The blockchain has an inherently distributed knowledge system that satisfies the condition of complete information in the traditional economic theory. The complete information does not only exist on both sides of the transaction but among the entire players in the blockchain ecosystem. This feature considerably improves the condition of asymmetric information and enables players to make decisions that satisfy their interests and other players. Furthermore, all players have equal trading rights on the blockchain. In the theory of classical economics, rational individuals achieve optimality through free trading decisions. However, in real cases, the trading rights are mostly not equivalent, and an absolutely free trading environment is hardly achievable. Therefore, under the blockchain mechanism, both players handling the transaction have completed the same transaction data, and everyone can make decisions independently according to the in-hand information.

5.1. Scenario 1: Non-Cooperative Game

In the case of non-cooperative games, the preferred solution is to purchase more mining machines excavating longer blockchains, considering gaining profit under the PoW consensus algorithm. However, investing costs are also high at the same time. Hence, the method for solving this problem is still to build up a mining pool by recruiting a couple of miners, namely the centralisation of computing power. Each miner brings part of its computing power into the mining pool and receives a proportional reward after successful mining activities. This is described by Equation (1).

$$B_m = \left(\frac{CP_m}{CP_t}\right) \times B_t \tag{1}$$

B_m is the allocated reward of mining a new block for each miner, CP_m is the computing power of a miner, CP_t is the computing power of the blockchain network, and B_t is the reward of mining one new block. If each miner of the blockchain network reduces his own computing power to 50%, the B_m corresponds to Equation (2).

$$B_m = \left(\frac{0.5 \times CP_m}{CP_t}\right) \times B_t \tag{2}$$

Even if the computing power of each miner is lower, the reward for mining a new block will not increase because the ratio of the individual computing power of the network has not changed. Thus, the optimal strategy of one mining pool should be that everyone proportionally reduces his computing power and obtains the same rewards with less mining cost. However, this is impossible. Even if each miner in the network promises to reduce its computing power, a "traitor" may attempt to spend money to increase its computing power. The initial reward distribution is broken, and the "traitor" will launch a 51% attack on the blockchain system easier. In addition, it will pay less computing cost compared to the original attacking one. The described situation is a non-cooperative game. To obtain more rewards, miners choose to maximise their computing power as much as possible, i.e., by purchasing new machines as much as they can afford. This is the optimal strategy for each miner in the mining pool. However, once a "traitor" appears, all other honest miners would suffer huge losses. Therefore, the miners still choose to continuously increase their investment in computing power, i.e., their mining cost to reach the dominant strategy equilibrium [66]. Miners are "forced" to select their optimal strategy, but this optimal strategy is the worst for the mining pool, as the total mining cost is growing, but the mining rewards stay unchanged. Table 5 shows an example of a non-cooperative game with two miners, where $\varepsilon \geq 0$ is the increased computing power of each miner and $0 < x < 1$ is the adjusting parameter for fluctuation of the obtained mining rewards.

Table 5. Non-cooperative game.

Non-Cooperative Game		**Miner B**	
		↑ Computing Power	**− Computing Power**
Miner A	↑ computing power	$\left(\frac{CP_m+\varepsilon.x}{CP_t}\right) \times B_t$ / $\left(\frac{CP_m+\varepsilon.x}{CP_t}\right) \times B_t$	0 / $\left(\frac{CP_m+\varepsilon.x}{CP_t}\right) \times B_t$
	− computing power	0 / $\left(\frac{CP_m+\varepsilon}{CP_t}\right) \times B_t$	$\left(\frac{CP_m}{CP_t}\right) \times B_t$ / $\left(\frac{CP_m}{CP_t}\right) \times B_t$

The payoff matrix in Table 5 suggests that all miners are rational, each of them has two possible actions (increasing computing power or keeping computing power unchanged),

and their goals are to maximise the mining profits. Then, the following three different situations arise:

- Each miner chooses to "betray" others, i.e., increase his computing power privately. Then, each could gain the payoff with $\left(\frac{CP_m+\varepsilon.x}{CP_t}\right) \times B_t$ principally. The parameter $0 < x < 1$ is introduced to describe the fluctuation of mining rewards. The total computing power in the network is increased, but the reward for mining each new block is unchanged, so the shared reward for the individual should be less than the original payoffs.
- Only one miner betrays others; then, the "traitor" could gain the maximum profit $\left(\frac{CP_m+\varepsilon}{CP_t}\right) \times B_t$ when all other miners are honest. In this situation, honest miners gain nothing (0) because the "traitor" would be the first who mines the new block successfully with his computing power.
- All miners are honest. This is the ideal situation where the mining rewards are fairly and equally distributed to everyone with $\left(\frac{CP_m}{CP_t}\right) \times B_t$.

In this game, the dominant strategy equilibrium (Nash equilibrium) is the one that increases the computing power of each miner. According to Laffont and Maskin [67], a dominant strategy is an optimal move for a player regardless of other players' strategies. Thus, the dominant strategy for both players has the payoff $\left(\frac{CP_m+\varepsilon.x}{CP_t}\right) \times B_t$ for each miner.

5.2. Scenario 2: Cooperative Game

This scenario tries to solve the prisoner's dilemma of Scenario 1 by introducing new rules. A possible solution is to establish a smart contract between miners. Each one should mortgage a certain amount of deposit in advance for guaranteeing not to increase his computing power furtively. If everyone in the mining pool can obey the rules, the profit from teamwork should be greater than separate working from everyone, as the mining cost is allocated. Meanwhile, individuals should gain more benefits compared to working alone. Table 6 shows an example of a cooperative game with two miners, where $d > \left(\frac{CP_m+\varepsilon}{CP_t}\right) \times B_t$ is the mortgaged deposit from each miner according to the smart contract.

Table 6. Cooperative game.

Non-Cooperative Game		**Miner B**	
		↑ Computing Power	**− Computing Power**
Miner A	↑ computing power	$\left(\frac{CP_m+\varepsilon.x}{CP_t}\right) \times B_t - d$ / $\left(\frac{CP_m+\varepsilon.x}{CP_t}\right) \times B_t - d$	0 / $\left(\frac{CP_m+\varepsilon.x}{CP_t}\right) \times B_t - d$
	− computing power	$\left(\frac{CP_m+\varepsilon}{CP_t}\right) \times B_t - d$ / 0	$\left(\frac{CP_m}{CP_t}\right) \times B_t$ / $\left(\frac{CP_m}{CP_t}\right) \times B_t$

The payoff matrix shown in Table 6 introduces a new parameter d into a smart contract for representing the deposit mortgaged from each miner in the mining pool, and it should be greater than the maximal mining rewards $\left(\frac{CP_m+\varepsilon}{CP_t}\right) \times B_t$ to restrain miners' behaviours more effectively. If any miner does not keep the promise, his deposit should be destroyed as a punishment. The losses for betraying others are much higher than mining rewards by privately increasing his computing power. Thus, the Nash equilibrium in Scenario 1 is broken. The best new strategy changes to decide that all miners should be honest, i.e., keeping their computing power unchanged for gaining the best payoff $\left(\frac{CP_m}{CP_t}\right) \times B_t$ for each one of them. In addition, the Pareto optimality is achieved as there is no better option to improve either of the players while keeping the payoff of another one

unchanged. Consequently, the original non-cooperative game is successfully turned into a cooperative game.

5.3. Scenario 3: Gambler's Ruin Theory

The Gambler's ruin theory states that if a gambler divides his money into n parts for gambling in a casino, his chances of winning or losing the gambling are one-half. If this gambling game is infinite, the gambler will finally lose all his money. This scenario is very similar to a blockchain attack. If the chain has already been mined by honest miners with n blocks and the chain from an attacker has m blocks, then $d = n - m$ is the times of the gambling game between attackers and honest miners. Once the honest miners have lost all the chances within d times because the attacker's mine has the same or more blocks than the honest miners, the computing power will automatically be transferred to the new fake chain, and the attacker wins the game. Figure 5 shows an example of a gambling game.

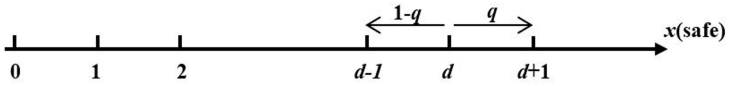


Figure 5. Gambling game in a blockchain attack.

The gambling game begins from the starting point p_1. Set $P_{(1)}$ as the probability of $p_1 \rightarrow p_0$, $P_{(2)}$ as the probability of $p_2 \rightarrow p_0, \ldots,$ $P_{(d)}$ as the probability of $p_d \rightarrow p_0$. Two possible events could happen at each time of the game, i.e., left moving with probability $(1 - q)$ or right moving with probability q. Moving left means the attackers have won and mined a block while moving right means the winners are honest miners. Then, the probability at p_1 can be calculated using Equation (3).

$$P_{(1)} = (1 - q) + q \times P_{(2)} \tag{3}$$

Analogue to p_1, the probability at p_2, i.e., $p_2 \rightarrow p_0$, is calculated considering two moves to the left, which is equal to duplicating the moving $p_1 \rightarrow p_0$ as shown in Equation (4).

$$P_{(2)} = P_{(1)}^2 \tag{4}$$

Combining Equations (3) and (4) and solving for $P_{(1)}$, Equation (5) is obtained as follows.

$$P_{(1)} = 1 - q + q \times P_{(1)}^2 \quad \therefore \quad P_{(1)} = \frac{1 - q}{q} \text{ or } P_{(1)} = 1 \tag{5}$$

If $q \leq 0.5$, then $P_{(1)} \geq 1$, the attack must be successful when the computing power of attackers reaches 50% of the entire network. If $q > 0.5$, attackers could not catch up to honest miners within a d-time gambling game. When the game is repeated infinite times ($d \rightarrow \infty$), the probability $P_{(d)}$ from $p_d \rightarrow p_0$ is getting close to 0.

A double-spending attack means that attacker A sends virtual currency to another account B (A $\rightarrow$ B) while sending the same amount to himself (A $\rightarrow$ A). After temporarily mastering more than 51% of the network's computing power, the attacker can pre-emptively create a longer, forged blockchain with a fake transaction. Since it is very difficult and meaningless to modify electronically signed or sealed transaction data in a block, the attacker will try to bypass the defence of the electronic seal/signature and adopt a more direct attacking method [68].

Set honest miners master q computing power of the whole blockchain network, and an attacker has $(1 - q)$ computing power. According to the protocol, during the period t of waiting for n blocks on the main chain to be created and confirmed, the transactions wrapped in before n blocks are recognised to be valid. The attacker has falsified the transaction and started to mine forged chains with m fake blocks. Figure 6 presents an example of a double-spending attack.

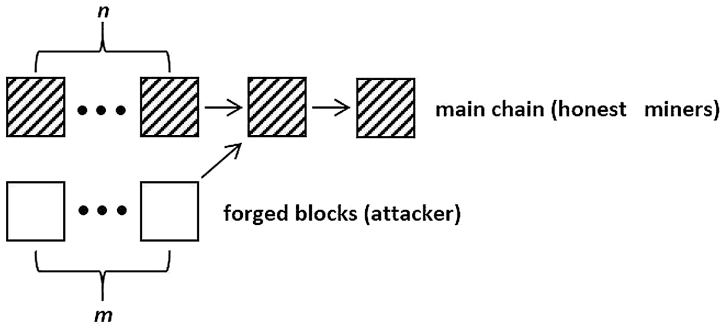


Figure 6. Double-spending attack.

Two situations could happen according to the above model: (1) $m > n$ and (2) $m \leq n$.

- Case 1: $m > n$. The attacker has mined more blocks than honest miners, so the forged chain is recognised to be valid and becomes the new main chain. Set λ as the expected value that the attacker mined a new block with $(1 - q)$ computing power within the period while honest miners mine n blocks on the main chain. It can be calculated as shown in Equation (6).

$$\lambda = n\left(\frac{1-q}{q}\right) \tag{6}$$

Then, the probability that the attacker could catch up to the honest miners with one more block and successfully forge the new blockchain, according to a Poisson distribution, is shown in Equation (7).

$$P_{(i)} = \sum_{m=n+1}^{\infty} \frac{\lambda^m e^{-\lambda}}{m!} \tag{7}$$

- Case 2: $m \leq n$. The attacker keeps selfish mining until his forged chain is longer than the main chain. Thus, the potential probability is calculated as shown in Equation (8).

$$P_{(ii)} = \sum_{m=0}^{n} \frac{\lambda^m e^{-\lambda}}{m!}\left(\frac{1-q}{q}\right)^{(n-m)} \tag{8}$$

Combining Equations (7) and (8), the probability that the attacker could catch up to honest miners is computed as shown in Equation (9).

$$\begin{aligned} P_{win} &= P_{(i)} + P_{(ii)} = \sum_{m=n+1}^{\infty} \frac{\lambda^m e^{-\lambda}}{m!} + \sum_{m=0}^{n} \frac{\lambda^m e^{-\lambda}}{m!}\left(\frac{1-q}{q}\right)^{(n-m)} = \\ P_{win} &= 1 - \sum_{m=0}^{n} \frac{\lambda^m e^{-\lambda}}{m!} + \sum_{m=0}^{n} \frac{\lambda^m e^{-\lambda}}{m!}\left(\frac{1-q}{q}\right)^{(n-m)} = 1 - \sum_{m=n+1}^{\infty} \frac{\lambda^m e^{-\lambda}}{m!}\left(1 - \frac{1-q}{q}\right)^{(n-m)} \end{aligned} \tag{9}$$

Several experiments were conducted to analyse the behaviour of the probability. Values of $1 - q \leq 0.5$ are calculated and observed under the circumstances where the attacker still can catch up with honest miners and successfully achieve the attack. Table 7 shows the obtained results.

When the attacker controls 10–30% of the computing power, and the honest miners have already mined more than five blocks than the attacker, the expected value from the latter is minus, and the system is safe. Similarly, if the attacker has reached 40% of the computing power, the situation becomes more dangerous, and the number of blocks that need to be confirmed should not be less than six. Moreover, when the attacker has more than 40% to nearly 50% of the computing power, the number of blocks that need to be confirmed soars to seventy-one, which could still ensure the system's security. Finally, if

the attacker controls 50% of the computing power, no matter how many blocks the honest miners have mined before, the attacker wins the game eventually.

Table 7. Probability of double-spending attack.

$1-q$	n	λ	Probability
0.1	1	9.00	1.00000
	2	18.00	0.84183
	3	27.00	0.51642
	4	36.00	0.05349
	5	45.00	−0.52254
0.2	1	4.00	1.00000
	2	8.00	0.77255
	3	12.00	0.30252
	4	16.00	−0.33931
0.3	1	2.33	1.00000
	2	4.67	0.79214
	3	7.00	0.37617
	4	9.33	−0.16651
0.4	1	1.50	1.00000
	2	3.00	0.88285
	3	4.50	0.66918
	4	6.00	0.41211
	5	7.50	0.14265
	6	9.00	−0.12692
...	...	...	...
0.49	70	72.86	0.00306
	71	73.90	−0.01282
...	...	...	...
0.5	10,000	10,000.00	1.00000

6. Discussion

As shown above, the development and implementation of blockchain for containers involve certain features that determine its performance. The evaluation of the practical effectiveness of the proposed model was based on the obtained results from the analysis of different scenarios in which an attacker controls a certain percentage of computing power. They showed that the proposed model ensures the system's security under certain conditions.

When the attacker controls between 10% and 30% of the computing power, and the honest miners have already mined more than five blocks than the attacker, the expected value from the attacker is negative, and the system is considered safe. However, when the attacker reaches 40% of the computing power, the situation becomes more dangerous, and the number of blocks that need to be confirmed should not be less than six. When the attacker has more than 40% and almost 50% of the computing power, the number of blocks that need to be confirmed has soared to 71, which can still ensure the system's security. However, when the attacker controls 50% of the computing power, no matter how many blocks the honest miners have mined before, the attacker wins the game eventually.

Regarding the features of the proposed prototype, ECC was chosen as the cryptographic algorithm for building the e-seal scheme. This provides stable and robust results, i.e., high consistency with shorter key length. However, ECC cannot be widely used without effective standardisation due to the complexity of selecting the proper elliptic curves under various conditions in practice and the difficulty in developing a set of universal standards. On the other hand, the consensus mechanism applied was PoW. It is considered the most classic and simplest method for practical implementation. Nevertheless, PoW is not sustainable for long-term use from long-standing strategic plans. PoW is particularly

flawed not only because of being inefficient but also consuming huge amounts of computing power generated from energy resources. This increases the operation cost. In addition, the drawback is aggravated by massive annual throughput and transaction volume in the container logistics industry and the intensive container handling process on terminals. For a public blockchain, the greater the required operation cost, the higher the security level the blockchain will have, i.e., it is more difficult to falsify the blockchain. The results highlight that the public blockchain cannot avoid 51% of the attacks under the PoW mechanism. Computing power plays a crucial role in the intermediary of transmission, expressing the true mechanisms. However, some measures can reduce the attack risk. An example is keeping the computing power scattered, as it is the principal cause of 51% of the attacks. Moreover, the cohesion of computing power is the most effective way to gain profits. On the other hand, establishing several early-warning mechanisms or systems is another way to reduce the adverse consequences of 51% of attacks. Blockchain-based trading platforms can take appropriate defensive measures to avoid further losses. The performed analysis suggests that blockchain technology in the container logistics industry can significantly reduce the time and cost of delivering paper documents. It usually takes days up to weeks and is more likely to be lost or damaged in practice. Using only the e-seal, an additional trusted third-party certification authority is necessary to issue credentials for certifying the authenticity of e-seals or signatures each time. Therefore, blockchain technology guarantees immutability, confidentiality, and traceability back to the original data source, making it a more secure and efficient solution for identification or authentication, especially when combined with electronic seal or digital signature technology. The transaction time per container is approximately 6 min when using RFID technology and 6.503 s when using blockchain technology. Therefore, blockchain can significantly reduce transaction time per container. The proposed prototype was tested in the Port of Hamburg, which managed 8.3 million TEU in 2022. The results showed that if container handling uses the technology developed in this study, a reduction in transaction time from 873,000 h to 94,619 h can be achieved. This means a decrease of 89% of the total time per transaction per container [69]. The model improves scalability and sustainability in container logistics by reducing the time and resources required to process transactions and increasing the transparency and security of the system. A blockchain-based solution deletes the need for intermediaries and paper-based documentation, reducing costs and increasing efficiency. Furthermore, smart contracts automate the execution of contracts and reduce the need for manual intervention. The proposed prototype reduces paper waste and carbon emissions by decreasing the need for intermediaries and paper-based documentation. Additionally, the increased transparency and security of the system could reduce the risk of fraud and improve trust between different parties in the logistics chain [55].

7. Conclusions

This paper develops a solution based on blockchain and electronic seal technology for improving security problems at container terminals on ports. The e-seal was designed as a digital signature based on cryptography. In addition, Petri Nets were applied to model the prototype and simplify the container operation process on a terminal. Next, the container operation procedures were standardised, i.e., setting up an SOP, and three algorithms were proposed to describe the core structure of the prototype. Performance tests were conducted to estimate the prototype's efficiency. The results concluded that each transaction needs around one second using the ECC NIST-521p curve. The total duration of a run-through of the prototype was approximately $t_{NIST521p} \approx 6.5$ s. Moreover, the efficiency of data transactions on container terminals is higher with the employment of blockchain. Therefore, the blockchain accelerates the entire data transmission time within the interactive communication cross-platform.

Some scenarios were designed to analyse blockchain behaviour and explore security issues based on non-cooperative games, cooperative games, and Gambler's ruin theory. The results showed that a blockchain could be safe when the attacker controls his computing

power under 50% of the total computing power. Therefore, it is critical to avoid the centralisation of computing power by, for example, building a warning system for detecting any trend of increasing computing power effectively.

Finally, future research should consider other external factors that affect the proposed models. For example, in the non-cooperative game model, it was considered that by increasing computing power the mining activity would be more profitable. However, other factors may strongly affect mining rewards, e.g., the increase in electricity cost or the decrease in the market value of the virtual currency could make the gain less than the cost, which leads to negative mining rewards. In addition, preventing double-spending attacks from blockchain systems must be included, even in simulated environments. Therefore, further research is required to focus on finding solutions that possibly predict the suspicious signals of attempting attack activities, namely building an early warning system to enhance the security level of blockchain.

Author Contributions: Conceptualization, A.M.-D. and S.V.; Methodology, W.L.; Software, W.L.; Validation, W.L.; Formal analysis, A.M.-D. and M.J.-D.; Writing—review & editing, M.J.-D.; Supervision, A.M.-D. and S.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. The APC was funded by Universidad del Norte.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Appendix A

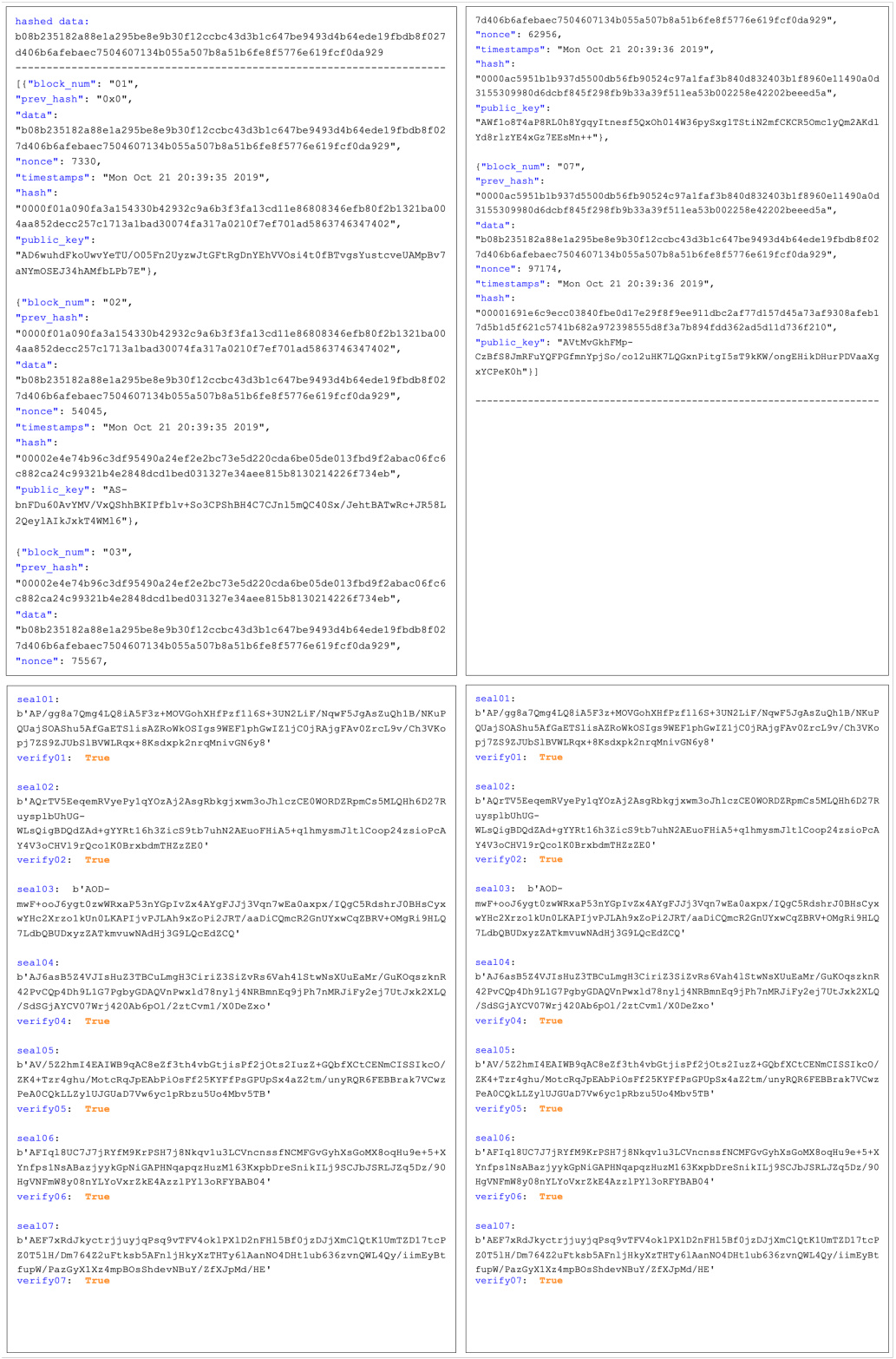


Figure A1. Proposed prorotype.

References

1. Jović, M.; Filipović, M.; Tijan, E.; Jardas, M. A review of blockchain technology implementation in shipping industry. *Pomorstvo* **2019**, *33*, 140–148. [CrossRef]
2. Maritime Transport Committee. *Container Transport Security across Modes*; ECMT/OECD: Paris, France, 2005.
3. McCormack, E.; Jensen, M.; Hovde, A. Evaluating the Use of Electronic Door Seals (E-Seals) on Shipping Containers. *Int. J. Appl. Logist. (IJAL)* **2010**, *1*, 13–29. [CrossRef]
4. Daschkovska, K. Decision Support in Supply Chains Based on E-Seals Secure System. *IFAC-PapersOnLine* **2017**, *50*, 14224–14229. [CrossRef]
5. Johnston, R.G. *Tamper-Indicating Seals: Practices, Problems, and Standards*; Technical Report; Los Alamos National Laboratory (LANL): Los Alamos, NM, USA, 2003.
6. Dib, O.; Brousmiche, K.L.; Durand, A.; Thea, E.; Hamida, E.B. Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun.* **2018**, *11*, 51–64.
7. Hasan, H.; AlHadhrami, E.; AlDhaheri, A.; Salah, K.; Jayaraman, R. Smart contract-based approach for efficient shipment management. *Comput. Ind. Eng.* **2019**, *136*, 149–159. [CrossRef]
8. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777.
9. Komathy, K. Verifiable and authentic distributed blockchain shipping framework for smart connected ships. *J. Comput. Theor. Nanosci.* **2018**, *15*, 3275–3281. [CrossRef]
10. Bauk, S. Blockchain conceptual framework in shipping and port management. In Proceedings of the Maritime Transport Conference, Barcelona, Spain, 27–29 June 2022.
11. Casado-Vara, R.; Prieto, J.; Corchado, J.M. How blockchain could improve fraud detection in power distribution grid. In Proceedings of the 13th International Conference on Soft Computing Models in Industrial and Environmental Applications, San Sebastian, Spain, 6–8 June 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 67–76.
12. Purba, R.; Yunis, R. Application of Blockchain technology to prevent the potential of plagiarism in scientific publication. In Proceedings of the 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, 16–17 October 2019; pp. 1–5.
13. Sunny, F.A.; Hajek, P.; Munk, M.; Abedin, M.Z.; Satu, M.S.; Efat, M.I.A.; Islam, M.J. A systematic review of blockchain applications. *IEEE Access* **2022**, *10*, 59155–59177. [CrossRef]
14. Hîrţan, L.A.; Dobre, C.; González-Vélez, H. Blockchain-based reputation for intelligent transportation systems. *Sensors* **2020**, *20*, 791. [CrossRef]
15. Li, Y.; Ouyang, K.; Li, N.; Rahmani, R.; Yang, H.; Pei, Y. A blockchain-assisted intelligent transportation system promoting data services with privacy protection. *Sensors* **2020**, *20*, 2483. [CrossRef]
16. Pournader, M.; Shi, Y.; Seuring, S.; Koh, S.L. Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *Int. J. Prod. Res.* **2020**, *58*, 2063–2081. [CrossRef]
17. Chaudhary, R.; Jindal, A.; Aujla, G.S.; Aggarwal, S.; Kumar, N.; Choo, K.K.R. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. *Comput. Secur.* **2019**, *85*, 288–299. [CrossRef]
18. Lei, A.; Cruickshank, H.; Cao, Y.; Asuquo, P.; Ogah, C.P.A.; Sun, Z. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet Things J.* **2017**, *4*, 1832–1843. [CrossRef]
19. Astarita, V.; Giofrè, V.P.; Mirabelli, G.; Solina, V. A review of blockchain-based systems in transportation. *Information* **2019**, *11*, 21. [CrossRef]
20. Fu, Y.; Zhu, J. Operation mechanisms for intelligent logistics system: A blockchain perspective. *IEEE Access* **2019**, *7*, 144202–144213. [CrossRef]
21. Mukherjee, B.K.; Pappu, S.I.; Islam, M.J.; Acharjee, U.K. An SDN based distributed IoT network with NFV implementation for smart cities. In Proceedings of the Cyber Security and Computer Science: Second EAI International Conference, ICONCS 2020, Dhaka, Bangladesh, 15–16 February 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 539–552.
22. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustain. Cities Soc.* **2020**, *63*, 102364. [CrossRef]
23. Zhang, W.; Wu, Z.; Han, G.; Feng, Y.; Shu, L. Ldc: A lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications. *Future Gener. Comput. Syst.* **2020**, *108*, 574–582. [CrossRef]
24. Vivekanandan, M.; U, S.R. BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 403–419. [CrossRef]
25. Rahman, A.; Sara, U.; Kundu, D.; Islam, S.; Islam, M.; Hasan, M.; Rahman, Z.; Nasir, M.K. Distb-sdoindustry: Enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture. *arXiv Preprint* **2020**, arXiv:2012.10011.
26. Rožman, N.; Corn, M.; Požrl, T.; Diaci, J. Distributed logistics platform based on Blockchain and IoT. *Procedia CIRP* **2019**, *81*, 826–831. [CrossRef]
27. Musamih, A.; Salah, K.; Jayaraman, R.; Arshad, J.; Debe, M.; Al-Hammadi, Y.; Ellahham, S. A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access* **2021**, *9*, 9728–9743. [CrossRef]

28. Lin, J.; Shen, Z.; Miao, C. Using blockchain technology to build trust in sharing LoRaWAN IoT. In Proceedings of the 2nd International Conference on Crowd Science and Engineering, Beijing, China, 6–9 July 2017; pp. 38–43.
29. Lin, J.; Shen, Z.; Zhang, A.; Chai, Y. Blockchain and IoT based food traceability for smart agriculture. In Proceedings of the 3rd International Conference on Crowd Science and Engineering, Singapore, 28–31 July 2018; pp. 1–6.
30. Awan, S.H.; Ahmed, S.; Nawaz, A.; Sulaiman, S.; Zaman, K.; Ali, M.Y.; Najam, Z.; Imran, S. BlockChain with IoT, an emergent routing scheme for smart agriculture. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 420–429. [CrossRef]
31. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
32. Westerkamp, M.; Victor, F.; Küpper, A. Tracing manufacturing processes using blockchain-based token compositions. *Digit. Commun. Netw.* **2020**, *6*, 167–176. [CrossRef]
33. Zorzo, A.F.; Nunes, H.C.; Lunardi, R.C.; Michelin, R.A.; Kanhere, S.S. Dependable IoT using blockchain-based technology. In Proceedings of the 2018 Eighth Latin-American Symposium on Dependable Computing (LADC), Foz do Iguacu, Brazil, 8–10 October; pp. 1–9.
34. Li, M.; Shao, S.; Ye, Q.; Xu, G.; Huang, G.Q. Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail. *Robot.-Comput.-Integr. Manuf.* **2020**, *65*, 101962. [CrossRef]
35. Tapscott, A.; Tapscott, D. How blockchain is changing finance. *Harv. Bus. Rev.* **2017**, *1*, 2–5.
36. Ozdemir, A.I.; Ar, I.M.; Erol, I. Assessment of blockchain applications in travel and tourism industry. *Qual. Quant.* **2020**, *54*, 1549–1563. [CrossRef]
37. Yermack, D. Corporate governance and blockchains. *Rev. Financ.* **2017**, *21*, 7–31. [CrossRef]
38. Ladia, A. Blockchain: A privacy centered standard for corporate compliance. *IT Prof.* **2021**, *23*, 86–91. [CrossRef]
39. Xinhua Net. China Launches First Blockchain E-Seal Application Platform. 2020. Available online: https://global.chinadaily.com.cn/a/202007/21/WS5f164870a31083481725aed0.html (accessed on 4 May 2023).
40. Arul, R.; Al-Otaibi, Y.D.; Alnumay, W.S.; Tariq, U.; Shoaib, U.; Piran, M.J. Multi-modal secure healthcare data dissemination framework using blockchain in IoMT. *Pers. Ubiquitous Comput.* **2021**, 1–13.. [CrossRef]
41. Joshi, A.P.; Han, M.; Wang, Y. A survey on security and privacy issues of blockchain technology. *Math. Found. Comput.* **2018**, *1*, 121. [CrossRef]
42. Morkunas, V.J.; Paschen, J.; Boon, E. How blockchain technologies impact your business model. *Bus. Horizons* **2019**, *62*, 295–306. [CrossRef]
43. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
44. Suankaewmanee, K.; Hoang, D.T.; Niyato, D.; Sawadsitang, S.; Wang, P.; Han, Z. Performance analysis and application of mobile blockchain. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 642–646.
45. Steger, M.; Boano, C.; Karner, M.; Hillebrand, J.; Rom, W.; Römer, K. Secup: Secure and efficient wireless software updates for vehicles. In Proceedings of the 2016 Euromicro Conference on Digital System Design (DSD), Limassol, Cyprus, 31 August–2 September 2016; pp. 628–636.
46. Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. Blockchain: A distributed solution to automotive security and privacy. *IEEE Commun. Mag.* **2017**, *55*, 119–125. [CrossRef]
47. Ordoñez, L.A.T.; Niviayo, E.J.R.; Molano, J.I.R. Approach to blockchain and smart contract in Latin America: Application in Colombia. In Proceedings of the Applied Computer Sciences in Engineering: 6th Workshop on Engineering Applications, WEA 2019, Santa Marta, Colombia, 16–18 October 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 500–510.
48. Thakur, V.; Doja, M.; Dwivedi, Y.K.; Ahmad, T.; Khadanga, G. Land records on blockchain for implementation of land titling in India. *Int. J. Inf. Manag.* **2020**, *52*, 101940. [CrossRef]
49. Elisa, N.; Yang, L.; Chao, F.; Cao, Y. A framework of blockchain-based secure and privacy-preserving E-government system. *Wirel. Netw.* **2018**, *29*, 1005–1015. [CrossRef]
50. Navadkar, V.H.; Nighot, A.; Wantmure, R. Overview of blockchain technology in government/public sectors. *Int. Res. J. Eng. Technol.* **2018**, *5*, 2287–2292.
51. Ayed, A.B. A conceptual secure blockchain-based electronic voting system. *Int. J. Netw. Secur. Its Appl.* **2017**, *9*, 1–9.
52. Islam, M.J.; Mahin, M.; Khatun, A.; Roy, S.; Kabir, S.; Debnath, B.C. A comprehensive data security and forensic investigation framework for cloud-iot ecosystem. *GUB J. Sci. Eng* **2019**, *4*, 1–12.
53. Li, M.; Lal, C.; Conti, M.; Hu, D. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Gener. Comput. Syst.* **2021**, *115*, 406–420. [CrossRef]
54. Rossi, J.; VK, T. Opportunities and risks of BlockchainTechnologies in payments—A research agenda. In Proceedings of the Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 4–7 January 2017.
55. Tijan, E.; Aksentijević, S.; Ivanić, K.; Jardas, M. Blockchain technology implementation in logistics. *Sustainability* **2019**, *11*, 1185. [CrossRef]
56. Dutta, P.; Choi, T.M.; Somani, S.; Butala, R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transp. Res. Part Logist. Transp. Rev.* **2020**, *142*, 102067. [CrossRef] [PubMed]

57. IBM. *Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitize Supply Chains*; PR Newswire: Chicago, IL, USA, 2018.
58. Crypto ICO Review. ICO Review—5 Reasons Why Blockshipping Should Be Revolution the Global Container Shipping Industry. 2018. Available online: https://medium.com/biomanforcerose/ico-review-5-reasons-why-blockshipping-should-be-revolution-the-global-container-shipping-be18595c6933 (accessed on 4 May 2023).
59. CargoX. CargoX and Fracht AG Partner to Reshape Global Trade with Blockchain. 2018. Available online: https://cargox.io/press-releases/CargoX-FrachtAG-partner-to-reshape-global-trade-with-blockchain/ (accessed on 4 May 2023).
60. Zhang, J.; Zhang, C. Smart Container Security: The E-Seal with RFID Technology. *Mod. Appl. Sci.* **2007**, *1*, 16–18. [CrossRef]
61. Daschkovska, K.; Scholz-Reiter, B. Electronic Seals Contribution to the Efficiency of the Global Container System. In *International Graduate School for Dynamics in Logistics*; International Graduate School for Dynamics in Logistics: Bremen, Germany, 2008; p. 16.
62. Shi, X.; Tao, D.; Voß, S. RFID technology and its application to port-based container logistics. *J. Organ. Comput. Electron. Commer.* **2011**, *21*, 332–347. [CrossRef]
63. Chin, L.P.; Wu, C.L. The role of electronic container seal (E-seal) with RFID technology in the container security initiatives. In Proceedings of the 2004 International Conference on MEMS, NANO and Smart Systems (ICMENS'04), Banff, AB, Canada, 25–27 August 2004; pp. 116–120.
64. Grover, A.; Berghel, H. A survey of RFID deployment and security issues. *J. Inf. Process. Syst.* **2011**, *7*, 561–580. [CrossRef]
65. Zhang, R. A transportation security system applying RFID and GPS. *J. Ind. Eng. Manag.* **2013**, *6*, 163–174. [CrossRef]
66. Nash, J.F., Jr. Equilibrium points in n-person games. *Proc. Natl. Acad. Sci. USA* **1950**, *36*, 48–49. [CrossRef]
67. Laffont, J.J.; Maskin, E. Nash and dominant strategy implementation in economic environments. *J. Math. Econ.* **1982**, *10*, 17–47. [CrossRef]
68. Pinzón, C.; Rocha, C. Double-spend attack models with time advantange for bitcoin. *Electron. Notes Theor. Comput. Sci.* **2016**, *329*, 79–103. [CrossRef]
69. Port of Hamburg. Container Handling. 2023. Available online: https://www.hafen-hamburg.de/en/statistics/containerhandling/ (accessed on 4 May 2023).