Decentralized Private Freight Declaration & Tracking with Data Validation

Li, Tianyu ; Vos, Jelle; Erkin, Zekeriya

DOI
10.1109/PerComWorkshops53856.2022.9767444

Publication date
2022

Document Version
Final published version

Published in
Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)

Decentralized Private Freight Declaration & Tracking with Data Validation

Tianyu Li
Cyber Security Group
Delft University of Technology
Delft, Netherlands
tianyu.li@tudelft.nl

Jelle Vos
Cyber Security Group
Delft University of Technology
Delft, Netherlands
j.v.vos@tudelft.nl

Zekeriya Erkin
Cyber Security Group
Delft University of Technology
Delft, Netherlands
z.erkin@tudelft.nl

2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) | 978-1-6654-1647-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/PerComWorkshops53856.2022.9767444

***Abstract*—In January 2017, a truck crossed the border between Spain and France for the first time using an e-CMR: An electronic version of the primary transport document required for inter-European logistics. Since that crossing, researchers and logistic organizations have proposed a large number of ideas to further digitize Europe's supply chain. Many of these ideas involve blockchains, but not all of them validate the data that is posted to them. As a result, participants can make illegitimate claims: Even though the blockchain enables transparency and immutability of the data stores, it does not ensure veracity. We provide several examples of works about information sharing in the supply chain that do not perform such validation. One work that does use the blockchain's validation functionality is DEFEND. DEFEND addresses customs agencies' lack of information for international freight inspection by tracking shipping containers throughout their journey. As containers pass from one operator to another, the blockchain participants ensure that containers are not doubly spent. In this work, we propose an extension of DEFEND, in which we further extend the capabilities for validation. Moreover, we provide actual cryptographic protocols to preserve participants' privacy while DEFEND only described privacy on a high level. Finally, by making a more fine-grained distinction between different actors in the chain, we model the entire supply chain from buyer to seller. As a result, the buyer and seller can now track the respective package's whereabouts through each leg of its journey.**

***Index Terms*—supply chain management, blockchain technology, freight declaration**

I. Introduction

Since the advent of e-CMR documents, much research has gone into further digitizing the supply chain. Much of this research consists of blockchain-based solutions. After all, blockchain technology promises an immutable ledger that offers a more or less consistent view to mutually distrusting participants. These properties underline the supply chain ideals of non-repudiation and transparency, respectively. However, by default, blockchain technology does not ensure the actual validity of the data that it stores: If there is no pre-described validation step, a blockchain participant is free to store false transactions in it. Since the number of blockchain papers is too much to cover, we give two examples of works that do not perform any validation. So for such a scheme, one must fully trust the participants when using their published information for practical operations.

The work by Kamath [1] discusses a pilot by IBM and Walmart regarding food safety for pork and mangoes. Kamath [1] explains how the actors involved in the supply chains of these goods publish data about them to the blockchain, which Walmart uses to analyze the risk associated with each separate product. However, the work does not describe any form of validation: The actors are free to publish any information. In that regard, a malicious actor can hide imperfect conditions in the production process by publishing fake information. The work also does not describe which participants have access to the published data. If the data is published in the clear, this intrudes on the actor's privacy, and if the data is only visible to Walmart, there is no need for a distributed ledger.

A similar work by Longo et al. [2] proposes an Ethereum-like blockchain solution for the supply chain. The proposed solution performs no validation other than checking if a mined block correctly contains the hash of the previous block. As such, participants are free to make any transactions. The paper goes on to question whether companies are discouraged from sharing inaccurate or counterfeit data. From their analysis, we conclude that there are some parties for which adversarial behavior is not profitable, but there remain parties that do profit. One of the proposed solutions to limit counterfeit data was only to allow write access to the largest retailers, but this limits the amount of information sharing.

Still, some works do take into account data validation. For example, the work by Saberi et al. [3] discusses a general blockchain model for the supply chain. The authors model the concept of 'ownership' through transfers that require both parties to participate. When a party makes a claim on the blockchain, the other participants validate that the party indeed has ownership of the product at that moment. At the least, this prevents parties from making claims about random products.

Vos et al. [4] propose DEFEND, a privacy-preserving blockchain-based freight declaration system that focuses on container freight tracking as part of the international supply chain. The information shared in the system empowers customs agencies to perform a better risk analysis, allowing operators to clear customs more quickly. This work also proposes validation through transfer claims to model the

This publication is part of the project Spark! Living Lab (with project number 439.18.453B of the research programme Duurzame Living Labs fase 2, which is (partly) financed by the Dutch Research Council (NWO).

concept of ownership. At the same time, the authors find a balance between public and private knowledge in that claims on a package level remain private between the sender and the receiving customs agency, and claims on a container level are public. Because container claims are public, the participants can validate claims about them. While the authors discuss these requirements on a high level, they do not detail the cryptographic primitives to realize them. In this work, we provide the cryptographic tools for these operations and propose an extension on DEFEND.

We summarize our contributions as follows:

- We further extend DEFenD's validation capabilities. For example, we enable key registration and revocation through customs agencies, allowing participants to verify the integrity of claims made to the blockchain.
- We detail the cryptographic protocols to achieve the necessary functionality while preserving confidentiality. Importantly, each party only requires one secret key to participate in the system, minimizing the risk of leaking secret information.
- By making a more fine-grained distinction between different actors in the chain, we model the entire supply chain from buyer to seller. As a result, the buyer and seller can now track the respective package's whereabouts through each leg of its journey.

II. Related work

A. Electronic bill of lading

Declaration of freight in international shipments currently relies on the *bill of lading*, which is a physical document that only has to be presented to customs agencies 24 hours in advance [4]. Works like DEFEND aim to replace this physical bill with an electronic bill of lading. Since then, several new initiatives have aimed to perform a similar feat. We shortly discuss three recent commercial initiatives.

1) TradeLens: TradeLens is a commercial venture by IBM and Maersk that digitizes the bill of lading. Their solution is based on Hyperledger Fabric [5]. Unfortunately, the work by Louw-Reimer et al. [5], which explains this venture, does not elaborate on whether participants perform any data validation.

2) Naviporta, dtledgers, TradeTrust: Naviporta, dtledgers and TradeTrust successfully collaborated in 2021 to perform a trial of an electronic bill of lading across multiple systems [6].

3) CargoSmart: The Global Shipping Business Network (GSBN) is a large consortium containing five of the largest ten container carriers [7]. The consortium collaborates with technology provider CargoSmart to digitize the supply chain altogether, using Hyperledger Fabric, among others.

B. Blockchain-based supply chains

Blockchain is an emerging technology that provides traceability and integrity for data, making it useful for international supply chains [8]. There are three main categories among all the supply chain solutions: electronic trading solutions [9]–[11], anti-counterfeit solutions [12]–[14], and supply chain management solutions [4], [15], [16]. In this paper, we focus on supply chain optimization solutions while validating claims from different actors.

Within the area of the supply chain, there are many existing works about preventing counterfeit products and regulating item transportation. For example, Bocek et al. [17] propose modum.io to reduce the operational costs in a pharmaceutical supply chain by monitoring the temperature and humidity of the environment. Users provide regulations for transportation, and the tracking number is associated with specific sensors. By doing that, the transportation company ensures the correct environment. However, there is no privacy considered when it comes to the sensor data, and a party's claims are not validated.

Imeri and Khadraoui [18] present a conceptual design to preserve security and protect traceability of shared information during the transportation of dangerous goods. They consider different entities, such as the provider, transport operator, authority, etc. However, all participants have the same permissions on the blockchain. As a result, all participants can see the information that is stored, which leaks information.

Also, there are several approaches for supply chain optimization, supply chain management, and information sharing. Engelenburg et al. [19] propose a system architecture for information sharing between the government and companies. The authors show the importance of data confidentiality from the side of companies and the need for information from the side of the government, which is the same situation as described in DEFEND. Data owners have their sharing strategy, and only the admitted people can access the needed data. Engelenburg et al. [19] apply cryptographic methods for access controls of users within an organization, but they do not discuss validating that data.

Wu et al. [20] present a tracking framework for supply chains by using a set of private ledgers and a public ledger to simplify its process. The private ledger is used to share the custody event among the partners of a specific shipment, and the public ledger includes the global tracking information for all users. Any node in the blockchain can create a block, and the consensus is done using proof of work. However, the application of both private chains and the public chain can increase the load of the consensus mechanism. Interestingly, Wu et al. [20] perform data validation by having the partners involved in one shipment validate whether the public ledger data corresponds to the private ledger data.

Finally, Vos et al. [4] propose DEFEND, which stores and shares data of goods and containers on a blockchain in a secure and privacy-preserving manner. However, no concrete cryptographic techniques are addressed in this paper. Our work is based on a similar setting to DEFEND, and we introduce the work further in Section IV.

In short, current literature about blockchain-based supply chains offer solutions that provide data immutability and transparency, but they fall short with regards to privacy preservation and data validations. In other cases, the concept of data validation is abstracted away through blockchain oracles, assuming that there is some ground truth that we can query reliably to fix the state of the blockchain.

III. Preliminaries

In this section, we discuss the cryptographic building blocks that our protocols rely on, and we give some background on the type of blockchain technology on which both DEFEND and our extension are based. In Table I, we present an overview of the notation used in this paper.

TABLE I
OVERVIEW OF NOTATION

Symbol	Description
	Blockchain participants
$\mathcal{P}_i$	The party with identifier i
sk_i	The secret key of party $\mathcal{P}_i$
pk_i	The public key of party $\mathcal{P}_i$
$tk_{i,j}$	The shared key between parties $\mathcal{P}_i$ and $\mathcal{P}_j$
	Elliptic curve groups
$\mathbb{Z}_x$	The group of integers modulo x
$\mathbb{G}$	Cyclic group in which DDH holds
G	Public generator element of $\mathbb{G}$
q	Size of group $\mathbb{G}$
	Cryptographic building blocks
$x \in_R X$	x is a random element from X
$\mathcal{E}_k(m)$	Symmetrically encrypt m with key k
$\mathcal{H}(\_)$	A key derivation function for $\mathcal{E}$

A. Diffie-Hellman key exchange & AES

The Diffie-Hellman key exchange is a standardized key agreement protocol between two parties. Before running the protocol, all parties agree on a cyclic group $\mathbb{G}$ of order q in which the Decisional Diffie Hellman (DDH) assumption holds and a corresponding generator element G. Then, both parties select a random integer $a, b \in_R \mathbb{Z}_q$ and compute public keys $A \leftarrow aG$ and $B \leftarrow bG$, where we write the group in additive notation. After sharing the public keys, the parties non-interactively generate a secret shared group element $aB = Ab$, which they can turn into a valid key for symmetric-key encryption using a key derivation. A common choice for group $\mathbb{G}$ is an elliptic curve group, such as Curve25519 [21]. For symmetric-key encryption, NIST recommends AES-128 [22].

B. Schnorr signatures

Where encryption provides confidentiality in sharing information with other parties, a signature scheme provides authentication. In our work, we choose Schnorr signatures [23], which can be defined over the same group as the Diffie-Hellman key exchange. As a result, a user requires just one secret key that they can use for both shared encryption and decryption, as well as signing their messages. The result of Schnorr's signature algorithm is a signature that can be verified using the public key generated according to the Diffie-Hellman key exchange.

C. Blockchain

Nakatomo [24] first introduced the idea of blockchain, which is a decentralized peer-to-peer database. In general, blockchain is a growing list of data blocks linked by cryptography and contain the hash of the previous block. Meanwhile, blockchain provides two main properties: immutability and transparency. These properties are highly desired for supply chains, where traceability and integrity are sought after.

There are different kinds of blockchains: mainly public and private. In a public blockchain, anyone can join the blockchain and take part in the consensus, but this requires expensive consensus protocols such as proof of work. In a private blockchain, there is an authority that allows participants in the system and takes control of the blocks. In that respect, a private blockchain is only partially decentralized. Secondly, private blockchains can be permissioned so that participants need permission to join after their identities are verified. Then the consensus is controlled by all the verified users. Also, transactions on permissioned blockchains are available to all users in the chain but not visible to anyone outside. Such properties make permissioned blockchains useful in a supply chain data sharing use case with multiple companies and participants. Hence, this is our choice of blockchain.

IV. DEFEND's solution

DEFEND models two types of actors: customs agencies and economic operators. Each trade bloc has its own trusted customs agency, but customs agencies of competing trade blocs do not trust each other. Customs agencies vote together to let new customs agencies join the system. Economic operators are parties that interact with packages and containers. For example, they might put packages into containers or ship containers and transfer them to another party. Based on these actors, DEFEND makes the following assumptions:

- Operators trust their own country's customs agency.
- Packages in the system may only be moved by shipping container.
- Only the customs agency at the end of a shipment must inspect a container.

Since operators trust their own country's customs agency, each customs agency is responsible for admitting their country's operators to the system.

Next, economic operators make claims about packages and containers. Package claims are encrypted claims that only the receiving customs agency can decrypt. They mention the identifier of a given package, whether it is inserted or removed from a container, and the identifier of that container. Container claims are unencrypted claims, stating that a party is transferring a container with a given identifier to another party. Container claims come in two parts: The first of the two parties makes a claim stating that it is handing over the container, while the other states it is receiving the container.

We summarize the actors and claim described above in Table II. Since both of the involved parties mirror container claims, the participants prevent double-spending of containers. Since package claims are encrypted, the other participants cannot perform any validation.

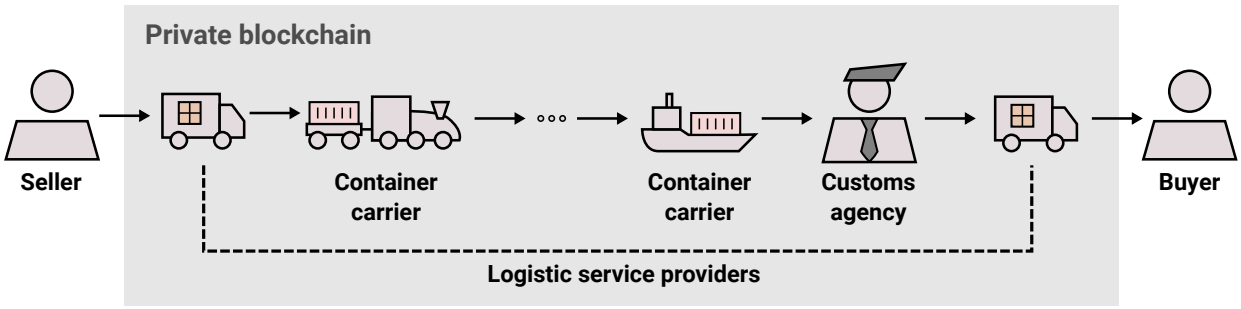

Fig. 1. The supply chain model in our extension of DEFEND.

TABLE II
AN OVERVIEW OF ACTORS DESCRIBED IN DEFEND, THE CLAIMS THEY MAKE AND THE PROPERTIES VALIDATED FOR THOSE CLAIMS.

	DEFenD	
Actors	Claim	Validation
Customs agency	-	-
Economic operator	Package	-
	Container	No double spending

TABLE III
AN OVERVIEW OF ACTORS IN OUR EXTENSION, THE CLAIMS THEY MAKE AND THE PROPERTIES VALIDATED FOR THOSE CLAIMS.

	Ours	
Actors	Claim	Validation
Customs agency	Identity	-
Logistic service provider	Package	Identity
Container carriers	Transfer	No double spending & Identity
	Location	Ownership & Identity

V. OUR EXTENSION OF DEFEND

In our extension of DEFEND, we make a further distinction between economic operators. We denote those who work on a package level as *logistic service providers* and those who work on a container level as *container carriers*. We make an additional assumption that the logistic service providers that interact with the seller and buyer are the same organization or closely collaborating partners. We highlight these actors and their position in the modeled supply chain in Figure 1.

In this system, logistic service providers make package claims, while container carriers make container claims. Furthermore, we introduce another type of container claim in the form of *location* claims, while we denote DEFEND's container claims as *transfer* claims. Moreover, DEFEND did not discuss key management, but in our extension, we explicitly manage keys through identity claims, which we describe in Subsection V-A. In Table III, we give an updated overview of the actors, claims, and the corresponding validated properties.

One shortcoming in DEFEND is that if operators encrypt package claims with the public key of the receiving customs agency using standard public-key cryptography, an operator cannot read back its claims from the blockchain. In Subsection V-B we provide a solution to this problem by letting the customs agency and the operator agree on a shared key non-interactively and using symmetric-key cryptography instead.

Finally, note that container carriers only make container claims in our system, meaning that logistic service providers are responsible for mapping which packages go into which containers. In Subsection V-C, we explain how the logistic service providers use this mapping to provide package tracking to the buyer and seller.

A. Management of operator's identities

When a logistic service provider or container carrier joins the system, it must generate a set of keys. We propose a one-time key generation protocol that only generates one secret key for a party to maintain. Our system assumes that customs agencies handle their keys responsibly, but operators sometimes forget their secret keys or must revoke their secret keys for other reasons. In such an instance, the customs agency publicly revokes the key, and the operator reruns this protocol. The operators use their secret key for shared-key encryption and signing, and they use their public key for shared encryption and signature verification. As explained in Section III, we rely on elliptic curve-based Diffie Hellman and AES, a standardized symmetric key cryptosystem for shared-key encryption. We elaborate on this in Subsection V-B. For signatures, parties use the Schnorr signature scheme.

While the logistic service provider or container carrier generates and maintains the secret key, the customs agencies share the public keys. In that regard, a party registers their public key with their customs agency, which makes an *identity* claim to the blockchain, publishing the public key while signing with their secret key. Customs agencies can also make an identity claim revoking a previous public key. As mentioned before, that party should then rerun the key generation protocol to register a new key and take part in the system again. We present the protocol below.

In all future claims, including claims not about the identity, the blockchain participants validate that the claim is not made with a revoked key. These identity claims realize a public-key infrastructure, and by integrating it in the blockchain, there is less room for discrepancies about the set of valid keys.

Key generation

1) Party $\mathcal{P}_i$ chooses secret key $sk_i \in_R \mathbb{Z}_q$, and computes the corresponding public key $pk_i \leftarrow sk_i G$.
2) Party $\mathcal{P}_i$ makes an identity claim:
   - If party $\mathcal{P}_i$ is a customs agency, it makes an identity claim for themselves, containing: public key pk_i, working name, identifier i.
   - If party $\mathcal{P}_i$ is an operator, it relays public key pk_i to their trusted customs agency $\mathcal{P}_j$, who makes an identity claim on behalf of the operator, sharing: pk_i, the operator's working name and id i, the customs agency's working name and id j. The agency signs the entire claim with signing key sk_j.

B. Shared-key encryption

DEFEND states that package claims should be encrypted so that the responsible customs agency is the only party that can decrypt them. Consequently, the operator that encrypts such a claim cannot decrypt it anymore. In other words, unless the operator keeps track of which unencrypted package data belongs to which encrypted claim, the operator cannot read its package data from the ledger. We solve this using a non-interactive version Diffie-Hellman key exchange so that package claims are encrypted with a shared symmetric key that is only known to the operator and the responsible customs agency. This key does not have to be stored; customs agencies and operators only keep their single private key safe, with which they generate the shared key efficiently. Below we describe the protocol for shared-key encryption on a message m so that parties $\mathcal{P}_i$ and $\mathcal{P}_j$ can both decrypt.

Shared-key encryption

1) Party $\mathcal{P}_i$ generates secret shared data $d_{i,j}$ with party $\mathcal{P}_j$ by computing $d_{i,j} \leftarrow sk_i pk_j$.
2) Party $\mathcal{P}_i$ uses a key derivation function on the shared data to derive a shared key $tk_{i,j} \leftarrow \mathcal{H}(d_{i,j})$. It encrypts message m, outputting ciphertext $c \leftarrow \mathcal{E}_{tk_{i,j}}(m)$.

The security of this scheme relies on the Decisional Diffie-Hellman assumption in $\mathbb{G}$, the uniformity of key derivation function $\mathcal{H}(\_)$ and the security of the encryption function $\mathcal{E}_k(m)$. As specified in Section III, Curve25519 and AES fulfill these security requirements for group $\mathbb{G}$ and encryption function $\mathcal{E}_k(m)$, respectively. For the key derivation function, we use PBKDF2 as described in RFC 8018 [25].

C. Track-and-trace for packages

When a seller ships a package to a buyer, the logistic service provider puts the package into a container. After that, only the logistic service provider knows which package is in which container. The logistic service provider then hands the container to a container carrier, which potentially transfers it to another carrier, and so forth. A container carrier knows the whereabouts of the containers it transports, which it shares on the blockchain in the form of *location* claims.

If a logistic service provider wants to know the location of a given package, they look up in what container they stored the package and scan the blockchain to find the latest location claim pertaining to that specific container. Since at one point in time, there should be only one carrier who claims the location of a specific container, the participants of the blockchain validate location claims by checking if the container carrier that made the claim actually owns that container using the transfer claims. For example, if truck A transfers a container x to freight train B, both A and B make a transfer claim. Now, truck A can no longer make claims about the locations of container x, but freight train B can.

If a buyer or seller wants to know the location of their package, they send a request to the corresponding logistic service providers. The logistic service provider then provides the method described above to find the corresponding container. Again, based on the container ID, the logistic service provider locates the container using the latest location claim. Finally, the logistic service provider shares the location with the buyer or seller without revealing which container the package is in.

The process above shows how to track a package in the supply chain for buyers and sellers. Meanwhile, the process is secure and privacy-preserving. Only the logistic service provider knows the location of packages and shares it with the package owner. Container carriers only know the location of containers, but they never know which packages are in which container. Finally, buyers and sellers learn the location of their packages, but they cannot use this location to obtain more information since they are not participants in the blockchain.

D. Efficiency

In Table IV we highlight performance by summarizing the complexity for the proposed operations in terms of elliptic curve (EC) multiplications, key derivation function (KDF) calls, and AES operations. Here, KeyGen refers to the operation described in Subsection V-A, while encryption and decryption refer to the shared-key encryption described in Subsection V-B along with signing or verification of a signature.

In the last row of Table IV, we provide references to run times reported in previous works for each primitive function. For Windows 7, the benchmark by Sotoodeh [26] shows that a curve multiplication using Curve25519 takes only 12.74 microseconds. A benchmark conducted on the `fastpbkdf2` library [27] indicates that the run time for key derivation is approximately 7.45 seconds for 2^{22} iterations on an AMD64 processor. Since NIST recommends at least 10,000 iterations [28], this would take approximately 18 milliseconds. Finally, Bernstein & Schwabe [29] reduce AES operations to less than 15 cycles per byte for Intel Pentium 4 processors.

VI. Conclusion

We propose data validation methods to ensure that data stored in blockchains for supply chain is not only immutable

TABLE IV
CALLS TO PRIMITIVE FUNCTIONS FOR EACH OPERATION

Operation	EC multiplications	KDF operations	AES operations
KeyGen	1	-	-
Encryption	2	1	1
Decryption	3	1	1
Run time 1x	12.74 μs [26]	18 ms [27]	15 c/b [29]

and transparent, but also trustworthy. We extend DEFEND to provide additional opportunities for data validation.

It remains an open engineering problem to implement our extension using an efficient private blockchain, allowing future research to compare performance with other solutions. Since DEFEND is implemented and tested on an older version of Hyperledger, one should consider how it would perform using state of the art implementations like the modern versions of Hyperledger and Ethereum. We refer interested readers to reference [4] for details how our extension can be implemented.

Still, our extension offers a promising direction in making supply chain data on the blockchain more reliable. Our contributions are threefold. Firstly, we propose extended data validation opportunities, applicable to package claims, transfer claims and location claims. Customs agencies can now issue or revoke a key, allowing participants to verify the integrity of any type of claims. Secondly, we extend DEFEND's underlying model to the whole supply chain from sellers to buyers, in which every actor's task is well-defined. By allowing container carriers to make claims about the location of the containers they are transporting, sellers and buyers can track and trace their packages by requesting this information from their logistic service provider. Thirdly, we introduce in detail how to achieve confidentiality in the proposed system using cryptographic protocols, bringing the system closer to be applied in practice, and preserving each participant's privacy.

REFERENCES

[1] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with ibm," *The Journal of the British Blockchain Association*, vol. 1, no. 1, p. 3712, 2018.

[2] F. Longo, L. Nicoletti, A. Padovano, G. d'Atri, and M. Forte, "Blockchain-enabled supply chain: An experimental study," *Computers & Industrial Engineering*, vol. 136, pp. 57–69, 2019.

[3] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.

[4] D. Vos, L. Overweel, W. Raateland, J. Vos, M. Bijman, M. Pigmans, and Z. Erkin, "Defend: a secure and privacy-preserving decentralized system for freight declaration," *arXiv preprint arXiv:1803.09257*, 2018.

[5] J. Louw-Reimer, J. L. M. Nielsen, N. Bjørn-Andersen, and N. Kouwenhoven, "Boosting the effectiveness of containerised supply chains: A case study of tradelens," in *Maritime Informatics*. Springer, 2021, pp. 95–115.

[6] "Singapore and rotterdam successfully complete trial with electronic bill of lading," May 2021. [Online]. Available: https://www.portofrotterdam.com/en/news-and-press-releases/singapore-and-rotterdam-successfully-complete-trial-with-electronic-bill-of

[7] N. Morris, "Five of top 10 container shippers join new blockchain consortium," Jan 2020. [Online]. Available: https://www.ledgerinsights.com/container-shipping-blockchain-consortium-cargosmart/

[8] H. Juma, K. Shaalan, and I. Kamel, "A survey on using blockchain in trade supply chain solutions," *IEEE Access*, vol. 7, pp. 184 115–184 132, 2019.

[9] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4601–4613, 2018.

[10] E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang, "A blockchain-based energy trading platform for smart homes in a microgrid," in *2018 3rd international conference on computer and communication systems (ICCCS)*. IEEE, 2018, pp. 472–476.

[11] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE transactions on industrial informatics*, vol. 14, no. 8, pp. 3690–3700, 2017.

[12] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain," *IEEE access*, vol. 5, pp. 17 465–17 477, 2017.

[13] G. Baralla, S. Ibba, M. Marchesi, R. Tonelli, and S. Missineo, "A blockchain based system to ensure transparency and reliability in food supply chain," in *European conference on parallel processing*. Springer, 2018, pp. 379–391.

[14] N. Alzahrani and N. Bulusu, "Block-supply chain: A new anti-counterfeiting supply chain using nfc and blockchain," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 2018, pp. 30–35.

[15] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," *Future Generation Computer Systems*, vol. 86, pp. 641–649, 2018.

[16] M. H. Meng and Y. Qian, "A blockchain aided metric for predictive delivery performance in supply chain management," in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*. IEEE, 2018, pp. 285–290.

[17] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE symposium on integrated network and service management (IM)*. IEEE, 2017, pp. 772–777.

[18] A. Imeri and D. Khadraoui, "The security and traceability of shared information in the process of transportation of dangerous goods," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 2018, pp. 1–5.

[19] S. van Engelenburg, M. Janssen, and B. Klievink, "Design of a software architecture supporting business-to-government information sharing to improve public safety and security," *Journal of Intelligent Information Systems*, vol. 52, no. 3, pp. 595–618, 2019.

[20] H. Wu, Z. Li, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, "A distributed ledger for supply chain physical distribution visibility," *Information*, vol. 8, no. 4, p. 137, 2017.

[21] D. J. Bernstein, "Curve25519: new diffie-hellman speed records," in *International Workshop on Public Key Cryptography*. Springer, 2006, pp. 207–228.

[22] M. J. Dworkin, "Sp 800-38d. recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac," Gaithersburg, MD, USA, Tech. Rep., 2007.

[23] Y. Seurin, "On the exact security of schnorr-type signatures in the random oracle model," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2012, pp. 554–571.

[24] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[25] K. Moriarty, B. Kaliski, and A. Rusch, "Pkcs #5: Password-based cryptography specification version 2.1," *Internet Eng. Task Force (IETF)*, vol. 8018, pp. 1–40, 2017.

[26] M. Sotoodeh, "Highly efficient implementation of elliptic curve 25519." [Online]. Available: https://github.com/msotoodeh/curve25519

[27] J. Birr-Pixton, "Ctz/fastpbkdf2: Fast pbkdf2 implementation in c." [Online]. Available: https://github.com/ctz/fastpbkdf2

[28] "Digital identity guidelines," 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html

[29] D. J. Bernstein and P. Schwabe, "New aes software speed records," in *International Conference on Cryptology in India*. Springer, 2008, pp. 322–336.