future internet

MDPI

Article

SmartDED: A Blockchain- and Smart Contract-Based Digital Electronic Detonator Safety Supervision System

Na Liu [1,*] and Wei-Tek Tsai [1,2,3,*]

[1] Digital Society& Blockchain Laboratory, Beihang University, Beijing 100191, China
[2] Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287, USA
[3] Fuzhou FuYao Institute for Advanced Study, Fuzhou 350300, China
* Correspondence: liuna1@sie.edu.cn (N.L.); tsai7@yahoo.com (W.-T.T.)

Abstract: Digital electronic detonators, as a civil explosive, are of prime importance for people's life and property safety in the process of production and operation. Therefore, the Ministry of Industry and Information Technology and the Ministry of Public Security of the People's Republic of China have extremely high requirements for their essential safety. Existing schemes are vulnerable to tampering and single points of failure, which makes tracing unqualified digital electronic detonators difficult and identifying the responsibility for digital electronic detonator accidents hard. This paper presents a digital electronic detonator safety supervision system based on a consortium blockchain. To achieve dynamic supply chain supervision, we propose a novel digital electronic detonator supervision model together with three codes in one. We also propose a blockchain-based system that employs smart contracts to achieve efficient traceability and ensure security. We implemented the proposed model using a consortium blockchain platform and provide the cost. The evaluation results validate that the proposed system is efficient.

Keywords: DED safety; supply chain; blockchain; smart contract

check for updates

Citation: Liu, N.; Tsai, W.-T. SmartDED: A Blockchain- and Smart Contract-Based Digital Electronic Detonator Safety Supervision System. *Future Internet* **2024**, *16*, 171. https://doi.org/10.3390/fi16050171

Academic Editor: Gianluigi Ferrari

Received: 22 March 2024
Revised: 3 May 2024
Accepted: 3 May 2024
Published: 16 May 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Digital electronic detonator (DED) safety is very crucial to people's lives. The security of electronic supervision has received much attention due to numerous underlying vulnerabilities, threats, and attacks. The security aspect of electronic systems has been limited to various vulnerabilities [1–3]. The DED supply chain involves three major problems. First, manufacturers might produce unqualified DEDs or even modify detonator records. Second, DED transportation might fail to comply with safety transportation regulations. Third, unqualified suppliers might collude with blasting enterprises (BAEs) to sell and use unqualified DEDs. Thus, there has since been an urgent call to develop a credibility and traceability system that ensures DED safety.

To address the aforementioned DED supply chain issues, establishing a DED traceability system can trace DED quality and protect DED circulation safety. The current DED traceability systems face many problems. For example, traditional information management suffers from single points of failure and tampering. In addition, each participant needs to maintain the data using its database, which causes an information island. Thus, it is not easy to build an efficient trust between all participants in the circulation of the DED. The data integrity of the blockchain is guaranteed from two aspects. First, due to hash function technology, a blockchain has the feature of immutability and tamper resistance. Second, powered by its consensus protocol, a blockchain ensures that all peers in the decentralized P2P network maintain the same replicas of the data. These cryptographic security mechanisms, as well as the decentralized architecture and provenance features enable blockchain as a potential technology that improves the system efficiency and guarantees the traceability and security of the supply chain.

Blockchain technology can be used in multiparty collaboration because it addresses problems such as data transparency, system efficiency, data provenance, and traceability and safety supervision in supply chains. Most research has been adapted to the application of supply chains using blockchain technology. Yan Cao et al. [4] proposed a blockchain-based system for tracing the quality of steel products. They combined blockchain, RFID, GPS, and a wireless sensor network to regulate the production, transportation, consumption, and supervision of steel materials. They prototyped the steel product traceability system on the Sawtooth platform of Hyperledger. Every steel product is identified by an RFID tag, which is the virtual identification of the product in the system. Agrawal et al. [5] presented a blockchain-based traceability framework for the Textile and Clothing (T&C) supply chain to address the issue of data manipulations. Although the proposed framework is designed for the T&C supply chain, it can be adapted to any supply chain by making certain modifications. Omar et al. [6] proposed an Ethereum-blockchain-based system that tracks and verifies Personal Protective Equipment (PPE) in a decentralized network using smart contracts and the Interplanetary File System (IPFS). Zoughalian et al. [7] proposed a prototype that ensures the integrity of data using zero-knowledge proof in a pharmaceutical distribution system and developed the Markov model to calculate the reputation score of each node in a trust-based decision-making process.

However, there is no perfect traceability system in the traditional explosives industry; especially, traditional detonator tracing systems are subject to tampering and single points of failure because each entity in the detonator circulation needs to store the circulation data in its database, which results in low transparency, centralization, and information island. Thus, an effective digital electronic supervision system is much desired. This system could help to solve the trust issue in the supply chain, especially when DED safety accidents occur. The primary goal of this paper is to develop a trusted, blockchain-based DED supervision system. There are two challenges in constructing an effective digital electronic detonator supervision system. First, there is a lack of reliable DED traceability management. For example, when a DED accident occurs, the BAE is unable to track the DED product and circulation information.

Second, the regulation of transportation still has challenges to be solved. The safety management regulation, especially during DED transportation, is known to have a significant impact on the system. Thus, preventing fatal accidents caused by premature explosions should be a very important requirement for DED tracing [8].

To meet these challenges, we propose a blockchain-based DED supervision system, which simultaneously ensures reliable DED traceability and transportation safety. This system enables the users to query the DED information from production and distribution to the blasting of DEDs. We propose a DED supervision model with three codes in one mechanism that store the DED data on a blockchain before querying, inserting, and modifying them in a distributively verifiable manner, which can track and trace the DEDs. To store the circulation data, the key–value tables serve as the primary data structure for maintaining DED circulation data. To ensure the safety supervision of the DEDs in the supply chain, we employ smart contracts to allow relevant participants to upload and validate DED data on the blockchain.

Our proposed system ensures DED safety supervision as follows. First, all the DED information stored on the blockchain cannot be modified. Once a DED explosion accident occurs, the information cannot be tampered with because of the consensus and cryptographic mechanism. Second, the DED information can be verified on the blockchain. Therefore, no one can deny his/her responsibility. Third, the data using the key–value stored on the blockchain contribute to tracking the provenance and transportation of DEDs. To summarize, we make the following major contributions:

- To the best of our knowledge, this is the first work on a DED supervision system to achieve traceability and verification on the blockchain network using blockchain and smart contracts.

- We propose a novel DED supervision model, together with three codes in one and the algorithms that can regulate the whole process of DED circulation.
- We designed a blockchain- and smart contract-based DED supervision system that instantiates the supervision model. We used a blockchain to store the circulation of the DED in the supply chain. During the circulation process, the smart contracts can be used to verify that the DED data on the blockchain are consistent with the received DED information.
- We leveraged a consortium blockchain platform, i.e., FISCO BCOS, to implement the DED system for supervision. We conducted empirical studies to validate the performance of the supervision system.

The rest of the paper is organized as follows. Section 2 describes existing studies on blockchain for supply chain management. In Section 3, we present a blockchain-based DED system architecture and a supervision model. The smart contract design for DEDs is introduced in Section 4. The result is presented in Section 5. Finally, Section 6 concludes.

2. Related Work

2.1. Blockchain for Supply Chain Management

With its decentralization features, blockchain technology can be adopted in scenarios of multiparty collaboration, since it addresses various issues such as data transparency, traceability, system deficiency management ability, and the system efficiency of important information in supply chains. Some researchers have utilized blockchain to develop the application of industrial and agricultural traceability systems. However, there is no research on DED safety issues using blockchain technology.

Malik et al. [9] proposed a consortium blockchain framework that can find food provenance and a holistic platform for participants, regulatory bodies, and consumers. Abeyratne et al. [10] presented a conceptual model in the manufacturing supply chain using blockchain and leveraged cardboard boxes as an example to explain the process from manufacturing to recycling. Liu et al. [11] proposed an architecture based on a consortium blockchain-empowered port supply chain system and presented a verification system framework for the smart contracts of the port supply chain with probabilistic behaviors. Zhang et al. [12] proposed a private chain to maintain the agriculture product traceability information and an alliance chain to search and share traceability information. Rajput et al. [13] presented an IoT-based food supply chain framework to utilize smart contracts to handle the transactions between parties for smart agriculture. These works presented frameworks and models of blockchain in supply chains. LI et al. [14] examined the coupling between blockchain technology and supply chain finance and then presented the conceptual framework of the blockchain-driven supply chain finance (BcSCFP) platform on which the process of three basic financing models was designed. Haque [15] presented a conceptual framework, which made use of blockchain and smart contracts to achieve efficient monitoring and traceability in the decentralized oil supply chain. In addition, more works have focused on protecting user privacy and data privacy. Maity et al. [16] integrated a blockchain system into the stochastic models to improve traceability and protect data privacy and security. Weber et al. [17] introduced a blockchain-based technology into the choreography of processes, which can coordinate the business processes in the execution of a collaborative process. Veerasamy et al. [18] proposed a blockchain-based peer-to-peer energy trading system that provides a robust and secure solution and presented a novel framework using local differential privacy (LDP) with federated learning for resilient frequency control in microgrids, considering the potential occurrence of adversarial attacks. Chen et al. [19] developed a blockchain-based searchable encryption for EHRs that leveraged an Ethereum smart contract to trace monetary rewards. The proposed index was constructed by a complex Boolean expression to achieve a reliable and confidential search mechanism. Zhuang et al. [20] adopted the blockchain technique and secret sharing scheme to present a privacy-preserving and traceability identity information management scheme for intellectual property.

There are also some research works that integrated blockchain and machine learning technology. Ismail et al. [21] presented an Intelligent supply chain framework, which integrated blockchain and machine learning to track and trace fish products throughout the entire life cycle in the fish supply chain. Dos Santos et al. [22] introduced a supervisory mechanism in the Agri-food supply chain, which leveraged smart contracts and Ethereum tokens to provide economic incentives to the participating stakeholders in the supply chain. Wu et al. [23] developed a novel framework that uses computer vision algorithms and blockchain technology to improve the traceability of on-site construction activities (OCAs).

2.2. Explosives Management System

Internet of Things (IoT) technology has been widely used for real-time monitoring of the environment With the improvement of our country's industrialization, enterprises' and our society's demand for dangerous goods is increasing. This makes dangerous goods logistics an important branch of the logistics area. With the application of the Internet of Things technology, the modernization of explosive dangerous goods' transport management is urgent. Liu, C et al. [24] leveraged GPS technology, RFID technology, and GPS mobile communication technology to monitor, track, and alarm. Applying Internet of Things technology to explosive dangerous goods' transport, it contributed to reducing the risk of accidents and protecting people and property. Qin, X et al. [25] designed an explosive production monitoring system based on the Internet of Things and proposed a new architecture including an explosives production information collection perception layer, network communication layer, and comprehensive application layer. Zhang, Li et al. [26] discussed a three-layer Mine IoT (MIoT) architecture, including a perception layer used for collecting data, a network layer used for transmitting data, and an application layer used for analyzing the data and information. However, there is no entire process of production information management platform including production, transport, sale, and blasts to alleviate social and public safety concerns.

3. Blockchain-Based DED Supervision Model and Architecture

This section presents the proposed DED supervision system architecture employing a consortium blockchain and smart contracts. To support effective supervision, we designed a supervision model for ensuring digital electronic detonators' safe circulation. However, traditional and popular methods of digital electronic traceability and supervision still face serious security issues including single points of failure and tampering with circulation data.

The primary purpose of the study is to extend research on digital electronic management mechanisms in China. The study aims to explore how blockchain can be used in existing regulatory practices to provide a supervision model.

3.1. DED Supervision Model

We first detail and describe the main factors including the members, work code, and circulation of DEDs. We then introduce an abstract model for regulating the whole process of the DEDs.

The Public Security organ is a supervisor authority to regulate DEDs in China. The National Industrial Electronic Detonation Cryptography Centre (NIEDCC) is responsible for storing and issuing work codes. The manufacturer (MAU) carries out the product plan. The sales enterprise (SAE) purchases DEDs from the MAU. The SAE sells the digital electronic detonator to the blasting enterprise (BAE). The blasting enterprise provides blasting services to the users. A competent logistics enterprise (LE) is in charge of transporting the digital electronic detonators. Thus, the system model involves the MAU, SAE, BAE, LE, NIEDCC, and supervisory agencies.

Work code: To achieve dynamic DED supply chain supervision, we integrated the production link, purchase link, transport link, and blasting link into the supervision model. We first established a mechanism of the DEDs with three codes in one mechanism, which

includes the chip UID code, initiating code, and detonator shell code. Three codes are encrypted to generate the work code; furthermore, the work code generates the identification code, which is labeled with the barcode. If a DED accident occurs, we can determine the DED and track it according to the three-code information. At each stage of the circulation of DEDs, it is necessary to update the DED information to track and verify the circulation of the electronic detonators.

In the production of DEDs, each electronic detonator is labeled with the barcode on the terminal clamp of the DED. First, the electronic detonators' information is recorded in an information system, which maintains all information about the product from the raw materials to the product, including the manufacturer, DED batch, DED name, and time. After receiving the DED, the SAE scans the barcode and checks the consistency of the barcode data and the records stored in the information system. After that, the sales enterprise uploads the data to the blasting enterprise. The blasting enterprise should also scan the barcode to verify the information on the DED before the electronic detonators are stored.

In the production of DEDs, the MAUs upload the work code to the NIEDCC and are put on record by the supervisory agent, and they can perform the production plan. The MAU's management system is associated with the supervision system, which means that the production records are involved in the supervision system to prevent falsified DED records of the MAU. The digital electronic detonators are only purchased from the MAU by the SAE. The information system comprehensively maintains all the processes of the DEDs from production to consumption.

In the transportation sector, the DEDs are sent from the manufacturer to the SAE and then transported from the SAE to the blasting enterprise. All logistic enterprises must also be put on record by the supervision agent.

In the blasting sector, the blasting enterprises need to apply to the National Industrial Electronic Detonator Cryptography Centre (NIEDCC) for the working code and then download the electronic detonator working code from the NIEDCC. Finally, the initiator loads and decrypts the encrypted information. All blasting enterprises must also be audited by the supervisor and have blasting qualifications to carry out blasting operations. After blasting, the detonator first feeds back the information, including the chip UID and the DED latitude and longitude, to the adapter through the regulatory authority. Next, the information is uploaded to the National Industrial Electronic Detonation Cryptography Centre, which contributes to identifying the reasons for and measures of Anti-explosion.

Figure 1 shows the DED supervision model. The supervision model is detailed as follows:

1. The manufacturer must submit application materials to apply for a safety production license and can carry out production activities after approval by a supervisory agent.

2. After reviewing the manufacturer's application materials, the supervisory agent returns the audit results regarding whether it will issue the certificates.

3. Each batch of DEDs is produced after approval.

4. When the electronic detonators are produced, the manufacture generates a working code and uploads it to the NIEDCC.

5–6. In the circulation process of the DEDs, the participants involved need to scan the labels and upload the DED data to the supervisory agent. The DED data include information such as the DED label, the barcode, and the SAE. When the digital electrical detonators are received, the SAE needs to check whether the data are consistent with those stored at the supervisory agent.

7. The blasting enterprise applies for a working code from the National Electronic Code Centre through the supervisory agency.

8. The blasting enterprise downloads the working code from the NIEDCC through the Industrial Electronic Detonator Working Code Download Adaptor.

9. The initiator loads and decrypts the encrypted information and then initiates the detonation.

10. The detonator feeds the information back to the adapter, including the product code information UID and the location information of the detonation's latitude and longitude. Then, the information is uploaded to the NIEDCC by the supervisory agency.

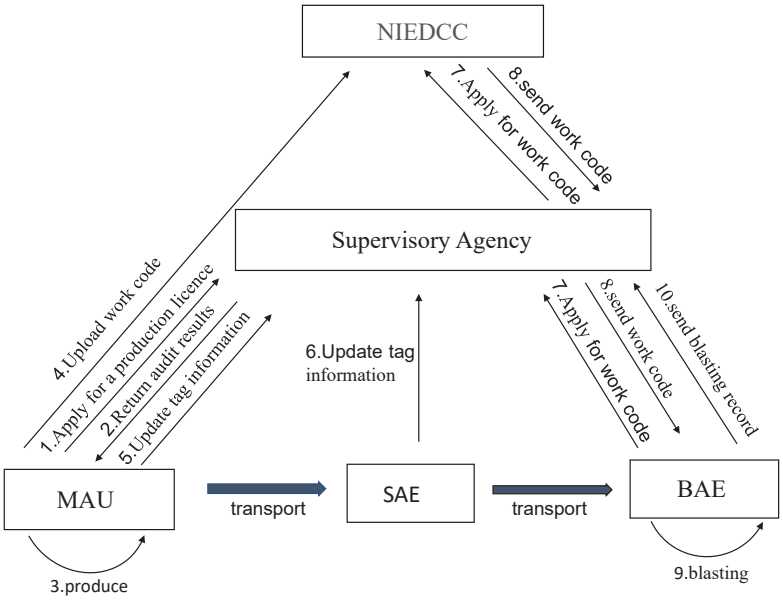


Figure 1. DED supervision model.

3.2. System Architecture

This paper proposes a blockchain-based DED safety supervision system. Figure 2 shows the system architecture, which involves three parts: (1) physical layer; (2) smart contract module layer; (3) blockchain layer. The system has five types of users, i.e., the MAU, SAE, LE, BAE, and supervisor. The DED traceability system leverages blockchain to record the circulation information during the whole process. As in the system model in Figure 1, the participants in DED traceability need to verify the safety and the correctness of the received DED. They should also prevent DED safety accidents, such as loss accidents and fatal accidents because of premature blasts.

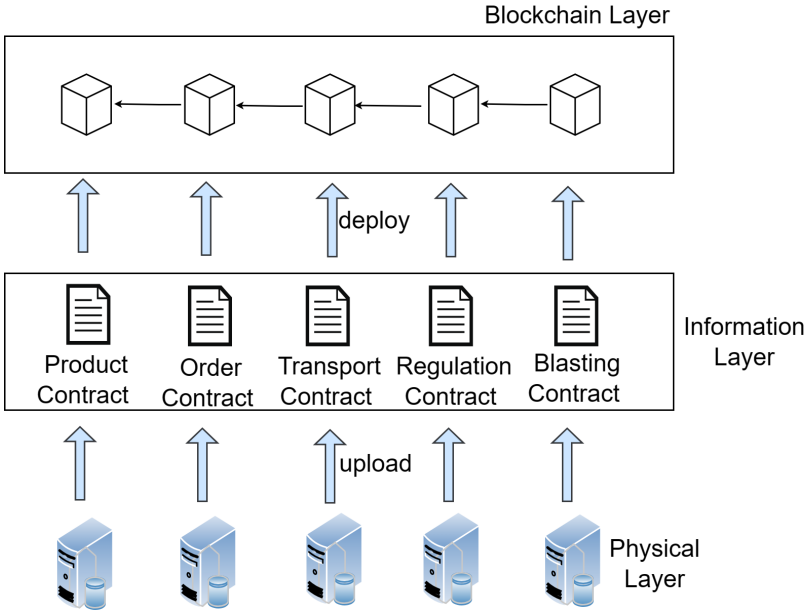


Figure 2. DED supervision system architecture.

Physical layer: The physical layer collects DED-related data in a timely manner, which leverages the Internet of Things (IoT) including survey cameras, wireless sensors, and GPS trackers to monitor temperature, pressure, and other environmental conditions [8].

Information layer: The information layer consists of five modules using the blockchain and smart contracts, the production transaction module, order transaction module, transportation transaction module, supervision module, and blasting module. The function of the production transactions module is to upload the work code to the NIEDCC, send the product information, and update the tag information.

The production transaction module is mainly used to manage the MAU record and upload the work code to the NIEDCC. The order transaction module is mainly used to process DED order transactions between the SAE and the MAU. The transportation transaction module is used to monitor the environment of the DEDs' transport, which includes the data collection of the temperature, humidity, pressure, and so on. The supervision management module is used for monitoring the DEDs to prevent loss and circulation records, which involves uploading the circulation record to the supervision system to bind with the identification code and verifying the data. The blasting module is responsible for managing the blasting process and uploading the blasting record to the NIEDCC.

Blockchain layer: The blockchain layer works as a peer-to-peer (P2P) network layer, which is used to integrate DED track-and-trace data for DED traceability. It records significant DED information regarding the circulation.

4. The Design of Smart Contracts

This section mainly designs the smart contracts to ensure DED traceability and safety in the DED supervision system. We first introduce five smart contracts to realize the corresponding module, namely product contracts, order contracts, transport contracts, regulation contracts, and blasting contracts, followed by the data structure of each contract. In addition, we designed another five contracts used for identity management, which can only be invoked by a supervisory agent.

The five smart contracts correspond to the five modules. First, The identity management contract needs to be accessed. After that, the supervisor provides query services for DED-related information. The data structure and the function of the contracts are described in the following. We used a key–value table to indicate a transaction, which contributes to query circulation data by key–value storage. Note that the WeBank FISCO BCOS consortium blockchain [27] provides a key–value storage for the contracts. In addition, all the participants involved in the system make use of an identity number as a unique identity.

4.1. Product Contract

MAUs submit a safety production license to the supervisor as a record. After the supervisor approves the production license, this batch of DEDs will be assigned a work code and submitted to the NIEDCC. Table 1 shows the structures of the product contract. The meanings of the structures are detailed in Table 2. The smart contracts primarily cover the following functions in Table 3.

The detailed procedure of submitting a detonation production is described in Algorithm 1. First, we check the contract address corresponding to the MAU number; we create the table object T and the entry object e; then, we insert the object T with DED information including pro_no, DED_batch, and so on. Finally, the result of the function is returned, for which return_value is set to 0 if we successfully insert the object.

Table 1. The table of product transactions.

Pro_No.	DED_Batch	Name	Amount	Time	State	Hash_Data	Identify_Code
010001	521,894	HHH	$0 \times 3971\ldots$	180,000	2023-6-1 15:43	1	300,000,000
010002	134,241	HHC	$0 \times 8456\ldots$	240,000	2023-6-1 16:45	1	300,000,000
...	...	...	...	...	...	...	

Table 2. Notation.

Notation	Description
Pro_no	MAU identity number
DED_batch	DED batch number
DED_name	DED name
Time	The time of submitting the operation such as production, purchase, and so on
State	The status value is initially set to 0. It is set to 1 if the supervisor approves and −1 if it is refused.
identify_code	Identification code converted from the work code
SAE_no	SAE identity
Order_no	Order identification number
BAE_no	BAE identity number
LE_no	Logistic enterprise number
Shipper_no	Shipper identity number
consignee_no	Consignee identity number
UID	The identity of the DED
latitude	The location of DED initiation
longitude	The location of DED initiation

Table 3. Function.

Function	Description
manufacturer_check	query the provider number in the identity management contract to verify if the caller's account address matches the address recorded in the table
DED_submit	apply and submit the data
DED_process	query the provider number in the identity management contract to verify whether the caller's account address matches the address stored in Table 1
order_submission	used by the SAE to submit order requests to the MAU
order_process	used by the manufacturer to process orders and modify the status value of the Table 4
order_select	used to query order data according to pro_no and order_no
transport_process	used by the MAU to process orders and change the status field in the Table 5
circulation_table_BAE_insert	used to insert circulation data in Table 6
circulation_table_SAE_insert	used to insert circulation data in Table 7
trace_select	used to query DED circulation data according to the label number
hash_submit	used to submit the hash value of environmental data
transport_select	used to query order information according to the manufacturer number and order number
blasting_submit	used by the BAE to submit blasting requests to the SAE
blasting_process	used to process blasting record and modify the status value of Table 8

Algorithm 1 Submit a detonator production

Input: MAU identity number *pro_no*, name, amount, batch number, raw materials, and suppliers
Output: $return\_value \in (0, 1)$

if (identity management passes) **then**
  create table T;
  create entry object e;
  $e.pro\_no \leftarrow pro\_no$;
  $e.DED\_batch \leftarrow batch$;
  $e.DED\_name \leftarrow name$;
  $e.DED\_amount \leftarrow amount$;
  $e.material \leftarrow material$;
  $e.suppliers \leftarrow suppliers$;
  $e.hash\_data \leftarrow hash\_data$;
  $e.time \leftarrow int(now)$;
  $return\_value \leftarrow T.insert(pro\_no, e)$;
end if
return *return_value*;

4.2. Order Contract

The purpose of the order contract module is to process the order agreements submitted from the SAE to the MAU. The purchase plan is assigned by the SAE, and the DED data such as the DED name, time, and quantity are submitted to the MAE. Then, the MAU manages the purchase order. Table 4 shows the structure of the order contract.

Table 4. The table of order transactions.

Pro_No.	Batch	Amount	Name	Time	State	Hash_Data	SAE_No.	Order_No.
010001	521,894	180,000	HHC	2023-7-2 15:43	1	$0 \times 3971\ldots$	020002	000245
010002	134,241	240,000	HHH	2023-7-2 16:45	1	$0 \times 8456\ldots$	020002	000246
...	...	...	...	...	...	...	...	

Algorithm 2 shows the order process in detail.

Algorithm 2 Submit a purchase order

Input: MAU identity number *pro_no*
Output: $return\_value \in (0, 1)$

if (identity management passes) **then**
  create table object T;
  create entry object e;
  create condition object condition;
  $e.state \leftarrow circulation$;
  $condition.order\_no \leftarrow order\_no$;
  $return\_value \leftarrow T.update(pro\_no, e, condition)$;
end if
return *return_value*;

4.3. Transport Contract

The transport contract's functionality is to store the transportation order's shipper and Consignee information, which includes two parts in the process. The first part is the distribution from the MAU to the SAE, and the second part is the distribution from the SAE to the BAE. Table 5 shows the structures of the transport contract.

Table 5. The table of transport transactions.

LE_No.	Shipper_No.	Consignee_No.	Time	State	Hash_Data	Order_No.
040002	010001	020003	2023-7-3 17:03	1	$0 \times 3971\ldots$	00001664
040002	020001	020003	2023-7-3 18:12	1	$0 \times 8456\ldots$	00001665
...	...	...	...	...	...	...

Algorithm 3 presents the environment hash of the contract. First, if the contract address of the identity management contract is verified corresponding to the LE number, the entry object and the condition object are created, denoted by T, e, and condition, respectively. Next, we update the condition corresponding to the order number. Finally, we update the table by using the entry object.

Algorithm 3 Submit an environment data hash

Input: $LE\_no, order\_no, hash\_data$
Output: $return\_value \in (0, 1)$

if (identity management passes) **then**
    create table object T;
    create entry object e;
    create condition object condition;
    e.set("transport_data",transport_data);
    $e.hash\_data \leftarrow hash\_data$;
    $condition.order\_no \leftarrow order\_no$;
    $return\_value \leftarrow T.update(LE\_no, e, condition)$;
end if
return $return\_value$;

4.4. Regulation Contract

The regulation contract's function is to guarantee the correctness during the whole DED circulation process. Further, it can be observed that the user can search the DED information including the MAU, the sales enterprise, the blasting enterprise, and the blasting instructions. Therefore, to preserve the data correctness, we designed the regulation contract, followed by Algorithm 4. The SAE scans the barcode and checks whether the barcode information and the data in the information system are consistent. Then, the sales enterprise uploads the data to the blasting enterprise. The blasting enterprise should also scan the barcode to verify the information on the DED before the electronic detonators are put into storage.

Tables 6 and 7, respectively contain the circulation process from the MAU to the SAE and from the SAE to the BAE.

Table 6. The table of distribution transactions (SAE to SAE).

Pro_No.	Batch	SAE_No.	BAE_No.	Time	State	Identify_Code
010001	521,894	020002	025001	2023-7-3 14:03	1	30,000,000
010002	134,241	020002	025002	2023-7-3 15:12	1	30,000,000
...	...	...	...	...	...	...

Table 7. The table of distribution transactions (SAE to BAE).

Pro_No.	DED_Batch	Shipper_No.	Consignee_No.	Time	State	Identify_Code
010001	521,894	02002	025001	2023-7-3 14:05	1	30,000,000
010002	134,241	02002	025002	2023-7-3 15:25	1	30,000,000
...	...	...	...	...	...	...

Algorithm 4 shows the DED query process for the regulation contract. The input parameter of this function is the label of the DED. The result of the function is the search data, which maintain the circulation information of the DED in the whole process (denoted by *circulation*). During the query process, we first query the SAE record in Table 6. Next, we search the results sent from the SAE to the BAE in Table 7, which is repeated until the returning shipper is the blasting enterprise, because the DEDs may be sent to the blasting enterprise through many SAEs. Finally, the circulation record in the whole procedure is returned as the query result.

Algorithm 4 Query circulating information (SAE to BAE, circulation_table)

Input: MAU number pro_no, order number $order\_no$, batch number DED_batch, $identi\_node$
Output: DED circulation data $circulation$

```
create new object SAE;
create new object BAE;
SAE ← get_SAE(pro_no, DED_batch, identi_code);
append(circulation,SAE[consignee_no]);
while BAE[consignee_no] = SAE do
    BAE ← get_BAE;
    append(circulation,BAE[consignee_no]);
end while
return circulation;
```

4.5. Blasting Contract

BAEs apply for the work code with information such as the initiator coding, UID, latitude, and longitude. After the supervisor approves the work code application, the initiator decrypts and downloads the working code and parses the UID code, the detonation password, and the detonator shell code. After the initiation is completed, the initiator uploads the information such as the initiation time and the initiation longitude and latitude to the NIEDCC through the supervision application. Table 8 shows the structure of the blasting contract.

Table 8. The table of blasting transactions.

BAE_No.	UID	Longitude	Latitude	Time	State
030002	010001	40.2583	116.2933	2023-7-4 13:06	1
030002	020001	30.2345	90.2357	2023-7-4 15:25	1
...	...	...	...	...	...

Algorithm 5 shows the submission of blasting information in the blasting contract.

Algorithm 5 Submit blasting information

Input: BAE_no, UID, latitude,longitude
Output: $return\_value \in (0, 1)$

```
if (identity management pass) then
    create table T;
    create entry object e;
    e.BAE_no ← BAE_no;
    e.UID ← UID;
    e.latitude ← latitude;
    e.longitude ← longitude;
    e.time ← int(now);
    return_value ← T.insert(BAE_no, e);
end if
return return_value;
```

5. System Simulation

5.1. Experimental Settings

We developed a prototype of the DED supervision system to analyze the performance of the proposed system, which incorporates the supervision model. To simulate the proposed system with the supervision model, a virtual machine on a personal computer with 16GB of memory and a 1 TB hard drive was adopted. The consortium blockchain called FISCO BCOS blockchain [27] was used as the blockchain platform. We chose the FISCO BCOS blockchain for building the prototype mainly due to its significant influence in China. Similarly, it is also simple to enhance the proof-of-concept prototype with FISCO BCOS as a practical and important system.

We set up eight MAU nodes, eight SAE nodes, eight LE nodes, and forty BAE nodes, with only one supervisory agent. Every node is involved in the consensus process of the blockchain. The configuration information of the blockchain is detailed in Table 9. The listen IP means the peer-to-peer listening IP address of the node, which uses the default address of 127.0.0.1. The listening port refers to the channel port, and we used the listening port corresponding to the default number 20,200. We assigned each node a range from 30,300 to 30,330. We set the default *Gas_limit* of each block as WEI 3×10^7.

Table 9. Configuration.

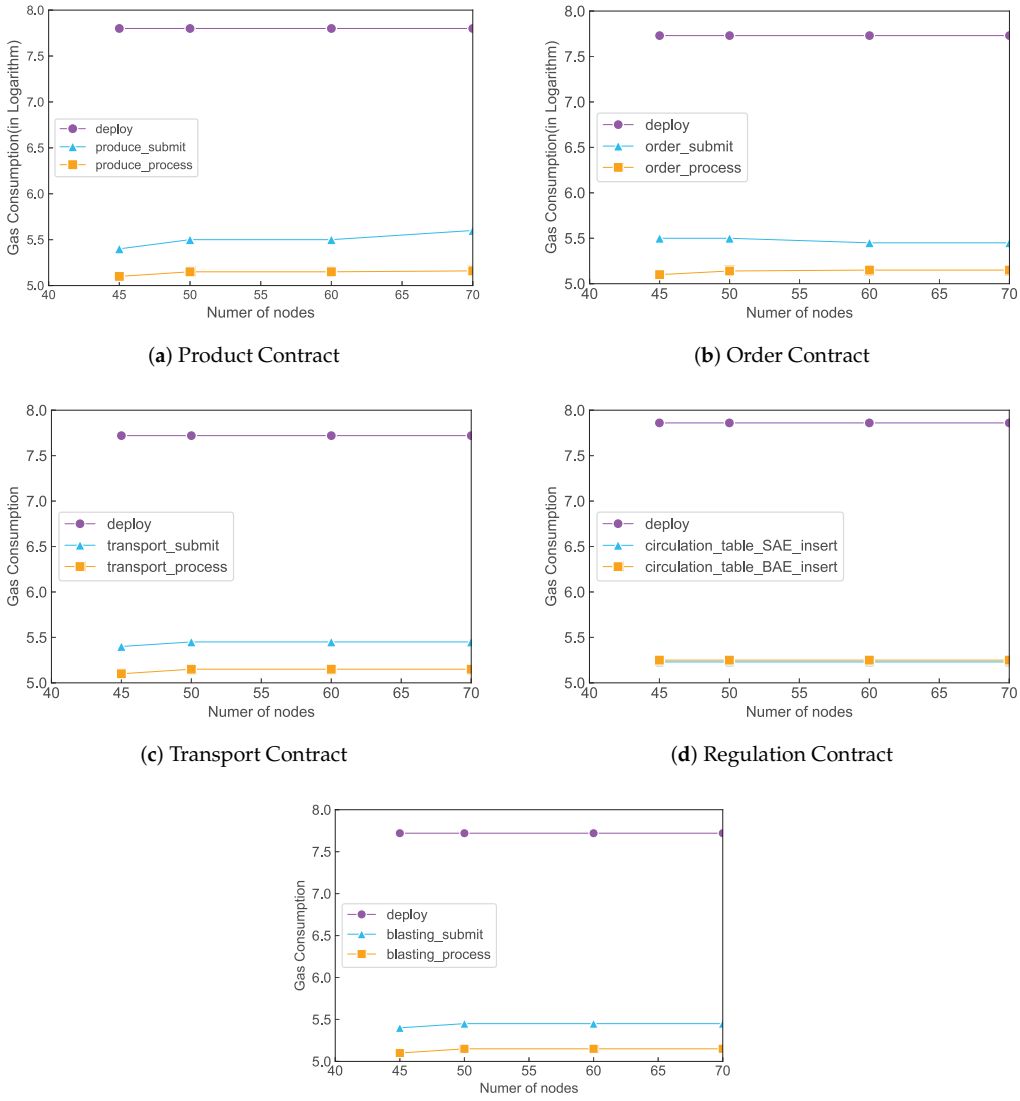
Object Size				Numbers of Nodes	Channel Listen Port	Node Port	Gas Limit (WEI)	Block Generate (s)
MAU	SAE	LE	BAE					
8	8	8	40	127.0.0.1	20,200	30,300-30,330	3×10^7	1

5.2. Performance Metrics

To evaluate the performance of the DED supervision system, we mainly used three metrics: (1) contract gas consumption, (2) communication, and (3) computation. The contract gas consumption consists of the gas for calling functions in smart contracts and the gas for deploying contracts. Communication consists of the input data size and output data size of smart contracts. The computation measures the time to submit the transactions to the blockchain.

5.3. Results

- Gap consumption: We examined the gas consumption for the smart contracts including both contract deployment, as well as contract calling. Every contract includes two functions. For example, the product contract corresponds to the function of pro_-submit, and pro_process.pro_submit means that the MAUs submit production data to the supervision organization. pro_process means that the supervision organization processes the productapplication. We set the number of blockchain nodes to 40, 45, 50, 55, 60, 65 and 70, respectively. The results of varying the total number of blockchain nodes are shown in Figure 3. We introduced a logarithmic overhead to the gas consumption. Clearly, the gas consumption is small, and the gas consumption does not increase with the expansion of nodes. This is because the gasLimit was introduced to prevent a smart contract from consuming too many computational resources, and hence, we can take the gas consumption as a metric of system performance.
- Communication:We measured the communication cost of invoking smart contracts corresponding to different numbers of nodes. Table 10 shows the communication cost in detail. It includes five aspects, which record the communication cost of every functional contract corresponding to the functions. It costs no more than 400 bytes when invoking smart contract functions. Note that the network bandwidth has been commonly measured as faster than 20 Mb/s (i.e., 2.5×10^6 bytes per second) in the network. Therefore, it is reasonably acceptable for practical use in terms of communication cost.



(**a**) Product Contract (**b**) Order Contract

(**c**) Transport Contract (**d**) Regulation Contract

(**e**) Blasting Contract

Figure 3. Contract gas consumption.

Table 10. Communication.

Contract	Function	Communication (byte)
Product Contract	pro_submit pro_process	365 236
Order Contract	order_submit order_process	338 237
Transport Contract	transport_submit transport_process	357 224
Regulation Contract	circulation_table_BAE_insert circulation_table_SAE_insert	391 385
Blasting contract	blasting_submit blasting_process	378 249

- Computation: To examine the computational cost to pack transactions, we varied the transaction pool from 1000 to 20,000. Table 11 shows the result of varying the transaction pools. It costs less than 1 s with the setting of the 20,000 transactions. The

computational cost increases linearly with increasing transactions. With the default setting of one second of block generation time, the highest number of processed transactions is about 30,000, which is not the upper bound of the supervision system. This is because the transaction packing time is dominated by the machine's performance and the algorithm's computation approach.

Table 11. Computation for various numbers of transaction.

Threshold	Product Contract	Order Contract	Transport Contract	Regulation Contract	Blasting Contract
1000	145	156	167	201	198
2000	246	211	254	287	205
6000	376	317	314	365	345
10,000	476	423	418	426	435
20,000	854	876	852	837	820

6. Conclusions

Ensuring DED safety is critical in industrial fields. We first studied the problem of quality traceability and safety in the DED supervision system. We presented a DED supervision system to make DED circulation traceable and verifiable for the DED supply chain. We also modeled the DED circulation process using smart contracts and a three codes in one mechanism. Based on that, we also introduced a DED supervision framework. In this system, DED quality and safety can be protected from production to blasting. Our proposed framework focusing on the design of smart contracts is practically implementable using the FISCO BIOS platform. However, the data size on the blockchain could become too large because it is widely used in the world. Blockchain integrated with the cloud could be used to reduce the storage cost and improve query performance. Specially, the off-chain storage of DED supervision information is outsourced to the cloud, while the small meta-data on-chain are stored on the blockchain.

The proposed blockchain solution provides new insights for researchers to ensure DED safety. There are several interesting research problems that deserve further investigation, e.g., how to reduce the blockchain storage cost and communication cost and how to leverage machine learning technology to analyze the production and blasting process for the prediction of DED quality and safety warning for production.

Author Contributions: Conceptualization, methodology, software, validation, writing—original draft, review and editing, N.L.; resources, supervision, project administration, funding acquisition, W.-T.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Chinese Ministry of Science and Technology (Grant No. 2018YFB1402700), the National Key Laboratory of Software Environment at Beihang University, the National 973 Program (Grant No. 2013CB329601), and the National Natural Science Foundation of China (Grant No. 61690202).

Data Availability Statement: Data are contained within the article.The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Roy, J.A.; Koushanfar, F.; Markov, I.L. EPIC: Ending piracy of integrated circuits. In Proceedings of the Conference on Design, Automation and Test in Europe, Munich, Germany, 10–14 March 2008; pp. 1069–1074.
2. Xu, X.; Rahman, F.; Shakya, B.; Vassilev, A.; Forte, D.; Tehranipoor, M. Electronics supply chain integrity enabled by blockchain. *ACM Trans. Des. Autom. Electron. Syst. (TODAES)* **2019**, *24*, 1–25. [CrossRef] [PubMed]
3. Jadon, S.; Rao, A.; Jagadish, N.; Nadakatti, S.; Thanushree, R.; Honnavalli, P.B. Blockchain in the electronics industry for supply chain management: A survey. *IEEE Access* **2024**, *12*, 7089–7120. [CrossRef]

4. Cao, Y.; Jia, F.; Manogaran, G. Efficient traceability systems of steel products using blockchain-based industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2019**, *16*, 6004–6012. [CrossRef] [CrossRef]
5. Agrawal, T.K.; Kumar, V.; Pal, R.; Wang, L.; Chen, Y. Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Comput. Ind. Eng.* **2021**, *154*, 107130. [CrossRef]
6. Omar, I.A.; Debe, M.; Jayaraman, R.; Salah, K.; Omar, M.; Arshad, J. Blockchain-based supply chain traceability for COVID-19 personal protective equipment. *Comput. Ind. Eng.* **2022**, *167*, 107995. [CrossRef] [CrossRef] [PubMed]
7. Zoughalian, K.; Marchang, J.; Ghita, B. A blockchain secured pharmaceutical distribution system to fight counterfeiting. *Int. J. Environ. Res. Public Health* **2022**, *19*, 4091. [CrossRef] [PubMed]
8. Mishra, P.; Bolic, M.; Yagoub, M.C.; Stewart, R.F. RFID technology for tracking and tracing explosives and detonators in mining services applications. *J. Appl. Geophys.* **2012**, *76*, 33–43.
9. Malik, S.; Kanhere, S.S.; Jurdak, R. Productchain: Scalable blockchain framework to support provenance in supply chains. In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 1–3 November 2018; pp. 1–10.
10. Abeyratne, S.A.; Monfared, R.P. Blockchain ready manufacturing supply chain using distributed ldedger. *Int. J. Res. Eng. Technol.* **2016**, *5*, 1–10.
11. Liu, Y.; Zhou, Z.; Yang, Y.; Ma, Y. Verifying the smart contracts of the port supply chain system based on probabilistic model checking. *Systems* **2022**, *10*, 19. [CrossRef] [CrossRef]
12. Zhang, X.; Sun, Y.; Sun, Y. Research on cold chain logistics traceability system of fresh agricultural products based on blockchain. *Comput. Intell. Neurosci.* **2022**, *2022*, 1957957. [CrossRef] [CrossRef]
13. Rajput, S.; Jadhav, A.; Gadge, J.; Tilani, D.; Dalgade, V. Agricultural Food supply chain Traceability using Blockchain. In Proceedings of the 2023 4th International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 11-12 February 2023; pp. 1–6.
14. Li, J.; Zhu, S.; Zhang, W.; Yu, L. Blockchain-driven supply chain finance solution for small and medium enterprises. *Front. Eng. Manag.* **2020**, *7*, 500–511. [CrossRef]
15. Haque, B.; Hasan, R.; Zihad, O.M. SmartOil: Blockchain and smart contract-based oil supply chain management. *IET Blockchain* **2021**, *1*, 95–104. [CrossRef]
16. Maity, M.; Tolooie, A.; Sinha, A.K.; Tiwari, M.K. Stochastic batch dispersion model to optimize traceability and enhance transparency using Blockchain. *Comput. Ind. Eng.* **2021**, *154*, 107134. [CrossRef] [CrossRef]
17. Weber, I.; Xu, X.; Riveret, R.; Governatori, G.; Ponomarev, A.; Mendling, J. Untrusted Business Process Monitoring and Execution Using Blockchain. In *Business Process Management*; BPM 2016. Lecture Notes in Computer Science; Springer, Cham, Switzerland, 2016; Volume 9850. [CrossRef]
18. Veerasamy, V.; Hu, Z.; Qiu, H.; Murshid, S.; Gooi, H.B.; Nguyen, H.D. Blockchain-enabled peer-to-peer energy trading and resilient control of microgrids. *Appl. Energy* **2023**, *353*, 122107. [CrossRef]
19. Chen, L.; Lee, W.K.; Chang, C.C.; Choo, K.K.R.; Zhang, N. Blockchain based searchable encryption for electronic health record sharing. *Future Gener. Comput. Syst.* **2019**, *95*, 420–429. [CrossRef]
20. Zhuang, C.; Dai, Q.; Zhang, Y. BCPPT: A blockchain-based privacy-preserving and traceability identity management scheme for intellectual property. *Peer-to-Peer Netw. Appl.* **2022**, *15*, 724–738. [CrossRef] [CrossRef]
21. Ismail, S.; Reza, H.; Salameh, K.; Kashani Zadeh, H.; Vasefi, F. Toward an Intelligent Blockchain IoT-Enabled Fish Supply Chain: A Review and Conceptual Framework. *Sensors* **2023**, *23*, 5136. [CrossRef] [CrossRef]
22. Dos Santos, R.B.; Torrisi, N.M.; Pantoni, R.P. Third party certification of agri-food supply chain using smart contracts and blockchain tokens. *Sensors* **2021**, *21*, 5307. [CrossRef]
23. Wu, H.; Li, H.; Luo, X.; Jiang, S. Blockchain-Based On-Site Activity Management for Smart Construction Process Quality Traceability. *IEEE Internet Things J.* **2023**, *10*, 21554–21565. [CrossRef] [CrossRef]
24. Liu, C.; Li, Y.D.; Ji, S.W. Application of the internet of things technology in explosive dangerous goods transport. *Appl. Mech. Mater.* **2012**, *178*, 1725–1728. [CrossRef]
25. Qin, X.; Ying, W. Design of explosive production information and managing system based on Internet of Things. In Proceedings of the 2015 International Conference on Control, Automation and Robotics, Singapore, 20–22 May 2015; pp. 173–176.
26. Zhang, H.; Li, B.; Karimi, M.; Saydam, S.; Hassan, M. Recent advancements in IoT implementation for environmental, safety, and production monitoring in underground mines. *IEEE Internet Things J.* **2023**, *10*, 14507–14526. [CrossRef]
27. FISCO BCOS. The Building Block of Open Consortium Chain. 2021. Available online: http://fisco-bcos.org (accessed on 6 May 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.