# Smart contract challenges and drawbacks for SME digital resilience

Zirar, Araz ; Jabbar, Abdul; Tchouamou Njoya, Eric ; Amoozad Mahdiraji, Hannan

*DOI:*
10.1108/JEIM-02-2023-0082

## 1. Introduction

In an increasingly digitalised world, many small to medium enterprises (SMEs) lack digital skills but are heavily reliant on technological infrastructure. An increase in cyber-attacks, hacking, fraud and viruses has created significant problems for SMEs as they attempt to navigate and build digital resilience (Hussain et al., 2023). In this paper the authors propose the potential of smart contracts (SCs) to enhance digital resilience due to its permanent, immutable, transparent, and traceable nature (Agrawal *et al.,* 2022; Elhidaoui *et al.,* 2022). Digital resilience is defined as an organisation's ability to withstand and recover from disruptions, threats, or challenges in the digital domain (Bavassano *et al.,* 2020). However, the innovation challenges for SMEs in developing resilience through the use of SCs require a skilled workforce and comes with its own unique challenges, it is these we explore further.

In the view of Leifels (2021) a sizable portion of German SMEs view digital skills as essential, with over 80% placing value on fundamental abilities and 25% demanding advanced knowledge. The difficulties experienced by SMEs in meeting the demand for digital skills are caused by factors including fast digital transition, an ageing workforce, and decreased investment in workplace education. Hence, many SMEs lack key skills in digital trust, security, and resilience, which are critical for organisational growth and new business model development (Bavassano et al., 2020). These challenges take on significant prominence when organisations attempt to develop organisational resilience through the use of new technology such as smart contracts. The concept of SCs was introduced by Nick Szabo in 1994 to mean a ‘set of promises, specified in a digital form, including protocols within which the parties perform on the other promises’ (Antonopoulos & Wood, 2018, p. 127, as cited in Jabbar & Dani, 2020). When a smart contract is called, it self-executes and self-enforces the contractual agreements encoded

in the piece of the code (Drummer & Neumann, 2020). Therefore, a smart contract establishes trust between transaction parties without intermediaries (Christidis & Devetsikiotis, 2016, as cited in Jabbar & Dani, 2020). Recent research by Devine *et al.,* 2021 and Jabbar & Dani (2020) view SCs as a solution to the critical issue of digital trust.

Thus, while there is a considerable amount of research on SCs, the majority of this looks at the "hype" around smart contract and eulogises its benefits without properly considering the drawbacks. In addition the majority of the research has a focus on their application and development within supply chains (Dal Mas et al., 2020; De Giovanni, 2020; Kordestani et al., 2023; Wang & Xu, 2022). The work around smart contracts has over the years blossomed, we argue that to discuss their role in digital resilience is still an area of growth, especially in the context of SMEs. Taking a novel approach the authors through the literature review explore the notion that while smart contracts can enhance resilience they are plagued with vulnerabilities, privacy concerns, legal obstacles, and performance limitations when considering digital resilience (Drummer & Neumann, 2020; Khan et al., 2021; Zou et al., 2021). These hurdles can impede the ability of smart contracts to effectively handle the complexities of contractual agreements in certain industries due to the rigid structure of smart contracts (Drummer & Neumann, 2020; Jabbar & Dani, 2020; Khan et al., 2021). To explore the research gap, a systematic literature review was conducted (Tranfield *et al.,* 2003) underpinned and analysed through thematic analysis (Braun and Clarke, 2022). The analysis indicates that it is crucial to address the multiple drawbacks of SCs for supply chain resilience. Although SCs hold significant potential for creating innovative business models, having a well-defined growth plan that acknowledges the key limitations is essential.

## 2. Literature review

Looking at SCs through the lens of digital resilience provides a new scope of enquiry aiming to investigate practical and theoretical elementss which focus on the pitfalls of digital disruption within supply chains or SMEs (Kumar et al., 2023). For areas such as supply chain management, the potential for disruption is significant, and the challenges are monumental. Historical research from supply chains looks at the blockchain and, to some extent, SCs as trusted intermediaries. Rashideh (2020) discusses this in more detail and argues that little thought up to this point has been given to applying SCs for SMEs in the context of digital resilience:

**Table 1.** Examples of earlier works on smart contracts as a trusted intermediary

| Reference | Key points |
|---|---|
| Thompson & Rust (2023) | Food fraud creates resistance to blockchain and smart contract adoption |
| Kordestani et al. (2023) | Smart contracts offer unique characteristics to combat counterfeit drugs |
| Wang & Xu (2022) | Smart contracts reduce overpricing behaviour |
| Tan et al. (2022) | Smart contracts to improve halal supply chain food |

### *2.1 Industry 4.0 and SMEs*

SMEs play a vital role in developed and developing economies, representing more than 99% of all businesses in the EU (European Parliament, 2021), about 90% of all businesses globally, accounting for more than 50% of total employment worldwide. Because of their importance in driving economic growth, governments worldwide have prioritised the development of SMEs. Industry 4.0 is an umbrella term for various technologies, such as the Internet of Things (IoT), autonomous robots, big data, blockchain, additive manufacturing, and cloud computing (Pozzi et al., 2023). However, research suggests that

industry-specific and country-specific barriers and overregulation impede implementation (Ślusarczyk, 2018; Kumar and Singh, 2021). This line of research suggests that the main drivers for implementing Industry 4.0 technologies include knowledge, expected benefits (Yu and Schweisfurth, 2020), and structural and cultural changes (Jerman *et al.,* 2020; Vrchota *et al.,* 2021). Müller, Kiel et al. (2018) show that strategic, operational, environmental, and social opportunities of Industry 4.0 implementation positively affect manufacturing tendencies.

Another strand of the literature has assessed the factors that influence the implementation of the industry 4.0 concept in the SME sector, focusing on organisational readiness and maturity (Müller, Buliga et al., 2018; Müller, Kiel et al., 2018). Müller, Buliga, et al. (2018) examine maturity/readiness/assessment models and their fit for SMEs, concluding that a limited number of the available smart manufacturing/Industry 4.0 roadmaps, maturity models, frameworks and readiness assessments reflect the specific requirements and challenges of SMEs.

### *2.2 Digital Resilience*

Holling (1996), as stated in Wright (2016), outlines two definitions of resilience; the first is '*engineering resilience'*, which is the ability to recover quickly to a prior desired state, and the second is '*ecological resilience'*, which considers whether a system can recover to a prior desired state. Accordingly, digital resilience is the ability to withstand and recover from technological disruptions and threats (Wright, 2016). Digital resilience is becoming increasingly critical in the face of frequent, unpredictable disruptions and the rise of new Industry 4.0 technologies such as cloud computing, artificial intelligence (AI), blockchain, and quantum technology. Digital resilience for SMEs is concerned with the ability to adapt to and recover from the impacts of digital disruption (Etalong *et al.,* 2022).

For SMEs to build digital resilience, Fernandez-Jardon *et al. (*2020) prescribe three key focus areas: strategy, technology, and culture. A clear and comprehensive digital strategy outlines the steps needed to adapt and benefit from the changes brought about by digital disruption. Investment in technology and infrastructure will enable SMEs to thrive in the digital economy (Asadi et al., 2023; Masood & Sonntag, 2020). Finally, cultivating a digital-first culture encourages innovation and supports new technology adoption (Moeuf et al., 2020; Masood & Sonntag, 2020). Resilience development should involve training employees for the required skill set in the digital economy, as well as a focus on fostering collaboration and encouraging open communication (Arslan et al., 2021; Zirar et al., 2023).

**Table 2.** Historical research on digital resilience

| Source | Purpose | Major findings |
|---|---|---|
| Burgel et al. (2023) | Impact of digitalisation on organisational resilience in times of pandemic crises | Entrepreneurial firms with more digitalized business models show higher resilience to pandemic crises |
| Corvello et al. (2022) | Impact of digital technologies on the development of antifragility in SMEs | Key factors enabling anti-fragile behaviour in organizations include slack financial resources, strategic agility, and relations with research institutions, and digital technologies. |
| Costa and Castro (2021) | e-commerce adoption by SMEs | e-commerce adoption by SMEs is crucial for maintaining the vibrancy of the business ecosystem and facilitating economic recovery. |
| Di Vaio et al. (2023) | Role of artificial knowledge and digitalization in supply chain management accountability and sustainable performance | Artificial knowledge and digitalization are crucial in achieving sustainable and resilient supply chain management (SCM) business models aligned with the UN 2030 Agenda. |
| Florek-Paszkowska et al. (2021) | Impact of entrepreneurship, and innovation on business resilience, stability, and competitive advantage | Factors contributing to business innovation include human-based factors, such as competent and open-minded leaders, and talented employees, as well as non-human-based factors, including a supportive business culture, transformative business models, novel strategies, and disruptive technologies depending on digital maturity. |
| Guo et al. (2020) | Relationship between SMEs' digitalization and their public crisis responses | Digitalization empowers SMEs to effectively respond to crises and leverage their dynamic capabilities, leading to improved performance. |
| Han and Trimi (2022) | Link between Industry 4.0 and organizational agility, adaptability, and resilience | The paper offers solutions for SMEs to address technology, trust, and big data challenges in adopting Industry 4.0. |
| Hossain et al. (2022) | Impact of Covid-19 on SMEs | Cash flow shortages and Supply Chain Disruptions are the critical constraints of SMEs, while digital transformation, including technology adoption, digital marketing, and innovations, has been instrumental in achieving success and profitability during the crisis. |

| | | |
|---|---|---|
| Hu and Kee (2022) | Impact of Covid-19 on SMEs | In the post-COVID-19 era, SMEs must be dynamic, forward-looking, and transformational to seize regional and global market opportunities by enhancing internal competencies and aligning their business strategies accordingly. |
| Kang et al. (2016) | Survey and analyse articles related to Smart Manufacturing in order to identify key technologies, assess the current state, and predict future trends | Smart Manufacturing involves the convergence of cutting-edge ICT technologies with existing manufacturing technologies, enabling real-time decision-making and enhancing competitiveness in the manufacturing industry |
| Khalil et al. (2022) | Impact of digital technologies on the resilience of SMEs during the COVID-19 pandemic | Digital technology has played a crucial role in helping SMEs survive the pandemic and become more resilient |
| Khurana et al. (2022) | Impact of digital technologies on SMEs resilience capability during a crisis | The study reveals a multilevel model of resilience capability in SMEs, where they shift focus from core to periphery, emphasizing dynamic capabilities and digital technologies' transformative potential. |
| Nan and Park (2022) | Impact of mobile money on SMEs' resilience in times of crisis | SMEs are more susceptible to significant sales decline but incorporating digital technologies can mitigate this vulnerability. |
| North et al. (2020) | Guidance for SMEs to sense, seize, and transform through digital opportunities and project-based learning for competitiveness in turbulent environments. | SMEs demonstrate moderate maturity in digitalization, with a focus on sensing opportunities but a need to improve their ability to seize them. |
| Santos et al. (2023) | Role of digital technologies in entrepreneurial resilience during the COVID-19 pandemic | Digital artifacts, platforms, and infrastructures were identified as key elements used by entrepreneurs to exhibit resilience. |
| Westerlund (2020) | Compare internationally oriented online SMEs with domestically-focused SMEs in terms of their digitalization | Internationally oriented SMEs show higher usage of information systems, greater extent of value networks, emphasis on key internal resources, and attention to cybersecurity. |

### *2.3 Smart Contracts*

SCs are tools designed to remove intermediaries from transactions (Petersson, 2018). A decentralised smart contract, or "programmable' contract', automatically executes agreed contracts transparently and without human influence or intervention (Drummer and Neumann, 2020; Ferreira, 2021; Sharma et al., 2022). SCs experienced a practical breakthrough with the emergence of blockchain technology after 2008, as the underlying blockchain technology provided a platform to disintermediate the storage and execution of trust and data integrity (Drummer and Neumann, 2020; Ferreira, 2021). Further, despite being introduced in 1994 and the emergence of blockchain technology after 2008, smart contracts only gained popularity with the introduction of the Ethereum public blockchain in 2013 (Petersson, 2018). This is mainly because, unlike the Bitcoin blockchain, smart contracts appended to the Ethereum blockchain execute faster in higher quantities with cheaper costs (Jabbar and Dani, 2020).

SCs are self-executing and self-enforcing scripts that follow a sequence of commands when activated and recorded on the blockchain (Sunny et al., 2020; Yong et al., 2020). These trustless, autonomous, decentralised, and transparent contractual agreement scripts are typically irreversible and unmodifiable when appended to a blockchain (Dal Mas et al., 2020; Sharma et al., 2022). Any changes to the script will create a new block on the concerning blockchain. The code that defines the transaction processes is the final arbiter of the terms in a smart contract (UK Jurisdiction Taskforce, 2019; Drummer and Neumann, 2020).

First and second parties, when transacting by calling a smart contract, do not need to trust one another or request the services of third parties as intermediaries (Drummer and Neumann, 2020; Ferreira, 2021). Instead, the smart contract will render such transactions allowing the first and second parties to reach a consensus and record such

transactions immutably on the assigned blockchain (Ferreira, 2021; Sharma et al., 2022; Sukumar et al., 2022). A smart contract embeds the terms and conditions of the contract between the parties, and the parties can transact (generally) anonymously (Drummer and Neumann, 2020; Ferreira, 2021; Sharma et al., 2022; Dewitt et al., 2022). Therefore, without efficient and effective smart contracts, the benefits will not be realised (Qin et al., 2021). Because of the developing nature of smart contract technology, this literature is fragmented and inconclusive, still in its early phases (Hughes et al., 2019; Saberi et al., 2019). The literature is generally engaged with propositions (Manupati et al., 2020), prototypes (Chang et al., 2019; Sahoo et al., 2021), and concept-centric approaches (Mendhurwar and Mishra, 2021).

### *2.4 SMEs' digital resilience and SCs*

In our research, we have highlighted the various impacts of smart contracts (SCs) on automation, cost savings, efficiency gains, risk management, and resilience in SMEs' business processes (Katsikouli et al., 2021; Kaur et al., 2022; Prisco et al., 2022). By utilizing SCs, SMEs can save costs by reducing errors, labour, and the need for intermediaries like lawyers and banks (Khan et al., 2021; Zou et al., 2021). Furthermore, there are efficiency gains as SCs streamline the execution of agreements, reducing time and effort (Drummer & Neumann, 2020) and improving access to credit (Kaur et al., 2022).

Existing literature suggests that SMEs' decision to adopt SCs is influenced by opportunity costs. Similar to large organizations, SMEs face pressure to optimize and streamline contractual agreements (Asante Boakye et al., 2023; Faasolo & Sumarliah, 2022; Wong et al., 2020). While risk aversion or resilience may not be the primary drivers for SMEs to adopt SCs, the need to streamline business operations compels their use (Faasolo & Sumarliah, 2022). However, unlike larger organizations with more resources,

SMEs base their decisions on the perceived usefulness and associated risks of SC adoption (Clohessy & Acton, 2019; Faasolo & Sumarliah, 2022).

While SCs enhance SMEs' resilience in areas such as security, transparency, immutability (Asadi et al., 2023; Faasolo & Sumarliah, 2022; Iranmanesh et al., 2023), traceability, fair trade, and authenticity documentation (Katsikouli et al., 2021), the risks, such as limited capital for SC investment and the potential for wasted resources (Faasolo & Sumarliah, 2022; Ilbiz & Durst, 2019; Katsikouli et al., 2021), often outweigh the perceived usefulness. Unless adoption decisions are informed by research, SMEs are left to make decisions based on perceived usefulness and perceived risks (Asante Boakye et al., 2023; Bracci et al., 2021; Sun et al., 2021).

## 3. Methodology

The article collection process consisted of formulating the review question, determining the keywords, and identifying, collecting, analysing and synthesising the relevant literature (Tranfield et al., 2003; Klein and Potosky, 2019; Green et al., 2022).

### *3.1 Review Question*

To fully explore the phenomenon of smart contract challenges, we first explored published articles which included the keywords 'smart contracts', 'supply chains' and SMEs. In this endeavour, we looked at different articles, such as Badi et al. (2021), Drummer and Neumann (2020), Ferreira (2021), Grida and Mostafa (2022) and others to understand the line of research that refers to the challenges of employing smart contracts. This investigation led to the following research question:

*RQ: Within digital resilience, what are the challenges of employing smart contracts for SMEs?*

### *3.2 Keywords Identification*

For detailed keyword identification, we use a three-level-keyword assembly structure (Table 3). At level 1, we search for “smart contract” for a holistic overview. We then build on this, and in level 2, we define a more complex search term. This Boolean string was built on published articles, such as Masood & Sonntag (2020). Similarly, we retrieved the keywords in the third level on supply chain from published articles in this area, such as Modgil et al. (2023).

**Table 3.** A three-level-keywords assembly structure

| | |
|---|---|
| Level 1 | "smart contract" |
| Level 2 | "small business" OR "small ? medium sized enterprise*" OR smes OR micro?business OR micro?enterprise OR micro?firm* |
| Level 3 | "supply chain" OR "value chain" OR "demand chain" |

### *3.3 Search String Formulation*

From the identified keywords, we formulated the following search string:

*( ("smart contract") AND ( ("small business" OR "small ? medium sized enterprise*" OR smes OR micro?business OR micro?enterprise OR micro?firm* ) OR ("supply chain" OR "value chain" OR "demand chain") ) )*

Initially, we used the Boolean operator “AND” between keywords on level 2 and level 3 (Table 3). However, this attempt forced the search string to return articles only if such articles had the three-level keywords. We reasoned that this approach would significantly narrow the list of returned articles. We, therefore, changed “AND” between the second and third-level keywords to “OR”. This way, we ensured that articles with “smart contract” and keywords from second or third levels were returned.

### *3.4 Searching the Scopus Database*

Using a systematic literature search, we utilised Scopus to locate relevant articles (Tranfield *et al.,* 2003). The existing literature suggests that the choice of Scopus vs other databases can also depend on their availability at an institute level (Burnham, 2006, p. 1). Therefore, we chose the Scopus database as it was available to the authors. The process of selecting the articles is illustrated in Figure 1.

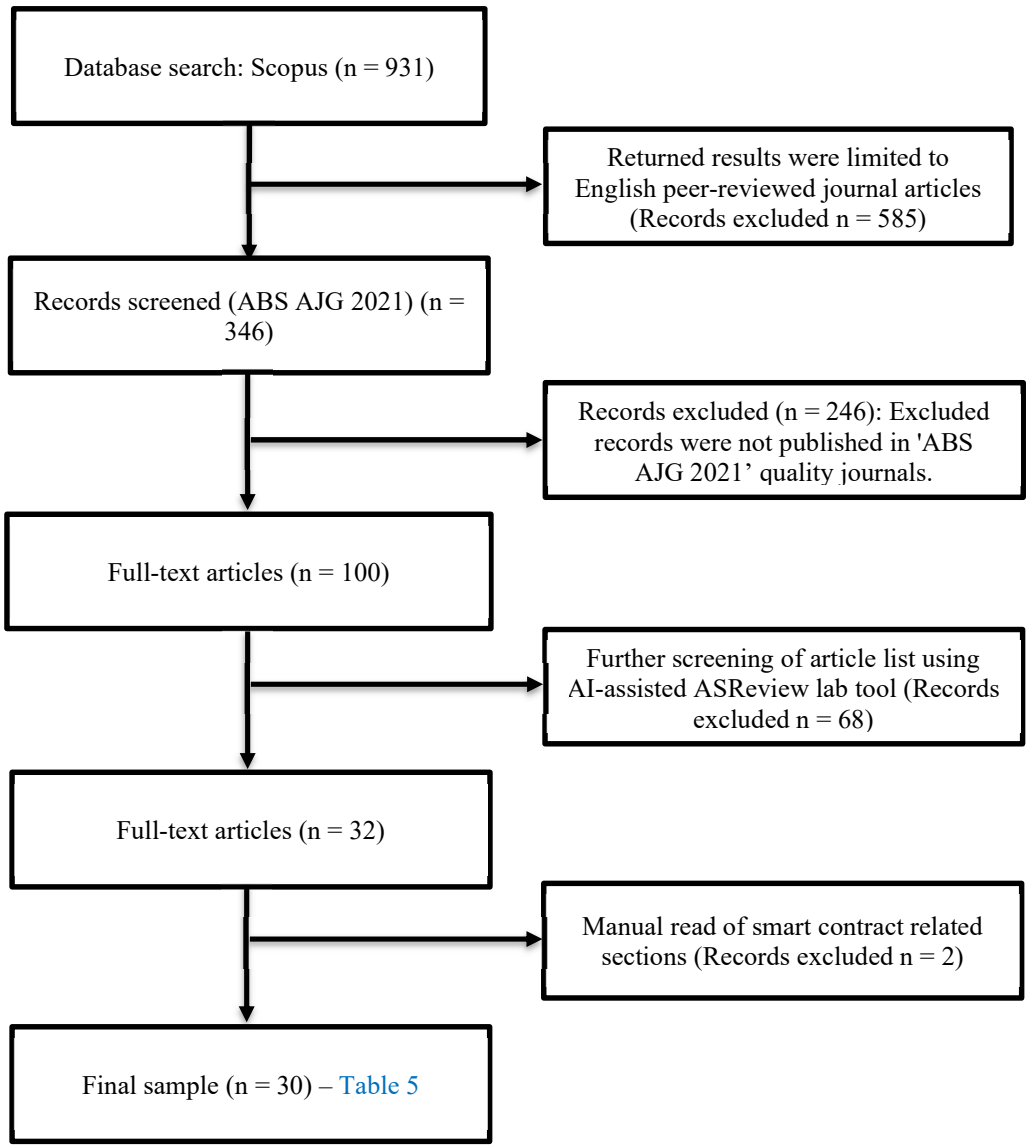


**Figure 1.** The process of selecting the articles

### *3.5 Document Filtering*

The search initially retrieved 931 documents based on the search string. However, after applying inclusion and exclusion criteria, including language (English), source (journal), and document type (article), the list was reduced to 346 articles. To further refine the selection, only peer-reviewed articles published in journals ranked in the 'ABS AJG 2021' list were included. The ABS list was used as a filter based on recommendations from existing literature (e.g., Purkayastha & Kumar, 2021; Soundararajan et al., 2018; Zirar et al., 2023). This approach ensured that the chosen articles were from journals that underwent peer review, editorial scrutiny, and expert judgment. Non-peer-reviewed articles, PhD dissertations, books, and book chapters were excluded from the list. The Scopus field code EXACTSRCTITLE () was employed to limit the results to ABS-listed journals, using a supplied list of ABS-ranked journals. A further reduction was made by using the AI-assisted ASReview tool (van de Schoot *et al.,* 2021; Satyanarayana *et al.,* 2022). ASReview is a machine learning-based screening system that accelerates screening titles and abstracts when conducting a systematic review, improving the efficiency of the screening process of titles and abstracts (van de Schoot et al., 2021). Articles had to satisfy thematic requirements to be included in the analysis. The final list of articles for the analysis was reduced to 30 full-text articles.

**Table 4.** The inclusion and exclusion criteria

| | |
|---|---|
| Language | English Language |
| Source type | Journal |
| Document type | Article |
| Source journal rating | CABs Ranked – Using the field code EXACTSRCTITLE () |
| Further screening | Using the AI-assisted ASReview lab tool |
| Thematic requirements | Manual reading of smart contract-related sections |

### *3.6 Analysis Process*

For this stage, we organised the articles into themes and adopted reflexive thematic analysis to interpret the data (Braun and Clarke, 2019, 2022). 'This analysis method relies on the researchers' interpretation and active engagement with the data considering the research question (Braun and Clarke, 2022; Byrne, 2022; Terry and Hayfield, 2020). Thematic analysis allows researchers to perceive data on a deeper level, helping them immerse themselves in the data, identify hidden interpretations and assumptions and explore the implications of meaning (Braun and Clarke, 2022; Byrne, 2022). Thematic analysis is an iterative process where data is investigated and explored via multiple rounds (Braun and Clarke, 2022; Byrne, 2022; Terry and Hayfield, 2020). They are meaningful entities from codes that capture the essence of meanings from data (Braun and Clarke, 2022; Terry and Hayfield, 2020).

The researchers used the six phases of thematic analysis (Braun and Clarke, 2006; Braun et al., 2019) to guide them in anchoring data to themes. In the first phase, the researchers immersed themselves in the selected articles by re-reading them to familiarise themselves with the data. In the second phase, the researchers started anchoring statements from the selected articles to interesting codes such as "legal issues", "security concerns", etc. In the third phase, constructing themes, themes were "built, folded, and given meaning" (Braun and Clarke, 2019). The researchers explored latent meanings, connections, and possible interpretations such as "smart contracts in their current format are inaccessible to legislators" (Boubeta-Puig *et al.,* 2021) or "smart contracts prone to human error at the entry phase" (Liu *et al.,* 2021) etc. The researchers reviewed the candidate themes in the fourth and fifth phases and revised and defined them. The researchers discussed the themes among themselves and in research circles to enhance reflexivity and interpretative depth (Braun and Clarke, 2022). In the sixth phase, the

researchers used an iterative approach to report the themes with supporting references from the list of selected articles and relate the analysis to the research question (Braun and Clarke, 2022).

## 4. Thematic Analysis

We identified seven key drawbacks of smart contracts (Table 5). The identified areas were as follows:

- Manipulation (15 Instances)
- Legality (22 Instances)
- Hacking and Security Concerns (14 Instances)
- Confidentiality (7 Instances)
- Fraud (10 Instances)
- Human Error (12 Instances)
- Technical Limitations (15 Instances)

In Table 5, we utilise the seven key criteria to organise the literature to better identify the key challenges in SC adoption within the context of digital resilience. We have combined Hacking and Security Concerns into one criterion for brevity. To organise and recognise the key areas of concern and drawbacks of smart contracts, we use the work of Khan *et al.* (2021) and Zou *et al.* (2021) to group the seven key drawbacks.

**Table 5.** Key drawback summary

| Reference | Mp | Lg | Hck | Con | Frd | HE | TL | Key comments |
|---|---|---|---|---|---|---|---|---|
| Omar *et al. (*2022) | • | • | • | • | • | • | | Smart contracts find applications in various sectors, including pharmaceuticals and manufacturing. However, our analysis indicates that research on smart contracts primarily focuses on their potential within supply chains, overlooking digital resilience and the development of new business models. It is crucial to establish sector-specific smart contracts that adhere to standards, policies, and procedures. While some articles acknowledge additional costs, there is a need for better comprehension of concepts such as the right to be forgotten, the absence of legal governance over smart contracts, and the complexity of code and contract encoding. Current smart contract forms lack graphical representation and flexibility to accommodate diverse country policies. We argue that digital resilience requires addressing disputes arising from non-human-readable smart contracts that are challenging to modify. |
| Elbashbishy *et al.* (2022) | | • | | | | • | • | |
| Rozario and Thomas (2019) | • | • | • | | | | | |
| Albizri and Appelbaum (2021) | • | | | | • | • | | |
| Agrawal *et al.* (2021) | | • | | | | | • | |
| Asante *et al.* (2021) | • | • | • | | • | • | • | |
| Leduc *et al.* (2021) | | • | | | | | • | |
| Varriale *et al.* (2021) | • | | • | | | | • | |
| Wang *et al.* (2021) | | • | | | | | | |
| De Giovanni (2020) | | | | | | | • | |
| Dolgui *et al.* (2020) | • | | | | | | • | |
| Epiphaniou *et al.* (2020) | • | | • | | | | • | |
| Gourisetti *et al.* (2020) | | | | | | | • | |
| Jabbar and Dani (2020) | • | | • | | • | • | | |
| Papathanasiou *et al.* (2020) | • | | • | • | | | | |
| Yong *et al.* (2020) | • | • | • | • | • | • | | |
| Chang *et al.* (2019) | | • | | | | | | |
| Saberi *et al.* (2019) | | • | | | | | | |
| Tan *et al.* (2022) | | • | | | | | • | |
| Badi *et al.* (2021) | | • | • | • | • | • | | |
| Boubeta-Puig *et al.* (2021) | | • | | | | | • | |
| Ferreira (2021) | | • | | | | | | |
| Mehta *et al.* (2021) | • | • | • | • | • | • | | |
| Qin *et al.* (2021) | | • | | | | • | • | |
| Wasim Ahmad *et al.* (2021) | • | • | • | | • | • | • | |
| Kumar *et al.* (2020) | • | • | • | | | | • | |
| Hasan *et al.* (2019) | • | • | • | • | • | • | | |
| Hughes *et al.* (2019) | | • | | | | | • | |
| Alexander *et al.* (2020) | • | • | • | • | • | • | | |
| Kshetri (2017) | | • | | | | | | |

Manipulation (Mp); Legal (Lg); Hacking and Security Concerns (Hck); Confidentiality (Con); Fraud (Frd); Human Error (HE); Technical Limitations (TL)

The instances of the drawbacks, implied or explicit, in the corresponding articles (●)

We recognise these issues as significant challenges in new business model creation and digital resilience. Their use should reflect compelling and big scale 'real-world' business case studies rather than prototypes, small-scale applications, or understandings of smart contracts in cryptocurrency. SMEs might only consider the internalisation of smart contracts when their value proposition reflects compelling real-world case studies. In our analysis (Table 5), there are seven drawbacks impinging on adopting SCs and creating an environment where digital resilience is delayed, and there is a detriment to creating new business models.

From the seven drawbacks, we highlight three overarching key themes that impinge on digital resilience for SCs and how they relate to the seven identified drawbacks and their impact on digital resilience.

**Table 6.** Key themes of SCs impacting resiliency

| Theme | Drawbacks | Impact on Resilience |
|---|---|---|
| Theme 1: Legal issues - smart contracts' enforceability, interpretation, and jurisdiction | Hacking, Fraud, Confidentiality | Smart contracts can be hacked or subject to fraud and interpretation due to their complex code, which can undermine the digital resilience of businesses. Legal frameworks must be established to address enforceability, interpretation, and jurisdiction to ensure disputes and breaches of contracts can be resolved. |
| Theme 2: Security issues – smart contracts are not securely designed and implemented | Manipulation, Technical Limitations, Hacking, Fraud | Smart contracts will positively impact businesses' digital resilience if proper design, implementation, and testing are ensured. Poorly written or tested code or issues with the underlying blockchain platform can negatively impact the performance of a contract. The code can compromise the security and reliability of the contract. |
| Theme 3: Human error issues – users making mistakes when interacting with smart contracts | Manipulation, Hacking, Human Error, Fraud, Confidentiality | A user may input the wrong data into a smart contract, leading to incorrect calculations or transactions. Such mistakes can seriously harm businesses, including financial losses or reputational damage. Businesses need measures to detect and possibly, correct errors before or as they occur. |

Table 6 plays a significant role in bridging our understanding between the key drawbacks of SCs and digital resilience. While we have argued that the value of smart contracts to SMEs lies in automation, cost savings, efficiency gains, risk management and resilience (Katsikouli et al., 2021; Kaur et al., 2022; Prisco et al., 2022), there are also strategic concerns which need addressing. In Table 6, we identify the importance of SCs and the dearth of research within SMEs and supply chains, especially in relation to digital resilience and innovation. To this effect, our analysis represents the view that there is a need for a better understanding of concepts like the "right to be forgotten", and an increased importance for legal governance. In Table 6, we contend that achieving digital resilience necessitates addressing disputes arising from non-human-readable smart contracts that are difficult to modify.

### *4.1 Theme 1: Legal Issues*

In the first theme, the researchers find that smart contracts have the capability and technical infrastructure to replace traditional contractual agreements (Drummer and Neumann, 2020; Mehta *et al.,* 2021). While their current application is primarily for supply chains and SMEs to improve traceability, there is potential for additional applications (Kim and Laskowski, 2018; Yong *et al.,* 2020). The challenges in this context relate to legal-related issues such as enforceability, interpretation, and jurisdiction. Another challenge is smart contracts' immutability; while this is a technological advantage, it has serious implications in terms of GDPR and the right to be forgotten (Khan *et al.,* 2021). This immutability also causes issues where a contract cannot be changed or updated after an agreement has been deployed on a blockchain (Devine *et al.,* 2021). As a result, SCs are rigid and inflexible, with little room for manoeuvre if a contract error occurs.

As the legislation and governance around SCs start to mature, there will be tensions between smart contract technology and the law (Drummer & Neumann, 2020). This is an issue we identify in Table 6, where we highlight the need for standards, regulation, and legislation to deal with multiple issues ranging from a 'lack of sector-specific smart contracts' (Agrawal et al., 2021; Xu et al., 2021) to 'smart contract execution across jurisdictions and lack of governing law for interpretation and disputes' (A. Kumar et al., 2020). A lack of regulation and protocol in this area can create trust issues in the initial stages of SCs development. Thus, while a smart contract can notify of a dispute, intermediaries and legal frameworks are required to resolve the dispute (Mehta et al., 2021). In the legal context, another stakeholder significantly influences the implementation and deployment of SCs is the developer. While the SCs developer plays a crucial role in creating specific smart contracts, they may not be adept at turning human-readable contractual terms into computer-readable contract terms (Chong, 2021; Qin et al., 2021). Thus, additional human resources are generally required to ensure that the terms of human-readable contracts are translated into a language that smart contract developers can comprehend and write in smart contract programming languages (Chong, 2021; Qin et al., 2021).

Thus, in concluding this theme, we argue that multiple legal issues need to be resolved for SC implementation. Poor focus in this critical area can significantly impact digital resilience and implementation from an SME perspective. Hence, there is healthy scepticism regarding smart contracts and if they are legally binding (Drummer & Neumann, 2020), with systems yet to figure out how to deal with business agreements encoded in smart contracts (Ferreira, 2021; Hughes et al., 2019).

### *4.2 Theme 2: Security Issues*

In our second identified theme, we discuss the importance of security within SME digital

resilience. Currently, smart contracts are written by programmers, which are prone to errors and bugs, and when written on an Ethereum blockchain, for example, they are vulnerable to exploitation, errors, and out-of-gas bugs (Jabbar & Dani, 2020). One pertinent recent example is the DAO incident in which the developed smart contract contained a security exploit which allowed an attacker to drain millions of dollars' worth of funds (Cryptopedia Staff, 2022). This led to a dispute between the parties involved, and ultimately to rectify the issue, a new blockchain was created (Cryptopedia Staff, 2022).

Opportunistic human behaviour, such as exploiting gas fees (Asante et al., 2021) or tampering with data in transit, is not limited to smart contract code (Epiphaniou et al., 2020). Off-chain data access (Kumar et al., 2020; Khan et al., 2021) and timestamp dependence (Mendhurwar and Mishra, 2021) are also issues that can lead to failure points and erroneous data (Khan et al., 2021). Excessive use of smart contracts on a blockchain can also slow down a blockchain and lead to a denial of service (DoS) attack (Jabbar & Dani, 2020; Khan et al., 2021; Wang et al., 2021; Zou et al., 2021). This may occur for several reasons, but current literature suggests that this is mainly due to the infancy of the technology and the non-graphical nature of smart contracts, making it difficult for involved parties to check the quality of contracts before deployment (Boubeta-Puig et al., 2021; Dal Mas et al., 2020; Saberi et al., 2019). The real challenge is rectifying issues when they have been located, currently, to fix them, a new version of the contract must be published, resulting in a new block on the blockchain or a "hard fork" (Destefanis et al., 2018).

As smart contracts and their associated programming languages evolve, new programming vulnerabilities may emerge that current tools cannot detect and protect against (di Angelo & Salzer, 2019). Security has always been an issue as part of digital

resilience and digital transformation. In this context, we find that the main application behaviours inside a smart contract can also act as the key challenges that need rectifying for digital resilience to become a reality for SMEs and blockchain.

### *4.3 Theme 3: Human Error*

In the final theme, we discuss the critical issues around human errors. The idea of smart contracts to automate transactions and make them immutable is exciting (Liu et al., 2021; Yong et al., 2020). However, the involvement of humans in executing smart contracts introduces the possibility of errors that can have negative consequences for all parties involved. In one example, an employee of a cryptocurrency exchange allegedly mistyped the account number instead of the intended amount, leading to a transfer of AUD$10.5 million instead of the intended AUD$100 refund (Sun, 2022). This incident highlights the inherent risks of human error when utilizing smart contracts. Another example is the "Parity Wallet" incident, in which a user accidentally deleted the library contract that controlled the wallets of many users, resulting in the loss of over $150 million worth of funds (Browne, 2017; Parity Technologies, 2017). The non-graphical nature and lack of human-readability of smart contracts also add to this issue (Boubeta-Puig *et al.,* 2021; Qin *et al.,* 2021).

Papathanasiou *et al.* (2020) also suggest that the exposure of information in the code of a smart contract, whether intentional or unintentional, poses a threat to competition and the survival of involved parties if that information is meant to remain confidential. This threat can arise from losses and disruptions due to design errors (Dolgui *et al.,* 2020; Wasim Ahmad *et al.,* 2021) or the smart contract's complexity (Jabbar & Dani, 2020). Therefore, in our research, we argue that the confidentiality challenges (Badi *et al.,* 2021) extend beyond the parties involved in a traditional contract to include other parties, such as the smart contract developers. Developers can make mistakes when

coding smart contracts and are susceptible to bribery and fraud, leading to opportunistic and unethical behaviour (Albizri & Appelbaum, 2021; Wasim Ahmad et al., 2021). Unless additional safeguards are put in place, human error and malicious intent will always be an issue which needs addressing for digital resilience (Albizri & Appelbaum, 2021; Sharma et al., 2022).

## 5. Discussion

In this paper, we conducted an extensive literature review to review the drawbacks of SCs within the context of digital resilience. We find that while there is sufficient research which "eulogises" the use of blockchain and SCs across a range of industries, we find very little which takes a critical look at these technologies. We find that while SCs have emerged as a catalyst for entrepreneurial orientation and digital resilience (Florek-Paszkowska et al., 2021). We find that there are a trinity of challenges; legality, security, and human error, as identified in the key themes. Costa and Castro (2021) argue that's SCs in their current state, may impede the vibrancy of the business ecosystem for SMEs and hinder economic growth and recovery. This we argue is based on the permanent nature of SCs, once they are coded and agreed making changes later can be costly and time consuming. Another challenge we find is the key legal issues which can void any contract, as many contracts are not legally binding. Various solutions have been proposed to make SCs more flexible one of which is the amendable smart contracts, however this creates a new set of challenges, not least the potential exploitation, and the need for additional human resources to bridge the gap between human-readable contract terms and smart contract development. The very notion of amendable smart contracts raises questions regarding their fundamental purpose.

In conclusion, our research underscores the importance of recognizing the potential drawbacks of smart contracts and the need for comprehensive understanding

and proactive measures to improve digital resilience in SMEs. By addressing the risks and challenges associated with smart contracts, organizations can strengthen their digital resilience and navigate the evolving digital landscape effectively. Further research and practical initiatives are necessary to develop robust legal frameworks, governance structures, and policies that can facilitate the secure and efficient utilization of smart contracts in the context of digital resilience for SMEs.

### *5.1 Contribution*

From the three themes, the main contribution of this paper is the notion of "centralised control in decentralised solutions". While this notion may seem contradictory our research suggests that smart contracts provide freedom from centralised control, however there needs to some centralised control to overcome the negative components of SCs and create true digital resilience. Fundamentally we argue that while the network is robust, all actors cannot be fully trusted. A reflection and introspection period are critical in understanding the impact of smart contracts on digital resilience within supply chains. In addition to this we find that there is still a lack of knowledge around SCs and their usage, this we attribute to a limited resources and low skills which significantly impact SME adoption rates.

For our second contribution we argue that there is a significant lack of legal frameworks and dispute resolution mechanisms specifically designed for smart contracts. Current research in this area argues that if SCs are employed legally these can be challenged and, in some cases, SCs can be unenforceable (e.g., Ferreira, 2021; Asante et al., 2021; Omar et al., 2022). This coupled with the security issues of employing smart contracts and the strategies necessary for mitigating security issues before adopting smart contracts can create significant legal issues. However, as identified in the themes a crucial component is ensuring that strategies for reducing human error, whether through user-

friendly interfaces or providing training and support, are in place. This will reduce security issues and create a wider awareness of the key legal implications.

Finally, from a practical perspective it is clear from our research that low awareness and limited knowledge among SMEs regarding smart contracts contribute to a low adoption rate within supply chains (Asante Boakye et al., 2023; Bracci et al., 2021). The adoption of smart contracts by SMEs is influenced by their knowledge, perceived usefulness, and ease of use (Bracci et al., 2021). It is essential to build awareness among SMEs to help them comprehend the potential benefits of smart contracts in terms of efficiency, security, and cost savings (Bracci et al., 2021; Ragazou et al., 2022). By being aware of the challenges associated with smart contract implementation, SMEs can proactively take precautionary measures or develop coping strategies if safeguards are unavailable (Asadi et al., 2023; Sun et al., 2021).

## 6. Limitations and Future Recommendations

In this paper, we would like to acknowledge several limitations that were encountered during the course of our research. Firstly, the search string was formulated to locate relevant publications in the Scopus database. We considered both Scopus and Web of Science (WOS) to obtain the necessary articles, and while Scopus offers breadth in terms of coverage, the WOS provides more in-depth coverage of scholarly literature. Our research has uncovered a debate within the academic community regarding the trade-off between depth and breadth in research databases. Our decision to use Scopus was based on its availability to the authors, and we acknowledge that relevant scholarly publications may exist outside of Scopus.

Secondly, within the context of supply chain, while the keywords used in our search were derived from related publications, it is possible that relevant articles containing alternative keywords were not captured. Despite these limitations, our analysis

aims to stimulate further research into the challenges and intricacies within the supply chain industry, particularly in the realm of smart contracts.

For our final limitation, we identify the limitations of the ASReview tool in screening abstracts. It is important to note that the tool is still in the process of fine-tuning and establishing an accurate estimate of its error rate. Additionally, the tool's performance benchmarks are yet to be established for purposes other than systematic reviews. We acknowledge these limitations, but we argue that this research provides a unique and valuable insight into the potential drawbacks of smart contracts.

### *6.1 Future Areas of Research*

Looking ahead, we have identified multiple areas of research which should be considered in future work, within supply chain resilience for SMEs. In Table 7, we outline some key questions and some potential areas for future research.

**Table 7.** Research questions for future studies

| Theme | Potential research questions |
|---|---|
| Legal issues - smart contracts' enforceability, interpretation, and jurisdiction | • How can enforceability, interpretation, and jurisdiction challenges in smart contracts be addressed?<br>• What are the implications of the privacy and data protection regulations (e.g., GDPR) on the immutability of smart contracts?<br>• How can the advancement of smart contract technology be aligned with the slow-moving process of regulation and legislation?<br>• How can the legal system respond to illegal or malicious smart contracts?<br>• How can a party of a smart contract seek redress when the execution of a smart contract fails and results in a loss? |
| Security issues – smart contracts are not securely designed and implemented | • How does human behaviour contribute to the security flaws in supply chain smart contracts?<br>• How can issues in supply chain smart contracts be rectified and fixed?<br>• What is the potential impact of security flaws in smart contacts on supply chains and SMEs?<br>• How do supply chains and SMEs mitigate the adverse impact of security flaws in smart contracts on their operations? |
| Human error issues – users making mistakes when interacting with smart contracts | • How can unethical behaviour, such as fraud and bribery, be discouraged from manual data input to call a smart contract? |

| Theme | Potential research questions |
|---|---|
| | • What are the potential risks of human error in employing smart contracts, and how can human errors' adverse effect on involved parties be limited?<br>• How can the confidentiality of agreements and transparency of smart contracts be balanced?<br>• What level of effort and additional human resources is required from a supplier to implement safeguards when employing smart contracts? |

While we have identified a key contribution around smart contract enforcement, there is potential to develop research around legal governance using artificial intelligence (AI). This technology can be used to empower smart contracts and make them more "intelligent" in areas where human interpretation and discretion are required. Overall, there are significant challenges to adopting smart contracts in supply chains, in particular SMEs, and more research is needed to understand how these challenges can be addressed.

**References**


Agrawal, T. K., Angelis, J., Khilji, W. A., Kalaiarasan, R., and Wiktorsson, M. (2022). Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration. *International Journal of Production Research*, *0*(0), 1–20. https://doi.org/10.1080/00207543.2022.2039413

Agrawal, T. K., Kumar, V., Pal, R., Wang, L., and Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers and Industrial Engineering*, *154*, 107130. https://doi.org/10.1016/j.cie.2021.107130

Albizri, A., and Appelbaum, D. (2021). Trust but Verify: The Oracle Paradox of Blockchain Smart Contracts. *Journal of Information Systems*, *35*(2), 1–16. https://doi.org/10.2308/ISYS-19-024

Alexander, C., Choi, J., Massie, H. R. A., and Sohn, S. (2020). Price discovery and microstructure in ether spot and derivative markets. *International Review of Financial Analysis*, *71*, 101506. https://doi.org/10.1016/j.irfa.2020.101506

Arslan, A., Cooper, C., Khan, Z., Golgeci, I., & Ali, I. (2021). Artificial intelligence and human workers interaction at team level: A conceptual assessment of the challenges and potential HRM strategies. *International Journal of Manpower*. https://doi.org/10.1108/IJM-01-2021-0052

Asadi, M., Hashemkhani Zolfani, S., Pamucar, D., Salimi, J., & Saberi, S. (2023). The appropriation of blockchain implementation in the supply chain of SMES based on fuzzy LMAW. *Engineering Applications of Artificial Intelligence*, *123*, 106169. https://doi.org/10.1016/j.engappai.2023.106169

Asante Boakye, E., Zhao, H., Coffie, C. P. K., & Asare-Kyire, L. (2023). Seizing technological advancement; determinants of blockchain supply chain finance adoption in Ghanaian SMEs. *Technology Analysis & Strategic Management*, *0*(0), 1–17. https://doi.org/10.1080/09537325.2022.2163384

Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M., and Ghafoor, K. Z. (2021). Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey. *IEEE Transactions on Engineering Management*, 1–27. https://doi.org/10.1109/TEM.2021.3053655

Badi, S., Ochieng, E., Nasaj, M., and Papadaki, M. (2021). Technological, organisational and environmental determinants of smart contracts adoption: UK

construction sector viewpoint. *Construction Management and Economics*, *39*(1), 36–54. https://doi.org/10.1080/01446193.2020.1819549

Bavassano, G., Ferrari, C., and Tei, A. (2020). Blockchain: How shipping industry is dealing with the ultimate technological leap. *Research in Transportation Business and Management*, *34*, 100428. https://doi.org/10.1016/j.rtbm.2020.100428

Boubeta-Puig, J., Rosa-Bilbao, J., and Mendling, J. (2021). CEPchain: A graphical model-driven solution for integrating complex event processing and blockchain. *Expert Systems with Applications*, *184*, 115578. https://doi.org/10.1016/j.eswa.2021.115578

Bracci, E., Tallaki, M., Ievoli, R., & Diplotti, S. (2021). Knowledge, diffusion and interest in blockchain technology in SMEs. Journal of Knowledge Management, 26(5), 1386–1407. https://doi.org/10.1108/JKM-02-2021-0099

Braun, V., and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., and Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, *11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Braun, V., and Clarke, V. (2022). Conceptual and design thinking for thematic analysis. *Qualitative Psychology*, *9*(1), 3–26. http://dx.doi.org/10.1037/qup0000196

Braun, V., Clarke, V., Hayfield, N., and Terry, G. (2019). Thematic Analysis. In P. Liamputtong (Ed.), *Handbook of Research Methods in Health Social Sciences* (pp. 844–858). Springer.

Browne, R. (2017, November 8). *"Accidental" bug may have frozen $280 million worth of digital coin ether in a cryptocurrency wallet*. CNBC. https://www.cnbc.com/2017/11/08/accidental-bug-may-have-frozen-280-worth-of-ether-on-parity-wallet.html

Burgel, T.R., Hiebl, M.R. and Pielsticker, D.I. (2023), € "Digitalization and entrepreneurial firms' resilience to pandemic crises: evidence from COVID-19 and the German Mittelstand", Technological Forecasting and Social Change, Vol. 186, 122135.

Byrne, D. (2022). A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality and Quantity*, *56*(3), 1391–1412. https://doi.org/10.1007/s11135-021-01182-y

Chang, S. E., Chen, Y.-C., and Lu, M.-F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change*, *144*, 1–11. https://doi.org/10.1016/j.techfore.2019.03.015

Chong, F. H. L. (2021). Enhancing trust through digital Islamic finance and blockchain technology. *Qualitative Research in Financial Markets*, *13*(3), 328–341. https://doi.org/10.1108/QRFM-05-2020-0076

Christidis, K., and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Clohessy, T., & Acton, T. (2019). Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective. Industrial Management & Data Systems, 119(7), 1457–1491. https://doi.org/10.1108/IMDS-08-2018-0365

Corvello, V., Verteramo, S., Nocella, I. and Ammirato, S. (2022), "Thrive during a crisis: the role of digital technologies in fostering antifragility in small and medium-sized enterprises", Journal of Ambient Intelligence and Humanized Computing, Vol. ahead-of-print No. ahead-of-print, pp. 1-13, doi: 10.1007/s12652-022-03816-x.

Costa, J. and Castro, R. (2021), "SMEs must go online—E-commerce as an escape hatch for resilience and survivability", Journal of Theoretical and Applied Electronic Commerce Research, Vol. 16 No. 7, pp. 3043-3062.

Cryptopedia Staff. (2022, March 16). *What Was the DAO Hack?* Gemini. https://www.gemini.com/cryptopedia/the-dao-hack-makerdao, https://www.gemini.com/cryptopedia/the-dao-hack-makerdao

Dal Mas, F., Dicuonzo, G., Massaro, M., and Dell'Atti, V. (2020). Smart contracts to enable sustainable business models. A case study. *Management Decision*, *58*(8), 1601–1619. https://doi.org/10.1108/MD-09-2019-1266

De Giovanni, P. (2020). Blockchain and smart contracts in supply chain management: A game theoretic model. *International Journal of Production Economics*, *228*. https://doi.org/10.1016/j.ijpe.2020.107855

Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., and Hierons, R. (2018). Smart contracts vulnerabilities: A call for blockchain software engineering? *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 19–25. https://doi.org/10.1109/IWBOSE.2018.8327567

Dewitt, S., Jafari-Sadeghi, V., Sukumar, A., Aruvanahalli Nagaraju, R., Sadraei, R., & Li, F. (2022). Family dynamics and relationships in female entrepreneurship: An exploratory study. *Journal of Family Business Management*.

Devine, A., Jabbar, A., Kimmitt, J., and Apostolidis, C. (2021). Conceptualising a social business blockchain: The coexistence of social and economic logics. *Technological Forecasting and Social Change*, *172*, 120997. https://doi.org/10.1016/j.techfore.2021.120997

di Angelo, M., and Salzer, G. (2019). A Survey of Tools for Analyzing Ethereum Smart Contracts. *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, 69–78. https://doi.org/10.1109/DAPPCON.2019.00018

Di Vaio, A., Latif, B., Gunarathne, N., Gupta, M. and D'Adamo, I. (2023), "Digitalization and artificial knowledge for accountability in SCM: a systematic literature review", Journal of Enterprise Information Management. doi: 10.1108/JEIM-08-2022-0275.

Dolgui, A., Ivanov, D., Potryasaev, S., Sokolov, B., Ivanova, M., and Werner, F. (2020). Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *International Journal of Production Research*, *58*(7), 2184–2199. https://doi.org/10.1080/00207543.2019.1627439

Drummer, D., and Neumann, D. (2020). Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. *Journal of Information Technology*, *35*(4), 337–360. https://doi.org/10.1177/0268396220924669

Elbashbishy, T. S., Ali, G. G., and El-adaway, I. H. (2022). Blockchain technology in the construction industry: Mapping current research trends using social network analysis and clustering. *Construction Management and Economics*. http://www.tandfonline.com/doi/abs/10.1080/01446193.2022.2056216

Elhidaoui, S., Benhida, K., El Fezazi, S., Kota, S., and Lamalem, A. (2022). Critical Success Factors of Blockchain adoption in Green Supply Chain Management: Contribution through an Interpretive Structural Model. *Production and*

*Manufacturing Research*, *10*(1), 1–23. https://doi.org/10.1080/21693277.2021.1990155

Epiphaniou, G., Pillai, P., Bottarelli, M., Al-Khateeb, H., Hammoudesh, M., and Maple, C. (2020). Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security. *IEEE Transactions on Engineering Management*, *67*(4), 1059–1073. https://doi.org/10.1109/TEM.2020.2965991

Etalong, C. A., Asogwa-Chibuzo, O. C., and Etalong, T. A. (2022). Covid-19's Socio-Economic Impact On Small and Medium Enterprises and Household Income in Enugu State, Nigeria: The Political Economy Perspective. *International Journal of Public Health Pharmacy and Pharmacology*, *7*(4), 41–48. https://doi.org/10.37745/ijphpp.15/vol7n44148

European Parliament. (2021, October). *Small and medium-sized enterprises*. Fact Sheets on the European Union. https://www.europarl.europa.eu/factsheets/en/sheet/63/small-and-medium-sized-enterprises

Faasolo, M. B., & Sumarliah, E. (2022). An Artificial Neural Network Examination of the Intention to Implement Blockchain in the Supply Chains of SMEs in Tonga. Information Resources Management Journal (IRMJ), 35(1), 1–27. https://doi.org/10.4018/IRMJ.287907

Fernandez-Jardon, C., Martinez-Cobas, X., and Martinez-Ortiz, F. (2020). Technology and Culture in Subsistence Small Businesses. *Sustainability*, *12*(22), Article 22. https://doi.org/10.3390/su12229694

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, *45*(2). https://doi.org/10.1016/j.telpol.2020.102081

Florek-Paszkowska, A., Ujwary-Gil, A. and Godlewska-Dziobon, B. (2021), "Business innovation and critical success factors in the era of digital transformation and turbulent times", Journal of Entrepreneurship, Management, and Innovation, Vol. 17 No. 1, pp. 7-28.

Green, E., Sukumar, A., Jafari-Sadeghi, V., Pandya, K., & Khavarinezhad, S. (2022). Analysis of factors impeding access to finance in internet enabled crowdfunding: a systematic literature review. *International Journal of Technology Transfer and Commercialisation*, *19*(2), 249-269.

Gourisetti, S. N. G., Mylrea, M., and Patangia, H. (2020). Evaluation and Demonstration of Blockchain Applicability Framework. *IEEE Transactions on Engineering Management*, *67*(4), 1142–1156. https://doi.org/10.1109/TEM.2019.2928280

Guo, H., Yang, Z., Huang, R. and Guo, A. (2020), "The digitalization and public crisis responses of small and medium enterprises: implications from a COVID-19 survey", Frontiers of Business Research in China, Vol. 14 No. 1, pp. 1-25.

Hasan, H., AlHadhrami, E., AlDhaheri, A., Salah, K., and Jayaraman, R. (2019). Smart contract-based approach for efficient shipment management. *Computers and Industrial Engineering*, *136*, 149–159. https://doi.org/10.1016/j.cie.2019.07.022

Han, H. and Trimi, S. (2022), "Towards a data science platform for improving SME collaboration through Industry 4.0 technologies", Technological Forecasting and Social Change, Vol. 174 No. 1, 121242.

Hossain, M.R., Akhter, F. and Sultana, M.M. (2022), "SMEs in covid-19 crisis and combating strategies: a systematic literature review (SLR) and A case from emerging economy", Operations Research Perspectives, Vol. 1, 100222.

Hu, M.K. and Kee, D.M.H. (2022), "Fostering sustainability: reinventing SME strategy in the new normal", Foresight, Vol. 24 Nos 3/4, pp. 301-318.

Hughes, A., Park, A., Kietzmann, J., and Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons*, *62*(3), 273–281. https://doi.org/10.1016/j.bushor.2019.01.002

Hussain, Z., Jabbar, A., & Kong, K. (2023). Power, dominance and control: implementing a new business intelligence system. *Digital Transformation and Society*.

Ilbiz, E., & Durst, S. (2019). The Appropriation of Blockchain for Small and Medium-sized Enterprises. Journal of Innovation Management, 7(1), Article 1. https://doi.org/10.24840/2183-0606_007.001_0004

Iranmanesh, M., Maroufkhani, P., Asadi, S., Ghobakhloo, M., Dwivedi, Y. K., & Tseng, M.-L. (2023). Effects of supply chain transparency, alignment, adaptability, and agility on blockchain adoption in supply chain among SMEs. Computers & Industrial Engineering, 176, 108931. https://doi.org/10.1016/j.cie.2022.108931

Jabbar, A., and Dani, S. (2020). Investigating the link between transaction and computational costs in a blockchain environment. *International Journal of*

*Production Research*, *58*(11), 3423–3436. https://doi.org/10.1080/00207543.2020.1754487

Jerman, A., Pejić Bach, M., and Aleksić, A. (2020). Transformation towards smart factory system: Examining new job profiles and competencies. *Systems Research and Behavioral Science*, *37*(2), 388–402. https://doi.org/10.1002/sres.2657

Katsikouli, P., Wilde, A. S., Dragoni, N., & Høgh-Jensen, H. (2021). On the benefits and challenges of blockchains for managing food supply chains. Journal of the Science of Food and Agriculture, 101(6), 2175–2181. https://doi.org/10.1002/jsfa.10883

Kang, H.S., Lee, J.Y., Choi, S., Kim, H., Park, J.H., Son, J.Y., Kim, B.H. and Noh, S.D. (2016), "Smart manufacturing: past research, present findings, and future directions", International Journal of Precision Engineering and Manufacturing – Green Technology, Vol. 3 No. 1, pp. 111-128.

Kaur, J., Kumar, S., Narkhede, B. E., Dabić, M., Rathore, A. P. S., & Joshi, R. (2022). Barriers to blockchain adoption for supply chain finance: The case of Indian SMEs. Electronic Commerce Research. https://doi.org/10.1007/s10660-022-09566-4

Khalil, A., Abdelli, M.E.A. and Mogaji, E. (2022), "Do digital technologies influence the relationship between the COVID-19 crisis and SMEs' resilience in developing countries?", Journal of Open Innovation: Technology, Market, and Complexity, Vol. 8 No. 2, p. 100.

Khalil, A., Bousselmi, H. el W., El Amine Abdelli, M., Baccouche, I., Caridad y López del Río, L., and Nasr, H. E. (2022). The Impact of Digital Technologies on SMEs' Resilience During the COVID-19 Pandemic. In N. Chemma, M. El Amine Abdelli, A. Awasthi, and E. Mogaji (Eds.), *Advanced Series in Management* (pp. 111–126). Emerald Publishing Limited. https://doi.org/10.1108/S1877-636120220000029008

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., and Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, *14*(5), 2901–2925. https://doi.org/10.1007/s12083-021-01127-0

Khurana, I., Dutta, D.K. and Ghura, A.S. (2022), "SMEs and digital transformation during a crisis: the emergence of resilience as a second-order dynamic capability

in an entrepreneurial ecosystem", Journal of Business Research, Vol. 150 No. 1, pp. 623-641.

Kim, H. M., and Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management*, *25*(1), 18–27. https://doi.org/10.1002/isaf.1424

Klein, H. J., and Potosky, D. (2019). Making a conceptual contribution at Human Resource Management Review. *Human Resource Management Review*, *29*(3), 299–304. https://doi.org/10.1016/j.hrmr.2019.04.003

Kordestani, A., Oghazi, P., & Mostaghel, R. (2023). Smart contract diffusion in the pharmaceutical blockchain: The battle of counterfeit drugs. *Journal of Business Research*, *158*, 113646. https://doi.org/10.1016/j.jbusres.2023.113646

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003

Kumar, A., Liu, R., and Shan, Z. (2020). Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities. *Decision Sciences*, *51*(1), 8–37. https://doi.org/10.1111/deci.12396

Kumar, P., and Singh, R. K. (2021). Application of Industry 4.0 technologies for effective coordination in humanitarian supply chains: A strategic approach. *Annals of Operations Research*. https://doi.org/10.1007/s10479-020-03898-w

Kumar, V., Sindhwani, R., Behl, A., Kaur, A., & Pereira, V. (2023). Modelling and analysing the enablers of digital resilience for small and medium enterprises. Journal of Enterprise Information Management, ahead-of-print(ahead-of-print). https://doi.org/10.1108/JEIM-01-2023-0002

Leduc, G., Kubler, S., and Georges, J.-P. (2021). Innovative blockchain-based farming marketplace and smart contract performance evaluation. *Journal of Cleaner Production*, *306*, 127055. https://doi.org/10.1016/j.jclepro.2021.127055

Leifels, A. (2021). German SMEs lack digital skills, need more training. KfW Research.

Liu, X., Barenji, A. V., Li, Z., Montreuil, B., and Huang, G. Q. (2021). Blockchain-based smart tracking and tracing platform for drug supply chain. *Computers and Industrial Engineering*, *161*, 107669. https://doi.org/10.1016/j.cie.2021.107669

Manupati, V. K., Schoenherr, T., Ramkumar, M., Wagner, S. M., Pabba, S. K., and Inder Raj Singh, R. (2020). A blockchain-based approach for a multi-echelon

sustainable supply chain. *International Journal of Production Research*, *58*(7), 2222–2241. https://doi.org/10.1080/00207543.2019.1683248

Masood, T., and Sonntag, P. (2020). Industry 4.0: Adoption challenges and benefits for SMEs. *Computers in Industry*, *121*, 103261. https://doi.org/10.1016/j.compind.2020.103261

Mehta, D., Tanwar, S., Bodkhe, U., Shukla, A., and Kumar, N. (2021). Blockchain-based royalty contract transactions scheme for Industry 4.0 supply-chain management. *Information Processing and Management*, *58*(4), 102586. https://doi.org/10.1016/j.ipm.2021.102586

Mendhurwar, S., and Mishra, R. (2021). 'Un'-blocking the industry 4.0 value chain with cyber-physical social thinking. *Enterprise Information Systems*, 1–48. https://doi.org/10.1080/17517575.2021.1930189

Modgil, S., Singh, R. K., & Agrawal, S. (2023). Developing human capabilities for supply chains: An industry 5.0 perspective. *Annals of Operations Research*. https://doi.org/10.1007/s10479-023-05245-1

Moeuf, A., Lamouri, S., Pellerin, R., Tamayo-Giraldo, S., Tobon-Valencia, E., and Eburdy, R. (2020). Identification of critical success factors, risks and opportunities of Industry 4.0 in SMEs. *International Journal of Production Research*, *58*(5), 1384–1400. https://doi.org/10.1080/00207543.2019.1636323

Müller, J. M., Buliga, O., and Voigt, K.-I. (2018). Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0. *Technological Forecasting and Social Change*, *132*, 2–17. https://doi.org/10.1016/j.techfore.2017.12.019

Müller, J. M., Kiel, D., and Voigt, K.-I. (2018). What Drives the Implementation of Industry 4.0? The Role of Opportunities and Challenges in the Context of Sustainability. *Sustainability*, *10*(1), Article 1. https://doi.org/10.3390/su10010247

Nan, W. and Park, M. (2022), "Improving the resilience of SMEs in times of crisis: the impact of mobile money amid Covid-19 in Zambia", Journal of International Development, Vol. 34 No. 4, pp. 697-714.

North, K., Aramburu, N. and Lorenzo, O.J. (2020), "Promoting digitally enabled growth in SMEs: a framework proposal", Journal of Enterprise Information Management, Vol. 33 No. 1, pp. 238-262.

Omar, I. A., Hasan, H. R., Jayaraman, R., Salah, K., and Omar, M. (2021). Implementing decentralized auctions using blockchain smart

contracts. *Technological Forecasting and Social Change*, *168*, 120786. https://doi.org/10.1016/j.techfore.2021.120786

Papathanasiou, A., Cole, R., and Murray, P. (2020). The (non-)application of blockchain technology in the Greek shipping industry. *European Management Journal*, *38*(6), 927–938. https://doi.org/10.1016/j.emj.2020.04.007

Parity Technologies. (2017, November 15). *A Postmortem on the Parity Multi-Sig Library Self-Destruct | Parity Technologies*. Parity. https://www.parity.io/blog/a-postmortem-on-the-parity-multi-sig-library-self-destruct/

Petersson, D. (2018, October 24). *How Smart Contracts Started And Where They Are Heading*. Forbes. https://www.forbes.com/sites/davidpetersson/2018/10/24/how-smart-contracts-started-and-where-they-are-heading/

Pozzi, R., Rossi, T., & Secchi, R. (2023). Industry 4.0 technologies: Critical success factors for implementation and improvements in manufacturing companies. *Production Planning & Control*, *34*(2), 139–158. https://doi.org/10.1080/09537287.2021.1891481

Prisco, A., Abdallah, Y. O., Morande, S., & Gheith, M. H. (2022). Factors affecting blockchain adoption in Italian companies: The moderating role of firm size. Technology Analysis & Strategic Management, 0(0), 1–14. https://doi.org/10.1080/09537325.2022.2155511

Purkayastha, A., & Kumar, V. (2021). Internationalization through foreign listing: A review and future research agenda. Journal of World Business, 56(3), 101189. https://doi.org/10.1016/j.jwb.2021.101189

Qin, P., Tan, W., Guo, J., and Shen, B. (2021). Intelligible Description Language Contract (IDLC) – A Novel Smart Contract Model. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-021-10138-4

Ragazou, K., Passas, I., & Sklavos, G. (2022). Investigating the Strategic Role of Digital Transformation Path of SMEs in the Era of COVID-19: A Bibliometric Analysis Using R. Sustainability, 14(18), 11295. https://doi.org/10.3390/su141811295

Rashideh, W. (2020). Blockchain technology framework: Current and future perspectives for the tourism industry. *Tourism Management*, *80*, 104125. https://doi.org/10.1016/j.tourman.2020.104125

Robertson, J., Botha, E., Walker, B., Wordsworth, R., and Balzarova, M. (2022). Fortune favours the digitally mature: The impact of digital maturity on the

organisational resilience of SME retailers during COVID-19. *International Journal of Retail and Distribution Management*, *50*(8/9), 1182–1204. https://doi.org/10.1108/IJRDM-10-2021-0514

Rozario, A. M., and Thomas, C. (2019). Reengineering the Audit with Blockchain and Smart Contracts. *Journal of Emerging Technologies in Accounting*, *16*(1), 21–35. https://doi.org/10.2308/jeta-52432

Saberi, S., Kouhizadeh, M., Sarkis, J., and Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Sahoo, S., Mukherjee, A., and Halder, R. (2021). A unified blockchain-based platform for global e-waste management. *International Journal of Web Information Systems*, *17*(5), 449–479. https://doi.org/10.1108/IJWIS-03-2021-0024

Santos, S.C., Liguori, E.W. and Garvey, E. (2023), "How digitalization reinvented entrepreneurial resilience during COVID-19", Technological Forecasting and Social Change, Vol. 189, pp. 122398- 122412, doi: 10.1016/j.techfore.2023.122398.

Satyanarayana, K., Chandrashekar, D., Sukumar, A., & Jafari-Sadeghi, V. (2022). How does international entrepreneurial orientation influence firms' internationalization? An exploration with Indian software product top management teams. *International Journal of Entrepreneurial Behavior & Research*, (ahead-of-print).

Sharma, P., Jindal, R., and Borah, M. D. (2022). A review of smart contract-based platforms, applications, and challenges. *Cluster Computing*. https://doi.org/10.1007/s10586-021-03491-1

Singh, R., Chandrashekar, D., Hillemane, B. S. M., Sukumar, A., & Jafari-Sadeghi, V. (2022). Network cooperation and economic performance of SMEs: Direct and mediating impacts of innovation and internationalisation. *Journal of Business Research*, *148*, 116-130.

Ślusarczyk, B. (2018). INDUSTRY 4.0-ARE WE READY? *Polish Journal of Management Studies*, *17*. https://doi.org/10.17512/pjms.2018.17.1.19

Soundararajan, V., Jamali, D., & Spence, L. J. (2018). Small Business Social Responsibility: A Critical Multilevel Review, Synthesis and Research Agenda.

International Journal of Management Reviews, 20(4), 934–956. https://doi.org/10.1111/ijmr.12171

Sukumar, A., Jafari-Sadeghi, V., Xu, Z., & Tomlins, R. (2022). Young students and desire to social entrepreneurship: the impact of government's role. *International Journal of Entrepreneurship and Small Business*, *46*(4), 526-554.

Sun, Z. (2022, August 30). *Crypto.com accidentally transferred $10.5M to client instead of $100 refund*. Cointelegraph. https://cointelegraph.com/news/crypto-com-accidentally-transfered-10-5m-to-client-instead-of-100-refund

Sunny, J., Undralla, N., and Madhusudanan Pillai, V. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Computers and Industrial Engineering*, *150*. https://doi.org/10.1016/j.cie.2020.106895

Sun, W., Dedahanov, A. T., Shin, H. Y., & Li, W. P. (2021). Using extended complexity theory to test SMEs' adoption of Blockchain-based loan system. PLOS ONE, 16(2), e0245964. https://doi.org/10.1371/journal.pone.0245964

Tan, A., Gligor, D., and Ngah, A. (2022). Applying Blockchain for Halal food traceability. *International Journal of Logistics Research and Applications*, *25*(6), 947–964. https://doi.org/10.1080/13675567.2020.1825653

Terry, G., and Hayfield, N. (2020). 38. Reflexive thematic analysis. In M. R. M. Ward and S. Delamont (Eds.), *Handbook of Qualitative Research in Education* (pp. 430–441). Edward Elgar Publishing Limited. http://ebookcentral.proquest.com/lib/hud/detail.action?docID=6317815

Thompson, B. S., & Rust, S. (2023). Blocking blockchain: Examining the social, cultural, and institutional factors causing innovation resistance to digital technology in seafood supply chains. Technology in Society, 73, 102235. https://doi.org/10.1016/j.techsoc.2023.102235

Tranfield, D., Denyer, D., and Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, *14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

UK Jurisdiction Taskforce. (2019). *Legal statement on cryptoassets and smart contracts*. The LawTech Delivery Panel. https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-

content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf

van de Schoot, R., de Bruin, J., Schram, R., Zahedi, P., de Boer, J., Weijdema, F., Kramer, B., Huijts, M., Hoogerwerf, M., Ferdinands, G., Harkema, A., Willemsen, J., Ma, Y., Fang, Q., Hindriks, S., Tummers, L., and Oberski, D. L. (2021). An open source machine learning framework for efficient and transparent systematic reviews. *Nature Machine Intelligence*, *3*(2), Article 2. https://doi.org/10.1038/s42256-020-00287-7

Varriale, V., Cammarano, A., Michelino, F., and Caputo, M. (2021). New organizational changes with blockchain: A focus on the supply chain. *Journal of Organizational Change Management*, *34*(2), 420–438. https://doi.org/10.1108/JOCM-08-2020-0249

Vrchota, J., Řehoř, P., Maříková, M., and Pech, M. (2021). Critical Success Factors of the Project Management in Relation to Industry 4.0 for Sustainability of Projects. *Sustainability*, *13*(1), Article 1. https://doi.org/10.3390/su13010281

Wang, Y., Chen, C. H., and Zghari-Sales, A. (2021). Designing a blockchain enabled supply chain. *International Journal of Production Research*, *59*(5), 1450–1475. https://doi.org/10.1080/00207543.2020.1824086

Wang, X., & Xu, F. (2022). The Value of Smart Contract in Trade Finance. Manufacturing & Service Operations Management. https://doi.org/10.1287/msom.2022.1126

Wasim Ahmad, R., Hasan, H., Yaqoob, I., Salah, K., Jayaraman, R., and Omar, M. (2021). Blockchain for aerospace and defense: Opportunities and open research challenges. *Computers and Industrial Engineering*, *151*. https://doi.org/10.1016/j.cie.2020.106982

Westerlund, M. (2020), "Digitalization, internationalization and scaling of online SMEs", Technology Innovation Management Review, Vol. 10 No. 4, pp. 48-57.

Wong, L.-W., Tan, G. W.-H., Lee, V.-H., Ooi, K.-B., & Sohal, A. (2020). Unearthing the determinants of Blockchain adoption in supply chain management. International Journal of Production Research, 58(7), 2100–2123. https://doi.org/10.1080/00207543.2020.1730463

Wright, D. J. (2016). Toward a digital resilience. *Elementa: Science of the Anthropocene*, *4*, 000082. https://doi.org/10.12952/journal.elementa.000082

Xu, Z., Sukumar, A., Jafari-Sadeghi, V., Li, F., & Tomlins, R. (2021). Local-global design: entrepreneurial ecosystem approach for digital gaming industry. *International Journal of Technology Transfer and Commercialisation*, *18*(4), 418-438.

Yong, B., Shen, J., Liu, X., Li, F., Chen, H., and Zhou, Q. (2020). An intelligent blockchain-based system for safe vaccine supply and supervision. *International Journal of Information Management*, *52*. https://doi.org/10.1016/j.ijinfomgt.2019.10.009

Yu, F., and Schweisfurth, T. (2020). Industry 4.0 technology implementation in SMEs – A survey in the Danish-German border region. *International Journal of Innovation Studies*, *4*(3), 76–84. https://doi.org/10.1016/j.ijis.2020.05.001

Zirar, A., Ali, S. I., & Islam, N. (2023). Worker and workplace Artificial Intelligence (AI) coexistence: Emerging themes and research agenda. Technovation, 124, 102747. https://doi.org/10.1016/j.technovation.2023.102747

Zou, W., Lo, D., Kochhar, P. S., Le, X.-B. D., Xia, X., Feng, Y., Chen, Z., and Xu, B. (2021). Smart Contract Development: Challenges and Opportunities. *IEEE Transactions on Software Engineering*, *47*(10), 2084–2106. https://doi.org/10.1109/TSE.2019.2942301