Peer-to-Peer Networking and Applications (2020) 13:671–683
https://doi.org/10.1007/s12083-019-00730-6

Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment

YongJoo Lee[1] · Keon Myung Lee[2] · Sang Ho Lee[2]

Received: 29 October 2018 / Accepted: 4 February 2019 / Published online: 11 May 2019

Abstract
Blockchain enables users to be autonomous without the need of trust by using a digital ledger of decentralized consensus. Blockchain-based IoT allows service providers to transfer the security and maintenance responsibility to self-maintaining customers. Adopting peer-to-peer (P2P) networking and computing for more than billions of transactions can reduce the costs arising from the installation and maintenance of centralized systems. Small manufacturers providing industrial IoT (IIoT) services can participate more actively in blockchain-based IIoT applications with three-dimensional printing and digital manufacturing technologies, but the measure to maintain privacy on a blockchain is not robust. Here, we propose a P2P networking-based custom manufacturing service, which is an order-driven trading service between a manufacturer and a customer in the blockchain-based IIoT architecture. The proposed system consists of reputation management and service architecture. We propose a new reputation assessment method customized to increase the reliability and accuracy of industrial manufacturing systems. We also propose a manufacturer rating classification to guide the customers' decision making in a reliable manner and a malicious evaluator identification to exclude feedbacks from malicious evaluators. The proposed service architecture is composed of trustless P2P protocols designed for preserving privacy and providing non-repudiation. We used a cryptographic algorithm for ensuring transaction privacy and the digital signing of blockchain for non-repudiation. We also analyzed the proposed service architecture and the possible attack scenarios to verify the security requirements. We verified that the reputation management system was influenced by each feedback dynamically and guided the customer's present decision making with reliable and classified manners, by simulating reputation classification and malicious evaluator identification. Further, we have summarized the originality and the characteristics of the proposed approach by comparing closely related studies and concluded with a future research guide.

Keywords Peer to peer networking · Blockchain · Reputation · Custom manufacturing · Trustless

1 Introduction

Industry 4.0 is focused on creating smart products and processes and managing complexity well. The implementation of Industry 4.0 can be used to manufacture goods more efficiently [1]. As industrial IoT (IIoT) is becoming more popular in the development of Industry 4.0, the scale of industrial networks is gradually expanding. The industrial solution built on a centralized network incurs high costs to construct and maintain huge servers. The high cost can be dramatically reduced by adopting P2P technologies that can handle more than billions of transactions without any centralized center or storage from the manufacturer's view, as well as enable the customers to control security through transparency [2]. Blockchain is fundamentally a distributed ledger of transactions that are generated by the participants. The ledgers are composed of blocks that are cryptographically linked with each other [3]. It is extremely difficult to change or remove the blocks of data stored on the ledger of blockchain. A blockchain-based IIoT allows manufacturers to transfer the maintenance ownership to self-maintaining customers, making the system future-proof [4]. Three-dimensional (3D) printing and digital manufacturing technologies on blockchain enable manufacturers and customers to participate in a new type of decentralized manufacturing service. If customers and manufacturers are

This article is part of the Topical Collection: *Special Issue on P2P Computing for Intelligence of Things*
Guest Editors: Sunmoon Jo, Jieun Lee, Jungsoo Han, and Supratip Ghose

✉ Keon Myung Lee
kmlee@cbnu.ac.kr

YongJoo Lee
xyleekor@gmail.com

Sang Ho Lee
shlee@cbnu.ac.kr

[1] Global IT Research Institute, KNUT, Daehak-ro 61, Jungpyung 27909, Chungbuk, South Korea

[2] Department of Computer Science, Chungbuk National University, chungdaero1, Seowon-gu, Cheongju 28644, Chungbuk, South Korea

placed in complicated procedures with low security, technology development can be slowly progressed and depressed by low service satisfaction.

The rest of this paper is organized as follows. Section 2 introduces a few closely related studies for reputation management and blockchain-based protocols. Section 3 provides a detailed description of the proposed manufacturing system. Detailed analysis and evaluation are presented in Section 4. Comparison and discussion are presented in Section 5. Section 6 provides the conclusion and the directions for future work.

2 Related work

2.1 Network architecture evolution to P2P networking

Blockchain is a technology to build distributed ledgers in a decentralized network. The ledgers are duplicated to every node by P2P technologies, and transactions stored in ledgers are autonomously controlled by the owner of the transactions rather than being centrally controlled. Each block contains a time value stamped by an internal time server. Former blocks are always generated earlier than the latter blocks, and every block carries a transaction [5]. The blockchain technology has the following strengths [6]:

- Decentralization: Blockchain does not rely on a specific system; instead, every node can equally participate in the verification and maintenance of the transactions.
- Trustless: It does not need trust, trusting the blockchain software instead.
- Collective maintenance: Blocks in a blockchain are maintained by all the nodes accessible to anyone.
- Anonymity: Users do not need a private identity to exchange data; instead, an unidentifiable address is adapted.
- Safe and reliable: All the activities of every node in the system are monitored by the entire network.
- Smart contract: It can reduce the contract signing, enforcement, and regulatory costs.

Thus, main advantages of blockchain are to provide essential parts of the solution that can deviate from centralized management with a trusted broker or centralized storage. A secure hash algorithm is used to provide transaction integrity after distributed consensus algorithm execution, and a digital signature algorithm is used to verity transparency of the transactions in a trustless network [2]. The trusted third party is not required by utilizing these fundamental capabilities of blockchain framework based on trustless P2P networking as shown in Fig. 1 [7, 8].

2.2 Trust and traditional reputation management

Trust is a complicated concept and a subjective probability by an individual, but reputation is generally said or believed about persons or things. The difference between them is that A can trust B because of B's good reputation, but A can trust B despite B's bad reputation. Reputation management involves several fields, including economics, sociology, marketing, and computer science. Reputation management research has been performed for both theoretical fields and practical applications in computer science [9]. In particular, reputation studies have been actively applied to P2P networks, web search engines, e-businesses, multi-agent systems, etc. We briefly introduce a few reputation management frameworks closely related to our research [10, 11]. Figure 2 shows a general reputation framework where three properties are required.

The general reputation system collects the ratings from the direct experience of the participants. Nevertheless, A and B have never met in the past; their reputations are stored and adapted and guide their present decision. We basically follow the properties to design the proposed reputation management.

2.3 RATEWeb: Reputation assessment for web service

Malik et al. [12] proposed a reputation assessment framework for web services to facilitate trust-based selection. The reputation evaluation metrics include rater credibility, majority rating, past rating history, and temporal sensitivity and operate in the web service model. They viewed this web service reputation as a reflection of the web service quality. They considered participants such as web service applications, service providers, service registries, and service consumers who participated in various services. They accepted the Euclidean distance between the majority rating (M) and the reported rating (V) for the rater credibility (Cr) of malicious users. They used the reputation fader (fd) for the temporal sensitivity to assign more weight to the recent observations by using the time-stamped submission for calculating the reputation ratings. Although it has a completely different environment, this framework is basically based on the feedback for the reputation management system. A feedback from a rater is inserted into the framework and is expressed as the assessed reputation through internal calculations, as shown in Fig. 3. We need to customize the reputation management theories for an industrial manufacturing service.

2.4 Fair payment with reputation by trustless P2P networking

Zhao et al. [13] proposed blockchain-based secure pub-sub payment with a reputation system. They provided anonymity by using a blockchain where nobody can link the pseudonym to a real identity, such as the ID-card number and the telephone number. They accepted the publish and subscribe

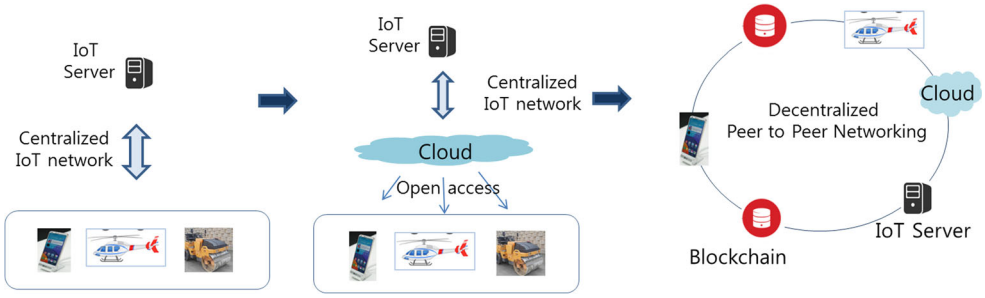


Fig. 1 Architectural evolution to P2P networking

protocols based on blockchain to exchange issues and interests without a trusted third party. A traditional publish-and-subscribe system needs a broker as a trusted third party, who matches the message of the publisher and the subscription of the subscriber and notifies the result to the subscriber. Wang [14] proposed an SDN-based publish-and-subscribe platform for IoT services, but it is based on a centralized controlling system that enables the integration of fundamentally heterogeneous devices. The blockchain-based publish-and-subscribe system does not need a broker with trustless P2P networking. Figure 4 shows a Bitcoin-based payment system by using the P2P networking.

This research also includes a reputation system that integrates the implicit rating and the explicit rating by distinguishing between the positive and the negative activities. This reputation algorithm was originally proposed for social networks by Bok et al. [15]. They set the fixed value θ to determine believable publishers. If the reputation of a user is higher than θ, then the user is highly trusted. This mechanism cannot control the fixed criteria flexibly nor apply previous feedback to the present one in real time. Therefore, we need to design a reputation approach that controls the criteria for identifying trusted users in real time.

3 Custom manufacturing service

Here we propose a custom manufacturing service as a P2P networking-based application that provides requirements for privacy, fairness, and anonymity. The proposed system consists of a reputation management and a manufacturing service architecture. The proposed reputation management is customized for the order-driven manufacturing service and includes the reputation assessment, the manufacturer classification and the malicious evaluator identification flexibly reflecting previous ratings. The proposed manufacturing service architecture is composed of P2P networking-based protocols: the setup, publish, subscribe, accept, confirm, and evaluate (SPSACE) protocol.

3.1 Reputation management

The purpose of the reputation management in this study is to guide a customer's present decision making by providing the reliable reputations of the manufacturers participating in a manufacturing service. The proposed reputation management considers the requirements of a general reputation system and an industrial manufacturing service. Considerable reputation research has been performed on social networks, internet open markets, web services, etc. [16]. The main differences between the proposed research and reputation-related studies can be summarized in two main ways: The first is that in the proposed research, not only feedbacks but also the credibility and the capability of manufacturing systems in the real world are important. The second is that the reputation of a specific manufacturer can be included in the lowest rating even though the reputation has never been in that class. Single production on demand can cause this situation because the criteria of quality are decided by the ordering customer. We consider the credit rating (*CR*) to take into account the first issue and propose new malicious evaluator management to consider the second issue. A detailed description is provided in the following sections.

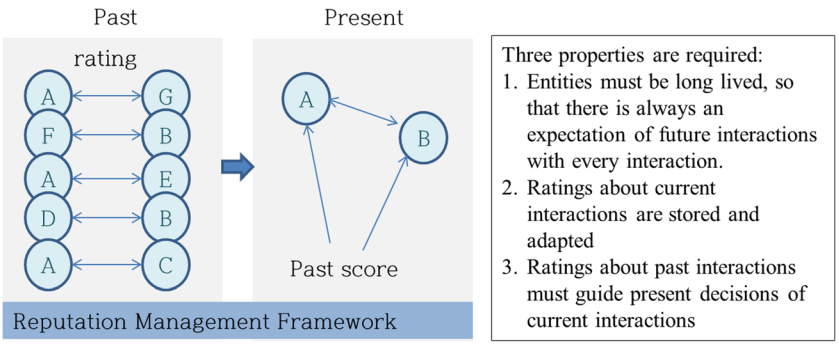


Fig. 2 General framework for reputation system

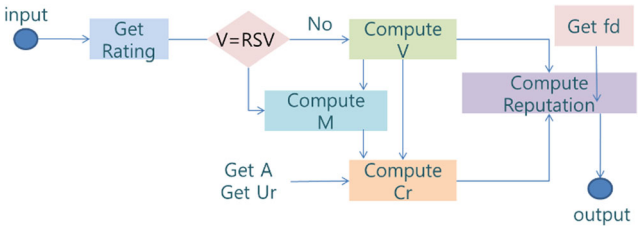


Fig. 3 Reputation evaluation metrics by Malik et al. [12]

3.1.1 Definition

A manufacturer is the user who participates in a service and produces an item as ordered by a customer who also participates in the service as the counterparty. Each manufacturer has an integrated reputation rating, and a customer can evaluate a manufacturer for the service by providing feedback. The manufacturers can begin to produce items after getting an order from a customer. Hence, we need to consider the manufacturers' credibility and the capability of the manufacturing facilities in the real world. The proposed reputation management is designed in accordance with the reliability in the real world and the cyber world. We defined a variable credit rating (*CR*) to consider the credibility in the real world and the credit evaluation (*CE*) as the feedback provided by a customer for a manufacturing service.

We used two parameters: weight rating (*wr*) and weight evaluation (*we*); the sum of *wr* and *we* had to be 1. We proposed assigning a weight to *CE* in case the manufacturing facility or the credibility of the product domain was not important or was not easy to calculate. Then, the rate of *CE* was increased as compared to *CR*. Therefore, we used the weight parameters for the integration. Each manufacturer had a reputation rating (*R*), which included *CE* and *CR*, as shown in Eq. (1):

$$\mathrm{R} = (\mathrm{wr}\cdot\mathrm{CR}) + (\mathrm{we}\cdot\mathrm{CE}) \tag{1}$$

CR includes the credibility and the production capacity of the manufacturing facilities in the real world. It can be registered by service vendors through the submission of certificated documents and can be updated periodically as necessary. The detailed description of *CR* depends on the situation of the specific manufacturing field and the service type. It is not the role of a trusted third party but an optional attribute to increase service reliability. Every manufacturer who joins the service has *R* combined from *CR* and *CE*. The advantage of considering *CR* is not just assessing the credibility of the real manufacturing facilities but also increasing the trust of reputation management system in that the manufacturers cannot change their identifiers (IDs) once they are registered. If they can easily change their IDs, the stored and integrated reputation ratings for old IDs will point to the lost owners and the reliability of the system will decrease. Past evaluations from all customers except malicious evaluators should be integrated to derive the total *CE* of a manufacturer.

3.1.2 Domain management

Products that can be made from a manufacturing service are not just small items from 3D printing but also products covering various domains including intellectual property rights for products without real shapes, goods invented by a customer, electronics with unique designs, and complex object produced by collaboration. Diversity is expected to increase with a combination with artificial intelligence (AI) by the development of the related technologies. Therefore, we need to divide the product field into specific domains to manage it in detail. This can lead to an increase in the credibility and the accuracy of the reputation system. Different strategies with domain management can be adapted to evaluation management. Therefore, we propose a domain evaluation vector (*DEV*) to apply different rating factors according to the domain that the requested product is included in. Reputation management is integrated from all the domains per manufacturer and not restricted by the manufacturer's domain.

3.1.3 Reputation assessment

R represents reputation, and R_{mj} denotes the reputation of a service manufacturer, m_j. *M* is the set of manufacturers, m_j; *C* is the set of customers c_x who use the manufacturing services. c_x can evaluate m_j by providing feedback, that is, CE_x^j. The domain evaluation vector (*DEV*) is defined to give different rating factors per domain. It can be used to add attributes to specific rating elements of a domain. (m_j) is given to each

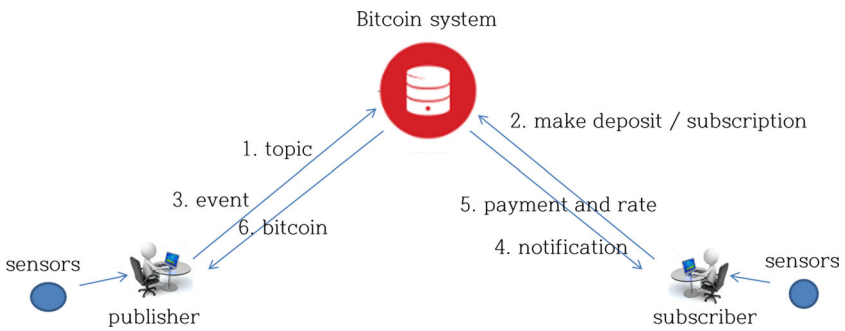


Fig. 4 Fair payment based on P2P networking by Zhao et al. [13]

attribute, h. L is the number of evaluation elements, and the evaluation of m_j by c_x is expressed in Eq. (2):

$$CE_x^j = \frac{1}{L}\sum_{h=1}^{L}\left(\left(m_j\right)^x \ DEV\right)h \tag{2}$$

The final reputation of a manufacturer is calculated from all the evaluations. CR is represented as P, which has elements $P = [p1 \ldots pp]$. P^j is the average of the elements for m_j. Nc is the number of customers who participate in an evaluation for a manufacturer, and CR^j are the credit rating (CR) of m_j. Here, we propose a method to exclude a malicious evaluator, $M(x)$, whose value is either 0 or 1. If $M(x)$ is 0, c_x is malicious or not honest, and the evaluation is excluded from reputation management.

$$R_{mj} = \left\{CR^j \cdot wr\right\} + \left\{\frac{\sum_{x=1}^{Nc}\left(CE_x^j \, M(x)\right)}{\sum_{x=1}^{Nc} M(x)} \cdot we\right\} \tag{3}$$
$$where \ M(x) \in \{0, 1\}$$

3.1.4 Reputation classification

We divided the total manufacturer into four classes and proposed a suitable method for each class in order to increase the reliability of the service by reflecting the output of the reputation system. Every manufacturer should be included in one of the four classes. Manufacturer classification is designed to recommend highly reliable manufacturers to customers and protect from damage caused by low-rated manufacturers during a service. Every evaluation is reflected in the total classification system. We propose a method by using the average (R_a) and the standard deviation (R_{sd}) calculated using the reputation ratings of all the manufacturers. N_t is the number of participating manufacturers in Eqs. (4 and 5).

$$R_a = \frac{1}{N_t} \ \sum_{j=1}^{N_t} R_{mj} \tag{4}$$

$$R_{sd} = \sqrt{\frac{1}{N_t}\sum_{j=1}^{N_t}\left(R_{mj} - \overline{R_{mj}}\right)^2} \tag{5}$$

All the participating manufacturers are divided into four classes by using Eq. (6) as shown in Table 1.

$$\alpha \leftarrow \left(R_a + R_{sd}\right), \quad \beta \leftarrow \left(R_a - R_{sd}\right) \tag{6}$$

The manufacturers in the R class cannot upgrade their rating by the feedback of services because of the restriction on their participation. A manufacturer is expected to be classified into the R class mainly because of low CR and not just from continuous low CE. The R class is defined to give more opportunities to the highly trusted manufacturers in the real world. Hence, the manufacturers need to improve their CR first.

3.1.5 Malicious evaluator identification

The proposed malicious evaluator management focuses on identifying incorrect or false evaluations based on several malicious motives of the evaluators, which is known as the foremost drawback of a feedback-only based system [12]. A malicious evaluator is defined as a customer who does not honestly or intentionally evaluate some manufacturers. Inaccurate reputation management influenced by malicious evaluators can cause a decrease in the reliability of the reputation system; therefore, the method of excluding malicious evaluators has an effect on the quality of the service. A centralized reputation system is used by a few existing online systems such as eBay, Amazon, Yahoo!, and Auctions. These systems rely on numerical feedback from users as a simple aggregation of received ratings with a supplement measure of textual feedback. In fact, eBay as the most highly used online reputation system asks sellers and buyers to rate each other on a three-point scale (−1, 0, and 1) and computes the reputation as a summation of all the negative and the positive ratings [10]. Amazon uses an average of all the ratings to compute the users' reputations. The new approach to overcome these drawbacks is the majority opinion, which uses a clustering technique to define the majority opinion by grouping similar feedback ratings [12]. Malicious user identification for social networks classifies users into four types according to their negative or positive comments [16, 17].

We focused on the differences between the related studies and the proposed research. The foremost difference was that the manufacturers began the manufacturing after the contract with customers was finalized, which makes their products different from readymade products. The quality of the product is not guaranteed, and the majority satisfaction is not verified; hence, the feedback may be totally different from the majority's opinion and each average rating. This implies that the manufacturers that had the first-class rating in the previous evaluations may get the lowest-class rating from different evaluators. Therefore, we propose a new malicious evaluator identification method that does not connect the present evaluation with the average reputation or majority rating. It compares the present rating with just the previous rating for the same customer, domain code, and manufacturer, because we can surely say that, if customer A was not satisfied with manufacturer B for a product of a specific domain code C and then gave the R class rating, A will choose other manufacturers for his/her future orders in the same domain field. If A chooses B again and gives the R class rating consecutively, then A's intention does not seem honest. To propose new malicious evaluator management, we define $\overline{R}$ from the average CEs of all the manufacturers, as shown in Eq. (7):

Table 1 Four classes

Class	S: Superb	P: Pass	D: Deposit	R: Reject
Equation	($R_{mj} \geq \alpha$)	($R_{mj} \geq R_a$)	($R_{mj} \geq \beta$)	($R_{mj} < \beta$)
S (Superb)	In the *S* class, the manufacturer's R_{mj} is higher than the standard deviation plus the average, and the manufacturer is highly recommended to the customers.			
P (Pass)	In the *P* class, the manufacturer's R_{mj} lies between the standard deviation plus the average and the average. It can be broadly said to be better than average.			
D (Deposit)	In the *D* class, the manufacturer's R_{mj} is lower than the average but lies within the standard deviation minus the average. It can submit a proposal in the case of setting a deposit for a smart contract.			
R (Reject)	Manufacturers in the *R* class will be rejected and will not be allowed to submit their proposals.			

$$\overline{R} = \frac{1}{N_c} \sum_{x=1}^{N_c} \left(CE_x^j \right) \tag{7}$$

We defined R'_{sd} and R'_a from $\overline{R}$, and four classes (S', P', D', R') from the equation given in Table 1. R_{mj} is replaced by $\overline{R}$ in Eqs. (4, 5) to calculate R'_{sd} and R'_a. We also defined the previous reputation CE'. If the previous and the present ratings of a customer c_x for manufacturer m_j of a product of the same domain field is included in the R' class consecutively, 0 is assigned to $M(x)$ and c_x is managed as a malicious list of blockchain, such as black list management. The equation for malicious evaluator identification is shown in Eq. (8):

$$\mathrm{M(x)} = 0, \quad if \left(CE'^j_x \in R' \ and \ CE^j_x \in R' \right) \tag{8}$$

3.1.6 Management model

Customer, c_x's feedback CE is integrated into m_j's average reputation after malicious user detection. All the manufacturers are classified into four classes by using the manufacturer classification method. When a new customer C_{x+1} requests m_j's reputation for a new service, the manufacturer's class and reputation scores are provided together. It can help the new customer to make a decision easily, as shown in Fig. 5.

The list of malicious customers and reputations can be managed as blockchain transactions stored on distributed ledgers that guarantees the integrity of the data. Each participant is connected to the system by P2P protocols that will be specifically explained in the next section. The P2P networking in the proposed model enables the participants to voluntarily subscribe, publish, and confirm the contents, because each participant in every node is equal without a trusted third party. The contents stored in blockchain are protected from malicious manipulation, and the deposit function is connected to the smart contract. Applications equipped with the capabilities of smart contract can provide more plentiful features to users.

3.2 Service architecture: SPSACE protocol by P2P networking

We proposed P2P networking-based protocols using blockchain technologies. Each party could act without a trusted party to provide the required level of security because every node in P2P networking environment is a monitor and a verifier at the same time. We utilized the functionalities of smart contract, which is one of the most well-known applications of blockchain, but we represented it as blockchain, because the potential reviewed in this paper is not limited to only the smart contract characteristics.

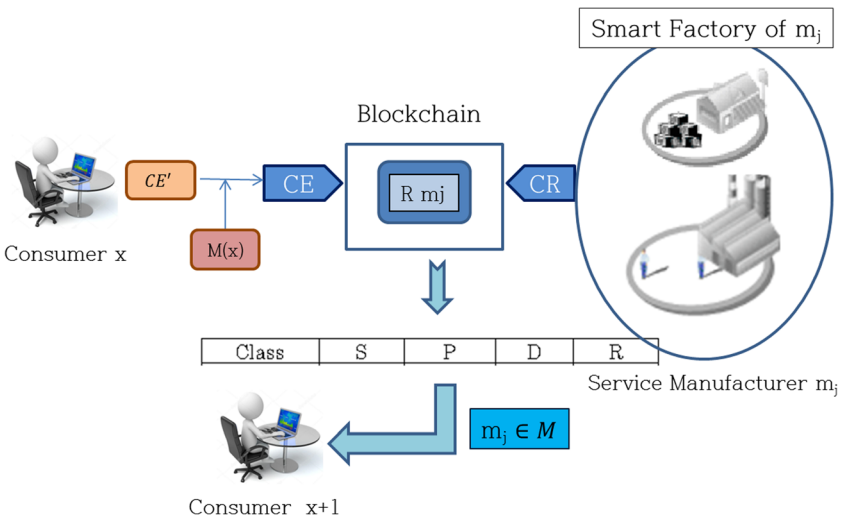


Fig. 5 Reputation management framework in P2P network

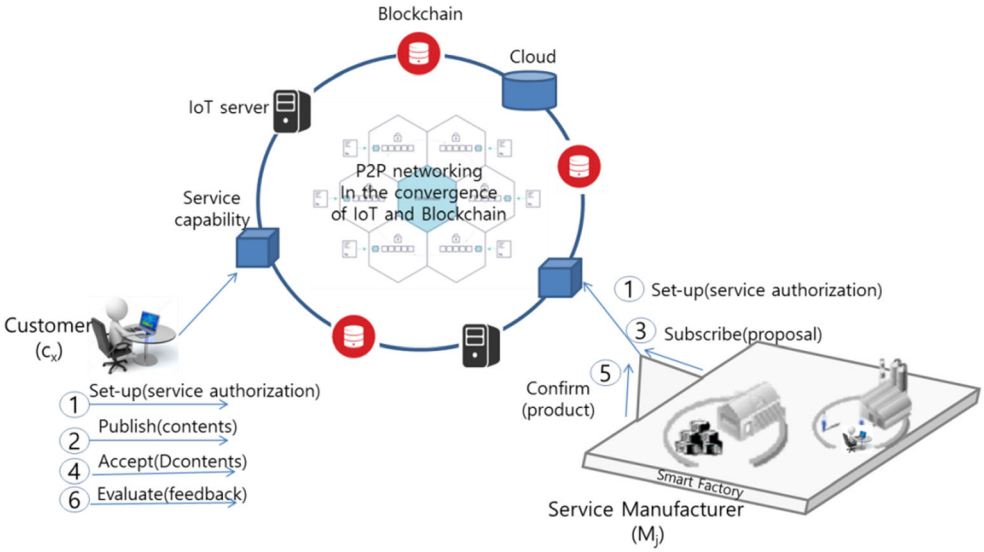


Fig. 6 The SPSACE protocol controlled by P2P networking

Here, we propose a P2P networking-based SPSACE protocol for a custom manufacturing service, as shown in Fig. 6. The SPSACE aims to provide requirements for privacy, non-repudiation, anonymity, and product confirmation for the service. All the participants can voluntarily invoke and response each protocol that can be implemented by P2P networking-based blockchain technologies. One of the most well-known platforms is Ethereum which is based on unstructured overlay in pure P2P architecture. Every node has an equal role and access without a pre-defined network topology in the architecture. The transactions submitted by each protocol are duplicated to every node and synchronized. The service as a P2P networking-based application enables all the participants to maintain the same transactions in a decentralized network and control the security of their contents autonomously without a trusted broker or centralized storage, because each participant is equal in a P2P network. Hence no centralized server has responsibility for processing power, storage or bandwidth in the P2P-based service architecture [8, 11].

When a user creates an account of blockchain, a pair of cryptographic keys are generated and regarded as the identity and security credential. Blockchain provides a digital signing algorithm with the transaction owner's private key for ensuring data integrity, tamper-proof characteristics, etc. [18, 19]. We used digital signing of blockchain for non-repudiation and product confirmation. The privacy guaranteed is provided by the indistinguishable owner of transactions with the automatically generated addresses expressed as hash values. Hence all the transactions have the vulnerability to be revealed when the users are in a specific service environment [20]. A few blockchain systems such as Bitcoin and Zcash provide a mechanism to protect privacy. A one-time account or new private key per transaction is used. We proposed to manage another public key pair for each user. Then the proposed P2P networking-based applications can allow each user to protect the transactions by specifying the partner who can access the contents. We used an encryption algorithm to allow only the permissioned user to read the contents of the transactions. Then each participant can be a user and manager at the same time in the P2P network where no authorized node or server exists.

Setup We assumed that the customers and the manufacturers were connected by P2P networking-based protocols and authenticated. We did not describe an authentication mechanism. The customers do not need to open their private information to obtain service authorization with a blockchain account. They were required to create a blockchain account, a public key pair (p, q), and open the public key p in the service channel. The public key pair was created and managed by the user separately from the system identity. Customers and manufacturers in the D class were required to set the deposit.

Table 2 Privacy of transaction

Contents	Encrypted contents	Users
Proposal	$P_x^j = enc\ (proposal)\ \ with\ \ p_x$ $proposal = dec\ (P_x^j)\ \ with\ \ q_x$	From: m_j To: c_x
Detailed Contents	$DC_x^j = enc\ (Dcontents)\ \ with\ \ p_j$ $Dcontents = dec\ (DC_x^j)\ \ with\ \ q_j$	From: c_x To: m_j
Product	$PA_x^j = enc\ (PA_x^j)\ \ with\ \ p_x$ $product = dec\ (PA_x^j)\ \ with\ \ q_x$	From: m_j To: c_x

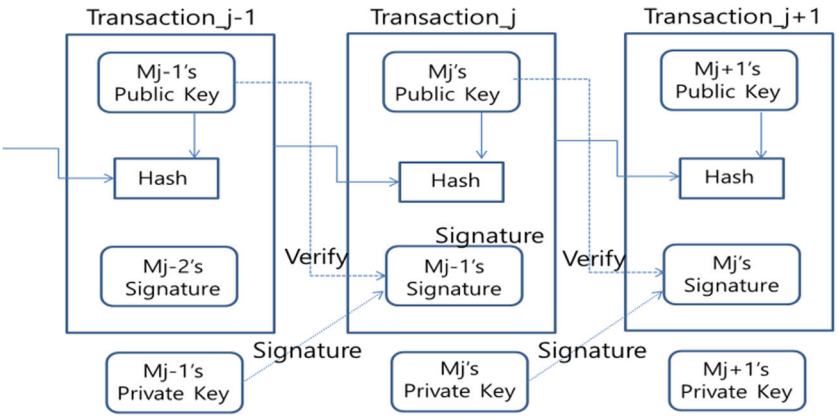


Fig. 7 Digital signing of blockchain for non-repudiation

Publish Customer, c_x published the contents to get the proposals from the manufacturers. We did not use encryption for the publish mechanism to open the contents. Only the outline with the domain code was included in the contents. c_x published the contents as a transaction, T_x through blockchain.

$$T_x \leftarrow contents \tag{9}$$

Subscribe Any manufacturer except the R class manufacturers could subscribe to transactions and submit their proposal. The manufacturer m_j encrypted the proposal with c_x's public key. Only customer c_x could open the encrypted proposal. The integrity and the tamper-proof characteristic of the transactions were guaranteed from the cryptographic technologies.

$$P_x^j = enc\,(proposal)\ \ with\ \ p_x \tag{10}$$

Accept Customer c_x decrypted the proposal. c_x could make a decision after confirming m_j's reputation class. If customer c_x accepted the proposal, c_x encrypted the detailed contents (Dcontents) with m_j's public key. Dcontents could be opened only by m_j who had the private key. They signed a contract to order the manufacture of Dcontents. m_j produced the product as the following Dcontents. The digital signing of transactions by blockchain prevents future problems from being denied. Due to the nature of the service that starts manufacturing after ordering, various problems can arise depending on the result of production after the completion of the service.

$$DC_x^j = enc\,(Dcontents)\ \ with\ \ p_j \tag{11}$$

Confirm Production was confirmed by the manufacturer m_j after the completion of production. The product in Eq. (12) could be a real product or a proof of delivery connected to the smart distribution system. It can also be a key value associated with an external repository to improve performance and reduce storage of blockchain.

$$PA_x^j = enc\,(product)\ \ with\ \ p_x \tag{12}$$

Evaluate Customer c_x could rate the manufacturer m_j as a feedback of the service. After evaluation, the payment for the service was completed, and if the consumer did not evaluate the manufacturer within a given period of time, the payment was executed automatically by the deposited money.

4 Evaluation

4.1 Security evaluation

We analyzed security requirements that should be provided in performing service protocols. We established privacy, non-repudiation, fairness, and anonymity as service requirements and verified that they are delivered properly in following section.

Table 3 Fairness cases

Case	Description	Proposed approach
Case 1	manufacturer m_j is honest and customer c_x is malicious and does not evaluate m_j to avoid payment	We ask all customers to set aside a deposit to participate in this service. If this case happens, payment will be released after a given period of time.
Case 2	customer c_x is honest and manufacturer m_j is not honest	Propose four classes of manufacturers. The R class will be rejected and will not be allowed to join the service; the D class will be required to set aside a deposit against damages.

Table 4 Domain management

DomainCode	Example of SpecificField		Contents			Manufacturing		Delivery	
			Design	Quality	Performance	Period	Cost	Service	Period
IP: ImmaterialProduct	1.Music, 2.Book, 3.Design, 4.Translation	IP	10	10	–	10	10	–	–
ET: Electronics	1.Home, 2.Tele, 3.Computer, 4.Custom	ET	10	10	10	10	10	10	10
HI: SmallItems	1.Household, 2.Decoration, 3.Toy	HI	10	10	–	10	10	10	10
FG: FasionGoods	1.Clothes, 2.Accessory, 3.Shoes	FG	10	10	–	10	10	10	10
SE: Equipments	1.Construction, 2.Sports, 3.Save	SE	10	10	10	10	10	10	10

4.1.1 Privacy

Privacy means hiding personal context [20]. User identity is hidden by pseudonyms in blockchain. When the implication from blockchain is provided under a specific service environment, the privacy of a transaction can be breached, and the private context can be revealed. We used a cryptographic algorithm with another public key pair. The data that we tried to protect was the proposal from a manufacturer, detailed contents from a customer, and products from the manufacturer [21]. By allowing the sender to specify the recipient, the sender-initiated privacy is provided, and only the recipient with the private key can verify the contents as shown in Table 2.

4.1.2 Non-repudiation

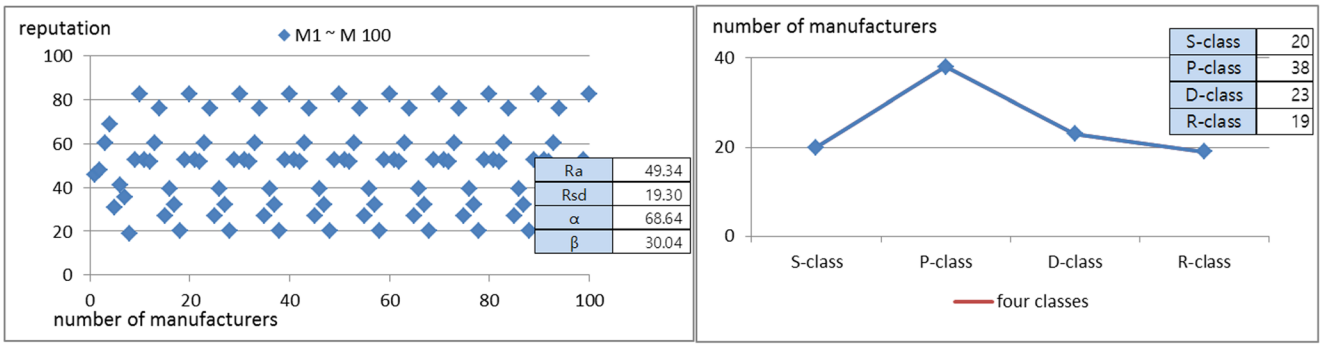
The users should not be allowed to deny their behavior after the service has been performed. The protocols provided include not denying the customer's order and not denying the service provider's offer. The transactions of ordering contents signed by the customer's private key are stored in blockchain. When a transaction is added in a ledger, after verification by the consensus of a majority of the participants, it can never be manipulated or erased. Hence, the user cannot repudiate performing the transaction and will be held responsible for a voluntary transaction. Figure 7 shows the digital signing inside of blockchain where the transactions are linked with each other and digitally signed by the transaction owner's private key and the previous public key, which is automatically generated by blockchain [5, 6]. We tried to make the most of the benefits of the blockchain so that we did not do redundant work to improve the performance of the system.

4.1.3 Fairness

Suppose that one of the two parties is not honest, then the partner of the dishonest user has to lose money. We need a way to prevent them from performing the protocol. We proposed the use of the deposit function to protect manufacturers from dishonest and malicious customers and manufacturer classification to protect customers from bad credit manufacturers [13] (Table 3).

4.1.4 Anonymity

Anonymity means hiding the owner performing an act. The users in blockchain use pseudonyms instead of their real names. The degree of user anonymity provided by blockchain is expressed through indistinguishable transactions and random identities [20, 21]. The proposed system does not request any private information from the customers and the manufacturers. We did not describe the user authentication mechanism. If user information is required for cryptographic currency exchange, it is independent of the contents of the service. Manufacturers need to complete some preliminary jobs to get *CR*; nevertheless, detailed contents and private information are not disclosed.



a) Reputation of 100 manufacturers

b) Classification of manufacturers

Fig. 8 Simulation of manufacturer classification

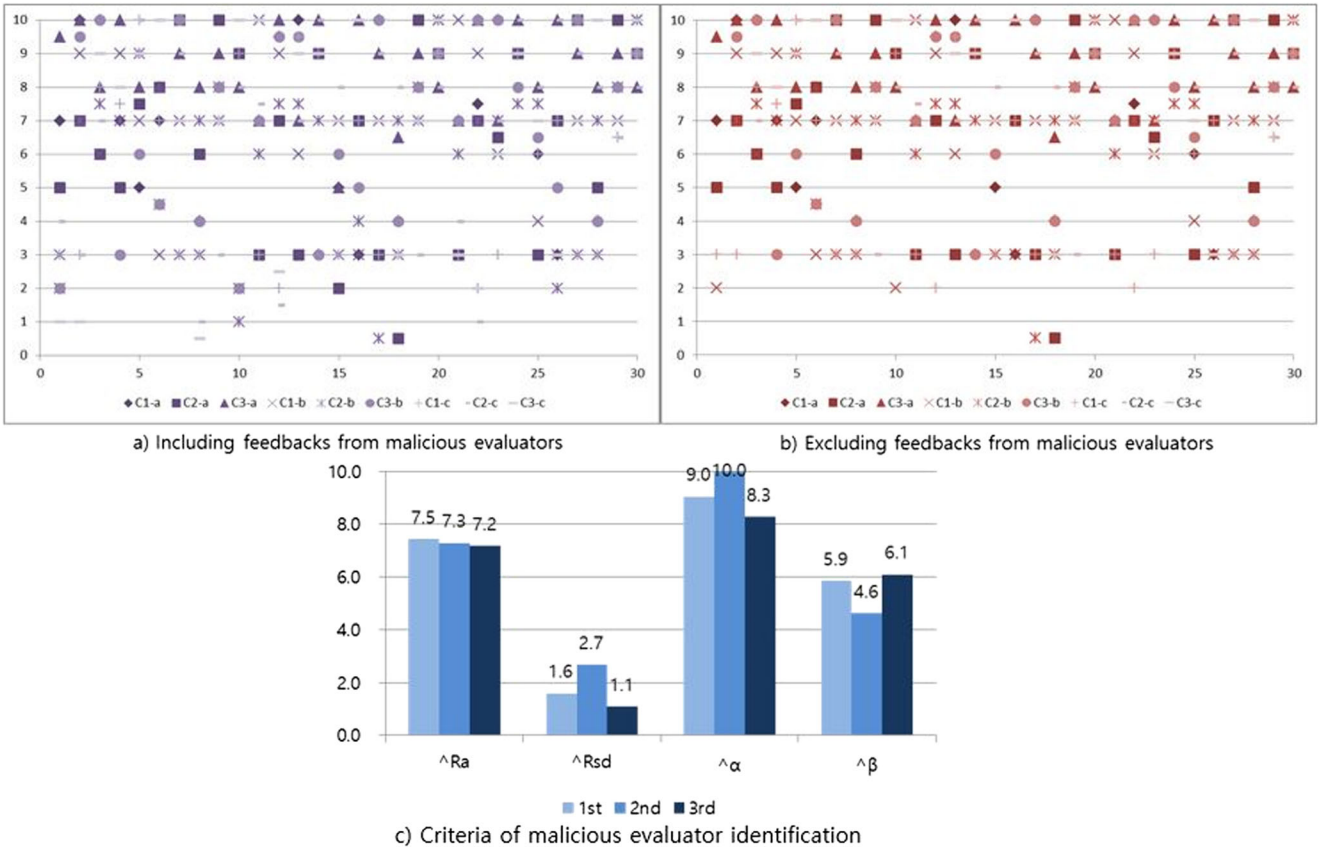


Fig. 9 Simulation of malicious evaluator identification

4.2 Malicious evaluator

We defined the reputation management with malicious management in Eq. (3) and malicious evaluator identification in Eq. (8). It is aimed at increasing the reliability of the reputation management result by excluding the feedback from malicious or dishonest evaluators during the reputation assessment.

Proof

$$\mathrm{N} = \{1, 2, \ldots \mathrm{L}\} \quad M = \{k | M(x) = 0, k \in N\}$$

$$\mathrm{x} \in \mathrm{N}, \quad \text{if} \quad \mathrm{M} = \varnothing$$

$$R(m_j)' = \{CR^j \cdot wr\} + \left\{ \frac{\sum_{x=1}^{Nc} \left(CE_x^j M(x)\right)}{\sum_{x=1}^{Nc} M(x)} \cdot we \right\}$$

$$= \{CR^j \cdot wr\} + \left\{ \frac{\sum_{x=1}^{Nc} \left(CE_x^j\right)}{L'} \cdot we \right\}$$

$$R(m_j) \leftarrow R(m_j)', \quad \text{where} \quad \mathrm{L}' = \mathrm{Nc}$$

Otherwise

$$R(m_j)'' = \{CR^j \cdot wr\} + \left\{ \frac{\sum_{x=1}^{Nc} \left(CE_x^j M(x)\right)}{L''} \cdot we \right\}$$

$$\left(if \;\; x = k, CE_x^j = 0\right)$$

$$R(m_j) \leftarrow R(m_j)'', \quad \text{where} \quad \mathrm{L}'' = \mathrm{Nc}{-}\mathrm{n}(\mathrm{M})$$

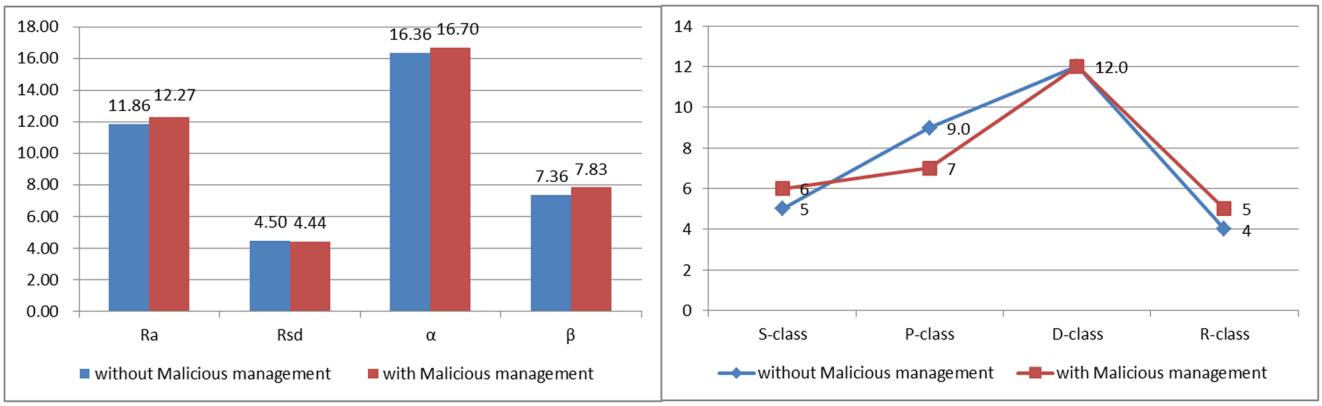
Here M is a set of malicious evaluators. If M is empty, there is no malicious user. Then, every $M(x)$ has 1, and all feedbacks are reflected. When x is k who satisfies malicious Eq. (8), CE_k^j as the k^{th} evaluation is 0 and L'' is the number of participating customers minus M's element number. Evaluations from $M(x)$ are excluded and do not influence the total reputation management.

4.3 Simulation of reputation management system

We divided the product fields into specific domains to manage them in detail and increase the credibility and the accuracy of the reputation system. We proposed different elements according to the domain features. A domain was represented with two letters and 1 digit by applying a two-step categorization; therefore, SE1 denotes the equipment in the construction domain, as shown in Table 4. We gave examples of a few representative domains, as shown in Table 4.

4.3.1 Reputation classes

We defined the experimental reputation ratings of 100 manufacturers. We assigned 10 evaluators for each manufacturer and assigned random CE for each evaluator and CR for each manufacturer, as shown in Fig. 8a.



a) Change of criteria b) Number of manufacturers in four classes

Fig. 10 Simulation of criteria and classes

Four reference values: R_a, R_{sd}, α, and β were calculated from the reputations of 100 manufacturers using Eqs. (4, 5, 6). Manufacturers were grouped into four classes according to the reference values obtained from Fig. 8a and distribution chart shown in Fig. 8b was calculated as following Table 1.

4.3.2 Malicious evaluator

We simulated the manufacturers' reputation and reference values through the equations proposed in this paper to demonstrate increased reliability compared to when malicious user detection was used and not. We gave three customers' three consecutive experimental ratings to 30 customers ($C1$ to $C30$). In all, 270 ratings are shown in Fig. 9a. Figure 9b illustrates the exclusion of feedbacks from malicious evaluators using Eqs. (3, 7, 8). Figure 9c shows the change in the criteria used to determine the malicious evaluator in Fig. 9b. The values shown in Fig. 9c were calculated and reflected for each evaluator's third assessment.

We observed how the criteria changed in the two cases shown in Figs. 10a, b on the basis of the data shown in Fig. 9. Figure 10a shows a comparison of the criteria: R_a, R_{sd}, α, and β according to the reflection of malicious management using Eqs. (3, 8). The total reputation average was reflected from the malicious management in real time. Figure 10b shows the change in the number of manufacturers in the four classes upon malicious evaluator identification. Figure 10b shows that manufacturers' classes change by detecting malicious users even if the manufacturers' ratings do not change, and this relates to increasing the reliability of the system.

Figure 11 shows the reputation change of 30 manufacturers on the basis of the data shown in Figs. 9 and 10. We divided the 30 manufacturers into three groups. We assigned the domain weight (wr: 0.4, we: 0.6) to the first group ($m1$–$m10$), domain weight (wr: 0.5, we: 0.5) to the

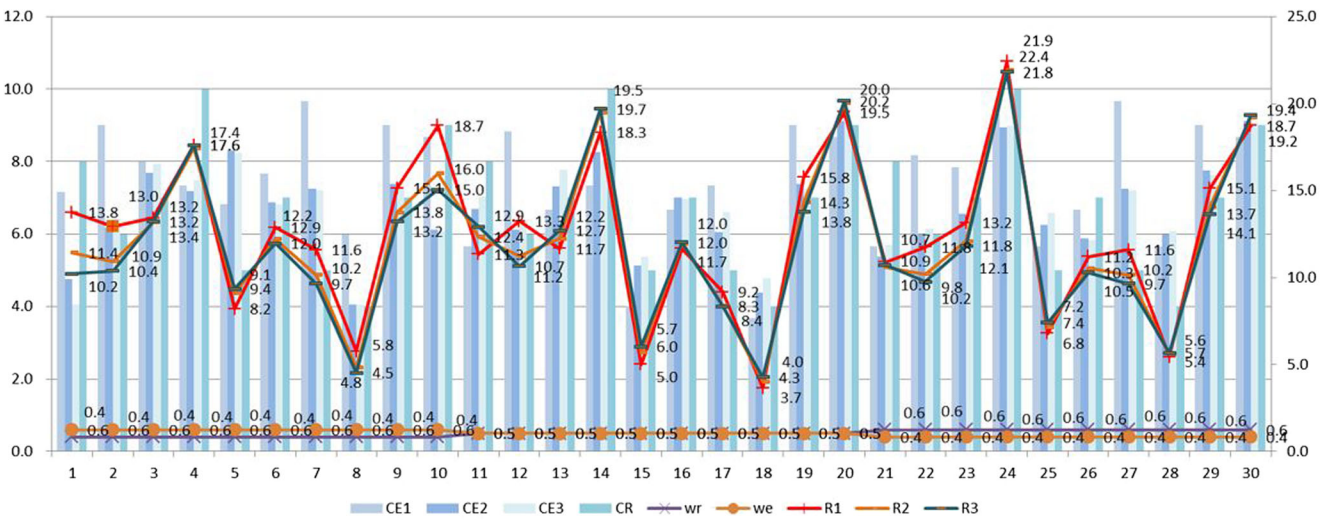


Fig. 11 Reputation observation for manufacturers 1–30

Table 5 Comparison with related research

Research	Difference	Limitation
Malik et al. [12]	Reputation assessment framework for web services was proposed. Weight was given to recent feedback by using a fader parameter with a time stamp. Majority opinion was considered for the identification of malicious users.	Not based on a decentralized system. Security depended on centralized storage. No classification to guide customers.
Bok et al. [15]	Reputation management for social networks. It classified users into four types according to negative and positive activities for malicious user identification. It considered implicit and explicit ratings for the reputation of the social networks.	No flexible user classification. No clear method for malicious user identification. Limitation with centralized control and storage.
Zhao et al. [13]	It used fixed criteria to determine the rater's dishonesty. It applied the implicit reputation research of social networks to fair payment. This mechanism could not control the fixed criteria flexibly.	No feedback reflection for malicious user identification. No classification to guide customers.
Nitti et al. [22]	Trustworthiness management in the social IoT was proposed. The approach was divided into two types according to subjective and objective storage types (rater based and distributed).	Not based on decentralized control. No feedback reflection of malicious user identification.
Wang et al. [14]	SDN-based publish-and-subscribe system. Topic-based middleware with centralized control.	Privacy and anonymity were not considered. Limitations from the centralized system.

second group ($m11$–$m20$), and domain weight (wr: 0.6, we: 0.4) to the last group ($m21$–$m30$). We verified the reputation change of the 30 manufacturers as the result of the weight assignment and the feedback change from the malicious evaluator management.

5 Comparison and discussion

We compared the closely related studies with the proposed approach to summarize the detailed view shown in Table 5. The proposed approach was based on decentralized control by accepting the trustless P2P networking of blockchain. The participants could control the maintenance of their interactions by themselves. The proposed reputation system reflected the recent ratings to guide the customers' present decision making and provided a rating classification to guide the customers. The proposed service architecture provided privacy, non-repudiation, anonymity, and fairness.

6 Conclusions

We proposed a blockchain-based custom manufacturing service as a P2P networking-based application where customers and manufacturers can sign a contract to produce goods on demand. Customers can participate in this service without revealing their real identity and invading data privacy, and manufacturers can decrease the costs of running their manufacturing business and easily join the service by providing protection against future damage. The proposed reputation management system can guide the customers' decision making with the classified and reliable manner provided by the manufacturer classification. We increased the reliability of the reputation system by proposing new malicious evaluator identification customized for manufacturing systems. The proposed SPSASE protocol in the service architecture enabled the participants to be connected with decentralized P2P control with privacy and non-repudiation, and fairness. We used a cryptographic algorithm to preserve the transaction privacy and utilized the digital signing of blockchain for non-repudiation and product confirmation. We verified that the security requirements were satisfied and past feedbacks guided the customer's present decision making in a reliable manner. We compared the differences and the originality with the related studies to summarize the proposed approach. Although offering a number of advantages, the proposed protocol has room for improvement. We expect that an increased variety of products will be manufactured through P2P networking-based applications. We need to fractionize the domain fields for sensitive management. We also need to investigate the relationship of the attributes that affect the manufacturing system.

Acknowledgements This work was supported by the Next-Generation Information Computing Development Program through the National Research Foundation of Korea, Republic of Korea (Grant no.: NRF-2017M3C4A7069432).

References

1. Kenning, Lagermann, "Recommendations for implementing the strategic initiative INDUSTRIES 4.0. Industries 4.0 working Group, April 2013
2. V. Pureswaran, Veena, P. Brody, "Device democracy: saving the future of the internet of things. IBM Corporation. Sep, 2015
3. Kshetri N (2017) Can Blockchain strengthen the internet of things? IT Professional 19(4):68–72
4. Christridis K, Devetsikiotis A (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303

5. Crosby M, Pattanayak P, Verma A (2016) Blockchain technology beyond bitcoin. Applied Innovation 2:6–10
6. Tschorsch F, Scheuermann B (2016) Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials 18(3):2084–2123
7. Novo O (April 2018) Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J 5(2): 1184–1195
8. Sohn I, Yoon S, Lee S (January 2018) Distributed scheduling using belief propagation for internet-of-things (IoT) networks. Peer-to-Peer Networking and Applications 11(1):152–161
9. Beltran R, Fuentes F (August 2018) Hierarchical P2P architecture for efficient content distribution. Peer-to-Peer Networking and Applications (PPNA):1–16
10. Jøsang A, Ismail R, Boyd C (2007) A survey of trust and reputation systems for online service provision. Decis Support Syst 43(2): 618–644
11. Meng X (May 2018) sureTrust: a super peer-aware trust model for 2-level P2P networks. Peer-to-Peer Networking and Applications (PPNA) 11(3):619–631
12. Malik Z, Bouguettaya A (2009) RATEWeb: reputation assessment for trust establishment among web services. VLDB J 18(4):885–911
13. Zhao Y, Li Y, Mu Q (2018) Secure pub-sub: Blockchain based fair payment with reputation for reliable cyber physical systems. IEEE Access 6:12295–12303
14. Wang Y, Zhang Y, Chen J (2018) An SDN-based publish/subscribe-enabled communication platform for IoT services. China Communications 15(1):95–106
15. Bok K, Yun J, Kim Y, Lim J, Yoo J (2017) User reputation computation method based on implicit ratings on social media. KSII Transactions on Internet and Information Systems (TIIS) 11(3): 1570–1594
16. S. Adali, "Measuring behavioral Trust in Social Networks. IEEE International Conference on Intelligence and Security Informatics, Vancouver, BC, Canada, May 2010
17. Yan Z, Vasilakos V (2014) A survey on Trust Management for Internet of things. J Netw Comput Appl 42:120–134
18. Resnick P, Zeckhauser R, Fredman R, Kuwabra K (December 2000) Reputation systems. Commun ACM 43(12):45–48
19. X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, "A Survey on the Security of Blockchain Systems. Future Generation Computer System, 2017
20. M. Khalilov, A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Communications Surveys & Tutorials 20(3):2543–2585. https://doi.org/10.1109/COMST.2018.2818623
21. Vertino E, Khan L (2006) Secure knowledge management: confidentiality, trust, and privacy. IEEE Transactions on systems, man, and cybernetics-Part A: Systems and humans 36(3):429–438
22. Nitti M, Girau R, Atzori L (2014) Trustworthiness Management in the Social Internet of things. IEEE Trans Knowl Data Eng 26(5): 1253–1266

YongJoo Lee received the M.S., and Ph.D. from Chungbuk National University, Korea. She had been a senior researcher at ETRI in Korea from 2001 to 2009. She is currently a chief researcher at IT global research institute of KNUT in Korea. Her research interest includes network, security, cryptology, blockchain, P2P, and IoT.

Keon Myung Lee received B.S., M.S., and Ph.D. from KAIST, Korea. He is a professor at Department of Computer Science, Chungbuk National University. His research interest includes machine learning, data mining, big data, blockchain, and artificial intelligence applications.

Sang Ho Lee received B.S., M.S., and Ph.D. from Sungsil University, Korea. He had been a professor at Department of Computer Science, Chungbuk National University from 1981 to 2018. He is an honorary professor at Department of Computer Science, Chungbuk National University. His research interest includes network, security, IT convergence, P2P, and Smart factory.