Review

Journal of Economics and Social Research
Ekonomi ve Sosyal Araştırmalar Dergisi
ISSN: 2148-1407/ e-ISSN: 2651-3250

Makale Başvuru/Kabul Tarihleri:
Received/Accepted Dates:
07.06.2019/15.07.2020

Cilt 7, Sayı 14, Yıl 2020

Risk Assessment in Digital Supply Chains

Res. Asst. Özden ÖZKANLISOY
İstanbul Aydın University
Faculty of Economics and Administrative Sciences
ozdenozkanlisoy@aydin.edu.tr
ORCID: 0000-0001-7879-0733

Prof. Dr. Erkut AKKARTAL
Yeditepe University
Faculty of Commercial Sciences
erkut.akkartal@yeditepe.edu.tr
ORCID: 0000-0002-7090-4449

Abstract

The introduction of digital transformation into our lifes provides several advantages for companies and the supply chains. However, with the digital supply chains created by digital transformation, some new risks have arisen in the supply chain. In order to ensure long-term benefits and prevent losses in digital supply chain (DSC), the risk management should be given significance in DSC to prevent losses in the DSC. Since this study is essentially for discovery, a literature review has been carried out, and the risk assesments have been made, which is a stage of risk management for the DSC, according to the relevant literature. In this scope, the risks are divided into two groups as internal risks and external risks. In scope of this study, the published academic studies and risk reports of companies are evaluated. It is specified the significance of risk management in DSC. In the second part of this study, occuring the supply chain risks cases in the past are evaluated. In addition, it is referred to new technologies in the light of Industry 4.0. In the third part,strategic decisions taken as a result of risk management, future plans for DSC and bitcoin, financial instruments in DSC are specifed. In the following part, blockchain technology, the risks posed by blockchain, the benefits and implemented fields are evaluated. The study ends with a summary of the findings and a brief evaluation.

Keywords: Digital Supply Chain, Risk Assessment, Risk Management, Technology.

1. INTRODUCTION

The level of competition between businesses has increased with the globalization and the competition is no longer just a phenomenon among the organizations. This has revealed the concept of supply chain. While single businesses were competing in the past, supply chains in which businesses are members compete today. In other words, the competition has occurred among global supply chains (Sinha and Van de Ven, 2005:3).

The supply chain is a chain that not only consists of producers and suppliers, but also encompasses transporters, warehouse providers, wholesalers, customers and all other actors in order to meet direct and indirect customer demands. (Chopra and Meindl, 2015: 1). Supply chain management with a short definition; integration of all business processes with each other, which gives significant values such as product, service and information sharing to customers and other collaborators in a supply chain (Lambert et al., 1998: 1).

The birth of digital age began in the last decade of the 20th century and continues to evolve in the 21st century (Bowersox et al., 2002: 3). In today's world, while technology is a need in human life, it has become a requirement for effective business operations in supply chains (Basheer et al., 2019: 279). Therefore, every business continues to become digital. The digitalization of businesses has the capability to change the supply chain by making the supply chain more priceless and affordable. A new viewpoint must be created for digital technologies to create new supply chain occasions. Companies should redesign the supply chain not only as physical product and service flows, but also as a digital supply network that combines talent, knowledge and finance (Raj and Sharma, 2014: 12).

Digital supply chains are supply chains that provide enhanced agility, reliability and flexibility compared to conventional supply chains, and are proceeding with common knowledge, more collaboration and communication on digital platforms. Conventional supply chains are not willing to share information openly, which reduces supply chain performance (Raab and Griffin-Cryan, 2011:12). Digital supply chains support interactions between globally distributed organizations. It does this by using systems such as software, hardware, and communication networks that regulate the activities of collaborators in the supply chains (Bhargava, 2013: 1637).

The digital supply chain offers the companies a competitive advantage by offering faster integration with intermediate products, visibility of deliveries with tracking, lower cost cloud solutions through information and communication technologies. In addition, finance providers offer working capital through the transaction banking services in DSC (Korpela et al., 2017: 4182).

Digital supply chains are supply chains that make the supply chain more dynamic, enable more effective integration with technology, share access to customer demand effectively, and increase supply chain visibility through monitoring good and service deliveries (Korpela et al., 2017: 4182).

According to the results of the supply chain management survey implemented by PWC in 2019, digitalization takes the first place among the initiatives of supply chain managers in the next term supply chain strategies. It is seen that digitization will take an even more important part in the investment decisions of the supply chain leaders. Therefore, the ratio of digital supply chains will increase even more (PWC, 2019: 24).

Supply chain management is an inter-organizational collaborative effort to identify, assest, mitigate, and track macro and micro cases or unforeseen disruptions that could adversely affect any part of the supply chain. The basis of supply chain management is qualitative and quantitative risk management methodologies (Cheng et al., 2012: 3; Ho et al., 2015: 6).

The concept of risk management (RM) is not a new concept for companies, especially for those operating in the financial and information sector. However, the issue was taken earnestly in the supply chain, after the September 11 Attacks. When the studies in the field of supply chain risk management are analyzed, it is seen that there are few studies conducted until 2000. After this date, the studies in this field have continued to increase until today (Ghadge et al., 2012: 317).

Supply chain risk is described as the cause and effect of unanticipated macro or / or microprocessing cases or status leading to supply chain outages. Supply chain disruptions cause operational, tactical or strategic level breakdowns or distortions in the supply chain (Ho et al., 2015: 5). Supply chain risk is the potential variability in results that causes in a decrease in value added in any activity in the supply chain (Bogataj and Bogataj, 2007: 291).

Supply chain risk management can be described as managing risks through collaboration and coordination with supply chain members to assure profitability and constancy throughout the supply chain (Blos et al., 2009: 247). Supply chain risk management; is extremely significant for a fruitful, competitive and sustainable supply chain in the long run. There have been many devastating risk cases that have had a global impact in the historical process. The losses resulting from these risk cases brougt out how fragile supply chains are against risks. When the risk cases that trigger the development of supply chain risk management are examined, it is seen that many of these cases do not only affect the company and the market in which they occur (Vilko and Hallikas, 2012: 587).

The aim of supply chain risk management is to be flexible to mitigate the likelihood of risky cases and to improve as a result of disruptions. It is less costly to determine the risk beforehand and prevent it from occurring after the risk occurs. For this reason, the risks should be determined in advance and they should be saved from losses. This protects all processes of supply chain operations (production, storage, transportation, insurance, distribution, value-added transactions and customs clearance) from losses and damages (Tang, 2006: 452).

When digital supply chain (DSC) is examined, there are some risks in the literature about digital transformation in the supply chain. It is very dangerous to give new powers to the supply chain by digital transformation. The operations in the supply chain can be negatively affected to the same extent as the level of digital transformation, because when digital technologies fail, the operations of the firm and the supply chain will not work correctly (Chopra ve Meindl, 2015: 517).

Companies that have digitally transformed their supply chains are racing ahead and reaping huge benefits (Westerman et al., 2014: 65). However, it should not be forgotten that, supply chains will face some new risks with digital transformation in supply chains.

In a past study for the transformation of conventional supply chains, the mentioned challenges were encountered. Accenture, Stanford University and global trade school INSEAD have created a team and studied on the conventional supply chains with this team. In their study, it was revealed that more than half of the companies they included in the study encountered unexpected challenges during the supply chain transformation. These challenges can be listed as follows (Blanchard, 2003: 4):

- Technology applications did not work as promised.
- Projects cost more and did not meet the goals of the services.
- Supply chain projects were inconsistent with the company's current business strategy.
- Managing change internally and externally was difficult.

Nowadays, although many of the businesses and supply chains are not aware of them, similar challenges will also arise for digital supply chains. Considering that every challenge is a risk in the supply chains, after the digital transformation, new supply chain risks should be identified and the supply chains should be focused on risk management again.

There is a gap in the literature in this field as there is no study on risk assessment in digital supply chains. The aim of this study is to determine new risk factors that will emerge in digital supply chains that may occur after digital transformation, and to increase awareness of companies and supply chains in which they are members.

2. BACKGROUND

2.1. History

When supply chain risk management is analyzed historically, Supply chain management studies first appeared in the fields of operation strategies and financial risk management in 1995 and the fields that these studies focus on rapidly expanded. Application areas of the supply chain risk management studies has expanded as financial risk management, operation strategies, environmental information management and outsourcing (Tang and Musa, 2011: 27).

Supply chain risk cases that occurred in the historical process have had devastating consequences and had a global impact. The losses have shown how fragile supply chains are against risks. For this causation, supply chain risk cases will be given together with successful and unsuccessful cases to highlight the significance of supply chain risk management in this section.

Supply chain risk factors are defined as various cases and situations that lead to a particular type of risk (Ho et al., 2015: 6). Before talking about supply chain risk cases, supply chain risk factors need to be understood. In the studies existing in the literature, risk factors are grouped in different ways However, when all subtitles are considered as a whole, the risks are the same. Types of supply chain risks in this study; it has been re-grouped by taking into account the studies of different researchers.

In this context, the types of risks are separated to two groups as internal and external risks. Internal and external risks are shown in Table 1 and Table 2 (Zsidisin and Henke, 2019: 357-358; Cook, 2017: 61; Westerman et al, 2014: 138-139; Waters, 2007: 7; Chopra and Sodhi, 2004: 54):

Table 1. Risks internal to the supply chain

Category of Risk	Definition	Drivers of Risk
Supplier operational	These risks are undesirable cases that may prejudice supplier throughput in the way of quality, quantity and cost.	Quality challenges, unforeseeable quantity and cost, significant alteration in lead time, supplier retardation, material availability, improper technology.
Supplier economic	These risks are undesirable cases that could adversely alter a supplier's financial position and bring about bankruptcy or financial instability.	Adversities in making payments, financial instability, challenges in cash flows, finite number of customers, raw material shortage, retrograde reputation in the industry.
Cultural	These risks are cultural risk factors that can lead to disruptions in the supply chain.	Language differences, finite knowledge about cultural differences.
Relational	These risks are known as "*chaos effects*" arising from supply chain complicacy.	Distrust, lack of distrust, second-guessing, supply chain complicacy.
Demand	Potential dissimilarity between forecasted demand and actual demand.	Prediction errors, low level of supply chain association, low level of information sharing, long-term horizons, demand instability and shortage rumours.
Transportation	These risks are undesirable cases that may bring about delay in the consignment of raw materials or finished goods.	Port strikes, malfunctions during distribution and transportation, unreachable information about shipping.
Inventory	These risks are those created by storage activities that may adversely affect the supply chain.	High level of inventory cost, value of goods, excessive amount of inventory, rate of obsolescence of goods.
Legal, bureaucratic and regulatory	Lawsuits filed against the company by collaborators in the supply chain.	Lawsuits filed by supply chain stakeholders such as suppliers and customers.
Sustainability	Environmental, social or ethical infractions that occur during the accomplishment of global activities by supply chain partners (eg suppliers, distributors), causing harmful responses from external stakeholders (eg NGOs) that may harm the company at its focal point.	CO2 emissions by chain partners, health and safety infractions, child labour, the absence of water purification, futile packaging, low wages, not using eco-friendly waste disposal.

Financial capacity (receivables),	Financial difficulties of customers, which can bring about retardations or disruptions in the flow of money towards a focus company.	Deferred payments from payers, alterations in the financial situation of customers, bankruptcy of customers, number of customers.
Consumer risk	A focus firm's failure to meet customer priorities.	Difficulties in order fulfilment, changes in customer preferences, delayed delivery, inappropriate quality (Zsidisin and Henke, 2019: 357-358).
Technology and Cybersecurity	The risks that the technology used and the system created may pose.	Cyber-attack, spyware virus, unauthorized access, data theft, risk of loss of reputation due to technology, privacy violations, sharing information in inappropriate ways (Cook, 2017: 61; Westerman et al., 2014: 138-139)
System risks	The risks related to the systems that supply chain members use for their activities.	Faults in information technology systems (Waters, 2007: 7), information infrastructure not working, system mergers or extended system networks, e-commerce (Chopra and Sodhi, 2004: 54)

Source: Authors

A challenge with raw material procurement, which is a risk of the supplier operational, occurred in Boeing Company in 1997, when the concept of supply chain risk management was still a new concept. Boeing Company had a challenge with the critical raw material supply used in the manufacturing process of the company in 1997. As a result of this challenge, Boeing suffered a loss of approximately $ 2.6 billion (Muellerleile, 2009: 668).

Another supplier challenge is that of Ericson and Nokia in the 2000s. In 2000, Ericsson's revenue was $ 30 billion and nearly 30% of its revenue came from mobile phone sales. Ericsson was working with one supplier for cell phone chips due to low cost and fast delivery. The chip factory of Philips, the sole supplier of Ericsson, broke out in March 2000 and as a result, thousands of chips became unusable. There was no other chip supplier since Ericsson worked with only one supplier. Ericsson's only direct 2001 loss was $ 400 million. The total damage caused by this case to the firm, including indirect causes, was $ 1.7 billion. After that case, Ericsson decided to stop the production of mobile phones and have it manufactured by Flextronics International. In that year when that fire broke out in Philips' chip factory, the mobile phone industry was the leading Nokia Company. Mobile phone sales accounted for more than 70% of its revenue, which is about $ 20 billion annually. For that period, there were two important points separating Nokia and Ericsson. Unlike Ericsson, Nokia had alternative suppliers and a risk management system. Those have caused Nokia to not be affected by that case as much as Ericsson (Norrman and Jansson, 2004: 441-442; Tang and Musa, 2011: 25; Basole and Bellamy, 2014:110).

The supplier of Land Rover Company went bankrupt in 2001. Therefore, Land Rover had to lay off 1400 employees (Norrman and Jansson, 2004: 441). Another supplier challenge is that of Motorola and Sony in 2003. As the Christmas shopping demand reached a very high level in that year, Motorola and Sony Ericsson could not meet the demand due to the supply of critical parts used in their mobile phone production. This situation resulted in loss of customers due to customers turning to other companies (Vesa, 2005: 33). A supplier challenge that occurred in 2005 is that Bosch Company sells damaged pumps to its customers. That case caused the company to lose millions of dollars. That faulty production occurred due to a sub-supplier of Bosch. Unfortunately, Bosch was the first company affected by this case. As seen in this case and other cases, supply chain risks may arise due to the interdependence and integration of the stakeholders of the supply chain (Thun, Hoeing, 2011: 243).

A case of demand risk is the supply chain risk faced by Cisco Company in 2001. Due to the economic crisis that occurred in that year, the demand for information systems decreased and CISCO Company had to bear the extra stock cost of approximately 2 billion dollars (Christopher and Lee, 2004: 392).

If a case is given to the distribution network from transportation risks, Dell wanted to break the perceived niche in the early 1990s. The company started a short flirt for this purpose with conventional retail distribution channels. Retaied sales declined when Dell offered a new PC through its direct channel. Dell was compelled to compansate the retailers for their losses. As a result, the company posted the first ever loss (36 million dolars) in 1993. The ill-judged foray was a salutary lesson in the perils of attempting to operate through conflicting distribution channels and a vindication of its original low-cost direct sales strategy. Dell pulled out of the retail market in 1994 and retrenched with a vengeance, rebounding immediately with profits of 149 million dolars (Leeman, 2010: 184).

The cases of stock risk may be given the challenge experienced by Argos Company. The retail chain Argos had a strategy of ambitious expansion, which it supported with large stocks of goods. When trading conditions changed it moved to a more limited expansion, but it already had excess stocks sitting in supply chains. The result was a write-down of stock value and a substantial fall in share price (Water, 2007: 14).

Technological developments have enabled the utilization of information sharing, monitoring and surveillance activities more effectively. With the introduction of the software, the visibility of the activities and functions on the supply chain has been provided. Furthermore, thanks to the provision of information instantly and accurately, incomplete and incorrect information transfer errors are eliminated and supply chain risks are reduced. However, technology brought new risks such as leakage of information into supply chains and privacy violations despite these benefits. NIKE experienced an information leak in demand planning software in 2000, which caused a supply bottleneck for the Air Jordan model that will be released that summer. This resulted in approximately $ 100 million in sales loss for NIKE (Koch, 2004: 57).

If another case of cyber security risks is given, according to the data of IMAA Institute, it is thought that the total value of mergers and acquisitions in 2018 reached $ 4 trillion worldwide. This rapidly increases cyber security risks. Cyber attackers often target firms that are in the process of being bought by larger firms, and hence the entire supply chain is also affected. In a new merger or acquisition process, a cyber attack that may occur before the deal is completed can significantly reduce the purchase price. No matter how strong and hassle-free the corporate cyber security approaches of the purchasing company, it is necessary to examine whether the company to be purchased or merged fulfills the same cyber security priorities (Imaa Institute).

According to the World Economic Forum Global Risks 2020 Report, "*the largest scale of cyber attacks and critical information infrastructure and networks collapse*" ranks second among the most strongly linked global risks. One of the focal points of the 2020 report is the gaps in technology management. Emerging technologies continue to offer hope for solutions to most existing challanges. However, the speed of technological change has uncertain effects (WEF 2017 Global Risk Report; WEF 2020 Global Risk Report).

Cyber security risks constitute the biggest part of company-originated cyber risks. In 2018, a survey was conducted by cyber security experts. As a result of the survey, it was revealed that 53% of the institutions experienced an internal attack. According to the results of the same study, 51% of respondents were concerned about accidentally clicking on phishing links, while 47% were concerned about malicious employee behavior (AON 2019 Cyber Security Risk Report).

In 2018, many legal regulations regarding cyber security enured all over the world. Accordingly, the risk of compliance with the legal regulations of companies should be evaluated more carefully and the necessary measures should be taken. The European Union (EU) brought a large amount of penalties to cyber security violations with legal regulations. GDPR (European Union General Data Protection Regulation), which encountered force in May 2018 and started to be implemented in EU member countries, brought serious sanctions up to 20 million euros or 4 percent of an organization's annual global turnover in case of violation (AON, 2019).

Risks external to the supply chain are; competitiveness is gathered under 5 headings: input market, political risk, catastrophic and financial market. It is shown in Table 2 (Zsidisin and Henke, 2019: 359):

Table 2: Risks external to the supply chain

Category of Risk	Definition	Drivers of Risk
Competitiveness	These risks are those that affect the competitive position of the focus firm and its supply chain.	Quick alterations in goods or process technology, lack of information about the rival.
Input market	The failure of a focus company to obtain input or quantity in the transformation process affects the competitive power and profitability of a supply chain.	Lack of additional suppliers, incapability to responce significant quantity increments, instability in quality of raw materials, undesirable raw material increments, scarceness of raw materials.
Political risk	Undesirable dramatic changes in the political system. It can negatively affect the competitiveness of a focus firm.	Political convulsion, perturbations from countries concerned of the focal company's project, unstrong government and nationalization, increment of trade tariffs, quota limitation, altering in taxation
Catastrophic	These risks are low in probability but high impact in the supply chain if they occur. They are possible case related with man-made planned situations and unplanned man-made actions or natural hazards.	Terrorism, war, nuclear accidents, earthquakes, hurricanes, tsunamis, floods
Financial market	Alterations related to macro-economic factors, primarily foreign exchange, inflation or interest rates. This can lead to higher raw material prices.	Alterations in exchange rates, high rates of inflation, alterations to interest rates (Zsidisin and Henke, 2019: 359)
Global trade risks	The risks that may occur while companies carry out international trade activities.	Customs security programs, contracts, impact on trade regulation, variable government regulation (Cook, 2017: 62)

Source: Zsidisin, G. A. and Henke, M. (Eds.). (2019). *Revisiting Supply Chain Risk.* Cham: Springer. p. 359; Cook, T. A. (2017). *Enterprise Risk Management in the Global Supply Chain*. CRC Press. p. 62

Natural disasters and accidents occurring in the world cause unpredictable supply chain interruptions and losses from the companies' supply chains. In 2007, Mattel Company collected back 19 million toys with lead paint or loose magnets that children could swallow, as they had fatal dangers. Hurricane Mitch destroyed banana plantations in Hurricane in South America in 1998, and that damage caused the food company Dole to a high level of income. Ford Company had to close its 5 factories for a while on the grounds of the temporary cessation of air traffic after the terrorist attack on September 11, 2001 (Norrman and Jansson, 2004: 441).

Another natural disaster incident was the earthquake that occurred in Taiwan in 1999. As a result of that earthquake, many semiconductor manufacturers could not produce due to damaged power lines. For that reason, Apple and Dell lost sales due to lack of components (Sheffi, 2005: 14).

Worker-employer challenges and worker strikes pose a significant challenge because it affects the supply chains. In 1997, truck drivers went on strike for two weeks. UPS Company held 80% of cargo deliveries in the USA. Along with UPS, the logistics of many producers were affected by this strike (Rothstein, 1997: 474).

2.2. Today

Nowadays, the biggest risk today is thought to be pandemic. This pandemic requires reconsidering all the risks in the global supply chain. When it comes to current external supply chain risks, COVID-19 appears a risk external to the supply chain as a catastrophic in 2020. The World Health Organization (WHO) proclaimed the new type of COVID-19, which appeared in China on the 11th of March 2020 and spread rapidly around the world, as a pandemic. In the past, epidemics such as SARS have appeared all over the world, but they are less contagious although they are more lethal than COVID-19 (WHO, 2020). The emergence, spread and effects of COVID-19 all over the world is a very significant risk case for the supply chains.

The coronavirus named COVID-19 first appeared in China in December 2019 and continues to act in a way that is difficult to model, measure and predict in operations and supply chains around the world. Since the geographical regions affected by this virus are at the center of many global supply chains, these countries are in a strategic position for their supply chains. The lack of quantitative data and the increasing amount of exhausted or wasted stock raise the concern that companies cannot fulfill their contractual obligations (PWC, 2020: 1).

Nowadays, some products have become unobtainable all around the world with COVID-19, product prices have doubled and production factories have stopped due to the challenges of part supply. While the states take additional measures to protect manufacturers, e-commerce has grown rapidly. Truck transitions stopped at the borders, and vehicle drivers started to apply a 14-days quarantine period. In Ro-Ro transportation, the drivers could not be transported by plane and their stay in the European Union was shortened. There have been restrictions in road transport. Due to these constraints, freight transport has shifted to maritime and rail transport. Since most of the freight was carried by passenger aircraft, the cancellation of passenger aircraft flights affected negatively airline freight transport. As a result of the decrease in the load capacity, the reservations for the transportations are started to be given weeks later. The fact that import containers cannot be emptied on time in maritime transportation has increased the need for empty containers in export ports. This case led to a significant increase in prices. The pandemic created by the COVID-19 has revealed the significance of the bullwhip effect in the supply chain (LODER, 2020: 1).

Operating in a wide geographical area, Arçelik has temporarily stopped its manufacturing and sales operations in Pakistan, Bangladesh, South Africa and Russia, as it has declared a curfew in the context of combating the epidemic in Pakistan, Bangladesh, South Africa and Russia. Arçelik officially announced that the share of discontinued operations in total production is 15% and its share in total sales is 10%. The curfew will have been anticipated to terminate on 5 April 2020 in Bangladesh, 6 April 2020 in Pakistan and Russia, and 17 April 2020 in South Africa (KAP, 2020a).

Akçansa Cement, on the other hand, declared on 25.03.2020 that it will continue its activities without interrupting its processes as a result of our effective work in the field of technological infrastructure and digitalization. By implementing public health guidelines announced to the public, it enabled the office employees to switch to the remote working model (KAP, 2020b).

Within the framework of measures to reduce the effects of COVID-19, Aksa Energy aims to ensure that the company's activities are not had an impact by the measures taken and to protect their employees. Accordingly, it has been officially announced that the personnel will go to work alternately or work remotely as of March 16, 2020 at the headquarters. In addition, they stated that a sufficient number of staff will continue to work to ensure uninterrupted energy production at the power plants in order to avoid supply chain interruptions (KAP, 2020c).

While all these cases happen, there are also measures taken by countries and their states to protect their supply chains. Ontario, the province of Canada, has taken measures to support the procurement of critical goods and services and their distribution to the most needed locations. Accordingly, they have declared the "*Supply Chain Management Law*" to ensure that they are able to place crucial materials, equipment and services where they are demanded most. This law will open a door to public sector supply chains to be managed centrally. This will enable the development of a virtual inventory tool, in addition to enabling the accumulation of significant data on stock-taking, orders and supply restrictions, and enabling significant inventory demand to be visible and traceable (Ontario, 2020).

Considering supply chain risk mitigating strategies that have been applied in the past, Ontario's strategy is a case of the strategy of developing joint efforts to enhance the visibility of the supply chain from collaboration strategies. Supply chain risk mitigating strategies are given in Table 3 below:

Table 3. Risk Mitigating Strategies in Supply Chains

Strategy	Explanation
Avoidance	Withdrawal from the product, the industry or the geographical field to be operated.
Control	Vertical integration, Creating safety stocks, Creating extra volume in production, storage, handling and transportation, Forcing contractual necessities on suppliers.
Co-operation	Developing collective efforts to increase the visibleness of the supply chain, Developing collective efforts to share information on risks, Developing common plans for supply chain continuity, Postponement strategies.
Flexibility	Working with multiple suppliers, Working with local suppliers.

Source: Jüttner, U., Peck, H. and Christopher, M. (2003). Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, 6(4), 197-210. p. 206.

Aselsan continues to cooperate with their suppliers by implementing the "*co-operation*" strategy, which is one of the supply chain risk mitigating strategies. Aselsan does not have any dependency on Far East countries in their total supply. It is also compatible with the "*flexibility*" strategy. Limited material purchases in the Far East regions can be substituted both domestically and abroad very quickly. Another factor that has made Aselsan successful in mitigating supply chain risks in this period is that it works in stock for products that are critical materials due to its strategic quality. In other words, they have created a safety stock. The structure established by kaphave great importance in terms of the sustainability of the production during the pandemic period (Bharat, 2019).

To summarize after all these cases that happened, companies want to guarantee themselves with contracts but this is not enough for companies. Challenges that will arise along the supply chain reveal situations and risks that will impact the operational, tactical and strategic decisions of other companies that are members of the chain. Considering the size, scope, source, spread and impact of the supply chain risk, a supply chain risk management system must be established. A balance must be struck between supply chain profitability and supply chain risk. In other words, the balance between the delivery of the product on time, meeting the required demand, providing service at the desired quality and capacity, and timely information flow between companies and the profitability of the companies should be ensured through supply chain risk management (Giannakis and Louis, 2011: 30).

2.3. New Technologies and Risks in light of Industry 4.0

Industry 4.0 technologies enable digitalization in supply chain. In addition, it enhances automation, brings transparency, increases mobility and enables socialization in the supply chain that creates a network. Industry 4.0 has caused radical changes in some business models and environments with a huge impact on digitization and data accumulation. The greatest impact of industrial technologies on the supply chain has transformed into more common, especially in the supply, distribution and production processes (Pfohl et al., 2015: 44).

The implementation of Industry 4.0 with its concepts and technical approaches is accompanied by changes in applied hardware, software and communication technology. As a consequence, the results of the value added process in the supply chain appear (Schröder et al., 2014: 116). The digitalizations in the companies from Industry 1.0 to Industry 4.0, called the 1st Industrial Revolution, are as follows in Table 4:

Table 4. The long road to Industry 4.0, the digitalization of every aspect of business

			Today	
1800 **Industry 1.0**	1900 **Industry 2.0**	1970s **Industry 3.0**	2015+ **Industry 4.0**	2030+ **Digital Ecosystem**
The invention of water and steam powered mechanical production and the beginning of the 1st Industrial Revolution.	• Starting mass production with machines powered by electric and combustion engines, • Introduction of assembly lines.	• Advanced automation of production processes with electronic, IT (Information Technology) and industrial robots, • Beginning of the information age with electronics, IT and internet.	• Digital supply chain • Smart manufacturing • Digital products, services, and business models • Digital analytics and operations as a core competency	• Resilient and close-knit value chain • Virtualized processes • Virtualized customer interface • Industry collaboration as a key value driver

Source: Schrauf, S. and Bertram, P. (2016). Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused. Price Waterhouse Coopers Strategy. p.8. https://www.strategyand.pwc.com/gx/en/insights/2016/industry-4-digitization/industry40.pdf

Industry 4.0 relates to many technology areas. Technology groups in the supply chains are mobile actuators, stationary actuators, sensors, identifiers, mobile devices, wearables, human-machine-interface, machine-machine-interface, cloud computing, software solutions, big data, additive manufacturing (Zimmermann et al., 2019: 1757).

If some of the technologies used in supply chains are given with possible risks, Big Data can store and analyze large amounts of data and also provides users with advanced analysis and modeling opportunities. Big data can only be used to store data for a particular department. In addition, it is able to analyze data collected from all sources. This can be offered to its users in a beneficial way. Thus, users can create a large database by legally combining the data they think will be useful for them. Therefore, it can compile information from multiple sources and present information that cannot be accessed from a single source. They also provide a significant competitive advantage for the decision making process by increasing the handiness and accuracy of the information (Bharat, 2019).

While big data offers significant benefits for many users, it also poses significant security risks. These risks arise from the fact that big data tools store, manage, analyze, visualize and share various data collected from all available sources. Due to the discovery and reinforcement of certain behavioral data, it brings about those who manufacture big data, especially internet users, to transform into defenseless in the way of the emergence of sensitive information. In other words, collecting too much data in big data analysis leads to many infractions of privacy and security infractions (Gahi et al., 2016: 952).

While new technologies provide many benefits, they bring many new risks. The biggest risk of big data is the need to manage the transition process effectively in order to use big data effectively (McAfee and Brynjolfsson, 2012: 72). According to a world-scale study, 94% of managers say that complexity is the most crucial challenge with Big Data, and that information management is the way to solve the challenge is 84%. (Johnson, 2012: 51).

IoT technology, also called 'Internet of Things: "*IoT, is an emerging internet-based information architecture that can be used to facilitate the flow of information in the supply chain networks*". Thanks to the digital functionality of things in IoT technology, the things can be automatically defined and monitored by this technology. It simplifies the management of the supply chain (Xu, 2011: 188). IoT enables data creation and improvement of data details and data quality. In addition, IoT contributes to higher data availability in the Internet of services, blockchain, memory computing and data lakes usage point. In this way, it turns out substantial for the horizontal joining of information systems between the organizations (Pflaum et al., 2018: 3925).

According to the report published by OWASP in 2014, the most significant risk factors for IoT are as follows (Meucci and Muller, 2014):

- Insecure web interface (web, mobile, cloud),
- Inadequate authentication,
- Deficient delegation,
- Insecure network services,
- Deficiency of transmission encryption and entirety confirmation,
- Privacy challenges,
- Insufficient security configuration, software,
- Low level of physical security.

According to the IoT security report published by Kaspersky Company in 2017, it is seen that IoT devices, which are widely used from white goods to industrial systems, are exposed to cyber-attacks at the rate of 45% (Kaspersky, 2017). In addition, the Smart Home Network Security Summary, published by Trend Micro in 2017, has described the 10 countries most affected by threats posed by IoT security vulnerabilities. In the report, the USA, China and the UK ranked first three, with rates of 28%, 7% and 7%. It is seen that Hong Kong, Canada, Australia, Sweden, Netherlands, Taiwan and Russia followed them respectively. It is stated in the report that cyber-attacks in these countries constituted 70% of the attacks in the World (Trendmicro, 2017).

The transition from corporate data centers to the cloud has provided supply chain management data more accessible, especially with technologies such as Iot (AON 2019 Cyber Security Risk Report). It is obvious that cloud computing will have a crucial effect on information technologies and supply chains.

However, the application of IoT technology encompasses some risks for the supply chain. These risks encompass security, privacy, performance and legal barriers (Zissis and Lekkas, 2012: 586; Svantesson and Clarke, 2010: 392-394; Subashini ve Kavitha, 2011: 1).

A new era has begun with digital supply chains. In this new age, it is more difficult to uncover the facts that can consist of the basis for assessment of risks. This station reveals the fact that technology is progressively inconceivable (Corrales et al., 2019: 264).

In this study, risk factors for digital supply chains are discussed in Tables 2 and 3 as internal and external risks. For this reason, the risks for technologies used in digital supply chains have not been evaluated separately on a technology basis, but only an overview has been provided.

2.4. Literature Review

In the literature, there is no study on risk management in digital supply chains yet. In literature review, only publications containing risk assessment has been taken. In this context, publications related to risk management in the supply chain and the methods utilized in these publications are given in Table 5 below:

Table 5: The publications and methods used in SCRM process

The Process of SCRM	The Method	Publications
Risk Identification and Assessment	Analytical hierarchy process	Wu and Chidambaram, 2006: 350.
	Bayes networks	Badurdeen and Wijekoon, 2014: 631.
	DEMATEL, Analytical network process	Fazli and Vosooghidizaji, 2015: 453.
	Fuzzy Analytical hierarchy process, Fuzzy logic	Suharjito and Marimin, 2015: 11.
	Exploratory study methodology	Blos et al., 2009: 247.
Risk Assessment and Mitigation	Simulation	Li et al., 2016: 71.
	Quantitative survey analysis	Speier et al., 2011: 721.
	Economic value added (EVA), Stochastic programming	Hahn and Kuhn, 2012: 591.
	Fuzzy bow tie analysis, Error type and effects analysis	Aqlan and Ali, 2014: 39.
Risk Assessment and Tracking and Surveillance	Multi-criteria SCOR model	Blackhurst et al.,2008: 143.
	House of risk (HOR)	Pujawan and Geraldin, 2009: 953.
Risk Identification, Assessment and Mitigation	Interpretive structural modeling	Kleindorfer and Saad, 2005: 53.
	Network reliability theory	Ohmori and Yoshimoto, 2013: 103.
	A path analytic model using partial least	Kern et al., 2012: 60.

	squares analysis	
	Brainstorming technique, Fault type and effects analysis, 5N analysis, Dimension-effect analysis, Recovery planning	Norlaile and Abu Bakar, 2015: 799.
	Fault type, effects and criticality analysis, Experimental design approach, Discrete event simulation, Analytical hierarchy process, Desirability Function Approach (DFA)	Elleuch et al., 2014: 641.
	Interview, The house of risk (HOR), SCOR model	Anggrahini et al., 2015: 252.

Source: Authors

3. STRATEGIC DESICIONS

Supply chain risk management affects companies' operational, market and financial performance. Therefore, it can be experienced as a strategic management operation of companies (Ram and Srinivas, 2009: 114). According to the definition of Wieland and Wallenburg (2012); "*Supply chain risk management is the execution of strategies for managing ordinary and particular risks grounded on continuous risk assessment in order to diminish vulnerability and insure persistence throughout the supply chain*" (Wieland and Wallenburg, 2012: 890). According to this definition, it is clear that the two most important issues in risk management in the supply chain are risk assessment and risk management strategies.

Risk assessment contains the determination and analysis of the likelihood of the identified risks and the effects they will cause. It includes the stages of interpretation of risks, analysis of their impacts and assessment of the importance of risks. Risk assessment can be done in two ways by using qualitative and quantitative methods. The purpose of the risk assessment is to prioritize the risks in terms of the supply chain by calculating the probability and effects of the risks. In this way, the significant risks to be taken and minor risks to be neglected are determined (Waters, 2007: 127).

The two most significant issues to be considered in risk assessment are the likelihood of read the significance of consequences and losses. Risk assessment is not just making scientific calculations involving the probability and impact of item losses and measurable assets. At the same time, intangible assets that may be affected by risk like dignity, status, authority and trust should also be taken into account. Contrary to general view, there is no zero risk. Modern business management includes risk and risk-taking (Christine Harland et al., 2003: 53-55).

In the first stage, the likehood of emergence of the risk is determined. The probability can be determined by two different methods, as seen in Table 6, quantitative and qualitative. In the quantitative method, the probability ranges from 0 to 1. Risks can be expressed at certain intervals instead of expressing the probability in a clear figure. There are different percentage expressions in the literature about the likehood of emergence. In this study, probability values created by Merna and Al-Thani (2008) are taken as basis. In the qualitative method, the probability of emergence of the risk can be subjectively expressed in five categories as very low, low, medium, high and very high. The probabilities are valued by a number from one to five as a result of both methods (Merna and Al-Thani, 2008: 75).

Table 6. Risk Probability Categories

Sequence Number	Probability	Percentage Expression	Description
1	Very Low	%0-%10	The probability that the risk will emerge is very low.
2	Low	%11-%30	The probability of emergence of the risk is less than the probability of not emerging.
3	Medium	%50	The probability of risk emergence and non- emergence is equal.
4	High	%71-%90	The probability of occurrence of the risk is more than the probability that the risk will not occur.
5	Very High	%91-%100	The probability of the risk emerging is almost certain.

Source: Merna, T. and Faisal, F. (2008). Al-Thani. *Corporate risk management (2nd Edition)*. USA: John Wiley & Sons. p.75

In the second stage, the negative effects of supply chain risks are determined. Risks have negative effects on cost, time and quality (Baccarini and Archer, 2001: 142). According to the severity of the effects of supply chain risks, they are qualitatively expressed in five different categories, namely very light, light, moderate, heavy and very heavy, as indicated in Table 7, and are valued from one to five.

Table 7. Risk Impact Categories

Sequence Number	Probability	Description
1	Very Weak	There is no visible effect, it is insignificant.
2	Weak	There are minor effects and losses that can be tolerated.
3	Moderate	It causes short-term challenges.
4	Grave	It causes long-term challenges and serious interruptions of operations.
5	Very Grave	It causes the operations to be completely interrupted and terminated.

Adapted from source: Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V. M. and Tuominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics*, 90(1), 47-58. p.53.

In the third and final stage, following the computing of the probability and impact values of supply chain risks, risk index is computed by multiplying probability and risk values.

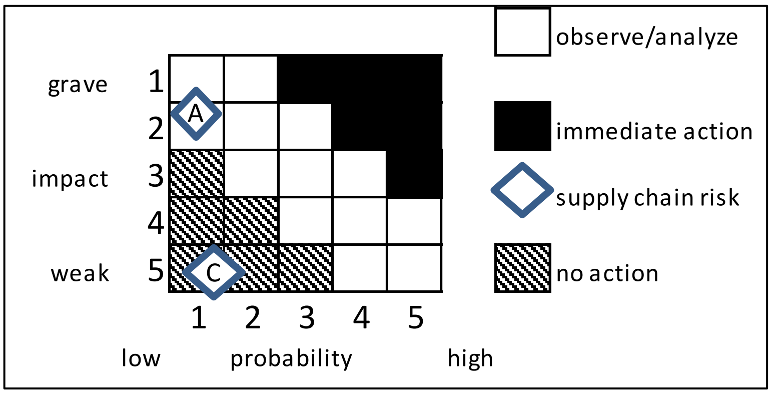

Figure 1: Probability Impact Matrix

Reproduced from the source: Thun, J. H. and Hoenig, D. (2011). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics*, 131(1), 242-249. p.247.

As a result of the computing of the risk index, the probability impact matrix, which is a case in Figure 1, is created. Each supply chain risk source is placed in the matrix with respect to the computed risk index. The risk probability impact matrix can be divided into three parts as shown in Figure 1. The risk management strategy to be determined in the next process is determined according to these three parts in the risk probability matrix.

The process of fulfilment of risk management strategies covers the stages of assessment of strategies, decision making and fulfilment of strategies in line with the risk probability impact matrix obtained during the risk assessment phase. The purpose of this process is to create and implement possible alternative strategies to help reduce risks in the supply chain (Sinha et al., 2004: 164).

There are a number of strategies applied by companies against adverse situations caused by supply chain risks. These strategies, called supply chain risk management strategies, are given below (Lavastre et al., 2012: 831):

- ***Transfer of the risk:*** Risk is turned over another collaborator in the supply chain.
- ***Sharing of the risk:*** Risk is shared and managed by dividing the risk with other collaborator in the supply chain.
- ***Reducing or eliminating the risk within the company****:* The risk affecting the supply chain can be reduced or eliminated within the company by the company (Erşen, 1999: 72). Supply chain risk mitigating strategies are explained in 2.1 section number of this study in detail.
- ***Reducing or eliminating the risk with collaborators:*** Reduces or eliminates risk with companies or individuals with whom it collaborates in the supply chain.
- ***Funding the risk:*** It is funded by devoting budgets to mitigate the effect of supply chain risk and outcome. It is also called the risk insurance (Akkartal, 2018: 1525). With this method, companies often insure against risks like natural disasters and accidents.
- ***Accepting the risk:*** Nothing is done by the company regarding the risk and the risk is not taken. This strategy is usually implemented in two cases. The first is applied in cases where the risk is unlikely to be impacted and unlikely. The second is applied when the cost of eliminating/ mitigating /funding of risk is higher than its expected effect (Aqlan and Lam, 2015: 5642).

The decisions to be taken by companies against the supply chain risks they face are a strategic decision. As seen above, the scope of strategic decisions consists of determining the probability and impact of risks and creating the risk probability impact matrix and choosing the most appropriate supply chain risk management strategy as a result of the risk index computed.

4. STRATEGIC FRAMEWORK

In this part of the study, the subject is dealt with as two main issues. The first one consists of suggestions given to the member companies of supply chain. The second point clarifies the strategies they can apply in case of supply chain disruptions.

The most significant suggestion to be given to companies in their future plans is that companies need to look further. Looking ahead in the new digital age is more important than ever. In most companies, roles are not forward-oriented. The familiar works and processes are completely based on the near and distant past. A case of this is that sales results are based on long-term decisions. Similarly, case studies in companies show what was done before, from annual results to best practices. Companies need to change their focus more than ever. Agility was what has been offered to firms and supply chains for decades as a prescription. However, it would be correct to say that agility, also called quick response, is now slow with the changes in technologies today (Goodwin, 2018: 189-190).

The second most significant suggestion is that companies from the supply chain should see digital transformation in their supply chains as an integrated and continuous part of any overall business strategy. Businesses that do this face less risk in the digital supply chain or are less affected by supply chain disruptions. Many companies that see digital transformation as a significant part of their business strategy have created new digital transformation departments and hired digital experts to guide the digital transformation strategy (Schallmo and Williams, 2018: 7). The employed persons must have the necessary technical knowledge and expertise to implement the necessary projects. For this purpose, various programs such as branding and quality programs, which will encourage employees to take the necessary steps in digitization and direct their companies from design to implementation for the projects to be carried out, can be implemented. These programs are programs that will allow you to encounter less risk of the supply chain. For instance, the turquality program in Turkey is a case of this can be given (Kantarcı et al., 2017: 8). In the digital supply chains, the more effectively the digitization is implemented, the lower level of the supply chain risks encountered.

One of the most significant risks in the digital supply chain is the cyber security issue. Companies can get help from the International Chamber of Commerce (ICC) on cyber security issues. The issues ICC provides companies with help are fighting commercial crime, new criminal threats, stamping out corruption, commercial crime services and fighting counterfeiting and piracy of goods (Cook, 2017: 70-71).

Cyber risks are risks that can pose serious risks as much as operational risks. One of the principles applied in this direction is to transfer the risk mentioned in the previous topic through insurance and reduce the risk. Cyber risk insurance has become widespread especially in the USA and U.S. (PWC, 2019). It is estimated that the budget of cyber security expenditures calculated globally until 2027 will be over 10 billion dollars. When cyber-attacks were examined, it was observed that they made more than half of these attacks for small companies. The reason for this is that small companies ignore cyber threats and see the amount to be spent for their cyber security as an unnecessary expense. As a result, hackers see these businesses as easier prey and select these companies (Powell, 2019). For these reasons, it is very significant to make cyber insurance in digital supply chains by seeing the future.

The decisions taken as a result of different regulatory areas and laws may cause some confusion and conflicts. These risks, which are considered as global trade risks in the history section of this study, should be considered. While various measures are implemented to protect consumers on issues such as information security, their positive and negative effects on the industry should be evaluated within a broad framework.

The concept of corporate governance with digital supply chains has become more prominent. Corporate Governance as the new management approach adopted by companies can be defined as "*a new form of management in which individuals are engaged in mutual communication and interaction, rather than a unilateral impact, such as governing and managed*". Digital supply chains have revealed new demands for digital talents and new risks from digital operations. This has revealed the obligation of "*corporate governance*" for all organizations in the digital supply chains (Westerman et al., 2014: 138). Therefore, companies must keep up with this new form of management.

Strategies implemented regarding supply chain disruptions resulting from by supply chain risks are the second important consideration for future plans. Robust supply chain strategies that have turned out advantageous in coping with supply chain disruptions include the following (Olson, 2014: 24-26):

- ***Postponement strategy*** is a strategy grounded on delaying goods differentiation. This strategy is resisted on a number of conception concepts like standardization, common structure and modular conception. It implements later customization in the production cycle for special products produced according to a more general product collection demand. This special product responds more flexibly. Postponement enhances the company's capability to conduct resources and offers more goods resiliency.
- ***Strategic stock strategy*** is utilized to benefit from security stocks for all key items, without the cost of overstocking. This strategy provides higher levels of customer service without overstocking costs. Strategic stocks increase product availability. Therefore, it provides a faster reaction.
- ***Flexible supply base strategy*** reduces the risks caused by single resource use through multiple suppliers. This opens a door to some volume slack to get through supply disruptions through enhancing supply resiliency.
- ***Make-and-buy strategy*** is basically in line with its flexible supply base strategy. In addition, it includes external production as an alternative resource. The advantages are the same as with former strategy.
- ***Economic supply incentives strategy*** is the utilization of economic supply incentives even if production cannot be changed. The utilization of economic supply incentives may enhance attendance in an industry for avoiding future scarceness.
- ***Flexible transport strategy*** is a strategy that guarantees deliverance. It is able to be performed in different ways, including multimodal transport. The scope of this strategy includes changing the mode of transport quickly when a glitch is encountered, using multi-mode mode, and performing it at low cost. The utilization of multiple routes is a third transportation strategy, facilitating bypassing of nonpermanent bottlenecks. Multicarrier transportation provides a regularly flow of materials.
- ***Dynamic pricing and promotion strategies*** are states of income administration strategies. Income administration rises check over goods demand and allows the company to impress customer goods preference.
- ***Dynamic product diversity planning*** is the strategy whose basis is to impress the demand for consumer goods according to display position.
- ***Silent product migration strategy*** includes slow leaking of new goods without official announcements. This strategy heartens customers to select correct goods in default of wanting goods that are phased out or not in stock. Thus, all goods are substitutions that accelerate supply or demand cuts as well as dealing with supply fluctuations.

5. A FINANCIAL INSTRUMENT: BITCOIN

The concept of Bitcoin (Nakamoto, 2008) is often confused with the concept of blockchain. Bitcoin is a virtual currency. As described by Mukhopadhyay et al. (2016), "*Bitcoin is a virtual cryptocurrency that provides a certain privacy to its owner and allows to pay any place in the world with low transmission charges without the requirement of a central authority's approval*" (Mukhopadhyay et al., 2016: 745). Bitcoin ensured a great advantage to users by responding to the need for a quick payment system that can adapt to the new communication method (fast, secure and unlimited money) (Antonopoulos, 2014: 1).

Unfortunately, the emergence of a fully feasible digital currency posed two main challenges. One of them is the challenge of double spending. In contrast to physical money and assets, digital money and other digital assets are just a computer file. In other words, they are a series of bits and are able to be transcribed like any other digital file. If the account holder does not have an instrument that keeps their balances, such as cash or securities account balances, they can dispatch the file and hold a copy. This is called a double spending issue. To avoid double spending, it is important that each note is checked online against a central ledger when it is spent (Chaum, 1992: 98). This has revealed the requirement of an authorized record of all transactions of the digital asset. Other crucial matter for Bitcoin is ratification of authenticity. In the Bitcoin system, it is controlled by bitcoin miners whether every transaction is valid. The lack of these two challenges provides that the blockchain data structure, which is the backbone of the bitcoin system, progresses in a healthy and safe manner (Franco, 2015: 143).

Nakamoto worked out the double spending challenge related to the Bitcoin system. Nakamoto's blockchain development technology is crucial because of a solution to the double spending. Other scholars working on this subject only developed non-Bitcoin uses of Blockchain technology. For instance, the definition of the concept of "*smart contracts*" by Bheemaiah (2015) is as follows: "*Smart contracts are programs that encode certain conditions and results. When a transaction occurs between the two parties, the program can verify whether the product/service has been sent by the supplier. However, after verification, the amount transferred to the supplier account is calculated*" (Bheemaiah, 2015). Figure 2 shows a simple overview of the Bitcoin network and its main elements.

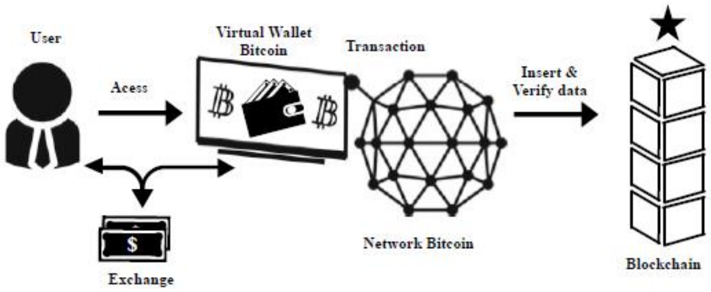

Figure 2: A Sample Bitcoin Network

Source: da Rosa Righi, R., Alberti, A. M. and Singh, M. (2020). *Blockchain Technology for Industry 4.0.* Boston: Springer.p.30. https://doi.org/10.1007/978-981-15-1137-0_1

The concept of "*Blockchain 2.0*" emerged with the blockchain view after Bitcoin in 2014. This offers users new technologies that use blockchain to create a safer trading book (Bheemaiah, 2015). It was mentioned above that blockchain was created in order to prevent double spending challenge in cryptocurrency. However, blockchain is actually a distributed ledger system in the application. The aim of the participants in the blockchain is to create individual actions that act as a chained ledger by building blocks on the chain. A blockchain is a decentralized distributed ledger. Consequently, more than one participant building the blocks can keep a copy of the ledger. Technically, every attendant holding a copy of the blockchain is a "*node*". Each node is a copy of the ledger record. For this reason, the ledger does not exist in one place. Namely, the notebook is not central. Nodes add new blocks to the chain by processing transactions including blocks with one-way encryption that are not able to be changed retrospectively. This is the most crucial task in the nodes' blockchain. This gives the blockchain the advantage of pulling away as an open and distributed ledger that records transactions between different parties efficiently, verifiable and enduringly (Lakhani and Iansiti, 2017: 98). These secure transactions can be advantageous for organizations that want to keep information as safe and effective like the records of medical or banking.

Before discussing the blockchain in detail, it is useful to mention the differences between the current model of the banking and bitcoin. The differences between Bitcoin and the current banking model are given below in Table 8:

Table 8: The differences of banking model and Bitcoin

Characteristic	**Bitcoin**	**Banking Model**
Audit	Compromise	The central bank
Transaction Verification	Compromise	Central
Money Making	Mining	Credits
Value of Money	Proof of work, supply-demand, trust	Exchange rate
Source of Money	Limited edition	Unlimited in theory
Money transfer	Direct, irreversible	Mediated, reversible
Privacy	To some extent anonymous	Depending on the application
Processing Fee	Fixed transaction fee In theory	Account fee, transaction fee
Processing Time	In the range of minutes	Theoretically instantaneous, practically daily

Source: Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Commun. Surv. Tutor*. 18: 2084–2123. p.8.

6. BLOCKCHAIN

Blockchain is one most important structure motivated by Bitcoin. In this section, managerial risks, smarts contracts, risks, cost risks and blockchain vulnerabilities and attacks will be talked about and implemented fields will be given, after the definition of Bitcoin is given.

6.1. Definition of Blockchain

"*The Blockchain is a decentralized and distributed cryptographic digital "ledger" that is used to record transactions*". One of the principles of blockchain technology is that people who do not know or trust each other create a large digital record of the "*who owns what*" that will apply the consent of everyone concerned (Economist, 2015). Blockchain functions as a consistent transaction history that all "*nodes*" accept as a result (Wattenhofer, 2016: 85). Blockcherain is actually a public database. It is capable of storing and transferring tangible assets and intangible assets such as votes, reputation, intent, information, software, and even thoughts (Swan, 2015: 16).

Blockchain is not a verification system that only allows Bitcoin from cryptocurrencies. It is also a system that allows all cryptocurrencies like Ethereum and Ripple (Walch, 2018: 245; Corrales et al., 2019: 3). In addition to cryptocurrencies, this technology also offers different types of applications, platforms, information storage and distribution systems. Accordingly, blockchain is described as a revolutionary technology in almost all fields of the business life. It promises the change of record keeping currently applied (Tomas, 2017: 28).

Investments in Blockchain and cryptocurrencies, which are used in many fields, have increased dramatically in the last few years. Since 2017, investments have shown a marked upward trend. Capital investment in blockchain and cryptocurrencies has remained below $1 billion from 2013 to 2016 due to the fact that the concept is new and unpopular. Blockchain investments experienced a sudden boom in 2017, as shown in Fig. 3, was 4.8 billion (da Rosa Righi et al., 2020: 22).

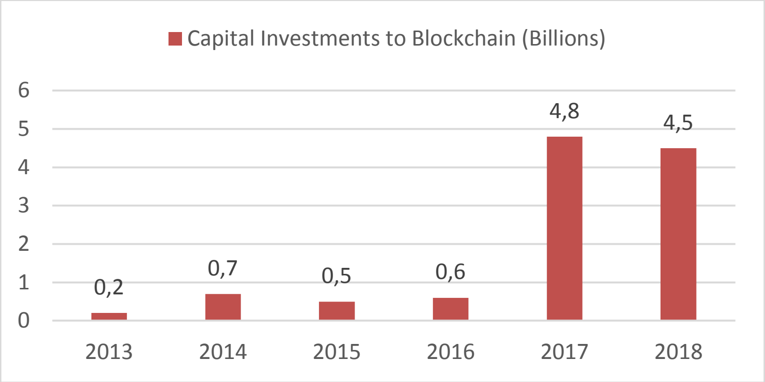

Figure 3: Capital Invested in Blockchain Technology

Reproduced from the source: da Rosa Righi, R., Alberti, A. M. and Singh, M. (2020). *Blockchain Technology for Industry 4.0.* Boston: Springer.p.122. https://doi.org/10.1007/978-981-15-1137-0_1

Blockchain allows synchronization of ledger content copied between multiple operators. It also utilized community verification. Blockchain's origins are based on technologies introduced decades ago, but this technology has gained popularity in recent years with Bitcoin (Aste et al., 2015: 18). According to the original blockchain concept announced by the Bitcoin inventor, blockchain technology has been improved to overcome certain issues and make the technology more scalable for regulators. Another aim of these improvements is to make this technology less enemy to reduce supply chain risks (Hofmann et al., 2018: 35). While blockchain technology carries supply chain risks, it can also help identify and manage supply chain risk. It performs this task by serving as an appropriate processing layer for information. Blockchain ensures the opportunity to enhance the visibility in the structure of supply chains by creating a digital backbone with IoT.

Blockchain technology is at the center of supply chain processes (Babich and Hilary, 2018: 7-8, 14). When digital supply chains are based on blockchain technology, they get the opportunity to verify the source of the goods. It was mentioned above that another possibility that blockchain gives to digital supply chains is the constant recording of the activities of every object in the supply chain. In addition, this technology allows for backward monitoring of operations in supply chains (Satyavolu and Sangamnerkar, 2016). By increasing the visibility of the digital supply chain, companies and supply chains can foresee potential bottlenecks. In addition, they can predict the likelihood of adverse cases occurring. This is crucial for the supply chain risk assessment, as it gives digital supply chains the chance to evaluate the consequences of adverse cases at an early stage (Babich and Hilary, 2018: 11). When moving from conventional supply chains to digital supply chains, the risk assessment process should be implemented again to discover potential bottlenecks. At this point, the significance of risk management becomes evident when discovering potential bottlenecks.

Traditional supply chains offer corporate solutions by centrally storing and isolating relevant data. In contrast to this case, digital supply chains offer corporate solutions by securely digitizing many existing transactions with Blockchain and sharing all transaction information between network parties (Yoo, 2017: 313). In digital supply chains, information asymmetry is eliminated in this way. Thus, supply chain risk management turns into a data-driven system. More research is needed on the role of the new information structure for RM processes in DSC compared to conventional supply chains (Babich and Hilary 2018: 12).

Blockchain technology facilitates trust among supply chain agents. Blockchain does this by providing a copy of the information record that cannot be changed without their consent. It also protects against tampering with malicious resources and the security of information in the chain. Therefore, it is possible to state that Blockchain serves as a secure encryption method (Zsidisin and Henke, 2019:8).

The technological advantages that blockchain provides to users as the results of its structural architecture are mentioned above. If these advantages are grouped, they can be listed as endurance, transparency, Immutability and integrity of process (Abeyratne and Monfared, 2016: 3; Apte and Petrovsky, 2016: 77). These key technological advantages, which provide significant benefits to digital supply chains, are briefly detailed in Table 9 below:

Table 9: Inherent technological advantages of blockchain technology

Advantage	**Description**
Endurance	“*Since decentralized networks eliminate single points of failure, this risk distribution among nodes makes them much more durable in blockchain-based digital supply chains than central systems. Furthermore, malicious entries have a deterrent effect*”.
Transparency	“*An identical copy of a blockchain is held by each node in the network. This enables real-time monitoring of data sets. This level of transparency makes network activities and operations highly visible and facilitates trust*”.
Immutability	“*The data stored on the blockchain is practically unchanged due to the need to be approved by other nodes and the traceability of the changes. This allows users to have the highest level of confidence that the data chain is unaltered and accurate*”.
Integrity of Process	“*The execution of distributed open source protocols exactly as written in the code ensures that the actions described in the protocol are executed correctly and on time without the need for human intervention*”.

Adapted from source: Abeyratne, S. A. and Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(9), 1–10. p. 3.

Blockchain is considered as a tool to increase the security and cost effectiveness of transactions in digital supply chains. Blockchain is a technology that is often used to integrate over the internet and to perform secure transactions at a faster and lower cost (Abeyratne and Monfared 2016: 3; Korpela et al. 2017: 4183).

Ultimately, it is believed that this technology, which deals with risks related to digital supply chain transparency, traceability, and originality issues, will reduce fears and anxieties (Zsidisin and Henke, 2019: 310).

6.2. Risks in Blockchain

6.2.1. Managerial Risks

6.2.1.1. Standards and Central Model Requirement

To be effective, blockchain and smart contracts require standards such as a set of common rules in which all participants operate to ensure accuracy and reliability. The model must be central. Because a decentralized model creates difficulties when the rules need to be changed. Because these changes need to be agreed and accepted for all participants to work consistently.

6.2.1.2. Management Framework Requirement

A management framework will be required to implement and operate blockchain as a legal practice and should take into account surveillance and monitoring functions, rule setting, admission and change control management. In general, management will be a requirement not only for legal but also for all technologies that manage information. Management standards around the blockchain will contribute to technology and market confidence in the legal and regulatory environment. This will speed up the adoption and success of the smart contract.

6.2.2. Smarts Contracts

Smart contracts were defined in 1994 by computer scientist and encryption specialist Nick Szabo as follows: "*Smart contracts are a set of commitments that are digitally ordered and contain protocols, where the parties perform their commitments according to these protocols*" (Szabo, 2018). In blockchain technology, smart contracts eliminate the broker and offer fast and affordable solutions thanks to the opportunities offered by the technology. All these reasons make smart contracts attractive (Heckelmann, 2018: 504-505). In addition to these advantages, there are a number of supply chain risks created by the utilization of smart contracts. These risks are volatility that creates potential industry bubbles, deficiency of adjustment and irreversibility of concords (Piazza 2017: 288). However, the risks of smart contracts are mitigated compared to conventional contracts. Because smart contracts are largely autonomous, self-contained and decentralized contracts (Ross 2017: 360). As the applications of smart contracts are new, their pros and cons are not yet definitely explained (Surujnath 2017: 264). However, it is among the risks brought by blockchain technology for digital supply chains.

6.2.3. Blockchain Vulnerabilities and Attacks

There are cases when blockchain service and blockchain-based application are vulnerable to certain attacks that are difficult to detect or prevent. Cases of these situations are that the network node is compromised and adversely affects the mining process or consensus process. Thus, there are several vulnerabilities for the blockchain and thus digital supply chain risks (Treiblmaier and Beck, 2019: 138-141).

- **Block Withholding Attack:** It is a type of attack that creates the intention of malicious nodes to join the pool (Rosenfeld, 2011: 23-24).
- **Block Discarding Attack:** It is the type of attack that occurs when a node controls most network connections with other nodes. The occurrence of this attack requires that a mined block be approved by most nodes and added to the blockchain (Bahack, 2013: 1).
- **Replay Attack:** It is a type of attack that occurs in networks where the attackers try to repeat or delay the data transmission captured and where the message exchange and distribution is high (Dua et al., 2013: 59).
- **Middle Attack Man:** A type of attack in which attackers try to interrupt the message between two honest parties, change it and then give false messages (Callegati et al., 2009: 78). Time is a critical factor for these attacks.
- **Potential Privacy Risks:** Node connection causes a major privacy problem. Each node actively participates in the network to broadcast messages and receive rewards, and transactions can be monitored by other nodes. This is one of the biggest supply chain risks brought by Blockchain.
- **Majority Hash Rate Attack:** Miners try to control the source of mining power to get a high level of profit. If an attacker controls more than 50% of all mining power, he can reverse the transactions he sends while in control. This can also prevent transactions from being approved (Treiblmaier and Beck, 2019: 140-141).

All blockchain security vulnerabilities and attacks above pose a significant risk for digital supply chains.

6.2.4. Cost Risk

Bitcoin is a very energy-intensive application. It needs a high level of electricity in exchange for building new blocks. This situation has negative effects both environmentally and costly. Developers of blockchain platforms are working on different consensus algorithms such as Proof of Stake for this situation. If confirmatory Proof of Bet uses consensus, it must maintain a certain percentage of the network's total value (Gupta 2016: 16). All cryptocurrencies do not have the same cost and environmental risk. Ethereum, a cryptocurrency, uses different authentication protocols, and these protocols are much less energy intensive.

6.3. Implemented Fields

This SCM idea through blockchain is conceptualized by Wal-Mart, who uses technology to track bacterial formations in food and identify the source and limit the number of items to remember (Nofer et al., 2017: 183). Blockchain technology has also been implemented to end unethical behavior in the diamond industry (Underwood, 2016: 16).

Blockchain technology is also used as a voting system. In 2014, a blockchain voting system was used by the Danish political party Liberal Alliance (Pilkington 2015: 243). In March 2018, Sierra Leone became the first country to use blockchain to provide trust and transparency in presidential election processes (Kazeem, 2018). The utilization of blockchain in voting systems allows every voting to be recorded accurately and more transparency (Pilkington 2015: 243).

Although blockchain technology was originally brought out to be utilized on the substructure of conjectural currencies like Bitcoin, nowadays it has the possible to be utilized in dissimilar industries such as finance, healthcare, real estate, supply chain, government agencies and telecommunications. The utilization of money for the blockchain structure is not mandatory and can be utilized for any value transfer or ownership commercial operations that can be expressed numerically (Gupta, 2017: 25-30).

Blockchain can be used to monitor and control specific assignments such as government-level polling systems, tax collection, passport extraction, title deeds, grants (Asharaf and Adarsh, 2017: 33). Blockchain applications are given in Table 10 with examples below (Nofer et al., 2017: 185):

Table 10: Applications of Blockchain

Type	Application	Cases
Financial applications	Cryptocurrencies	Bitcoin
		Litecoin
		Ripple
		Monero
	Securities issuance, trading and settlement	NASDAQ private equity
		Medici
		Blockstream
		Coinsetter
	Insurance	Everledger
Non- financial applications	Cancellarius	Stampery
		Viacoin
		Ascribe
	Music industry	Imogen heap
	Decentralized evidence of entity of certificates	www.proofofexistence.com
	Decentralized storage	Storj

	Decentralized IoT	Filament ADEPT
	Anti-counterfeit Solutions	Blockverify
	Internet applications	Namecoin

Source: Adapted from Nofer, M., Gomber, P., Hinz, O. and Schiereck, D. (2017). Blockchain. *Business and Information Systems Engineering*, 59(3), 183–187. p.185.

5. CONCLUSION

Many things have changed with the introduction of Industry 4.0. This concept, signified to as the 4th Industrial Revolution, has accomplished digital transformation in many companies with technologies, and this transformation has been reflected in the supply chains of which companies are members.

New technologies in the light of Industry 4.0 enable digitalization in the supply chain. In addition, it enhances automation, brings transparency, increases mobility and enables socialization in the supply chain that creates a network. Industry 4.0 has caused radical changes in some business models and environments with a huge impact on digitization and data accumulation. The greatest impact of industrial technologies on the supply chain has turn out more common, especially in the supply, distribution and production processes. Digital supply chains are supply chains that provide enhanced agility, reliability and flexibility compared to conventional supply chains, and are proceeding with common knowledge, more collaboration and communication on digital platforms.

Transformation from conventional supply chains to digital supply chains has brought new and unexpected risks. In order not to suffer from supply chain disruptions, it is essential to become aware of the new risks to be faced well and actively implement the risk management. In this study, a risk assessment was conducted to identify possible new risks that digital supply chains may face. In consequence of the literature review, the internal risks that await digital supply chains include technology and cybersecurity risks and system risks that include digital systems. Technology and cybersecurity risks are cyber-attack, spyware virus, unauthorized access, data theft, risk of loss of reputation due to technology, privacy violations and sharing information in inappropriate ways. System risks are faults in information technology systems, information infrastructure not working, system mergers or extended system networks and e-commerce. External digital supply chain risks are global trade risks. It is also possible to examine digital supply chain risks on a technology basis. For instance, blockchain technology has increased the amount of investment in recent years in companies and their supply chains, bringing the risks of smart contracts, managerial issues, cost and security vulnerabilities and attacks that blockchain technology has. However, blockchain risks are explained but the risks were handled considering all supply chain technologies in this study.

It can be concluded that risk assessment is a strategic decision to identify the risks that arise with new technologies in digital supply chains. First of all, possible new risks should be identified in the supply chain risk method. These risks should be determined probability and impacts and a probability and impact matrix should be created. According to the risk index obtained with this matrix, risks are divided into three groups as risks to be kept under control (risk observing and analysis), risks that need to be intervened immediately (immediate action) and risks that will not be intervened (no action). Based on the findings obtained, the risk management strategy to be applied is selected. Choosing a risk management strategy is as crucial as reaching the risk index. The purpose of implementing these strategies is to create and carry out possible alternative strategies to help reduce risks in the supply chain.

There are other issues in digital supply chains that are as significant as risk identification and assessment. In digital supply chains, supply chain plans should differ compared to conventional supply chains. In digital supply chains, supply chain plans should differ compared to conventional supply chains. The most significant suggestion to be made in this regard is the necessity of the supply chain to look forward. The supply chain needs to change its focus. It needs to change its focus more than ever. The second most significant suggestion is that companies in the supply chain should view digital transformation in their supply chains as an integrated and continuous part of any overall business strategy. Companies that do this face less risk in the digital supply chain or are less affected by supply chain disruptions.

Corporate Governance is a new management approach adopted by companies. New talent requirements and new risks arising from digital activities have emerged with digital supply chain. This brought forward the concept of corporate governance for digital supply chains and made it mandatory. Therefore, companies must keep up with this new form of management.

For further studies, one of the most crucial risks in the digital supply chain is the issue of cyber security. Companies can get help from the International Chamber of Commerce (ICC) on cyber security issues. As a recommendation, the issues ICC provides companies with help are fighting commercial crime, new criminal threats, stamping out corruption, commercial crime services and fighting counterfeiting and piracy of goods. Because it is one of the most common digital supply chain risks, it is very significant to make cyber insurance in digital supply chains by seeing the future. Cyber risk insurance has become widespread especially in the USA and U.S.

Reassessing the supply chain risk serves as a significant bridge between the existing supply chain risks and the major changes that have occurred with the emergence of the 4th Industrial Revolution called Industry 4.0. Therefore, risk assessment is very significant for digital supply chains. It’s a modern digital twist on a story as old as time: with major advantages comes major risks. Digital supply chains should focus more on risk management than ever before to achieve advantages. Redefine and evaluate risks and decide on appropriate supply chain risk management strategies as a result of valuation. This study was prepared to alert digital supply chains against new risks and guide them in risk assessment processes.

REFERENCES

BOOKS

Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking digital cryptocurrencies. California: O'Reilly Media, Inc.

Asharaf S. and Adarsh S. (2017). Decentralized computing using blockchain technologies and smart contracts: emerging research and opportunities. Hershey: Information Science Reference (IGI Global).

Bowersox, D., Closs, D. and Cooper, M. B. (2002). Part I logistics in supply chain management. Supply chain logistics management, New York: McGraw-Hill Companies Inc. Series.

Chopra, S. and Meindl, P. (2015). Supply Chain Management: Strategy, Planning, and Operation (7th Edition) (What's New in Operations Management. London: Pearson.

Cook, T. A. (2017). Enterprise Risk Management in the Global Supply Chain. Abingdon: CRC Press, Taylor & Francis Group.

Corrales, M., Fenwick, M. and Haapio, H. (2019). Digital technologies, legal design and the future of the legal profession. In Legal Tech, Smart Contracts and Blockchain (pp. 1-15). Singapore: Springer.

da Rosa Righi, R., Alberti, A. M. and Singh, M. (2020). Blockchain Technology for Industry 4.0. Boston: Springer.

Franco, P. (2015). Understanding Bitcoin Cryptograpy, engineering, and economics, USA: John Wiley & Sons.

Goodwin, T. (2018). Digital Darwinism: Survival of the Fittest in the Age of Business Disruption. London: Kogan Page Publishers.

Gupta, M. (2017). Blockchain for dummies. New Jersey, USA: Hoboken.

Gupta, M. (2018). Blockchain for Dummies (IBM Limited Edition). USA: John Wiley & Sons.

Hofmann, E., Strewe, U. M. and Bosia, N. (2018). Supply chain finance and blockchain technology: the case of reverse securitization. Boston: Springer.

Leeman, J. J. (2010). Supply chain management: Fast, flexible supply chains in manufacturing and retailing. BoD–Books on Demand.

Merna, T. and Faisal, F. (2008). Al-Thani. Corporate risk management (2nd Edition). USA: John Wiley & Sons.

Olson, D. L. (2014). Supply chain risk management: tools for analysis (2nd edition). Business Expert Press: New York.

Schallmo, D. R. and Williams, C. A. (2018). Digital Transformation Now!: Guiding the Successful Digitalization of Your Business Model. Boston: Springer.

Swan M. (2015). Blockchain: Blueprint for a new economy (1st edition). Sebastopol (CA): O'Reilly.

Tomas, P. (2017). Cryptocurrency 101: A Beginners Guide to Understanding Cryptocurrencies and Tow to Make Money from Trading. London: Pronoun Press.

Treiblmaier, H. and Beck, R. (Eds.). (2019). Business Transformation through Blockchain Volume I. Cham: Palgrave Macmillan.

Treiblmaier, H. and Beck, R. (Eds.). (2019). Business Transformation through Blockchain Volume II. Cham: Palgrave Macmillan.

Waters, D. (2007). Supply chain risk management: vulnerability and resilience in logistics. London: Kogan Page Publishers.

Wattenhofer, R. (2016). The science of the blockchain. ABD: CreateSpace Independent Publishing Platform.

Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading digital: Turning technology into business transformation. Harvard Business Press.

Vesa, J. (2005). Mobile Services in The Networked Economy, IGI Global.

Zsidisin, G. A. and Henke, M. (Eds.). (2019). Revisiting Supply Chain Risk. Cham: Boston: Springer.

BOOK CHAPTERS

Walch, A. (2018). Open-source operational risk: should public blockchains serve as financial market infrastructures? In *Handbook of Blockchain, Digital Finance, and Inclusion*, Volume 2 (pp. 243-269). Cambridge: Academic Press.

Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019

ARTICLES

Abeyratne, S. A. and Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(9), 1–10.

Aqlan, F. and Lam, S. S. (2015). Supply chain risk modelling and mitigation. *International Journal of Production Research*, 53(18), 5640-5656.

Aqlan F and Ali E.M. (2014). Integrating lean principles and fuzzy bow-tie analysis for risk assessment in chemical industry*. Journal of Loss Prevention in the Process Industries*, 29, 39-48.

Anggrahini D., Karningsih P.D. and Sulistiyono M. (2015). Managing quality risk in a frozen shrimp supply chain: a case study. *Procedia Manufacturing*, 4, 252-260.

Apte, S. and Petrovsky, N. (2016). Will blockchain technology revolutionize excipient supply chain management? *Journal of Excipients and Food Chemicals*, 7(3), 76–78.

Aste, T., Tasca, P. and Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. *Computer*, 50(9), 18-28.

Babich, V., & Hilary, G. (2019). Distributed ledgers and operations: What operations management researchers should know about blockchain technology. *Manufacturing & Service Operations Management, Vol. 22 No. 2, 1-18.*

Baccarini, D., and Archer, R. (2001). The risk ranking of projects: a methodology. *International Journal of Project Management*, 19(3), 139-145.

Badurdeen F., Shuaib M., Wijekoon K., Brown A., Faulkner W. and Amundson J. (2014). Quantitative modeling and analysis of supply chain risks using bayesian theory. *Journal of Manufacturing Technology Management*, 25(5), 631-654.

Basheer, M., Siam, M., Awn, A. and Hassan, S. (2019). Exploring the role of TQM and supply chain practices for firm supply performance in the presence of information technology capabilities and supply chain technology adoption: A case of textile firms in Pakistan. *Uncertain Supply Chain Management*, 7(2), 275-288.

Basole, R. C. Bellamy M.A. (2014). Visual Analysis of Supply Network Risks: Insights from The Electronics Industry*, Decision Support Systems*, 67, 109-120.

Blos, M., Quaddus, M., Wee, H. and Watanabe, K. (2009). Supply chain risk management (SCRM): a case study on the automotive and electronic industries in Brazil. *Supply Chain Management*, Vol. 14 No. 4, 247-252. https://doi.org/10.1108/13598540910970072

Blackhurst J.V., Scheibe K.P. and Johnson D.J. (2008). Supplier risk assessment and monitoring for the automotive industry. *International Journal of Physical Distribution and Logistics Management*, 38(2), 143-165.

Blos, M. F., Quaddus, M., Wee H.M. and Watanabe K. (2009). Supply Chain Risk Management (SCRM): A Case Study on the Automotive and Electronic Industries in Brazil. *Supply Chain Management: An International Journal*, 14(4), s. 247-252.

Bogataj, D. and Bogataj, M. (2007). Measuring the supply chain risk and vulnerability in frequency space*. International Journal of Production Economics*, 108(1-2), 291-301.

Callegati, F., Cerroni, W. and Ramilli, M. (2009). Man-in-the-Middle Attack to the https Protocol. *IEEE Security Privacy*, 7(1), 78–81.

Chaum, D. (1992). Achieving electronic privacy. *Scientific American*, 267(2), 96-101.

Chopra, S. and Sodhi, M. S. (2004). Supply-chain breakdown. *MIT Sloan Management Review*, 46(1), 53-61.

Cheng, T. C. E., Yip, F. K. and Yeung, A. C. L. (2012). Supply risk management via guanxi in the Chinese business context: The buyer's perspective. *International Journal of Production Economics*, 139(1), 3-13.https://doi.org/10.1016/j.ijpe.2011.03.017

Christopher, M. and Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management*, Vol. 34 No. 5, pp. 388-396. https://doi.org/10.1108/09600030410545436

Elleuch H, Hachicha W. and Chabchoub H. (2014). A combined approach for supply chain risk management: description and application to a real hospital pharmaceutical case study. *Journal of Risk Research*, 17(5), 641-663.

Fazli S., Mavi R.K. and Vosooghidizaji M. (2015) Crude oil supply chain risk management with DEMATEL-ANP. *Operational Research*, 15(3), 453-480.

Ghadge, A., Samir, D. and Kalawsky R. (2012). Supply Chain Risk Management: Present and Future Scope. *The International Journal of Logistics Management*, 23(3), 313-339.

Giannakis, M. and Louis, M. (2010). A multi-agent based framework for supply chain risk management. *Journal of Purchasing and Supply Management*, 17, 23–31.

Hahn G.J. and Kuhn H. (2012). Designing decision support systems for value-based management: A survey and an architecture. *Decision Support Systems*, 53(3), 591-598.

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V. M. and Tuominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics*, 90(1), 47-58.

Harland, C., Brenchley, R. and Walker, H. (2003). Risk in supply networks. *Journal of Purchasing and Supply management*, 9(2), 51-62.

Heckelmann, M. (2018). Zulässigkeit und handhabung von smart contracts. *Neue Juristische Wochenschrift: NJW*, 71(8), 504-510.

Ho, W., Zheng, T., Yildiz, H. and Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research*, 7543 (September), 1–39.

Jaklič, J., Groznik, A., and Kovačič, A. (2003). Towards E–Government: The role of Simulation Modeling. *Simulation in Industry. SCS, Delft*, 257-262.

Johnson, J. E. (2012). Big data+ big analytics= big opportunity: big data is dominating the strategy discussion for many financial executives. As these market dynamics continue to evolve, expectations will continue to shift about what should be disclosed, when and to whom. *Financial Executive*, *28*(6), 50-54.

Jüttner, U., Peck, H., and Christopher, M. (2003). Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, 6(4), 197-210.

Kern D., Moser R., Hartmann E. and Moder M. (2012). Supply risk management: model development and empirical analysis. *International Journal of Physical Distribution and Logistics Management*, 42(1), 60-82.

Kleindorfer P.R. and Saad G.H. (2005). Managing disruption risks in supply chains. *Production and Operations Management,* 14(1), 53-68.

Koch, C. (2004). Nike Rebounds How (and Why) Nike Recovered from Its Supply Chain Disaster. *CIO-FRAMINGHAM MA-*, 17(17), 56-63.

Lambert, D. M., Cooper, M. C. and Pagh, J. D. (1998). Supply chain management: implementation issues and research opportunities. *The International Journal of Logistics Management*, 9(2), 1-20.

Lavastre, O., Gunasekaran, A. and Spalanzani, A. (2012). Supply chain risk management in French companies. *Decision Support Systems*, 52(4), 828-838.

Li C., Ren J. and Wang H. (2016). A System dynamics simulation model of chemical supply chain transportation risk management systems. *Computers and Chemical Engineering*, 89, 71-83.

Muchfirodin M., Guritno A.D. and Yuliando H. (2015). Supply chain risk management on tobacco commodity in temanggung, central java (Case Study at Farmers and Middlemen Level). *Agriculture and Agricultural Science Procedia*, 3, 235-240.

Muellerleile, C. M. (2009). Financialization takes off at Boeing. *Journal of Economic Geography*, 9(5), 663–677. doi:10.1093/jeg/lbp025

Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L. and Brooks, R. (2016). A brief survey of Cryptocurrency systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST),* 745–752.

Narasimhan, R. and Talluri, S. (2009). Perspectives on risk management in supply chains. *Journal of Operations Management*, Vol:27, No:2, 114–18.

Nishat Faisal, M., Banwet, D. and Shankar, R. (2006), Supply chain risk mitigation: modeling the enablers. *Business Process Management Journal*, 12(4), 535-552. https://doi.org/10.1108/14637150610678113

Nyoman Pujawan, I. and Geraldin, L. H. (2009). House of risk: a model for proactive supply chain risk management. *Business Process Management Journal,* 15(6), 953-967.

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

Norlaile S.H. and Abu Bakar A.H. (2015). Supply chain risk management in automotive small and medium enterprises in Malaysia. *Applied Mechanics and Materials*, 773, 799-803, 2015.

Norrman, A. and Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International journal of physical distribution & logistics management*. Vol: 34, No:5, 434–56.

Nyoman Pujawan, I. and Geraldin, L. (2009). House of risk: a model for proactive supply chain risk management. *Business Process Management Journal*, Vol. 15 No. 6, 953-967. https://doi.org/10.1108/14637150911003801

Ohmori S. and Yoshimoto K. (2013). A framework of managing supply chain disruption risks using network reliability. *Industrial Engineering and Management Systems*, 12(2), 103-111.

Piazza, F. S. (2017). Bitcoin and the blockchain as possible corporate governance tools: Strengths and weaknesses. *Penn State Journal of Law & International Affairs*, 5(2), 262–301.

Ross, E. S. (2017). Nobody puts blockchain in a corner: The disruptive role of blockchain technology in the financial services industry and current regulatory issues. *Catholic University Journal of Law and Technology,* 25(2), 353–386.

Rothstein, R. (1997). Union Strength in the United States: Lessons from the UPS Strike. *International Labour Review*, 136(4), 469-491.

Sheffi, Y. (2005). Preparing for the big one [supply chain management]. *Manufacturing Engineer*, 84(5), 12-15.

Sinha, P. R., Whitman, L. E. and Malzahn, D. (2004). Methodology to mitigate supplier risk in an aerospace supply chain. *Supply Chain Management: An International Journal*, Vol:9, No:2, 154–68.

Sinha, K. K. and Van de Ven, A. H. (2005). Designing work within and between organizations. *Organization Science*, 16(4), 389-408.

Speier C., Whipple J.M., Closs D.J. and Voss M.D. (2011). Global supply chain design considerations: Mitigating product safety and security risks. *Journal of Operations Management*, 29(7), 721-736, 2011.

Subashini, S. and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11.

Suharjito M. and Marimin M. (2015). DSS for agricultural products supply chain risk balancing using stakeholder dialogues and fuzzy nonlinear regression. I*nternational Journal of Hybrid Information Technology*, 8(1), 11-26.

Surujnath, R. (2017). Off the chain! A guide to blockchain derivatives markets and the implications on systemic risk. *Fordham Journal of Corporate & Financial Law*, 22(2), 256–304.

Svantesson, D. and Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law & Security Review*, 26(4), 391-397.

Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,(16)*, *18*, 2.

Tang, S. C. (2006). Perspectives in Supply Chain Risk Management. *International Journal of Production Economics*, 103 (2), 451–488.

Tang, O. and Musa S.N. (2011). Identifying Risk Issues and Research Advancements in Supply Chain Risk Management. *International Journal of Production Economics*, 133(1), 25-34.

Tang, O. and Musa, S. N. (2010). Designing fuzzy- genetic learner model based on multi-agent systems in supply chain management. *Internation Journal of Production Economics*, 133, 25–34.

Thun, J. H. and Hoenig, D. (2011). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics*, 131(1), 242-249.

Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084-2123.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, 59(11), 15–17. https://doi.org/10.1145/2994581

Vilko, J. P. and Hallikas, J.M. (2012). Risk Assessment in Multimodal Supply Chains. *International Journal of Production Economics*, 140(2), 586-595.

Wieland, A. and Wallenburg, C. M. (2012). Dealing with supply chain risks. *International Journal of Physical Distribution & Logistics Management*, Vol:42, No:10, 887–905.

Wu T., Blackhurst J., Chidambaram V. A. (2006). Model for inbound supply risk analysis. *Computers in Industry*, 57(4), 350-365.

Xu, L. D. (2011). Information architecture for supply chain quality management. *International Journal of Production Research*, 49(1), 183-198.

Yoo, S. (2017). Blockchain based financial case analysis and its implications. *Asia Pacific Journal of Innovation and Entrepreneurship*, 11(3), 312–321.

Yu, M.-C. and Goh, M. (2014). A multi-objective approach to supply chain visibility and risk. *European Journal of Operational Research*, 233(1), 125–130.

Zimmermann, M., Rosca, E., Antons, O. and Bendul, J. C. (2019). Supply chain risks in times of Industry 4.0: Insights from German cases. *IFAC-PapersOnLine*, 52(13), 1755-1760.

Zissis, D. and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592.

PROCEEDINGS

Akkartal, G. (2018). Determination of Ris Management Maturity Levels of Supply Chain Management Companies. *25th EBES Conference - Berlin Proceedings* - Vol 3. 23-25 May 2018, Berlin, Germany.

Bahack, L. (2013). Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft). *arXiv preprint arXiv:1312.7013*.

Bhargava, B., Ranchal, R., and Ben Othmane, L. (2013). Secure information sharing in digital supply chains. *In 2013 3rd IEEE International Advance Computing Conference (IACC)*, 1636–1640. http://doi.org/10.1109/IAdCC.2013.6514473

Blanchard, D. (2003). Moving Past the Problems Can Be Problematical. *Chief Logistics Officer,* 5(4).

Dua, G., Gautam, N., Sharma, D. and Arora, A. (2013). Replay attack prevention in Kerberos authentication protocol using triple password. *ArXiv Preprint arXiv:1304.3550*.

Gahi, Y., Guennoun, M., & Mouftah, H. T. (2016, June). Big data analytics: Security and privacy challenges. In *2016 IEEE Symposium on Computers and Communication (ISCC)* (pp. 952-957). IEEE.

Korpela, K., Hallikas, J. and Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. *In proceedings of the 50th Hawaii international conference on system sciences.*

Lakhani, K. R. and Iansiti, M. (2017). The truth about blockchain. *Harvard Business Review*, *95*, 118-127.

McAfee, A. and Brynjolfsson, E. (2012). Büyük Veri, Yönetim Devrimi'. *Harvard Business Review Türkiye, Ekim*, 70-77.

Pflaum, A., Prockl, G., Bodendorf, F. and Chen, H. (2018). The digital supply chain of the future: from drivers to technologies and applications. minitrack ıntroduction. *The 51st Hawaii International Conference on System Sciences.* HICSS 2018 Hawaii International Conference on System Sciences (pp. 3924-3925).

Rosenfeld, M. (2011). Analysis of bitcoin pooled mining reward systems. *ArXiv Preprint arXiv:1112.4980.*

WEB RESOURCES

Bharat, P. (2019). Improving Retail Effectiveness Through Technology, Web Site, Retrieved from https://pdfs.semanticscholar.org/fdf8/4c1ba40683f59637f9a7efe9c92b6eb05b19.pdf Accessed 15 January 2019.

Ontario, 2020. Retrieved from https://news.ontario.ca/mgs/en/2020/03/ontario-protecting-supply-chains-to-support-covid-19-emergency-response.html

KAP (2020a). Retrieved from https://www.kap.org.tr/en/Bildirim/833484 Accessed 13 May 2020

KAP (2020b). Retrieved from https://www.kap.org.tr/en/sirket-bilgileri/ozet/838-akcansa-cimento-sanayi-ve-ticaret-a-s Accessed 13 May 2020

KAP (2020c). Retrieved from https://www.kap.org.tr/en/Bildirim/831663 Accessed 13 May 2020

REPORTS

AON (July 2019). The price of data security: A guide to the insurability of GDPR fines across Europe (2nd Edition), DLA Piper. Retrieved from https://www.aon.com/risk-services/gdpr-fines-guide.jsp

AON Cyber Security Risk Report (2019). Retrieved from https://www.aon.com/getmedia/4c27b255-c1d0-412f-b861-34c5cc14e604/Aon_2019-Cyber-Security-Risk-Report.aspx

Kantarcı, Ö., Özalp, M., Sezginsoy, C., ÖZAŞKINLI, O. and Cavlak, C. (2017). Dijitalleşen dünyada ekonominin itici gücü: E-ticaret. TUSIAD Yayınları, İstanbul.

LODER Lojistik Derneği, (2020). Koronavirüs Tedarik Zincirlerini Kırdı, Yazar: Tanyaş Mehmet. s. 1-3. Retrieved from https://mcusercontent.com/833f5af578ece3a8381433fe4/files/34ca29b5-c471-45f1-ae64-2ada1c980a98/Koronaviru_s_LODER_Gorusu_24_03_2020_1_.pdf

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system (Technical Report). Retrieved from www.bitcoin.org

PWC-PriceWaterHouseCoopers (2019). Tedarik Zinciri Yönetimi Araştırması 2019. Çevrimiçi https://www.pwc.com.tr/tr/hizmetlerimiz/danismanlik/yayinlar/tedarik-zinciri-yonetimi-arastirmasi-2019.html

PWC- PriceWaterHouseCoopers (2019). ''Siber risk sigortası hakkında bilinmesi gerekenler'' Retrieved from https://www.pwc.com.tr/tr/hizmetlerimiz/dijital-hizmetler/siber-guvenlik-ve-verikoruma-hizmetleri/yayinlar/siber-risk-sigortasi-hakkinda-bilinmesi-gerekenler.html/ Accessed 05.10.2019

PWC-PriceWaterHouseCoopers (2020). COVID-19: Operasyonlar ve Tedarik Zinciri Etkisi 2020. Retrieved from https://www.pwc.com.tr/tr/Hizmetlerimiz/danismanlik/tedarik-zinciri-yonetimi/covid-19-operasyonlar-ve-tedarik-zinciri-etkisi.pdf

Powell, M., (2019). '11 Eye Opening Cyber Security Statistics For 2019'. Retrieved from https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-securitystatistics-for-2019// Accessed 02 November 2019

Schrauf, S. and Bertram, P. (2016). Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused. Price Waterhouse Coopers Strategy. Retrieved from https://www.strategyand.pwc.com/gx/en/insights/2016/industry-4-digitization/industry40.pdf

Szabo, N. (2017). Smart Contracts: Building Blocks for Digital Markets. 1996. Retrieved from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool 2006/szabo.best.vwh.net/smart_ contracts_2.html (дата обращения: 30 июля 2018 г.). Accessed August 2018

Raab, M. and Griffin-Cryan, B. (2011). Digital Transformation of Supply Chains: Creating Value – When Digital Meets Physical. Capgemini Consulting, p. 12. Retrieved from https://www.capgemini.com/resources/digital-transformation-of-supply-chains/

Raj, S. and Sharma, A. (2014). Supply chain management in the cloud. Accenture Global Management Consulting, 1-12.

Trendmicro (2017). Retrieved from https://newsroom.trendmicro.com/press-release/commercial /trend-micro-reveals-top-ten-regions-affected-iot-security-threats Accessed 15 August 2017

WEF (World Economic Forum) (2017). The Global Risks Report 2017. Retrieved from http://www3.weforum.org/docs/GRR17_Report_web.pdf

WEF (World Economic Forum) (2020). The Global Risks Report 2020. Retrieved from http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

THESIS

Erşen, İlker, (1999), Sigortacılıkta Risk Yönetimi, Yayınlanmamış Y.Lisans Tezi, İTÜ Sosyal Bilimler Enstitüsü, İstanbul.

WEB SOURCES

Bheemaiah, K. (2015). Blockchain 2.0: The renaissance of money. Retrieved from https://www.wired.com/insights/2015/01/block-chain-2-0/

Imaa Institute. Retrieved from https://imaa-institute.org/mergers-and-acquisitions-statistics/

Kaspersky. (2017). Retrieved from https://www.kaspersky.com.tr/about/press-releases/2017_turkiye-yi-de-kapsayan-bolgenin-siber-tehdit-trenleri-aciklandi Accessed 20 May 2017

Kazeem, Y. (2018). The world's first blockchain-supported elections just happened in Sierra Leone. Retrieved from https://qz.com/1227050/sierra-leone-elections-powered-by-blockchain/ Accessed 29 March 2018.

Meucci, M. and Muller, A. (2014). OWASP Testing Guide V. 4.0. Open Web Application Security Project, 30.

Satyavolu, P. and Sangamnerkar, A. (2016). Blockchain's Smart Contracts: Driving the Next Wave of Innovation Across Manufacturing Value Chains. Cognizant 20-20- Insights, (June). Retrieved from https://www.cognizant.com/whitepapers/blockchains-smart-contracts-driving-the-next-waveof-innovation-across-manufacturing-value-chains-codex2113.pdf

The Economist (2015). The great chain of being sure about things. Retrieved from http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trusteach-other-build-dependable Accessed 15 Oct 2017

WHO (2020). World Health Organization. Retrieved from https://www.who.int/news-room/q-a-detail/q-a-coronaviruses