

INFLUENCE OF BLOCKCHAIN AND SMART CONTRACTS ON PARTNERS' TRUST, VISIBILITY, COMPETITIVENESS, AND ENVIRONMENTAL PERFORMANCE IN MANUFACTURING SUPPLY CHAINS

Ping-Kuo CHEN¹, Qiu-Rui HE^{1*}, Shiping CHU²

¹*Business School, Shantou University, Shantou City, China*

²*Security Management Department, Zhejiang Institute of Security Technology,
Wenzhou City, China*

Received 24 May 2021; accepted 08 November 2021; first published online 02 March 2022

Abstract. This study investigates the influence of blockchain and smart contracts on partners' trust, increasing visibility, competitiveness, and environmental performance when implemented in manufacturing supply chains. Partial least squares (PLS) was the main method used to test and verify the research model and hypotheses. According to the test results, blockchain and smart contracts positively influence partners' trust. Increasing trust produces a positive effect on increasing visibility, further promoting competitiveness and environmental performance. However, the vulnerability of smart contracts still causes information security concerns. If smart contracts are adopted for an extended time, partners will worry about problems of information vulnerability stemming from the smart contract, further reducing trust and affecting visibility. Regarding academic implications, this study not only proves the relationship between blockchain, smart contracts, partners' trust, increasing visibility, competitiveness, and environmental performance. In addition, we also proved the vulnerability of smart contracts; our test results fill these gaps. Regarding practical implications, with extended contract periods, partners may expand their doubt in the smart contract and reduce information sharing, further affecting visibility. Manufacturers are reminded that smart contracts may carry hidden trouble that disrupts the relationship between partners' trust and visibility.

Keywords: supply chain, blockchain, smart contract, trust, visibility, competitiveness, environmental performance.

JEL Classification: M15, M11, L23.

Introduction

In the supply chain of heavy manufacturing industries, visibility is a critical factor in raising production and manufacturing efficiency in the industry. Supply chain visibility is defined as the extent to which actors within a supply chain have access to or share information that

*Corresponding author. E-mail: a1104100@ms23.hinet.net

they consider key or useful to their operations and that they consider will be of mutual benefit (Barrat & Oke, 2007). Kurniawan et al. (2017) indicated that a greater level of visibility offers a complete view of the production process, from outbound suppliers to the ultimate customers. Visibility also improves confidence and helps maintain practices of related production activities under the supply chain, assisting firms in controlling production costs. In addition, other priorities, including quality, delivery, and production flexibility (Somapa et al., 2018), can all be improved and further realize competitiveness. Moreover, greater visibility also helps control and improves the production environment. Therefore, air emissions, recycling wastewater, solid waste discharge, and the consumption of hazardous, harmful, and toxic materials can be controlled and improved (Dubey et al., 2020), achieving greater environmental performance.

To raise visibility, information sharing between manufacturers and partners is important for increasing visibility. Information sharing in the supply chain is defined as partners' willingness to make strategic and tactical data, such as inventory levels, forecasts, sales promotion, strategies, and marketing strategies, available to firms forming supply chain nodes (Al-Doori, 2019). Lotfi et al. (2013) indicated that information sharing brings a significant advantage in increasing visibility. However, effective information sharing depends on trust between partners. High levels of trust will drive partners' willingness to share related information, and a lack of trust may impede information sharing (Lotfi et al., 2013). Based on the above, to increase visibility, trust should be improved between partners.

However, in the real world, promoting trust is a serious problem. Li and Wang (2021) indicated that low safety factors of information sharing and high-risk coefficients exist in the linkage between manufacturers and partners. Partners worry that strategic and tactical information can be leaked under the information sharing process, causing serious benefit damage. Therefore, to improve partners' trust, information security should be strengthened. Information security is defined as protecting information assets, such as an organization's core technology (Park et al., 2021). When information security is strengthened, it is possible to promote partners' trust. When the trust level rises significantly, partners will increase their intention to share related information (Panahifar et al., 2018), resulting in increased visibility.

Although practitioners have tried to implement different information technologies to strengthen information security, information vulnerability is consistently difficult to improve. With the emergence of blockchain technology and smart contracts, information security has improved significantly. Based on the effects of blockchain and smart contracts on information security, related studies, such as Çolak et al. (2020), found that partners' trust can increase significantly because information security is ensured. Habib et al. (2020) pointed out a key reason: the method's decentralization and immutability characteristics highly improve information security. In addition, a smart contract is usually involved in implementing the blockchain in supply chain operational operations. Smart contracts can analyse information sharing and further produce decisions to improve related production activities. According to Francisco and Swanson (2018), applying a smart contract can ensure that information sharing and processing occur without human interaction; therefore, smart contracts reduce information leaking and significantly increase partners' trust and intent to share information. This is why implementing blockchains and smart contracts can ensure increasing visibility. In

addition, related studies, such as Dujak and Sajter (2019) and Hamledari and Fischer (2021), indicated that implementing blockchain and smart contracts raises partners' trust and further promotes information sharing intention. As a result, information process transparency also improves, which again increases visibility.

The above discussion suggests a conceptual framework: implementing block chains and smart contracts positively influences information security and partners' trust level and further promotes the visibility of the manufacturing supply chain. With visibility increasing, competitiveness and environmental performance are also realized and achieved.

Implementing block chains and smart contracts seems to have greater influence in raising partners' trust, increasing visibility, and realizing greater competitiveness and environmental performance; however, smart contracts still have a hidden issue in information security. The smart contract's algorithm code is usually open on a blockchain platform (Chia et al., 2018; Demir et al., 2019), and in the real world, malicious attackers can steal internal information and cause serious damage to the blockchain. A few real cases exist in which vulnerability related to smart contracts caused attacks. Thus, information security is possibly threatened due to the vulnerability of the smart contract. If the hidden trouble of smart contracts exists, it also affects the blockchain. Due to this smart contract vulnerability, an increasing number of practitioners are asking if the influence of blockchain and smart contracts truly, positively affects partners' trust and increases visibility.

This study will explore and verify the influence of block chains and smart contracts and try to understand whether the implementation of block chains and smart contracts has positive effects on partners' trust, increasing visibility, competitiveness, and environmental performance. This study will also explore the hidden trouble of smart contract vulnerability and its potentially negative effect in disrupting partners' trust and visibility, further affecting competitiveness and environmental performance. Based on our research purpose, the study structure is as follows. In Section 1, we describe the literature review. In Section 2, we build research hypotheses and a theoretical framework. Section 3 describes the methodology. In Section 4, we test and verify the research hypotheses and discuss them using empirical cases, followed by our conclusions.

1. Literature review and theoretical framework development

1.1. Development of block chain and smart contracts

The manufacturing supply chain faces a serious challenge: increasing information security to ensure partners' trust. For this reason, blockchain technology seems to be a viable solution. The first mention of blockchain goes back to 1991, when Stuart Haber and Scott Stornetta described a cryptographically secured blockchain (Hechler et al., 2020). Then, in 1992, the system was upgraded with the Merkle tree approach, which optimized and combined all tasks into one. Although its patent was cancelled in 2004, in 2008, Bitcoin emerged (Nakamoto, 2008).

Blockchain and Bitcoin were developed before we all became part of the world of centralization, in which any transaction depends on third-party institutions, such as banks, exchange houses, or supervisor units. However, transactions related to centralization have

potential transaction time costs (Treiblmaier, 2018). Transaction records can be changed or leaked when subjected to malicious web attacks, affecting new transaction verification or business information security. When Bitcoin emerged, it helped to eradicate most of these problems. Bitcoin is a virtual currency, and its practice depends on blockchain technology; it uses distributed ledger technology to finish transactions. How does this distributed ledger technology support Bitcoin transactions? First, only two roles exist in the transaction environment, namely, traders and miners. When a transaction appears, a third-party institute is not required to verify that the transaction is credible; thus, traders can directly complete transactions with other Bitcoin traders. However, all transaction records are verified and encrypted by miners' algorithms and then saved in Bitcoin. Next, the Bitcoin transaction records are uploaded to every trader as a block of information. Due to the miners' help verifying the transaction's credibility, they are rewarded with a few Bitcoins. When new transactions appear, miners can help to verify them; the related blockchain information is seen as immutable, and traders can review previous records and track transactions. Every trader can also check the credibility of new transactions based on prior transaction records. This application of Bitcoin is called "blockchain 1.0" (Angelis & da Silva, 2019).

The concept of smart contracts began in 1994 (Szabo, 1997), and smart contracts have been widely applied in Bitcoin. Ether is a new virtual currency, and its concept is the same as that of Bitcoin; however, Ether is combined with smart contracts to enhance the transaction function. Smart contracts are executable codes that run on top of a blockchain to facilitate, execute, and enforce an agreement between untrusted parties without involving a trusted third party (Alharby & Van Moorsel, 2017). Traders can jointly design and develop better transaction decisions to enhance their cooperative efficiency. This process is referred to as "blockchain 2.0" (Angelis & da Silva, 2019). Blockchain has recently been combined with the Internet of Things and is widely applied in different areas while disassociated from Bitcoin; this is referred to as the "blockchain 3.0 era".

1.2. The relationships between partners' trust and the increase in visibility, competitiveness, and environmental performance

According to Yu and Goh (2014), "operationally, supply chain visibility has been linked to the capability of sharing timely and accurate information on exogenous demand, quantity and location of inventory, transport-related cost, and other logistics activities throughout an entire supply chain". Barratt and Oke (2007) and Brandon-Jones et al. (2014) indicated that visibility is essential in managing supply chains. Dubey and Altay (2018), combined with the view of Christopher and Lee (2004) and Brandon-Jones et al. (2014), further indicated that "visibility is related to the flow of information and allows supply chain partners to coordinate as they can see each other's inventory levels and replenishment quantities. This transparency in information flows can improve confidence and reduce interventions, which in turn improves decision-making". Singh et al. (2019) indicated that visibility is defined as the ability of supply chain managers to see and locate disruptive events from one end of the supply chain to another.

Why does visibility play a critical factor in promoting manufacturing supply chain competitiveness and environmental performance? When visibility is expanded, the production

process of the manufacturing supply chain becomes apparent, which can encourage production practices, avoid waste, and decrease redundant production activities (Zhuo et al., 2021). In addition, manufacturers can understand different situations, such as inventory, capacity, and related production resources. Therefore, it is easy for manufacturers to coordinate with partners to develop or improve a production process (Li et al., 2019). According to Brusset (2016) and Prajogo et al. (2018), the production process can be improved to maximize process performance, such as cost, quality, delivery, and flexibility, and further realize highly level competitiveness. In addition to competitiveness, environmental performance can also be realized. Klueber and O’Keefe (2013) indicated that increasing visibility contributes to improved performance in environmental sustainability, such as air emissions, recycling wastewater, preventing solid waste discharge, and preventing the consumption of hazardous, harmful, and toxic materials (Dubey et al., 2020). Therefore, Saqib and Zhang (2021) indicated that supply chain visibility has a critical influence on promoting sustainable manufacturing supply chain practices. Thus, it will further impact sustainable environmental performance.

Based on the above, understanding the issue of how to expand visibility is essential. According to Kumar et al. (2018), effective information sharing enhances visibility. Therefore, having high levels of information sharing intention is important in promoting increased visibility. However, having high information sharing intention depends on partners’ trust (Ha et al., 2011). Based on the above, we can infer that if partners lack increased levels of trust, then it is difficult to require partners to share related information, which affects increasing visibility. Trust is defined as an actor’s expectation that other actors will perform without monitoring or control mechanisms in ways that consider mutual benefits (Benitez et al., 2020; Dubey et al., 2020). In addition, trust is a key predictor of information exchange (Moberg et al., 2002). Barratt and Oke (2007), Fawcett et al. (2007), and Frazier et al. (2009) also indicated the importance of trust in information sharing between supply chain partners through empirical tests. Through trust, connectivity between partners can be improved. Dubey et al. (2017) explored the relationship between connectivity between partners, information sharing, and supply chain visibility through a resource-based view. They indicated that supply chain visibility is a critical resource. Producing visibility as a critical resource depends on excellent, trust-based supply chain connectivity.

Based on the above, three possible path relationships exist, and the following three hypotheses can be developed:

- H1. Partners’ levels of trust have a positive effect on increasing visibility.
- H2a. Increasing visibility promotes competitiveness.
- H2b. Increasing visibility promotes environmental performance.

1.3. The influence of blockchain in the relationship between partners’ trust and increasing visibility

In the existing research, more researchers have focused on the relationship between blockchain and information security and relationships with partners’ trust and increasing visibility.

First, in information security, Namasudra et al. (2021) indicated that data or information security had become a critical issue in the information technology industries. Block chain

technology is widely used for improving data or information security because it has several key properties, such as decentralization and immutability. Based on decentralization and immutability, when blockchain is implemented in the manufacturing supply chain, its efficiency in information security promotes partners' trust, driving all partners to share related information and further improving efficiency in increasing visibility. Decentralization refers to the transfer of control and decision-making from a centralized entity to a distributed network. Therefore, shared information from partners is impossible to control. Primarily, the distributed network uses distributed ledger technology to save every transaction or shared information; therefore, all data have the feature of immutability (Domingo et al., 2020). Based on decentralization and immutability, all information from partners is then uploaded to the blockchain to create a reliable, transparent, and secure decentralized platform, where all supply chain actors can interact in a highly secure environment and touch real information (Tian, 2016; Azzi et al., 2019). Based on the above, Kshetri (2018) and Moosavi et al. (2021) indicated that blockchain could help achieve robust cybersecurity, increasing partners' trust.

Second, according to Valero et al. (2020) and Piñeiro-Chousa et al. (2021), the implementation of blockchain changes the original organizational environment. Based on trust and high information security, every participant on the blockchain platform will raise intention and further share related information to interact with other participants. Therefore, communication will be easy in the organizational environment, and all corporate environments will become transparent. Thus, when blockchain is implemented in a manufacturing supply chain, transparency will increase supply chain visibility. Rogerson and Parry (2020) found that implementing the blockchain creates a reliable transparency transaction environment, and all transactions and shared information exist unchangeably without anyone's control. Therefore, it has a positive effect on increasing visibility.

Based on the above, we can develop the following hypotheses:

H3a. The influence of blockchain technology has a positive effect on partners' trust.

H3b. The influence of blockchain technology has a positive effect on increasing visibility.

1.4. The direct, mediating, and moderating effects of smart contracts

Smart contracts are also involved in block chains, and they apply in related information processing in the manufacturing supply chain. Specifically, the application of smart contracts can be designed in two ways: the first is to enhance distributed ledger technologies (Al Khalil et al., 2017). Therefore, it can improve the ability to save information. Second, smart contracts can be applied to process and analyse related information, further producing related decisions to promote operational efficiency in the manufacturing supply chain. The application of smart contracts also features decentralization; therefore, they can effectively process and analyse related information without human interaction (Francisco & Swanson, 2018). Based on the above, participants' trust in the blockchain will rise significantly, and they will be more willing to share related information due to the application of smart contracts (Kirkman, 2018; Javaid et al., 2019). In addition, smart contracts can enhance information saving, analysis, and processing and raise participants' trust and willingness to share related information; thus,

they also generate information and transaction transparency. Therefore, smart contracts will positively affect the increase in visibility (Montes et al., 2019). Moreover, according to Chang et al. (2019) and De Giovanni (2020), the application of smart contracts also promotes the influence of the blockchain in information security. Therefore, Choo et al. (2020) believed that smart contracts play a more significant mediating role between blockchain contracts and participants' trust.

However, the current study reinforces the conflicts and questions related to the application of smart contracts. Such conflict may break partners' trust and limit increasing visibility when smart contracts' information security and vulnerability are questioned because the smart contracts' code is usually open on a blockchain platform, where information vulnerability may appear. A blockchain safety service provider, PeckShield, indicated that more than 12 hacker events occurred from 2018 to 2020, all of which attacked the vulnerability of smart contracts, even affecting and seriously damaging the blockchain platform. Therefore, Chen et al. (2020) indicated that smart contracts still have user risks, which will affect trust and the use of smart contracts. If trust is damaged, visibility will be affected. Therefore, smart contracts may have a moderating effect on the relationship between trust and visibility. In addition, if a moderating effect exists, smart contracts may not positively promote blockchain technology, which is a conflict noted in the existing studies. Based on the above, we propose the following hypotheses:

H4a. Smart contracts have a positive effect on partners' trust.

H4b. Smart contracts have a positive effect on increasing visibility.

H5. Smart contracts also have a mediating effect on the relationship between blockchain and partners' trust.

H6. Smart contracts have a moderating effect on the relationship between partners' trust and increasing visibility.

1.5. Theoretical framework

According to the related literature review and hypothesis development, this study develops a theoretical framework, as shown in Figure 1.

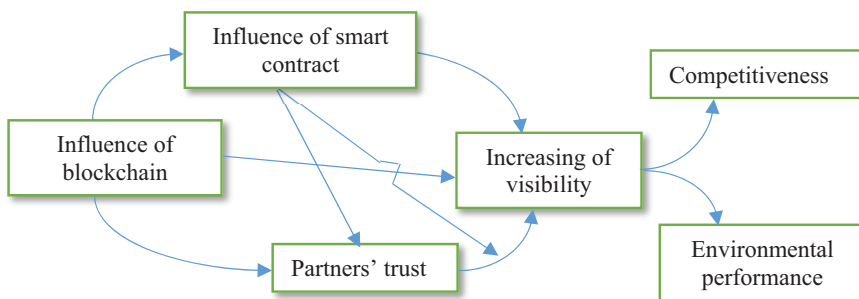


Figure 1. Research theoretical framework

2. Methodology

2.1. Questionnaire construction, data collection, and sample profile

Based on the theoretical framework, the authors designed a questionnaire to collect data to verify the hypotheses. Six constructs, namely, partners' trust, increasing visibility, competitiveness, environmental performance, the influence of the blockchain, and smart contract application, are involved in the theoretical framework; we used related literature to design measurement items for these six constructs. The responses were based on a five-point Likert scale, and the questionnaire is shown in Table 1. The questionnaire was distributed in China to 1000 manufacturers who implemented blockchain and smart contracts to promote information sharing security and filter fake information during the sharing process of their manufacturing supply chain. This study focuses on the supply chain of the heavy manufacturing industry; therefore, our sample collection follows the classification of the manufacturing industry in the International Standard Industrial Classification (ISIC). In the ISIC, heavy manufacturing industry includes manufacture of fabricated metal products, except machinery and equipment; manufacture of computer, electronic and optical products; manufacture of electrical equipment; manufacture of machinery and equipment not elsewhere classified; manufacture of motor vehicles, trailers and semi-trailers; manufacture of other transport equipment; and others' production fabrication. We received 397 completed questionnaires for a response rate of 39.7 percent. Table 2 shows the respondents' profiles.

Table 1. Constructions and items, and citation sourcing

| Constructs | Items | Citation sourcing |
|--------------------------|---|---|
| Partners' trust | PT1: I am willing to share any valuable information with my partners | Kim and Shin (2019) and Queiroz et al. (2020) |
| | PT2: I believe that our partners are certainly willing to offer real information to enhance our integration and collaboration to achieve more efficiency. | |
| | PT3: I fully believe that any information from partners certainly promotes cooperation between partners. | |
| Increasing of visibility | LV1: Increasing partners' capability for process integration means the visibility will be increased significantly. | Zhu et al. (2018) and Dubey et al. (2020) |
| | LV2: When partners' abilities regarding integration sourcing, transport, service process, and other internal areas improve significantly, visibility will be increased. | |
| | LV3: It is easier to share and obtain operational plans (i.e., distribution and storage plans) with partners, which means increased visibility. | |
| | LV4: It is easier to share and obtain strategic information, which means visibility will be increased. | |
| Competitiveness | CT1: Cost. | Somapa et al. (2018) |
| | CT2: Quality. | |
| | CT3: Delivery. | |
| | CT4: Flexibility. | |

End of Table 1

| Constructs | Items | Citation sourcing |
|-----------------------------|--|---------------------------------------|
| Environmental performance | EP1: The control of air emissions. | Dubey et al. (2020) |
| | EP2: The improvement of recycling wastewater. | |
| | EP3: The prevention of solid waste discharge. | |
| | EP4: The prevention of the consumption of hazardous, harmful, and toxic materials. | |
| Influence of blockchain | BI1: The company and partners will promote their information sharing intentions due to the immutability and decentralized block chain technology, which can avoid security breaches. | Shin (2019) and Falcone et al. (2021) |
| | BI2: Due to the efficiency of the immutability and decentralized block chain technology, the related information security is better than that of other information technology. | |
| | BI3: Decentralization will establish a closed-loop peer-to-peer network, and any information sharing in the network is immutable. | |
| Influence of smart contract | SC1: A smart contract provides secured information analysis and processing. | Badi et al. (2021) |
| | SC2: A smart contract reduces the occurrence of disputes among contracting parties. | |
| | SC3: A smart contract increases trust among contracting parties. | |

Table 2. Sample profile

| Characteristics | Profiles |
|--|---|
| Rank of respondents | Supervisor = 62.2% Middle manager = 28.7% Executive = 9.1% |
| Type of product (Industry description) | Manufacture of fabricated metal products, except machinery and equipment = 13.6% Manufacture of computer, electronic and optical products = 25.4% Manufacture of electrical equipment = 21.2% Manufacture of machinery and equipment not elsewhere classified = 20.4% Manufacture of motor vehicles, trailers and semi-trailers = 11.1% Manufacture of other transport equipment = 7.6% Others = 0.8% |
| Age of implementation of blockchain and smart contract | Under 1 year = 8.82% 1 year to 3 years = 54.91% 3 years to 5 years = 25.19% Over 5 years = 11.08% |

2.2. Research methods

Partial least squares (PLS) analysis is convenient for estimating path relationship models with latent variables while including mediation and moderation effects. In PLS analysis, bootstrapping is used to test the statistical significance of the hypothesized relationships.

The bootstrapping procedure entails generating 5000 subsamples of randomly selected cases with replacement. Under the analysis process, the path coefficients are generated for each randomly selected subsample, and the t value is calculated for every coefficient. According to the calculation results, the path coefficient and t value are statistically significant and can thus be applied to evaluate the research hypotheses. As the analysis tool, we use SmartPLS 3.0.

The constructs' validity and reliability are tested first to determine the theoretical framework and hypotheses with PLS. Factor loadings, composite reliability (CR), and average variance extracted (AVE) are the main indices used to measure validity and reliability. Regarding the requirements of the indices, the factor loadings should exceed 0.3. According to Ghorbani et al. (2019), "if the factor loading is lower than 0.3, the relationship is considered weak and is discarded. In the 0.3–0.6 range, it is deemed acceptable, and if greater than 0.6, it is very desirable". Likewise, the CR and AVE values should exceed 0.7 and 0.5, respectively (Hair et al., 2016). However, if an AVE value is lower than 0.5 and a CR value is above 0.6, then the situation can be accepted (Fornell & Larcker, 1981).

After testing with PLS, the model's goodness of fit is measured using the standardized root-mean-square residual (SRMR) as the main index. SRMR was initially proposed for use in combination with CB-SEM, but it has also been extended to PLS. This study implements SRMR because it provides an approximate measure of model goodness of fit and has been widely adopted for this purpose.

Finally, we must consider covariance-based SEM, such as AMOS & Lisrel, to analyse our theoretical framework. According to Hair et al. (2011), if the research predicts key target constructs, identifies key driver constructs, is exploratory, or is an extension of an existing structural theory, then PLS can be adopted. If the research tests or compares alternative theories, then a covariance-based SEM such as AMOS & Lisrel should be adopted. Our theoretical framework explores key driver constructs, such as the efficiency of blockchain and the influence of smart contracts; therefore, we adopted PLS.

3. Results and discussion

3.1. Test results

We first analyse the validity and reliability of the constructs, as shown in Table 3. The factor loadings of the items related to partners' trust, the increasing visibility, environmental performance, the influence of blockchain, and the smart contract application are all higher than 0.3. However, the factoring loadings of the items related to competitiveness have an unusual situation, i.e., item CT1 (cost) is lower than 0.3. Therefore, these loadings should be dropped; however, the results may indicate that cost performance is hard to realize by increasing visibility. After dropping CT1, all the factor loadings from the six constructs are higher than 0.3. In the CR and AVE, the CR and AVE values of partners' trust, increasing visibility, efficiency of blockchain, and the influence of smart contracts are higher than 0.7 and 0.5. However, the AVE values for competitiveness and environmental performance are lower than 0.5, while their CR values are higher than 0.6. Thus, according to Fornell and Larcker (1981), situations of competitiveness and environmental performance can be accepted.

Table 3. Test results of construction validity and reliability

| Constructions | Items | Factor loading | CR | AVE |
|-----------------------------|-------|----------------|-------|-------|
| Partners' trust | PT1 | 0.782 | 0.849 | 0.651 |
| | PT2 | 0.819 | | |
| | PT3 | 0.820 | | |
| Increasing of visibility | LV1 | 0.778 | 0.858 | 0.601 |
| | LV2 | 0.736 | | |
| | LV3 | 0.814 | | |
| | LV4 | 0.772 | | |
| Competitiveness | CT2 | 0.568 | 0.617 | 0.362 |
| | CT3 | 0.761 | | |
| | CT4 | 0.429 | | |
| Environmental performance | EP1 | 0.349 | 0.650 | 0.353 |
| | EP2 | 0.880 | | |
| | EP3 | 0.318 | | |
| | EP4 | 0.645 | | |
| Influence of blockchain | BI1 | 0.863 | 0.866 | 0.683 |
| | BI2 | 0.782 | | |
| | BI3 | 0.833 | | |
| Influence of smart contract | SC1 | 0.835 | 0.834 | 0.628 |
| | SC2 | 0.718 | | |
| | SC3 | 0.818 | | |

The PLS test results are shown in Table 4. In terms of construct variances, partners' trust represents 63.2% of the variance, increasing visibility represents 72.9%, competitiveness represents 7.3%, environmental performance makes up 2.4%, and 33.0% of the variance is allocated to the application of smart contracts.

Regarding the test results of the hypotheses, the path coefficient for the relationship between partners' trust and increasing visibility is 0.196 ($p < .01$); thus, H1 is supported. The path coefficients for the relationship between increasing visibility, competitiveness, and environmental performance are 0.269 ($p < .01$) and 0.155 ($p < .01$), respectively, which supports H2a and H2b. The path coefficient for the relationship between the influence of blockchain and partners' trust is 0.706 ($p < .01$), and the path coefficient for the relationship between the influence of blockchain and increasing visibility is 0.533 ($p < .01$), which supports H3a and H3b. The path coefficient for the relationship between the application of smart contracts and partners' trust is 0.141 ($p < .01$), and the path coefficient for the relationship between the application of smart contracts and increasing visibility is 0.155 ($p < .01$). Thus, this supports H4a and H4b. The path coefficient for the relationship between the application of smart contracts and the influence of blockchain is 0.574 ($p < .01$). Combined with the results of H3a and H4a, H5 was supported; thus, we can prove that the influence of smart contracts also has a mediating effect on the relationship between the influence of blockchain and partners'

trust. Finally, the path coefficient of the moderating impact on smart contracts is -0.062 ($p < .05$); therefore, its moderating effect exists. In addition, this path coefficient is negative, which means that if a smart contract exists, it is possible to weaken the relationship between partners' trust and increasing visibility.

Table 4. PLS structural model results

| Hypotheses | Path coefficient | t-value | Results |
|---|------------------|----------|--------------|
| Partners' trust -> increasing of visibility | .180 | 3.669** | Supported |
| Increasing of visibility -> competitiveness | .279 | 6.445** | Supported |
| Increasing of visibility -> environmental performance | .163 | 3.599** | Supported |
| Influence of blockchain -> partners' trust | .706 | 19.978** | Supported |
| Influence of blockchain -> increasing of visibility | .533 | 9.858** | Supported |
| Influence of blockchain -> influence of smart contract | .150 | 4.792** | Supported |
| Influence of smart contract -> partners' trust | .141 | 3.437** | Supported |
| Influence of smart contract -> increasing of visibility | .155 | 4.725** | Supported |
| Moderation effect of smart contract | -.062 | 2.157* | Supported |
| Variance explained in the endogenous variables | | | |
| Partners' trust | | | $R^2 = .632$ |
| Increasing of visibility | | | $R^2 = .729$ |
| Competitiveness | | | $R^2 = .073$ |
| Environmental performance | | | $R^2 = .024$ |
| Influence of smart contract | | | $R^2 = .330$ |
| Model fit | SRMR | .072 | |

Note: ** $p < .01$, * $p < .05$.

Based on the above, we can provide an answer for our research purpose. Blockchain and smart contracts have a significant positive influence on increasing partners' levels of trust, thereby increasing visibility and furthering the realization of competitiveness in environmental performance. In addition, smart contracts have a mediating effect on the relationship between blockchain and partners' trust. Its application can produce a greater stimulus to promote the influence of blockchain and further increase partners' trust, thereby promoting competitiveness and environmental performance. In addition, the influence of blockchain and the application of smart contracts have a positive effect on increasing visibility. In addition, Figure 2 presents proof of the moderating effect of smart contracts. Therefore, this proved that the vulnerability of smart contracts still has a negative impact; it will gradually weaken the relationship between partners' trust and increasing visibility. Therefore, while smart contracts have a positive effect, their application is still doubted and not highly trusted.

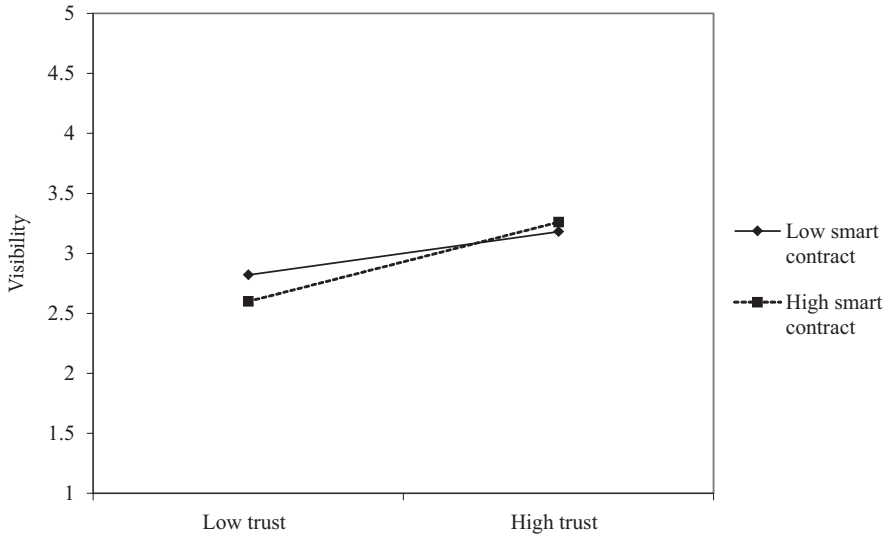


Figure 2. Test result for moderation effect

3.2. Discussion

This section further discusses the test results, according to which, implementing blockchain and smart contracts positively affects partners' trust. Partners' trust will rise because blockchain and smart contracts can improve information security. When information security is ensured, partners will raise their trust and information sharing intention, producing greater efficiency in increasing visibility. The influence of blockchain and smart contracts on information security drives the saving of related information, and processing becomes transparent without human interaction. Therefore, test results also found that blockchain and smart contracts directly promote increased visibility. The test results are the same as those of existing studies, such as Sunmola and Apeji (2020) and Hamledari and Fischer (2021). With the visibility increase, manufacturers and their partners will easily improve and control all production processes, promoting production priorities and controlling redundant production activities, further realizing and achieving high levels of competitiveness and environmental performance. These test results are also the same as those of existing studies, such as Brusset (2016), Prajogo et al. (2018), Klueber and O'Keefe (2013), and Saqib and Zhang (2021).

However, this does not mean that the influence of blockchain and smart contracts is always positive. According to the test results, smart contracts moderate the relationship between partners' trust and increasing visibility, meaning that smart contracts' vulnerabilities can cause partners to worry. Therefore, a long-existing smart contract will weaken the relationship between partners' trust and increasing visibility. Because a smart contract's code is open on blockchain platforms, many hacker attacks target the information vulnerability of smart contracts. Based on the above information and following our test results, we believe that smart contracts positively promote partners' trust; however, partners also doubt the effects of smart contracts regarding information security and worry that vulnerabilities

may cause information leaks. Therefore, if the problem is difficult to solve, smart contracts' efficiency may gradually reduce and affect partners' trust. Additionally, the influence of blockchain can be expanded through smart contracts; therefore, when the effects of smart contracts are doubted, blockchain influence can potentially decrease partners' trust and visibility. An increasing number of practitioners indicate that smart contract vulnerability is hidden when blockchain and smart contracts are implemented in the manufacturing supply chain operational environment. Therefore, more researchers, such as He et al. (2020) and Xing et al. (2020), provide practical approaches to detecting and protecting smart contract vulnerability. However, according to our test results, if the vulnerability of smart contracts persists, its negative influence will expand gradually and further weaken the relationship between partners' trust and increasing visibility. Therefore, addressing vulnerability concerns regarding smart contracts is challenging if manufacturers hope to improve partners' trust and further increase visibility through block chains and smart contracts.

Conclusions

Based on our test results, this study provides valuable implications. Regarding academic implications, although the existing studies suggest that the implementation of blockchain and smart contracts positively affects and influences the relationship between partners' trust, increasing visibility, competitiveness, and environmental performance, the evidence necessary to prove this relationship and explain it in detail is still lacking. A few studies have considered the controversy associated with smart contracts, but they lack exploration and explanation. The current study provides empirical test results and fills the gaps in the existing studies, and the results extend to related research issues. For practical implications, our test results demonstrate the problems related to smart contracts; these results point out phenomena present in the real world and prove their existence through empirical testing. Therefore, when manufacturers and partners implement blockchain and smart contracts, our test results remind them to be attentive concerning the hidden trouble of smart contract vulnerability. With such hidden trouble existing for an extended period, it will gradually weaken the relationship between partners' trust and visibility. Therefore, manufacturers should reduce negative influence when implementing blockchain and smart contracts in the manufacturing supply chain.

Although our research questions and test results provide valuable suggestions and contributions, a few problems remain for future studies to explore. First, although we demonstrated the controversy regarding smart contracts, we did not explore how to improve smart contracts. Second, although implementing block chains and smart contracts positively affects partners' trust and increasing visibility, we further suggest that competitiveness and environmental performance can also be promoted; however, this study did not examine a more detailed process between blockchain, smart contracts, partners' trust, visibility, competitiveness, and environmental performance. Based on the stated limitations, future research may explore these problems and provide further information.

Funding

This study was supported by National Natural Science Foundation of China (NSFC, Grant No. 71872131) and STU Scientific Research Initiation Grant (SRIG, Grant No. 20007). Fundings provide related research cost supporting.

Author contributions

Ping-Kuo Chen conceived the study and were responsible for the design and development of the data analysis. Qiu-Rui He and Shiping Chu was responsible for literature review, data collection and analysis. Ping-Kuo Chen, Qiu-Rui He, and Shiping Chu were responsible for data interpretation. Ping-Kuo Chen wrote the draft of the article.

Disclosure statement

This paper has not any competing financial, professional, or personal interests from other parties.

References

- Al Khalil, F., Butler, T., O'Brien, L., & Ceci, M. (2017). Trust in smart contracts is a process, as well. In M. Brenner et al. (Eds.), *Lecture notes in computer science: Vol. 10323. International Conference on Financial Cryptography and Data Security* (pp. 510–519). Springer, Cham. https://doi.org/10.1007/978-3-319-70278-0_32
- Al-Doori, J. A. (2019). The impact of supply chain collaboration on performance in automotive industry: Empirical evidence. *Journal of Industrial Engineering and Management*, 12(2), 241–253. <https://doi.org/10.3926/jiem.2835>
- Alharby, M., & Van Moorsel, A. (2017). *Blockchain-based smart contracts: A systematic mapping study*. arXiv:1710.06372. <https://doi.org/10.5121/csit.2017.71011>
- Angelis, J., & da Silva, E. R. (2019). Blockchain adoption: A value driver perspective. *Business Horizons*, 62(3), 307–314. <https://doi.org/10.1016/j.bushor.2018.12.001>
- Azzi, R., Chamoun, R. K., & Sokhn, M. (2019). The power of a blockchain-based supply chain. *Computers & Industrial Engineering*, 135, 582–592. <https://doi.org/10.1016/j.cie.2019.06.042>
- Badi, S., Ochieng, E., Nasaj, M., & Papadaki, M. (2021). Technological, organisational and environmental determinants of smart contracts adoption: UK construction sector viewpoint. *Construction Management and Economics*, 39(1), 36–54. <https://doi.org/10.1080/01446193.2020.1819549>
- Barratt, M., & Oke, A. (2007). Antecedents of supply chain visibility in retail supply chains: A resource-based theory perspective. *Journal of Operations Management*, 25(6), 1217–1233. <https://doi.org/10.1016/j.jom.2007.01.003>
- Benitez, G. B., Ayala, N. F., & Frank, A. G. (2020). Industry 4.0 innovation ecosystems: An evolutionary perspective on value cocreation. *International Journal of Production Economics*, 228, 107735. <https://doi.org/10.1016/j.ijpe.2020.107735>
- Brandon-Jones, E., Squire, B., Autry, C. W., & Petersen, K. J. (2014). A contingent resource-based perspective of supply chain resilience and robustness. *Journal of Supply Chain Management*, 50(3), 55–73. <https://doi.org/10.1111/jscm.12050>

- Brusset, X. (2016). Does supply chain visibility enhance agility? *International Journal of Production Economics*, 171, 46–59. <https://doi.org/10.1016/j.ijpe.2015.10.005>
- Chang, S. E., Chen, Y. C., & Lu, M. F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change*, 144, 1–11. <https://doi.org/10.1016/j.techfore.2019.03.015>
- Chen, J., Xia, X., Lo, D., Grundy, J., & Yang, X. (2020). *Maintaining smart contracts on Ethereum: Issues, techniques, and future challenges*. arXiv:2007.00286.
- Chia, V., Hartel, P., Hum, Q., Ma, S., Piliouras, G., Reijnders, D., Staalduinen, M. Van, & Szalachowski, P. (2018). Rethinking blockchain security: Position paper. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1273–1280). IEEE. https://doi.org/10.1109/Cybermatics_2018.2018.00222
- Choo, K. K. R., Dehghantanha, A., & Parizi, R. M. (Eds.). (2020). *Advances in information security: Vol. 79. Blockchain cybersecurity, trust and privacy*. Springer Nature. <https://doi.org/10.1007/978-3-030-38181-3>
- Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management*, 34(5), 388–396. <https://doi.org/10.1108/09600030410545436>
- Çolak, M., Kaya, I., Özkan, B., Budak, A., & Kardeş, A. (2020). A multi-criteria evaluation model based on hesitant fuzzy sets for blockchain technology in supply chain management. *Journal of Intelligent & Fuzzy Systems*, 38(1), 935–946. <https://doi.org/10.3233/JIFS-179460>
- De Giovanni, P. (2020). Blockchain and smart contracts in supply chain management: A game theoretic model. *International Journal of Production Economics*, 228, 107855. <https://doi.org/10.1016/j.ijpe.2020.107855>
- Demir, M., Alalfi, M., Turetken, O., & Ferworn, A. (2019). Security smells in smart contracts. In *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 442–449). IEEE. <https://doi.org/10.1109/QRS-C.2019.00086>
- Domingo, R. S., Piñero-Chousa, J., & López-Cabarcos, M. Á. (2020). What factors drive returns on initial coin offerings? *Technological Forecasting and Social Change*, 153, 119915. <https://doi.org/10.1016/j.ijpe.2020.107855>
- Dubey, R., & Altay, N. (2018). Drivers of coordination in humanitarian relief supply chains. In *The Palgrave handbook of humanitarian logistics and supply chain management* (pp. 297–325). Palgrave Macmillan. https://doi.org/10.1057/978-1-137-59099-2_10
- Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Blome, C., & Luo, Z. (2017). Antecedents of resilient supply chains: An empirical study. *IEEE Transactions on Engineering Management*, 66(1), 8–19. <https://doi.org/10.1109/TEM.2017.2723042>
- Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Luo, Z., & Roubaud, D. (2020). Upstream supply chain visibility and complexity effect on focal company's sustainable performance: Indian manufacturers' perspective. *Annals of Operations Research*, 290(1), 343–367. <https://doi.org/10.1007/s10479-017-2544-x>
- Dujak, D., & Sajter, D. (2019). Blockchain applications in supply chain. In A. Kawa & A. Maryniak (Eds.), *SMART supply network* (pp. 21–46). Springer, Cham. https://doi.org/10.1007/978-3-319-91668-2_2
- Falcone, E. C., Steelman, Z. R., & Aloysius, J. A. (2021). Understanding managers' reactions to blockchain technologies in the supply chain: The reliable and unbiased software agent. *Journal of Business Logistics*, 42(1), 25–45. <https://doi.org/10.1111/jbl.12263>
- Fawcett, S. E., Osterhaus, P., Magnan, G. M., Brau, J. C., & McCarter, M. W. (2007). Information sharing and supply chain performance: The role of connectivity and willingness. *Supply Chain Management: An International Journal*, 12(5), 358–368. <https://doi.org/10.1108/13598540710776935>

- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. <https://doi.org/10.1177/002224378101800104>
- Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, 2(1), 2. <https://doi.org/10.3390/logistics2010002>
- Frazier, G. L., Maltz, E., Antia, K. D., & Rindfleisch, A. (2009). Distributor sharing of strategic information with suppliers. *Journal of Marketing*, 73(4), 31–43. <https://doi.org/10.1509/jmkg.73.4.031>
- Ghorbani, A., Danaei, A., Zargar, S. M., & Hematian, H. (2019). Designing of smart tourism organization (STO) for tourism management: A case study of tourism organizations of South Khorasan province, Iran. *Heliyon*, 5(6), e01850. <https://doi.org/10.1016/j.heliyon.2019.e01850>
- Ha, B. C., Park, Y. K., & Cho, S. (2011). Suppliers' affective trust and trust in competency in buyers: Its effect on collaboration and logistics efficiency. *International Journal of Operations & Production Management*, 31(1), 56–77. <https://doi.org/10.1108/01443571111098744>
- Habib, M. A., Sardar, M. B., Jabbar, S., Faisal, C. N., Mahmood, N., & Ahmad, M. (2020). Blockchain-based supply chain for the automation of transaction process: Case study based validation. In *2020 International Conference on Engineering and Emerging Technologies (ICEET)* (pp. 1–7). IEEE. <https://doi.org/10.1109/ICEET48479.2020.9048213>
- Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage publications.
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152. <https://doi.org/10.2753/MTP1069-6679190202>
- Hamledari, H., & Fischer, M. (2021). *Measuring the impact of blockchain and smart contract on construction supply chain visibility*. arXiv:2104.07532.
- He, D., Deng, Z., Zhang, Y., Chan, S., Cheng, Y., & Guizani, N. (2020). Smart contract vulnerability analysis and security audit. *IEEE Network*, 34(5), 276–282. <https://doi.org/10.1109/MNET.001.1900656>
- Hechler, E., Oberhofer, M., & Schaeck, T. (2020). AI and Blockchain. In *Deploying AI in the enterprise* (pp. 253–271). Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6206-1_11
- Javid, U., Aman, M. N., & Sikdar, B. (2019). DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts. In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)* (pp. 1–5). IEEE. <https://doi.org/10.1109/VTCSpring.2019.8746499>
- Kim, J. S., & Shin, N. (2019). The impact of blockchain technology application on supply chain partnership and performance. *Sustainability*, 11(21), 6181. <https://doi.org/10.3390/su11216181>
- Kirkman, S. (2018). A data movement policy framework for improving trust in the cloud using smart contracts and blockchains. In *2018 IEEE International Conference on Cloud Engineering (IC2E)* (pp. 270–273). IEEE. <https://doi.org/10.1109/IC2E.2018.00054>
- Clueber, R., & O'Keefe, R. M. (2013). Defining and assessing requisite supply chain visibility in regulated industries. *Journal of Enterprise Information Management*, 26(3), 295–315. <https://doi.org/10.1108/17410391311325243>
- Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80–89. <https://doi.org/10.1016/j.ijinfomgt.2017.12.005>
- Kumar, R. S., Pugazhendhi, S., Muralidharan, C., & Murali, S. (2018). An empirical study on effect of information sharing on supply chain performance – the case of Indian automotive industry. *International Journal of Logistics Systems and Management*, 31(3), 299–319. <https://doi.org/10.1504/IJLSM.2018.095821>
- Kurniawan, R., Zailani, S. H., Iranmanesh, M., & Rajagopal, P. (2017). The effects of vulnerability mitigation strategies on supply chain effectiveness: Risk culture as moderator. *Supply Chain Management: An International Journal*, 22(1), 1–15. <https://doi.org/10.1108/SCM-12-2015-0482>

- Li, Q., & Wang, L. (2021). Research on the information sharing in the linkage between manufacturing and logistics industry based on blockchain. *Journal of Physics: Conference Series*, 1774(1), 012055. <https://doi.org/10.1088/1742-6596/1774/1/012055>
- Li, S., Cui, X., Huo, B., & Zhao, X. (2019). Information sharing, coordination and supply chain performance: The moderating effect of demand uncertainty. *Industrial Management & Data Systems*, 119(5), 1046–1071. <https://doi.org/10.1108/IMDS-10-2018-0453>
- Lotfi, Z., Mukhtar, M., Sahran, S., & Zadeh, A. T. (2013). Information sharing in supply chain management. *Procedia Technology*, 11, 298–304. <https://doi.org/10.1016/j.protocy.2013.12.194>
- Moberg, C. R., Cutler, B. D., Gross, A., & Speh, T. W. (2002). Identifying antecedents of information exchange within supply chains. *International Journal of Physical Distribution & Logistics Management*, 32(9), 755–770. <https://doi.org/10.1108/09600030210452431>
- Montes, J. M., Ramirez, C. E., Gutierrez, M. C., & Larios, V. M. (2019, October). Smart Contracts for supply chain applicable to Smart Cities daily operations. In *2019 IEEE International Smart Cities Conference (ISC2)* (pp. 565–570). IEEE. <https://doi.org/10.1109/ISC246665.2019.9071650>
- Moosavi, J., Naeni, L. M., Fathollahi-Fard, A. M., & Fiore, U. (2021). Blockchain in supply chain management: A review, bibliometric, and network analysis. *Environmental Science and Pollution Research*, 1–15. <https://doi.org/10.1007/s11356-021-13094-3>
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Manubot.
- Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. (2021). The revolution of blockchain: State-of-the-art and research challenges. *Archives of Computational Methods in Engineering*, 28(3), 1497–1515. <https://doi.org/10.1007/s11831-020-09426-0>
- Panahifar, F., Byrne, P. J., Salam, M. A., & Heavey, C. (2018). Supply chain collaboration and firm's performance: The critical role of information sharing and trust. *Journal of Enterprise Information Management*, 31(3), 358–379. <https://doi.org/10.1108/JEIM-08-2017-0114>
- Park, S., Yu, H., & Chang, H. (2021). Design of the required tasks of industrial security experts based on job openings. *Security Journal*. <https://doi.org/10.1057/s41284-020-00279-7>
- Piñeiro-Chousa, J., López-Cabarcos, M. Á., & Ribeiro-Soriano, D. (2021). The influence of financial features and country characteristics on B2B ICOs' website traffic. *International Journal of Information Management*, 59, 102332. <https://doi.org/10.1016/j.ijinfomgt.2021.102332>
- Prajogo, D., Toy, J., Bhattacharya, A., Oke, A., & Cheng, T. C. E. (2018). The relationships between information management, process management and operational performance: Internal and external contexts. *International Journal of Production Economics*, 199, 95–103. <https://doi.org/10.1016/j.ijpe.2018.02.019>
- Queiroz, M. M., Fosso Wamba, S., De Bourmont, M., & Telles, R. (2020). Blockchain adoption in operations and supply chain management: Empirical evidence from an emerging economy. *International Journal of Production Research*, 1–17. <https://doi.org/10.1080/00207543.2020.1803511>
- Rogerson, M., & Parry, G. C. (2020). Blockchain: case studies in food supply chain visibility. *Supply Chain Management: An International Journal*, 25(5), 601–614. <https://doi.org/10.1108/SCM-08-2019-0300>
- Saqib, Z. A., & Zhang, Q. (2021). Impact of sustainable practices on sustainable performance: The moderating role of supply chain visibility. *Journal of Manufacturing Technology Management*, 32(7), 1421–1443. <https://doi.org/10.1108/JMTM-10-2020-0403>
- Shin, D. D. (2019). Blockchain: The emerging technology of digital trust. *Telematics and Informatics*, 45, 101278. <https://doi.org/10.1016/j.tele.2019.101278>
- Singh, C. S., Soni, G., & Badhotiya, G. K. (2019). Performance indicators for supply chain resilience: Review and conceptual framework. *Journal of Industrial Engineering International*, 15(1), 105–117. <https://doi.org/10.1007/s40092-019-00322-2>

- Somapa, S., Cools, M., & Dullaert, W. (2018). Characterizing supply chain visibility – a literature review. *The International Journal of Logistics Management*, 29(1), 308–339. <https://doi.org/10.1108/IJLM-06-2016-0150>
- Sunmola, F., & Apeji, D. U. (2020). Blockchain characteristics for sustainable supply chain visibility. In *5th NA International Conference on Industrial Engineering and Operations Management*. Detroit, Michigan, USA.
- Szabo, N. (1997). The idea of smart contracts. *Nick Szabo's Papers and Concise Tutorials*, 6(1).
- Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In *2016 13th International Conference on Service Systems and Service Management (ICSSSM)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICSSSM.2016.7538424>
- Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management: An International Journal*. <https://doi.org/10.2139/ssrn.3224145>
- Valero, S., Climent, F., & Esteban, R. (2020). Future banking scenarios. Evolution of digitalisation in Spanish banking. *Journal of Business Accounting and Finance Perspectives*, 2(2), 13. <https://doi.org/10.35995/jbafp2020013>
- Xing, C., Chen, Z., Chen, L., Guo, X., Zheng, Z., & Li, J. (2020). A new scheme of vulnerability analysis in smart contract with machine learning. *Wireless Networks*, 1–10. <https://doi.org/10.1007/s11276-020-02379-z>
- Yu, M. C., & Goh, M. (2014). A multi-objective approach to supply chain visibility and risk. *European Journal of Operational Research*, 233(1), 125–130. <https://doi.org/10.1016/j.ejor.2013.08.037>
- Zhu, S., Song, J., Hazen, B. T., Lee, K., & Cegielski, C. (2018). How supply chain analytics enables operational supply chain transparency. *International Journal of Physical Distribution & Logistics Management*, 48(1), 47–68. <https://doi.org/10.1108/IJPDLM-11-2017-0341>
- Zhuo, N., Ji, C., & Yin, N. (2021). Supply chain integration and resilience in China's pig sector: Case study evidences from emerging institutional arrangements. *Environmental Science and Pollution Research*, 28(7), 8310–8322. <https://doi.org/10.1007/s11356-020-11130-2>