CoC: Secure Supply Chain Management System based on Public Ledger

Lei Xu, Lin Chen, Zhimin Gao, Yang Lu, and Weidong Shi
Computer Science Department, University of Houston, Houston, Texas, 77004

***Abstract*—Modern supply chain is a complex system and plays an important role for different sectors under the globalization economic integration background. Supply chain management system is proposed to handle the increasing complexity and improve the efficiency of flows of goods. It is also useful to prevent potential frauds and guarantee trade compliance. Currently, most companies maintain their own IT system for supply chain management. However, this approach has some limitations that prevent one to get most of the supply chain information. Using emerging decentralized ledger technology to build supply chain management system is a promising direction. However, decentralized ledger usually suffers from low performance and lack of capability to protect information stored on the ledger. To overcome these challenges, we propose CoC, a novel supply chain management system based on hybrid decentralized ledger. We develop an efficient block construction method with the model and security mechanism to prevent unauthorized access to data stored on the ledger.**

I. Introduction

Modern economy heavily depends on global collaboration, especially advanced manufacturing. According to the WTO report, the international trade volume keeps increasing at a high rate in the past decades and merchandise exports from WTO members achieved US$ 18.0 trillion in 2014 [1]. Behind this explosive growth, supply chain plays a critical role. Besides classical functions such as making movements of goods smoother and reducing the cost of international transportation, modern supply chain system is becoming the center of various business activities such as planning/forecasting, procurement, customer services, and performance measurement. Due to the large scale and complex functionalities of supply chain, it is not easy to efficiently manage it. In response to such demands, the concept of supply chain management system was introduced by Keith Oliver in 1982 [2], and the market of supply chain management software outpaced most software markets to total US$ 9.9 billion in 2014 [3]. A lot of work has been done to improve supply chain management system efficiency and add more features. For example, researchers proposed to integrate sensors (e.g., GPS receiver and RFID) into the supply chain to provide more information to the end user, and combine the cyber world and the physical world more closely [4]. As cloud computing technology emerges, cloud based supply chain management system is also developed to improve the reliability and reduce the cost [5].

However, existing supply chain management systems suffer from some limitations that prevent the users from achieving most out of the value of supply chain information. The two major issues are: (i) Supply chain in nature involves multiple parties. However, most companies and stakeholders nowadays use their own supply chain management systems, which are difficult to be integrated together to provide a unified platform. Therefore, it is not convenient to offer end-to-end tracking and share information to enable new functionalities and services. Furthermore, supply chain information is sensitive and the companies may not be willing to disclose and share with others. (ii) As an IT system, supply chain management system also faces cyber attacks, especially breaches of the integrity of supply chain information, which may lead to fraud, losses of goods, and trade incompliance. The recent rising of Ransomware attack also poses a significant risk to supply chain management system as losing access to historical data can cause financial damage [6], [7].

Decentralized ledger technology (DLT), which has been used in Bitcoin and similar decentralized systems implementing crypto-currency for recording and sharing transaction history [8], is maintained by a group of users and each of them can maintain a local copy of the ledger. A group of records are embedded into a block and blocks are linked through hash values. A consensus mechanism helps these users achieve agreement when a new block is added to the system. In order to modify an existing record, an adversary has to compete with all honest users [9], [10]. These features make decentralized ledger a promising technology to enable global supply chain management system in distributed environment. Both technology startups and transnational corporations start to experiment supply chain management systems based on distributed ledger [11]–[13].

Most of the existing efforts on creating supply chain management system with decentralized ledger are straightforward examples of direct application of DLT as decentralized storage with consensus assurance, i.e., storing supply chain related information in blocks rather than traditional file system, but ignore the downsides of the technology: (i) Decentralized ledger usually has performance issues such as limited throughput and long latency for adding new blocks, which may not be sufficient to support application scenarios with requirements to store high volume of supply chain operation records and support high transaction throughput; (ii) Information stored in decentralized ledger is distributed to and maintained by different nodes; and there is a lack of mechanism to enforce access policies and control access to the data stored in the distributed ledger.

To address these shortcomings, we propose CoC (supply **c**hain **o**n block**c**hain), a novel supply chain management system leverages the decentralized ledger technology. CoC uses a

978-1-5090-2991-4/17/$31.00 ©2017 IEEE

hybrid model and two-steps block construction method for the underlying distributed ledger, which achieve a good balance between security and performance. In addition, it introduces a new storage scheme that reduces data redundancy while at the same time sufficiently satisfying the demands of supply chain management.

Because supply chain management system plays a central role in business operations that involve sensitive information, a protection mechanism is built on top of the hybrid model and storage scheme to guarantee that only authorized user can access corresponding data on the ledger. We also evaluate the proposed system from performance and security perspectives to demonstrate its usefulness in real environment.

Our contributions in this work are summarized as follows:

- We propose a novel design of supply chain management system based on public ledger that serves as a unified platform for different parties and stakeholders involved in the supply chain ecosystem to conduct transactions and share information;
- We develop a two-step block generation method for the system which has low latency, and an efficient storage scheme that alleviates the concern of storage overhead of decentralized ledger technology; and
- We describe the design of identity management and data protection scheme that addresses security issues for decentralized ledger based supply chain management system.

The remainder of this paper is organized as follows: Section II briefly describes the supply chain management system and decentralized ledger technology. In Section III, we provide an overview of the proposed CoC system and the hybrid model for ledger construction. Detailed design of critical components of CoC is given in Section IV. Section V reviews related work and we conclude the work in Section VI.

II. Background

In this section, we briefly review the supply chain management system and blockchain technologies.

A. Supply Chain Management System

Supply chain management is more than an extension of logistics management and the integration of business processes from end users through original suppliers that provide products, services, and information that add value for customers [14]. Typical supply chain management functions include ordering/receipt of raw materials/products, supporting customer services, and performance measurements. The coordination of multiple functions across the enterprise is required to provide rapid and quality response to supply chain events [15]. Fig. 1 depicts the functions of supply chain management and its position in business operation. Besides handling physical cargos, supply chain system is now also used for data transfer (e.g., Fedex is helping Amazon customers to move giant amount of data).

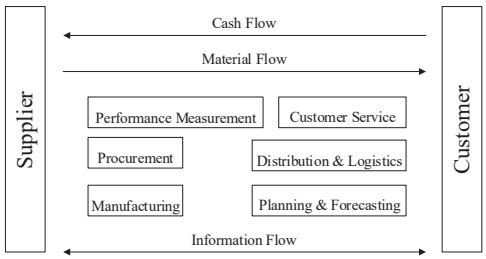


Fig. 1. Role of supply chain in business operation. It manages the information flow and provides the foundation for various functions [15].

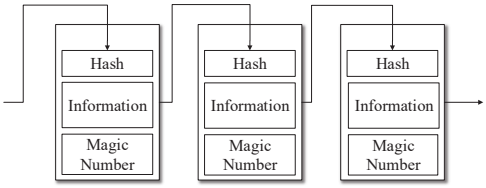


Fig. 2. Basic working principles of decentralized ledger with proof-of-work. Information is embedded into a block, which also contains a hash value from the previous block and a magic number. The magic number is found out through a brute-force search process, i.e., one searches all possible values of magic number to make sure the hash value of the triple (previous hash value, embedded information, and magic number) satisfies pre-defined condition (e.g., the hash value has a certain number of leading zeros).

B. Decentralized Ledger Technology

Decentralized ledger, or blockchain technology, is first introduced by Bitcoin as a distributed book-keeping system to prevent double-spending [8]. The generation of blocks is based on proof-of-work (as depicted in Fig. 2) and each participant keeps a complete copy of the chain. They achieve consensus by adopting the longest chain, and if an attacker wants to modify the content of a block in the chain, he/she has to compete with all honest participants of the system to generate valid blocks.

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

One major issue of blockchain is the high latency of block generation, which is caused by the expensive proof-of-work process (e.g., brute-force search for pre-image of a hash function). To make the block generation faster, two different strategies are proposed: proof-of-stake and permissioned blockchain. TABLE I summarizes characters of these strategies.

III. Overview of CoC and Hybrid Model

In this section, we provide an overview of CoC and describe the hybrid model.

Participants in CoC. As a unified supply chain management platform, CoC needs to support different types of participants, which are divided into three groups:

- Ordinary users. An ordinary user can use CoC for different supply chain related operations, e.g., submitting new

TABLE I
SUMMARIZATION OF DIFFERENT DECENTRALIZED LEDGER CONSTRUCTION STRATEGIES.

Name	Description	Pros and Cons
Proof-of-work [9]	In order to construct a new block and add to the blockchain, a participant has to compute a hard problem and attach the result to the new block.	Pros: The mechanism is simple and fair. Cons: It wastes a lot of computation resources and has relatively high latency.
Proof-of-stake [16]	Participants accumulate stake according to the pre-defined accumulation scheme, and a certain amount of stake has to be used to create a new block. Therefore, any participant who has enough stake can generate a new block instantly.	Pros: This approach can generate blocks with very low latency when the system has enough stake available. Cons: It is a challenge to design a stable stake accumulation scheme; and the system may go to two extreme statuses: no one has enough stake to generate a block or everyone has enough stake to generate a block.
Permissioned [17]	A set of trusted parties is responsible for block generation. One party belongs to the set can attach a signature to the block and the block is recognized as a valid one.	Pros: The mechanism is simple and new blocks can be generated very fast. Cons: This strategy requires a different security model (e.g., Some nodes are trusted). It only fits certain scenarios such as transactions between financial institutes.

request for raw material, tracking transportation information, processing bill of lading, and analyzing historical data related to the user. Supply chain is a complex system and CoC supports multiple ordinary users to collaborate with each other;

- Third party users. Besides ordinary users, there is another group of users, third party users, who mainly monitor supply chain information with CoC. Typical third party users include government regulators like CBP and insurance companies who need to monitor the status of the goods; and
- Supporting entities. CoC also includes supporting entities for the supply chain operations. Two of the main supporting entities are identity management component and financial institutions. Here identity management can be part of CoC, while financial institutions have their own IT system and only interact with CoC to provide required services such as payment processing.

In the following of the paper, "If not explicitly stated otherwise, the term "user" stands for both *ordinary user* and *third party user*.

Hybrid model of decentralized ledger and system overview. Existing models of decentralized ledger do not fit the requirements of supply chain management very well:

- Proof-of-work involves heavy computation and is usually slow, which may not be able to satisfy the performance and operation requirements of supply chain management;
- Proof-of-stake is not stable for supply chain management system as it is non trivial to predict the demands of blocks;
- CoC aims at providing a unified supply chain management platform that can serve multiple entities that do not need to fully trust each other; and it may be difficult to achieve consensus on compromised nodes of a permissioned blockchain network for block construction.

CoC separates the right to submit records and the right to build blocks by using a hybrid model to organize the distributed ledger. Specifically, CoC allows only *users*, *third party users*, and *supporting entities* to submit supply chain related records to the system, but the block construction is open to the public and based on proof-of-work. These who contribute their computation resources to help to build and maintain the distributed ledger are called *helper*s. The number of helpers can be relatively large and driven by the demands of transactions. CoC does not put much restriction on helpers. They can join or leave the system at any moment by themselves. Fig. 3 illustrates the system and different types of entities involved.

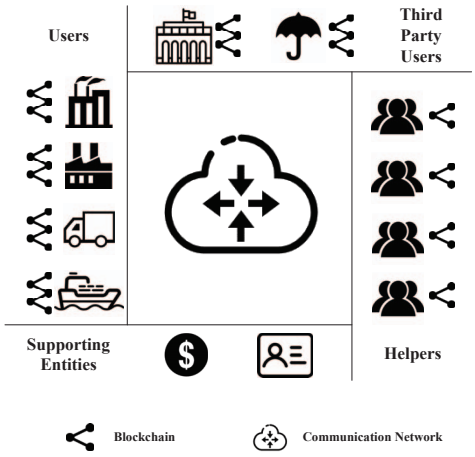


Fig. 3. Overview of CoC. Users (e.g., factories, transportation companies) use the system for supply chain information management. Third party users include insurance companies and government regulators. In most cases, they just monitor information stored in CoC and do not add new information. Support entities include financial institutions for payment service and identity management component. The system also involves a large number of helpers, who facilitate generation of blocks that are used to hold supply chain information and transaction records.

Security model. We assume that *supporting entities* are trusted, e.g., they will follow pre-defined protocols to collaborate with other parties and will not try to inject faked information into the system. *Third party users* are usually large companies and government agencies, and are also trusted. They will follow the policies to perform their tasks (e.g., generating certificate of compliance). Any individual *helper* is not trusted,

he/she may try to compromise the system using different ways. However, the number of *helpers* is usually large, and it is assumed that majority of them are honest and will follow predefined protocols. The users are not fully trusted. Although they have the incentives to keep accurate information to support their business activities, it is difficult to guarantee that all of the users have adequate cyber protection and they may be compromised (e.g., loss of private key, infected by Trojan or viruses). A compromised user may generate invalid supply chain information and/or try to modify historical data. We also assume that the communication between different parties are protected and secure, i.e., an attacker cannot tamper or eavesdrop the messages between different parties.

IV. Detailed Design of Key Components of CoC

In this section, we describe the design of key components of CoC.

A. Block Construction for Supply Chain Information

One of the main challenges to decentralized ledger based supply chain management system is the capability to support a large number of operations within a short time window. As discussed in Section III, *users* are not trusted and permissioned blockchain system cannot be used to reach low latency block construction. The proof-of-stake strategy does not work well neither for supply chain management because the amount of transactions is dynamic and there is a risk and likely scenario that a stake based system goes to one of the two extreme cases (i.e., no one has enough stake or everyone has enough stake to create a valid block).

Two-step block construction.

To overcome the performance obstacles of blockchain technology while taking supply chain management characteristics into consideration, we propose a novel two-step approach for block construction for CoC. The basic idea is to allow users to reserve blocks for near future usage based on their prediction, and then the users can use reserved blocks immediately when they are needed (as depicted in Fig. 4). Specifically, the two-steps block construction mechanism works as follows:

- **Step 1:** Generation of reservation blocks. When a user submits his/her reservation request to the system, the request is distributed to all helpers through gossip protocol. The helpers who receive the request try to create a block through mining. Fig. 5(a) depicts the structure of the reservation chain. For each block included in the chain, it contains the user information who wants to reserve the block; the fee that the user wants to pay for the block; identity of the helper who creates it; and other essential information. Note that all participants have to reach a consensus on the reservation chain, which is achieved through proof-of-work.
- **Step 2:** Generation of data blocks. When a user has one supply chain record that needs to be added to the blockchain that holds real data, it first checks the reservation chain to see whether he/she has available reservations for block generation. If he/she has an available reservation, a data block is constructed for supply chain record and the proof of reservation is included in the block. Fig. 5(b) shows the structure of a data block. Adding this block to the chain does not require proof of work. When other peers receive a new block, it first checks its validity: whether the block is properly constructed and whether reservation is valid. If it passes all the checks, the new block is accepted and added to the chain. The system also needs to achieve a consensus on all accepted blocks and we can apply different consensus protocols for this purpose (e.g., Paxos protocol [18]).

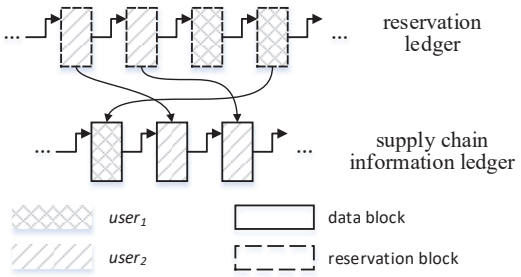
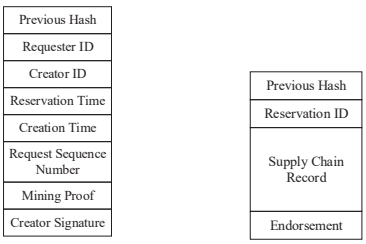


Fig. 4. Two step block generation. Before a user can put a supply chain record into the chain, he/she has to make a reservation in another chain. The reservation is confirmed by proof-of-work, i.e., someone has to complete a computation intensive task for a reservation. As showed in the figure, $user_1$ and $user_2$ reserve two blocks for their supply chain information in the reservation ledger. $user_1$ uses one of his/her reservation and $user_2$ uses both. If $user_2$ wants to insert additional information to the supply chain information chain, he/she has to make extra reservations.



(a) Reservation block.

(b) Data block.

Fig. 5. Two block structures for reservation and supply chain data. For data block, the field "Supply Chain Record is used to hold various information from order, payment, to bill of lading.

The two-steps block construction method does not reduce the overall work load or latency compared with proof-of-work based blockchain construction (in fact, the work load and latency for the first step is very similar to classical proof-of-work based blockchain construction). But it provides a mechanism to hide/shift the latency: as long as a *user* has enough reservations, the latency of adding a new supply chain record can be significantly reduced.

For the reservation step, the latency is determined by both the demands (number of reservation requests) and supply (the number of reservations can be generated within a given period). This is a typical supply-demand equilibrium problem. As increasing the supply of block constructions does not require much time (more *helpers* can contribute to block generation from supply side), the latency for the system to achieve an

equilibrium can be short.

The first step of making reservation is based on proof-of-work and the ratio of reservation blocks generation is proportional to the number of *helpers* participate in the system [19]. As *users* pay for reservation, the market mechanism can automatically adjust based on supply and demand.

The two-steps block construction method can also be applied to other scenarios where the requirements are similar to the supply chain management system discussed in this work. Compared with proof-of-stake approaches, the two-step block generation does not suffer from oversupply or undersupply of stakes.

B. Storage Design of CoC

Information storage is the foundation for other supply chain management operations. According to the design of two-step block construction, CoC needs to maintain two decentralized ledgers: the reservation ledger and the data ledger. The simplest approach to maintain the two ledgers is to let everyone keep full copies of both of them. However, this is not efficient and increases the cost of the participants. We propose a more efficient storage scheme for CoC to manage the two decentralized ledgers. Because the two ledgers serve different purposes, we adopt different methods to manage them.

Reservation ledger storage. The construction of reservation ledger involves *users* and *helpers*, where *users* submit requests and *helpers* conduct mining to build blocks. The *helpers* play a similar role as miners in Bitcoin system, and they do not need to store the whole reservation chain. Instead, they can run the simplified verification protocol (SVP) for reservation block construction [8], e.g., each *helper* only keeps a small number of reservation blocks and accept one if there are enough number of blocks that are added after it. At the same time, CoC needs a set of *full nodes* that keep the whole reservation chain. The *users* can maintain a whole copy of the reservation chain and work as full nodes, as they need to use the reservation information for the data ledger. To reduce the storage cost for full nodes, the system can set a live time for reservation blocks; and full nodes can only keep the recent blocks in the chain. This also discouragew the *users* to hoard unnecessary reservation blocks.

Data ledger storage. Data ledger is used to store real supply chain information. It is not necessary for *supporting entities* and *helpers* to keep track of the supply chain information, so they do not need to store the data chain. *Third party users* usually need to monitor supply chain information of different users, and they keep a full copy of the data chain. For *users*, they do not have to store unrelated supply chain information to save their storage resources. There are still a reasonable number of copies of each piece of supply chain information as supply chain operations usually involve multiple parties.

When decentralized ledger is used to construct digital currency system, participants have to keep all transaction histories to prevent double-spending. The situation for supply chain management is different as the transactions are sometimes independent of each other. Therefore, old information can be discarded to further reduce the storage cost.

C. Identity Management of CoC

Decentralized ledger used in Bitcoin system does not have a centralized identity management component as it is anonymous and each participant can generate their own credentials (e.g., public/private key pairs) to use in the system. However, CoC targets at the supply chain management scenario with different requirements from Bitcoin or crypto-currency. Participants of CoC play different roles in the system (as depicted in Fig. 3). Therefore, their identities have to be managed with different strategies.

Helper is the largest group in CoC, and this group is usually quite dynamic and expensive to manage using a centralized approach. Furthermore, helpers only contribute their computation resources to maintain CoC and there is no need to authenticate their identities. Therefore, *helpers* in CoC can generate their own public/private key pairs without notifying others. *Users* generate supply chain information; and it is necessary to bind information with its creators. CoC uses traditional identity management component to generate public/private key pairs for the *users* and they use the keys to generate digital signatures for the information submitted to CoC to ensure authenticity/integrity. There are active and on-going research efforts on building PKI with decentralized ledger [20], [21]. When these schemes are mature enough, they can be used to replace a centralized identity management system. For financial institutions that work as supporting entities, they maintain their own identity management system as they usually have their own standards and compliance requirements.

Identity management doesnt have to be operated by a single entity. Multiple identity management systems can be integrated as long as they can interoperate. Besides using public/private key pair to identify a user, CoC also supports using biometrics for identity management.

D. Supply Chain Management Information Protection

When stakeholders, users, and companies of the supply chain ecosystem interact with CoC, their supply chain management related records and transactions are mixed and stored on the distributed ledger. However, it is apparent that they do not want to disclose information to unrelated parties. To address this requirement, encryption is used to protect supply chain management records on the ledger.

- Record encryption. The creator of a record selects a random AES key dek to encrypt the record. It is the creator's responsibility to selects adequate attributes of the record to encrypt and keep other parts in plaintext;
- Authorizing access. The creator also creates a list of users/supporting entities, e.g., involved companies, government agencies, or financial institutions. By working together with the identity management component, the creator further encrypts dek with public keys of users/supporting entities in the list. Ciphertexts of dek can be stored together with the encrypted record on the distributed ledger as evidence that the creator has allowed these accesses.

With this design, helpers and unrelated users/supporting entities are not able to learn useful information by observing the distributed ledger because they do not have access to the key dek. This approach is independent of the underlying decentralized ledger; and it can support flexible access control at record level. If a group of records are shared with the same set of users/supporting entities, the creator can use the same dek to avoid multiple time key distribution. Other encryption techniques that are used for secure data distribution can be applied as well, e.g., attribute encryption and proxy re-encryption [22].

V. Related Work

In this section, we briefly review existing works on using DLT for supply chain management.

Korpela, Hallikas, and Dahlberg noticed that blockchain technology offers a public model to connect different stakeholders; and provided a set of factors that affect the adoption of such system [23]. Tian proposed a design of agri-food supply chain that combines RFID and decentralized ledger. This work mentioned some performance limitations of blockchain but did not provide any solution [24]. IBM introduced its blockchain based supply chain management system and blockchain based bill of lading system on top of the Hyperledger project, which is a purely permissioned decentralized ledger platform [25]. There are other works along this direction [11]–[13], [26]. However, they did not consider performance limitation, collaborations between different companies, and security requirements.

VI. Conclusion and Future Work

Supply chain management plays an important role in the economy, especially when business entities are more dependent on each other. CoC uses a hybrid model and two-steps method to maintain a decentralized ledger based on blockchain technology for managing supply chain information more efficiently without compromising desirable features of decentralized ledger. In addition, it introduces a protection mechanism to prevent supply information stored on the ledger from being accessed by unauthorized participants.

For the next step, we plan to implement a fully functional prototype and evaluate its effectiveness in production environment. As current design involves a centralized identity management component, the objective is to design a decentralized identity management scheme to make the whole system decentralized, and consequently further enhance resilience, dependability, and security of the overall system.

Acknowledgement

The authors were supported in part by National Science Foundation grant DGE 1433817 and NATO grant G110696. The views and opinions expressed in this article are those of the authors. They don't reflect the official policy or position of any government agency.

References

[1] World Trade Organization, "International trade statistics 2015," 2015. [Online]. Available: https://www.wto.org/english/res_e/statis_e/its2015_e/its15_toc_e.htm

[2] K. Oliver, "When will supply chain management grow up?" *Strategy+ Business*, no. 32, 2003.

[3] J. Rivera and R. van der Meulen, "Gartner says worldwide supply chain management and procurement software market grew 10.8 percent in 2014," May 2015. [Online]. Available: http://www.gartner.com/newsroom/id/3050617

[4] W. He, E. L. Tan, E. W. Lee, and T. Li, "A solution for integrated track and trace in supply chain based on RFID & GPS," in *Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on*. IEEE, 2009, pp. 1–6.

[5] M. Lindner, F. Galán, C. Chapman, S. Clayman, D. Henriksson, and E. Elmroth, "The cloud supply chain: A framework for information, monitoring, accounting and billing," in *2nd International ICST Conference on Cloud Computing (CloudComp 2010)*, 2010.

[6] A. Gazet, "Comparative analysis of various ransomware virii," *Journal in computer virology*, vol. 6, no. 1, pp. 77–90, 2010.

[7] G. O'Gorman and G. McDonald, *Ransomware: a growing menace*. Symantec Corporation, 2012.

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

[9] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2015, pp. 281–310.

[10] V. L. Lemieux and V. L. Lemieux, "Trusting records: is blockchain technology the answer?" *Records Management Journal*, vol. 26, no. 2, pp. 110–139, 2016.

[11] V. Morabito, "Blockchain practices," in *Business Innovation Through Blockchain*. Springer, 2017, pp. 145–166.

[12] W. Lehmacher, "Global dynamics and key trends," in *The Global Supply Chain*. Springer, 2017, pp. 67–112.

[13] L. Parker, "Blockchain tech companies focus on the $40 trillion supply chain market," *Brave New Coin, February*, vol. 2, 2016.

[14] M. C. Cooper, D. M. Lambert, and J. D. Pagh, "Supply chain management: more than a new name for logistics," *The international journal of logistics management*, vol. 8, no. 1, pp. 1–14, 1997.

[15] M. S. Fox, J. F. Chionglo, and M. Barbuceanu, "The integrated supply chain management system," Technical report, Department of Industrial Engineering, University of Toronto, Tech. Rep., 1993.

[16] V. Buterin, "What proof of stake is and why it matters," *Bitcoin Magazine, August*, vol. 26, 2013.

[17] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, "The blockchain as a software connector," in *Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, 2016.

[18] L. Lamport, "The part-time parliament," *ACM Transactions on Computer Systems (TOCS)*, vol. 16, no. 2, pp. 133–169, 1998.

[19] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, and P. Saxena, "SCP: a computationally-scalable Byzantine consensus protocol for blockchains," Cryptology ePrint Archive, Report 2015/1168, Tech. Rep., 2015.

[20] K. Lewison and F. Corella, "Backing rich credentials with a blockchain PKI," Tech. Rep., 2016.

[21] M. Al-Bassam, "SCPKI: A smart contract-based PKI and identity system," in *AsiaCCS Workshop on Blockchain, Cryptocurrencies and Contracts*, 2017.

[22] L. Xu, X. Wu, and X. Zhang, "CL-PRE: a certificateless proxy re-encryption scheme for secure data sharing with public cloud," in *7th ACM Symposium on Information, Compuer and Communications Security - AsiaCCS 2012*, 2012.

[23] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[24] F. Tian, "An agri-food supply chain traceability system for china based on RFID & blockchain technology," in *Service Systems and Service Management (ICSSSM), 2016 13th International Conference on*. IEEE, 2016, pp. 1–6.

[25] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 2016.

[26] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," 2016.