DOI: 10.1002/jsc.2484

RESEARCH ARTICLE

WILEY

The influence of blockchains and internet of things on global value chain

Arthur Egwuonwu | **Chima Mordi** | **Ambrose Egwuonwu** | **Olayinka Uadiale**

Brunel University London, Uxbridge, UK

Correspondence
Arthur Egwuonwu, Brunel Business School,
Brunel University London, Uxbridge,
Middlesex UB8 3PH, UK.
Email: arthur.egwuonwu@brunel.ac.uk

Abstract

Despite the increasing proliferation of deploying the internet of things (IoT) in the global value chain (GVC), several challenges might lead to a lack of trust among value chain partners, for example, technical challenges (i.e., confidentiality, authenticity, and privacy); and security challenges (i.e., counterfeiting, physical tampering, and data theft). In this study, we argue that blockchain technology (BT), when combined with the IoT ecosystem, will strengthen GVC and enhance value creation and capture among value chain partners. Therefore, we examine the impact of BT combined with the IoT ecosystem and how it can be utilized to enhance value creation and capture among value chain partners. We collected data through an online survey, and 265 U.K. Agri-food retailers completed the survey. Our data were analyzed using structural equation modeling. Our finding reveals that BT enhances GVC by improving IoT scalability, security, and traceability combined with the IoT ecosystem. Moreover, the combination of BT and IoT strengthens GVC and creates more value for value chain partners, which serves as a competitive advantage. Finally, our research outlines the theoretical and practical contribution of combining BT and the IoT ecosystem.

KEYWORDS
blockchain technology, global value chain, internet of things, technical challenges, value creation

JEL CLASSIFICATION
L14, M15, O33

1 | INTRODUCTION

The concept of internet of things (IoT) has been around for nearly 20 years, and it first appeared in the late 1990s. The term was coined in the context of global value chain (GVC) by Kevin Ashton, a British scientist while working on a research project at the Massachusetts Institute of Technology's Auto-ID center to study options to strengthen operational efficiency by connecting radio frequency identification (RFID) information technology (IT) to the Internet (de Vass, Shee, & Miah, 2021). Presently, there is no universal definition of IoT; however, it refers to integrating physical items that communicate with each other over the Internet to achieve a specific outcome (Borgia, 2014; de Vass et al., 2021; Whitmore, Agarwal, & Xu, 2014).

IoT enables a secure and trustworthy transfer of information about products and services in a GVC (Mishra et al., 2016). Moreover, IoT can increase the attractiveness of GVC by censoring product/service distribution more effectively, leading to an enhanced change in vital processes and timely schedules (Mital, Chang, Choudhary, Papa, & Pani, 2018). Li et al. (2011) highlighted that the IoT ecosystem could help to shorten the feedback circle, allowing for a fasters decision-making facilitate which helps to mitigate delay risk and improve the efficiency of the transmitting information related to production, locations of goods, quality assurance, distribution, and logistics. Therefore, when implemented into the GVC, it can improve efficiency, minimize operating costs, and increase customer loyalty (Rejeb, Keogh, & Treiblmaier, 2019).

While IoT's possible advantages in GVC are well recognized in the literature, the concept yet carries several challenges (Haddud, Desouza, Khare, & Lee, 2017). For instance, all value chain stakeholders have technical issues such as authenticity, confidentiality, and privacy (Tzounis, Katsoulas, Bartzanas, & Kittas, 2017). Ahlmeyer and Chircu (2016) highlight that security is the most important concern in IoT applications. Correspondingly, Dorri, Kanhere, Jurdak, and Gauravaram (2017) state that current security systems do not fit properly, as existing IoT platforms can be heavy energy-consuming. In addition to security challenges, problems such as forgeries, cloud data theft, product tampering, and hacking could lead to mistrust between value chain associates (Rejeb et al., 2019). Hence, it is crucial to shield IoT against cyberattacks (Tzounis et al., 2017).

To protect IoT against external attacks and enhance the trust of connected smart devices in GVC, blockchains, if embedded with the IoT systems, can provide solutions to the IoT challenges as mentioned earlier (Clohessy & Clohessy, 2020; Clohessy, Treiblmaier, Acton, & Rogers, 2020; Rejeb et al., 2019). Blockchains are sets of distributed networks that provide data integrity across many transactional parties by providing all participants in the ecosystem with a working proof of decentralized trust without the assistance of intermediaries (Clohessy & Clohessy, 2020). Blockchains are also known as a *"ledger"* that logs transaction records into blocks created by nodes where each block has a header, the relevant transaction data to be protected, and ancillary security metadata (e.g., creator identity, signature, last block number, and so on.) (Minoli & Occhiogrosso, 2019, p. 5). Blockchain technology (BT) will enhance information transparency, improve trust among value chain stakeholders, and support interoperability (Clohessy et al., 2020; Rejeb et al., 2019). Consequently, embedding blockchains with other technologies has gained considerable attention in GVC literature (Casado-Vara, Prieto, & Corchado, 2018). Moreover, digitalization has transformed the modern GVC (Hirsch-Kreinsen, 2016). According to Helmerich, Raj-Reichert, and Zajak (2020), digitalization has turned GVC into value-creating networks, with the value chain being a critical source of sustainable competitive advantage for organizations. Likewise, scholars are developing research that combines BT with IoT ecosystems, resulting in innovative value chain systems, new alliances, and new forms of coordination and value generation across value chain networks (Rejeb et al., 2019). However, these studies are mainly review or conceptual papers with no empirical analysis.

Therefore, our research aims to empirically examine the impact of BT when combined with the IoT ecosystem on GVC, and how it can be utilized to enhance value creation and capture among value chain partners. More specifically, our research attempts to answer the following two main research questions:

> **RQ1.** How does BT, when combined with the IoT ecosystem, affect GVC?
>
> **RQ2.** To what extent does BT, when combined with IoT, enhance value creation and capture among GVC partners?

This research focuses on the U.K. Agri-food retail sector. The retail sector is at the forefront of adopting IoT to tackle the challenges faced by its new operations and business needs (Nurgazina, Pakdeetrakulwong, Moser, & Reiner, 2021). Acknowledging that Agri-food retailers have close interaction with their consumers, digital connectivity with distributors is essential for timely and complete restocking products to ensure stock availability. The U.K. Agri-food retail industry was chosen for the research since prior studies have shown the coexistence of different IoT types. For instance, Zhao, Zuo, and Blackhurst (2019), in their recent review research, highlighted that U.K. Agri-food retailers use IoT in various ways, including GPS, and RFID-based location tracker, internet-based barcode readers, sensors and scanners, palm-held tablets/smart devices, smartphones, mobile apps, and internet-based security and surveillance, with at least a single form of IoT in each supply chain.

Similarly, Fu and Fu (2012) highlighted some other IoT technologies that delivery drivers mostly use across the United Kingdom, such as sensor systems that aid in collecting vehicle navigation systems, location to allow proactive alert system and camera-based technology to increase safe driving and reduce exhaustion. Other research documented a range of IoT systems that allows integration of supply chain activities among exchange partners (de Vass et al., 2021). Accordingly, this study's assertion that BT, when combined with the IoT ecosystem, will strengthen GVC and enhance value creation and capture among GVC partners.

The remainder of this article is organized as follows. First is the background literature on IoT, the application of IoT to GVC and BT. Second is the conceptual model development, which paved the way for the research methodology and the reports on the quantitative findings. The paper then discusses the results and theoretical and managerial implications. Finally, the paper concludes with study limitations.

2 | LITERATURE REVIEW

2.1 | The concept of IoT

IoT is constituted of three major components: web-based (middleware), thing-based (e.g., sensors), and semantic-based (knowledge). IoT was described by Mital et al. (2018) as intelligent and self-configuring nodes (things) integrated into a dynamic and global network infrastructure. It is a disruptive technology that enables ubiquitous and pervasive computing applications. It is also defined as a network of hardware, software, devices, databases, objects, sensors, and systems that all work together to improve lives (Rong, Hu, Lin, Shi, & Guo, 2015). RFID technology is a fundamental technology for the IoT allowing microchips to wirelessly communicate identification information to a reader (Reaidy, Gunasekaran, & Spalanzani, 2015). The IoT enables physical things to see, hear, think, and perform tasks by allowing them to "talk" to each other, share information, and coordinate choices. These physical objects become smart by utilizing underlying technology such as ubiquitous and pervasive computing, embedded devices, communication technologies, sensor networks, internet protocols, and applications (Mital et al., 2018). Gartner identifies the top 10 IoT technologies for 2017 and 2020 (Gartner Top Technology Trends, 2022) (see Table 1).

TABLE 1 IoT technologies for 2017 and 2020

Technology	Explanation
IoT security	Security measures will be necessary to safeguard IoT devices and applications from both information assaults and physical manipulation.
IoT analytics	Sophisticated analytics tools and algorithms are required now, but as data volumes rise through 2021, IoT demands may drift even more from machine learning.
IoT device (thing) management	The IoT also introduces new scalability issues to the project implementation. Tools must be able to manage and monitor hundreds, if not millions, of devices.
Short-range IoT networks	Through 2025, low-power, short-range networks will dominate wireless IoT connectivity, greatly outnumbering connections via wide-area IoT networks.
Wide-area networks	A wide-area IoT network's long-term goal is to provide download speeds ranging from hundreds of bits per second (bps) to tens of kilobits per second (kbps), with nationwide coverage, a battery life of up to 10 years, endpoint hardware costing less than $5, and support for hundreds of thousands of connected devices to a base station or its similar.
IoT processors	Many of the capabilities of IoT devices are defined by their processors and architectures, such as whether they are capable of strong security and encryption, power consumption, and whether they are sophisticated enough to support an operating system, updatable firmware, and embedded device management agents.
IoT operating systems	A diverse set of IoT-specific operating systems has been created to accommodate a broad range of hardware footprints and feature requirements.
Event stream processing	DSCPs have evolved. They generally employ parallel architectures to analyze extremely high-rate data streams in order to accomplish tasks such as real-time analytics and pattern recognition.
IoT platforms	IoT platforms combine several of an IoT system's infrastructure components into a single product: (a) device control and operations at the lowest level; (b) IoT data gathering, translation, and administration; and (c) IoT application development
IoT standards and ecosystems	Standards and their related APIs will be critical because IoT devices will need to interoperate and communicate, and many IoT business models will rely on data sharing across various devices and organizations.

Abbreviations: APIs, application programming interfaces; DSCPs, distributed stream computing platforms; IoT, internet of things.

2.2 | IoT and GVC

Integration of the value chain is critical for enhancing corporate success. This may be accomplished by lowering costs, enhancing responsiveness, raising service levels, and making easier decisions. The fundamental aspects of value chain integration include information exchange and cooperation, and agility (Guo, Yu, Zhou, & Zhang, 2012; Tan & Wang, 2010). In terms of GVC, the IoT may enable machine-enabled decision making with little or no human interaction. It is concerned with integrating and enabling information communication technologies such as RFID, wireless sensor networks, machine-to-machine systems, and mobile apps (Rejeb et al., 2019). The application of IoT in the GVC may provide visibility to each item, resulting in a highly transparent value chain. The position and attributes of all objects in the value chain could be determined at any time (Nagy, Oláh, Erdei, Máté, & Popp, 2018). IoT application within the GVC leads to increased profitability, reduced surplus goods that quickly lose value, faster reaction to changing customer demands or supplier availability, and greater shipping optimization and guarantee of complete deliveries (Wielki, 2017). Firms that adjust to the rapid expansion of IoT will reap more benefits and gain a competitive advantage in the new business climate (Atzori et al., 2018).

2.3 | Challenges of IoT in GVC

Although the IoT has several benefits in the GVC (e.g., it optimizes value chain operations, enhance information transparency, and improves the integrity of production data and the identity of products; however, the need for security becomes very important. According to Khan, Khan, Zaheer, and Khan (2012), 70% of IoT systems had defective conditions because of lack of encryption, insecure protocols, insufficient software coverage and incomplete authorization. However, they are conventional security measures used in IoT (e.g., trusted platform modules for authentication and trusted network connect to check for malicious firmware) (Rejeb et al., 2019). Cam-Winget, Sadeghi, and Jin (2016) contend that conventional security technologies do not meet real-time standards because of scalability problems to process and interpret data distributed from vast networks of embedded systems. Moreover, the IoT network's traditional security and privacy measures are now considered irrelevant since its complex nature (Ferretti & Schiavone, 2016). Subsequently, IoT systems do not have a service level arrangement to protect the personally identifiable information required by regulatory standards. As a result, it can adversely affect data confidentiality and security and negatively affect personal and organizational privacy protection (Kim-Hung, Datta, Bonnet, Hamon, & Boudonne, 2017).

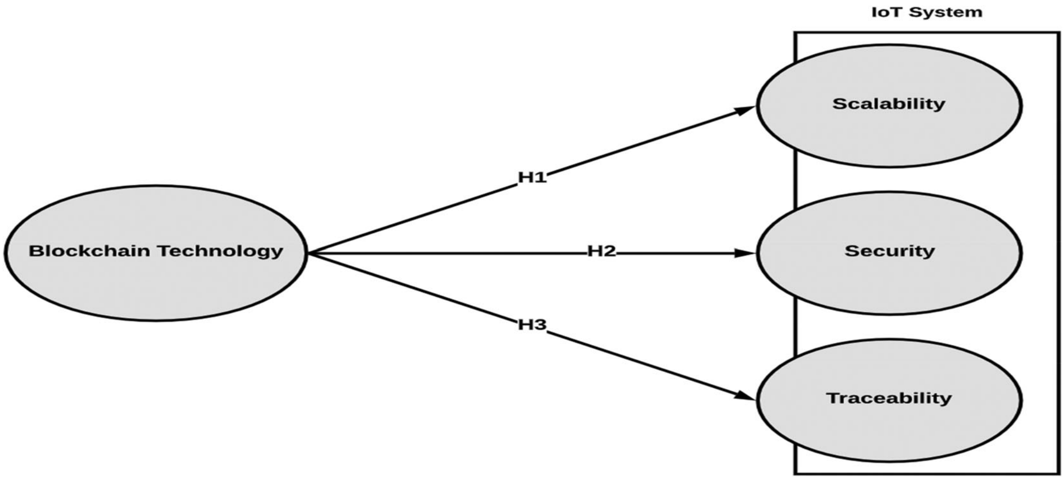

FIGURE 1 The impact of Blockchain technology on IoT system

The implementation of IoT in GVC involves system centralization. Abdel-Basset, Manogaran, and Mohamed (2018) state that centralization may lead to skepticism or mistrust, which may restrict the organization's development of supply chain operations. A central data hosting and management strategy will contribute to a range of operational risk and organizational problems relating to information transparency, protection, and privacy (Fang, Liu, Pardalos, & Pei, 2015). For instance, in other world areas, cloud-based IoT solutions can be subject to problems resulting in privacy regulations when exporting comprehensive classified and susceptible data to external providers (Fang, Liu, Pardalos, & Pei, 2015). Furthermore, cloud-based solutions can induce obscurity and increase information asymmetry between value chain clients; however, blockchain technologies can help solve many of these challenges (Rejeb et al., 2019).

2.4 | Blockchain technology

BT is a public ledger mechanism that maintains transaction information confidentiality and is recognized primarily as a Bitcoin cryptocurrency (Clohessy et al., 2020). It was first used after introducing the Bitcoin cryptocurrency, and to this day, Bitcoin is still the most commonly used application using blockchains (Rejeb, Keogh, Zailani, Treiblmaier, & Rejeb, 2020). Clohessy, Treiblmaier, Acton, and Rogers (2020, p. 547) defined BT as a "digital, decentralized and distributed ledger in which transactions are logged and added in chronological order to create permanent and tamperproof records." BT is a modem computing system for encrypting, storing, and sharing data between multiple nodes in a network (Tapscott & Tapscott, 2017). A blockchain differs from the conventional centralized solution by processing data over a distributed and integrated node network (Treiblmaier, 2019). According to Treiblmaier (2019), blockchains' critical features are shared recordkeeping, immutability, decentralization, distributed trust, and consensus.

BT can be programmed to record, encrypt, and store day-to-day supply chain transactions data using an intelligent encryption procedure based on conditions the network has agreed upon. The blockchain system can support multiple global supply chain transactions by encrypting user identities, allowing access and boosting transaction recordkeeping (Tapscott & Tapscott, 2017). The functionality of the blockchains is possible through the cryptographic mechanism and recursive hashing of blocks. Rejeb et al. (2019) argue that BT and the IoT network share comparable characteristics; as such, the centralized approach used in supply chain operations to collect, store, and analyze supply chain transaction data may cause delays and lead to a situation called "single point of failure." Consequently, BT can address the IoT challenges highlighted above by providing a trust-based decentralization to value chain exchange partners (Clohessy & Clohessy, 2020). In essence, the absence of centralized control of blockchains, the use of resources of all nodes and removal of multiple traffic flows guarantees a high degree of scalability and stability (Nofer, Gomber, Hinz, & Schiereck, 2017).

From the literature review on IoT, the application of IoT to GVC and the integration of blockchains in IoT systems, a conceptual model can be developed to portray the impact of IoT on GVC when combined with BT (see Figure 1). More specifically, the conceptual model depicts BT's influence on value chain IoT scalability, security, and traceability.

3 | HYPOTHESES DEVELOPMENT

3.1 | The influence of BT on IoT scalability

Rejeb et al. (2019) argue that creating scalable BT (e.g., proof of stake and proof of work) will significantly enhance IoT scalability for value chain operations. Additionally, IoT-specific network configuration will benefit from blockchain integration and allow for designing content-focused consensus mechanisms (Viriyasitavat & Hoonsopon, 2019). Blockchain can be particularly well-suited for enabled distribution networks wherein the active chain within the blockchains levers fewer recurrent transnational transactions (e.g., international distribution). In contrast, the less active chain within the blockchain is nurtured for keeping frequent local transactions (e.g., national/local distributions) (Khan & Salah, 2018). These progressive measures would collectively increase sensory data's completeness by cross-validating sensory data from other IoT nodes and historical data (Clohessy & Clohessy, 2020).

BT has a finite number of nodes and IoT data filters, which could help multiple value chain applications improve scalability (Wang et al., 2019). According to Rejeb et al. (2019), blockchains is changing cloud computing technology to facilitate greater IoT scalability and mobility levels. For instance, the IBM Watson IoT blockchain operates in a cloud environment and helps to process massive amounts of data among heterogeneous devices (Kshetri, 2017). To enable and maintain IoT devices in a trust-free ecosystem, Pan et al. (2020, p. 7) suggest the "combination of service-centric networking and blockchains, in which the blockchain is backed up by the omnipresent of IoT system mobility will ensure scalability." Based on the above discussion, we hypothesize the following:

Hypothesis H1. *BT is positively related to IoT scalability in the GVC.*

3.2 | The influence of BT on IoT security

Empirical research suggests that BT can significantly secure IoT system applications in GVC (Khan & Salah, 2018). According to Morales-Molina et al. (2021), value chain exchange partners are now driven to secure their data and information exchanges as well as the integrity of their physical objects to protect against theft and various forms of illicit trade, including diversion and counterfeiting, due to the increasing complexity of supply chains and the proliferation. For instance, organizations need to keep pace with the continuous development of covert, overt forensic technologies to secure or monitor their entire value chain activities (Xu, Trappe, Zhang, & Wood, 2005). As such, blockchain and IoT ecosystem are two complementing emerging technologies that can enhance productivity and assist in assuring the integrity and trust demanded by value chain exchange cohorts (Rejeb et al., 2020).

BT provides a trustworthy decentralized management system that tracks every point in the value chain activities (Khan & Salah, 2018). These activities can include multiple players such as warehouse operations, transportation and distribution (Haddud et al., 2017). BT mitigates the risk of what is commonly known as a "single point of failure" due to its decentralization approach (Borgia, 2014). Mainly, BT helps eliminate the risk of network failure and collapse in a node crash, thus enhancing IoT devices used in value chain activities (Geerts & O'Leary, 2014). BT can foster the protection of a value chain IoT from most malicious attacks (Woodside et al., 2017). Moreover, Siegfried, Rosenthal, and Benlian (2020) confirm BT's efficacy in securing an IoT device by facilitating communication between trustworthy nodes while avoiding malicious nodes. Therefore, BT restricts some selected devices' access and minimizes unauthorized access possibilities (Minoli & Occhiogrosso, 2018).

BT potentially offers a decentralized authentication that provides single and multiparty authentication to IoT devices (Ahmed, Ullah, Muhammad, & Pathan, 2020). The authentication enhances data transparency and trust once entered into the blockchain system. It is considered immutable and tamperproof (Inukollu, Arsi, & Ravuri, 2014). An attempt to manipulate or tamper with the data will be detected immediately and, retrospectively, traced back to its source (Martino et al., 2018). Consequently, GVC risk will be significantly reduced due to blockchains effective fraud detection protocol (Bahga & Madisetti, 2016). In addition, the application of BT in GVC can help validate the IoT ecosystem's identity. Moreover, the IoT system's protection against counterfeiting and forging commodities is achieved with the BT's tamper-resistant nature (Minoli & Occhiogrosso, 2018). Based on the above discussion, we hypothesize the following:

Hypothesis H2. *BT is positively related to IoT security in the GVC.*

3.3 | The influence of BT on IoT traceability

Blockchains, IoT, and RFID technologies have recently reshaped modern GVC operations with far-reaching implications for value chain traceability (Casino, Dasaklis, & Patsakis, 2019). For instance, an IoT system driven by RFID technology may be used to trace products and relevant conditions (e.g., temperature, appearance, damage, and humidity) when these products are transported and or distributed. The IoT ecosystem can also be used for counterfeit detections and value chain origin (Caro, Ali, Vecchio, & Giaffreda, 2018). Elmessiry and Elmessiry (2018) argue that a value chain traceability system is developed by integrating blockchain and IoT systems. Moreover, integrating blockchain and IoT in GVC allows for traceability along the process. It provides organization and their exchange partners with ample information about the product's originality, authenticity, and reliability to make an informed purchase decision. Based on the above discussion, we hypothesize the following:

Hypothesis H3. *BT is positively related to IoT traceability in the GVC.*

4 | RESEARCH METHODOLOGY

4.1 | Survey instrument development

To test our hypotheses, we first identified our constructs and developed our objects by critically analyzing the literature published in organizational studies, operational management, and computer science. Second, we adapted the items to fit the U.K. Agri-food retail industry. We derived our measurements from the pertinent literature (see Table 1). Specifically, BT was based on the work of Hughes et al. (2019) and was operationalized as a high-order reflective scale containing four items. For IoT scalability, all items were of this study adopted from the literature.

Regarding IoT security, items were based on the study of Ho-Sam-Sooi, Pieters, and Kroesen (2021). Moreover, we adopted the Zheng, Shou, and Yang (2021) scale with IoT traceability. To further evaluate the items' accuracy, we pretested the questionnaire with five academic professors and four retail managers of an Agri-food company to test for relevance, flow, and readability. For instance, we asked these experts to view the clarity and appropriateness of the measures purporting to tap the constructs. We also followed a 7-point Likert scale where *"strongly disagree" (1)* and *"strongly agree" (7)* endpoints evaluate measures for all latent variables and collect responses for all items. On this basis, we tested the material validity of the designs and their associated measurement items.

4.2 | Sampling design

Since the study's empirical context is based on U.K.'s Agri-food retail industry, the study constructs were grounded to examine the Agri-food value chain between partnering organizations, viewed from the focal organization's perspective. Informed by Dubey, Gunasekaran, Bryde, Dwivedi, and Papadopoulos's (2020) works, our measures were based on one key informant's perceptions. Due to the newness of data sharing tendency in the industry, it was difficult to access an Agri-food sector-oriented repository. We, therefore, matched the key informants' organization and company details from KOMPASS[1] with similar data from Bureau van Dijk Financial Analysis Made Easy database. Further, we ensured that the respondents were knowledgeable about BT and IoT systems in their GVC operations; we inserted a set of questions on a 7-point scale where *(1) "very low"* and *(7) "very high."* The survey questionnaire was only prepared in English, as English is the official language in the United Kingdom.

4.3 | Data collection

Data were collected following Dubey et al. (2020) tailored methodology. This method has been adopted by researchers investigating similar research interests to increase response rates (e.g., Dubey, Gunasekaran, Childe, Papadopoulos, et al., 2019; Dubey, Gunasekaran, Childe, Roubaud, et al., 2019; Dubey, Gunasekaran, Childe, Wamba, et al., 2019; Moshtari, 2016). We began our data collection in March 2020 and finished it in December 2020. Through email, we reached 960 participants with a package consisting of an invitation letter, which specifically outlined our research's intent, and with confirmation to each respondent that absolute privacy and confidentiality of their details will be upheld. We followed the initial invitation with reminder emails every 3 weeks, and as a result, we obtained 265 usable responses, providing a successful response rate of 27.9%. This response rate is low, although it is consistent with related research (e.g., Dubey et al., 2020; Moshtari, 2016). Our research's key informants were senior managers in their organizations (e.g., CEO or Chairman, Retail/Operations/Logistics/Supply Chain managers). Their profiles are shown in (Table 2). Our respondents were divided as follows: 20% of animal feed additives and supplements, 34.3% fertilizers and herbicides, 17.9% dairy products, 22.2% of spicy and herbs product company, and 7% of food restaurants that offer deliveries. These companies operate within England, Scotland, Wales, and Northern Island.

Following Armstrong and Overton (1977), we tested the response bias by comparing each measurement item's response between the early and the late response. The test assumes that the late respondents are equivalent to nonrespondents (Armstrong & Overton, 1977). We found no statistically significant differences for every measurement item. We observed ($p > .25$) between early and late respondents in responses for all measurement items. Therefore, nonresponse bias is not a concern in our research.

5 | FINDING

We analyzed in two steps using the structural equation modeling (SEM) program on AMOS 26. The first phase provides details on the measurement model and explains the method of data purification. In the next step, we present the results of the structural model.

5.1 | Measurement model

We evaluated the relationship between the constructs and their indicators using the confirmatory factor analysis (CFA), where a primary determining factor constrained all observable items. At the same time, the underlying variables were allowed to correlate (Anderson & Gerbing, 1988). The elliptical reweighted least square technique was used to approximate the calculation model, showing a reasonable fit to the data (X^2/df 1.539, $p = .000$; standard fit index [NFI] 0.91; nonstandard fit index [NNFI] 0.90; comparative fit index [CFI] 0.92, and root mean square error of approximation [RMSEA] 0.05) (Diamantopoulos & Siguaw, 2009) (see Table 3).

TABLE 2 Profile of the respondents

Organizations main service	Frequency ($n = 265$)	Percentage ($n = 265$)
Animal feed additives and supplements	53	20
Fertilizers and herbicides	88	34.3
Dairy products	46	17.9
Spicy and herbs product company	57	22.2
Food restaurants that offer deliveries	18	7

TABLE 3 Reflective constructs and items for construct measurement

Factors and items	Standardized loadings	Cronbach's alpha	Composite reliability	AVE
Please indicate to what degree you agree with the following statement:				
Blockchain technology (mean 4.52, *SD* = 1. 19)				
BT1: We use ledger technology to ensure integrity	0.852	.71	2.16	0.51
BT2: We use ledger technology to improve transparency	0.807			
BT3: We use ledger technology to improve traceability	0.775			
BT4: We use ledger technology to ensure security and privacy	0.861			
Scalability (mean 4.34, *SD* = 1. 12)				
Scal1: Our IoT system is uniquely identifiable remotely to ensure scalability	0.865	.79	1.42	0.53
Scal2: Our IoT system is heterogeneous, capable of connecting devices from different systems and protocols	0.734			
Scal3: Our IoT system is has the ability to support increasing number of connected devices without degradation in quality of service	0.876			
Security (mean 4.67, *SD* = 1. 14)				
Sec1: We pay attention to the security risks of our IoT system	0.848	.75	2.19	0.70
Sec2: Security of our IoT systems is important to us	0.830			
Sec3: Information of our supply chain operations are protected sufficiently	0.810			
Traceability (mean 4.10, *SD* = 1. 50)				
Tra1: Our traceability system can effectively identify and trace product purchase to delivery	0.820	.84	2.87	0.63
Tra2: Our supply chain partners can be identified through our traceability system	0.805			
Tra3: Our traceability system can is able to identify and trace product purchase to delivery	0.852			

Note: Diagnostics for measurement model: X^2/df 1.539, $p = .000$, NFI 0.91, NNFI 0.90, CFI 0.92, RMSEA 0.05. Items fixed to set the scale.
Abbreviations: AVE, average variance derived; CFI, comparative fit index; IoT, internet of things; NFI, standard fit index; NNFI, non-standard fit index; RMSEA, root mean square error of approximation.

Convergent validation was obtained with respect to data refining; since the t-value was consistently high and significant for each predictor, all the standard errors of the predicted coefficients were shallow, and the average variance derived (AVE) for each latent variable was equal to and above the 0.50 minimum threshold (Hair, 2007). Discriminatory validity was also apparent as for each pair of constructs investigated, the confidence interval around the estimated correlation did not include 1.00 (Anderson & Gerbing, 1988). In contrast, the correlation for each pair of constructs did not surpass the AVE square root; (Fornell & Larcker, 1981) (see Table 3). The reliability of constructs was likewise satisfactory since the Cronbach alphas for all structures were greater than .70. The composite reliability test also exceeded the minimum threshold value of 0.70.

TABLE 4 Constructs correlation and discriminant validity

Constructs		1	2	3	4
Blockchain technology	1	0.71			
Scalability	2	0.42***	0.79		
Security	3	0.46***	0.25***	0.81	
Traceability	4	0.28*	0.41**	0.48**	0.75

Note: *$p < .05$, **$p < 01$, ***$p < 00$.

5.2 | Common method bias

We utilized a CFA technique to control common method bias, which constrained all variables to load in a specific factor (Venkatraman & Prescott, 1990). However, the goodness fit indices showed very low values far below the acceptable threshold (X^2/df 4.55136, $p = .000$; NFI 0.61; NNFI 0.75; CFI 0.82, and RMSEA 0.09). Then we employed a post hoc identification for the marker variable by defining the second-lowest positive link among our model structures (Malhotra, Kim, & Patil, 2006). Our results show no significant association with the other components of this marker variable. In contrast, the importance of the correlation coefficient did not alter following the different partial correlation modifications (Lindell & Whitney, 2001). The findings of the two experiments showed no common technique bias.

We next conducted a two-phase, smaller-square methodology to assess endogeneity potential in our study by utilizing the Social Sciences Statistics Package. As instrumental variables for all IoT variables, we leverage BT. The corresponding endogenous explanatory factors were linked to these instrumental factors. To check the robustness of instrumental variables with *F*-tests, we also examined the strength (Stock & Watson, 2011) and added an efficient model and a constant model. The tests at Durbin-Watson show that the F statistics for all

TABLE 5 Structural model results

Hypothesized association				Standard path coefficient	*t*-Value	*p*-Value
H1	Scalability	<—	Blockchain technology	.35	6.262	.000
H2	Security	<—	Blockchain technology	.34	6.083	.000
H3	Traceability	<—	Blockchain technology	.14	2.314	.021

Note: Model diagnostics X^2/df 1.535, $p = .000$, NFI 0.93, NNFI 0.92, CFI 0.93, RMSEA 0.04. *$p < .05$, **$p < .01$, ***$p < .00$.

instrumental variables were above 10 (Stock and Watson, 2011). So, in this research, common method bias is not a problem.

5.3 | Hypotheses tests

We employed the SEM approach to testing our hypotheses, using the elliptical reweighted least-squares technique. The SEM results demonstrated an acceptable model fit given the various indicators (X^2/df 1.535; NFI 0.93; NNFI 0.92; CFI 0.93, and RMSEA 0.04). Table 4 shows the standardized path coefficients with corresponding *t*-values for each hypothesis tested.

Hypotheses regarding the influence of BT on IoT scalability, IoT security, and IoT traceability were all supported. Specifically, in support of H1, BT impacts positively on the scalability of IoT ($\beta = .35$, $t = 6.26$, $p = .000$). Also, with H2, BT impacts positively on the security of IoT ($\beta = .34$, $t = 6.08$, $p = .000$) leads support to H2. Finally, as predicted in H3, BT impacts positively on traceability of IoT ($\beta = .14$, $t = 2.314$, $p = .002$) (see Table 5).

6 | DISCUSSION

The purpose of this study is to examine the impact of IoT on GVC when combined with BT and how it can be utilized to increase GVC and value-creating networks. As shown in Table 5, the findings of this study indicate that organizations are likely to benefit from adopting and integrating BT with IoT systems as perceived by the participants of this research. First, the hypothesis between BT and IoT scalability revealed a substantial connection, implying that when blockchains are combined with IoT systems, it allows the value chain network to operate adeptly without unnecessary delay while improving interoperability and the governance of IoT systems. This finding affirms the theoretical and empirical assumptions of scalability in IoT networks in GVC demonstrated in several studies (e.g., Haddud et al., 2017; Rejeb et al., 2019). Second, the interaction between BT and IoT security was positive and significant, indicating that combining BT with IoT would help organizations resolve security oversight, anonymity, trust, and accountability among various value chain partners. Third, there was a positive and significant correlation between BT and IoT traceability, denoting that BT improves stock tracking and traceability, inventory safety and management, and competitive advantage, enabling value chain efficiency and effectiveness. These findings support theoretical and empirical evidence in this field of study to improve value chain performance levels of Agri-food product replenishment processes, delivery and warehousing management by reducing inefficiencies and inaccuracy (Fan, Tao, Deng, & Li, 2015; Reaidy et al., 2015).

6.1 | Theoretical implication

This study contributes by empirically examining the impact of IoT on GVC when combined with BT and how it can be used to increase GVC and value-creating networks. Therefore, the findings of this study provide a wealth of knowledge about the impact of blockchain and IoT on GVC and how using this technology can increase value chain performance. Also, the study serves as a basis for incorporating blockchain and IoT technologies through GVC and a primary source for future research to understand further the business benefits of blockchain and IoT system integration and application. By and large, the findings of this study fill some of the holes in the literature found by previous studies. (e.g., Borgia, 2014; Clohessy et al., 2020; Clohessy & Clohessy, 2020; Haddud et al., 2017; Lee & Lee, 2015; Rejeb et al., 2019).

6.2 | Managerial implication

In addition to the discussed theoretical contributions, this study concludes with relevant blockchains and IoT integration for value chains organizations. GVC companies, especially in the United Kingdom and other parts of Europe, have recently begun allocating capital to implement blockchain and IoT initiatives. This proliferation of blockchains and IoT systems is due to its combined benefits. Blockchains embedded with IoT systems improve interoperability between multiple value chain organizations while generating valuable data (Clohessy & Clohessy, 2020). Furthermore, as BT is paired with IoT systems, value chain stakeholders will obtain new and timely insights into their supply chains in real time and more accurate and reliable knowledge about key operations, activities, and product attributes such as quality, performance, and availability. The integration of blockchains and IoT systems would help to improve end-to-end traceability and allow the rapid recall of unsafe products. As a result, exchange partners will be advised about the goods, possible risks, and protective and corrective measures required to ensure a continuous supply of healthy products to final customers. Therefore, this research attempted to generate valuable insights for top managers of retail companies supply chain and other professionals from manufacturing and service industries. Our finding is beneficial for supply chain companies that have adopted and applied local programs involving emerging innovations such as "smart things "and data analytics for blockchain technologies and IoT systems within their current operations.

Our research assists retail GVC executives in further understanding the functional effects of blockchain and IoT integration. Managers will gain a more comprehensive understanding of the possible advantages of blockchain and IoT integration. As a result of this insight, the organization will better understand the top elements and factors that should be considered and addressed in advance when adopting blockchains and IoT applications. Such understanding will lead to better strategic decisions about acquiring the suitable technologies required to implement blockchain and IoT integration. Moreover, it will result in implementing best practices to fulfill the organizations' quest to develop value chain effectiveness and efficiency through a better level of business competitiveness, which will, in turn, enhance value creation among value chain stakeholders. Consequently, the results should be used as solid proof to encourage GVC managers, suppliers of raw materials, warehouse/industry organizations, and policymakers to facilitate budgets in blockchain and IoT integration decisions and related policy. Finally, this technological advancement can improve customer service at a lower cost while protecting the environment and maintaining social aspects.

7 | CONCLUSION

This empirical research of U.K. Agri food industry retail GVC shows that integrating blockchains with IoT strengthens value chain operations and creates value among exchange partners. The findings of this study show how the convergence of blockchains and IoT systems reinforces and builds on the largely theoretical implications discussed in the literature. Our covariance-based SEM analysis of a web-based survey of GVC practitioners reveals that blockchains combined with IoT systems improve GVC scalability, security, and traceability—allowing for the convergence of logistics systems and increasing value chain efficiency dynamics in terms of expense, consistency, distribution, and versatility, and is a significant source of competitive advantage that enhances value chain networks. Our findings can encourage GVC managers, warehouse/industry organizations, and policymakers to recognize the value of IoT-enabled smart supply chains in this digitalization era.

According to Müllner and Filatotchev (2018), the fusion of blockchain and IoT could be hampered by legislative complexities and a lack of market standards in a foreign company. In contrast, BT can improve peer-to-peer collaboration among value chain stakeholders. The convergence of blockchain and IoT calls to question some of the institutional standards common in international business (Müllner & Filatotchev, 2018). Standardization of data privacy legislation continues to be a challenge. However, greater business self-regulation is needed to regulate and monitor access to data and coordinate its dissemination both nationally and internationally. Since the study's empirical context is based on U.K.'s Agri-food retail industry value chain operations trading within the United Kingdom (domestic market only); therefore, it will be interesting for future research to explore the effects of blockchain combined with IoT system with GVC operation beyond geographical boundaries to explain different institutional and legal challenges rigorously, as recommended by Müllner and Filatotchev (2018).

Finally, we used a quantitative research approach focused on a closed-ended survey to investigate the implications of integrating blockchains with IoT structures in value chain operations. Future studies may investigate the implications of blockchains when combined with IoT systems using a qualitative research methodology—as the qualitative study may result in reporting different impacts, which is not included in our research. Furthermore, while this study investigated the possible advantages of integrating blockchains and IoT systems, it did not pursue how best companies should integrate blockchains combined with IoT implementation within GVC. Therefore, further research into this field could be conducted. Furthermore, our report did not investigate approaches to address possible obstacles of blockchains combined with IoT systems, which could be another prospective research area.

ENDNOTE

[1] https://gb.kompass.com/s/agriculture-food/01/. Kompass is a business directory with 53 million enterprises and 34 million business-to-business (B2B) suppliers in the United Kingdom, Ireland, and across the globe.

REFERENCES

Abdel-Basset, M., Manogaran, G., & Mohamed, M. (2018). Internet of things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. *Future Generation Computer Systems*, *86*, 614–628.

Ahlmeyer, M., & Chircu, A. M. (2016). Securing the internet of things: A review. *Issues in Information Systems*. *17*(IV), 21–28. https://doi.org/10.48009/4_iis_2016_21-28

Ahmed, M., Ullah, B., Muhammad, A. S. S., & Pathan, A.-S. K. (2020). *Security analytics for the internet of everything*. Boca Raton, Florida: CRC Press.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411–423.

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research*, *14*(3), 396–402.

Atzori, L., Campolo, C., Da, B., Iera, A., Morabito, G., Esnault, P. P., & Quattropani, S. (2018). Leveraging social notions to improve ID-to-locator mapping in IoT identity oriented networks. *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. https://doi.org/10.1109/wf-iot.2018.8355205.

Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, *09*(10), 533–546.

Borgia, E. (2014). The internet of things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1–31.

Cam-Winget, N., Sadeghi, A.-R., & Jin, Y. (2016). Invited—Can IoT be secured. Proceedings of the 53rd Annual Design Automation Conference. https://doi.org/10.1145/2897937.2905004.

Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R. (2018). Blockchain-based traceability in Agri-food supply chain management: A practical implementation. *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)*. http://doi.org/10.1109/iot-tuscany.2018.8373021

Casado-Vara, R., Prieto, J., & Corchado, J. M. (2018). How blockchain could improve fraud detection in power distribution grid. *Advances in Intelligent Systems and Computing International Joint Conference SOCO'18-CISIS'18-ICEUTE'18*.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*, 55–81.

Clohessy, T., & Clohessy, S. (2020). What's in the box? Combating counterfeit medications in pharmaceutical supply chains with blockchain vigilant information systems. In H. Treiblmaier & T. Clohessy, *Blockchain and Distributed Ledger Technology Use Cases. Progress in IS* (pp. 51–68). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-44337-5_3

Clohessy, T., Treiblmaier, H., Acton, T., & Rogers, N. (2020). Antecedents of blockchain adoption: An integrative framework. *Strategic Change*, *29*(5), 501–515.

de Vass, T., Shee, H., & Miah, S. J. (2021). IoT in supply chain management: A narrative on retail sector sustainability. *International Journal of Logistics Research and Applications*, *24*(6), 1–20.

Diamantopoulos, A., & Siguaw, J. A. (2009). *Introducing LISREL: A guide for the uninitiated*. London: Sage Publications.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. https://doi.org/10.1109/percomw.2017.7917634.

Dubey, R., Gunasekaran, A., Bryde, D. J., Dwivedi, Y. K., & Papadopoulos, T. (2020). Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *International Journal of Production Research*, *58*(11), 3381–3398.

Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Blome, C., & Luo, Z. (2019). Antecedents of resilient supply chains: An empirical study. *IEEE Transactions on Engineering Management*, *66*(1), 8–19.

Dubey, R., Gunasekaran, A., Childe, S. J., Roubaud, D., Wamba, S. F., Giannakis, M., & Foropon, C. (2019). Big data analytics and organizational culture as complements to swift trust and collaborative performance in the humanitarian supply chain. *International Journal of Production Economics*, *210*, 120–136.

Dubey, R., Gunasekaran, A., Childe, S. J., Wamba, S. F., Roubaud, D., & Foropon, C. (2019). Empirical investigation of data analytics capability and organizational flexibility as complements to supply chain resilience. *International Journal of Production Research*, *59*(1), 110–128.

Elmessiry, M., & Elmessiry, A. (2018). Blockchain framework for textile supply chain management. In S. Chen, H. Wang & L. J. Zhang, *Lecture notes in computer science blockchain* (Vol. 10974, pp. 213–227). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-94478-4_15

Fan, T., Tao, F., Deng, S., & Li, S. (2015). Impact of RFID technology on supply chain decisions with inventory inaccuracies. *International Journal of Production Economics*, *159*, 117–125.

Fang, C., Liu, X., Pardalos, P. M., & Pei, J. (2015). Optimization for a three-stage production system in the internet of things: Procurement, production and product recovery, and acquisition. *The International Journal of Advanced Manufacturing Technology*, *83*(5–8), 689–710.

Ferretti, M., & Schiavone, F. (2016). Internet of things and business processes redesign in seaports. The case of Hamburg. *Business Process Management Journal*, *22*(2), 271–284.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50.

Fu, J., & Fu, Y. (2012). Case-based reasoning and multi-agents for cost collaborative management in supply chain. *Procedia Engineering*, *29*, 1088–1098.

Gartner Top Technology Trends (2022). Gartner. Available at https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwjGz4-bkIn1AhUB7e0KHfHCDWAYABAAGgJkZw&ae=2&ohost=www.google.com&cid=CAESQOD2HfineSVa13JFiVN6sJ7Z3NSQzMLq-wDskx-q9DLAmy-unTy-BpcLgBY9ONIIOkcvR6LUU0O4a570bGPYCBc&sig=AOD64_0AyDr9Aq_HmSPL4IjEeJjvf-cjlw&q&adurl&ved=2ahUKEwiG04ebkIn1AhVSecAKHS5HCHwQ0Qx6BAgFEAE.

Geerts, G. L., & O'Leary, D. E. (2014). A supply chain of things: The EAGLET ontology for highly visible supply chains. *Decision Support Systems*, *63*, 3–22.

Guo, B., Yu, Z., Zhou, X., & Zhang, D. (2012). Opportunistic IoT: Exploring the social side of the internet of things. *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. https://doi.org/10.1109/cscwd.2012.6221932.

Haddud, A., Desouza, A., Khare, A., & Lee, H. (2017). Examining potential benefits and challenges associated with the internet of things integration in supply chains. *Journal of Manufacturing Technology Management*, *28*(8), 1055–1085.

Hair, J. F. (2007). *Research methods for business* (Vol. 49, pp. 336–337). New York, NY: Wiley.

Helmerich, N., Raj-Reichert, G., & Zajak, S. (2020). Exercising associational and networked power through the use of digital technology by workers in global value chains. *Competition & Change*, *25*(2), 142–166.

Hirsch-Kreinsen, H. (2016). Digitization of industrial work: development paths and prospects. *Journal for Labour Market Research*, *49*(1), 1–14.

Ho-Sam-Sooi, N., Pieters, W., & Kroesen, M. (2021). Investigating the effect of security and privacy on IoT device purchase behaviour. *Computers & Security*, *102*, 102132.

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, *49*, 114–129.

Inukollu, V. N., Arsi, S., & Ravuri, S. R. (2014). Security issues associated with big data in cloud computing. *International Journal of Network Security & its Applications*, *6*(3), 45–56.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411.

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. *2012 10th International Conference on Frontiers of Information Technology*. https://doi.org/10.1109/fit.2012.53.

Kim-Hung, L., Datta, S. K., Bonnet, C., Hamon, F., & Boudonne, A. (2017). A scalable IoT framework to design logical data flow using virtual sensor. *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*: https://doi.org/10.1109/wimob.2017.8115775.

Kshetri, N. (2017). Can blockchain strengthen the internet of things?. *IT Professional*, *19*(4), 68–72.

Lee, I., & Lee, K. (2015). The internet of things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440.

Li, X., Lu, R., Liang, X., Shen, X., Chen, J., & Lin, X. (2011). Smart community: An internet of things application. *IEEE Communications Magazine*, *49*(11), 68–75.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114–121.

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, *52*(12), 1865–1883.

Martino, B. D., Rak, M., Ficco, M., Esposito, A., Maisto, S., & Nacchia, S. (2018). Internet of things reference architectures, security and interoperability: A survey. *Internet of Things*, *1-2*, 99–112.

Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things*, *1-2*, 1–13.

Minoli, D., & Occhiogrosso, B. (2019). Practical aspects for the integration of 5G networks and IoT applications in smart cities environments. *Wireless Communications and Mobile Computing*, *2019*, 1–30.

Mishra, D., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Dubey, R., & Wamba, S. (2016). Vision, applications and future challenges of internet of things. *Industrial Management & Data Systems*, *116*(7), 1331–1355.

Mital, M., Chang, V., Choudhary, P., Papa, A., & Pani, A. K. (2018). Adoption of internet of things in India: A test of competing models using a structured equation modeling approach. *Technological Forecasting and Social Change*, *136*, 339–346.

Morales-Molina, C. D., Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Perez-Meana, H., Olivares-Mercado, J., … Garcia-Villalba, L. J. (2021). A dense neural network approach for detecting clone ID attacks on the RPL protocol of the IoT. *Sensors*, *21*(9), 3173.

Moshtari, M. (2016). Inter-organizational fit, relationship management capability, and collaborative performance within a humanitarian setting. *Production and Operations Management*, *25*(9), 1542–1557.

Müllner, J., & Filatotchev, I. (2018). The changing face of international business in the information age. In *International business in the information and digital age. Progress in international business research* (Vol. 13, pp. 91–121). Bingley: Emerald Publishing Limited. https://doi.org/10.1108/S1745-886220180000013005

Nagy, J., Oláh, J., Erdei, E., Máté, D., & Popp, J. (2018). The role and impact of industry 4.0 and the internet of things on the business strategy of the value chain—The case of Hungary. *Sustainability*, *10*(10), 3491.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187.

Nurgazina, J., Pakdeetrakulwong, U., Moser, T., & Reiner, G. (2021). Distributed ledger technology applications in food supply chains: A review of challenges and future research directions. *Sustainability*, *13*(8), 4206.

Pan, X., Pan, X., Song, M., Ai, B., & Ming, Y. (2020). Blockchain technology and enterprise operational capabilities: An empirical test. *International Journal of Information Management*, *52*, 101946.

Reaidy, P. J., Gunasekaran, A., & Spalanzani, A. (2015). Bottom-up approach based on internet of things for order fulfillment in a collaborative warehousing environment. *International Journal of Production Economics*, *159*, 29–40.

Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2019). Leveraging the internet of things and blockchain technology in supply chain management. *Future Internet*, *11*(7), 161.

Rejeb, A., Keogh, J. G., Zailani, S., Treiblmaier, H., & Rejeb, K. (2020). Blockchain technology in the food industry: A review of potentials, challenges and future research directions. *Logistics*, *4*(4), 27.

Rong, K., Hu, G., Lin, Y., Shi, Y., & Guo, L. (2015). Understanding business ecosystem using a 6C framework in internet-of-things-based sectors. *International Journal of Production Economics*, *159*, 41–55.

Siegfried, N., Rosenthal, T., & Benlian, A. (2020). Blockchain and the industrial internet of things. *Journal of Enterprise Information Management. (Epub ahead of print)*, http://doi.org/10.1108/jeim-06-2018-0140

Stock, J. H., & Watson, M. W. (2011). *Dynamic Factor Models*. Oxford Handbooks Online.

Tan, L., & Wang, N. (2010). Future internet: The internet of things. *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*. https://doi.org/10.1109/icacte.2010.5579543.

Tapscott, D., & Tapscott, A. (2017). How blockchain will change organizations. *MIT Sloan Management Review*, *58*(2), 10–13.

Treiblmaier, H. (2019). Combining blockchain technology and the physical internet to achieve triple bottom line sustainability: A comprehensive research agenda for modern logistics and supply chain management. *Logistics*, *3*(1), 10.

Tzounis, A., Katsoulas, N., Bartzanas, T., & Kittas, C. (2017). Internet of things in agriculture, recent advances and future challenges. *Biosystems Engineering*, *164*, 31–48.

Venkatraman, N., & Prescott, J. E. (1990). Environment-strategy coalignment: An empirical test of its performance implications. *Strategic Management Journal*, *11*(1), 1–23.

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32–39.

Wang, X., Yu, G., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., … Niu, X. (2019). Capacity of blockchain based internet-of-things: Testbed and analysis. *Internet of Things*, *8*, 100109.

Whitmore, A., Agarwal, A., & Xu, L. D. (2014). The internet of things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261–274.

Wielki, J. (2017). The impact of the internet of things concept development on changes in the operations of modern enterprises. *Polish Journal of Management Studies*, *15*(1), 262–274.

Woodside, J. M., Augustine, F. K., & Giberson, W. (2017). Blockchain technology adoption status and strategies. *Journal of International Technology and Information Management*, *26*(2), 4.

Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks, Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc '05.

Zhao, K., Zuo, Z., & Blackhurst, J. V. (2019). Modelling supply chain adaptation for disruptions: An empirically grounded complex adaptive systems approach. *Journal of Operations Management*, *65*(2), 190–212.

Zheng, R., Shou, B., & Yang, J. (2021). Supply disruption management under consumer panic buying and social learning effects. *Omega*, *101*, 102238.

AUTHOR BIOGRAPHIES

Arthur Egwuonwu is a lecturer in Marketing at Brunel Business School, UK. His current research interests revolve around the impact of distance (e.g., psychic and cultural) in buyer–seller relationships. He is also interested in value creation and advanced services.

Chima Mordi is a reader in management within the College of Business, Arts and Social Sciences at Brunel University, UK. His key research examines International business in emerging and developing markets. It examines the state of labor relations, comparative people management in Africa, Europe, and the Middle East.

Ambrose Egwuonwu is a Doctoral Researcher at the College of Business, Arts and Social Sciences at Brunel University, UK. His research interests include board effectiveness, information security and IT management and the internet of things (IoT) application.

Olayinka Uadiale is a lecturer in Accounting at the College of Business, Arts and Social Sciences at Brunel University, UK. Her research interests include performance management in health service organizations and public sector accounting and accountability.

SUPPORTING INFORMATION

Additional supporting information may be found in the online version of the article at the publisher's website.

How to cite this article: Egwuonwu, A., Mordi, C., Egwuonwu, A., & Uadiale, O. (2022). The influence of blockchains and internet of things on global value chain. *Strategic Change*, *31*(1), 45–55. https://doi.org/10.1002/jsc.2484