Addressing challenges of digital transformation with modified blockchain

Gajendra Liyanaarachchi, Giampaolo Viglia, Fidan Kurtaliqi

Addressing challenges of digital transformation with modified blockchain

Gajendra Liyanaarachchi[a], Giampaolo Viglia[a,b,1], and Fidan Kurtaliqi[c]

[a] *Department of Strategy, Marketing and Innovation, University of Portsmouth, Portsmouth, UK*
[b] *Department of Economics and Political Science, University of Aosta, Aosta, Italy*
[c] *Department of Marketing, Audencia Business School, Nantes, France*

1 giampaolo.viglia@port.ac.uk, corresponding author
Richmond Building, PO13HL, Portsmouth (UK)

Abstract : This conceptual paper challenges the notion that the enhanced data security of blockchain results in superior privacy. Blockchain's fundamental characteristics - immutability, decentralization, and transparency - promote an excessive reliance on historical data. This reliance, in turn, leads to inaccurate predictions and misguides consumer privacy preferences. The paper contends that this stern protection conflicts with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). We argue that the lack of choice in managing data denies freedom, causing psychological reactance. Additionally, the dependence on past data contributes to an intensified privacy paradox as consumers need to assert accurate privacy preferences. These combined effects result in increased consumer digital vulnerability, which arises from an imbalanced power dynamic in data management. We propose a novel approach, which we call "modified blockchain". The approach is based on three pillars: i) selective immutability, ii) federal decentralization, and iii) supervised transparency. These pillars aim to effectively integrate regulations, organizations, and end-users within advocating for a socio-technical decision-making approach. This work also broadens the scope of the psychological reactance theory and the privacy paradox literature by affirming that a lack of autonomy in data management leads to digital vulnerability.

Keywords: blockchain; digital vulnerability; selective immutability; federal decentralization; supervised transparency; privacy paradox; psychological reactance

1. Introduction

Digital transformation is pivotal for firm growth and performance (Alalwan et al., 2021; Baiyere et al., 2020; Cao et al., 2022; Kraus et al., 2022). Companies must adapt to digital transformation and build dynamic consumer relationships to create a competitive advantage (Palacios-Marqués et al., 2021). Among the strategic challenges related to growth and performance is efficient data transactions. The business landscape is becoming more complex due to digital-enabled online personal data misuse issues (see Saura et al., 2023). Many businesses try to reassure consumers that online data will be treated confidentially or that consumers have complete control of their data (Saura et al., 2022). Blockchain is an open, decentralized, distributed digital ledger technology that records transactions across multiple systems, ensuring transparency, security, and immutability (Cozzio et al., 2023).

Blockchain will represent ten percent of the worldwide GDP by 2027 (World Economic Forum, 2015). Initially considered for cryptocurrencies like Bitcoin and Ethereum, blockchain has extended into diverse industries, including health, supply, digital voting, and national security (Mitzner, 2022). Major corporations such as Amazon, Walmart, IKEA, Nestle, and Alibaba have partnered with IBM and Microsoft to integrate blockchain technology into their operations. Blockchain has transformed e-commerce by ensuring data security and offering an immutable and transparent system that prevents data manipulation (Peres et al., 2022; Chan et al., 2023). Furthermore, blockchain assures privacy for consumers through enhanced transparency and visible transaction history (Joo et al., 2022).

The adoption of Central Bank Digital Currencies by over 100 countries underscores the increasing interest in blockchain technology (Stanley, 2023). In 2023, the United States alone boasts approximately 45 million crypto users, with 16% of Americans engaging in cryptocurrency activities (Ariella, 2023). The global user base for blockchain wallets has

reached 85 million (Howarth, 2023). However, blockchain's immutability poses challenges to regulatory compliance, particularly concerning the "right to forget" principle in GDPR and the "right to request deletion" of the CCPA (Alza, 2020). Once data is recorded on a blockchain, adhering to regulations mandating data erasure becomes exceedingly complex. Also, to ensure effective user privacy, systems should delete data within a 30-days, substantiated by verifiable evidence (Ribeiro-Navarrete et al., 2021).

Despite the blockchain design for transparent information transmission, consumers generally perceive blockchain-provided information as less credible (Mazzù et al., 2023). The authors emphasize a more inclusive relationship-based approach, providing social proof, such as positive customer reviews, to establish credibility. Understanding these dynamics can help companies improve consumer trust in blockchain technology and facilitate effective adoption. Therefore, while blockchain establishes credibility in preserving past privacy, it needs more flexibility in addressing future privacy concerns. As a result, organizations will underestimate privacy perpetuated through past incidents (Marthews & Tucker, 2022). However, contrary to the acclaimed blockchain security, issues regarding credibility and cyber-attacks persist. Schlatt et al. (2023), in their analysis of 87 attacks on blockchain-based systems, underscore the imperative of establishing a stringent multi-stakeholder approach to managing consumer data. Organizations should consider integrating regulators, organizations, developers, and end-users within broader ecosystems, mandating a socio-technical decision-making approach.

Consumers adapt their privacy intentions based on circumstances, exhibiting dynamic rather than static privacy behavior (Liyanaarachchi, 2021). We argue that due to the inherent data security of blockchain technology, companies have disregarded the psychological aspects of data privacy from the consumer perspective. In the retail sector, blockchain raises concerns surrounding data ownership and the potential for misuse, emphasizing the need for effective data visibility control (Dwivedi et al., 2023). Existing literature has predominantly

focused on the technical aspects of blockchain, overlooking the dynamic nature of privacy behavior (Liyanaarachchi et al., 2019 ; Schlatt et al., 2023). The research on blockchain technology remains relatively new and rapidly evolving (Chan et al., 2023; Tan & Saraniemi, 2023). Despite its increasing popularity and adoption in various industries, the scholarly exploration of blockchain's multifaceted aspects is still in the infancy (Frizzo-Barker et al., 2020; Javaid et al., 2021; Liu et al., 2023; Xu et al., 2019; Wang et al., 2021).

As a digital transformation, blockchain profoundly affects global businesses while presenting critical social challenges (Ante, 2021; Baquero, 2023; Li et al., 2023; Raddatz et al., 2023) and resistance due to lack of consumer autonomy (Li et al., 2023; Mashatan et al., 2022). As a result, Baquero (2023) introduces three strategies to enhance blockchain adaptation in social and regulatory contexts: i) redesigning blockchain for human oversight of privacy, ii) prioritizing effective privacy design, and iii) establishing clear responsibilities for data. Further, these strategies underscore the need for greater academic scrutiny (Baquero, 2023).

This study addresses a notable research gap in the literature, emphasizing the necessity to investigate the neglect of social perspectives on blockchain privacy. This emphasis stems from the prevailing focus on technical facets of blockchain security in existing research, as highlighted by scholars (Mazzù et al., 2023 ; Patil et al., 2023; Schlatt et al., 2023). Existing literature highlights the stern privacy approach of blockchain applications and the resulting lack of consumer trust in managing their data (Liang & Ji, 2022; Utz et al., 2023). Consequently, consumers perceive product information from blockchain as less credible than information from human experts (Walsh et al., 2021). While prior research has explored strategies for reducing consumer resistance to technological transformations, a gap persists in understanding the specific reasons for this resistance (Alam et al., 2021; Mazzù et al., 2023). A customer-centric strategic approach is necessary to advance blockchain's

practical implementation and customer adoption (Patil et al., 2023; Zheng & Lu, 2022). To address this gap, the paper draws on psychological reactance theory and privacy paradox, with the failure of blockchain to comply with global data privacy regulations. The study identifies three key factors—psychological reactance, privacy paradox, and non-compliance with data privacy regulations—that contribute to increased consumer digital vulnerability. We argue that blockchain's core characteristics, such as immutability, decentralization, and transparency, exacerbate these issues by promoting reliance on historical data, resulting in inaccurate predictions and misguided privacy preferences.

The paper proposes a novel approach, the "modified blockchain," incorporating three pillars: selective immutability, federal decentralization, and supervised transparency. These pillars aim to balance the power dynamic in data management by integrating regulations, organizations, and end-users, advocating for a socio-technical decision-making approach. The research highlights the importance of addressing the mismatch between organizational blockchain use and consumer expectations (Ehrenberg & King, 2020 ; Mazzù et al., 2023 ; Schlatt et al., 2023 ; Tan, & Saraniemi, 2023; Tan & Salo, 2023). The proposed modified blockchain model offers actionable managerial insights to mitigate digital vulnerability and foster a more balanced approach to data management.

2. Conceptual underpinnings

2.1 Regulation

Privacy laws and blockchain technology have continuously evolved, driven by technological advancements and an increasing recognition of privacy rights (Gurzhii et al., 2022). Nevertheless, concerns have arisen regarding the potential implications for privacy rights, particularly on compliance with GDPR and CCPA (Alza, 2020). CCPA represents the most

rigorous data privacy and digital consumer rights legislation in the United States. Drawing inspiration from the GDPR, often called the "California GDPR," the CCPA signifies a transformative shift in American digital regulation (Hennel, 2021). Further, several US states, including Colorado, Connecticut, Utah, and Virginia, introduced similar data privacy laws in 2023, expecting more states to follow suit (Riela, 2023).

Although initially focused on California residents, the impact of the CCPA extends beyond state borders, affecting businesses and personal data nationwide. Technology giants like Facebook, Microsoft, Samsung, Apple, and Amazon must adhere to CCPA compliance requirements (Hennel, 2021). GDPR provides more comprehensive and robust guidelines directly applicable to blockchain than the CCPA (Alza, 2020). Therefore, this paper primarily focuses on GDPR as the regulatory framework to examine the impact of blockchain technology due to its more comprehensive global presence. Blockchain technology, known for its data protection assurance, presents a significant challenge when considering GDPR guidelines (Haque et al., 2021).

The GDPR Articles 17, 25, and 4 are particularly affected by blockchain applications, necessitating innovative approaches to ensure regulatory compliance (Tatar et al., 2020). Article 17 of the GDPR, known as the “right to be forgotten,” mandates that organizations erase personal data once its original purpose has been fulfilled (Finck, 2018). However, this contradicts a fundamental aspect of blockchain technology, which relies on permanence and immutability. Data stored on a blockchain ledger cannot be deleted as such action will compromise the entire system's integrity. Blockchain's immutability, while ensuring data integrity, directly contradicts Article 17 of the GDPR. This right allows individuals to request the deletion of their data, emphasizing individual data control.

The permanence of blockchain data makes it impossible as data removal disrupts its continuity, undermining one of its core principles, immutability. The foundation of Article 17 originates from the EU Data Protection Directive, influenced by the “Google Spain” case. Mr. Costeja González sought to remove outdated data from the Google search engine that included his past financial situation. He argued that when users searched his name on Google, the results included links to a 1998 newspaper article that represented a closed matter. In May 2014, the European Court of Justice (ECJ) ruled in favor of Mr. González on the freedom of information and expression (Frantziou, 2014).

Article 25 of the GDPR requires data processing systems to incorporate "privacy by design" and “privacy by default” during design and development (Tatar et al., 2020). Unfortunately, blockchain's inherent characteristics, such as transparency, pose significant challenges to complying with this GDPR requirement. Blockchain's transparent and tamper-proof data storage contradicts, emphasizing confidentiality and availability (Liu et al., 2023). Further, GDPR introduces the “data controller” role in Article 4 to designate entities responsible for personal data processing (Tatar et al., 2020). However, the decentralized nature of blockchain technology challenges this conventional concept. Unlike the GDPR's assumption of centralized data management, blockchain operates on a distributed ledger system without a central authority. The blockchain does not include the option of a central data controller with specific responsibility for data protection.

This paper mainly focuses on Articles 4, 17, and 25 due to the direct impact on consumers and their sensitive information. Blockchain's focus on past data needs to account for consumers' evolving privacy concerns and their need to change and adapt their data usage preferences. The concept of a single customer view, which allows tracking across various online platforms, must be more accurate to simplify complex customer privacy needs (Tucker & Catalini, 2018). Identifying consumers based on past data creates a misleading privacy

situation, as it does not reflect the dynamic nature of consumer online behavior. We consider the lack of adherence to privacy regulation as a critical setback in recognizing blockchain as a digital transformation. A more collaborative approach is required to balance the regulator's concern for consumer privacy to validate the blockchain technology (Su et al., 2023).

2.2 Psychological reactance

Psychological reactance theory depicts how individuals respond to perceived threats invading their autonomy and freedom of choice (Brehm, 1966). When faced with a threat to freedom, people encounter a state of reactance, compelling them to resist reclaiming freedom actively. Also, they can respond with anger and counteraction, leading to psychological reactance to restore freedom (Badewi et al., 2023). This paper argues that a lack of freedom in managing data with blockchain can evoke psychological reactance. Customers might opt to withhold or limit their engagement with blockchain-based platforms due to concerns about needing more data control.

In 2022, the blockchain-based cryptocurrency has witnessed a series of significant security breaches, with the five most extensive violations amounting to over $3 billion (Bambysheva & Linares, 2022). Also, the additional risks, such as ransomware associated with indefinite data availability, illustrate reactance to blockchain technology (Martin et al., 2022). By 2031, ransomware is expected to impose a staggering annual cost of approximately $265 billion (USD), with a new incident every two seconds (Morgan, 2023). Despite the potential for blockchain congestion, severe vulnerabilities have brief lifespans, prompting opportunistic large-scale ransomware attacks (Lee & Choi, 2022).

These threats encompass various forms, such as data breaches, security vulnerabilities, hacking incidents, and financial fraud. Data threats are a predominant concern within information systems, with data integrity being crucial (Dwivedi et al., 2023). Despite

perceiving blockchain as a secure technology, scholars have yet to determine the ecosystem's operational reliability, citing the potential for data misuse (Chan et al., 2023; Schlatt et al., 2023). Companies fear the loss of customer trust that could arise from data misuse facilitated by blockchain vulnerabilities (Li et al., 2023). As a result, companies may resist adopting blockchain technology, opting for more familiar and controllable alternatives. In a study involving 360 retailers, Dwivedi et al. (2023) unveiled resistance toward blockchain adoption due to a need for more data ownership.

Data immutability within blockchain may conflict with consumer aspirations for heightened control over their personal information. Future research should focus on consumer attitudes toward autonomy and personal freedom in the context of blockchain technology (Ford et al., 2023; Martin et al., 2022; Perdana et al., 2021). There can be reactance when consumers perceive an unequal power dynamic concerning the rigid privacy measures of the blockchain. This paper advocates that companies should adjust the blockchain applications to empower consumers to minimize reactance. A dynamic balance is needed to reconcile blockchain's technological strengths with the psychological reactance from limited data control (Friedman & Ormiston, 2022). Exploring user-friendly implementations of blockchain that enable individuals to manage data to some extent within its framework while preserving its core benefits might be a viable direction (Wong et al., 2023). There is a need to design mechanisms that allow individuals the freedom to manage data in the blockchain while maintaining the technology's core advantages.

2.3 Privacy paradox

The privacy paradox depicts the dichotomy between an individual's attitude and the behavior of disclosing personal information (Cloarec et al., 2022; Norberg et al., 2007). Consumers need to be more consistent with protecting their privacy and continue to disclose information

despite the risk creating inconsistent online behavior (Liyanaarachchi, 2021). The privacy paradox arises when individuals' normative privacy attitudes contradict actual behavior due to specific privacy situations (Acquisti et al., 2023; Kokolakis, 2017). Blockchain technology can intensify this paradox due to retaining data, leading to conflict with future privacy behaviors.

This discrepancy profoundly impacts blockchain as consumers' past privacy preferences are visible to the public, which may not reflect current privacy concerns, leading to a heightened privacy paradox with blockchain. Consider a consumer cautious about investing in the stock market six months ago, creating a specific consumer profile shared with financial institutions and brokering firms. However, this consumer may be more willing to take risks due to changing financial conditions and evolving business developments. Unfortunately, stockbrokers and other institutions might not recognize these risk appetite changes, causing the consumer to miss potential market opportunities.

Similarly, an individual who has recently recovered from a health condition may encounter constraints imposed by previously recorded preferences prohibiting certain activities, such as travel. These static privacy profiles hinder future actions and aspirations, intensifying the privacy paradox within the blockchain system and creating uncertainty about sharing information. Moreover, with blockchain, organizations struggle to interact with consumers based on outdated and contradictory past privacy preferences, leading to a privacy paradox (Bonsón & Bednárová, 2019). Their decision-making processes predominantly rely on historical data, which fails to align with their customers' dynamic and evolving privacy needs and preferences. Also, blockchain applications with immersive technology and metaverse lead to more profound privacy situations (Dwivedi et al., 2023). With blockchains, anyone can access the entire history of transactions on a given chain, a measure taken to ensure the security and integrity of the network.

However, this transparency with immersive technology creates a higher privacy risk and a dilemma for customers to engage with blockchain (Kaaniche et al., 2020). Transparency enhances trust and accountability in various applications and exposes transaction details to anyone, potentially compromising user anonymity (Wang et al., 2023). The increase in financial fraud and cybercrime, especially in the context of financial risk, is evidence of such visibility (Liyanaarachchi et al., 2019). The privacy paradox becomes evident as the value of consumer data continues to escalate over time, which necessitates robust privacy protection (Acquisti et al., 2023). This paradox persists due to the enduring online data availability long after its initial use, a formidable challenge for organizations Fusing blockchain (Bonsón & Bednárová, 2019).

The existing privacy paradox particularly emphasizes the disclosure of confidential data. In typical situations, unauthorized actions or data misuse can lead to consequences. In specific conditions, data misuse can result from unauthorized actions or hacking of systems. Blockchain technology exacerbates this situation due to a critical difference – the data is entirely visible to the public. This heightened transparency means hackers can trace an individual, effectively connecting past disclosures to the present (Corbet et al., 2020). The concept of a single customer view, facilitating the tracking of a customer across various online platforms, poses limitations when comprehending intricate customer requirements (Tucker & Catalini, 2018).

Blockchain systems focus on pseudonymity, where users operate under pseudo-identity to safeguard their identity (Zhang et al., 2022). Assigning unique codes to each transaction enhances data protection. The challenge arises when a skilled hacker can discern the data source and trace it back to the original provider (Corbet et al., 2020). This capability introduces a significantly higher privacy risk and amplifies the complex privacy paradox. We argue that the privacy paradox, amplified by blockchain technology, underscores the

disconnect between consumers' past and present privacy concerns. The past data in the blockchain hinders consumers and organizations from making informed decisions, manifesting the need to address this paradox (Bonsón & Bednárová, 2019; Wang et al., 2021).

2.4 Digital vulnerability

The rising value stored in blockchain systems has led to higher digital vulnerability, making individuals increasingly attractive targets for cybercrime (Schlatt et al., 2023). Consumer vulnerability originates from power imbalances in organizational interactions (Baker et al., 2005). As a result, they are overly dependent on organizations for knowledge and information (Echeverri & Salomonson, 2019). Concerns about unauthorized access and exploitation of personal information drive data vulnerability (Martin et al., 2017). Consumers possess restricted options for data privacy (Acquisti et al., 2023) and lack awareness regarding their vulnerability (Liyanaarachchi et al., 2021). Further, consumers alone cannot identify and manage vulnerability (Berg, 2015). Despite the importance of mitigating consumer vulnerability, there is a scarcity of research focused on identifying strategies to empower consumers (Basu et al., 2023; Galli, 2022; Miglionico, 2023).

Through a review of the literature spanning over 25 years, Basu et al. (2023) identify four major research themes: i) fraud, ii) well-being, iii) ethics, and iv) the impact of disability and gender on managing future consumer vulnerability. Unlike businesses, consumers lack experience handling digital transactions, creating the need to manage vulnerability to prevent imbalanced relationships. Therefore, to address digital vulnerability, consumers should possess higher capability and ability to implement correct choices in information disclosure (Glavas et al., 2020). Prioritizing user-friendly applications in organizations is crucial for managing digital vulnerability and providing autonomy to customers (Liyanaarachchi et al.,

2021). The growth of digital payments and consumer neglect of self-regulatory privacy behavior creates more opportunities for data breaches with blockchain (Miglionico, 2023).

The research gap on consumer vulnerability intensifies as companies rely excessively on aggressive marketing strategies, neglecting societal concerns (Stewart, 2022). Developments in cyber threats underscore the need to design secure applications addressing data vulnerability with blockchain (Prakash et al., 2022; Walsh et al., 2021). Variations across multiple blockchain application domains make it challenging to organize a uniform path toward developing strategies to prevent data vulnerability (Perdana et al., 2021). As more industries adopt blockchain solutions (Friedman & Ormiston, 2022), the complexity of blockchain networks increases, expanding the scope for unauthorized access to data (Prakash et al., 2022). One grave threat is the "51% attack", in which an entity or group gains control of over 50% of the network's computing power (Schlatt et al., 2023). Such authority enables the attacker to change the details of any transaction stored in the blockchain, rendering the entire system vulnerable.

The organization's complete control over data causes consumers to be vulnerable due to an imbalanced exchange relationship with blockchain, exposing them to digital fraud (Tan & Saraniemi, 2023). Therefore, leveraging blockchain technology with potential legal reforms and better consumer adaptability is crucial in mitigating digital vulnerabilities (Miglionico, 2023).

3. The conceptual model

3.1 The Blockchain

The core features of blockchain on data security are immutability, transparency, and decentralization (Rawat et al., 2020; Shafay et al., 2023; Tatar et al., 2020; Yli-Huumo et al., 2016). We contend that these three key features result in an overemphasis on operational

efficiency while neglecting the customer perspective. Furthermore, these three core aspects of blockchain technology conflict with GDPR, giving rise to customer reactance and the emergence of a privacy paradox, which is detrimental to the growth of blockchain as a digital transformation.

3.1.1 Immutability

Immutability refers to the inherent property of blockchain data, once recorded, becoming exceedingly resistant to alteration or deletion (Li et al., 2023). The immutable nature of data on the blockchain conflicts with GDPR Article 17 compliance concerns data erasure after use (Haque et al., 2021). The perception of data permanence on the blockchain can elicit psychological reactions among consumers due to the lack of freedom to manage data. Immutability can result in a privacy paradox due to potential data misuse with the visibility of sensitive information to third parties. Both reactance and privacy paradox aggravate as the data remains with blockchain beyond its intended use. We argue that companies must devise strategies to mitigate psychological reactance and privacy paradox by adhering to GDPR Article 17.

3.1.2 Decentralization

Decentralization in blockchain refers to distributing data and control across a network of computers (nodes) rather than relying on a central authority (Onjewu et al., 2023). Decentralization conflicts with centralized data management, with a specific data controller recommended by GDPR Article 4 (Finck, 2018). Decentralization can lead to fear of data misuse due to the need for more specific authority and accountability in data management. As a result, consumers can experience psychological reactance that prompts them to resist data-sharing practices facilitated by blockchain systems (Martin et al., 2022). Data management uncertainty due to the need for a central body within decentralization creates a dilemma for

consumers, potentially leading to a privacy paradox. Initially, consumers may share their data despite privacy concerns due to limited options, but they later regret this choice because of uncertainty about data usage.

3.1.3 Transparency

Blockchain technology is renowned for its transparency, which underpins its integrity and accountability (Zhu et al., 2022). Within the blockchain, all transactions and data are inherently transparent and visible to participants in the network. However, the transparency of blockchain technology contradicts GDPR Article 25 (Finck, 2018; Haque et al., 2021). In fact, the transparency of data and its visibility to anyone in the network can prompt resistance due to perceived threats to consumer freedom (Ford et al., 2023). Consumers have no intention of exposing sensitive personal data to unintended recipients. Transparency and traceability will create doubt about data security, leading to privacy paradoxes and fear of unauthorized data access (Kaaniche et al., 2020). Moreover, due to this complete visibility, hackers can trace historical data and predict a consumer's future intentions, further increasing doubts about future disclosures (Corbet et al., 2020).

To address the critical issues of the blockchain that hinder digital transformation, we propose a modified blockchain that adheres to the GDPR guidelines, consumer reactance, and privacy paradox implications based on the three pillars mentioned below.

3.2 Modified blockchain

This paper presents digital vulnerability as a form of consumer vulnerability resulting from the application of blockchain in the digital space. Managing digital vulnerability is pivotal in blockchain's wider acceptance and application as a digital transformation. We propose that the combined effect of the lack of adherence to regulation, the privacy paradox, and

psychological reactance leads to digital vulnerability. Hence, due to blockchain's rigidity, organizations cannot adhere to regulations, creating a false sense of security.

Consumers ascribe heightened certainty to blockchain technology, engendering a misleading privacy paradox. Contrary to this perception, the factual scenario unfolds as an exacerbated privacy paradox, thereby exposing consumers to digital vulnerability. Hence, an increased privacy paradox occurs due to a lack of understanding of its underlying conditions leading to digital vulnerability (Liyanaarachchi et al., 2021). Consequently, this knowledge gap increases consumers' risk of encountering digital vulnerabilities within the blockchain ecosystem. Further, blockchain's decentralized structure, lacking flexibility, triggers psychological reactance (Mazzù et al., 2023).

The reactance, stemming from perceived restrictions on freedom, drives counterproductive behaviors. Users may resist established protocols, neglect security practices, and make inaccurate decisions, resulting in worsening digital vulnerability (Walsh et al., 2021). Lack of trust is a critical factor contributing to customer vulnerability that manifests reactions to accepting blockchain (Tan & Saraniemi, 2022). To reduce reactance, Friedman and Ormiston (2022) suggest that organizations should transition from a one-dimensional control-driven approach to a more customer-friendly approach. Thus, to facilitate effective adoption, organizations should acknowledge blockchain as a socio-technical system (Ehrenberg & King, 2020). Based on the above, we propose that:

P1: Blockchain technology conflicts with regulation, fosters the privacy paradox, and causes psychological reactance, leading to digital vulnerability.

3.2.1 Selective immutability

To address consumer concerns regarding the persistence of sensitive data beyond its original purpose, firms should prioritize immediately deleting such data within the blockchain system.

Companies should establish deletion criteria through negotiable data privacy contracts with consumers. Implementing selective immutability will be pivotal in reducing privacy risks by ensuring that confidential data remains inaccessible, thereby mitigating the privacy paradox and reactance. Furthermore, these efforts align with GDPR Article 17, upholding the "right to forget" principle concerning sensitive data. When a user initiates a data deletion request, the system should promptly trigger a process that removes or anonymizes the relevant data from off-chain storage and updates the blockchain accordingly.

Companies must maintain a comprehensive audit trail of all data-related activities, including data access, modifications, and erasure requests. This documentation serves to demonstrate GDPR compliance, which can be invaluable in the event of audits or investigations. By emphasizing the immediate deletion of such data, firms proactively address these concerns, thereby reducing the likelihood of users experiencing reactance. Introducing selective immutability addresses this paradox by aligning the system's data-handling practices with user expectations. Consequently, users are likelier to trust the system and feel less conflicted about sharing their data, leading to a harmonious balance between privacy protection and data utility. We portray that:

P2: Selective immutability (i.e., identifying criteria for data deletion) is pivotal for the strategic redesign of blockchain

3.2.2 Federal decentralization

Decentralization, involving distributed nodes for transaction processing without a central authority, creates challenges for consumers in identifying entities handling their data (Xue et al., 2021). The absence of clear accountability raises concerns about legal repercussions in case of data mishandling or breaches. Participation of multiple parties in validation without

robust access control mechanisms poses risks of unauthorized data access (Zachariadis et al., 2021). Consumer worries about vetting and security of data access arise. Blockchain's decentralization limits consumer control over data, lacking clear options for consent, retrieval, or deletion (Centobelli et al., 2021), leading to concerns about potential misuse. Decentralized systems struggle to adhere to stringent data protection regulations like GDPR, risking consumer resistance if perceived non-compliance undermines privacy laws (Belen-Saglam et al., 2023).

Despite the benefits of enhanced security through interconnectivity in data processing, challenges to consumer privacy emerge. Addressing these requires a delicate balance between decentralized advantages and mechanisms providing control, responsibility, and confidence in data management (Xue et al., 2021). Organizations should consider establishing a central authority for specific data management, delineating roles with GDPR Article 4 to mitigate decentralization issues while preserving its benefits and ensuring compliance. Streamlining data formats and exchange protocols through interoperability standards facilitates seamless data sharing, guaranteeing adherence to regulation. The proposed federal decentralization facilitates data transfer between blockchain networks, minimizing regret and establishing authority through legal agreements with data-collecting entities. Consumers are pivotal in this context, empowered to oversee data collection firms assert their right to assume control and influence data management. Hence, federal decentralization effectively reduces reactance and mitigates the privacy paradox. We propose that:

P3: Establishing federal decentralization (enabling data guardians) is pivotal for the strategic redesign of blockchain.

3.2.3 Supervised transparency

The transparency of blockchain transactions, which benefits accountability, raises heightened privacy concerns and consumer resistance (Schlatt et al., 2023; Tan & Salo, 2023). Consumers feel uneasy about the accessibility of their transaction history, potentially revealing sensitive information (Tan & Salo, 2023). Addressing these challenges requires careful consideration of technical, legal, and user-centric solutions to ensure a harmonious integration of blockchain and consumer privacy (Dwivedi et al., 2023). While ensuring openness, this transparency may lead to a perceived lack of control over personal data, triggering consumer resistance (Walsh et al., 2021). The traceability and automated decision-making aspects of blockchain conflict with GDPR principles, requiring more customer-centric privacy management (Belen-Saglam et al., 2023; Raddatz et al., 2023).

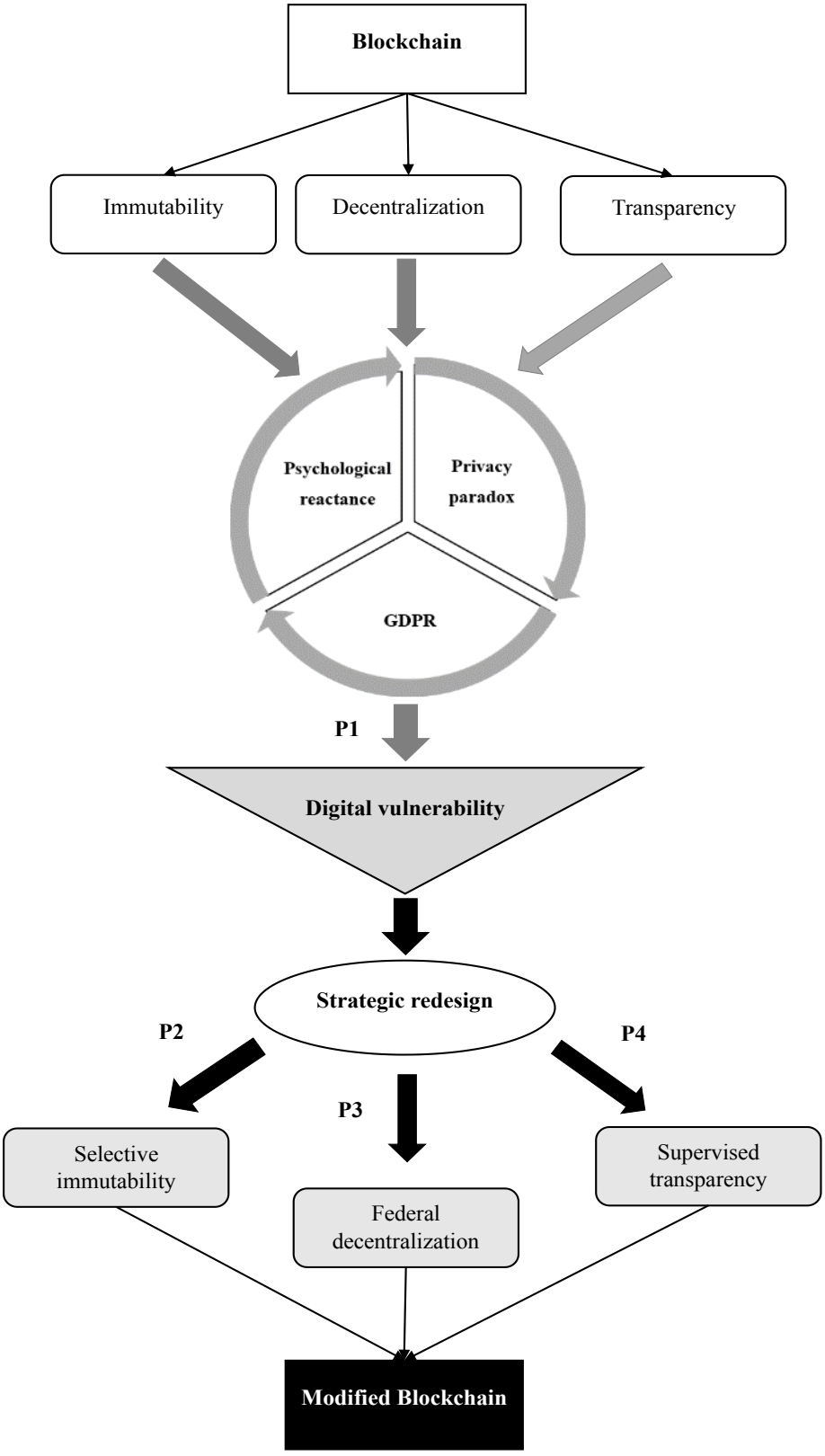
To address privacy issues and resistance, we propose "supervised transparency." This approach involves continuously monitoring data behavior within the blockchain, tracking movements and third-party actions to ensure privacy. Companies should establish a recording system listing entities accessing data, making results available to customers for credibility and accountability. Supervised transparency aligns with GDPR Article 25, embodying "data protection by design and default." This enables the integration of privacy-enhancing features into the blockchain architecture, ensuring inherent data protection. Online real-time supervision empowers users to assert authority over their data, reducing psychological reactance and facilitating control. This ensures accessibility while maintaining a manageable level of privacy grounded in consumer privacy concerns.

Supervised transparency establishes a harmonious relationship between blockchain technology and data protection. This not only ensures compliance but also preserves user trust and freedom. In light of these considerations, we propose that:

P4: Supervised transparency (i.e., traceability with an audit trail at the company level) is pivotal for the strategic redesign of blockchain.

Figure 1 presents the conceptual model, highlighting our suggested modified blockchain framework.

Figure 1: Modified blockchain



4. Conclusion, implications, and future research direction.

4.1 Conclusion

This study depicts significant privacy concerns associated with applying blockchain technology in consumer perspectives and regulatory governance, impeding its role in digital transformation. We introduce the "modified blockchain" concept, highlighting the impact of consumer reactance, the privacy paradox, and adherence to privacy regulation in managing digital vulnerability. The conceptual model, encompassing four actionable propositions, offers organizations a structured framework to revamp existing blockchain methodologies, nurturing a customer-centric paradigm. This transformative shift empowers organizations to transition from an internally focused blockchain approach to one that integrates social considerations, manifesting a social-technical approach.

Addressing a literature gap where technical aspects overshadowed consumer resistance and privacy concerns (Alam et al., 2021; Mazzù et al., 2023; Schlatt et al., 2023; Tan & Salo, 2023), we emphasize the importance of exploring social perspectives on blockchain privacy. The paper identifies psychological reactance, privacy paradox, and non-compliance with data privacy regulations leading to consumer digital vulnerability. Therefore, advocates for the effective adoption of blockchain through a customer-oriented stakeholder approach rather than a single-dimensional imbalanced power-based approach.

4.2. Theoretical implications

The paper offers three theoretical contributions. First, it provides a novel avenue for the blockchain literature, which has traditionally focused on improving efficiency. The modified blockchain encourages an 'outside-in' perspective driven by a customer-centric approach instead of a technology-centric one. This shift aims to drive long-term benefits and sustainable competitive advantages by managing digital vulnerability. This paper introduces the concept of digital vulnerability resulting from the influence of contemporary blockchain

applications. Additionally, it extends the existing body of literature on consumer vulnerability, establishing connections among psychological reactance, privacy paradox, and regulation within the digital domain. Furthermore, it addresses the scholarly call for more research in blockchain adaptability within social contexts, aligning with the future trajectory of consumer vulnerability research (Basu et al., 2023; Galli, 2022; Miglionico, 2023; Prakash et al., 2022; Schlatt et al., 2023; Tan & Saraniemi, 2023). Additionally, it answers the call from scholars for a stronger connection between blockchain technology and consumers to strike a more balanced relationship (Dwivedi et al., 2023; Ford et al., 2023; Li et al., 2023; Shafay et al., 2023).

Second, the study recognizes the profound impact of blockchain technology on psychological reactance theory, particularly concerning individuals' autonomy in managing their data. While the prevailing literature generally suggests that heightened data security reduces consumer reactance (Badewi et al., 2023; Martin & Murphy, 2017; Ogbanufe & Gerhart, 2022), this research introduces a groundbreaking perspective. We contend that increased control over personal data, often facilitated by enhanced security within the blockchain, can adversely lead to elevated levels of psychological reactance. This counterintuitive viewpoint challenges conventional wisdom and significantly diverges from the established discourse. Further, the conceptual model proposed in this study provides a robust foundation for addressing the scholarly call to explore the influence of advanced technology usage on psychological reactance (Badewi et al., 2023; Chang et al., 2023; Martin et al., 2022). This groundbreaking doctrine, proposing that heightened data security measures may increase consumer reactance, initiates a new research path, opening up a fresh avenue for scholarly investigation. The psychological reactance emerges due to the lack of choice in managing customer data. The modified blockchain is designed to overcome this imbalance of power that leads to a lack of freedom. Federal decentralization enables the customers to

exercise autonomy over data. Selective immutability enables data deletion, shifting the ownership from the blockchain system to the customer. Supervised transparency provides continuous freedom for customers to verify the data status throughout decision-making. Organizations, in turn, must proactively formulate innovative strategies to surmount reactance and attain proficient user adoption of the blockchain (Mazzù et al., 2023). The combined effect of the changes introduced through the modified blockchain will reduce the antecedents that lead to the threat of freedom to manage data and reduce the reactance. Reducing barriers encourages increased engagement with blockchain systems and facilitates effective adoption.

Third, this study extends the privacy paradox theory by introducing a new dimension: a shift in the locus of privacy controls from organizations to consumers. Within this innovative conceptual framework, we posit that consumers increasingly seek active involvement in managing their privacy, even when dealing with technologically assured systems like blockchain. This paradigm shift challenges the conventional approach (Acquisti et al., 2023; Kokolakis, 2017; Martin & Murphy, 2017), primarily relying on technology-driven solutions to address privacy concerns. The expanded perspective on the privacy paradox resonates with contemporary privacy discourse and suggests potential avenues for developing more user-centric privacy practices. Furthermore, it addresses the research gap by examining the privacy paradox within a broader sociotechnical paradigm, in line with the suggestions of Acquisti et al. (2023).

Data visibility, reliance on past data, and lack of flexibility in data management exacerbate the privacy paradox in the blockchain. A primarily system-driven approach to managing consumer data creates a power imbalance, heightening privacy concerns and resistance due to a lack of choices (Liyanaarachchi et al., 2023). However, a modified blockchain mitigates this risk by providing control through federal decentralization,

enhancing flexibility. The modified blockchain ensures higher data protection by employing selective immutability, allowing the deletion of sensitive data. Further, implementing supervised transparency minimizes the risk of public visibility of data. These three features of modified blockchain empower consumers to manage the privacy paradox, overcoming the additional threat posed by an imbalanced, one-dimensional, system-driven approach to privacy.

4.3. Managerial implications

The selective immutability, federal decentralization, and supervised transparency proposals have implications for users, policy makers, and companies. At the very heart of blockchain usage are the users/consumers of the service (see Figure 2). As we mentioned earlier, they may feel vulnerable to using this technology due to its flaws, and consequently find themselves in situations of privacy paradox or trigger reactance. It seems essential as a first step, that policy makers put in place the first foundation, which is federal decentralization. Just as the GDPR law has been able to structure companies' activities about protecting consumers' privacy, decentralization would be the first point of support for companies so that they can have an orientation on what they need to do to comply with the GDPR rules when using blockchain.

Policy makers, through federal decentralization, would be relays that would come in support to guide companies to comply. Their overall role would be to guide compliance with the GDPR rules, with a more specific role on blockchain for compliance with selective immutability and supervised transparency. For selective immutability, policy makers are responsible for defining what constitutes sensitive data to protect users. It is also the responsibility of policy makers to demand that each company be able to i) offer each user access to all the personal data held on them on a single platform, ii) highlight the sensitive

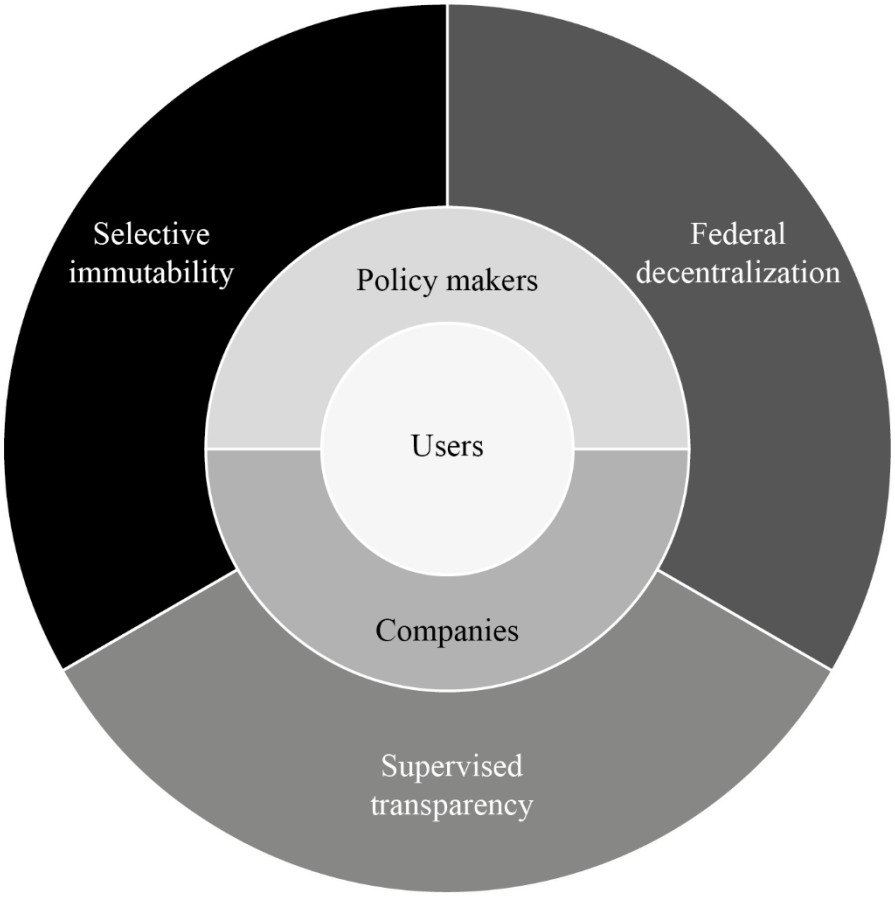
nature of certain data, and iii) give the possibility for the user to delete it at any time. In this way, the modified blockchain's third pillar of supervised transparency would be respected. By having a legal basis and federal decentralization, policy makers will have both the role of guiding companies and ensuring that companies apply the rules properly. A training offer for companies by this decentralized authority should accompany this guiding role.

On the company side, a modified blockchain would have a major impact on how data is managed. While expecting from a decentralized state authority, companies can already try to implement tools enabling customers to delete data they consider sensitive. The company also must provide each customer with transparent, real-time access to all the data it holds. Only in this way, with acute transparency and the possibility of modifying or deleting data at any time, can the privacy paradox, vulnerability, and consumer reactance be reduced. To achieve this, companies must conduct an in-depth internal study to identify any flaws in the system that do not comply with articles 4, 17, and 25 of the GDPR to be able to comply. Based on the internal vulnerability assessment and the establishment of a benchmark, the company must prioritize the implementation of solutions to comply with the modified blockchain. This crucial task can only be accomplished by creating a dedicated internal department. It seems essential to emphasize the importance of prioritizing these changes because implementing a modified blockchain can be a competitive advantage for the company. There are already embryonic industry attempts to overcome these issues (see AliAzad (2022).

In conclusion, we must emphasize that modifying blockchain involves major technical, financial, and human barriers. Not only does it require an internal department, but also an in-depth diagnosis of the system. This has already been highlighted concerning adopting blockchain in companies (Khan et al., 2023; Komulainen & Nätti, 2023). However,

having a federal state authority as a guide and support can alleviate these barriers and allow companies to implement a modified blockchain confidently.

Figure 2: Modified blockchain implications on main shareholders



4.4. Limitations and future research direction

The theoretical nature of this work presents some limitations, highlighting opportunities for future research to validate the applicability of a redesigned blockchain based on private paradox, psychological reactance, and GDPR principles.

First, this research prompts a consideration of the discussed paradigm in an international context, moving beyond the European Union, where GDPR is enforced. Notably, non-EU nations, including China, Japan, and Singapore, have widely adopted blockchain technology under their distinct legal systems (Kisters, 2022). Consequently, there

is an opportunity for future research to explore how these countries address digital vulnerabilities through blockchain in the absence of GDPR mandates. It's worth noting that these countries, particularly China, encounter challenges in aligning with GDPR standards (Li et al., 2019). Singapore's approach to data protection, the PDPA, is also noteworthy for its business-friendly stance, navigating the interplay between commerce and privacy (Tan et al., 2023).

Next, our study centers on consumer perspectives, analyzing the effects of controlled immutability and regulated transparency on issues like the privacy paradox, psychological reactance, and digital vulnerability. We encourage researchers to delve into the interplay of these factors, illuminating how they may shape the evolution of blockchain technology. With an emphasis on decentralized federal structures, our goal is to bolster consumer trust in blockchain adoption. Future studies might explore how this trust transfers from decentralized systems to blockchain mechanisms, particularly regarding data sharing behaviors.

Furthermore, future investigations could assess the influence of an evolved blockchain on corporate reputation and its potential to foster competitive differentiation. We extend an invitation to researchers to empirically test these theories in varied blockchain uses, including finance, supply chains, and healthcare. The application of our conceptual framework could extend to digital services like payment systems, including PayPal, and cryptocurrencies. Additionally, there is scope to examine how such a blockchain modification could improve internal organizational processes, efficiency, and productivity. An in-depth exploration into how a restructured blockchain could integrate across different organizational departments presents another promising research trajectory.

Last, we call upon scholars to evaluate the application of this modified blockchain in both national and international policy-making, particularly concerning e-commerce and digital innovation. This involves crafting tailored policies and strategies for implementing

this blockchain variant to address digital vulnerabilities. Future research should also contemplate the creation of appropriate codes of conduct, educational initiatives, and financial incentives under a central authority, to strike a strategic balance among the interests of various stakeholders. It's critical to develop a comprehensive policy framework on a global level, acknowledging that the regulation of blockchain and related phenomena, such as cryptocurrencies, extends beyond traditional legal confines.

References

Acquisti, A., Adjerid, I., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., ... & Wilson, S. (2023). Nudges (and Deceptive Patterns) for Privacy: Six Years Later. In *The Routledge Handbook of Privacy and Social Media* (pp. 257-269). Routledge.

Alalwan, A. A., Baabdullah, A. M., Dwivedi, Y. K., Rana, N. P., Lal, B., & Raman, R. (2021). Et-moone and marketing relationship governance: The effect of digital transformation and ICT during the COVID-19 pandemic. *Industrial Marketing Management*, *98*, 241-254.

Alam, S., Shuaib, M., Khan, W. Z., Garg, S., Kaddoum, G., Hossain, M. S., & Zikria, Y. B. (2021). Blockchain-based initiatives: current state and challenges. *Computer Networks*, *198*, 108395.

AliAzad (2022) *What's the meaning of compliant privacy?*, *Medium*. Available at: https://medium.com/omniaprotocol/whats-the-meaning-of-compliant-privacy-88bae3d22ada (Accessed: 15 December 2023).

Alza, G Jr (2020). Blockchain & CCPA. *Santa Clara High Technology Law Journal 37*, 231–255.

Ante, L. (2021). Smart contracts on the Blockchain–A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519.

Ariella, S (2030). *30 Striking Cryptocurrency Statistics [2023]: Market Value, Bitcoin Usage, and Trends*. Retrieved 15.09.2023 from https://www.zippia.com/advice/cryptocurrency-statistics/#:~:text=There%20are%20an%20estimated%20420,users%20grew%20by%20190%25%20globally.

Badewi, A. A., Eid, R., & Laker, B. (2023). Determinations of system justification versus psychological reactance consumer behaviors in online taboo markets. *Information Technology & People*, *36*(1), 332-361.

Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building understanding of the domain of consumer vulnerability. *Journal of macromarketing*, *25*(2), 128-139.

Baiyere, A., Salmela, H., & Tapanainen, T. (2020). Digital transformation and the new logic of business process management. *European Journal of Information Systems*, *29*(3), 238-259.

Bambysheva, N., & Linares, M. G. S. (2022). *Over $3 Billion Stolen In Crypto Heists: Here Are The Eight Biggest. Forbes*. Retrieved 05.09.2023 from https://www.forbes.com/sites/ninabambysheva/2022/08/01/over-3-billion-stolen-in-crypto-heists-here-are-the-eight-biggest/?sh=22b4976e5cc8.

Basu, R., Kumar, A., & Kumar, S. (2023). Twenty- five years of consumer vulnerability research: Critical insights and future directions. *Journal of Consumer Affairs*, *57*(1), 673-695.

Baquero, P. M. (2023). Layers of privacy in the blockchain: from technological solutionism to human-centred privacy-compliance technologies. *International Journal of Law in Context*, *19*(1), 51-69.

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2023). A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*, 100129.

Berg, L. (2015). Consumer vulnerability: are older people more vulnerable as consumers than others?. *International Journal of Consumer Studies*, *39*(4), 284-293.

Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research*, *27*(5), 725-740.

Brehm, J.W. (1966). *A Theory of Psychological Reactance*, Academic Press, New York.

Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering*, *90*, 106897.

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

Centobelli, P., Cerchione, R., Esposito, E., & Oropallo, E. (2021). Surfing blockchain wave, or drowning? Shaping the future of distributed ledgers and decentralized technologies. *Technological Forecasting and Social Change*, *165*, 120463.

Chan, H. L., Choi, T. M., & De la Torre, D. M. (2023). The "SMARTER" framework and real application cases of blockchain. *Technological Forecasting and Social Change*, *196*, 122798.

Chang, J. Y. S., Konar, R., Cheah, J. H., & Lim, X. J. (2023). Does privacy still matter in smart technology experience? A conditional mediation analysis. *Journal of Marketing Analytics*, 1-16.

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2020). The destabilising effects of cryptocurrency cybercriminality. *Economics Letters*, *191*, 108741.

Cozzio, C., Viglia, G., Lemarie, L., & Cerutti, S. (2023). Toward an integration of blockchain technology in the food supply chain. *Journal of Business Research*, *162*, 113909.

Dongqin, C., Can, P. & Guanglei, Y. (2022). The pressure of political promotion and renewable energy technological innovation: A spatial econometric analysis from China. *Technological Forecasting and Social Change*, *183*, 121888.

Dwivedi, Y. K., Balakrishnan, J., Das, R., & Dutot, V. (2023). Resistance to innovation: A dynamic capability model based enquiry into retailers' resistance to blockchain adaptation. *Journal of Business Research*, *157*, 113632.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542.

Echeverri, P., & Salomonson, N. (2019). Consumer vulnerability during mobility service interactions: causes, forms and coping. *Journal of Marketing Management*, *35*(3-4), 364-389.

Ehrenberg, A. J., & King, J. L. (2020). Blockchain in context. *Information Systems Frontiers*, *22*, 29-35.

Friedman, N., & Ormiston, J. (2022). Blockchain as a sustainability-oriented innovation?: Opportunities for and resistance to Blockchain technology as a driver of sustainability in global food supply chains. *Technological Forecasting and Social Change*, *175*, 121403.

Finck, M. (2018). Blockchains and data protection in the European Union. *European Data Protection Law Review*, *4*, 17-35

Ford, J., Jain, V., Wadhwani, K., & Gupta, D. G. (2023). AI advertising: An overview and guidelines. *Journal of Business Research, 166,* 114124.

Frantziou, E. (2014). Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos. *Human rights law review*, *14*(4), 761-777.

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, *51*, 102029.

Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR compliant blockchains–a systematic literature review. *IEEE Access*, *9*, 50593-50606.

Hennel, C (2021), *CCPA: California Consumer Privacy Act Explained*, Retrieved 15.09.2023 from https://termly.io/resources/articles/ccpa/#what-is-ccpa-california-consumer-privacy-act-of-2018

Galli, F. (2022). Digital Vulnerability. In *Algorithmic Marketing and EU Law on Unfair Commercial Practices* (pp. 181-207). Cham: Springer International Publishing.

Glavas, C., Letheren, K., Russell-Bennett, R., McAndrew, R., & Bedggood, R. E. (2020). Exploring the resources associated with consumer vulnerability: Designing nuanced retail hardship programs. *Journal of Retailing and Consumer Services*, *57*, 102212.

Gurzhii, A., Islam, A. N., Haque, A. B., & Marella, V. (2022). Blockchain enabled digital transformation: a systematic literature review. *IEEE Access*, *10*, 79584–79605

Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. *Blockchain: Research and Applications*, *2*(4), 100027.

Joo, M., Kim, S. H., Ghose, A., & Wilbur, K. C. (2022). Designing Distributed Ledger technologies, like blockchain, for advertising markets. *International Journal of Research in Marketing*, *40*(1), 12-21.

Kaaniche, N., Laurent, M., & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *Journal of Network and Computer Applications*, *171*, 102807.

Khan, S., Haleem, A., Husain, Z., Samson, D. and Pathak, R.D. (2023), "Barriers to blockchain technology adoption in supply chains: the case of India", Operations Management Research, Vol. 16 No. 2, pp. 668–683, doi: 10.1007/s12063-023-00358-z.

Kisters, S (2022). *The Top 10 Countries that Use Crypto and Bitcoin the Most*, Retrieved 18.01.2024 from https://originstamp.com/blog/the-top-10-countries-that-use-crypto-and-bitcoin-the-most/

Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Manage*ment, *63*, 102466.

Kohli, R., & Liang, T. P. (2021). Strategic integration of blockchain technology into organizations. *Journal of Management Information Systems*, *38*(2), 282-287.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134.

Komulainen, R. and Nätti, S. (2023), "Barriers to blockchain adoption: Empirical observations from securities services value network", Journal of Business Research, Vol. 159, p. 113714, doi: 10.1016/j.jbusres.2023.113714.

Lee, H., & Choi, K. S. (2022). Interrelationship between Bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework. In *The New Technology of Financial Crime* (pp. 82-103). Routledge.

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1-6.

Li, Y., Liao, A., Li, L., Zhang, M., Zhao, X., & Ye, F. (2023). Reinforcing or weakening? The role of blockchain technology in the link between consumer trust and organic food adoption. *Journal of Business Research*, *164*, 113999.

Liang, W., & Ji, N. (2022). Privacy challenges of IoT-based blockchain: a systematic review. *Cluster Computing*, *25*(3), 2203-2221.

Liu, Y., Lu, Q., Zhu, L., Paik, H. Y., & Staples, M. (2023). A systematic literature review on blockchain governance. *Journal of Systems and Software*, *197*, 111576.

Liyanaarachchi, G., Thaichon, P. & Weaven, S. (2019). *Managing the Privacy Paradox through Sharing Economy*. Proceedings of the Australian and New Zealand Marketing Academy Conference (ANZMAC), Wellington, New Zealand.

Liyanaarachchi, G. (2021), Managing privacy paradox through national culture: Reshaping online retailing strategy. *Journal of Retailing and Consumer Services*, *60*, 02500.

Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2021). Market-oriented corporate digital responsibility to manage data vulnerability in online banking. *International Journal of Bank Marketing*, *39*(4), 571-591.

Liyanaarachchi, G., Viglia, G., & Kurtaliqi, F. (2023). Privacy in hospitality: managing biometric and biographic data with immersive technology. *International Journal of Contemporary Hospitality Management*. Ahead-of-print, https://doi.org/10.1108/IJCHM-06-2023-0861.

Maesa, D. D. F., & Mori, P. (2020). Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing*, *138*, 99-114.

Mashatan, A., Sangari, M. S., & Dehghani, M. (2022). How perceptions of information privacy and security impact consumer trust in crypto-payment: an empirical study. *IEEE Access*, *10*, 69441-69454.

Martin, B. A., Chrysochou, P., & Strong, C. (2022). Crypto freedom! Effects of trait reactance and regulation content on intention to buy cryptocurrency. *Personality and Individual Differences*, *194*, 111659.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*, 135-155.

Marthews, A., & Tucker, C. (2023). What blockchain can and can't do: Applications to marketing and privacy. *International Journal of Research in Marketing*, *40*(1), 49-53.

Mazzu, M.F., Pozharliev, R., Andria, A. & Baccelloni, A. (2023), Overcoming the blockchain technology credibility gap. Psychology and Marketing, *40* (9), 1791-1807

Miglionico, A. (2023). Digital payments system and market disruption. Law and Financial Markets Review, 1-16.

Mitzner. D. (2022), *Smart Regulations Can Boost Blockchain Adoption In Retail And Ecommerce*, Retrieved 05.09.2023 from https://www.forbes.com/sites/dennismitzner/2022/05%20/12/smart-regulations-can-boost-blockchain-adoption-in-retail-and-ecommerce/?sh%20=36f2e36a786c.&sh=224e5702b85e

Morgan, S. (2023), *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*, Retrieved 05.09.2023 from https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

Ogbanufe, O., & Gerhart, N. (2022). Exploring smart wearables through the lens of reactance theory: Linking values, social influence, and status quo. *Computers in Human Behavior, 127*, 107044.

Onjewu, A. K. E., Walton, N., & Koliousis, I. (2023). Blockchain agency theory. *Technological Forecasting and Social Change, 191*, 122482.

Patil, K., Ojha, D., Struckell, E. M., & Patel, P. C. (2023). Behavioral drivers of blockchain assimilation in supply chains–A social network theory perspective. *Technological Forecasting and Social Change, 192*, 122578.

Palacios-Marqués, D., Gallego-Nicholls, J. F., & Guijarro-García, M. (2021). A recipe for success: Crowdsourcing, online social networks, and their impact on organizational performance. *Technological Forecasting and Social Change, 165*, 120566.

Perdana, A., Lee, W. E., & Robb, A. (2021). From enfant terrible to problem-solver? Tracing the competing discourse to explain blockchain-related technological diffusion. *Telematics and Informatics, 63*, 101662.

Peres, R., Schreier, M., Schweidel, D. A., & Sorescu, A. (2023). Blockchain meets marketing: Opportunities, threats, and avenues for future research. *International Journal of Research in Marketing, 40*(1), 1-11.

Politou, E., Alepis, E., Virvou, M., Patsakis, C., Politou, E., Alepis, E., . . . Patsakis, C. (2022). The "right to be forgotten" in the GDPR: implementation challenges and potential solutions. *Privacy and Data Protection Challenges in the Distributed Era*, 41-68.

Prakash, R., Anoop, V. S., & Asharaf, S. (2022). Blockchain technology for cybersecurity: A text mining literature analysis. *International Journal of Information Management Data Insights*, *2*(2), 100112.

Raddatz, N., Coyne, J., Menard, P., & Crossler, R. E. (2023). Becoming a blockchain user: understanding consumers' benefits realisation to use blockchain-based applications. *European Journal of Information Systems*, *32*(2), 287-314.

Rawat, D.B., Chaudhary, V., Doku, R. (2020), Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems. *Journal of Cybersecurity and Privacy*, *1*(1), 4-18.

Ribeiro-Navarrete, S., Saura, J. R., & Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. *Technological Forecasting and Social Change*, *167*, 120681.

Riela, M. J. (2023). Comprehensive Data-Privacy Laws May Affect a Distressed-Asset Sale. *American Bankruptcy Institute Journal*, *42*(7), 24-55.

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, *39*(4), 101679.

Saura, J. R., Palacios-Marqués, D., & Ribeiro-Soriano, D. (2023). Privacy concerns in social media UGC communities: Understanding user behavior sentiments in complex networks. *Information Systems and e-Business Management*, 1-21.

Schlatt, V., Guggenberger, T., Schmid, J., & Urbach, N. (2023). Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. *International journal of information management*, *68*, 102470.

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. Electronic Markets, 32(3), 1779-1794.

Shafay, M., Ahmad, R. W., Salah, K., Yaqoob, I., Jayaraman, R., & Omar, M. (2023). Blockchain for deep learning: review and open challenges. *Cluster Computing*, *26*(1), 197-221.

Stanley, A (2023), *More than half of the world's central banks are exploring or developing digital currencies*, Retrieved 15.09.2023 from https://www.imf.org/en/Publications/fandd/issues/2022/09/Picture-this-The-ascent-of-CBDCs

Stewart, D.W. (2022) Marketing's contribution to consumer welfare: a research agenda. *Journal of Consumer Affairs*, *56*(4), 1423–1432.

Su, D., Zhang, L., Peng, H., Saeidi, P., & Tirkolaee, E. B. (2023). Technical challenges of blockchain technology for sustainable manufacturing paradigm in Industry 4.0 era using a fuzzy decision support system. *Technological Forecasting and Social Change*, *188*, 122275.

Tan, S. Y., Taeihagh, A., & Pande, D. (2023). Data sharing in disruptive technologies: lessons from adoption of autonomous systems in Singapore. *Policy Design and Practice*, *6*(1), 57-78.

Tan, T. M., & Saraniemi, S. (2023). Trust in blockchain-enabled exchanges: Future directions in blockchain marketing. *Journal of the Academy of marketing Science*, *51*(4), 914-939.

Tan, T. M., & Salo, J. (2023). Ethical marketing in the blockchain-based sharing economy: Theoretical integration and guiding insights. *Journal of Business Ethics*, *183*(4), 1113-1140.

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law & Security Review*, *38*, 105454.

Tucker, C., & Catalini, C. (2018). *What Blockchain Can't Do*. Retrieved 10.09.23 from https://hbr.org/2018/06/what-blockchain-cant-do

Utz, M., Johanning, S., Roth, T., Bruckner, T., & Strüker, J. (2023). From ambivalence to trust: Using blockchain in customer loyalty programs. *International Journal of Information Management*, *68*, 102496.

Walsh, C., O'Reilly, P., Gleasure, R., McAvoy, J., & O'Leary, K. (2021). Understanding manager resistance to blockchain systems. *European Management Journal, 39*(3), 353-365.

Wang, Z., Zheng, Z., Jiang, W., & Tang, S. (2021). Blockchain- enabled data sharing in supply chains: Model, operationalization, and tutorial. *Production and Operations Management*, *30*(7), 1965-1985.

Wang, C., Zhang, N., & Wang, C. (2021). Managing privacy in the digital economy. *Fundamental Research*, *1*(5), 543-551.

Wong, L.-W., Tan, G.W.-H., Ooi, K.-B. and Dwivedi, Y. (2023). The role of institutional and self in the formation of trust in artificial intelligence technologies, *Internet Research,* ahead-of-print https://doi.org/10.1108/INTR-07-2021-0446

World Economic Forum. (2015). *Deep Shift Technology Tipping Points and Societal Impact Survey Report*. Retrieved 04.09.2023 from http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015. Pdf.

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation, 5*(1), 1-14.

Xue, X., Dou, J., & Shang, Y. (2021). Blockchain-driven supply chain decentralized operations–information sharing perspective. *Business Process Management Journal*, *27*(1), 184-203.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), e0163477.

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, *29*(2), 105-117.

Zhang, Z., Ren, D., Lan, Y., & Yang, S. (2022). Price competition and blockchain adoption in retailing markets. *European Journal of Operational Research*, *300*(2), 647-660.

Zheng, X. R., & Lu, Y. (2022). Blockchain technology–recent research and future trend. *Enterprise Information Systems*, *16*(12), 1939895.

Zhu, Q., Bai, C., & Sarkis, J. (2022). Blockchain technology and supply chains: The paradox of the atheoretical research discourse. *Transportation Research Part E: Logistics and Transportation Review*, *164*, 102824.