sensors

MDPI

Article

A Business-to-Business Collaboration System That Promotes Data Utilization While Encrypting Information on the Blockchain

Hiroaki Nasu [1,*], Yuta Kodera [2] and Yasuyuki Nogami [2]

[1] Graduate School of Natural Science and Technology, Okayama University, Okayama 700-8530, Japan
[2] Faculty of Natural Science and Technology, Okayama University, Okayama 700-8530, Japan; yuta_kodera@okayama-u.ac.jp (Y.K.); yasuyuki.nogami@okayama-u.ac.jp (Y.N.)
* Correspondence: ptk36s3v@s.okayama-u.ac.jp

Abstract: Ensuring the reliability of data gathering from every connected device is an essential issue for promoting the advancement of the next paradigm shift, i.e., Industry 4.0. Blockchain technology is becoming recognized as an advanced tool. However, data collaboration using blockchain has not progressed sufficiently among companies in the industrial supply chain (SC) that handle sensitive data, such as those related to product quality, etc. There are two reasons why data utilization is not sufficiently advanced in the industrial SC. The first is that manufacturing information is top secret. Blockchain mechanisms, such as Bitcoin, which uses PKI, require plaintext to be shared between companies to verify the identity of the company that sent the data. Another is that the merits of data collaboration between companies have not been materialized. To solve these problems, this paper proposes a business-to-business collaboration system using homomorphic encryption and blockchain techniques. Using the proposed system, each company can exchange encrypted confidential information and utilize the data for its own business. In a trial, an equipment manufacturer was able to identify the quality change caused by a decrease in equipment performance as a cryptographic value from blockchain and to identify the change one month earlier without knowing the quality value.

Keywords: business-to-business data collaboration; industrial supply chain; blockchain; homomorphic encryption

Citation: Nasu, H.; Kodera, Y.; Nogami, Y. A Business-to-Business Collaboration System That Promotes Data Utilization While Encrypting Information on the Blockchain. *Sensors* **2022**, *22*, 4909. https://doi.org/10.3390/s22134909

Academic Editor: Nikos Fotiou

Received: 31 May 2022
Accepted: 27 June 2022
Published: 29 June 2022

1. Introduction

In order to promote Society 5.0, the Industrial Internet of Things, Industry 4.0, and so forth, it is important to connect and share data so that all IoT devices and all members can trust them. Blockchain (BC) technology is attracting attention as an advanced tool. Blockchain is a digital ledger for record-keeping over peer-to-peer (P2P) networks [1,2]. It is decentralized and dispersed in nature with tamper-resistant and tamper-evident features [3–5]. Each peer stores a copy of the blockchain and verifies the validity of the stored data, such that no peers can tamper with the data. For example, in the blockchain, all money in and out is stored in the block as historical data and connected in chronological order. The hash value of the previous block is included in the next block. Even if a peer participating in the network falsifies the data of a certain block, the hash value of the block will change, so it will not match the hash of the next block connected to it. Therefore, the fraud of the peer can be immediately revealed.

The concept of blockchain technology was derived from Bitcoin cryptocurrency, and then it spread to the financial field. This is still the main field in which blockchain technology is used [6,7]. Currently, in addition to the financial field, the blockchain technique is used in smart homes [8], smart cities [9,10], smart agriculture [11,12], smart power grids [13], smart transportation and automotives [14], smart healthcare [15,16], IoT networks [17,18], and security privacy [19]. In the smart-manufacturing field, much research

has been conducted related to the certificate of origin, procurement, production, inspection, logistics, and sales [20–27]. In the business-to-business (B2B) manufacturing industry, the demands for high-quality product development and plan optimization can be met by sharing manufacturing data among companies in the supply chain (SC) [28–31]. To meet these demands, manufacturers need an environment where the data shared by the company cannot be tampered with. Additionally, each company's manufacturing and inspection process data must be connected throughout the SC, from materials to products. BC technology is one an effective approach for building such an environment. However, production or inspection data collaboration using BC has not progressed sufficiently among companies in the industrial SC. One of the main reasons is that production and inspection data are highly confidential and therefore difficult to disclose to other companies (e.g., product quality data, equipment data, and order-shipping data) [32].

There are movements to improve data infrastructure beyond companies, mainly in Europe [33,34]. Attention is also focused on efforts to optimize the entire SC by constructing twin digital platforms. However, no matter how much infrastructure and how many platforms are built, in terms of B2B manufacturing data collaboration, it will be difficult to freely link highly confidential data unless two companies can agree on a contract. With data collaboration based on a contract between two companies, it is difficult to build an ecosystem in which data is widely and freely linked among companies. Even if a consortium were to be formed, as long as there is competition among companies, companies would not be able to safely disclose their data, which is the source of their revenue.

Regarding this issue, refs. [35,36] proposed methods for privacy protection for the IoT by combining encryption with BC or IOTA. Ref. [37] proposed an algorithm of the privacy-preserving OLPA for big data analysis. However, there is another major reason why data collaboration between companies is not progressing; the merits of data collaboration in a concrete manufacturing scene are not readily apparent, and its implementation with respect to both business and technology is difficult. It is important to design the benefits of being able to put data into a BC while ensuring a company's competitive advantage. The authors of [35–37] have not been able to propose a protocol in consideration of the utilization in business after encryption. In order to achieve B2B collaboration between companies in the industrial SC, it is important to have a protocol and a system that can both "protect data" and "utilize data in the manufacturing process".

This paper proposes a B2B collaboration system using homomorphic encryption (HE) and BC techniques. Using the proposed system, each company in the industrial SC can exchange confidential information, such as quality data, in an encrypted manner and utilize the data in their own manufacturing. In addition, this paper shows a scenario, system architecture, and protocol for upstream companies to grasp changes in the manufacturing quality of downstream companies. In this scenario, this paper evaluates the merit of concrete data collaboration in actual business using the proposed system.

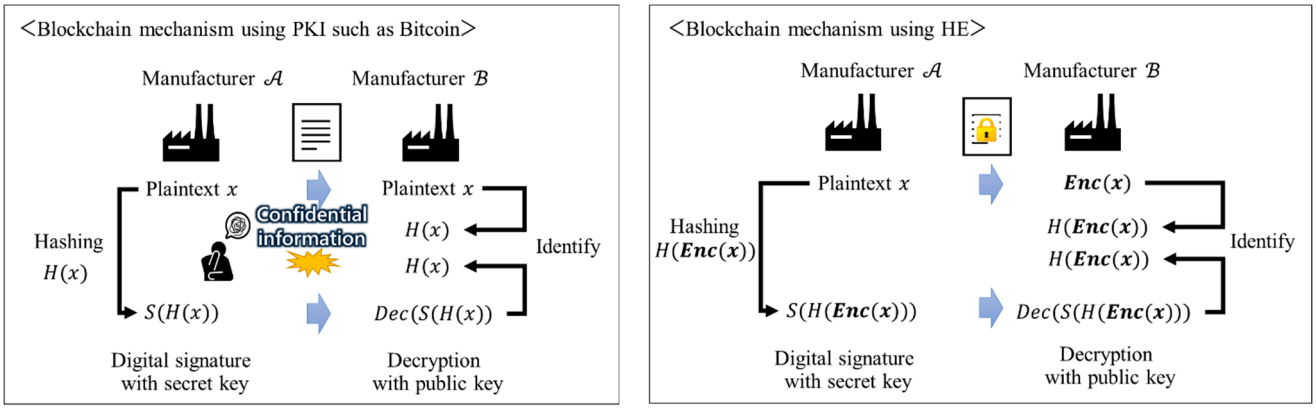
The paper is structured as follows: Section 2 describes the blockchain issue in data linkage, a scenario for realizing B2B collaboration in the production process in the SC, and the issue of numerical comparison while maintaining the encryption required in the scenario. Section 3 proposes a secure comparison protocol and a B2B collaboration system to resolve these issues. Section 4 demonstrates the usefulness of the proposed system and protocol in an actual business scenario, and Section 5 evaluates the safety of the proposed system.

2. Preliminaries

2.1. The Problem of BC Utilization and the Secure Approach in B2B Collaboration in the SC

In the B2B manufacturing industry, it is difficult for each company to disclose confidential information regarding its manufacturing know-how, even if it is a company that transacts in the SC. Blockchain mechanisms such as Bitcoin, which uses public key cryptography (PKI), require that plaintext be sent to identify a company (Figure 1a). Therefore,

blockchains are not widely used for collaboration between companies in the manufacturing SC [32].



(**a**) (**b**)

Figure 1. The issue of BC utilization and the secure approach in B2B collaboration. (**a**) Issue of BC utilization; (**b**) Secure approach in B2B collaboration.

Regarding this issue, this paper proposes a secure B2B collaboration system in the SC that enables open data transfer and business coordination by combining blockchain technology and homomorphic encryption. In 1978, Ronald Rivest et al. suggested a proposal on the concept of homomorphic encryption [38]. Later, Craig Gentry proposed fully homomorphic encryption that computes an arbitrary number of additions and multiplications to encrypted data [39]. This scheme enables the programs for any desirable functionality, such as homomorphic property, to run on encrypted data and produce an encryption of the result. A partial homomorphic encryption exhibits either an additive or multiplicative homomorphism, but not both. In addition, the efficiency of some partial homomorphic encryption schemes is high enough for practical applications [40].

In a secure collaboration system that uses partial HE and blockchain techniques, each company in the SC can exchange confidential information using encrypted data and utilize it for their own business needs (Figure 1b). In this paper, as shown in Figure 1b, the encryption of plaintext x using HE is denoted as $Enc(x)$.

2.2. A B2B Collaboration Scenario on the Industrial SC

Let us consider a scenario in which $\mathcal{A}$ manufactures a product $P_\mathcal{A}$ of quality $Q_\mathcal{A}$ with equipment $E_\mathcal{A}$ and delivers $P_\mathcal{A}$ to $\mathcal{B}$. $\mathcal{B}$ uses $P_\mathcal{A}$ as a material to manufacture a product $P_\mathcal{B}$ of quality $Q_\mathcal{B}$ with equipment $E_\mathcal{B}$. At this time, $\mathcal{A}$ wants to optimize the production plan by identifying the level of quality $Q_\mathcal{B}$ that can be produced when the product $P_\mathcal{A}$ is put into the equipment of $\mathcal{B}$. Although $\mathcal{B}$ wants a stable supply of high-quality materials from $\mathcal{A}$, it does not want to disclose its own manufacturing information because it is confidential. For this scenario, in this research, $\mathcal{B}$ sends $Enc(P_\mathcal{B}, Q_\mathcal{B}, E_\mathcal{B})$ to $\mathcal{A}$ using HE. Therefore, $\mathcal{A}$ can calculate its relationship and compatibility with $(P_\mathcal{A}, Q_\mathcal{A}, E_\mathcal{A})$ without knowing the specific product name $P_\mathcal{B}$, quality $Q_\mathcal{B}$, and equipment $E_\mathcal{B}$, and it can formulate the optimum production plan for $\mathcal{A}$.

In the field of chemistry, products are manufactured by reacting materials. Therefore, the impact on product quality caused by the physical properties of materials and the compatibility of equipment is important. The utilization of the proposed scenario in real businesses can be expected.

In regard to the above scenario, this paper focuses on quality data. $\mathcal{A}$ wants to catch the change of $Enc(Q_\mathcal{B})$ at time t and $t+1$, and if there is a big change, $\mathcal{A}$ will identify its own manufacturing factors, leading to optimum production. Therefore, in order to realize the proposed scenario, it is important to have a comparison protocol for the values of t and $t+1$ so as to encrypt them. In the protocol, a function to put quality data into the blockchain

and a function to get them from the blockchain are also important for implementing the proposed scenario.

The final system for the B2B collaboration is shown in Figure 2. In this final system, manufacturing companies can chain data without disclosing their quality data, while also guaranteeing their identities using blockchain. Even if the encrypted quality data were to be tampered with by an attacker, the hash value of the encrypted quality data would not match the value after decrypting the signature. Therefore, tampering could be detected immediately. In addition, traceability in the SC is possible by including the lot number of each company's products in the encryption. Under such a secure data linkage, $\mathcal{A}$ will be able to identify changes in the quality data of downstream companies in a timely manner and to utilize that information in its own manufacturing.

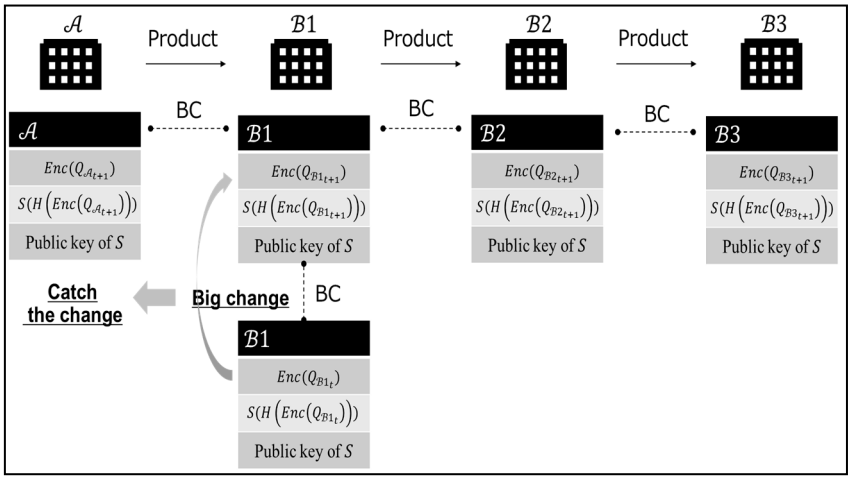


Figure 2. The final system of the B2B collaboration.

2.3. Conventional Comparison Protocol Using HE and Issues with B2B Collaboration

In 2016, Wu et al. proposed a comparison protocol based on Paillier cryptography, a kind of additive homomorphic encryption [41]. In the protocol, the client and server have the values x and y, respectively. Neither party learns anything else about the other party's input.

In the protocol, suppose the binary representations of x and y are $x_0, x_1, \ldots, x_{k-1}$ (k bits) and $y_0, y_1, \ldots, y_{k-1}$ (k bits), respectively. Using the following proposition, $x > y$ or $x < y$ is determined.

Proposition 1. *$x < y$ if and only if there exists some index $i \in [k-1]$ that satisfies Formula (1). $x > y$ if and only if there exists some index $i \in [k-1]$ that satisfies Formula (2).*

$$x_i - y_i + 1 + 3\sum_{j<i}(x_j \oplus y_j) = 0, \tag{1}$$

$$x_i - y_i - 1 + 3\sum_{j<i}(x_j \oplus y_j) = 0. \tag{2}$$

Here are the details. The client and server encrypt x_i and y_i with the public key, respectively. The client sends $Enc(x_i)$ to the server. The server calculates Formula (1) or (2) by substituting $Enc(x_i)$ and $Enc(y_i)$ and using plaintext y_i for XOR. The client receives the calculation result, decrypts it with the secret key, and checks for zero. Therefore, the client can determine that $x > y$ or $x < y$ without disclosing the value of x to the server.

In the proposed scenario for B2B collaboration, $\mathcal{B}$ has both x and y of the quality data, and $\mathcal{A}$ has $Enc(x)$ and $Enc(y)$. Therefore, $\mathcal{A}$ cannot calculate XOR using the above formula, and this conventional protocol is difficult to apply to B2B collaboration in the SC.

In addition, in order to realize the proposed scenario in an actual business, it is necessary to consider a system architecture, including business viewpoints and a comparison protocol, according to the architecture.

3. Proposal B2B Collaboration System on the SC

In [42], our previous work showed a secure comparison protocol for B2B collaboration in the SC at ICCE-TW2021. This paper shows the concrete system architecture required to implement the proposed scenario for the actual business. This paper also shows the usefulness of the proposal system by adding the evaluation results in specific business situations.

3.1. System Architecture of the B2B Collaboration

This paper shows the system architecture for implementing the proposed scenario in Figure 3. In a real business, it is necessary to have a servicer that provides value by exchanging data and guaranteeing the service level. In other words, the servicer is the company responsible for realizing the proposed scenario and the solution engineer who builds the data platform business. Therefore, the proposed system has a servicer S, as well as the manufacturers $\mathcal{A}$ and $\mathcal{B}$. Each organization has at least one peer and certificate authority (CA) that manages the members of the organization, and the data is put into the blockchain by the orderer. Each peer has a state database that records the state of the data and a chaincode that holds the history of data transfers as a distributed ledger of the blockchain.

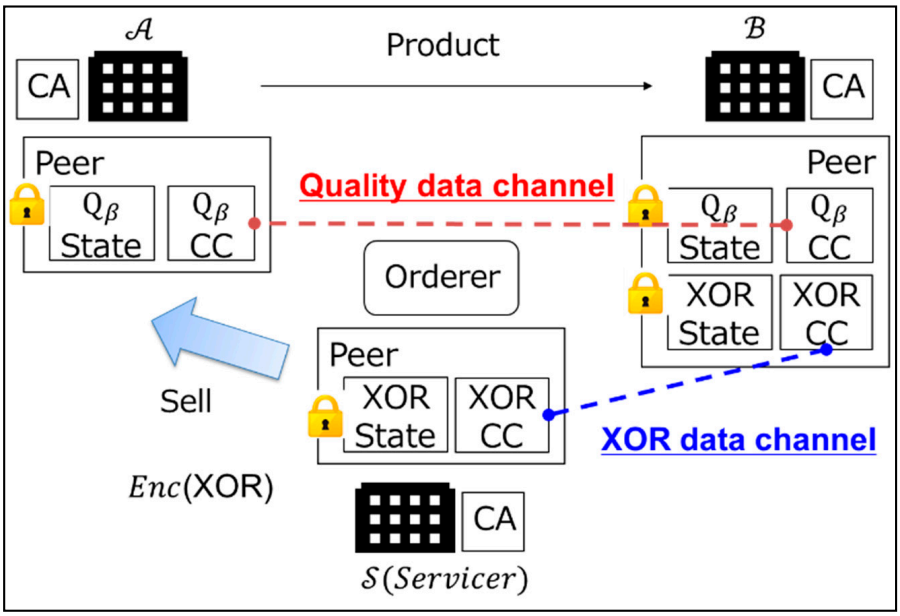


Figure 3. Proposed B2B collaboration system.

As shown in Figure 3, this paper proposes a multi-channel system architecture that separates the chaincode for the quality data and the XOR data. $\mathcal{B}$ has both x and y of the quality data and $\mathcal{B}$ puts $Enc(x)$ and $Enc(y)$ into the quality chaincode of $\mathcal{B}$ (Q_β CC). $\mathcal{A}$ can get $Enc(x)$ and $Enc(y)$ from Q_β CC. In the proposed scenario, the XOR data of $\mathcal{B}$ are essential for the calculation of Formulas (1) and (2). These are important key data, from both a technical and a business perspective. Therefore, in the proposed system architecture, $\mathcal{B}$ calculates $x \oplus y$ and puts $Enc(x \oplus y)$ into the XOR chaincode (XOR CC). S can get $Enc(x \oplus y)$ from XOR CC and sell $Enc(x \oplus y)$ to $\mathcal{A}$ as a servicer. The reason that the servicer does not have the quality data is that the servicer and $\mathcal{B}$ may be in a competitive relationship. The servicer is only positioned to provide the key XOR data. Only $\mathcal{A}$, which has a transaction with $\mathcal{B}$ in the SC, can grasp the change in quality.

There is another secondary reason for the architecture to have multiple channels with S. It is robust access control. If the product of $\mathcal{B}$ is manufactured from the materials of $\mathcal{A}$ and $\mathcal{A}'$, $\mathcal{A}'$ might get the big quality change in the material of $\mathcal{A}$ from Q_β CC as a business opportunity and make an offer to $\mathcal{B}$ to replace an order for the material of $\mathcal{A}$. Even if $\mathcal{A}'$ obtains the private key of $\mathcal{A}$ by some means, if S manages the XOR data and does not sell the data to $\mathcal{A}'$, $\mathcal{A}'$ cannot calculate Formula (1) or (2) without the XOR data.

3.2. Implementation of the Comparison Protocol to Realize the B2B Collaboration System

This paper proposes an improved secure comparison protocol for implementation in the B2B collaboration system using a variant of Wu's protocol, which is based on Paillier cryptography. X and Y are the quality data (plaintexts) of $\mathcal{B}$ at time t and $t+1$, respectively.

In this proposed protocol, $Enc(x_i)$, $Enc(y_i)$, and $Enc(x_i \oplus y_i)$ are encrypted with Paillier cryptography [43]. In Paillier cryptography, message $m \in \mathbb{Z}_n$ is encrypted by (3) with integers $n = p \cdot q$, $g = 1 + n \bmod n^2$, where p and q are prime numbers of about 3000 bits, r is a random number $0 < r < n \in \mathbb{Z}^*_{n^2}$, and $\gcd(r,\ n) = 1$. The public key is $(n,\ g)$. The secret key is $(p,\ q)$.

$$C = g^m \cdot r^n \bmod n^2 \tag{3}$$

Decryption is carried out via the following formula using Carmichael's theorem: $r^{n\lambda} \bmod n^2 = 1$. Here, $\lambda = lcm(p-1,\ q-1)$ and a function $L(u) = (u-1)/n$.

$$C^\lambda = g^{\lambda m} \cdot r^{n\lambda} \bmod n^2 = (1 + \lambda mn) \bmod n^2 \tag{4}$$

Therefore,

$$m = L\left(C^\lambda \bmod n^2\right) / L\left(g^\lambda \bmod n^2\right) \bmod n. \tag{5}$$

1. Cryptographic Protocol of $\mathcal{B}$ Table 1 shows the cryptographic protocol of $\mathcal{B}$. First, $\mathcal{B}$ binary-expands the quality data X and Y. Additionally, $\mathcal{B}$ encrypts the x_i bit of X, the y_i bit of Y, and $x_i \oplus y_i$ using Formula (3). Then, it puts $Enc(x_i)$, $Enc(y_i)$, $Enc(x_i \oplus y_i)$, and the public key into the blockchain, as shown in Figure 3 and Appendix A.

Table 1. Encryption Protocol of $\mathcal{B}$.

Step	Processing
1	$\mathcal{B}$ binary-expands X and Y and encrypts x_i and y_i (i = 0~k-1 bits) with the public key.
2	$\mathcal{B}$ puts $Enc(x_i)$, $Enc(y_i)$, and the public key into the quality data chaincode Q_β CC, as seen in Figure 3.
3	$\mathcal{B}$ calculates $Enc(x_i \oplus y_i)$ with the public key.
4	$\mathcal{B}$ puts $Enc(x_i \oplus y_i)$ and the public key into the XOR data chaincode XOR CC, as seen in Figure 3.

2. Calculation Protocol of S Table 2 shows the calculation protocol of S. S gets and saves $Enc(x_i \oplus y_i)$ and the public key from XOR CC, as seen in Figure 3. If there is a request from $\mathcal{A}$, S uses the public key as a key to identify $Enc(x_i \oplus y_i)$ and sends the $Enc(x_i \oplus y_i)$ to $\mathcal{A}$. S is a servicer that handles important XOR data in this B2B collaboration system.

Table 2. Calculation Protocol of S.

Step	Processing
1	S gets and saves $Enc(x_i \oplus y_i)$ and the public key from the XOR data chaincode XOR CC, as seen in Figure 3.
2	S receives an XOR data request and a public key from $\mathcal{A}$.
3	S identifies the $Enc(x_i \oplus y_i)$ that has the same public key sent by $\mathcal{A}$ in Step 2.
4	If there is an $Enc(x_i \oplus y_i)$, S sends the $Enc(x_i \oplus y_i)$ to $\mathcal{A}$.

3. Calculation Protocol of $\mathcal{A}$ Table 3 shows the calculation protocol of $\mathcal{A}$. $\mathcal{A}$ gets $Enc(x_i)$, $Enc(y_i)$, and the public key from Q_β CC, as seen in Figure 3. Additionally, $\mathcal{A}$ gets $Enc(x_i \oplus y_i)$ from S by sending a public key of t and $t+1$, where $\mathcal{A}$ wants to identify the change. $\mathcal{A}$ calculates those quality data using Formulas (1) and (2) while keeping them encrypted.

Table 3. Calculation Protocol of $\mathcal{A}$.

Step	Processing
1	$\mathcal{A}$ gets $Enc(x_i)$, $Enc(y_i)$, and the public key from the quality data chaincode Q_β CC as seen in Figure 3.
2	$\mathcal{A}$ sends the public key to S and receives $Enc(x_i \oplus y_i)$ from S.
3	From the most significant bit, $\mathcal{A}$ calculates $Enc(z_i) = Enc\left(x_i - y_i \pm 1 + 3\sum_{j<i}\left(x_j \oplus y_j\right)\right)$.
4	$\mathcal{A}$ sends $Enc(z_i)$ to $\mathcal{B}$.

In the proposed protocol for Step 3, it is necessary to calculate $Enc(-y_i)$ from $Enc(y_i)$. This proposed protocol uses Formula (6) from Paillier cryptography to calculate $Enc(-y_i)$.

$$C^{n-1} = (g^m.r^n)^{n-1} \bmod n^2 \tag{6}$$

4. Decryption Protocol of $\mathcal{B}$ Table 4 shows the decryption protocol of $\mathcal{B}$. Using the secret key and Formula (5), $\mathcal{B}$ decrypts $Enc(z_i)$ and searches for the bit, where $z_i = 0$.

Table 4. Decryption Protocol of $\mathcal{B}$.

Step	Processing
1	$\mathcal{B}$ receives $Enc(z_i)$ from $\mathcal{A}$.
2	$\mathcal{B}$ decrypts $Enc(z_i)$ with the secret key.
3	If there is $z_i = 0$, $\mathcal{B}$ sends i to $\mathcal{A}$.

5. Comparison Protocol of $\mathcal{A}$ Table 5 shows the comparison protocol of $\mathcal{A}$. Finally, $\mathcal{A}$ receives i or knows that $z_i = 0$ did not occur. If $\mathcal{A}$ receives i while using Formula (1), then $X < Y$ can be determined. If $\mathcal{A}$ receives i while using Formula (2), then $X > Y$ can be determined. Here, i is the first different bit when comparing X and Y from the most significant bit. Therefore, using this proposed protocol, $\mathcal{A}$ can grasp $X < Y$ or $X > Y$ and the scale of the difference between X and Y without knowing the numbers that X and Y represent; that is, $\mathcal{A}$ can confirm the change in quality data in the time series.

Table 5. Comparison Protocol of $\mathcal{A}$.

Step	Processing
1	$\mathcal{A}$ receives i when $z_i = 0$ or knows that $z_i = 0$ did not occur.
2	If $\mathcal{A}$ receives i while using Formula (1), then $X < Y$ can be determined. If $\mathcal{A}$ receives i while using Formula (2), then $X > Y$ can be determined.
3	$\mathcal{A}$ checks the difference between the numbers at times t and $t+1$ by calculating 2^i.

3.3. System Configuration

The proposed system was constructed as shown in Figure 4. A company was set up as one organization in a docker container on the AWS EC2. A blockchain network was built using Hyperledger Fabric, which utilizes the Amazon Managed Blockchain (AMB) service. Hyperledger Fabric was adopted to build a private blockchain for companies in the SC. In order to efficiently calculate multi-length arithmetic, the encryption, decryption, and calculation of the data were programmed by C++. APIs for both putting data into and getting data from the blockchain were developed by Golang.

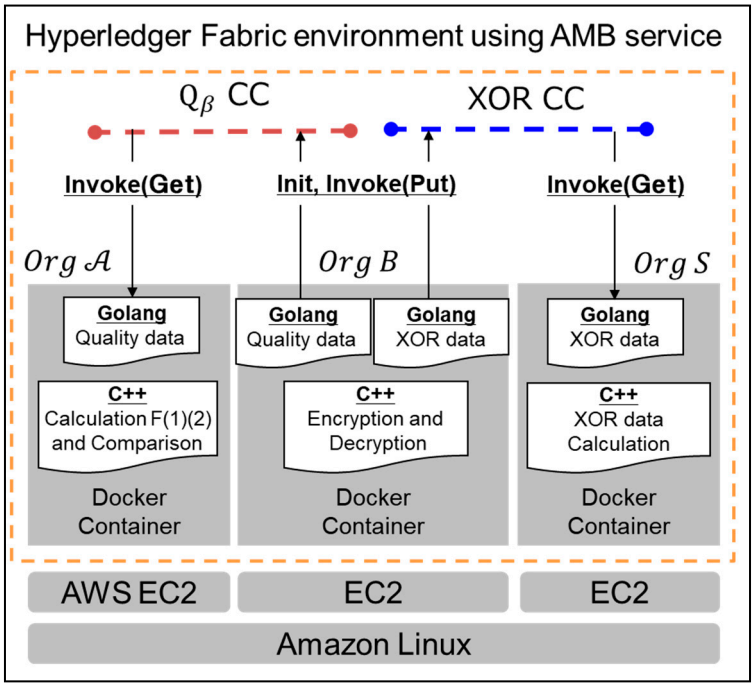


Figure 4. Configuration of proposed the B2B collaboration system.

4. Evaluation Result of the Concrete Data-Collaboration's Merits

Finally, this paper considers the usefulness of the proposed system and protocol. In the actual case in Figure 5, manufacturer $\mathcal{A}$ provided dry dehumidifiers to the dry products of manufacturer $\mathcal{B}$. One day, a complaint was made about the decreased performance of the dehumidifiers from $\mathcal{B}$, and it turned out that the friction-reducing film, which should have been attached to the dehumidifying rotors, was not attached. It took four months from delivery for the performance reduction of be noticed. By applying the proposed protocol, $\mathcal{B}$ was able share product moisture data, which are confidential manufacturing data, with $\mathcal{A}$ in an encrypted manner. This paper evaluates whether $\mathcal{A}$ was able to notice the quality change at an early stage in the actual business setting.

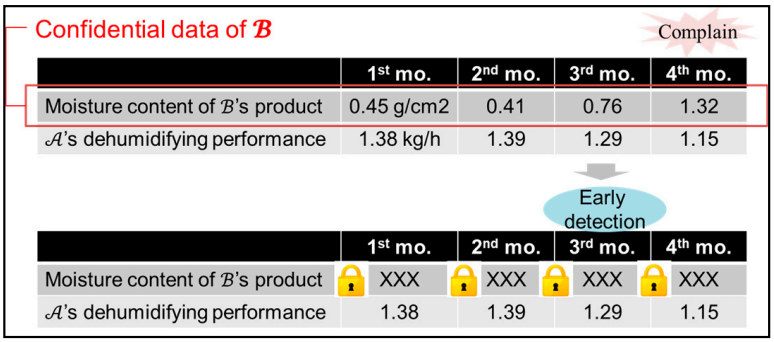


Figure 5. An actual business example of concrete data collaboration.

Figure 6 shows the result of an experiment where the proposed protocol and system were applied. $\mathcal{B}$ was able to provide confidential moisture data encrypted as messages 1 and 2. Using the proposed system, $\mathcal{A}$ was able to detect the decreased performance in the third month by getting 10-times the encrypted moisture data from the quality chaincode and encrypted XOR data from the XOR chaincode so as to observe the changes in quality each month. In Paillier cryptography, message $m \in \mathbb{Z}_n$ is required, so the quality data are multiplied by 10. As can be seen in Figure 6, $\mathcal{A}$ does not know the specific numerical value of the quality data. This paper confirms the behavior and usefulness of the proposed system.

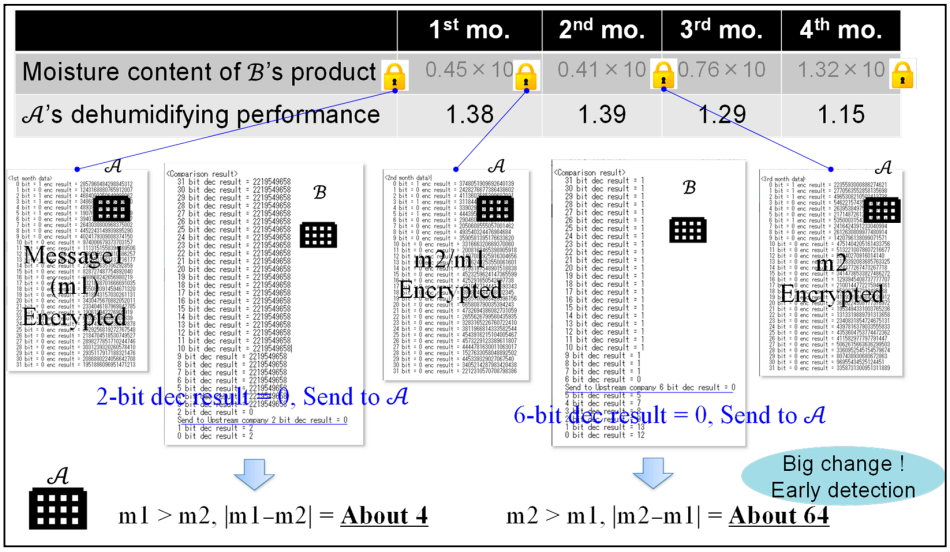


Figure 6. Evaluating the result of the concrete data collaboration.

5. Safety Evaluation of the Proposed System

This paper does not consider the case where $\mathcal{B}$ maliciously puts incorrect quality data $Enc(x_i)$ and $Enc(y_i)$ to Q_β CC in Step 2 of Table 1. The incorrect quality data put by $\mathcal{B}$ means to disrupt the SC for their own material procurement. Such cases are nonsensical from a business perspective and are not worth considering.

In Paillier cryptography, since $\mathcal{A}$ does not know $(p,\ q)$ and g^m is masked by $r^{p \cdot q}$ in Formula (3), it is difficult to solve the discrete logarithmic problem in the exponential part of Formula (3). Thus, the message m cannot be identified [43].

In the proposed comparison protocol of the B2B collaboration system, since ciphertexts are encrypted using random number r in Formula (3), $\mathcal{A}$ cannot identify x_i or y_i by comparing $Enc(x_i)$, $Enc(y_i)$, and $Enc(x_i \oplus y_i)$, as can be seen in Figure 6.

In the B2B collaboration system, there is a risk that company $\mathcal{C}$, participating in the quality channel, will impersonate $\mathcal{A}$. Since $\mathcal{C}$ participates in the quality channel, $\mathcal{C}$ can get the public keys. If $\mathcal{C}$ intercepts $\mathcal{A}$'s $Enc(z_i)$, falsifies the encrypted data with Paillier cryptography, and sends it to $\mathcal{B}$, $\mathcal{A}$ will not be able to grasp the change in quality. However, since $\mathcal{C}$ is also a company in the SC related to $\mathcal{B}$'s products, when it is found that it is impersonating $\mathcal{A}$, $\mathcal{C}$ will receive great punishment. That is, $\mathcal{C}$ will not be able to trade with any other company. Therefore, it is unlikely that spoofing by a company such as $\mathcal{C}$ will occur in the proposal system. Even if the encrypted data were to be leaked to a company that does not participate in a blockchain channel, it would not be tampered with unless the public key were leaked.

6. Conclusions

This paper proposed a secure comparison protocol for the sharing and grasping of changes to even highly sensitive data between companies by keeping the data encrypted. By implementing the protocol on a blockchain that connects companies in the industrial SC, this paper also proposed a B2B collaboration system. In a scenario with a business focusing on quality data, which is the most sensitive data in manufacturing, this paper showed that a company can grasp the change in the quality data of their business partner, while keeping the data encrypted, and subsequently feed that change back into its own manufacturing.

By using the proposed system, upstream companies will be able to grasp the quality changes of downstream companies. Combined with data from IoT sensors attached to their equipment, upstream companies will be able to proactively respond to the decreased performance of delivery equipment, which is directly linked to quality. In addition, small- and medium-sized manufacturers are said to lack sales resources, but the proposed system enables them to grasp the quality improvement needs of downstream companies in advance

and reflect those needs in their own functional development. Upstream companies, many of which are large companies, do not disclose the quality value to other companies via encryption, and there is no concern that quality data will be tampered with by other companies by BC, so data can be provided with peace of mind. The social implementation of this research will create an ecosystem of collaboration among companies in the industrial SC, which will enable highly efficient manufacturing.

Note that the proposed protocol uses Paillier cryptography, which requires the use of a 6000-bit space for secure encryption and decryption. Investigating speed-up using elliptic cryptography or other methods is the goal for future research.

Author Contributions: Conceptualization, methodology, validation, and formal analysis, H.N.; software, H.N.; writing—original draft preparation, H.N.; writing—review and supervision, Y.N. and Y.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the JSPS KAKENHI Grant-in-Aid for Challenging Research (Pioneering) (20K20484).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This work was partially supported by the Research Support Program toward Society 5.0 provided by Cypher at Okayama University, Japan. We are grateful to Ryota Miyamoto, who participated in helpful discussions and prototype development.

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

Appendix A

Figure A1a,b shows the data structure of Q_β CC and XOR CC, respectively. Quality data and XOR data are put into the BC with a common lot number and public key n to identify when they were put and the production lot data to which they correspond. In Figure A1, "Pubkey_n" is the Paillier cryptography public key. Figure A1 shows an example where n is 32 bits. "T1Q_args" and "T2Q_args" are the quality data of times t and $t+1$, respectively. "XOR_args" is the XOR data. The quality data and XOR data are bit-expanded and encrypted, respectively. The public key is updated every time, for a set of t and $t+1$.

```
Lot_Num1
{ Pubkey_n:2830121771
  Pubkey_n_squared:8009589238688176441
  Pubkey_n_plusone:2830121772
  T1Q_args:
  [4980725921889483287 61531755845479325O5 5152481051748019804
   581307518391497185l 3053687218029093382 7519445935057616693
   5554622124560261958 7416830349963219832 3731218581147927956
   7737816729750121605 6407087674629651145 2616497229643427468
   7073255490218694482 3489053961054357288 1312997492291069014
   7289821191676242269 1214332198022297545 4025988039903818004
   6064746189589985122 4802322551839231456 7424715945851842271
   3220673806708617670 2103533827695848779 7260652711655389472
   4722437745875975257 6866162819685730117 1702410146952475749
   3071162096418209633 4684195174004811485 863137609772694266
   5462066504891676597 7655984581615439345 ]
  T2Q_args:
  [2447649126763497706 5735021179952371458 2086631069180094640
   5721113090521884487 599323575824742571 4996588965493540626
   6257710524633230928 3958355396103966338 7573512328406491778
   7034578379659091l7 1842181989505388935 2744728351232161022
   4128917455875014382 5395656243828366O 2120818422813844792
   2733856400927777620 2559371979199980996 3746243217245918378
   7072557803810737241 7232506223968543817 6909550095870789716
   5159912136778587406 5808041864759782390 1[3532122650097847S3
   3319164070715731022 1336692394470427843 5923883745587898103
   1400869709299149335 4918479723931233979 5146918150838047487
   3740148318216792464 2854361354933483043]
]
```

(**a**)

```
Lot_Num1
{ Pubkey_n:2830121771
  Pubkey_n_squared:8009589238688176441
  Pubkey_n_plusone:2830121772
  XOR_args:
  [5834801600703424l3 607114339157570618 5461098146576138368
   1676259776696891574 5230036970634472003 7916196753652125780
   4654056267859177446 4848538767933050945 1270393055511576187
   3737497856746955616 3487718159105781131 2338826278447765788
   1476089699837314077 2910208189690723267 2382146379745738126
   2116589399509535665 1895107401328832684 2520109880548933048
   6353506828654654944 909583095077380766 3151624486558981203
   7996395695254786788 7971087722132611181 7816078966235414548
   4700375503791476593 6619578153789915468 6455507538950446359
   1415177324329643893 5627751940736229135 3950287318182962S
   3143128945322885899 1924370384420209838]
]
```

(**b**)

Figure A1. Data structure. (**a**) Data structure of Q_β CC; (**b**) Data structure of XOR CC.

References

1. Satoshi, N. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 21 June 2022).
2. Gadekallu, T.R.; Pham, Q.V.; Nguyen, D.C.; Maddikunta, P.K.R.; Deepa, N.; Prabadevi, B.; Pathirana, P.N.; Zhao, J.; Hwang, W.J. Blockchain for edge of things: Applications, opportunities, and challenges. *IEEE Internet Things* **2021**, *9*, 964–988. [CrossRef]
3. Mills, J.; Hu, J.; Min, G. Multi-Task Federated Learning for Personalised Deep Neural Networks in Edge Computing. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *33*, 630–641. [CrossRef]
4. Yu, Z.; Hu, J.; Min, G.; Zhao, Z.; Miao, W.; Hossain, M.S. Mobility-aware proactive edge caching for connected vehicles using federated learning. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 5341–5351. [CrossRef]
5. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.
6. KPMG LLP. Blockchain and the Future of Finance: A Potential New World for CFOs—And How to Prepare. Available online: https://assets.kpmg/content/dam/kpmg/ca/pdf/2019/05/blockchain-and-the-future-of-finance.pdf (accessed on 21 June 2022).
7. Du, M.; Chen, Q.; Xiao, J.; Yang, H.; Ma, X. Supply Chain Finance Innovation Using Blockchain. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1045–1058. [CrossRef]
8. Alam, M.R.; Reaz, M.B.I.; Ali, M.A.M. A Review of Smart Homes—Past, Present, and Future. *IEEE Trans. Syst. Man Cybern. Part C* **2012**, *42*, 1190–1203. [CrossRef]
9. Batty, M.; Axhausen, K.W.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart Cities of the Future. *Eur. Phys. J. Spec. Top.* **2012**, *214*, 481–518. [CrossRef]
10. Sun, M.; Zhang, J. Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. *Comput. Commun.* **2020**, *149*, 332–342. [CrossRef]
11. Dagar, R.; Som, S.; Khatri, S.K. Smart Farming—IoT in Agriculture. In Proceedings of the International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 11–12 July 2018.
12. Saurabh, S.; Dey, K. Blockchain technology adoption, architecture, and sustainable agri-food supply chains. *J. Clean. Prod.* **2021**, *284*, 124731. [CrossRef]
13. Shahinzadeh, H.; Moradi, J.; Gharehpetian, G.B.; Nafisi, H.; Abedi, M. IoT Architecture for Smart Grids. In Proceedings of the International Conference on Protection and Automation of Power System (IPAPS), Tehran, Iran, 8–9 January 2019.
14. Menon, V.G.; Jacob, S.; Joseph, S.; Sehdev, P.; Khosravi, M.R.; Turjman, F.A. An iot-enabled intelligent automobile system for smart cities. *Internet Things* **2022**, *18*, 100213. [CrossRef]
15. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
16. Badhotiya, G.K.; Sharma, V.P.; Prakash, S.; Kalluri, V.; Singh, R. Investigation and assessment of blockchain technology adoption in the pharmaceutical supply chain. *Mater. Today Proc.* **2021**, *46*, 10776–10780. [CrossRef]
17. Zheng, J.; Dike, C.; Pancari, S.; Wang, Y.; Giakos, G.C.; Elmannai, W.; Wei, B. An In-Depth Review on Blockchain Simulators for IoT Environments. *Future Internet* **2022**, *14*, 182. [CrossRef]
18. Javed, A.R.; Hassan, M.A.; Shahzad, F.; Ahmed, W.; Singh, S.; Baker, T.; Gadekallu, T.R. Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey. *Sensors* **2022**, *22*, 4394. [CrossRef] [PubMed]
19. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy Challenges. *Internet Things* **2019**, *8*, 100107. [CrossRef]
20. Santhi, A.R.; Muthuswamy, P. Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics. *Logistics* **2022**, *6*, 6010015.
21. Akaba, T.I.; Norta, A.; Udokwu, C.; Draheim, D. A Framework for the Adoption of Blockchain-Based e-Procurement Systems in the Public Sector: A Case Study of Nigeria. In *Responsible Design, Implementation and Use of Information and Communication Technology*; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2020; Volume 12066, pp. 3–14. [CrossRef]
22. Guo, D.; Ling, S.; Li, H.; Ao, D.; Zhang, T.; Rong, Y.; Huang, G.Q. A framework for personalized production based on digital twin, blockchain and additive manufacturing in the context of Industry 4.0. In Proceedings of the 2020 IEEE 16th International Conference on Automation Science and Engineering (CASE), Hong Kong, China, 20–21 August 2020.
23. Chen, J.; Xu, S.; Liu, K.; Yao, S.; Luo, X.; Wu, H. Intelligent Transportation Logistics Optimal Warehouse Location Method Based on Internet of Things and Blockchain Technology. *Sensors* **2022**, *22*, 1544. [CrossRef]
24. Wu, L.; Lu, W.; Xue, F. Construction Inspection Information Management with Consortium Blockchain. In *Proceedings of the 25th International Symposium on Advancement of Construction Management and Real Estate*; Springer: Singapore, 2020; pp. 1397–1406. [CrossRef]
25. Bellavista, P.; Esposito, C.; Foschini, L.; Giannelli, C.; Mazzocca, N.; Montanari, R. Interoperable Blockchains for Highly-Integrated Supply Chains in Collaborative Manufacturing. *Sensors* **2021**, *21*, 4955. [CrossRef]
26. Tijan, E.; Aksentijevic, S.; Ivanic, K.; Jardas, M. Blockchain Technology Implementation in Logistics. *Sustainability* **2019**, *11*, 1185. [CrossRef]
27. Jæger, B.; Bach, T.; Pedersen, S.A. A Blockchain Application Supporting the Manufacturing Value Chain. In *Advances in Production Management Systems. Production Management for the Factory of the Future. IFIP Advances in Information and Communication Technology*; Springer: Cham, Switzerland, 2019; Volume 566, pp. 466–473. [CrossRef]

28. Leunga, S.C.H.; Tsanga, S.O.S.; Nga, W.L.; Wub, Y. A robust optimization model for multi-site production planning problem in an uncertain environment. *Eur. J. Oper. Res.* **2007**, *181*, 224–238. [CrossRef]
29. Tao, F.; Qi, Q.; Liu, A.; Kusiak, A. Data-driven smart manufacturing. *J. Manuf. Syst.* **2018**, *48*, 157–169. [CrossRef]
30. Johnson, J.S.; Friend, S.B.; Lee, H.S. Big Data Facilitation, Utilization, and Monetization: Exploring the 3Vs in a New Product Development Process. *J. Prod. Innov. Manag.* **2017**, *34*, 640–658. [CrossRef]
31. METI. Connected Industries Tokyo Initiative 2017. In Proceedings of the Connected Industries Conference, Tokyo, Japan, 4 October 2017.
32. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
33. The Federal Ministry for Economic Affairs and Climate Action; GAIA-X. Available online: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html (accessed on 13 June 2022).
34. IOTA. Available online: https://www.iota.org/ (accessed on 13 June 2022).
35. Yan, X.; Wu, Q.; Sun, Y. A Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8832341. [CrossRef]
36. Nakanishi, R.; Zhang, Y.; Sasabe, M.; Kasahara, S. IOTA-Based Access Control Framework for the Internet of Things. In Proceedings of the Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 27–30 September 2020.
37. Cuzzocrea, A.; Maio, V.D.; Fadda, E. Experimenting and Assessing a Distributed Privacy-Preserving OLAP over Big Data Framework: Principles, Practice, and Experiences. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020. [CrossRef]
38. Ronald, R.L.; Adi, S.; Leonard, A. A method for obtaining digital signatures and public key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
39. Gentry, C. A Fully Homomorphic Encryption Scheme. Ph.D. Thesis, Stanford University, Stanford, CA, USA, 2009.
40. Fen, B. Cryptanalysis of a provable secure additive and multiplicative privacy homomorphism. In Proceedings of the International Workshop on Coding and Cryptography (WCC), Versailles, France, 24–28 March 2003.
41. Wu, D.J.; Feng, T.; Naehrig, M.; Lauter, K. Privately evaluating decision trees and random forests. *Proceeding Priv. Enhancing Technol. (PoPETs)* **2016**, *2016*, 335–355. [CrossRef]
42. Nasu, H.; Kodera, Y.; Nogami, Y. Secure Comparison Protocol for Promoting Business to Business Collaboration on the Blockchain. In Proceedings of the International Conference on Consumer Electronics-Taiwan (ICCE-TW), Penghu, Taiwan, 15–17 September 2021.
43. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Advances in Cryptology-EUROCRYPT '99*; Springer: Berlin/Heidelberg, Germany, 1999.