applied sciences

MDPI

Article

# On the Design and Implementation of a Blockchain-Based Data Management System for ETO Manufacturing

**Zhengjun Jing [1,2,*], Niuping Hu [1], Yurong Song [2], Bo Song [2], Chunsheng Gu [1] and Lei Pan [3]**

[1] School of Computer Engineering, Jiangsu University of Technology, Changzhou 213001, China
[2] College of Automation & Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[3] Cyber Security Research and Innovation, School of Information Technology, Deakin University, Waurn Ponds, Geelong, VIC 3216, Australia
* Correspondence: zhengjun_jing@163.com or jzjing@jstu.edu.cn

**Abstract:** Engineer-to-order (ETO) is a currently popular production model that can meet customers' individual needs, for which the orders are primarily non-standard parts or small batches. This production model has caused many management challenges, including the difficulty of tracing the production process data of products and the inability to monitor order status in real-time. In this paper, by analyzing the steps of ETO manufacturing and the business process between departments in the manufacturing industry, a blockchain-based process data management system (BPDMS) is proposed. The immutable nature of the blockchain data ensures the data's validity and consistency in each production step. Furthermore, by embedding the sequential aggregate signature in the system, the sequence verification of discrete process steps can be completed in time. Finally, an electrical equipment assembly production platform is used to discuss the specific implementation on top of the Hyperledger Fabric, a permissioned blockchain. The experiment results show that the proposed system effectively manages the process data of ETO-type production, and the real-time querying of the production status of the orders.

**Keywords:** blockchain-enabled; ETO-type production; sequential aggregate signature; data management

check for updates

**Citation:** Jing, Z.; Hu, N.; Song, Y.; Song, B.; Gu, C.; Pan, L. On the Design and Implementation of a Blockchain-Based Data Management System for ETO Manufacturing. *Appl. Sci.* **2022**, *12*, 9184. https://doi.org/10.3390/app12189184

Academic Editor: Eui-Nam Huh

Received: 16 August 2022
Accepted: 9 September 2022
Published: 13 September 2022



## 1. Introduction

Engineer-to-order (ETO) production means that products are engineered and produced after orders have been received. This production method helps to meet the exact specifications of customers [1]. With the increasing personalized needs of customers, more and more enterprises have adopted the production model of ETO for their development, which accounts for an increasing proportion in the manufacturing industry. The ETO production mode is a highly discrete production type and is the most complex in the manufacturing environment. ETO manufacturing faces many challenges in production [2–5]. Customers' needs are personalized and diversified, making it impossible to reuse the manufacturing process of the produced products. Furthermore, the relevant information about the new product can only be determined after the design drawings are released, including material code, BOM, and process route. This delay also directly leads to the lack of effective control of the collaborative cost of production. In addition, enterprises in the ETO production model have many discrete workshops for processing semi-finished products. Therefore, to meet the customer's customized needs for products and the traceability of the production process, it is necessary to ensure the accuracy of product processing and the credibility of the production process information after the product is completed.

Through production process data management, not only can the production process of orders be tracked in real-time, but production problems can also be found in time and improved through data analysis. Therefore, the validity of data in manufacturing is crucial to improving production quality and efficiency. Due to the above reasons, each change in the process data or transformation event should be traceable in a record that cannot be deleted or changed. Building efficient multi-department collaboration to achieve credible and traceable production process data, and traceability of the production process, has always been a key research issue in the manufacturing field. The blockchain has the characteristic that data cannot be tampered with in a distributed environment, and is thus highly suitable for data management scenarios in manufacturing [6–11].

### 1.1. Research Objective

Compared with other production types of manufacturing enterprises, ETO manufacturing usually starts with sales business, followed by product design, supporting procurement, online production, delivery, and other business processes, and ends with after-sales service business. The specific process and the roles involved are shown in Figure 1. The sales department generates contract orders according to user requirements, while the technical department is responsible for the product design of the orders and generates the BOM list and production work orders. After that, the purchasing department purchases raw materials according to the BOM list to be prepared for production. The manufacturing center plans and produces work orders, while product quality inspections are completed. After the product is delivered to the user, the sales department is responsible for the after-sales service of the contract order.

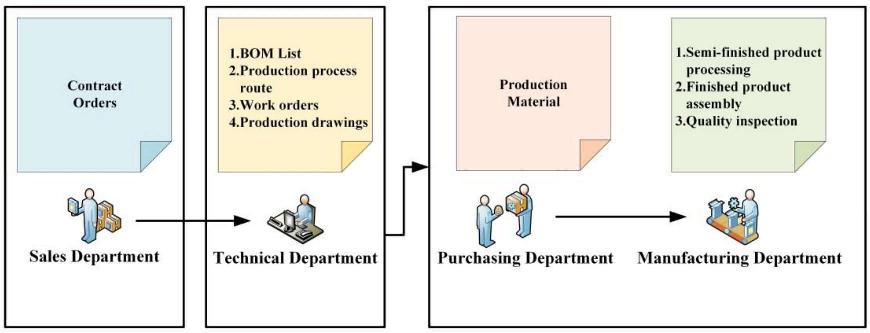



**Figure 1.** Production process of ETO manufacturing.

The production of a finished product in the manufacturing process includes two stages: semi-finished product processing and product assembly. In addition, each stage also has quality inspection. Importantly, the production process routes of different customized products are entirely different, while the process routes of semi-finished products are almost discrete.

Manufacturers using ETO production have realized that each product they produce has its own problems and challenges, which are mainly the following:

1. Tracking data in engineering production. Generally speaking, manufacturing companies that use made-to-order (MTO) production will standardize production. Once the customer order is received, it can be produced directly according to the existing design. However, ETO manufacturing requires the completion of a new design of a product to meet a customer's unique specifications. This results in production process data constantly changing between customers and manufacturers, even during production. Therefore, there is a need for a data management platform that can track all the changes the product undergoes throughout the process.

2. Security risks of data being tampered with or misused. Due to the numerous and discrete steps of ETO-type production, the business process between production departments is complicated. When business data are transferred from one department to the next, workers may violate company security regulations by tampering with or stealing data. Therefore, each data node in the production process needs to have the ability to trace the data to ensure its validity and consistency.

3. Lack of effective validation of the execution of the process design. Since ETO manufacturing is completely designed and customized to customer specifications, even

similar products may have different production routes. This requires a method to determine whether the production routing is correctly executed.

### 1.2. Major Contribution

After careful analysis of the characteristics of ETO manufacturing, new ideas are proposed in this paper to try to solve the above problems by using blockchain technology. The main contributions are as follows:

1. A production process traceability model based on blockchain technology is proposed. The detailed description shows that the scheme can be applied to ETO manufacturing. The immutability of the data on the blockchain ensures the data validity and consistency of each production node.
2. In order to ensure the correct execution of the production process route, a sequential aggregation signature is introduced, which can complete the sequential verification of discrete process steps in time.
3. The solution is implemented on a permissioned blockchain platform, including data upload and query algorithms. The experimental results show that the proposed system can effectively manage the data of ETO manufacturing.

### 1.3. Outline

The organization of this paper is as follows. Section 2 introduces the related work on ETO manufacturing, blockchain technology, and aggregated signatures. Next, Section 3 presents a process data management architecture based on blockchain for ETO manufacturing, followed by Section 4, which presents the system implementation and performance. Section 5 concludes this paper, and notes the limitations of this study and directions for future research.

## 2. Background and Related Works

In the introduction to related work, the key features offered by blockchain technology, the concept of smart contracts, and the current applications of blockchain technology in engineering and manufacturing are first provided. The aggregated signature technique is also described as a cryptographic primitive that can be used to authenticate discrete manufacturing processes in the proposed scheme.

### 2.1. Blockchain in Engineering and Manufacturing

Blockchain is an electronic distributed ledger with the features of decentralization, data immutability, consensus mechanism, and many more [12–16]. Blockchain technology, as a new model of data sharing, provides a means for parties to build mutual trust without the need for a trusted third party. This mechanism records data changes in a block as a transaction and uploads them to the chain. Since all participants jointly maintain the ledger, any party's changes to the data can only be recognized through consensus; otherwise, the transaction will be rejected. Most importantly, when smart contracts are integrated into the blockchain, the application scenarios of blockchain technology become more and more extensive. Smart contracts are a computer protocol linking multiple parties to complete a dedicated contract. Smart contracts are supported by major blockchain development platforms, such as Ethereum and Hyperledger [17,18].

To date, many studies have shown that the application of blockchain in production scenarios has many advantages, and its distributed storage structure greatly ensures the security of data, which are extremely difficult to tamper with [19–25]. The storage structure ensures the data are immutable and facilitates the traceability of the data. Thus, it helps to achieve transparent tracking of the production process. Kasten [26] undertook a detailed review of the application of blockchain technology in engineering and manufacturing in terms of achieving three outcomes: protecting data validity [27–32], enhancing communication within an organization [33–38], and improving manufacturing production efficiency [39–43]. Kumar et al. [44] discussed in detail the use of an Ethereum-based distributed ledger technology to improve information trustworthiness and access control in cloud-based manufacturing. To solve the data sharing problem of the production supply chain in the Industrial Internet of Things (IIoT), Wen et al. [45] proposed a new blockchain-based supply chain structure, which integrates attribute encryption to make data access more fine-grained. At the same time, it further improves the reliability and traceability of IIoT data. Rathee G. et al. [46] proposed a hybrid blockchain mechanism to provide security for multinational IIoT data with offices in multiple countries. A blockchain-based resource-sharing collaboration framework was designed by Agrawal et al. [47], which can support ecosystems with established collaborations and hierarchies. While blockchain technology has provided many benefits for smart manufacturing, there are still many problems in applying it to ETO-type manufacturing, especially in ensuring the validity of production chain data when the production process route is uncertain.

### *2.2. Sequential Aggregate Signature*

An aggregate signature is a cryptographic primitive that can aggregate different signatures of multiple signers into a single signature [48]. Since the size of the aggregate signature remains the same as that of a single signature, it can effectively reduce the communication cost when an authenticated message must be forwarded from one partner to another. A sequential aggregate signature is a variant that supports data aggregation that depends on the order of the parties. It relies not only on the public data but also on the order of all previously aggregated data. The sequential aggregate signatures play a key role in situations such as verifying routing information or certificate chains, where the verification of the order of signature steps is important.

In the ETO-type production model, the sequential execution of discrete production process routes needs to be guaranteed. By integrating the sequential aggregate signature into the blockchain, verification and traceability of the execution steps of the production process route is ensured. Generally, a sequential aggregate signature scheme consists of three parts: key generation algorithm, signature aggregation algorithm, and aggregate verification algorithm. Specifically, when the signer receives an ordered set of public keys PK=(pk1,...pki) and messages M=(m1,...mi), and an aggregate signature corresponding to the sequence, the signer uses its own private key, *sk*, to derive a new aggregate signature on its message, m, using an aggregation algorithm, which takes m#M and pk#PK as input parameters. In our proposed scheme, the sequential aggregate signature designed by Fischilin M. in [49] is adopted; this is mainly constructed based on bilinear mapping, and its security has been proved theoretically [49,50].

## 3. Architecture of Blockchain-based Process Data Management for ETO Manufacturing

Under the production type of ETO, a product is designed to a large extent according to the requirements of a specific customer, so supporting customized design is an important function of the production process. Because most products are tailored to specific customers, they may only be produced once, and their components cannot be reused in other new products. Therefore, in this type of production, products are generally produced in smaller batches, but the design work and the final product are often very complex. In the production process, each job must be handled individually because they may have different operations and different costs, and require different personnel to complete.

### *3.1. Blockchain-Based Production Process Management for ETO Manufacturing*

Due to the diverse and discrete process steps in ETO-type production, the traditional method of tracing data stored in the centralized database of the enterprise will result in low timeliness of data verification and the risk of data tampering and loss. The blockchain uses distributed ledgers instead of a central database to store enterprise production data. This approach can record product information positively in real-time, enhance the validity and reliability of the data, and improve the traceability of the production process.

A blockchain-based product data management system (BPDMS) is constructed for ETO-type production, as shown in Figure 2. The BPDMS can be divided into three levels from top to bottom: business logic, data acquisition, and the blockchain network. The three layers are interrelated.

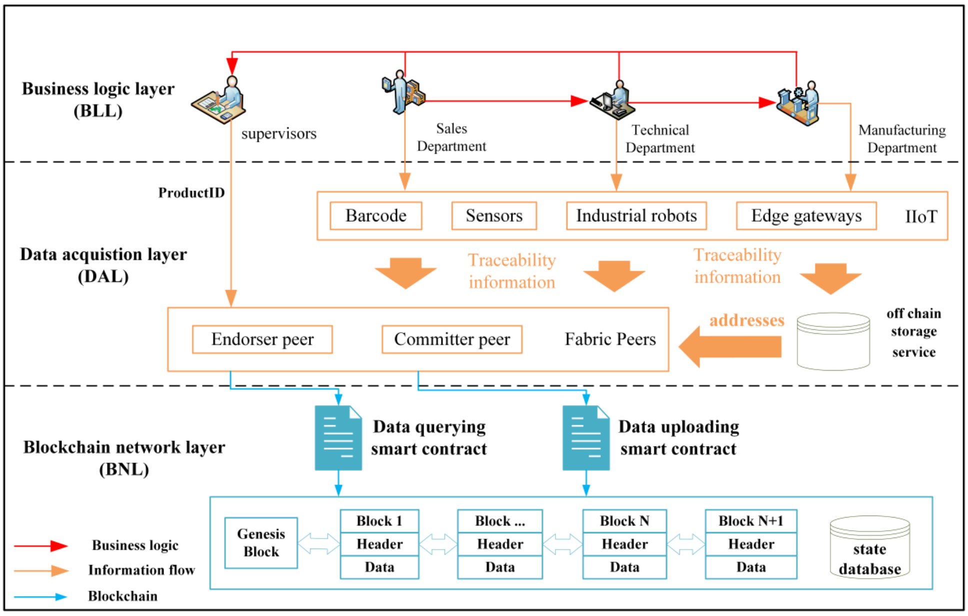



**Figure 2.** The architecture of BPDMS.

1. **Business logic layer (BLL)**. This layer represents the business process of ETO-type manufacturing production. In the BLL, the business starts with contract orders, decomposes into product designs, and forms production work orders and their production process routes. Next, according to the production process route, the semi-finished product processing and finished product assembly are completed in the manufacturing center. Finally, the quality inspection of the product needs to be completed.

Compared to the business process described in Figure 1 in Section 3.1, a supervisory role is added to the process, primarily responsible for the production process supervision and traceability query through the deployed smart contracts. In addition, the purchasing step is also ignored in this process because the framework focuses on the production process data. In the actual enterprise management, this layer mainly includes some related application software, such as ERP, 3D design software, and the MES system.

2. **Data acquisition layer (DAL)**. The DAL is the middle layer, and uses a variety of IoT devices to collect data on each business viewpoint of the business logic layer. For example, specific products can be identified by scanning the QR code corresponding to the work order generated in the ERP system with a barcode gun at the production station. Similarly, the operation data of various equipment with different functions are also collected through IoT terminals, such as sensors, industrial robots, and edge gateways.

In the DAL, the data collected on each business node can be stored and queried on the chain by calling the deployed smart contract. It should be noted that data such as production drawings and operation videos are stored off-chain, and the stored address index is then uploaded to the chain. This combination of on-chain and off-chain storage helps save blockchain storage resources and improve query efficiency.

3. **Blockchain network layer (BNL)**. The BNL adopts Hyperledger Fabric as the blockchain platform, which is a permissioned blockchain. In this type of blockchain, all participants who can trace the data must first register and obtain a legal identity; otherwise, they cannot access the blockchain. Since managers can control the size of the network by controlling the number of nodes, permissioned chains usually have a high transaction throughput.

In BPDMS, the channel technology of the Fabric blockchain is used to create a channel for each department in the production process, and each channel has an independent ledger, which ensures that each department's data are isolated from each other. In each channel, the production data collected by the DAL are packaged into transaction events and then uploaded to the blockchain network by calling the smart contract that stores the data to generate new blocks. The information of these transaction events is stored in the leaf node of the Merkle tree of the block body for block accounting, and then the returned transaction hash and block height are stored in the current state index database, CouchDB. Authorized users of each department can call smart contracts that query data to trace or track production data. Since the supervisory role has supervisory authority over the product production process, it can simultaneously call the smart contracts of one or more departments in the production chain to supervise the entire production process status regarding the specific product in real-time.

### 3.2. Metadata of Each Production Entity

As described in the first section, the production process of an ETO-type manufacturing enterprise mainly involves multiple entities, such as supervision, marketing, product design, production, and quality inspection. The production department will have two production lines: discrete semi-finished product processing lines and flow-type finished product assembly lines. Each entity in the BPDMS generates its process data and uploads it to the ledger of the corresponding channel.

Production is an orderly process from sales orders to qualified finished products. Therefore, each entity maintains an ordered relationship between the preceding and following entities by the relevant key fields in the metadata, as shown in Figure 3.

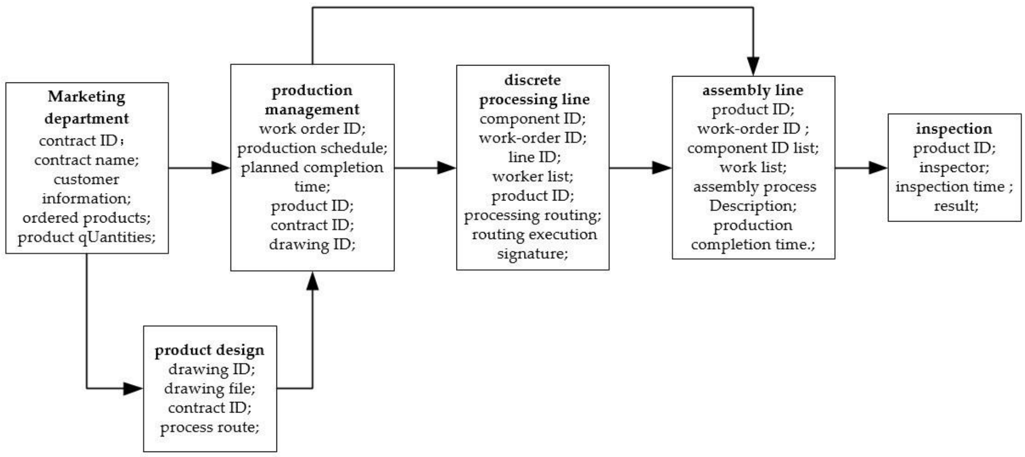



**Figure 3.** Metadata of each entity and its data flow.

- **Marketing department entity (sales department)** is mainly responsible for customer needs and obtaining contract orders with customers, which mainly include contract ID, contract name, customer information, and ordered products and quantities.
- **The product design entity** designs the product according to the requirements of the product ordered in the contract, and generates the production drawing and process route of the product, including the product ID, drawing ID, drawing file, product process route, and contract ID. Here, the contract ID is the data field associated with the preceding entity.
- **The production management entity** is an important unit of the production process, and converts product orders into production work orders. The main data fields here include production work order ID, production schedule, planned completion time, product ID, contract ID, and drawing ID. It should be noted that due to the different types of production lines, the types of work orders are also different, and can be divided into work orders for processing lines and work orders for assembly lines.

- **A discrete processing line** is a semi-finished product process, which mainly produces product components. Since the production processes of different components are different, it is necessary to record the production data of the components and determine in a timely manner whether the production is carried out according to the process route. The on-chain data of this production line entity include component ID, work-order ID, line ID, worker list, product ID, processing routing, and routing execution signature.
- **An assembly line** is a streamlined operation that produces a final product by assembling related components. The on-chain data of this entity mainly comprise work-order ID, component ID list, work list, assembly process description, product ID, and production completion time. The supervisor can track and trace the production process of the product by calling the query smart contract, where the product ID is the key field.
- **The quality inspection entity** is an important step in production, which mainly checks whether the product meets the specifications and requirements according to the product characteristics. The data on the chain include product ID, quality inspector, quality inspection time, and result.

### *3.3. Validation of Process Route*

A process route is a combination of multiple process definitions, and a process is an action or a series of actions performed by production operators or machines to complete a specified task. It is the most basic processing operation for processing materials and assembling products. Ensuring the validity and reliability of production data is the key concern in the data management of manufacturing enterprises. In discrete processing production, to ensure that the production is executed according to the process route, the sequential aggregate signature mechanism is introduced.

To facilitate interpretation and improve readability, the relevant notations in the SAS mechanism are listed, as shown in Table 1. The bilinear mapping on the elliptic curve $e(G1, G2) \rightarrow G3$, and the secure hash function $H(*) \rightarrow G1$ and $h : \{0,1\}^* \rightarrow \{0,1\}^n$, are used in the signature scheme. The SAS scheme designed in [49] is adopted, which extends the BSL03 [48] scheme architecture, including three parts:

- key generation $Kg(1^n)$: the algorithm can generate the signer's key $(pk, sk)$;
- signature $(sk, m)$: this algorithm takes messages m and a secret key $sk$ as input; it computes a signature $s = H(m)^{sk}$;
- signature verification $Vf(m, pk, s)$: if $e(s, g_2) == e(H(m), pk)$, then it outputs 1.

**Table 1.** Notation list.

| Notations | Description |
| --- | --- |
| $U$i | The ith node on the production process route. |
| $(pk_i, sk_i)$ | Node i's public and private key pair for signing. |
| $m_i$ | Each process name on the production route. |
| $e$ | The bilinear mapping on the elliptic curve. |
| $G_1,\ G_2,\ G_3$ | Three multiplicative cyclic groups. |
| $g_1,\ g_2$ | The generators of $G_1$, $G_2$, respectively. |
| $H(\,), h(\,)$ | The secure hash function. |
| *Vef* ( ) | The signature verification in [48]. |
| SAS$(\sigma, pk, c, s)$ | The sequential aggregate signature in [49]: $\sigma$ is an aggregate signature; $c$ is a hash value, and $s$ is the previous process node's non-aggregated signature. |

The general flow chart of the execution of the process route on the production line for a particular product is shown in Figure 4.

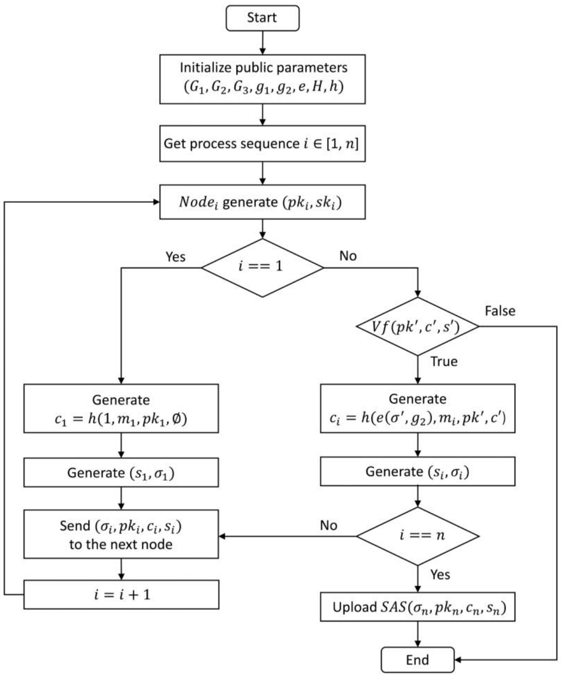



**Figure 4.** The flow chart of the execution of the process route.

For the convenience of description, the execution route of process II marked in red in Figure 5 can be taken as an example. If the process route of the product is set to pass through the production units A, B, and E in sequence, then the signature of the product needs to be generated by orderly aggregation of the signatures of the three production units in the order of A, B, and E. Finally, through the verification of the aggregated signature, it can be checked whether the production process is actually completed through each corresponding production unit in the order of route II.

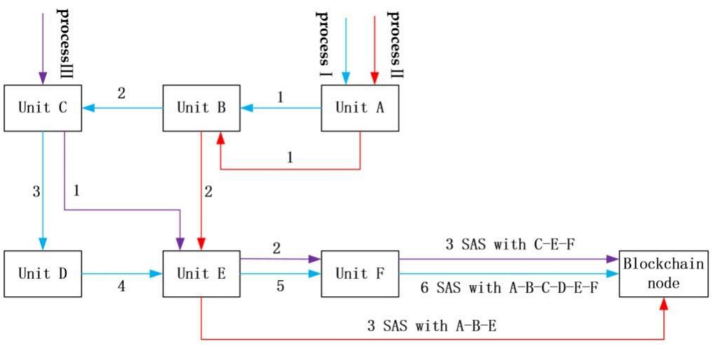



**Figure 5.** Sequential aggregate signatures in execution of production routing.

Using $Kg$ to generate the signature key pair $(pk_i, sk_i)$ of three production units $U$ (NodeA, NodeB, nodeE), the process name $M\{m_1, m_2, m_3\}$ of the process route II is set; then, the validation algorithm for sequential execution of processes is shown in Algorithm 1. In each verification step, the production unit Ui receives the aggregate-so-far $SAS\prime(\sigma', \mathrm{pk}', \mathrm{c}', \mathrm{s}')$, including an aggregate signature σ′, the signature public key pk′ of the previous process unit, a hash chain value c′, and the previous process unit's non-aggregated signature s′. The *Ui* first verifies that s′ is a valid signature for c′ under pk′. If it passes the verification, then *Ui* can extend the hash chain for the new process $m_i$. Then, a signature $s_i$ is generated for the new hash value $c_i$, and a new aggregated signature $\sigma_i$ is derived by aggregating the signature $s_i$. Finally, the $SAS(\sigma_i, \mathrm{pk}_i, \mathrm{c}_i, \mathrm{s}_i)$ is forwarded to the next process unit. When the last process unit passes the aggregate verification, the corresponding last aggregated signature $SAS(\sigma, \mathrm{pk}, \mathrm{c}, \mathrm{s})$ is recorded to the blockchain.

**Algorithm 1:** Validation algorithm for sequential execution of processes

**Input**: $(pk_i, sk_i)$, $SAS'(\sigma', \mathrm{pk}', \mathrm{c}', \mathrm{s}')$
**Output**: $SAS(\sigma, \mathrm{pk}, \mathrm{c}, \mathrm{s})$
1: Init $SAS(\mathrm{M}, \mathrm{PK}, \mathrm{U}, \mathrm{SAS}')$
2: **if** $Vf(pk', C', s\prime)$
3: $c_i = h(e(\sigma', g_2), m_i, pk', c')$
4: $s_i = Sig(sk_{i,} c_i)$
5: $\sigma_i = \sigma' \cdot s_i$
6: **return** $(\sigma_i, \mathrm{pk}_i, \mathrm{c}_i, \mathrm{s}_i)$
7: **else**
8: **return** (“False”) // the previous process sequence is incorrect.
9: **end if**

### *3.4. Smart Contract Logic*

Smart contracts can automatically execute contract logic when the trigger conditions are met. It disseminates, verifies, or executes contract agreements in an information-based manner, which enables the blockchain to respond to external governance in a timely manner [12]. The blockchain network of our solution is a consortium chain multi-channel network based on Fabric, which creates an interface for the exchange of ledger data for different production departments. Therefore, the nodes of each department can call the interface through the smart contract to realize the data interaction between the chains. In this proposal, the designed query smart contract is mainly used to track or trace the production process data, and the upload data smart contract is mainly used for each department to upload its own metadata.

Algorithm 2 describes the data uploading operation, and Algorithm 3 describes the data querying operation, in which steps (3)–(5) trace the product by entering the unique identification ID of the product.

**Algorithm 2:** Data uploading algorithm

**Input:** Identity information **auth**, on-chain information **chainData**
**Output:** The **TxID** of the completed transaction
1: **if** (auth==true) //authentication check
2: SDK(func==Set)
3: **if** (TypeLegal (chainData) == ok)
4: upload to the chain and synchronized to the corresponding ledger
5: **return** (TxID) //return the transaction number
6: **end if**
7: **end if**

**Algorithm 3:** Data querying algorithm

**Input**: identity information **auth**, production ID (**PID**)
**Output**: All production process related data for PID
1: **if** (auth==true)
2: SDK (func==trace)
3: **if** (PID exists in the component ledger)
4: Obtain the product work order number through the obtained PID, which can further trace the product production process information.
5: **return** (all kinds of production information related to PID)
6: **else**
7: **return** (Trace PID data error.) //trace error
8: **end if**
9: **return** (authError) //authentication error
10: **end if**

## 4. System Implementation and Performance

The BPDMS for ETO manufacturing is implemented with the Hyperledger Fabric2.3 framework, and the blockchain consensus mechanism adopts the Raft consensus, ensuring that the built network has very good crash fault tolerance. The smart contracts are written in the Go programming language. Furthermore, the hardware environment comprises one server, on which seven virtual machines are installed and the Ubuntu18.04 operating system is run.

It should be noted that, although the proposed solution can be applied to the general production line in the ETO-type manufacturing industry, the realization content of this section is a simplified production line. In reality, the actual production line is much more complicated. In the blockchain network configuration, the block generation policy is set to generate a block every 2 s, or every 50 transactions will be packaged to generate a block.

### *4.1. Implementation of Specific Functions*

In this section, the data of the semi-finished product processing department are uploaded to the blockchain as a test case. According to the execution process of the processing route in discrete workshops, the system packages the operation data of each production unit into transactions, and then uploads the transactions to the blockchain network to generate a new block. The generated transaction information and block information are shown in Figures 6 and 7, respectively.

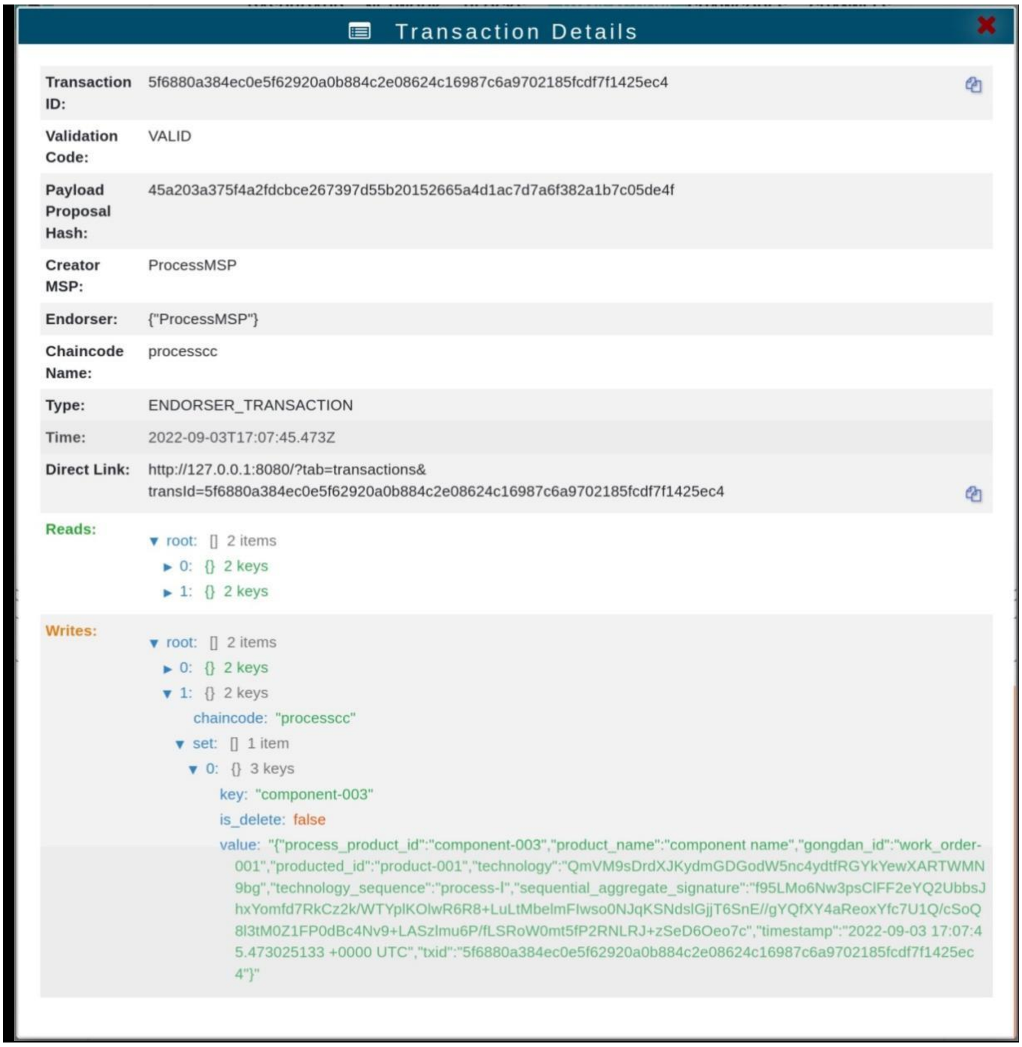
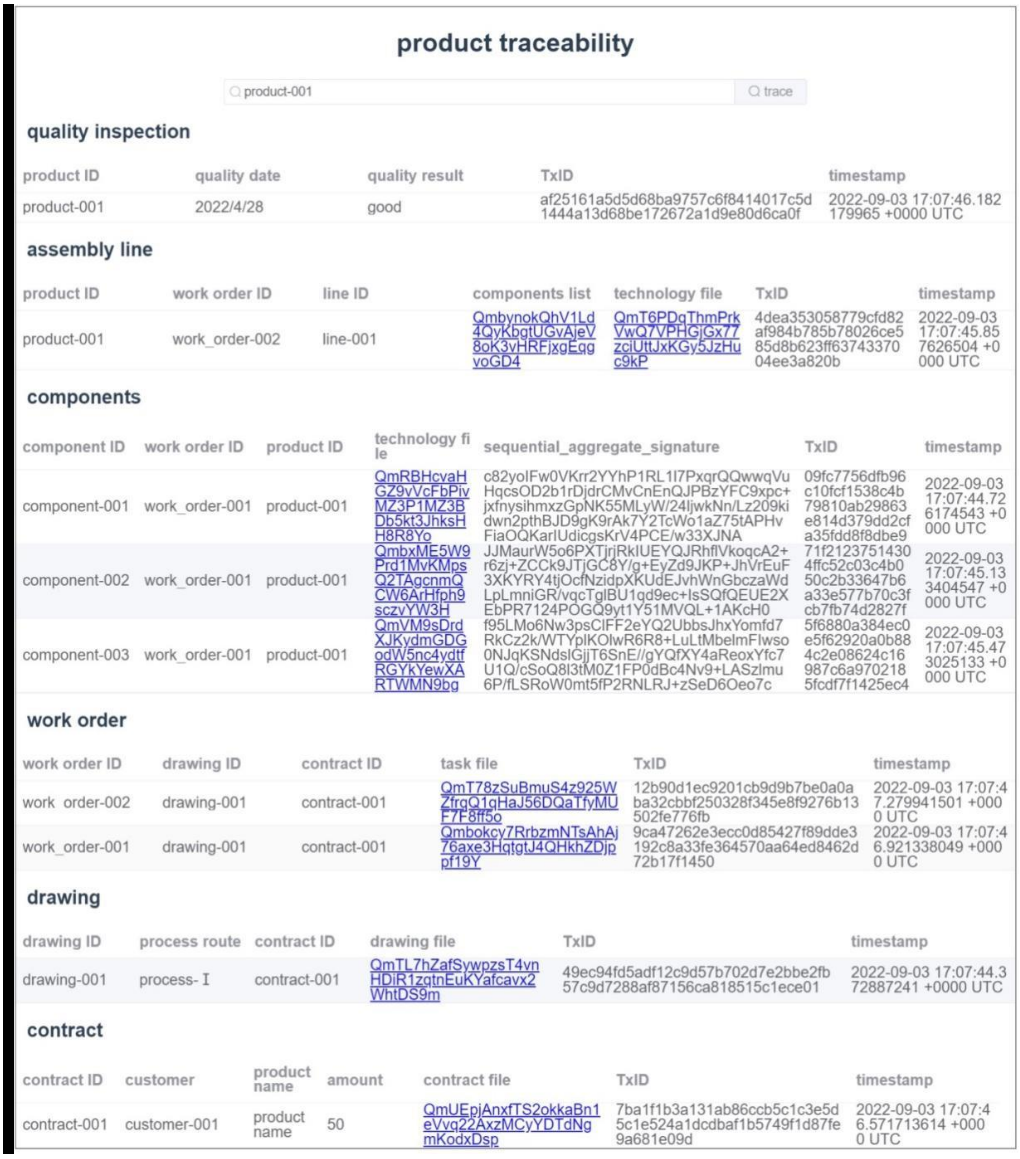



**Figure 6.** Transaction data generated by production units.

Block Details

| | |
|---|---|
| Channel name: | processchannel |
| Block Number | 8 |
| Created at | 2022-09-03T17:07:44.726Z |
| Number of Transactions | 3 |
| Block Hash | 0f7bbfd86bf0a09ae37b5563bf99175fa613047148d2dc611a6f1ab00168c5cd |
| Data Hash | 1129b5dc138a5a9d3552739639a4146cf10901bcb8a86262ac1b145397b512e6 |
| Prehash | 75df7cbc9668e25c025e4d88ccfe11ea962192ae605f5da332ea2afda5daf053 |

**Figure 7.** Block information generated by channels in discrete workshops.



product traceability

product-001 trace

quality inspection

| product ID | quality date | quality result | TxID | timestamp |
|---|---|---|---|---|
| product-001 | 2022/4/28 | good | af25161a5d5d68ba9757c6f8414017c5d1444a13d68be172672a1d9e80d6ca0f | 2022-09-03 17:07:46.182179965 +0000 UTC |

assembly line

| product ID | work order ID | line ID | components list | technology file | TxID | timestamp |
|---|---|---|---|---|---|---|
| product-001 | work_order-002 | line-001 | QmbynokQhV1Ld4QyKbgtUGvAjeV8oK3vHRFjxgEqgvoGD4 | QmT6PDqThmPrkVwQ7VPHGjGx77zciUttJxKGy5JzHuc9kP | 4dea353058779cfd82af984b785b78026ce585d8b623ff6374337004ee3a820b | 2022-09-03 17:07:45.857626504 +0000 UTC |

components

| component ID | work order ID | product ID | technology file | sequential_aggregate_signature | TxID | timestamp |
|---|---|---|---|---|---|---|
| component-001 | work_order-001 | product-001 | QmRBHcvaHGZ9vVcFbPivMZ3P1MZ3BDb5kt3JhksHH8R8Yo | c82yolFw0VKrr2YYhP1RL1l7PxqrQQwwqVuHqcsOD2b1rDjdrCMvCnEnQJPBzYFC9xpc+jxfnysihmxzGpNK55MLyW/24ljwkNn/Lz209kidwn2pthBJD9gK9rAk7Y2TcWo1aZ75tAPHvFiaOQKarlUdicgsKrV4PCE/w33XJNA | 09fc7756dfb96c10fcf1538c4b79810ab29863e814d379dd2cfa35fdd8f8dbe9 | 2022-09-03 17:07:44.726174543 +0000 UTC |
| component-002 | work_order-001 | product-001 | QmbxME5W9Prd1MvKMpsQ2TAgcnmQCW6ArHfph9sczvYW3H | JJMaurW5o6PXTjrjRkIUEYQJRhflVkoqcA2+r6zj+ZCCk9JTjGC8Y/g+EyZd9JKP+JhVrEuF3XKYRY4tjOcfNzidpXKUdEJvhWnGbczaWdLpLmniGR/vqcTglBU1qd9ec+IsSQfQEUE2XEbPR7124POGQ9yt1Y51MVQL+1AKcH0 | 71f21237514304ffc52c03c4b050c2b33647b6a33e577b70c3fcb7fb74d2827f | 2022-09-03 17:07:45.133404547 +0000 UTC |
| component-003 | work_order-001 | product-001 | QmVM9sDrdXJKydmGDGodW5nc4ydtfRGYkYewXARTWMN9bg | f95LMo6Nw3psClFF2eYQ2UbbsJhxYomfd7RkCz2k/WTYplKOlwR6R8+LuLtMbelmFlwso0NJqKSNdslGjjT6SnE//gYQfXY4aReoxYfc7U1Q/cSoQ8l3tM0Z1FP0dBc4Nv9+LASzlmu6P/fLSRoW0mt5fP2RNLRJ+zSeD6Oeo7c | 5f6880a384ec0e5f62920a0b884c2e08624c16987c6a9702185fcdf7f1425ec4 | 2022-09-03 17:07:45.473025133 +0000 UTC |

work order

| work order ID | drawing ID | contract ID | task file | TxID | timestamp |
|---|---|---|---|---|---|
| work_order-002 | drawing-001 | contract-001 | QmT78zSuBmuS4z925WZfrqQ1qHaJ56DQaTfyMUF7F8ff5o | 12b90d1ec9201cb9d9b7be0a0aba32cbbf250328f345e8f9276b13502fe776fb | 2022-09-03 17:07:47.279941501 +0000 UTC |
| work_order-001 | drawing-001 | contract-001 | Qmbokcy7RrbzmNTsAhAj76axe3HqtgtJ4QHkhZDjppf19Y | 9ca47262e3ecc0d85427f89dde3192c8a33fe364570aa64ed8462d72b17f1450 | 2022-09-03 17:07:46.921338049 +0000 UTC |

drawing

| drawing ID | process route | contract ID | drawing file | TxID | timestamp |
|---|---|---|---|---|---|
| drawing-001 | process- I | contract-001 | QmTL7hZafSywpzsT4vnHDiR1zqtnEuKYafcavx2WhtDS9m | 49ec94fd5adf12c9d57b702d7e2bbe2fb57c9d7288af87156ca818515c1ece01 | 2022-09-03 17:07:44.372887241 +0000 UTC |

contract

| contract ID | customer | product name | amount | contract file | TxID | timestamp |
|---|---|---|---|---|---|---|
| contract-001 | customer-001 | product name | 50 | QmUEpjAnxfTS2okkaBn1eVvq22AxzMCyYDTdNgmKodxDsp | 7ba1f1b3a131ab86ccb5c1c3e5d5c1e524a1dcdbaf1b5749f1d87fe9a681e09d | 2022-09-03 17:07:46.571713614 +0000 UTC |

**Figure 8.** Data list of traceable products.

## *4.2. Performance Evaluation*

The experiment uses the tool Tape to test the constructed Fabric network framework. The design department channel in BPDMS is taken as an example to test the network performance, including testing block generation time and transaction throughput. By setting 10 clients to connect to the node concurrently, and testing 24 groups of data with different transaction volumes, the number of transactions ranges from 50 to 1200, and each group is incremented by 50 transactions. It can be found that as the number of transactions increases, the transaction is completed; the time to generate blocks also gradually increases, and the transaction throughput value remains at a high level, of around 250. The test results are shown in Figure 9, and show that the BPDMS can support high query and write throughput.

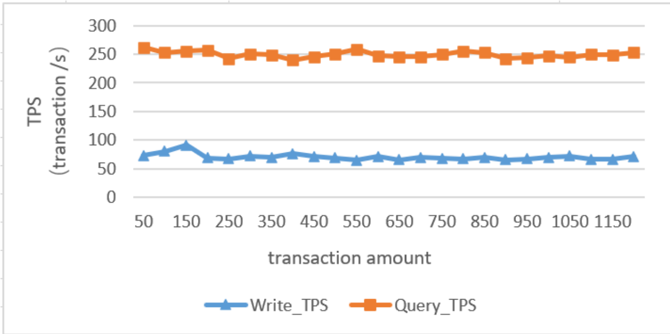



**Figure 9.** Network throughput testing of blockchain channel.

According to the structure of the BPDMS system, the data of a product include data of multiple departments, such as the sales department, design department, and production center. Moreover, the production center can also include semi-finished product discrete processing, product assembly, and product quality inspection. In the implementation on the Hyperledger Fabric platform, each role of the BPDMS system that generates partial data of the product corresponds to a specific channel. The performance of each channel in the BPDMS system is evaluated in an experimental way similar to the above design channel, including the accounting time and query delay of each channel. Accounting time (*Ta)* refers to the time from block generation to data synchronization of all nodes in the channel, and query delay (*Tq*) refers to the time from submitting query information to obtaining the returned result. The experimental results are shown in Table 2.

**Table 2.** The average value of *Ta* and *Tq* for each channel.

| | Sales Department | Product Design | Production Management | Discrete Processing | Assembly Line | Inspection |
|---|---|---|---|---|---|---|
| *Ta'* | 0.399s | 0.399s | 0.388s | 0.474s | 0.485s | 0.447s |
| *Tq'* | 0.322s | 0.365s | 0.356s | 0.398s | 0.381s | 0.374s |

The sequential aggregate signature is used both in discrete production of semi-finished products and in the assembly of products. The execution time of the sequential aggregate signature algorithm used to verify product routing is tested. When the process route is only one node, the signature time is only 0.799 s. Then, as the complexity of the component process increases, the number of processing units that need to be processed, and the signature time, also increase. As shown in Figure 10, when the number of signed nodes exceeds one, the signature time is increased by 66 ms for each additional node. The test results show that the sequential aggregation signature algorithm has good execution efficiency and fully meets the requirements of information collection in the production process.

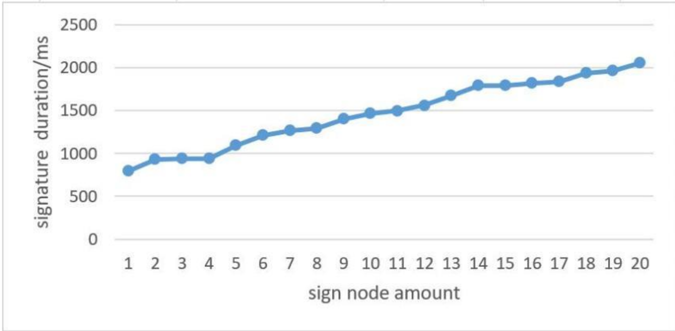



**Figure 10.** Efficiency of sequential aggregate signatures.

*4.3. Performance Comparison*

In order to more objectively evaluate the performance of the proposed scheme, a comparison is made with the data traceability scheme proposed by Yu et al. [36].

First, a comparison is made of the throughput rate of write data and query data of the channel in the blockchain network. The design department channel of BPDMS and a single chain in Yu's scheme is taken as an example. The experiment takes 25 transactions as a group, and adopts the method of gradually increasing the number of transactions. The results are shown in Figures 11 and 12, respectively. When the number of processing transactions is between 25 and 100, the write throughput increases linearly, and gradually flattens after reaching 100; when the number of processed transactions is between 25 and 200, the query throughput increases linearly, and gradually flattens after reaching 200. Compared with Yu's solution, the throughput performance of BPDMS is slightly poorer in terms of write performance, but superior in terms of query performance.

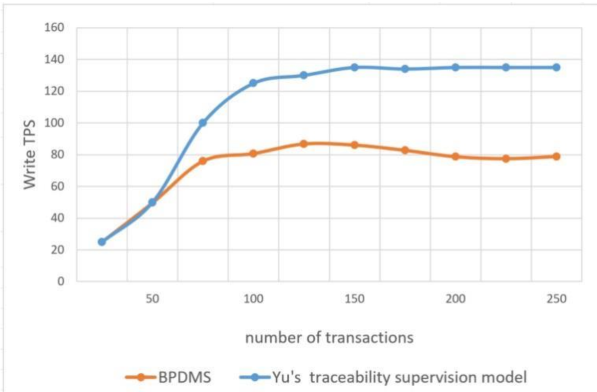



**Figure 11.** The throughput rate of write data.

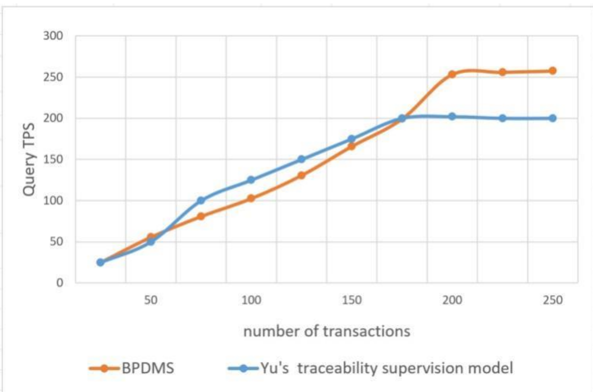



**Figure 12.** The throughput rate of query data.

In addition, the accounting time and query delay time of the blockchain network channels of the two systems are compared. The design department channel of BPDMS and a single chain in Yu's scheme are again taken as an example. The test of uploading 60 data blocks to the chain is used, and the results of the accounting time are shown in Figure 13. Similarly, 60 non-repeated queries are selected on the design department channel, and the results of the delay time are shown in Figure 14. Compared with Yu's solution, the accounting performance of BPDMS is better, and the query performance is similar.

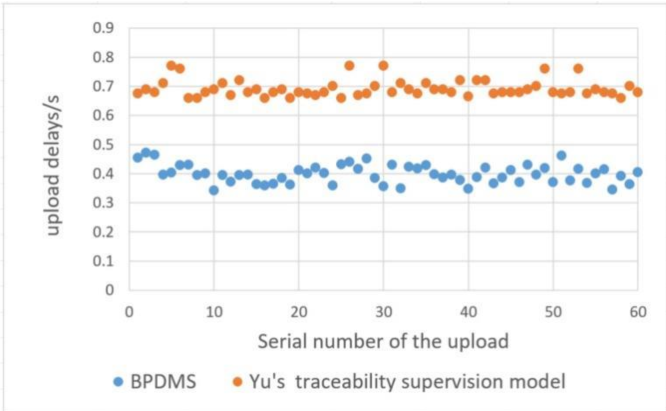



**Figure 13.** The comparison of accounting performance.

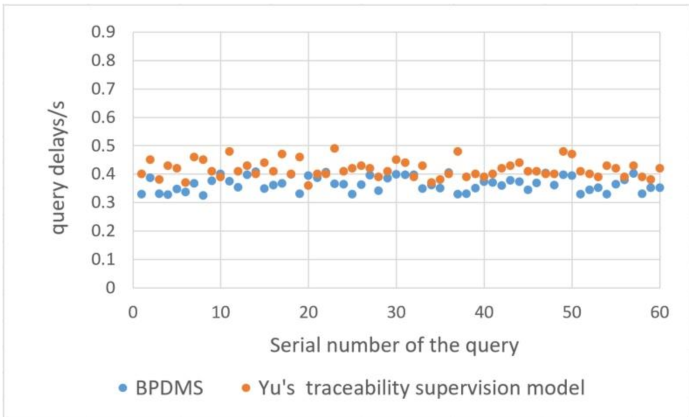



**Figure 14.** The comparison of query delay.

## 5. Conclusions

ETO-type production is the main production method used in the current manufacturing field. In this process, the production process data of the product are difficult to trace, and the production status data of the product are difficult to monitor in real-time. A production process traceability model based on blockchain technology is proposed, which can be applied to ETO-type production. By analyzing each data entity generated in the production process and the relationship between the data, the smart contracts for uploading data to the blockchain and data traceability are written. After integrating the sequential aggregate signature technology, the proposed scheme can be used to verify whether the production process is executed according to the designed process route. Based on the Hyperledger Fabric framework, the production process traceability system was designed and implemented. The experimental results show that the system can solve the problem of data traceability in the production process, and improve the security and traceability of data between each step of collaborative manufacturing of ETO-type production enterprises.

In future research, other parts of manufacturing, such as procurement of production materials, material management, product logistics, and after-sales service can be added, so that the data management of ETO manufacturing can be studied from a more systematic perspective.

**Author Contributions:** Conceptualization, Z.J., N.H. and Y.S.; methodology, Z.J., N.H. and Y.S.; software, N.H., B.S.; validation, Z.J.; formal analysis, Z.J. and N.H.; investigation, Z.J, Y.S.; resources, N.H.; data curation, N.H., C.G.; writing—original draft preparation, Z.J., N.H., Y.S.; writing—review and editing, Z.J., N.H., Y.S. and L.P. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Natural Science Foundation of Jiangsu Provence (SJ220036), the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (TJ220032).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Cannas, V.G.; Gosling, J. A decade of engineering-to-order (2010–2020): Progress and emerging themes. *Int. J. Prod. Econ.* **2021**, *241*, 108274. [CrossRef]
2. Swapnil, B.; Erlend, A.; Hans-Henrik, H. Tools and practices for tactical delivery date setting in engineer-to-order environments: A systematic literature review. *Int. J. Prod. Res.* **2022**, 1–33. [CrossRef]
3. McKendry, D.A.; Whitfield, R.I.; Duffy, A.H. Product Lifecycle Management implementation for high value Engineering to Order programmes: An informational perspective. *J. Ind. Inf. Integr.* **2022**, *26*, 100264. [CrossRef]
4. Cocca, P.; Schiuma, G.; Viscardi, M.; Floreani, F. Knowledge management system requirements to support Engineering-To-Order manufacturing of SMEs. *Knowl. Manag. Res. Pract.* **2021**, 1–14. [CrossRef]
5. Thajudeen, S.; Elgh, F.; Lennartsson, M. Supporting the Reuse of Design Assets in ETO-Based Components—A Case Study from an Industrialised Post and Beam Building System. *Buildings* **2022**, *12*, 70. [CrossRef]
6. Shahbazi, Z.; Byun, Y.C. Smart manufacturing real-time analysis based on blockchain and machine learning approaches. *Appl. Sci.* **2021**, *11*, 3535. [CrossRef]
7. Lim, M.K.; Li, Y.; Wang, C.; Mltd, E. A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Comput. Ind. Eng.* **2021**, *154*, 107133. [CrossRef]
8. Zhai, P.; He, J.; Zhu, N. Blockchain-Based Internet of Things Access Control Technology in Intelligent Manufacturing. *Appl. Sci.* **2022**, *12*, 3692. [CrossRef]
9. Manogaran, G.; Alazab, M.; Shakeel, P.M.; Hsu, C.H. Blockchain assisted secure data sharing model for Internet of Things based smart industries. *IEEE Trans. Reliab.* **2021**, *71*, 348–358. [CrossRef]
10. Mohamed, N.; Al-Jaroodi, J. Applying blockchain in industry 4.0 applications. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 852–858.
11. Cao, Y.; Jia, F.; Manogaran, G. Efficient Traceability Systems of Steel Products Using Blockchain-Based Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6004–6012. [CrossRef]
12. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
13. Leng, J.; Zhou, M.; Zhao, J.L.; Huang, Y.; Bian, Y. Blockchain security: A survey of techniques and research directions. *IEEE Trans. Serv. Comput.* **2020**, *15*, 2490–2510. [CrossRef]
14. Bhushan, B.; Sinha, P.; Sagayam, K.M.; Andrew, J. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Comput. Electr. Eng.* **2021**, *90*, 106897. [CrossRef]
15. Huang, H.; Kong, W.; Zhou, S.; Zheng, Z.; Guo, S. A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools. *ACM Comput. Surv.* **2022**, *54*, 44.1–44.42. [CrossRef]
16. Das, S.; Mohanta, B.K.; Jena, D. A state-of-the-art security and attacks analysis in blockchain applications network. *Int. J. Commun. Netw. Distrib. Syst.* **2022**, *28*, 199–218. [CrossRef]
17. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
18. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; Caro, A.D.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
19. Yu, B.; Wright, J.; Nepal, S.; Zhu, L.; Liu, J.; Rajiv, R. IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain. *IEEE Cloud Comput.* **2018**, *5*, 12–20. [CrossRef]
20. Wan, J.; Li, J.; Imran, M.; Li, D.; E-Amin, F. A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3652–3660. [CrossRef]

21. Jing, Z.; Gu, C.; Li, Y.; Mengshi, Z.; Guangquan, X.; Alireza, J.; Peizhong, S.; Chenkai, T.; Xi, Z. Security analysis of indistinguishable obfuscation for internet of medical things applications. *Comput. Commun.* **2020**, *161*, 202–211. [CrossRef]
22. Zhang, Q.; Li, Y.; Wang, R.; Liu, L.; Tan, Y.A.; Hu, J. Data security sharing model based on privacy protection for blockchain-enabled industrial Internet of Things. *Int. J. Intell. Syst.* **2021**, *36*, 94–111. [CrossRef]
23. Tan, C.; Bei, S.; Jing, Z.; Xiong, N.N. An atomic cross-chain swap-based management system in vehicular Ad hoc networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6679654. [CrossRef]
24. Xu, G.; Bai, H.; Xing, J.; Luo, T.; Xiong, N.N. SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles. *J. Parallel Distrib. Comput.* **2022**, *164*, 1–11. [CrossRef]
25. Dibaei, M.; Zheng, X.; Xia, Y.; Xu, X.; Jolfaei, A.; Kashif Bashir, A.; Tariq, U.; Yu, D.; Vasilakos, A.V. Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 683–700. [CrossRef]
26. Kasten, J.E. Engineering and manufacturing on the blockchain: A systematic review. *IEEE Eng. Manag. Rev.* **2020**, *48*, 31–47. [CrossRef]
27. Saxena, S.; Bhushan, B.; Ahad, M.A. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *J. Netw. Comput. Appl.* **2021**, *181*, 103050. [CrossRef]
28. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Alazab, M. Blockchain for industry 4.0: A comprehensive review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]
29. Khalid, R.; Samuel, O.; Javaid, N.; Aldegheishem, A.; Shafiq, M.; Alrajeh, N. A Secure Trust Method for Multi-Agent System in Smart Grids Using Blockchain. *IEEE Access* **2021**, *9*, 59848–59859. [CrossRef]
30. Liang, C.; Shanmugam, B.; Azam, S.; Karim, A.; Idris, N.B. Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems. *Electronics* **2020**, *9*, 1120. [CrossRef]
31. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy challenges. *Internet Things* **2019**, *8*, 100–107. [CrossRef]
32. Ferrag, M.A.; Shu, L. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet Things J.* **2021**, *8*, 17236–17260. [CrossRef]
33. Dutta, S.; Chakraborty, S. IoT-Based Secure Communication to Enhance Blockchain Model. In *Lecture Notes in Electrical Engineering: Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems*; Springer: Singapore, 2021; pp. 255–264.
34. Dorri, A.; Mishra, S.; Jurdak, R. Vericom: A Verification and Communication architecture for IoT-based blockchain. *Ad Hoc Netw.* **2022**, *133*, 102882. [CrossRef]
35. Centobelli, P.; Cerchione, R.; Del Vecchio, P.; Oropallo, E.; Secundo, G. Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Inf. Manag.* **2021**, 103508. [CrossRef]
36. Yu, H.; Xu, D.; Luo, N.; Xing, B.; Chuang, S. Design of the blockchain multi-chain traceability supervision model for coarse cereal supply chain. *Trans. Chin. Soc. Agric. Eng.* **2021**, *37*, 323–332.
37. Chen, S.; Cai, X.; Wang, X.; Liu, A.; Lu, Q.; Xu, X.; Tao, F. Blockchain applications in PLM towards smart manufacturing. *Int. J. Adv. Manuf. Technol.* **2022**, *118*, 2669–2683. [CrossRef]
38. Hader, M.; Tchoffa, D.; El Mhamedi, A.; Ghodous, P.; Dolgui, A.; Abouabdellah, A. Applying integrated Blockchain and Big Data technologies to improve supply chain traceability and information sharing in the textile sector. *J. Ind. Inf. Integr.* **2022**, *28*, 100345. [CrossRef]
39. Chung, K.; Yoo, H.; Choe, D.; Jung, H. Blockchain network based topic mining process for cognitive manufacturing. *Wirel. Pers. Commun.* **2019**, *105*, 583–597. [CrossRef]
40. Zuo, Y. Making smart manufacturing smarter–a survey on blockchain technology in Industry 4.0. *Enterp. Inf. Syst.* **2021**, *15*, 1323–1353. [CrossRef]
41. Cao, B.; Wang, X.; Zhang, W.; Song, H.; Lv, Z. A Many-Objective Optimization Model of Industrial Internet of Things Based on Private Blockchain. *IEEE Netw.* **2020**, *34*, 78–83. [CrossRef]
42. Huo, R.; Zeng, S.; Wang, Z.; Shang, J.J.; Chen, W.; Huang, T.; Shuo, W.; Richard, Y.F.; Yun, L. A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 88–122. [CrossRef]
43. Aoun, A.; Ilinca, A.; Ghandour, M.; Ibrahim, H. A review of Industry 4.0 characteristics and challenges, with potential improvements using blockchain technology. *Comput. Ind. Eng.* **2021**, *162*, 107746. [CrossRef]
44. Kumar, A.; Abhishek, K.; Bhushan, B.; Chakraborty, C. Secure access control for manufacturing sector with application of ethereum blockchain. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3058–3074. [CrossRef]
45. Wen, Q.; Gao, Y.; Chen, Z.; Da, W. A blockchain-based data sharing scheme in the supply chain by IIoT. In Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, 6–9 May 2019; pp. 695–700.
46. Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. *Inf. Process. Manag.* **2021**, *58*, 102526. [CrossRef]
47. Agrawal, T.K.; Angelis, J.; Khilji, W.A.; Kalaiarasan, R.; Wiktorsson, M. Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration. *Int. J. Prod. Res.* **2022**, 1–20. [CrossRef]

48. Boneh, D.; Gentry, C.; Lynn, B.; Shacham, H. Aggregate and verifiably encrypted signatures from bilinear maps. In *Lecture Notes in Computer Science: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 4–8 May 2003*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 416–432.
49. Fischlin, M.; Lehmann, A.; Schröder, D. History-free sequential aggregate signatures. In *Lecture Notes in Computer Science: Proceedings of the 2012 International Conference on Security and Cryptography for Networks, Amalfi, Italy, 5–7 September 2012*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 113–130.
50. Xu, G.; Dong, W.; Xing, J.; Wen, L.; Jian, L.; Li, G.; Mei, F.; Zheng, X.; Shao, L. Delay-CJ: A novel cryptojacking covert attack method based on delayed strategy and its detection. *Digit. Commun. Netw.* **2022**. [CrossRef]