Abstract

Supply chain management (SCM) has become an important way for the companies to improve the production efficiency and reduce the management cost. However, the existing SCM system is usually built and performed with the semi-trusted certificate authority, which may be susceptible to the collusion attack and tampering attack launched by the malicious certificate authority, resulting in illegal modification of product provenance record. Moreover, the lack of transparent and mutual trust among the stakeholders in the SCM system remains a great challenging issue. In this paper, we propose a blockchain-based decentralized supply chain system with secure information sharing, which can ensure the security of product provenance record without relying on any fully trusted intermediary. In our system, two validation mechanisms, i.e., one-way validation mechanism and transaction-based validation mechanism are built to help the stakeholders to perform the validation of product provenance record without accessing their original content. Furthermore, the blockchain-based smart contract is used to achieve secure registration, proper authentication and fair payment for all stakeholders, where the valid stakeholders can pay for the purchased products, automatically and reliably. Security analysis and performance evaluation demonstrate that our proposed scheme is secure, feasible and efficient with a limited and reasonable computation cost.

# 1. Introduction

Supply chain (Lin et al., 2015; Du et al., 2020) can provide suitable products for the enterprises or individual, which involves various stages, e.g., the collection of raw materials, the production of products, the transportation of products and the sale of products. In the supply chain system, there are several stakeholders, e.g., the supplier, the producer, and the retailer, who are responsible for transforming the raw materials into final products and delivering the products to end consumer by the information flow, capital flow and logistics. To improve the production efficiency, supply chain management (SCM) (Mehta et al., 2021; Bader et al., 2021; Choi et al., 2019; Wu and Wu, 2020) has become an indispensable part of the supply chain, which can make full of the internal and external resources of the supply chain to meet the needs of consumers and achieve final destination at the least cost. However, there are some deficiencies in the traditional SCM system. For example, many independent stakeholders usually locate in different places, which will lead to the information dissymmetry and make it difficult for the stakeholders to share the products information in the SCM system. Moreover, weak supervision in the product circulation causes the SCM system to be confronted with the collusion attack and tampering attack launched by the external and internal adversaries, resulting in illegal modification of product information.

With the development of cloud computing, the SCM system has resorted to cloud storage server provider (CSP) to enhance its sustainability and production efficiency. Giannakis et al. (Giannakis et al., 2019) discussed the potential advantages of cloud-based supply chain management system (C-SCM), and proposed a novel cloud-based supply chain management (C-SCM) architecture to enhance supply chain responsiveness (SCR). Dahbi et al. (Dahbi and Mouftah, 2016) proposed a cloud-based inventory management platform for supply chain, which can help the stakeholders in the supply chain system to efficiently manage their inventory by collecting and compiling the data related to the products. Gonul et al. (Gonul Kochan et al., 2018) developed a dynamics approach of hospital supply chain management system, which used the causal loop diagrams (CLDs) and their equivalent systems dynamics (SD) models to evaluate the performance and impact of information sharing on the hospital supply chain system. Peng et al. (Jinqi et al., 2017) proposed a cloud-based simulation model for supply chain by employing the COIN model and Q-learning algorithm. By the simulation model, each participant can make the decisions to reduce the cost of supply chain network. However, the schemes mentioned above mainly focus on the performance efficiency and do not consider the security protection of product data in the supply chain system. Moreover, there are the serious security issues in the C-SCM system due to the strong trust placed on the cloud storage server provider (CSP). Since CSP is a semi-trusted entity, it may directly disclose the product record to the adversaries.

In recent year, blockchain technology, as an emerging technology, has gained widespread attention and brought huge change to the SCM system. Le et al. (Le et al., 2020) proposed a blockchain-based data sharing scheme for supply chain, namely TrustedChain, which aimed to provide a trusted environment for the stakeholders and utilized the smart contract and interPlanetary file system (IPFS) to achieve secure data management. Koirala et al. (Koirala et al., 2019) proposed a supply chain model based on the Ethereum blockchain platform, which employed the smart contract to achieve the transparency and traceability of different transactions among the stakeholders. Lou et al. (Lou et al., 2021) proposed a blockchain-based supply chain framework (SESCF) to achieve the fairness and security in different processes of products circulation, i.e., information flow, capital flow, and logistics. In the framework, the smart contract is constructed to realize information symmetry for supply chain system, Furthermore, the proposed framework can support the fair payment. Dwivedi et al. (Dwivedi et al., 2020) proposed a blockchain-based pharmaceutical supply chain management system with secure information sharing, which used the smart contract to achieve secure distribution of cryptographic keys, and the consensus mechanism to check the validity of transaction and new block, respectively. However, the three schemes mentioned above are vulnerable to the collusion attack because of the introduction of the certificate authority (CA), where malicious CA may collude with internal and external adversaries to tamper with the product record for profit.

To solve the above problems, we propose a blockchain-based decentralized supply chain system with secure information sharing, which can achieve the security and confidentiality for the SCM system without relying on any fully trusted CA. As we all known, the blockchain has proved to be able to ensure the security of transaction information and prevent it from illegal modification. Consequently, we aim to take advantage of blockchain technology to ensure the security of product record in supply chain system. In the product circulation, each stakeholder can utilize the blockchain-based smart contract to perform secure transmission and validation of product provenance record. Meanwhile, the product provenance record will be integrated into a transaction by the cryptography technology and finally upload to the blockchain, so that each stakeholder can check the correctness of product provenance record without knowing its original content.

In summary, the main contributions are listed as follows:

* We propose a blockchain-based decentralized supply chain system, which constructs validation mechanisms, i.e., one-way validation and transaction-based validation to achieve the validation of the provenance record of product.
* We devise secure interactive protocols for supply chain by running the smart contract, where each stakeholder can achieve the secure registration, proper authentication and fair payment without relying on any fully trusted intermediary.
* The security analysis demonstrates that our scheme can thwart the collusion attack and tampering attack, and the performance evaluation shows that our scheme is efficient and feasible with a reasonable computation overhead.

The rest of the paper is organized as follows. In Section 2, we introduce the preliminaries used in our scheme. In Section 3, we present the problem statement of our scheme. In Section 4, we describe the details of our proposed SCM scheme. In Section 5, we present the security analysis of our proposed scheme. In Section 6, we provide the performance evaluation. At last, we draw the conclusion in Section 7.

# 2. Preliminaries

## 2.1. Notations

In this section, we present the notations used in our scheme and their descriptions shown in Table 1*.*

## 2.2. Bilinear maps

Defining two multiplicative groups as *G* and *GT*, they have a same prime order *p* and *g* is the generator of *G*. Especially, there is a bilinear map as *e*: *G* × *G* → *GT* with three properties (Boneh et al., 2004; Boneh and Franklin, 2003) as follows:

* Bilinearity: For *P*, *Q* ∈ *G* and *a*, *b* ∈ *Zp*, there is an equation as *e*(*Pa*, *Qb*) = *e*(*P*, *Q*) *ab*.
* Non-degeneracy: For *P*, *Q* ∈ *G* and *P* ∕= *Q*, there is an inequation as *e* (*P*, *Q*) ∕= 1*.*
* Computability: For all *P*, *Q* ∈ *G*, there is an algorithm to efficiently compute *e*.

## 2.3. Blockchain

Nowadays, the blockchain technology (Raj Kumar Reddy et al., 2021; Lim et al., 2021) has widely used in different application areas, e.

g., industry system (Biswas and Gupta, 2019; Bürer et al., 2019; Leng et al., 2021), healthcare system (Cao et al., 2019; Benil and Jasper, 2020; Zhang et al., 2021), cloud storage system (Wei et al., 2020; Zhang et al., 2021; Yuan et al., 2020) and e-commerce system (Rachana Harish et al., 2021; Li et al., 2019), etc., where Bitcoin (Nakamoto, 2008; Li et al., 2020) and Ethereum (Hu et al., 2021; Guo et al., 2019) are the most mature applications of blockchain, and have been widely known to the public. Specifically, blockchain is a decentralized and distributed database system, which is composed of quite a few data blocks. Specially, a data block in blockchain mainly comprises two parts, i.e., the block header and the block body, where each block connected by the secure hash algorithm will store lots of transaction information. By the characteristics of the blockchain. e.g., distributed structure, consensus mechanism and smart contract, etc., it can effectively prevent transaction information from illegal modification. As shown in Fig. 1, a transaction TX mainly contains the parameters, i.e., *From*, *To*, *Value*,

# *Data*, *Sig*. Especially, A transaction TX can be formalized as TX = *From*||*To*|| *Value*||*Data*||*Sig*

where *From* denotes the sender’s account address, *To* denotes the receiver’s account address, *Value* denotes the cost of creating the transaction TX, *Data* denotes the main information stored in the transaction TX, *Sig* denotes the signature of the transaction TX and || denotes catenation.

## 2.4. Smart contract

The smart contract (Alahmadi and Lin, 2019; Wang et al., 2020), first proposed by Nick Szabo in 1994, is an executable code and usually be used to build a variety of secure protocols. By the smart contract, the secure protocols can be performed automatically without relying on any trusted third-party intermediary. Furthermore, the content of protocols cannot be modified or deleted once the smart contract is deployed on blockchain. Thus, the smart contract has been one of the remarkable technologies of the Ethereum blockchain. In the Ethereum blockchain network, any user can create and submit the smart contract to the blockchain. **3. Problem statement**

## 3.1. System model

As shown in Fig. 2, we will introduce the system model, which comprises five stakeholders, i.e., Supplier(*S*), Producer(*P*), Retailer(*R*), User(*U*), Cloud server (*CS*), and Blockchain (*BC*).

* Suppliers, are the companies that will collect a considerable number of raw materials and provide them to the producer.
* Producers, are the companies that will use raw materials to produce a considerable number of products and sell them to the retailer.
* Retailers, are the companies that will institute a reasonable product price policy and sell the products to the user.
* Users, need to purchase the products provided by the retailers and pay for the products at the specified price. In our scheme, the user can check the validity of the product records by the blockchain.
* Cloud server, can provide sufficient storage space for the data provided by the stakeholders and reduce the cost of data management for the stakeholders. In our scheme, the product record provided by the stakeholders needs to be encrypted by secure encryption algorithm and uploaded to CS.
* Blockchain, can be viewed as a secure and decentralized management system with plenty of nodes. In our scheme, we will take advantage of the Ethereum blockchain with smart contract to ensure the security of product record in the supply chain system.

## 3.2. Threat model

Two adversaries, i.e., the external adversaries and internal adversaries, are taken into account in our proposed scheme, which will invade the supply chain system and learn the product provenance record. More specifically, the external adversaries will try to impersonate the valid user to access the SCM, so as to gain the confidence of the SCM system. Then, the external adversaries will try to learn useful information about the logistics after having certain understanding of the system protocol. The internal adversaries may be one of the participants in the supply chain system, which will collude with CSP to get the product data stored on the CS and tamper with its content for profit.

## 3.3. Security goal

Based on the above analysis, we will achieve the following security goals against the external adversaries and internal adversaries in our proposed scheme.

* Privacy preserving. In the supply chain system, every stakeholder needs to create and maintain a product provenance record, which stores some information of product, e.g., the date of manufacture, the address of manufacture and the material component, etc. Our proposed scheme needs to ensure the confidentiality of the provenance record and prevent it from the malicious attack, e.g., the tampering attack. The forgery attack and the impersonation attack.
* Record auditability. Our proposed scheme requires that every user can check the correctness of the product provenance record without knowing its original content.