Computers & Industrial Engineering 182 (2023) 109392

Contents lists available at ScienceDirect

Computers & Industrial Engineering

journal homepage: www.elsevier.com/locate/caie

# Blockchain-based decentralized supply chain system with secure information sharing

Guipeng Zhang [a], Zhenguo Yang [a,*], Wenyin Liu [a,b,*]

[a] School of Computer Science and Technology, Guangdong University of Technology, Guangzhou, China
[b] Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen, China

ARTICLE INFO

*Keywords:*
Supply chain management
Blockchain
Smart contract
Fair payment

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

[*] Corresponding authors at: School of Computer Science and Technology, Guangdong University of Technology, Guangzhou, China (W. Liu).
*E-mail address:* yzg@gdut.edu.cn (Z. Yang).

https://doi.org/10.1016/j.cie.2023.109392
Received 30 October 2021; Received in revised form 12 June 2023; Accepted 15 June 2023
Available online 20 June 2023

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 $G_T$, they have a same prime order $p$ and $g$ is the generator of $G$. Especially, there is a bilinear map as $e$: $G \times G \rightarrow G_T$ with three properties (Boneh et al., 2004; Boneh and Franklin, 2003) as follows:

- Bilinearity: For $P, Q \in G$ and $a, b \in Z_p$, there is an equation as $e(P^a, Q^b) = e(P, Q)^{ab}$.
- Non-degeneracy: For $P, Q \in G$ and $P \neq Q$, there is an inequation as $e(P, Q) \neq 1$.
- Computability: For all $P, Q \in G$, 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

**Table 1**
The notations and descriptions.

| Notations | Descriptions |
|---|---|
| $S$ | The supplier |
| $P$ | The producer |
| $R$ | The retailer |
| $U$ | The user |
| CSP | The cloud storage server provider |
| $X_i$ | The $i$-th stakeholder in SCM |
| $Add$ | The Ethereum account address |
| $pw$ | The password |
| $C$ | The ciphertext |
| $ID$ | The identity |
| $sk, pk$ | The key pair |
| $\omega$ | The Signature |
| $K$ | The symmetric key |
| $E$ | The symmetric encryption |
| $L$ | The auxiliary information |
| $D$ | The provenance record |
| $T$ | The current time |
| $h, h_1$ | The hash algorithm |

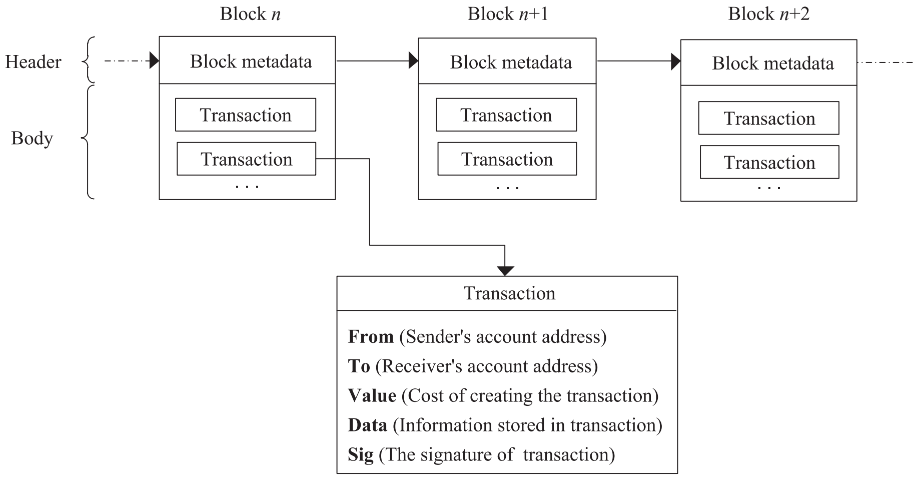

Block $n$
Block $n$+1
Block $n$+2
Header
Body
Block metadata
Transaction
Transaction
...
Transaction
From (Sender's account address)
To (Receiver's account address)
Value (Cost of creating the transaction)
Data (Information stored in transaction)
Sig (The signature of transaction)

**Fig. 1.** The structure of blockchain.

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 ($BC$).

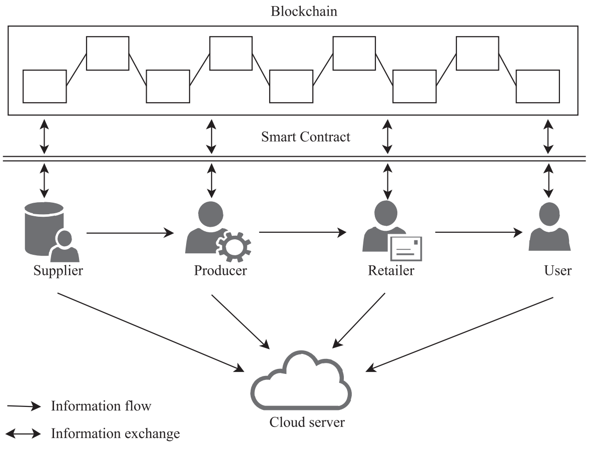


**Fig. 2.** System model.

- 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.
- Product traceability. Our proposed scheme can enable the stakeholder to learn the product logistics in the supply chain system without knowing the content of product provenance record, which can be achieved by secure hash algorithm and the transaction-based storage structure.
- Fair payment. In the SCM system, it is essential and challenging to achieve the fair payment among the stakeholders. Our proposed scheme requires that the stakeholders must pay the corresponding fees in terms of product provided by other stakeholders, which can be implemented by the smart contract deployed on the blockchain.

## 4. The detail of proposed scheme

### 4.1. Overview

In a SCM system, the information flow, capital flow and logistics need to be achieved among all stakeholders, to guarantee the final product to be delivered to end user, where three challenging issues need to be concerned in our scheme. The first issue is that how to ensure the security of the provenance record of product in the product circulation and prevent its content from illegal modification. The second issue is that how to check the correctness of provenance record without revealing its origin content to the auditors. The third issue is that how to realize fair payment among the stakeholders without relying on any fully-trusted financial institution.

In our scheme, the provenance record of product needs to be protected by secure encryption so that anyone cannot tamper with that without valid encryption key. Meanwhile, two validation mechanisms, i.e., one-way validation and transaction-based validation are build to achieve the correctness verification of the product provenance record without disclosing its origin content. As shown in Fig. 3, one-way validation mechanism can enable the participants (except for user) to check the correctness of the provenance record provided by previous participant, while the transaction-based validation mechanism will only be performed by the users and help them to remotely execute the validation of the provenance record stored on the CS. Moreover, the blockchain-based smart contract is employed to build secure payment protocols for supply chain system, by which each stakeholder can pay for the product in the capital flow, automatically and reliably.

### 4.2. System setup

- For the SCM system, there are commonly five stakeholders, i.e., the supplier $S$, the producer $P$, the retailer $R$, the user $U$ and the cloud storage server CS. Especially, we denote these five stakeholders mentioned above as $X_i$ ($i$ = 1,2,3,4,5), where every stakeholder $X_i$ will own a unique Ethereum account address $Add_{Xi}$, the RSA private key $sk_{Xi}$ and the RSA public key $pk_{Xi}$.
- For the key generation, there is a bilinear map as e: $G \times G \to G_T$, in which $G$ and $G_T$ are two multiplicative groups and g is the generator of $G$. Especially, each stakeholder selects a random number $p_i \in Z_p$ ($i$ = 1,2,3,4) and computes $q_i = g^{pi}$, where the public parameter is $q_i$ and the private parameter is $p_i$.
- For the payment in a SCM system, the stakeholder $X_i$ ($i$ = 2,3,4) needs to pay the stakeholder $X_{i+1}$ for the product when the stakeholder $X_{i+1}$ successfully receives the product, where we denote the expenses as $Q_E$. The stakeholder $X_i$ needs to make compensation to the stakeholder $X_{i+1}$ when the stakeholder $X_{i+1}$ fails to receive the product, where we denote the compensation expense as $Q_C$.

### 4.3. Secure supply chain management scheme

In this section, we will present the details of our proposed scheme, consisting of the following steps: Registration, Production circulation, Remote validation and Fair payment.

#### 4.3.1. Registration

To achieve secure identity authentication, every stakeholder $X_i$ can generate a secure and unique identity by using the smart contract. More specifically, the stakeholder $X_i$ can first use his/her own password $pw_{Xi}$ and the hash value of private key $h(sk_{Xi})$ to submit the Registration Contract. As shown in Fig. 4, the Registration Contract will run the registration algorithm *Register*(.) to compute the secure identity as

$$ID_{Xi} = Register(pw_{Xi}, h(sk_{Xi})) \tag{1}$$

where the registration algorithm *Register*(.) can be implemented by the secure hash function *h* (.). Finally, every stakeholder $X_i$ will receive the identity $ID_{Xi}$, which can resist the password guessing attack and will not disclose private information about the stakeholder $X_i$.

```
Registration Contract
Require {
        The stakeholder's password $pw_{Xi}$,
        The stakeholder's private key $sk_{Xi}$,
        The value of function $Register(pw_{Xi}, h(sk_{Xi}))$,
        }
Execute {
        Set $ID_{Xi}=Register(pw_{Xi}, h(sk_{Xi}))$ ;
        }
Output : $ID_{Xi}$
```

**Fig. 4.** Registration Contract.

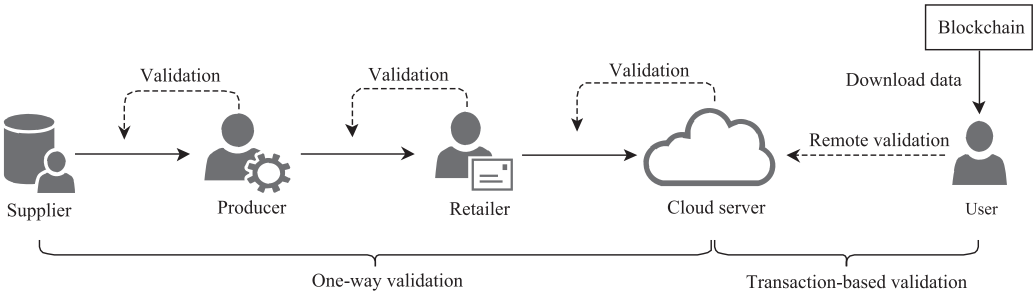


**Fig. 3.** The validation model.

### 4.3.2. Product circulation

To realize secure product information sharing in the product circulation of SCM system, we construct the one-way validation mechanism by BLS signature and encryption algorithm to enable each participant (except the user) to perform the verification of the product provenance record during the product circulation, which can realize the traceability of the product provenance record and prevent it from illegal modification by malicious participants.

Step 1(Supplier $S$ → Producer $P$): For the supplier $S$, the stakeholder $X_1$ provides the raw material to the producer $P$ and generates a provenance record $D_1$ as

$$D_1 = ID_{X1} \| ID_{D1} \| L_1 \tag{2}$$

where $ID_{X1}$ denotes the identity of the supplier $S$, $ID_{D1}$ denotes the identity of the raw material and $L_1$ denotes some auxiliary information about the raw material.

The supplier $S$ encrypts the record $D_1$ as

$$C_1 = E(K_1, D_1) \tag{3}$$

where $C_1$ denotes the ciphertext of the record $D_1$, $E$ denotes the symmetric encryption algorithm and $K_1$ is the encryption key.

The supplier $S$ computes

$$w_1 = h_1(C_1)^{p1} \tag{4}$$

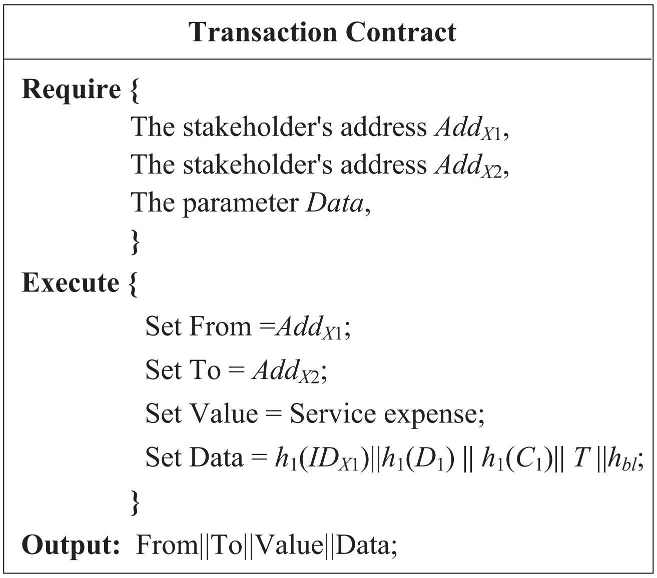
where $\omega_1$ denotes the signature of the ciphertext $C_1$.

Step 2(Supplier $S$ → Blockchain): The supplier $S$ can integrate the record $D_1$ into a transaction $TX_1$ and upload it to the blockchain. Specifically, the supplier $S$ computes

$$Data = h_1(ID_{X1}) \| h_1(D_1) \| h_1(C_1) \| T \| h_{bl} \tag{5}$$

where $T$ denotes the current time and $h_{bl}$ denotes the hash value of current block in the blockchain.

The supplier $S$ can submit the Transaction Contract shown in Fig. 5 to create a transaction $TX_1 = From||To||Value||Data$, where $From = Add_{X1}$, $To = Add_{X2}$, $Value$ = Service expense, $Data = h_1(ID_{X1})|| h_1(D_1) || h_1(C_1) || T || h_{bl}$. The supplier $S$ utilizes the private key $sk_{X1}$ to generate the signature $Sig(TX_1)$ and uploads the transaction $TX_1 = From||To||Value||Data||Sig(TX_1)$ to the blockchain. Finally, the supplier $S$ sends ($ID_{X1}$, $\omega_1$, $C_1$) to the producer $P$.



```
Transaction Contract
Require {
        The stakeholder's address $Add_{X1}$,
        The stakeholder's address $Add_{X2}$,
        The parameter $Data$,
        }
Execute {
        Set From =$Add_{X1}$;
        Set To = $Add_{X2}$;
        Set Value = Service expense;
        Set Data = $h_1(ID_{X1}) \| h_1(D_1) \| h_1(C_1) \| T \| h_{bl}$;
        }
Output: From||To||Value||Data;
```

**Fig. 5.** Transaction Contract.

Step 3(Producer $P$ → Retailer $R$): For the producer $P$, the stakeholder $X_2$ receives the raw material and needs to first check the validity of the provenance record $D_1$. Specifically, the producer $P$ computes

$$e(w_1, g) = e(h_1(C_1), q_1) \tag{6}$$

Only when the equation holds, the producer $P$ can produce the corresponding product by the raw material and generate a provenance record $D_2$ as

$$D_2 = ID_{X2} \| ID_{D2} \| L_2 \tag{7}$$

where $ID_{X2}$ denotes the identity of the producer $P$, $ID_{D2}$ denotes the identity of the product and $L_2$ denotes the auxiliary information about the product.

The producer $P$ computes

$$C_2 = E(K_2, D_2) \tag{8}$$

$$w_2 = h_1(C_1 \| C_2)^{p2} \tag{9}$$

$$Data = h_1(ID_{X2}) \| h_1(D_2) \| h_1(C_1 \| C_2) \| T \| h_{bl} \tag{10}$$

where $C_2$ denotes the ciphertext of the record $D_2$, $\omega_2$ denotes the signature of the ciphertext $C_1||C_2$. Similarly to Step 2, the producer $P$ also submit the Transaction Contract to create a transaction $TX_2$ as $TX_2 = From||To||Value||Data||Sig(TX_2)$, where From = $Add_{X2}$, To = $Add_{X3}$, Value = Service expense. Finally, the producer $P$ sends ($ID_{X1}||ID_{X2}$,$\omega_1||\omega_2$, $C_1||C_2$) to the retailer $R$.

Step 4(Retailer $R$ → Cloud server CS): The retailer $R$ (as the stakeholder $X_3$) receives the product provided by the producer $P$ and verifies the validity of the record $D_2$ by checking the equation as

$e(\omega_2, g) = e(h_1(C_1||C_2), q_2)$ (11)

The retailer $R$ computes

$$D_3 = ID_{X3} \| ID_{D2} \| L_3 \tag{12}$$

$$C_3 = E(K_3, D_3) \tag{13}$$

$$w_3 = h_1(C_1 \| C_2 \| C_3)^{p3} \tag{14}$$

where $ID_{X3}$ denotes the identity of the retailer $R$, $L_3$ denotes the auxiliary information, $C_3$ denotes the ciphertext of the record $D_3$, $\omega_3$ denotes the signature of the ciphertext $C_1||C_2||C_3$.

The retailer $R$ can submit the Transaction Contract to create a transaction $TX_3$ as

$$TX_3 = From \| To \| Value \| Data \| Sig(TX_3) \tag{15}$$

where $From = Add_{X3}$, $To = Add_{X4}$, $Value$ = Service expense, $Data = h_1(ID_{X3})||h_1(D_3) || h_1(C_1||C_2||C_3) || T || h_{bl}$.

Finally, the retailer $R$ can upload the transaction $TX_3$ to blockchain and send ($ID_{X1}||ID_{X2}||ID_{X3}$, $\omega_1||\omega_2||\omega_3$, $C_1||C_2||C_3$) to CS for storage. CS can verify the validity of the provenance record $D_3$ by checking the equation as

$$e(w_3, g) = e(h_1(C_1 \| C_2 \| C_3), q_3) \tag{16}$$

If it holds, CS receives ($ID_{X1}||ID_{X2}||ID_{X3}$, $\omega_1||\omega_2||\omega_3$, $C_1||C_2||C_3$) and records them in database.

As shown in Fig. 6, a computational example is presented to illustrate the process of step 1 in our scheme, and other steps, i. e., step 2, step 3 and step4 are similar. In step1, the supplier $S$ first computes the provenance record $D_1$ of the raw material and its ciphertext $C_1$when sending the raw material to the producer $P$, and then utilize the private key $p_i$ to generate the signature $\omega_1$ of the provenance record $D_1$. As last, the supplier $S$ can create a transaction TX stored on the blockchain by the Transaction Contract. (J1, J2, J3 and J4 denote different lengths).

### 4.3.3. Remote validation

When receiving the product, the user $U$, as an auditor, can remotely

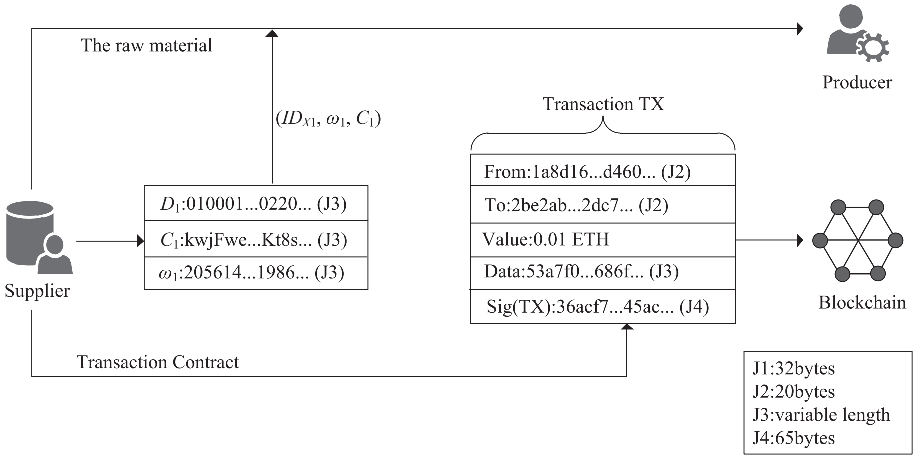

The raw material
Producer
$(ID_{X1}, \omega_1, C_1)$
Transaction TX
From:1a8d16...d460... (J2)
To:2be2ab...2dc7... (J2)
Value:0.01 ETH
Data:53a7f0...686f... (J3)
Sig(TX):36acf7...45ac... (J4)
$D_1$:010001...0220... (J3)
$C_1$:kwjFwe...Kt8s... (J3)
$\omega_1$:205614...1986... (J3)
Supplier
Blockchain
Transaction Contract
J1:32bytes
J2:20bytes
J3:variable length
J4:65bytes

**Fig. 6.** A computational example of step 1.

execute the validation of provenance record by the transaction-based validation mechanism, preventing the record stored on the CS from being illegal modified or replaced by malicious CSP. More specifically, the user $U$ can first download the transaction information from the blockchain, and then use the transaction information to perform the remote validation of provenance record with CS. More specifically, the user $U$ computes $ID_{Xi} = Register(pw_{Xi}, h(sk_{Xi}))$ and executes the Authentication Contract shown in Fig. 7 to prove that he/she is a valid user, where $t = 1$ denotes the authentication succeeds and $t = 0$ denotes the authentication fails. If $ID'_{Xi} = ID_{Xi}$, it means that the authentication succeeds and the user $U$ can go on performing the following steps:

- The user $U$ requires CS to offer the value $\omega_3$ and downloads the transaction TX$_3$ from blockchain.
- The user $U$ parses Data $= h_1(ID_{X3})||h_1(D_3)||h_1(C_1||C_2||C_3)||T||h_{bl}$ from the transaction TX$_3$ and checks the timeliness of the value $T$.
- The user $U$ checks the validity of the hash value $h_{bl}$ and parses $h_1(C_1||C_2||C_3)$ from Data.
- The user $U$ checks the correctness of equation as $e(\omega_3, g) = e(h_1(C_1||C_2||C_3), q_3)$.

*4.3.4. Fair payment*

In the SCM system, the stakeholders, i.e., the producer, retailer and the user need to pay for the raw material or product provided by previous stakeholder. To achieve fair payment in the SCM system, the stakeholders can utilize the smart contract to construct secure payment protocols. As shown in Fig. 8, the stakeholder $X_i$ ($i = 2,3,4$) submits the Payment Contract to blockchain, where the output result of the Payment Contract is $t$. When the equation holds as $e(\omega_i, g) = e(h_1(C_1||C_2||\cdots||C_i), q_i)$, the stakeholder $X_{i+1}$will be required to pay the stakeholder $X_i$ for the product. Otherwise, the stakeholder $X_i$ needs to make compensation to the stakeholder $X_{i+1}$.

## 5. Security analysis

In this section, we will provide the security analysis of our proposed scheme as follows.

### *5.1. Resistance to the tampering attack*

In our scheme, the product provenance record $D_i$ is encrypted by the secure symmetric encryption algorithm and converted into the ciphertext, where the content of ciphertext is chaotic and indistinguishable for all stakeholders. Thus, it is difficult for the adversaries to tamper with the product provenance record.

```
Authentication Contract
Require {
        The identity $ID'_{Xi}$ ,
        The user's password $pw_{Xi}$,
        The user's private key $sk_{Xi}$,
        The value of function $Register(pw_{Xi}, h(sk_{Xi}))$,
        }
Execute {
        if ($ID'_{Xi}$==$Register(pw_{Xi}, h(sk_{Xi}))$){
        Allow the user to access the blockchain;
        $t = 1$;                                   }
        else{
        Forbid  the user to access the blockchain;
        $t = 0$;                                   }
        }
Output : $t$
```

**Fig. 7.** Authentication Contract.

```
Payment Contract
Require {
        The stakeholder's address $Add_{Xi}$,
        The stakeholder's address $Add_{Xi+1}$,
        The value of function $e(w_i, g)$,
        The value of function $e(h_1(C_1||C_2||\cdots||C_i), q_i)$,
        }
Execute {
        if ($e(w_i, g)$==$e(h_1(C_1||C_2||\cdots||C_i), q_i)$){
        Pay $Q_E$ from $Add_{Xi+1}$ to $Add_{Xi}$;
        $t = 1$;                                   }
        else {
        Pay $Q_C$ from $Add_{Xi}$ to $Add_{Xi+1}$;
        $t = 0$;                                   }
        }
Output: $t$
```

**Fig. 8.** Payment Contract.

### 5.2. Resistance to the collusion attack

As previously mentioned, the product provenance record will be encrypted into the ciphertext $C$ and finally stored on CS. Thus, all stakeholders cannot modify or recover it to the plaintext without the valid encryption key $K$. The adversaries may launch the collusion attack to compromise the integrity of the ciphertext $C$. Specifically, they may collude with CSP to get the ciphertext $C$ stored on the CS, and replace the original ciphertext $C$ with the wrong ciphertext $C^*(C^*\neq C)$, where the end user finally downloads wrong data from CS. In our scheme, the user can utilize BLS signature to achieve the validation of product provenance record, where the correctness can be elaborated as follows:

$$e(\omega_3, g) = e(h_1(C_1||C_2||C_3)^{p3}, g)$$
$$= e(h_1(C_1||C_2||C_3), g^{p3})$$
$$= e(h_1(C_1||C_2||C_3), q_3)$$

When the above equation does not hold, it means that the integrity of ciphertexts $C_1||C_2||C_3$ stored on CS has been compromised. Therefore, our proposed scheme can effectively thwart collusion attack.

### 5.3. Resistance to the impersonation attack

In the traditional SCM system, the external adversaries may perform the password-guessing to extract the stakeholders' identity $ID$ from the password $pw$. If the external adversaries succeed, they can impersonate the legitimate stakeholders to access the SCM system and learn more private information about the products of SCM system. In our proposed scheme, specific identity token with higher security level is adopted, where each stakeholder needs a valid identity $ID$ to access the supply chain system. More specifically, we utilize the smart contract to achieve the secure registration for all stakeholders, where the Registration Contract can be performed to enable the stakeholders to get the final account address by multiple secure parameters, e.g., the hash function $h$(.), the hash value of privacy key $sk$. The external adversaries cannot modify the registration protocol and directly extract the stakeholders' identity $ID$ even if they know about the password $pw$. Therefore, our proposed scheme is secure against impersonation attack.

### 5.4. The necessity of blockchain

In our scheme, we mainly take advantage of the blockchain technology to construct a secure SCM system. On the one hand, we integrate some information, e.g., the identity of stakeholder, the hash value of ciphertext, the time, etc., into the transactions and deploy them on the blockchain, by which every stakeholder can achieve the auditability and traceability of product provenance record during the process of product circulation. On the other hand, we utilize the smart contract to construct secure payment protocols, by which the stakeholders have to abide by the payment protocols and pay for the product cost. Especially, if there is the human error or intentional misconduct in inputting the data onto the blockchain, the participant $X_{\text{i}}$ can only create a new transaction TX to fix the mistake. Specifically, each participant $X_{\text{i}}$ needs to compute the parameter $Data$ and take it as the input value to create a transaction TX. If the input value $Data$ uploaded by the participant $X_i$ is changed to the parameter $Data^*$ ($Data^*\neq Data$) due to the human error or intentional misconduct, a new transaction TX*(TX $^*\neq$ TX) will be created by the participant $X_i$. Due to the characteristics of blockchain, the invalid transaction TX* on the blockchain cannot be modified, edited and deleted by anyone. The participant $X_i$ can only create a new transaction TX again (The input value is $Data$) and then broadcast the valid transaction TX to other participants by the information flow of supply chain.

## 6. Performance evaluation

In this section, we will provide a simulation experiment to evaluate the performance of our proposed scheme, which is conducted on the test computer with Intel Core i5-7300HQ CPU, 16.0 GB RAM and 64-bit operating system.

### 6.1. Security comparison

In terms of SCM system, Giannakis et al. (Giannakis et al., 2019) proposed a cloud-based supply chain management (C-SCM) system to improve supply chain responsiveness (SCR), which used a sequential analytical method to analyze and present the internal structure of C-SCM. However, it may lead to data leakage in the product circulation due to the over-reliance on CSP. Dwivedi et al. (Dwivedi et al., 2020) proposed a secure and efficient supply chain system, which adopted the frequency identification (RFID) to create the unique identity of the product and the smart contract to achieve the fairness and security in the product circulation. Lou et al. (Lou et al., 2021) proposed a blockchain-based scheme for information sharing to realize a SCM system, which utilized the smart contract to achieve the management of key, the validation of transaction and block. However, the above two schemes will be subjected to the collusion attack owing to the introduction of fully trusted certificate authority (CA). In our proposed scheme, we utilize the blockchain technology and pairing-based cryptography to realize a more secure SCM without introducing any fully trusted intermediary. More security comparisons are shown in Table 2.

### 6.2. Computation cost

In this section, we will evaluate the computation cost of our proposed scheme, consisting of the three stages: Registration, Product circulation and Record validation, where the Production circulation stage includes four steps in our scheme, i.e., Step I, Step II, Step III, Step IV. Especially, the notations of cryptographic operation and their descriptions are summarized in Table 3. Table 4 shows the computation cost in different stages, which demonstrates our scheme is practice and efficient with a reasonable computation cost.

### 6.3. The gas cost of smart contract

In this section, we will evaluate the gas cost of Registration Contract and Authentication Contract proposed in our scheme, where the experimental platform is the Remix-IDE and the programing language is the solidity with version 0.4.19. We denote the supplier as "A", the provider as "B", the retailer as "C", the CS as "D" and the user as "E", respectively. The experiment result shown in Fig. 9, reveals the transaction gas consumed by different stakeholders in the Registration Contract and Authentication Contract, where the gas cost consumed is almost same in one smart contract.

### 6.4. The computation cost of validation

In this section, we will carry out an experiment to evaluate the computation cost of validation in the reality environment, where the processes of validation mainly include the encryption of product information, the signature of product information and the correction verification of product information. In our scheme, the stakeholders (except

**Table 2**
Security comparison.

| Scheme | Giannakis et al. (Giannakis et al., 2019) | Dwivedi et al. (Dwivedi et al., 2020) | Lou et al. (Lou et al., 2021) | Our scheme |
|---|---|---|---|---|
| Privacy protection | Y | Y | Y | Y |
| Traceability | N | Y | Y | Y |
| Fair payment | N | N | Y | Y |
| Resistance to collusion attack | N | N | N | Y |

**Table 3**
Notations and their descriptions.

| Notation | Description |
|---|---|
| $P_O$ | The pairing exponentiation |
| $P_E$ | The bilinear map function |
| $X_{OR}$ | The XOR operation |
| $M_G$ | The multiplication on group $G$, $G_T$ |
| $H$ | The SHA-256 hash function |
| $T_G$ | A transaction generation operation |
| $R_E$ | The encryption operation |

**Table 4**
The computation overhead in different stages.

| Stakeholder | Supplier | Producer | Retailer | User | CS |
|---|---|---|---|---|---|
| Registration | $2H+X_{OR}$ | $2H+X_{OR}$ | $2H+X_{OR}$ | $2H+X_{OR}$ | $2H+X_{OR}$ |
| Step I | $R_E+H+M_G$ | —— | —— | —— | —— |
| Step II | $T_G+3H$ | —— | —— | —— | —— |
| Step III | —— | $P_E+2P_O+5H+R_E+M_G+T_G$ | —— | —— | —— |
| Step IV | —— | —— | $P_E+2P_O+5H+R_E+M_G+T_G$ | —— | $P_E+H+2P_O$ |
| Remote validation | —— | —— | —— | $P_E+2P_O$ $2H+X_{OR}$ | —— |

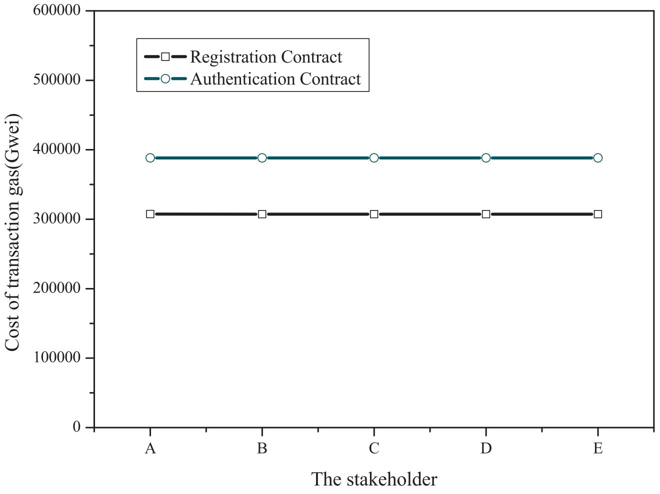


**Fig. 9.** The gas cost of smart contract.

the supplier), i.e., the producer, the retailer and CS, need to perform the correction verification of product information. Especially, a supply chain is simulated in the experiment, where SHA-256 and AES are used to compute secure hash values and ciphertexts, respectively. Meanwhile, the JPBC library (Caro and Iovino, 2011) is introduced to execute the pairing operation. We assume the number of supply chain is $n$ and each supply chain is independent, where one supply chain involves a supplier, a producer, a retailer and a CS. The experiment result shown in Fig. 10, demonstrates that our proposed scheme is efficient and feasible with less computation cost. For a retailer, it only takes 1.335 s to execute the validation of product record in one supply chain.

## 7. Conclusion and future work

In this paper, we propose a blockchain-based decentralized SCM system with secure information sharing, which utilizes the BLS signature to construct two validation mechanisms, i.e., one-way validation and transaction-based validation to achieve the validation of the product provenance record for the stakeholders in SCM system. Moreover, the payment protocols is designed to achieve fair payement by the smart contract,where the stakeholders can reliably pay for the product without relying on any certificate authority. The security analysis demonstrates that our scheme can achieve the resistance to the tampering attack, collusion attack and impersonation attack, and the performance evaluation show that our scheme is efficient and feasible with a reasonable computation cost.

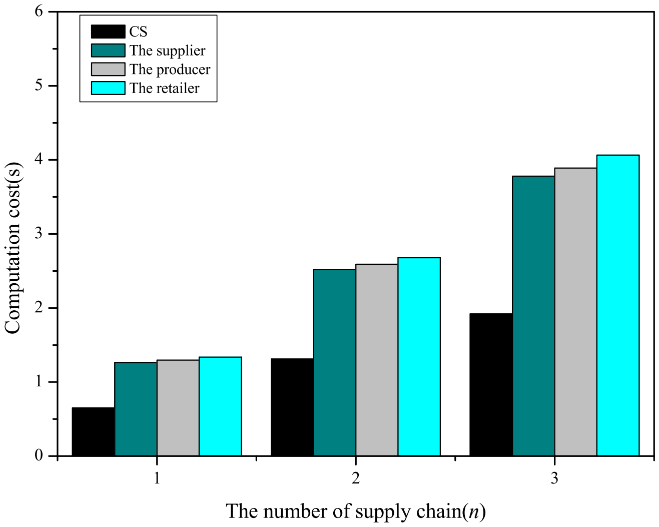


**Fig. 10.** The computation cost of validation.

In our scheme, we utilize the blockchain technology, i.e., smart contract and transaction-based storage structure, to achieve secure information sharing for the stakeholders in SCM system. However, the blockchain includes many other parts, such as the participation of miners, the consensus mechanism, and P2P network framework, etc., which have not been involved in our scheme and make it difficult to evaluate a comprehensive performance of proposed SCM system. For the future work, we will plan to study how to combine more structural features of blockchain with the traditional SCM system to construct a more secure and efficient SCM system.

## CRediT authorship contribution statement

**Guipeng Zhang:** Conceptualization, Methodology, Writing – review & editing. **Zhenguo Yang:** Conceptualization, Investigation. **Wenyin Liu:** Supervision, Project administration.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

The data that has been used is confidential.

## References

A. Alahmadi, X. Lin, Towards Secure and Fair IIoT-Enabled Supply Chain Management via Blockchain-Based Smart Contracts, in ICC 2019 - 2019 IEEE International Conference on Communications (ICC). 2019. p. 1-7.

Bader, L., Pennekamp, J., Matzutt, R., et al. (2021). Blockchain-based privacy preservation for supply chains supporting lightweight multi-hop information accountability. *Information Processing & Management, 58*(3), Article 102529.

Benil, T., & Jasper, J. (2020). Cloud based security on outsourcing using blockchain in E-health systems. *Computer Networks, 178*, Article 107344.

Biswas, B., & Gupta, R. (2019). Analysis of barriers to implement blockchain in industry and service sectors. *Computers & Industrial Engineering, 136*, 225–241.

Boneh, D., & Franklin, M. (2003). Identity-based encryption from the weil pairing. *SIAM Journal on Computing, 32*(3), 586–615.

Boneh, D., Lynn, B., & Shacham, H. (2004). Short signatures from the weil pairing. *Journal of Cryptology, 17*(4), 297–319.

Bürer, M. J., De Lapparent, M., Pallotta, V., et al. (2019). Use cases for Blockchain in the Energy Industry Opportunities of emerging business models and related risks. *Computers & Industrial Engineering, 137*, Article 106002.

Cao, S., Zhang, G., Liu, P., et al. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences, 485*, 427–440.

Caro, A.D., Iovino, V., jPBC: Java pairing based cryptography, in 2011 IEEE Symposium on Computers and Communications (ISCC). 2011. p. 850–855.

Choi, T., Cai, Y., & Shen, B. (2019). Sustainable fashion supply chain management: A system of systems analysis. *IEEE Transactions on Engineering Management, 66*(4), 730–745.

A. Dahbi, H.T. Mouftah, Supply chain efficient inventory management as a service offered by a cloud-based platform, in 2016 IEEE International Conference on Communications (ICC). 2016. p. 1-7.

Du, M., Chen, Q., Xiao, J., et al. (2020). Supply chain finance innovation using blockchain. *IEEE Transactions on Engineering Management, 67*(4), 1045–1058.

Dwivedi, S., Amin, R., & Vollala, S. (2020). Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. *Journal of Information Security and Applications, 54*, Article 102554.

Giannakis, M., Spanaki, K., & Dubey, R. (2019). A cloud-based supply chain management system: Effects on supply chain responsiveness. *Journal of Enterprise Information Management, 32*(4), 585–607.

Gonul Kochan, C., Nowicki, D. R., Sauser, B., et al. (2018). Impact of cloud-based information sharing on hospital supply chain performance: A system dynamics framework. *International Journal of Production Economics, 195*, 168–185.

Guo, D., Dong, J., & Wang, K. (2019). Graph structure and statistical properties of Ethereum transaction relationships. *Information Sciences, 492*, 58–71.

Hu, T., Liu, X., Chen, T., et al. (2021). Transaction-based classification and detection approach for Ethereum smart contract. *Information Processing & Management, 58*(2), Article 102462.

Jinqi, P., Taiyang, P., Lei, R., The Supply Chain Network on Cloud Manufacturing Environment Based on COIN Model with Q-Learning Algorithm, in 2017 5th International Conference on Enterprise Systems (ES). 2017. p. 52–57.

Koirala, R.C., Dahal, K., Matalonga, S., Supply Chain using Smart Contract: A Blockchain enabled model with Traceability and Ownership Management, in 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). 2019. p. 538–544.

Le, G., Gu, Q., Jiang, Q., et al., TrustedChain: A Blockchain-based Data Sharing Scheme for Supply Chain. 2020. 895-901.

Leng, J., Ye, S., Zhou, M., et al. (2021). Blockchain-secured smart manufacturing in industry 4.0: A survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51*(1), 237–252.

Li, L., Liu, J., Chang, X., et al. (2020). Toward conditionally anonymous bitcoin transactions: A lightweight-script approach. *Information Sciences, 509*, 290–303.

Li, M., Shen, L., & Huang, G. Q. (2019). Blockchain-enabled workflow operating system for logistics resources sharing in E-commerce logistics real estate service. *Computers & Industrial Engineering, 135*, 950–969.

Lim, M. K., Li, Y., Wang, C., et al. (2021). A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Computers & Industrial Engineering, 154*, Article 107133.

Lin, I., Hsu, H., & Cheng, C. (2015). A cloud-based authentication protocol for RFID supply chain systems. *Journal of Network and Systems Management, 23*(4), 978–997.

Lou, M., Dong, X., Cao, Z., et al. (2021). SESCF: A secure and efficient supply chain framework via blockchain-based smart contracts. *Security and Communication Networks, 2021*, 1–18.

Mehta, D., Tanwar, S., Bodkhe, U., et al. (2021). Blockchain-based royalty contract transactions scheme for Industry 4.0 supply-chain management. *Information Processing & Management, 58*(4), Article 102586.

S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system. 2008; Available: https://bitcoin.org/bitcoin.pdf.

Rachana Harish, A., Liu, X. L., Zhong, R. Y., et al. (2021). Log-flock: A blockchain-enabled platform for digital asset valuation and risk assessment in E-commerce logistics financing. *Computers & Industrial Engineering, 151*, Article 107001.

Raj Kumar Reddy, K., Gunasekaran, A., Kalpana, P., et al. (2021). Developing a blockchain framework for the automotive supply chain: A systematic review. *Computers & Industrial Engineering, 157*, Article 107334.

Wang, H., Qin, H., Zhao, M., et al. (2020). Blockchain-based fair payment smart contract for public cloud storage auditing. *Information Sciences, 519*, 348–362.

Wei, P. C., Wang, D., Zhao, Y., et al. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems, 102*, 902–911.

Wu, D., & Wu, D. D. (2020). A decision support approach for two-stage multi-objective index tracking using improved lagrangian decomposition. *Omega, 91*, Article 102017.

Yuan, H., Chen, X., Wang, J., et al. (2020). Blockchain-based public auditing and secure deduplication with fair arbitration. *Information Sciences, 541*, 409–425.

Zhang, G., Yang, Z., & Liu, W. (2021). Blockchain-based privacy preserving e-health system for healthcare data in cloud. *Computer Networks, 203*, Article 108586.

Zhang, G., Yang, Z., Xie, H., et al. (2021). A secure authorized deduplication scheme for cloud data based on blockchain. *Information Processing & Management, 58*(3), Article 102510.