# Binding the Physical and Cyber Worlds: A Blockchain Approach for Cargo Supply Chain Security Enhancement

Lei Xu [‡], Lin Chen [*], Zhimin Gao [*], Yanling Chang [†], Eleftherios Iakovou [†] and Weidong Shi [*]
[*]University of Houston
chenlin198662@gmail.com, mtion@msn.com, wshi3@uh.edu
[†]Texas A&M University
{yanling.chang, eiakovou}@tamu.edu
[‡]Conduent Labs
xuleimath@gmail.com

***Abstract*—Maritime transportation plays a critical role for the U.S. and global economies, and has evolved into a complex system that involves a plethora of supply chain stakeholders spread around the globe. The inherent complexity brings huge security challenges including cargo loss and high burdens in cargo inspection against illicit activities and potential terrorist attacks. The emerging blockchain technology provides a promising tool to build a unified maritime cargo tracking system critical for cargo security. However, most existing efforts focus on transportation data itself, while ignoring how to bind the physical cargo movements and information managed by the system consistently. This can severely undermine the effectiveness of securing cargo transportation. To fulfill this gap, we propose a binding scheme leveraging a novel digital identity management mechanism. The digital identity management mechanism maps the best practice in the physical world to the cyber world and can be seamlessly integrated with a blockchain-based cargo management system.**

***Index Terms*—blockchain, supply chain management, security**

## I. Introduction

The international trade volume keeps increasing at a high rate. According to WTO, the value of merchandise exports from WTO members reached $11.2 trillion in 2016 [1]. The trend leads to the growth of global goods movement employing various modes of transportation including ocean and coastal routes, inland waterways, railways, roads, and air freight. Within these globalized supply chain networks, over 90% of the cargo is carried by sea, as ocean transportation is the most cost-effective way to move masse goods and raw materials around the world [2].

Maritime supply chains involve sophisticated ecosystems with many stakeholders, e.g., exporters/importers, origin/destination agents, consolidating warehouse, customs bonded warehouses, ports, container terminal operators, shipping companies, insurance companies, and governmental agencies. This complexity results in enormous challenges in maintaining chain of custody and raises severe security problems: (i) Cargo losses. It is estimated that 30 to 50 billion USD worth of cargo is stolen every year; (ii) High burden in cargo inspection to prevent potential terrorist attacks and illicit activities. DHS requires the scanning of 100 percent of maritime cargo entering the United States from 2012, involving about 11.6 million containers every year [3].

Several collaborative security initiatives have been developed to mitigate the relevant risk, such as CargoNet [4], C-TPAT [5], and CSI [6]. These efforts depend heavily on efficient information sharing and exchange. Blockchain technology, which was first used in Bitcoin as a decentralized book keeping system to prevent double spending [7], provides a powerful tool to handle the complex maritime cargo transportation system. In a nutshell, blockchain can serve as a unified, immutable, and resilient

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

information management platform for all maritime transportation participants, on top of which a supply chain management system can be set up [8]. Using a blockchain-based supply chain management system to handle ocean-borne transportation can greatly improve the transparency cargo flow, expedite inspection process, and reduce fraud. However, most current schemes ignore the challenge of maintaining a consistent linkage between information stored on the blockchain and reality. Although the inconsistency can be finally detected, it introduces more uncertainty and consequently the detection can be seriously delayed.

To address this challenge, we propose a set of protocols for blockchain-based maritime transportation management that can better bind reality with the information system. These protocols take the best practices in the field into consideration and leverage the inherent consensus mechanism of blockchain together to prevent inaccurate information from entering the system in the first place.

In summary, our contributions in this paper include:

- We identify the critical challenges in maritime transportation that may lead to inaccurate information in the blockchain-based cargo management system;
- We propose a digital identity management scheme and detailed design, which can be integrated with blockchain maritime supply chain management systems to reduce information inconsistency.

## II. Background

In this section, we first provide background information about the blockchain technology and then discuss existing efforts of using blockchain for maritime cargo transportation management.

### A. Blockchain Technology

Blockchain technology provides a mechanism for decentralized book keeping. The first well-known application of blockchain is Bitcoin, which leverages the decentralized book keeping capability to prevent double-spending [7]. In a nutshell, blockchain consists of a sequence of blocks where each block contains multiple transactions. Each participant keeps a local copy of the current blockchain and then they work together to determine the next block using a consensus protocol. Typical blockchain construction methods include: (i) Proof-of-work. A participant needs to solve a computation intensive task and attaches the result to the new block. In most cases, the one who solves the task first can claim the block; (ii) Proof-of-stake. Each participant accumulates stakes according to a pre-defined rule, and the amount of stakes one owns determines the probability that he/she is selected to produce the next block; (iii) Byzantine fault tolerance (BFT). All participants run a BFT protocol to determine what is the next block. While Byzantine fault tolerance can determine the next block immediately, proof-of-work and proof-of-stake usually require to work with the longest-chain principle (the block will be confirmed until a certain number of blocks are added). TABLE I summarizes the common approaches for blockchain construction.

TABLE I
COMMON BLOCKCHAIN TYPES AND CONSTRUCTION APPROACHES.

| Blockchain Type | Construction Method |
|---|---|
| Public blockchain | • Proof-of-work<br>• Proof-of-stake |
| Permissioned blockchain | • Proof-of-work<br>• Proof-of-stake<br>• Byzantine fault tolerance |

In summary, blockchain has three key features: (i) Public accessibility. All information stored with blockchain is publicly accessible to everyone; (ii) Immutability. It is very hard or impossible to modify, alter, or remove information that has been added to the blockchain when the security assumption is satisfied; (iii) Resilience. Each participant of the system keeps an entire copy of the blockchain and no single point of failure can affect the availability of the stored information.

### B. Blockchain-based Maritime Cargo Management

Parties involved in maritime cargo transportation are not anonymous and are relatively stable. Considering the simplicity and performance benefit of permissioned blockchain, it is an adequate choice as the backbone of blockchain-based cargo management system. Several systems have been proposed along this direction [8], [9]. For such a system,

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

a set of nodes work together as the infrastructure to maintain the blockchain, and another group of nodes are participants of a cargo supply chain which generate new records and submit them to the blockchain. There could be an overlap between these two groups, i.e., some nodes are participants of the supply chain while they also help on the blockchain maintenance. Compared with centralized supply chain management systems, the blockchain-based approach has several advantages: (i) Consensus for data on the blockchain. All records accepted by the blockchain need to be verified by relevant participants and no single party can control the system; (ii) Immutable and robust storage. It is hard for an attacker to modify/remove records stored in the blockchain, and the multiple-copies architecture provides high availability; (iii) Better information sharing. Participants of the supply chain ecosystem can submit cargo information in real time to the system and stakeholders are informed instantly.

The effectiveness of a blockchain-based maritime cargo management system heavily relies on the assumption that information stored on the blockchain accurately captures reality, something which has not received enough attention as described in Section I.

## III. Binding Physical and Cyber Worlds

In this section, we provide detailed information on how to ensure information accuracy, i.e., guaranteeing that information managed by the blockchain is correctly reflecting reality.

### *A. Participants Vetting and Digital Identity Generation*

The first step to secure the maritime supply chains, especially cross border cargo flows, is to vet involved participants and set up digital identities for them.

A customized identity management system is developed to serve this purpose, which works as an extended public key infrastructure [10]. Specifically, a party $P$ that is involved in the maritime transportation uses a public/private key pair as its digital identity. The key pair can be RSA based, elliptic curve based, or other asymmetric key pair, as long as everyone in the system is in agreement on the common parameters and the capability to process corresponding operations.

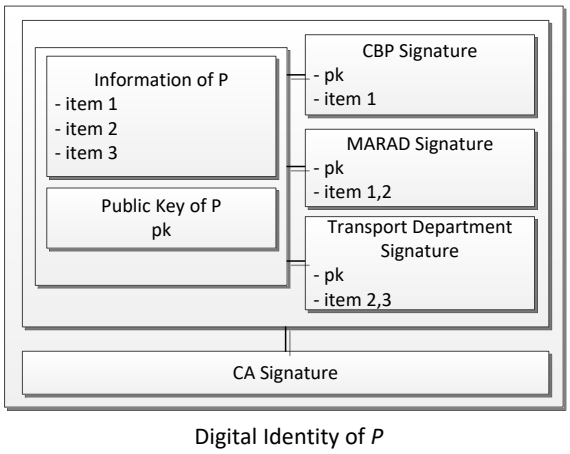


Fig. 1. Example structure of a digital identity of $P$. Multiple authorities check $P$'s attributes and digitally sign for those they know. A signature binds $P$'s public key and a subset of attributes. Finally the CA helps to assemble all signatures and check whether they cover all claimed attributes before wrap them and sign.

$P$ can generate a qualified public/private key pair by him/herself (denoted as $(pk, sk)$), where $sk$ is kept secret, and $P$ requests a certificate for $pk$, which is used by others to recognize $P$ in the blockchain-based supply chain management system. Unlike a classical PKI system, the generation of a certificate involves multiple authorities and incorporates the vetting procedure. For example, the Maritime Administration, the U.S. Department of Transportation, and CBP can check the information about $P$ independently and decide whether to sign $pk$. A certificate authority (CA) can then collect all signatures for $P$'s public key to generate a combined certificate as its digital identity in the blockchain management system. Fig. 1 depicts an example of digital identity. $P$ can provide a set of attributes about itself (item 1, item 2, item 3 in the example given in Fig. 1). An item can be the company name, registration information, etc.), and governmental agencies can verify a subset of them according to the information they have. The CA is responsible for collecting feedback from different agencies and determine whether it should issue the digital identity according to pre-defined rules.

When $P$ is involved in certain operations that need to be recorded in the blockchain, $P$ uses $sk$ to sign the corresponding message. When another party needs to verify whether the record is valid (e.g., $P$ is the correct entity), he/she verifies the digital identity by checking the included signatures.

If $P$ is a company, then a multiple of its em-

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

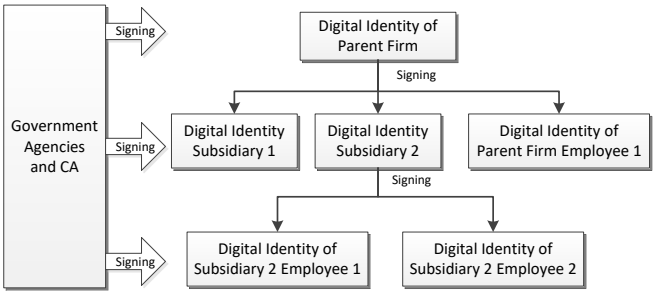


Fig. 2. Digital identities of employees and subsidiaries are organized as a tree. The parent node can sign the public key of its child nodes, and government agencies and CA can also be involved according to the pre-defined digital identity management rule.

ployees are involved in the handling of transported cargo, and each employee should has his/her own digital identity in order for others to verify his/her digital signature. These identities are generated and organized as a tree structure as illustrated in Fig. 2. For an employee, attributes can include personal information such as driver license and professional certification.

### B. Checking Digital Identity

Setting up the digital identity system is a necessary requirement to bind the physical and cyber worlds, but it is not sufficient. We also need to ensure that a participant can only use his/her own digital identity in the system.

To support field operations, the digital identity and the corresponding private key can be stored in a hardware token or a smart phone protected by password or biometrics. We use the following example to demonstrate how to prevent an adversary to use others' identities. When the cargo changes hand from participant $A$ to $B$, $B$ needs to use its private key to sign the record to reflect the transaction, and $A$ has to make sure that $B$ is using its own identity. Specifically, $A$ completes the following tasks:

- Checking whether the public key and private key are consistent. This can be done by using the public key to verify the signature generated by $B$;
- Checking whether the certificate of the public key is valid and contains required attributes. The validity of the certificate can be checked by verifying signatures of government authorities/CA, and one can also easily check all attributes embedded in the certificate to determine whether the required ones are included;
- Checking whether $B$ is the owner of the certificate. Based on the scenario, this can be done in different ways. For example, $A$ can physically check $B$'s government issued ID and compare it with attributes embedded in the certificate. The comparison activity is also saved in a record and then is submitted to the blockchain.

After $A$ finishes all the checking, he/she submits the checking records together with the original record of the cargo movement to the system. Only if the majority of all participants achieve consensus that this record should be accepted, it will then be finalized in the blockchain system.

### C. Leveraging Specific Hardware

Various hardware technologies have been developed to assist forwards martitime supply chain visibility, such as tracking devices [11], RFID tags [12], and smart containers [13]. These devices are usually tamper resistent and their digital identities can be safely stored inside the hardware. Note that the digital identity is generated in the same way as a company employee. When the device needs to update information about the cargo, it generates a new record and uses the private key related to its digital identity to sign the record before sending it to the blockchain-based management system. By checking the signature using the relevant public key embedded in its digital identity, other nodes can learn which device has created the record and then they work together to determine whether to include it in the blockchain with the underlying consensus protocol.

## IV. Conclusions

Blockchain technology is a potent tool for information exchange and recording, and it can be used as a underlying fundamental component of maritime cargo management system. To fully realize the potential of blockchains in securing the maritime cargo supply chain, preventing cargo loss, and reducing the burden of cargo inspection, we propose a scheme that helps to bind the physical and cyber worlds, i.e., information stored in the system can accurately reflect the status of the cargo. As the kernel component of the system, we design a collaboration mechanism for multiple governmental agencies to

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

cross check a participant before he/she can join the blockchain-based cargo management system. We also consider integrating existing cargo security improvement hardware such as smart GPS/container into the blockchain-based system.

## ACKNOWLEDGEMENT

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2015-ST-061-BSH001. This grant is awarded to the Borders, Trade, and Immigration (BTI) Institute: A DHS Center of Excellence led by the University of Houston, and includes support for the project "Secure and Transparent Cargo Supply Chain: Enabling Chain-of-custody with Economical and Privacy Respecting Biometrics, and Blockchain Technology" awarded to the University of Houston. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

## REFERENCES

[1] World Trade Organization, "International trade statistics review 2017," 2017. [Online]. Available: https://www.wto.org/english/res_e/statis_e/its2015_e/its15_toc_e.htm

[2] International Maritime Organization, "IMO Profile."

[3] J. B. McNeill and J. Zuckerman, "The cargo-screening clog: Why the maritime mandate needs to be re-examined," The Heritage Foundation, 2010.

[4] CargoNet. [Online]. Available: http://www.cargonet.com/

[5] CTPAT: Customs Trade Partnership Against Terrorism. [Online]. Available: https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat

[6] CSI: Container Security Initiative. [Online]. Available: https://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[8] L. Xu, L. Chen, Z. Gao, Y. Lu, and W. Shi, "Coc: Secure supply chain management system based on public ledger," in *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*. IEEE, 2017, pp. 1–6.

[9] K. Sadouskaya *et al.*, "Adoption of blockchain technologyin supply chain and logistics," 2017.

[10] C. Adams and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley Professional, 2003.

[11] N. Talukder, S. I. Ahamed, and R. M. Abid, "Smart tracker: Light weight infrastructure-less assets tracking solution for ubiquitous computing environment," in *Mobile and Ubiquitous Systems: Networking & Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on*. IEEE, 2007, pp. 1–8.

[12] X. Shi, D. Tao, and S. Voß, "Rfid technology and its application to port-based container logistics," *Journal of Organizational Computing and Electronic Commerce*, vol. 21, no. 4, pp. 332–347, 2011.

[13] J. Carn, "Smart container management: Creating value from real-time container security device data," in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*. IEEE, 2011, pp. 457–465.

978-1-5386-3443-1/18/$31.00 ©2018 IEEE