World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:16, No:3, 2022

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

Hiroaki Nasu, Ryota Miyamoto, Yuta Kodera, Yasuyuki Nogami

***Abstract*—**To promote Industry 4.0 and Society 5.0 and so on, it is important to connect and share data so that every member can trust it. Blockchain (BC) technology is currently attracting attention as the most advanced tool and has been used in the financial field and so on. However, the data collaboration using BC has not progressed sufficiently among companies on the supply chain of the manufacturing industry that handle sensitive data such as product quality, manufacturing conditions, etc. There are two main reasons why data utilization is not sufficiently advanced in the industrial supply chain. The first reason is that manufacturing information is top secret and a source for companies to generate profits. It is difficult to disclose data even between companies with transactions in the supply chain. Blockchain mechanism such as Bitcoin using Public Key Infrastructure (PKI) requires plaintext to be shared between companies in order to verify the identity of the company that sent the data. Another reason is that the merits (scenarios) of collaboration data between companies are not specifically specified in the industrial supply chain. For these problems, this paper proposes a Business to Business (B2B) collaboration system using homomorphic encryption and BC technique. Using the proposed system, each company on the supply chain can exchange confidential information on encrypted data and utilize the data for their own business. In addition, this paper considers a scenario focusing on quality data, which was difficult to collaborate because it is top-secret. In this scenario, we show an implementation scheme and a benefit of concrete data collaboration by proposing a comparison protocol that can grasp the change in quality while hiding the numerical value of quality data.

***Keywords*—**Business to business data collaboration, industrial supply chain, blockchain, homomorphic encryption.

I. Introduction

IN, order to promote Society 5.0, Industrial Internet, Industry 4.0, etc., it is important to connect and share data so that all members can trust. In the manufacturing industry of business to business (B2B), there is a growing demand for high-quality product development and a plan optimization by sharing manufacturing data among companies on the supply chain (e.g. product quality data, equipment data and order shipping data) [1]. Furthermore, it is important that not only existing companies on the supply chain, but also non-participating companies can freely enter the business and supply chain, exchange data, and trade. In such an ecosystem, it is necessary to have a mechanism that guarantees the identity of the company without having a central certificate authority. In order to build such an ecosystem, the blockchain technology is being utilized in the mainly financial field.

II. Problem of Blockchain Utilization in B2B Collaboration on the Supply Chain

In the manufacturing industry of B2B, it is difficult for each company to disclose confidential information regarding its manufacturing know-how, even if it is a company that has transactions on the supply chain. In the blockchain mechanism such as Bitcoin using PKI, in order to confirm the identity of the company that has sent the data, the plaintext must be shared between the companies (Fig. 1). Therefore, the blockchain is not widely used in collaboration among companies on the industrial supply chain [2].

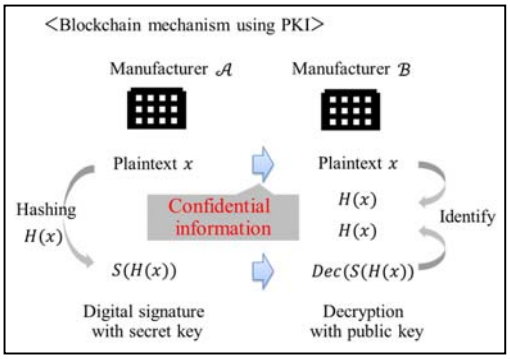

Fig. 1 Issue of blockchain utilization in B2B collaboration

III. B2B Collaboration Approach Combining Blockchain and Homomorphic Encryption (HE)

For the issue, this paper proposes a secure B2B collaboration system on the supply chain that enables open data transfer and business coordination by combining blockchain technology and homomorphic encryption. Homomorphic encryption scheme enables us the computation of addition or multiplication on encrypted data. In addition, C. Gentry in 2009 proposed a concrete construction of a fully homomorphic encryption scheme that allows both multiplication and addition [3]. In the secure collaboration system, using homomorphic encryption Enc (*) and blockchain technique, each company on the supply chain can exchange confidential information on encrypted data and utilize it for their own business (Fig. 2).

Hiroaki Nasu is with the Graduate School of Natural Science and Technology, Okayama University, Okayama-shi, Japan (e-mail: ptk36s3v@s.okayama-u.ac.jp).

Ryota Miyamoto, Yuta Kodera and Yasuyuki Nogami are with the Okayama University, Japan (e-mail: pw8i4gr1@s.okayama-u.ac.jp, yuta_kodera@okayama-u.ac.jp, yasuyuki.nogami@okayama-u.ac.jp).

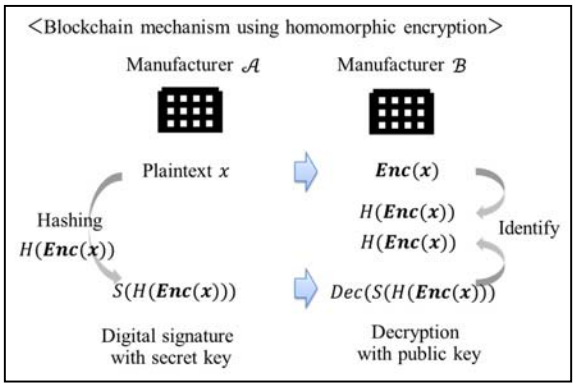

Fig. 2 The secure B2B collaboration approach

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 grasping what quality $Q_{\mathcal{B}}$ can be produced when the product $P_{\mathcal{A}}$ is put into which equipment of $\mathcal{B}$. Although $\mathcal{B}$ wants a stable supply of high-quality materials from $\mathcal{A}$, it does not want to disclose the own manufacturing information because it is a confidential know-how. For this scenario, in this research, $\mathcal{B}$ sends $Enc(P_{\mathcal{B}}, Q_{\mathcal{B}}, E_{\mathcal{B}})$ to $\mathcal{A}$ using homomorphic encryption. Therefore, $\mathcal{A}$ can calculate the 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 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 and this research can be expected.

In the above scenario, this paper focuses on quality data as shown in Fig. 3. $\mathcal{A}$ 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 the own manufacturing factor and lead to the optimum production. Therefore, in order to realize the proposed scenario, it is important to have a comparison protocol for the values of t and $t+1$ on encrypted. In the protocol, a function to put quality data into the blockchain and a function to get from the blockchain are also important to implement the proposed scenario.

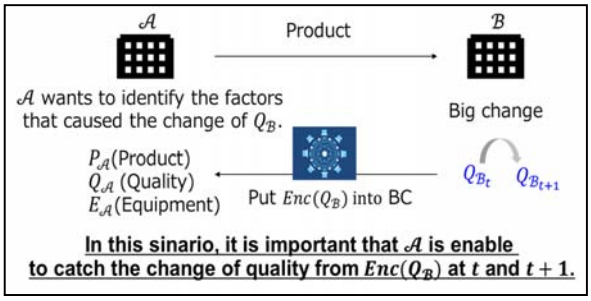

Fig. 3 Proposed scenario focusing on quality data

The final system of the B2B collaboration is shown in Fig. 4. In this final system, manufacturing companies can chain data without disclosing their quality data, while also guaranteeing their identities by using blockchain. Even if the encrypted quality data is tampered by an attacker, the hash value of the encrypted quality data and the value after decrypting the signature will not match. Therefore, tampering can be detected immediately. In addition, traceability on the supply chain will be possible by including the lot number of each company's products in the encryption. In such secure data linkage, $\mathcal{A}$ will be able to grasp changes in quality data of downstream companies in a timely manner and to utilize them in their own manufacturing.

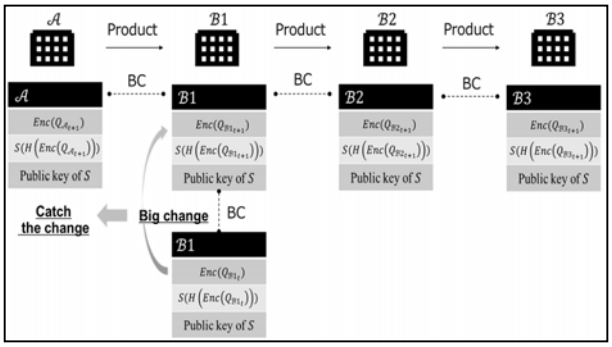

Fig. 4 The final system of the B2B collaboration

IV. Conventional Comparison Protocol Using HE and Issues for B2B Collaboration

In 2016, Wu et al. proposed a comparison protocol based on Paillier cryptography, which is an additive homomorphic encryption [4]. In the protocol, the client and server have 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 $i \in [k-1]$ satisfy the following formula (1). $x > y$ if and only if there exists some index $i \in [k-1]$ satisfy the following formula (2).

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

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

Here we describe 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 the formula (1) or (2) by substituting $Enc(x_i)$ and $Enc(y_i)$ and by using plaintext y_i for XOR. The client receives the calculation result, and then decrypts it with the secret key, and checks for zero. Therefore, the client can determine $x > y$ 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, $\mathcal{A}$ can not calculate XOR of the above formula and this conventional protocol is difficult to apply to B2B collaboration on the supply chain. In addition, in order to realize the proposed scenario in the actual business, it is necessary to consider a system architecture including business viewpoints and a comparison protocol according to the architecture.

V. Proposal B2B Collaboration System on the Supply Chain

In [6], we proposed a secure comparison protocol for B2B collaboration on the supply chain at ICCE-TW2021. In this paper, we show the concrete system architecture to implement the proposed scenario for the actual business. We improve the comparison protocol [6] to fit the system architecture of the B2B collaboration system.

A. System Architecture of the B2B Collaboration

This paper shows the system architecture to implement the proposed scenario in Fig. 5. In a real business, it is necessary to have a servicer that provides value by exchanging data and guarantees 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 Plat Form business. Therefore, the proposed system has a servicer $\mathcal{S}$ 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 Orderer. Each peer has a state database that records the state of data and a chaincode that holds the history of data transfer as a distributed ledger of the blockchain.

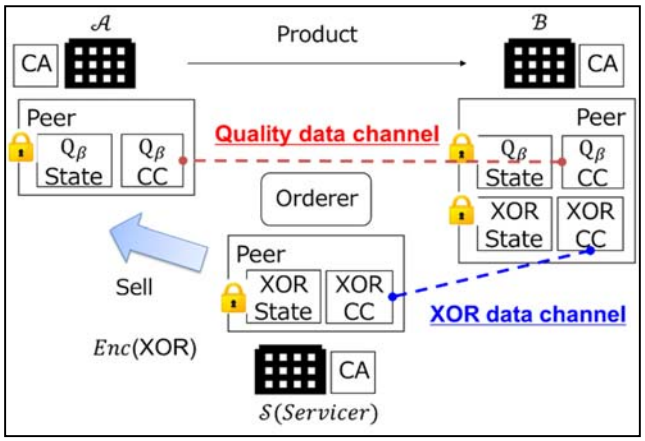

Fig. 5 Proposed B2B collaboration system

As shown in Fig. 5, this paper proposes a system architecture having a multi-channel that separates the chaincode for putting 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 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 $\mathcal{B}$ is essential for the calculation of (1) and (2) and must not be held by $\mathcal{A}$, so it is important key-data from both technical and business perspectives. Therefore, in the proposed system architecture, $\mathcal{B}$ calculates $x \oplus y$ and puts $Enc(x \oplus y)$ into XOR chaincode (XOR CC). $\mathcal{S}$ can get $Enc(x \oplus y)$ from XOR CC and sell $Enc(x \oplus y)$ to $\mathcal{A}$ as a servicer. The reason why 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 $\mathcal{B}$ on the supply chain, can grasp the change in quality.

B. Data Structure of Each Channel

Figs. 6 and 7 show the json data structure of Q_β CC, and XOR CC, respectively. "Pubkey_n" is public key of 32 bit. "T1Q_args" and "T2Q_args" are quality data of time t and $t+1$. "XOR_args" is XOR data. Quality data and XOR data are bit-expanded and encrypted. The public key is updated every time t and $t+1$ set.

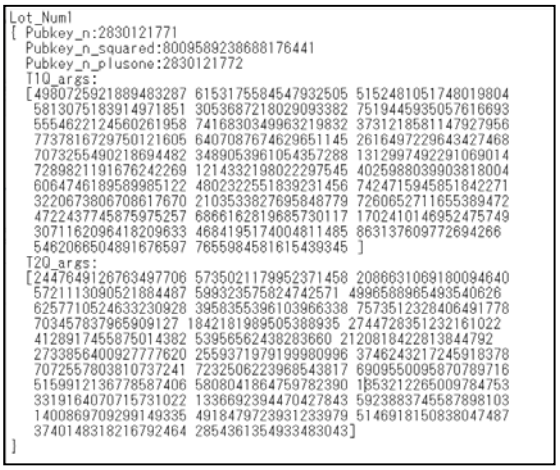

Fig. 6 Data structure of Q_β CC

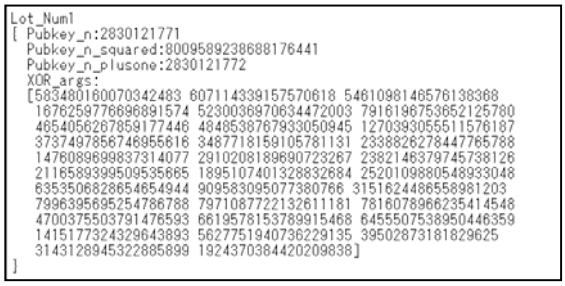

Fig. 7 Data structure of XOR CC

C. Prototype Implementation

A prototype of the proposed system is constructed as shown in Fig. 8. In this prototype, a company is set up as one organization in a docker container on the AWS EC2. A blockchain network is built by Hyperledger Fabric utilizing Amazon Managed Blockchain (AMB) service. BaaS (Blockchain as a Service) of full managed services are released from IBM and Oracle services too. In this prototype, AMB is adopted. The reason is that it is easy to build in the minimum configuration and to start small. In addition, Hyperledger Fabric is adopted to build a private blockchain for companies on the supply chain. In order to efficiently calculate multi-length

arithmetic, encryption, decryption and calculation of the data are programmed by C++. APIs for putting and getting data from the blockchain are developed by Golang. In the prototypes, C ++ programs pre calculate encrypted data and so on. Those data are embedded in the arguments of the above data structure with CA certificates, and "Invoke" of Golang programs are performed.

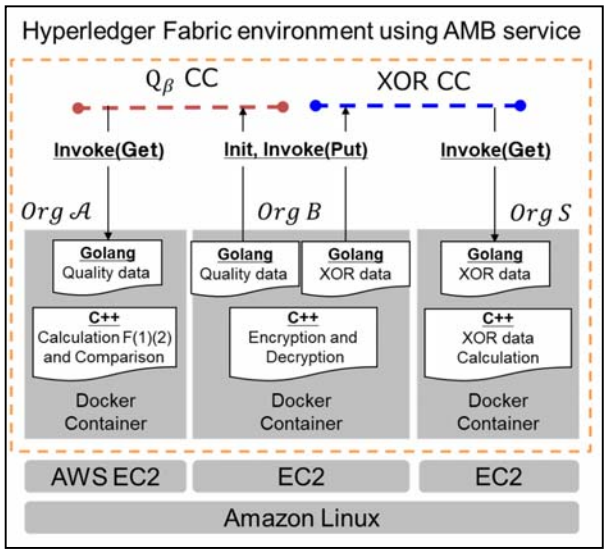

Fig. 8 B2B collaboration system prototype

VI. Implementation of Comparison Protocol to Realize B2B Collaboration System

This paper proposes an improved secure comparison protocol for implementation in the B2B collaboration system. We use a variant of Wu's protocol 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 [5]. In the Paillier cryptography, message $m \in \mathbb{Z}_n$ is encrypted with the following formula as $n = p \cdot q$, $g = 1 + n \bmod n^2$. Then, p and q are prime numbers about 3000 bits, and r is random number as $0 < r < n \in \mathbb{Z}_{n^2}^*$ and $\gcd(r, n) = 1$. Public key is (n, g). Secret key is (p, q).

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

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

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

Therefore,

$$m = \frac{L(C^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n \tag{4}$$

A. Cryptographic Protocol of $\mathcal{B}$

First, $\mathcal{B}$ binary-expands my quality data X and Y. And $\mathcal{B}$ encrypts x_i bit of X and y_i bit of Y and $x_i \oplus y_i$. Puts $Enc(x_i)$ and $Enc(y_i)$ and $Enc(x_i \oplus y_i)$ and public key into the blockchain as shown in Fig. 5.

TABLE I
Encryption Protocol of $\mathcal{B}$

Step	Processing
1	$\mathcal{B}$ binary-expands X and Y, encrypts x_i and y_i (i = 0~k-1 bits) with the public key.
2	$\mathcal{B}$ puts $Enc(x_i)$ and $Enc(y_i)$ and public key into quality data chaincode Q_β CC as seen in Fig. 5.
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 public key into XOR data chaincode XOR CC as seen in Fig. 5.

B. Calculation Protocol of S

S gets and saves $Enc(x_i \oplus y_i)$ and public key from XOR CC as seen in Fig. 5. 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 II
Calculation Protocol of S

Step	Processing
1	S gets and saves $Enc(x_i \oplus y_i)$ and public key from XOR data chaincode XOR CC as seen in Fig. 5.
2	S receives a XOR data request and public key from $\mathcal{A}$.
3	S identifies $Enc(x_i \oplus y_i)$ that has the same public key sent by $\mathcal{A}$ in step2.
4	If there is $Enc(x_i \oplus y_i)$, S sends the $Enc(x_i \oplus y_i)$ to $\mathcal{A}$.

C. Calculation Protocol of $\mathcal{A}$

$\mathcal{A}$ gets $Enc(x_i)$ and $Enc(y_i)$ and public key from Q_β CC as seen in Fig. 5. Also $\mathcal{A}$ gets $Enc(x_i \oplus y_i)$ from S by sending public key. $\mathcal{A}$ calculates those quality data using (1) and (2) while keeping them encrypted.

TABLE III
Calculation Protocol of $\mathcal{A}$

Step	Processing
1	$\mathcal{A}$ gets $Enc(x_i)$ and $Enc(y_i)$ and public key from quality data chaincode Q_β CC as seen in Fig. 5.
2	$\mathcal{A}$ sends public key to S and receives $Enc(x_i \oplus y_i)$ from S.
3	From the most significant bit, $\mathcal{A}$ calculates $Enc(z_i) = Enc(x_i - y_i \pm 1 + 3\sum_{j<i}(x_j \oplus y_j))$.
4	$\mathcal{A}$ sends $Enc(z_i)$ to $\mathcal{B}$.

In the proposed protocol of step3, it is necessary to calculate $Enc(-y_i)$ from $Enc(y_i)$. This proposed protocol uses the following property formula (5) of the Paillier cryptography to calculate $Enc(-y_i)$.

$$C^{n-1} = (g^m . r^n)^{n-1} mod n^2$$
$$= (1\text{-}mn) . r^{n(n-1)} mod n^2 = g^{-m} . r^{n(n-1)} mod n^2 \tag{5}$$

D. Decryption Protocol of $\mathcal{B}$

Using secret key and using (4), $\mathcal{B}$ decrypts $Enc(z_i)$ and searches for the bit where $z_i = 0$.

TABLE IV
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 secret key.
3	if there is $z_i = 0$, $\mathcal{B}$ sends i to $\mathcal{A}$.

E. 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 (1), then $X < Y$ can be determined. If $\mathcal{A}$ receives i while using (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 of X and Y themselves, that is, $\mathcal{A}$ can confirm the change of quality data in the time series.

TABLE V
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 (1), then $X < Y$ can be determined. If $\mathcal{A}$ receives i while using (2), then $X > Y$ can be determined.
3	$\mathcal{A}$ checks the difference between the numbers at time t and $t + 1$ by calculating 2^i.

VII. SAFETY EVALUATION OF THE PROPOSED SYSTEM

In this scenario, we do not consider the case where $\mathcal{B}$ maliciously puts incorrect quality data $Enc(x_i)$ and $Enc(y_i)$ to Q_β CC in the Step 2 of Table I. Putting incorrect quality data by $\mathcal{B}$ means disrupting the supply chain for their own material procurement. Such cases are nonsense from a business perspective and are not worth considering.

In the Paillier cryptography, since $\mathcal{A}$ does not know (p, q) and g^m is masked by $r^{p \cdot q}$ in the formula (3), it is difficult to solve the discrete logarithm problem in the exponential part of (3). The message m cannot be specified [5].

In the proposed comparison protocol of the B2B collaboration system, since ciphertexts are encrypted using random number r in the formulation (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 from Figs. 6 and 7.

In the B2B collaboration system, there is a risk that company $\mathcal{C}$ participating in the quality channel will impersonate on behalf of $\mathcal{A}$. $\mathcal{C}$ can know 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 supply chain 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 company. Therefore, it is unlikely that spoofing by a company like $\mathcal{C}$ will occur in the proposal system. Even if the encrypted data is leaked to a company that does not participate in blockchain channel, it will not be tampered with unless the public key is leaked.

VIII. CONCLUSION

This paper proposed a B2B collaboration system using blockchain for sharing even sensitive data between companies on the supply chain by keeping the data encrypted. We also proposed a specific utilization scenario in business focusing on quality data which is the most sensitive data in manufacturing. In this scenario, a company can grasp the change in quality data of the business partner while keeping the data encrypted and feed the change back to own manufacturing. This paper proposed a secure comparison protocol for grasping quality changes. Furthermore, in this paper, in order to implement this scenario, we designed a system architecture and developed a prototype of the B2B collaboration system.

Using the proposed system, it has become possible to utilize confidential information such as quality data among companies on the supply chain for their own business without disclosing the data.

ACKNOWLEDGMENT

This work was partially supported by Research Support Program toward Society 5.0 provided by Cypher in Okayama University, Japan.

REFERENCES

[1] METI (Ministry of Economy, Trade and Industry), “Connected Industries Tokyo Initiative,” Connected Industries Conference, 2017. https://www.meti.go.jp/english/press/2017/pdf/1002_004b.pdf
[2] F. Casino, T. K. Dasaklis, C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” Telematics and Informatics, vol. 36, pp. 55-81, 2019.
[3] C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.
[4] D. J. Wu, T. Feng, M. Naehrig, and K. Lauter. “Privately evaluating decision trees and random forests,” In Proceeding on Privacy Enhancing Technologies, vol. 2016, no. 4, pp. 1–21, 2016.
[5] P. Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” EUROCRYPT, pp. 223-238, 1999.
[6] H. Nasu, Y. Kodera, and Y. Nogami, "Secure Comparison Protocol for Promoting Business to Business Collaboration on the Blockchain," Proceedings of the International Conference on Consumer Electronics-Taiwan (ICCE-TW), Online conference, TWN, Sep 2021.