What makes you trust digital data wallets?

Antecedents of trust formation

Varvara Keba
[0000-0002-3686-3719]
20220011@novaims.unl.pt
NOVA Information Management School (NOVA IMS), Universidade Nova de Lisboa, Campus de Campolide, 1070-312 Lisboa, Portugal

Gurpreet Dhillon
[0000-0002-0487-4050]
College of Business Administration, University of Nebraska Omaha, Omaha, Nebraska, USA

Tiago Oliveira
[0000-0001-6523-0809]
NOVA Information Management School (NOVA IMS), Universidade Nova de Lisboa, Campus de Campolide, 1070-312 Lisboa, Portugal

This is the final Author Peer Reviewed version of:

Keba, V., Dhillon, G., & Oliveira, T. (2026). What makes you trust digital data wallets? Antecedents of trust formation. Journal of Enterprise Information Management. https://doi.org/10.1108/JEIM-12-2025-1258

Funding: We would like to thank the Fundação para a Ciência e aTecnologia (FCT) regarding the program UIDB/04152/2020-Centro de Investigação em Gestão de Informação –MagIC (NOVA IMS). This work was also supported by the European Union's Horizon 2020 innovation action program, project: SOTERIA, Grant agreement ID: 101018342.

This work is licensed under Creative Commons Attribution-NonCommercial 4.0 International. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc/4.0/ This means that anyone may distribute, adapt, and build upon the work for non-commercial purposes, subject to full attribution. If you wish to use this manuscript for commercial purposes, please contact permissions@emerald.com.

Journal of Enterprise Information Management

What makes you trust digital data wallets?
Antecedents of trust formation

Abstract

Purpose - Digital data wallets are emerging privacy-enhancing technologies that give users greater control over their personal information, yet trust remains a major barrier to adoption. This study aims to identify the factors shaping trust and how perceived risks moderate these relationships.

Design/methodology/approach – Using a mixed-methods approach, thirty qualitative interviews conducted in Austria, Romania, and Spain identified four key antecedents of trust: trust in the Internet, trust in the community of internet users, trust in the provider, and trust in the information system. A follow-up survey of 1,200 respondents tested the impact of these antecedents and the moderating role of perceived risks (identity theft and financial loss) on trust formation.

Findings – Results show that all antecedents, specifically performance expectancy, transparency, social influence, and safety, significantly related to their respective trust targets, and that trust relationships are interdependent across targets. Risk perceptions strengthen the influence of performance expectancy and social influence but weaken the effect of transparency.

Originality – The study contributes to research on trust in digital data wallets by empirically applying and extending the application network-of-trust model to the context of decentralized personal data management. The findings demonstrate that the trust formation is differentiated across multiple trust targets and shaped by context-specific antecedents and perceived risks. The study also provides actionable insights for designers and policymakers seeking to build trustworthy digital data wallets.

Keywords: Digital data wallets, privacy-enhancing technology, trust formation, risk perceptions, mixed-method

Paper type: Research paper

Journal of Enterprise Information Management

What makes you trust digital data wallets?
Antecedents of trust formation

1. Introduction

Digital platforms have extensively collected and commodified personal data, prompting serious concerns about data misuse and diminishing individual autonomy (Lukkien *et al.*, 2023; Silva *et al.*, 2022). A global survey revealed that 84% of users feel they lack control over their personal information, underscoring a deep crisis of trust and a structural asymmetry between data subjects and controllers (Cassie, 2024). This imbalance erodes user agency and fuels growing skepticism toward digital services, creating an urgent need for solutions that restore control and rebuild confidence in data exchanges (Ashuri, 2024). Privacy-enhancing technologies (PETs) have emerged in response to these concerns, offering users tools to manage their personal data more securely (Fischer-Hbner and Berthold, 2017). Among these, digital data wallets represent a particularly promising approach. Digital data wallets are designed to store and manage access to personal data (SOTERIA, 2023). By integrating decentralized data storage with secure identity management, these tools aim to empower individuals to control access to their personal information (European Commission, 2023; SOTERIA, 2023). However, the effectiveness of these technologies depends on public trust (Coopamootoo, 2020; Ghaiumy Anaraky *et al.*, 2024; Harborth and Pape, 2020).

Although trust is widely recognized as a critical factor in the adoption of PETs, there is limited understanding of how trust specifically develops in the context of digital data wallets, which combine elements of data management, credential storage, and user-controlled data sharing. Recent initiatives, including the EU Digital Identity Wallet (European Commission, 2023), Brazil's dWallet (Srnicek, 2026), and Soteria (SOTERIA, 2023), reflect a broader move toward user-centric data control and highlight the importance of understanding how trust forms in this emerging technology.

Previous literature on digital data wallets provides valuable insights into usability (Babel *et al.*, 2025), security (Sauer *et al.*, 2025), and governance (Lukkien *et al.*, 2023). However, it does not systematically examine how users develop trust in these technologies. Prior research has not investigated how different factors influence distinct trust targets - such as the system itself, the service provider, the internet, or the user community – within a unified framework (Kuen, Westmattelmann, *et al.*, 2023; Söllner *et al.*, 2016). Furthermore, perceived risks, including fears of identity theft or financial loss, complicate the formation and maintenance of trust (Yan *et al.*, 2024; Zou *et al.*, 2020).

This study investigates these dynamics by examining the antecedents of trust in digital data wallets. It explores how trust develops across distinct targets and how perceived risks moderate these relationships. Specifically, the research addresses three key questions: (1) What factors influence trust in digital data wallets? (2) How do these factors shape trust across different trust targets? (3) In what ways do risk perceptions alter these relationships? By answering these questions, the study contributes to the development of trustworthy digital identity infrastructures and advances theoretical understanding of trust in digital data wallets.

Journal of Enterprise Information Management

2. Theoretical background

Digital data wallets

Digital transformation has intensified data exchange between organizations and individuals while amplifying concerns about privacy, control, and data governance (Lukkien *et al.*, 2023). Digital data wallets have emerged as a distinct form of self-sovereign identity technology that allows individuals to store and selectively share personal data while accessing online services (Keba *et al.*, 2025; SOTERIA, 2023). Despite the establishment of governmental initiatives like the EU Digital Identity Wallet (European Commission, 2023), Brazil's dWallet (Srnicek, 2026), and commercial equivalence like Soteria (SOTERIA, 2023), understanding how end-users perceive and adopt these technologies remains limited (Babel *et al.*, 2025; Korir *et al.*, 2022).

Most research on digital data wallets and related technologies examines technical architecture (Sedlmeir *et al.*, 2021), conceptual foundations (Babel et al., 2025; Jørgensen and Beck, 2022), and regulatory frameworks (Comandè and Varilek, 2024; Ngwenyama *et al.*, 2021). Few studies examine a sociotechnical perspective that considers both technical and social factors (Keba *et al.*, 2025; Laatikainen *et al.*, 2025), leaving a gap in understanding end-users' behavior.

Usability emerges as a critical factor in engagement with digital data wallets (Korir *et al.*, 2022; Sauer *et al.*, 2025). Barriers such as technical complexity and a lack of user-friendly interfaces with privacy and control are confusing or difficult for users (Lukkien *et al.*, 2023; Podgorelec *et al.*, 2022; Yan *et al.*, 2024). Trust plays a pivotal role in the successful implementation and user adoption of digital data wallets. Previous research emphasized that robust security measures and regulatory frameworks are essential for protecting credentials and fostering trust (Ngwenyama *et al.*, 2023; Sauer *et al.*, 2025). Without sufficient trust, adoption barriers can reduce usage and limit the potential benefits, such as enhanced privacy. Digital data wallets are novel technologies. Therefore, deciding to use digital data wallets might be strongly influenced by users' trust in these technologies' ability to achieve their objectives.

Digital data wallets aim to empower users with greater control over their personal information in digital environments (European Commission, 2023; SOTERIA, 2023). These technologies integrate secure identity mechanisms and decentralized data storage to reduce unnecessary disclosure of personal information, embodying the principles of PETs (Fischer-Hbner and Berthold, 2017). Table 1 presents research on PETs from the behavioral perspective from the last 10 years.

Table 1. Research on PETs

Source	Context	Method	Main findings
Ashuri, (2024)	I*	Qualitative analysis	Users felt empowered but wanted more user-friendly solutions.
Ghaiumy Anaraky et al. (2024)	IoTInspector*	Experiment	Promotion-focused users prioritized benefits; prevention-focused users prioritized trust.
Lucier et al. (2023)	NeuroTechnology*z	Experiment	NeuroTech and mobile authentication reduced privacy risks, anxiety and increased download intention and positive attitudes.

Journal of Enterprise Information Management

Coopamootoo, (2020)	PETs	Qualitative and quantitative analysis	Awareness, usability, usefulness, need for privacy, cost, trust, and social support are obstacles to using advanced PETs.
Harborth and Pape, (2020)	Tor*	Quantitative analysis	Trust increased behavioral intention, especially among privacy-conscious and privacy-literate users.
Kaaniche et al. (2020)	PETs	Literature review	Solutions should be user-centered and easy to use.
Skalkos et al. (2020)	Anonymity tools	Qualitative analysis	Participants value anonymity tools for freedom, personal privacy, economic prosperity, professional development, and fear-free living.
Zou et al. (2020)	Security, privacy, and identity theft protection practices	Quantitative analysis	Low value, inconvenience, and subjective judgment led to abandoning protection practices.
Alaqra et al. (2018)	Redactable signature*	Qualitative analysis	Technical users lacked trust in the validity of the doctor's signature.
D'Ambrosio et al. (2016)	mNoTrace*	Experiment	Ad and privacy-related filtering reduce battery consumption on phones.

Notes: * - Name of a PET

While PETs are intended to reduce data processing and give users agency over their privacy (Fischer-Hbner and Berthold, 2017), prior research consistently shows that users perceive advanced PETs as technically complex and difficult to navigate (Ashuri, 2024; Kaaniche et al., 2020; Sauer et al., 2024; Zou et al., 2020).

Trust dynamics

Trust is a psychological state characterized by the readiness to accept vulnerability in exchange for positive expectations of the trustee (Gefen *et al.*, 2008; Mayer *et al.*, 1995; McKnight *et al.*, 2002). Previous information system (IS) literature analyzed trust as a single concept (Lin *et al.*, 2021; Oliveira *et al.*, 2014) or incorporated multiple trust targets (Shao *et al.*, 2022; Söllner *et al.*, 2016). Kuen, Westmattelmann, et al. (2023) highlighted that trust in the provider and in the technology are distinct yet interdependent, yet Söllner et al. (2016) emphasized that multiple trust targets should be considered to better explain information system adoption. Therefore, we adapted a network-of-trust model to capture a more holistic view of trust dynamics (Söllner *et al.*, 2016).

Unlike institutional trust which reflects confidence in formal institutions such as governments or regulatory bodies, Söllner et al. (2016) identify distinct trust targets - the provider, the information system, the Internet, and the community of users. Table 2 presents the antecedents of trust targets in various contexts (online health, the sharing economy, e-commerce, and others).

Table 2. Antecedents of trust targets

Trust target	Antecedents	Source
Trust in the Internet	Community attributes (recommendations, social influence)	(Belanche *et al.*, 2014)
	Technology attributes (service quality)	(Belanche *et al.*, 2014)
Trust in the community	Community and technology attributes (recommendations, perceived interactivity)	(Awais Shakir Goraya *et al.*, 2019)

of Internet users	Situational factors (member credibility, voluntary anti-consumption)	(Lee and Cha, 2022; Shao *et al.*, 2022)
	Trust network factors (trust in the Internet, trust in technology)	(Lee and Cha, 2022; Söllner *et al.*, 2016)
Trust in the provider	Personal characteristic	(Kuen, Westmattelmann, *et al.*, 2023)
	Community attributes	(Gong *et al.*, 2019)
	Situational factors (structural assurance, voluntary anti-consumption)	(Lee and Cha, 2022; Shao *et al.*, 2022)
	Technology attributes (perceived usefulness, perceived ease of use)	(Mou *et al.*, 2017)
	Trust network factors (trust in technology, institutional trust)	(Kuen, Westmattelmann, *et al.*, 2023; Lee and Cha, 2022; Mou *et al.*, 2020; Shao *et al.*, 2022; Söllner *et al.*, 2016)
	Values (hedonic, utilitarian)	(Zhang *et al.*, 2024)
Trust in the information system	Community attributes (recommendations, social influence)	(Awais Shakir Goraya *et al.*, 2019)
	Recognition factors (familiarity, reputation)	(Hallem *et al.*, 2021; Kuen, Schürmann, *et al.*, 2023; Shao and Yin, 2019)
	Personal characteristics (disposition to trust)	(Kuen, Westmattelmann, *et al.*, 2023; Müller *et al.*, 2024)
	Risks (privacy risk, performance risk)	(Martínez-López *et al.*, 2021; Wang *et al.*, 2013)
	Situational factors (blockchain certificate, trust in physician)	(Kim *et al.*, 2020; Shao *et al.*, 2022; Zhai and Chen, 2023)
	Technology attributes (perceived usefulness, security, quality)	(Awais Shakir Goraya *et al.*, 2019; Habib *et al.*, 2020; Hua *et al.*, 2021; Lee *et al.*, 2018; Liu *et al.*, 2023; Lu *et al.*, 2021; Mao *et al.*, 2020; Müller *et al.*, 2024; Prakash and Das, 2020; Shao *et al.*, 2019; Shao and Yin, 2019; Sun *et al.*, 2022)
	Trust network factors (trust in technology, institutional trust)	(Cha and Lee, 2022; Kuen, Schürmann, *et al.*, 2023; Mao *et al.*, 2020; Söllner *et al.*, 2016)
	Value (hedonic, utilitarian, functional)	(Singh and Malik, 2024; Vongvit *et al.*, 2024; Wang, 2014)

Trust in the provider refers to the organization or entity behind the system and is influenced by personal characteristics, community and recognition factors, situational conditions, technology attributes, and trust network factors, ncluding trust in technology, members, and the Internet (Kuen, Westmattelmann, *et al.*, 2023; Lee and Cha, 2022). Trust in the information system refers to the perception that the system is reliable and performs as expected, with technology attributes and trust network factors being the most frequently examined antecedents, alongside personal characteristics, situational factors, and value (Singh and Malik, 2024; Wang *et al.*, 2024). Trust in the Internet reflects an individual's perception of the Internet as a reliable infrastructure and has received limited attention as a dependent variable, with social influence and service quality identified as its main antecedents (Belanche *et al.*, 2014; Mensah *et al.*, 2022). Trust in the community of internet users reflects confidence in other users' behavior while using the system. It is often shaped by community attributes. Situational factors, and trust network factors, including trust in the Internet and technology (Cha and Lee, 2022; Söllner *et al.*, 2016).

Studies have shown that trust drivers vary significantly across domains - what builds trust in e-commerce may differ from what works in e-health or e-banking (Kuen, Westmattelmann, *et al.*, 2023; Mou and Cohen, 2015). Hence, the roles of trust targets and their relationships are context-specific. Users may trust a well-known provider based

Journal of Enterprise Information Management

on its reputation but still distrust the underlying system's technical functionality due to concerns about identity theft or hacking (Ngwenyama *et al.*, 2023). In the PET adoption literature, trust is a recurring theme and is often cited as the most significant barrier to adoption (Coopamootoo, 2020; Harborth and Pape, 2020). While digital data wallets are framed as tools that enhance user control and security, trust in these wallets remains fragile.

Risk perceptions

Prior research shows that individuals evaluate technological benefits in relation to potential privacy, security, and financial risks (Alalwan *et al.*, 2016; Hanif *et al.*, 2022; Marriott and Williams, 2018). Perceived risks reduce users' willingness to accept and use technology across diverse user groups and situational contexts (Bohari *et al.*, 2025; Zhao and Khaliq, 2024). While some studies conceptualize perceived risk as an antecedent or mediator of technology use, several empirical studies indicate that risk conditions how performance-related and institutional attributes influence usage intention (Padma Kiran and Vedala, 2025; Sinha *et al.*, 2024). Building on this perspective, this research considers risks as a moderator that influences the impact of antecedents on trust formation. Identity theft and financial risks are considered the major risks that are associated with identity management technologies (Ngwenyama *et al.*, 2023). Consistent with previous literature (Hanif *et al.*, 2022; Marriott and Williams, 2018; Ngwenyama *et al.*, 2023), we operationalized risks along two salient dimensions: identity theft and financial loss.

PETs are often introduced in high-risk scenarios, where individuals seek protection from privacy violations (Zou *et al.*, 2020). Nevertheless, it is precisely in these contexts that perceived risk tends to suppress adoption. Risks related to identity theft and financial loss have been shown to significantly reduce trust in digital platforms (Martínez-López *et al.*, 2021; Wang *et al.*, 2024). While technological coupling (e.g., integrating PETs with biometric or mobile authentication) can reduce anxiety and enhance adoption (Lucier *et al.*, 2023). Hence, these solutions may heighten concerns by introducing unfamiliar security mechanisms, especially in decentralized architectures (Yan *et al.*, 2024).

3. Theoretical and methodological framework

Trust formation in digital data wallets is a multidimensional and context-dependent, making it difficult to capture through purely deductive or quantitative approaches. While prior research has acknowledged the importance of trust in the adoption of PETs (Coopamootoo, 2020; Ghaiumy Anaraky *et al.*, 2024; Harborth and Pape, 2020), it often overlooks the contextual characteristics of digital data wallets, particularly their decentralized architecture and associated risks perceptions (Ngwenyama *et al.*, 2023; Yan *et al.*, 2024). To address this complexity, we adopt sequential exploratory mixed-methods with a developmental purpose, integrating qualitative exploration with quantitative assessment (Creswell, 2014; Venkatesh *et al.*, 2023).

The qualitative phase addressed the limited understanding of trust formation in digital data wallets by identifying context-specific antecedents that reflect users' perceptions. We conducted 30 semi-structured interviews across Austria (Central Europe), Romania (Eastern Europe), and Spain (Western Europe). The countries were selected to capture variation in regional contexts and digital maturity within the European Union, as reflected in European Commission's Digital Decade, (2025) report. Theoretically, our study builds

Journal of Enterprise Information Management

on the network-of-trust model (Söllner *et al.*, 2016). Through inductive coding and thematic analysis, we identified four key antecedents: performance expectancy, transparency, social influence, and safety. Each antecedent was mapped to a specific trust target within the network model: trust in the information system, the Internet, the user community, and the provider (Söllner *et al.*, 2016). Thus, the qualitative phase identified context-specific antecedents, which were subsequently incorporated into the theoretical network-of-trust model and tested quantitatively.

The quantitative phase operationalized these antecedents in a survey completed by 1,200 respondents across the same three European countries. Using Partial Least Squares Structural Equation Modeling (PLS-SEM) analysis, we validated the influence of each antecedent on its respective trust target and tested the moderating effect of perceived risks on these relationships (Cheng *et al.*, 2021; Wang *et al.*, 2024). The qualitative findings informed construct development, survey design and structural model (Venkatesh et al., 2016; Appendix A – Table 10). Figure 1 summarizes the research process.

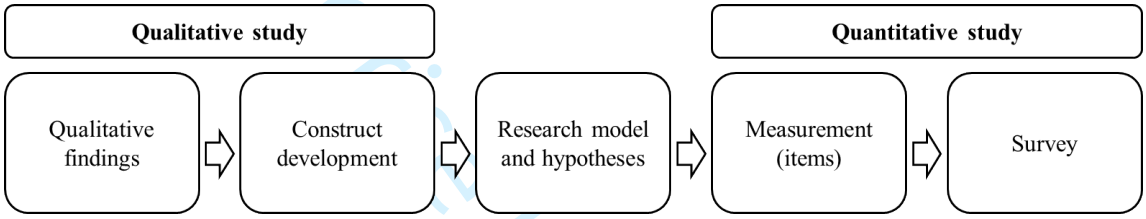

Figure 1. Research process

4. Qualitative phase

4.1 Context

Our literature review revealed that trust formation in digital platforms is highly context-dependent, with the salience and structure of trust targets shaped by the technological environment and user expectations (Kuen, Schürmann, *et al.*, 2023; Söllner *et al.*, 2016). Digital data wallets, a novel form of privacy-enhancing technology, leverage decentralized storage and user-controlled data permissions to give individuals greater agency over their digital identities (European Commission, 2023; SOTERIA, 2023). However, the adoption of such technologies remains low, in part due to their perceived complexity, limited usability, and concerns over security and transparency (Ashuri, 2024; Kaaniche *et al.*, 2020; Zou *et al.*, 2020).

Given the novelty of digital data wallets and the lack of research on how users form initial trust in them, we conducted a qualitative study to address the following research question: What are the antecedents of different trust targets in the context of digital data wallets? Specifically, we sought to identify user-defined antecedents of trust within the network-of-trust model (Söllner *et al.*, 2016), focusing on four primary trust targets: Trust in the Internet; Trust in the community of Internet users; Trust in the provider; Trust in the information system. This phase served as the foundation for developing the research model tested in the subsequent quantitative study.

4.2 Data collection

Journal of Enterprise Information Management

Journal of Enterprise Information Management

To ensure cultural and contextual diversity, 30 semi-structured interviews were conducted across three European countries—Austria (Central), Romania (Eastern), and Spain (Western Europe). Interviews were conducted in the participants' native languages—German, Romanian, and Spanish—to ensure depth, clarity, and comfort. All transcripts were professionally translated into English.

A purposive sampling strategy was used to maximize variation in age, gender, employment status, digital literacy, and nationality (Appendix B – Table 11). The participants were recruited through partner institutions and personal contacts. The inclusion criteria required participants to be at least 18 years old and to be residents of Austria, Romania, or Spain. Interviews ranged from 35 to 80 minutes and included a mix of open- and closed-ended questions (Appendix C). Three pilot interviews were conducted to refine the guide and ensure clarity of the questions. The final interviews began with general questions about digital privacy, then introduced digital data wallets, and concluded with targeted questions about trust perceptions, expectations, and concerns. Interviews were conducted until data saturation was reached, indicated by recurring conceptual patterns (Fusch and Ness, 2015). Saturation was assessed through ongoing preliminary coding and comparison of interviews, which revealed no substantial new themes in the later stages of data collection.

4.3 Qualitative data analysis

We employed an inductive open coding strategy to identify user-defined antecedents of trust, followed by axial and theoretical aggregation techniques to organize findings into a structured model (Miles, 1994). Two researchers conducted open coding of the interview transcripts. Differences in coding were discussed and resolved through consensus.

- **Open coding**: First-order codes were developed from direct statements across transcripts. These included concepts such as *"need for quick access"*, *"transparency about data usage"*, *"peer validation"*, and *"demand for security guarantees."*
- **Axial coding**: Related first-order codes were grouped into second-order categories, such as *task accomplishment*, *transparency mechanisms*, and *recommendations from important others*. This step allowed us to uncover patterns across interviews and cluster user sentiments into cohesive themes.
- **Theoretical aggregation**: These second-order codes were then synthesized into four overarching constructs: performance expectancy, importance of transparency, social influence, and safety. These constructs were systematically mapped to trust targets, drawing on established IS adoption theories, particularly the Unified Theory of Acceptance and Use of Technology (UTAUT) 2 (Venkatesh *et al.*, 2012) for performance expectancy and social influence, information privacy literature for transparency (Dinev *et al.*, 2013), and prior technology adoption for safety (Cheng et al., 2021; Yang et al., 2017). The coding structure, supporting quotes, and the full data structure are visualized in Table 3.

Table 3. First order, second order, and aggregate constructs

First-Order Select Interview Quotes	Interviewee(s)	Second-Order Construct	Aggregate Construct (Trust Antecedent)

"What matters to me is how quickly I can complete the task. If it's a simple document or verification, I shouldn't need to go through layers of steps." "I'm used to platforms that work immediately. If the wallet is slow, I'd think twice about trusting it with my data."	# 7	Perceived Responsiveness and Speed	
"Being able to see all the data that's stored about me, and delete it if I want to, is non-negotiable." "If I'm using a digital wallet, I need smart tools to manage what I share, not just basic settings hidden in menus."	#3	Task-Oriented Privacy Control	Performance Expectancy
"If it's just another app on my phone, I'll probably ignore it. But if it really adds value, I need to see that upfront." "I'd expect it to replace several apps or processes. If it can do that, then it's clearly useful." "Such a tool is more useful. If I were to use it, the factors that would influence its use would determine its utility."	#11	Functional Usefulness and Relevance	
"I'd feel more confident if I knew experts could examine how the wallet works—open source makes that possible." "To be able to trust, I want to understand how my data is used and stored."	# 2, #27	Mechanisms for Data Handling Transparency	
"It should be standard to get a clear explanation—who's collecting, for what purpose, and where it's going. Right now, it's all hidden behind layers of legal jargon." "I feel forced to agree. Most websites won't even let you browse unless you click 'accept all.' That's not real consent."	# 3, 16	Transparency about External Data Practices	Importance of Transparency
"Usually, I go by recommendations from people close to me. If they're on board, I'm more likely to follow." "Sometimes I'm not sure about a tech tool, but if enough people around me are using it, that gives me confidence." "If my friends or parents told me it was very good, I would use it."	# 24	Social Proof from Close Network	
"The experiences of other users give me a sense of whether the technology is actually trustworthy." "Before using anything new, I always check what others have said. Reviews help me decide if it's worth my time." "I'd consider using it if other people had positive experiences with it."	# 14, 8	Crowdsourced User Validation	Social Influence
"I only use platforms that have a strong track record when it comes to safety. That matters more than convenience." "Certainly, it should be a safe one, because otherwise it would make no sense. It should have some security guarantees."	# 17, 25	Provider Trust Guarantees	
"Centralized platforms are targets. If this gets hacked, my entire identity could be at risk." "What if someone gains access without my consent? That's what makes me hesitate." If	# 9, 30	Cybersecurity Risk Awareness	Safety

Journal of Enterprise Information Management

this platform had all the data, it would be a target for hackers... It's convenient, but also dangerous."

4.4 Identified constructs and trust targets

Performance expectancy → Trust in the information system
Performance expectancy refers to the perceived usefulness and efficiency of digital data wallets in enhancing users' digital productivity (Venkatesh *et al.*, 2003). Participants emphasized task facilitation, speed, and data control.

> "Such a tool is more useful. If I were to use it, the factors that would influence its use would determine its utility" (Interviewee 11).
> "You can always go on the platform and take it fast—it doesn't take as long as always searching for things on your phone" (Interviewee 7).

These perceptions align with the literature, which shows that performance expectancy significantly predicts both adoption and trust in digital systems (Jacob *et al.*, 2023; Kajol *et al.*, 2022).

Transparency → Trust in the Internet
Transparency emerged as a core concern. Participants expressed skepticism about current online privacy practices and demanded clear data usage disclosures from any new system.

> "To be able to trust, I want to understand how my data is used and stored" (Interviewee 27).
> "Even though we have GDPR, it's still very unclear what is happening with your data" (Interviewee 3).

Such expectations mirror prior findings that transparency mechanisms enhance perceived safety in online environments (Esmaeilzadeh, 2020; Mayr *et al.*, 2024).

Social influence → Trust in the community of internet users
Participants highlighted the value of peer recommendations in mitigating uncertainty, particularly in adopting unfamiliar technologies.

> "If my friends or parents told me it was very good, I would use it" (Interviewee 24).
> "I'd consider using it if other people had positive experiences with it" (Interviewee 14).

This pattern of responses aligns with findings from Venkatesh et al. (2012) and Zhang et al. (2020), which indicate that social influence is a strong predictor of trust in peer-based digital environments.

Safety → Trust in the provider
Security concerns were prevalent. Participants sought clear assurances from providers that their personal data would be safe from misuse or breaches.

> "If this platform had all the data, they would be a target for hackers... It's convenient, but also dangerous" (Interviewee 9).

Journal of Enterprise Information Management

Journal of Enterprise Information Management

> "Certainly, it should be a safe one, because otherwise it would make no sense. It should have some security guarantees" (Interviewee 17).

These insights reinforce the central role of perceived safety in trust-building, particularly for high-risk technologies (Cheng *et al.*, 2021; Kuen, Westmattelmann, *et al.*, 2023).

5. Research model

A research model is build based on the network-of-trust framework (Söllner *et al.*, 2016). Recognizing the context-specific nature of trust targets and their antecedents, we first conducted a qualitative study to identify relevant antecedents and then validated the model quantitatively. Additionally, we considered perceived risks—specifically financial loss and identity theft—as moderating variables that shape the influence of these antecedents on trust targets. Figure 2 depicts the research model.

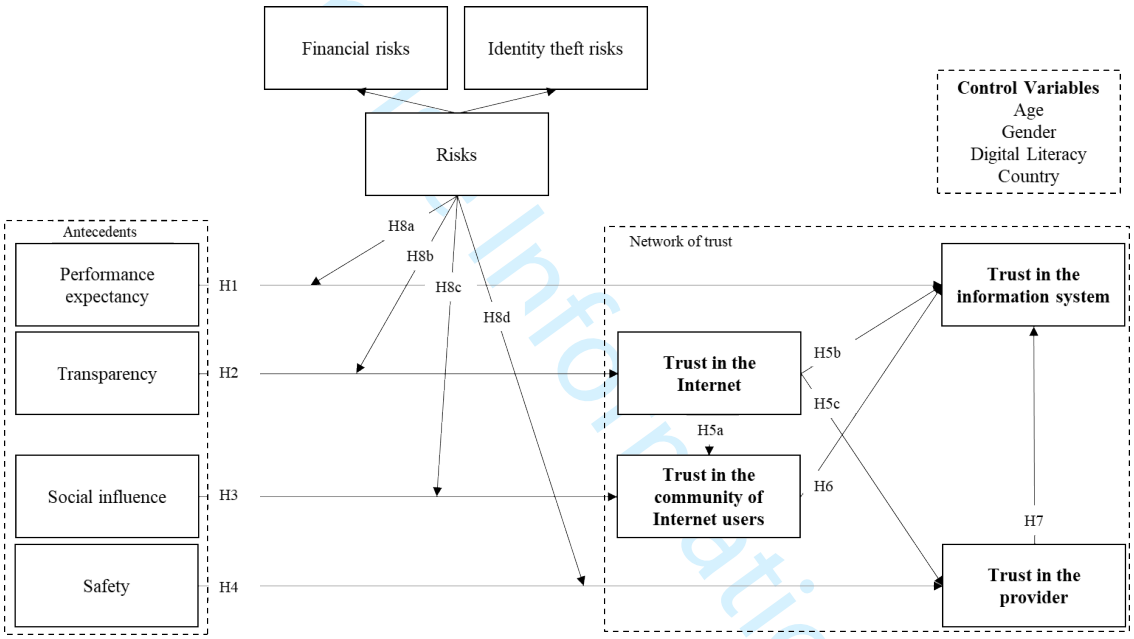

Figure 2. The research model

Performance expectancy → Trust in the information system

Performance expectancy has a positive effect on the acceptance of various technologies (Jacob *et al.*, 2023; Kajol *et al.*, 2022). Users who perceive a system as useful, efficient, and supportive of privacy control report higher trust in the information system. Participants emphasized the value of usefulness, speed, and control over personal data in fostering trust. One participant shared, "Such a tool is more useful. If I were to use it, the factors that would influence its use would determine its utility" (Interviewee 11). In the case of digital data wallets, performance expectancy could directly signal the system's capability to execute privacy-related functions, thereby contributing to trust in the information system. Hence, digital data wallets need to clearly demonstrate key performance attributes, in terms of productivity, privacy management, and usefulness.

> **H1**: Performance expectancy positively influences trust in the information system.

Transparency → Trust in the Internet

Transparency involves informing users about what data is collected and how it is processed (Dinev *et al.*, 2013). Previous literature suggests that transparency is positively associated with trust (Esmaeilzadeh, 2020; Mayr *et al.*, 2024). Participants linked transparency directly to trust, stating that they feel safer and more confident when data handling is clear. One participant noted, "To be able to trust, I want to understand how my data is used and stored." (Interviewee 27). According to the network-of-trust model, trust developed toward a specific digital service can extend beyond the focal technology to the broader technological environment in which it operates. When users perceive transparent data practices in a digital data wallet, they may infer that digital interactions within the online ecosystem are more predictable and trustworthy, strengthening trust in the Internet.

H2: Transparency positively influences trust in the Internet.

Social influence → Trust in the community of Internet users

Social influence is a significant factor in explaining both initial trust formation and technology adoption (Venkatesh *et al.*, 2012; Zhang *et al.*, 2020). Many participants reported relying on feedback and experiences from their social circle. For example, one participant said, "I think I would consider if other people use it or if they had a previous experience with it." (Interviewee 14). Such endorsements serve as trusted recommendations that develop confidence in other users. Although social influence originates from close referents, in situations of high uncertainty, users generalize these trusted opinions to infer the reliability of other users. Since digital data wallets are new technologies, recommendations from a close social circle can provide social cues that other users also perceive the technology as trustworthy, fostering broader users' recommendations.

H3: Social influence positively influences trust in the community of Internet users.

Safety → Trust in the provider

Safety is often considered a priority by users (Cheng, Su, et al., 2021). Safety concerns were strongly emphasized, with participants highlighting the importance of data protection and security guarantees. One user shared: "If this platform had all the data, it would be a target for hackers… the platforms are very convenient, but also very dangerous" (Interviewee 9). Users are more likely to trust providers who prioritize and communicate robust safety measures. Since digital data wallets include sensitive personal information, users associate the effectiveness of safety measures with providers' responsibility. Hence, if digital data wallet providers enable safe sharing and offer robust safety measures, users' trust in the provider will grow.

H4: Safety positively influences trust in the provider.

Interrelationships among trust targets

As posited in the network-of-trust model, trust in one domain often reinforces trust in others. Trust in the Internet has a positive effect on users' belief in the reliability of other users, the system, and the provider. Similarly, trusting the community positively influence trust in the provider, and trusting the provider positively influence trust in the system

Journal of Enterprise Information Management

Journal of Enterprise Information Management

(Söllner *et al.*, 2016). We argue that in the context of digital data wallets, trust in one domain will positively influence trust in others.

H5a: Trust in the Internet positively influences trust in the community of Internet users.
H5b: Trust in the Internet positively influences trust in the information system.
H5c: Trust in the Internet positively influences trust in the provider.
H6: Trust in the community of Internet users positively influences trust in the provider.
H7: Trust in the provider positively influences trust in the information system.

The moderating role of risk

Risks are potential negative outcomes arising from another party's actions that may lead to losses (Fox and James, 2021). Identity theft and financial risks are the major risks associated with identity management technologies (Ngwenyama *et al.*, 2023). Hence, it is argued that perceived risks—particularly concerns about identity theft and financial loss—moderate the strength of the relationships between antecedents and trust targets. If potential users consider digital data wallets too risky for privacy management, the expectation that the technology could improve productivity will be less relevant. Also, with high-risk perceptions, users may consider safety guarantees and transparency mechanisms insufficient to form trust in the provider and trust in the Internet. On the contrary, for users with high-risk perceptions, suggestions from important others could be an important factor in building trust in the Internet users' community.

H8a: Risks moderate the relationship between performance expectancy and trust in the information system, such that the relationship is weaker among users with high risk perceptions.
H8b: Risks moderate the relationship between transparency and trust in the Internet, such that the relationship is weaker among users with high risk perceptions.
H8c: Risks moderate the relationship between social influence and trust in the community of Internet users, such that the relationship is stronger among users with high risk perceptions.
H8d: Risks moderate the relationship between safety and trust in the provider, such that the relationship is weaker among users with high risk perceptions.

6. Quantitative phase

A quantitative study assessed the research model by examining the effects of antecedents on trust targets and the moderating role of risks.

An online questionnaire was designed to collect data, with constructs adapted to the study's context (Appendix D – Table 12). Items were measured on a 7-point numerical scale (1 = strongly disagree, 7 = strongly agree). The survey was administered in Austria, Romania, and Spain. The questionnaire was developed in English, translated into German, Romanian, and Spanish, and back-translated to ensure equivalence. A pilot test was conducted to ensure item clarity.

Participants were recruited through a professional marketing company to ensure a diverse and representative sample in Austria, Romania, and Spain. The company invited respondents who met age- and gender-based quotas in each country, resulting in 1,200 valid responses. A Chi-squared test confirmed that there were no significant differences between the sample and population distributions for age and gender (Appendix E – Table 13). Sample characteristics are presented in Table 4.

Table 4. Sample characteristics

Sample characteristics		Descriptive statistics
Gender	Female	50.9%
	Male	49.1%
Age	18-24	9.0%
	25-47	42.2%
	48-64	25.5%
	65+	23.3%
Occupation	Student	5.3%
	Employed	49.3%
	Self-employed	9.8%
	Unemployed / Retired	35.7%
Education	No school degree	0.1%
	Primary school	2.9%
	High school	25.7%
	Apprenticeship	25.2%
	Bachelor's degree	32.5%
	Master's degree	11.4%
	Doctoral Degree	2.3%

To reduce a common method bias, the questionnaire incorporated several procedural remedies, including respondent anonymity, psychological separation through distinct sections, and improved item design with clear wording. Furthermore, Harman's one-factor test was conducted to assess common method bias, with no indicator explaining more than 50% of the variance. Additionally, a marker variable test was conducted, producing a maximum shared variance of 0.025 (2.5%) (Lindell and Whitney, 2001), indicating no significant bias.

6.1 Measurement model

The partial least squares structural equation modeling method (PLS-SEM) was used to assess the research model, enabling us to test a new complex model with both reflective and formative constructs, and does not require strong distributional assumptions (Fornell and Bookstein, 1982). Following the network-of trust model, the four trust targets are formative constructs because each target is formed by a unique combination of beliefs specific to that referent (Internet, community of users, provider, and information system) rather than being a reflection of a single general trust factor. The antecedents and risks are reflective because the constructs are represented by the observed indicators. SmartPLS 4 was used to perform the analysis (Ringle *et al.*, 2022). First, the measurement model was assessed, followed by the structural model (Anderson and Gerbing, 1988).

Reflective constructs demonstrated composite reliability (CR) above 0.7 and average variance extracted (AVE) above 0.5, confirming reliability and convergent validity (Hair *et al.*, 2011). Discriminant validity was assessed using the Fornell-Larcker criterion (Fornell and Larcker, 1981), cross-loadings (Chin, 1998), and Heterotrait-Monotrait Ratio (HTMT) (Henseler *et al.*, 2015), with all criteria met: AVE square roots exceeded

Journal of Enterprise Information Management

inter-construct correlations, loadings surpassed cross-loadings (Appendix F – Table 14), and HTMT values were below 0.9 (Appendix F – Table 15). Table 5 presents the means, standard deviations, AVE, CR, Cronbach's alpha (CA), and the Fornell-Larcker criterion.

Table 5. Means, standard deviations, AVE, CR, CA, and the Fornell-Larcker criterion

	Mean	Std	AVE	CR	CA	PE	T	SI	Saf	FR	ITR
PE	4.60	1.73	0.87	0.95	0.95	**0.93**					
T	5.59	1.45	0.90	0.94	0.95	0.24***	**0.95**				
SI	3.73	1.88	0.93	0.96	0.96	0.71***	0.09**	**0.96**			
Saf	3.90	1.70	0.86	0.92	0.92	0.63***	0.09**	0.65***	**0.93**		
FR	4.04	1.52	0.81	0.89	0.89	-0.19***	0.06*	-0.12***	-0.21***	**0.90**	
ITR	4.28	1.64	0.89	0.94	0.94	-0.21***	0.09**	-0.17***	-0.28***	0.76***	**0.94**

Notes: *p<0.05, **p<0.01, ***p<0.001, PE – performance expectancy, T – transparency, SI – social influence, Saf – safety, FR – financial risks, ITR - identity theft risks

For the formative constructs, indicator multicollinearity, and the statistical significance and relevance of the outer weights were assessed (Becker *et al.*, 2012; Hair *et al.*, 2011). Table 6 presents variance inflation factors (VIFs), weights, and loadings. The VIFs are lower than 5, indicating no collinearity issues (Lee and Xia, 2010). Additionally, all items show statistically significant weights and loadings.

Table 6. Measurement model evaluation for formative constructs

	VIF	Weights	Loadings
TIn1	3.12	0.62***	0.97***
TIn2	3.12	0.43***	0.94***
TCIU1	2.70	0.43***	0.93***
TCIU2	2.99	0.32***	0.90***
TCIU3	3.30	0.34***	0.92***
TP1	2.60	0.24***	0.86***
TP2	4.15	0.34***	0.94***
TP3	3.41	0.50***	0.95***
TIS1	3.01	0.57***	0.96***
TIS2	2.40	0.27***	0.87***
TIS3	2.25	0.25***	0.85***

Notes: TIn - trust in the Internet, TCIU - trust in the community of Internet users, TP - trust in the provider, TIS - trust in the information system, *p<0.05, **p<0.01, ***p<0.001.

The standardized root mean square residual (SRMR) was used to assess model fit, yielding 0.086, indicating acceptable fit (Hu and Bentler, 1998; "Model Fit", 2026). The measurement model is considered adequate for subsequent structural model analysis.

6.2 Structural model

Multicollinearity was assessed, with all VIFs below 5, confirming no issues (Hair *et al.*, 2011). The structural model was evaluated using bootstrapping with 5,000 iterations. The model explained 31.6% of the variance in trust in the Internet, 56.1% in trust in the community of Internet users, 59.0% in trust in the provider, and 77.6% in trust in the information system. Figure 3 presents the structural model results.

Journal of Enterprise Information Management

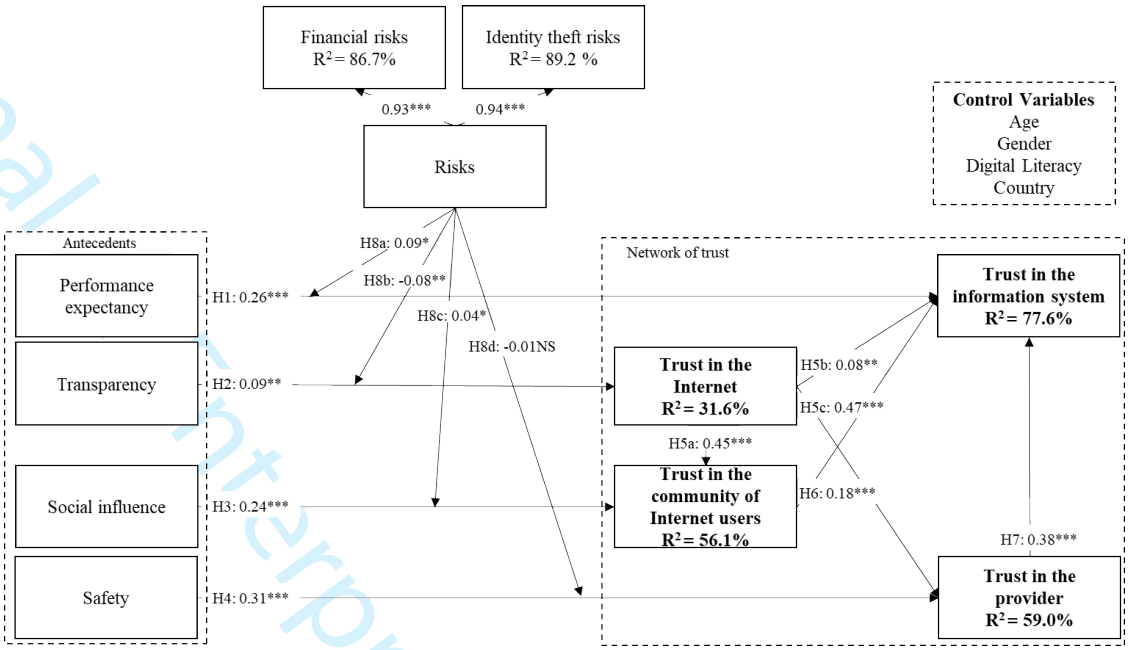

Figure 3. Structural model (*p<0.05, **p<0.01, ***p<0.001)

All antecedents significantly influenced their respective trust targets: performance expectancy positively affected trust in the information system (β=0.26, p<0.001), transparency positively affected trust in the Internet (β=0.09, p<0.01), social influence positively affected trust in the community of Internet users (β=0.24, p<0.001), and safety positively affected trust in the provider (β=0.31, p<0.001), supporting H1–H4. The network-of-trust model was also supported: trust in the Internet positively influenced trust in the community of Internet users (β=0.45, p<0.001), trust in the information system (β=0.08, p<0.01), and trust in the provider (β=0.47, p<0.001), supporting H5a–H5c. Trust in the community of Internet users (β=0.18, p<0.001) and trust in the provider (β=0.38, p<0.001) positively influenced trust in the information system, supporting H6 and H7. Risks moderated the relationships between performance expectancy and trust in the information system (β=0.09, p<0.05), transparency and trust in the Internet (β=-0.08, p<0.01), and social influence and trust in the community of Internet users (β=0.04, p<0.05), supporting H8a–H8c, but not H8d (β=-0.01, p>0.05).

As for control variables, Trust in the community of Internet users is lower (β = -0.06, p < 0.01) and Trust in the provider is higher (β = 0.04, p < 0.05) among older users. Trust in the community of Internet users (β = −0.14, p < 0.01) and trust in the provider (β = −0.18, p < 0.001) are lower among females. Digital literacy positively influences all trust targets, specifically Trust in the Internet (β=0.37, p<0.001), Trust in the community of Internet users (β=0.18, p<0.001), Trust in the provider (β=0.14, p<0.001), and Trust in the information system (β=0.13, p<0.001). Compared to Spain, trust in the provider is higher in Austria (β = 0.23, p < 0.01) and Romania (β = 0.08, p < 0.05). Also, trust in the information system is higher (β = 0.10, p < 0.01), and trust in the Internet is lower in Austria (β = -0.43, p < 0.001). Table 7 presents the results.

Table 7. Results of the research model

Hypotheses	β	95% CI
H1: PE → TIS	0.26***	[0.20, 0.32]
H2: T → TIn	0.09**	[0.03, 0.15]
H3: SI → TCIU	0.24***	[0.18, 0.29]

Journal of Enterprise Information Management

H4: Saf → TP	0.31***	[0.26, 0.38]
H5a: TIn → TCIU	0.45***	[0.38, 0.51]
H5b: TIn → TIS	0.08**	[0.02, 0.15]
H5c: TIn → TP	0.47***	[0.39, 0.54]
H6: TCIU → TIS	0.18***	[0.12, 0.25]
H7: TP →TIS	0.38***	[0.30, 0.45]
H8a: Risks x PE → TIS	0.09*	[0.002, 0.06]
H8b: Risks x T → TIn	-0.08**	[-0.14, -0.02]
H8c: Risks x SI → TCIU	0.04*	[0.001, 0.07]
H8d: Risks x Saf → TP	-0.01NS	[-0.04, 0.03]
Control variables		
Age → TIn	-0.01NS	[-0.06, 0.04]
Age → TCIU	-0.06**	[-0.10, -0.02]
Age → TP	0.04*	[0.004, 0.08]
Age → TIS	0.021NS	[-0.01, 0.05]
Gender → TIn	0.04NS	[-0.06, 0.13]
Gender → TCIU	-0.14**	[-0.22, -0.66]
Gender → TP	-0.18***	[-0.25, -0.10]
Gender → TIS	-0.01NS	[-0.06, 0.05]
DL → TIn	0.37***	[0.31, 0.43]
DL → TCIU	0.18***	[0.12, 0.24]
DL → TP	0.14***	[0.09, 0.20]
DL → TIS	0.13***	[0.09, 0.18]
Austria → TIn	-0.43***	[-0.54, -0.31]
Austria → TCIU	-0.03NS	[-0.13, 0.08]
Austria → TP	0.23**	[0.04, 0.33]
Austria → TIS	0.10**	[0.03, 0.17]
Romania → TIn	0.00NS	[-0.12, 0.11]
Romania → TCIU	-0.04NS	[-0.05, 0.13]
Romania → TP	0.08*	[0.01, 0.17]
Romania → TIS	0.02NS	[-0.04, 0.08]

Notes: PE – performance expectancy, T – transparency, SI – social influence, Saf – safety, TIn - trust in the Internet, TCIU - trust in the community of Internet users, TP - trust in the provider, TIS - trust in the information system, DL – digital literacy, NS – not significant *p<0.05, **p<0.01, ***p<0.001

To assess the model's predictive relevance, Q^2 values were calculated for each endogenous variable (Hair *et al.*, 2011), presented in Table 8. All Q^2 values are greater than 0, indicating that the model has predictive relevance. Appendix G presents the results of the robustness analysis. Overall, the results indicate that the main findings are robust to non-linearity, endogeneity bias, and unobserved heterogeneity.

Table 8. Q^2 values for endogenous variables

Constructs	Q^2
Identity theft risks	0.89
Financial risks	0.87
Trust in the information system	0.77
Trust in the provider	0.58
Trust in the community of Internet users	0.54
Trust in the Internet	0.29

Moderation effects were analyzed at one standard deviation above and below the mean, shown in Figure 4. Contrary to expectations, performance expectancy had a stronger effect on trust in the information system among users with high-risk perceptions. This finding suggests that perceived risk does not necessarily diminish the importance of performance expectancy. Instead, in the context of digital data wallets, expected functional effectiveness may remain an important consideration of trust even when users

Journal of Enterprise Information Management

perceive higher levels of risk. Transparency's effect on trust in the Internet was stronger among users with low-risk perceptions, suggesting that transparency alone may not be sufficient for high-risk users. Social influence had a stronger effect on trust in the community of Internet users among high-risk users, highlighting the role of social recommendations.

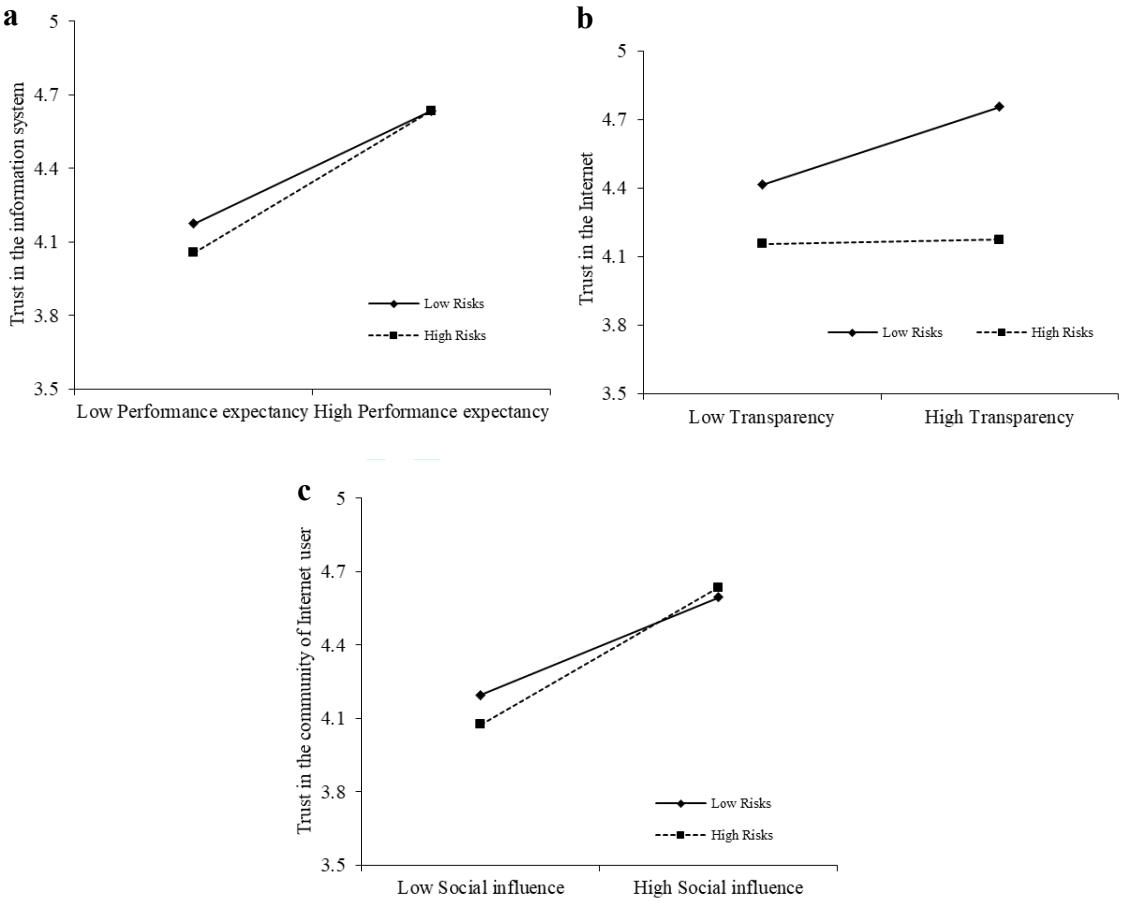

Figure 4. (a): Effects of risks and performance expectancy on trust in the information system; (b): Effects of risks and transparency on trust in the Internet; (c): Effects of risks and social influence on trust in the community of Internet users

6.3 Interpretations

This study examines trust formation and the role of risks in digital data wallets, within the European context, where digital data wallets are emerging under the eIDAS 2.0 regulation and GDPR, supported by relatively mature institutional mechanisms. Using a mixed-methods approach and drawing on the network-of-trust model, four antecedents were examined in terms of their impact on trust targets, as well as the moderating role of risks.

All antecedents had significant positive effect on their respective trust targets. Performance expectancy positively influences trust in the information system. It makes users more confident that digital data wallets will perform reliably and support their tasks. Transparency has a positive effect on trust in the Internet, although the effect was relatively small ($\beta = 0.09$, $p < 0.01$). Hence, transparency alone is a necessary but

insufficient condition for building trust in the Internet, and other factors, such as institutional assurances, also need to be considered. Social influence positively influences trust in the community of Internet users. Consequently, recommendations from friends, family, or close peers foster users' trust in the broader community of Internet users. Safety strengthened trust in the provider. Safety reassures users that the data is protected and handled securely, increasing trust in the provider. The applicability of the network-of-trust model was extended, with significant relationships among trust targets: trust in the Internet positively influenced other trust targets, and trust in the community of Internet users and the provider positively influence trust in the information system.

Risks (financial and identity theft) moderated key relationships. Overall, the modest moderation effects suggest that perceived risks act as a contextual influence rather than a dominant driver of trust formation, while influencing some relationships while leaving others. Performance expectancy and social influence had stronger effects on trust among high-risk users, suggesting that digital data wallets are perceived as privacy-enhancing tools and that social recommendations are critical for them. Conversely, transparency's effect on trust in the Internet was weaker among high-risk users, indicating that transparency alone is insufficient for building trust in high-risk contexts. Additionally, risks do not weaken the relationship between safety and trust in the provider. Users generally expect providers to ensure adequate security and data protection as basic conditions for using digital data wallets. Table 9 presents the meta-inferences.

Table 9. Qualitative Inferences, quantitative Inferences, and meta-inferences

Constructs	Qualitative inference	Quantitative inference	Meta-inference	Explanation
Performance expectancy	Digital data wallets' productivity is positively related to trust in the information system.	Consistent with qualitative findings.	Effective performance attributes of digital data wallets advance trust in the information system, enhancing privacy management.	Aligns with prior research (Hua *et al.*, 2021; Sun *et al.*, 2022), significantly increasing trust in the information system of digital data wallets.
Transparency	Transparency mechanisms have a positive effect on trust in the Internet.	Consistent with qualitative findings.	Transparent digital data wallets make the digital environment safer, fostering trust in the Internet.	Consistent with literature (Esmaeilzadeh, 2020; Mayr *et al.*, 2024), positively related to trust in the Internet.
Social influence	Recommendations from a close social circle have a positive effect on trust in the community of Internet users.	Consistent with qualitative findings.	Recommendations from close social circles are more reliable, increasing trust in the community of Internet users.	Supports trust formation and technology adoption (Venkatesh et al., 2012; Zhang et al., 2020), increasing trust in the community of Internet users.
Safety	Clear security measures positively influence trust in the provider.	Consistent with qualitative findings.	Safety guarantees in digital data wallets positively influence trust in the provider.	User priority (Cheng, Su, et al., 2021), strengthen trust in the provider of digital data wallets.
Trust in the Internet	-	Positively influence trust in the	Following the network-	Extended by identifying antecedents for each

Journal of Enterprise Information Management

		community, information system, and provider.	of-trust model (Söllner *et al.*, 2016), when individuals trust in the Internet, they also tend to trust in the community of Internet users, trust in the information system, and trust in the provider. Also, users who trust in the community of Internet users tend to trust in the provider. Users' trust in the provider has a positive effect on their trust in the information system.	trust target in digital data wallet adoption.
Trust in the community of Internet users	-	Positively influence trust in the provider.		
Trust in the provider	-	Positively influence trust in the information system.		
Risks	-	Moderates relationships between antecedents and trust targets.	Risks strengthen performance expectancy and social influence effects, but weaken transparency's effect on trust in the Internet.	Context-specific factor (Kuen, Schürmann, *et al.*, 2023; Lee and Turban, 2001), strengthening performance expectancy and social influence on trust, but weakening transparency's impact on trust in the Internet.

7. Discussion

7.1 Theoretical contributions

This study makes three theoretical contributions.

Advancing research on trust formation in privacy-enhancing technologies

The study empirically examines trust formation in digital data wallets—a novel class of PETs that enable decentralized personal data management (European Commission, 2023; SOTERIA, 2023). Drawing on the network-of-trust model (Söllner *et al.*, 2016), we identify four key antecedents: performance expectancy, transparency, social influence, and safety. Each maps onto a distinct trust target: the information system, the Internet, the community of Internet users, and the provider, respectively. Our findings indicate that each antecedent have a positive and significant effect on its corresponding trust target, resulting in a granular, empirically validated trust model tailored to digital data wallets. This work contributes to addressing a notable gap in IS research, namely the limited examination of PET adoption at the individual level (Coopamootoo, 2020; Ghaiumy Anaraky *et al.*, 2024; Harborth and Pape, 2020). This study contextualizes and reconfigures antecedents derived from a qualitative study and prior literature within digital data wallets, by extending the empirical account of how trust forms across multiple trust targets in this previously unexamined setting.

Journal of Enterprise Information Management

Extending the applicability of the network-of-trust model for decentralized infrastructures

We extend the applicability of the network-of-trust model to decentralized identity ecosystems. The findings show that trust targets are both context-specific and interdependent. Trust in the internet positively influence trust in the information system, provider, and community; trust in the provider strengthens trust in the system; and trust in the community has a positive effect on trust in the provider (Kuen, Westmattelmann, *et al.*, 2023; Söllner *et al.*, 2016). This layered interconnection demonstrates the applicability of the trust model to the context of digital data wallets and provides insights into trust formation in emerging digital ecosystems. Furthermore, different antecedents influence specific trust targets: performance expectancy has a positive effect on trust in the system, transparency is positively associated with trust in the Internet, social influence is positively related to trust in the user community, and safety positively influence trust in the provider. These results underscore the need for trust models that capture the differentiated nature of trust pathways in decentralized infrastructures.

Reconceptualizing risk as a contextual moderator

This study reconceptualizes perceived risk as a contextual moderator of trust formation rather than merely a barrier. Identity theft and financial risk—two common concerns in the adoption of decentralized technologies—shape how individuals evaluate trust antecedents (Ngwenyama *et al.*, 2023; Yan *et al.*, 2024). The modest and selective moderation effects indicate that perceived risk does not uniformly shape trust formation. Instead, it acts as contextual condition that strengthens or weakens specific trust mechanisms depending on the nature of the antecedent. High-risk perceptions strengthen the effect of performance expectancy on trust in the system and the importance of social influence on trust in the community of internet users. Privacy-conscious users are more likely to see digital data wallets as protective tools and to rely on peer recommendations (Lucier et al., 2023). Hence, users with high-risk perception appear to evaluate whether the digital data wallet, as a system, provides sufficient utility, such as enhanced privacy controls, to offset perceived threats. Similarly, social influence became more important under high perceived risk, indicating that users rely on more peer recommendations and collective experiences to reduce uncertainty and strengthen trust in the community of Internet users. Conversely, high risk dampens the effect of transparency on trust in the Internet, suggesting that openness alone may be insufficient for highly risk-averse users (Martínez-López *et al.*, 2021; Wang *et al.*, 2024). Hence, transparency alone may be insufficient to alleviate high-risk concerns. Highly risk-averse users may prioritize tangible protections, for example, safety features and recommendations. Additionally, risk does not influence the effect of safety on trust in the provider, indicating that security and data protection remain a key determinant of trust even when risk perceptions are high.

7.2 Practical contributions

Our study demonstrates that trust in digital data wallets is multifaceted, spanning four distinct targets: the information system, the Internet, the provider, and the user community. Each is driven by a specific antecedent—performance expectancy, transparency, safety, and social influence—requiring tailored strategies. Performance expectancy positively influence trust in digital data wallets, especially for high-risk users. Providers should prioritize features that deliver clear functional value, such as selective data sharing, automated identity verification, and interoperability with eIDAS-compliant public and private services. Transparency had a small effect on trust in the Internet and

Journal of Enterprise Information Management

Journal of Enterprise Information Management

weakened under high-risk perceptions. Hence, transparency is important, but not sufficient to build trust in the Internet. Nevertheless, even small improvements in transparency can still contribute meaningfully when implemented consistently. Providers should embed transparency through regular independent audits, GDPR and eIDAS compliance certifications, and public reporting of data processing activities. Social influence strengthens trust in the community of Internet users, especially among high-risk individuals. Community trust grows through peer validation. Hence, providers may collaborate with trusted intermediaries, such as universities, reputable organizations, and professional associations. Safety predicts trust in the provider and remains stable across risk levels. Hence, providers should guarantee safety through certified encryption, regular testing, and hardware-backed key management.

Extending the network-of-trust model, we show that trust targets are interdependent: trust in one domain (e.g., the Internet) reinforces trust in others (e.g., the provider or system). A coherent trust ecosystem requires unified governance frameworks, interoperable protocols (e.g. OpenID for Verifiable Credentials), and aligned privacy policies across all touchpoints. Unified branding, interoperable protocols, and aligned privacy policies support seamless user experiences and sustained trust across decentralized environments.

We also reframe perceived risk as a contextual moderator. Although the moderating effects are modest, their consistent significance indicates meaningful boundary conditions for trust formation under risk. High-risk perceptions heighten the importance of performance and social validation but weaken transparency. Hence, in high-risk sensitive contexts such as identity data management or financial data exchange, providers should emphasize functional benefits, peer endorsements, real-time audit trails, and customizable security settings. Transparency mechanisms should be paired with tangible reassurances, such as real-time alerts and verified certifications.

As for demographic variables, older users tend to rely on institutional providers rather than online communities, suggesting that trust-building efforts for this group should emphasize regulatory compliance and long-term service stability. Female users report lower trust in both providers and the internet community, indicating the need for stronger user control mechanisms, transparent compliance, and explicit safeguards against data misuse. Digital literacy has a significant effect on trust across all target groups, underscoring the importance of accessible onboarding, step-by-step tutorials, and user support. Additionally, cross-country differences imply that providers should adapt their governance and communication strategies to national regulatory cultures rather than rely on a single approach. For instance, in Spain, policymakers and providers should strengthen institutional assurances to effect on trust in the provider. In Austria, greater emphasis should be placed on reinforcing safety and transparency mechanisms to address lower trust in the Internet.

8. Limitations and future research

First, we focused on initial trust formation, using a cross-sectional design. User behaviors may evolve over time. Future longitudinal research could examine how trust develops and the identified relationships change with continued use. Second, the sample was restricted to three European countries, Austria, Romania, and Spain, which, despite EU diversity, share a relatively similar regulatory context. Future studies should expand to

non-EU contexts to examine cultural and institutional effects. Third, additional technology features, such as anonymity, granularity of privacy control, and data portability, may further influence trust formation. Finaly, the study adopts user-level perspective. Future research could examine broader organizational factors, such as organizational data governance or enterprise digital infrastructure design.

9. Conclusions

This study provides the empirical investigations into trust formation in digital data wallets—an emerging class of PETs—by integrating qualitative and quantitative data within a network-of-trust model. We identified four key antecedents of trust—performance expectancy, transparency, social influence, and safety—each linked to a specific trust target. We demonstrated that perceived risks (e.g., identity theft and financial loss) moderate these relationships. The integration of qualitative and quantitative methods strengthened the reliability of our findings. By identifying antecedents grounded in real user concerns and empirically validating them, this study offers both theoretical advancements and practical insights. Key performance attributes were found to drive trust in the system; transparency mechanisms have a positive effect on trust in the Internet; social influence positively influence trust in the user community; and safety assurances have a positive effect on trust in the provider. Interestingly, risk perceptions strengthen the effects of performance expectancy and social influence but weaken the effect of transparency, suggesting that trust-building strategies must be adapted to users' risk perceptions.

References

Alalwan, A.A., Dwivedi, Y.K., Rana, N.P.P. and Williams, M.D. (2016), "Consumer adoption of mobile banking in Jordan: Examining the role of usefulness, ease of use, perceived risk and self-efficacy", *Journal of Enterprise Information Management*, Emerald Group Publishing Ltd., Vol. 29 No. 1, pp. 118–139, doi: 10.1108/JEIM-04-2015-0035.

Alaqra, A.S., Fischer-Hübner, S. and Framner, E. (2018), "Enhancing privacy controls for patients via a selective authentic electronic health record exchange service: Qualitative study of perspectives by medical professionals and patients", *Journal of Medical Internet Research*, JMIR Publications Toronto, Canada, Vol. 20 No. 12, p. e10954, doi: 10.2196/10954.

Anderson, J.C. and Gerbing, D.W. (1988), "Structural equation modeling in practice: A review and recommended two-step approach.", *Psychological Bulletin*, American Psychological Association, Vol. 103 No. 3, p. 411, doi: 10.1037/0033-2909.103.3.411.

Ashuri, T. (2024), "Data management as a promise: The case of 'I'", *Computers in Human Behavior Reports*, Elsevier, Vol. 15, p. 100462, doi: 10.1016/j.chbr.2024.100462.

Awais Shakir Goraya, M., Jing, Z., Akhter Shareef, M., Imran, M., Malik, A. and Shakaib Akram, M. (2019), "An investigation of the drivers of social commerce and e-word-of-mouth intentions: Elucidating the role of social commerce in e-business", *Electronic Markets*, Vol. 31, pp. 181–195, doi: 10.1007/s12525-019-00347-w/Published.

Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M.F., Sedlmeir, J., *et al.* (2025), "Self-sovereign identity and digital wallets", *Electronic Markets*, Springer Science and Business Media Deutschland GmbH, Vol. 35 No. 1, doi: 10.1007/s12525-025-00772-0.

Becker, J.-M., Klein, K. and Wetzels, M. (2012), "Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective-formative type models", *Long Range Planning*, Elsevier, Vol. 45 No. 5–6, pp. 359–394, doi: 10.1016/j.lrp.2012.10.001.

Journal of Enterprise Information Management

Belanche, D., Casaló, L. V, Flavián, C. and Schepers, J. (2014), "Trust transfer in the continued usage of public e-services", *Information & Management*, Elsevier, Vol. 51 No. 6, pp. 627–640, doi: 10.1016/j.im.2014.05.016.

Bohari, S.A., Wahab, A.A. and Abdul-Rahim, R. (2025), "Navigating fintech adoption through the role of perceived benefits and risks: The moderating role of generational cohorts", *International Journal of Bank Marketing*, Emerald Publishing, Vol. 43 No. 9, doi: 10.1108/IJBM-01-2024-0064.

Cassie. (2024), *Privacy beyond Borders Insights from around the World*.

Cha, M.-K. and Lee, H.-J. (2022), "Does social trust always explain the active use of sharing-based programs?: A cross-national comparison of Indian and US rideshare consumers", *Journal of Retailing and Consumer Services*, Elsevier, Vol. 65, p. 102515, doi: 10.1016/j.jretconser.2021.102515.

Cheng, X., Su, L., Luo, X., Benitez, J. and Cai, S. (2021), "The good, the bad, and the ugly: Impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing", *European Journal of Information Systems*, Taylor & Francis, Vol. 31 No. 3, pp. 1–25, doi: 10.1080/0960085X.2020.1869508.

Chin, W.W. (1998), "Commentary: Issues and opinion on structural equation modeling", *MIS Quarterly*, JSTOR, Vol. 22 No. 1, pp. vii–xvi.

Comandè, G. and Varilek, M. (2024), "The many features which make the eIDAS 2 Digital Wallet either risky or the ideal vehicle for the transition to post-quantum encryption", *Computer Law and Security Review*, Elsevier Ltd, Vol. 54, doi: 10.1016/j.clsr.2024.106022.

Coopamootoo, K.P.L. (2020), "Usage patterns of privacy-enhancing technologies", *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1371–1390, doi: 10.1145/3372297.3423347.

Creswell, J.W. (2014), *The Selection of a Research Approach*, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Sage Thousand Oaks, CA.

D'Ambrosio, S., De Pasquale, S., Iannone, G., Malandrino, D., Negro, A., Patimo, G., Scarano, V., *et al.* (2016), "Energy consumption and privacy in mobile Web browsing: Individual issues and connected solutions", *Sustainable Computing: Informatics and Systems*, Elsevier, Vol. 11, pp. 63–79, doi: 10.1016/j.suscom.2016.02.003.

Dinev, T., Xu, H., Smith, J.H. and Hart, P. (2013), "Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts", *European Journal of Information Systems*, Springer, Vol. 22 No. 3, pp. 295–316, doi: 10.1057/ejis.2012.23.

Esmaeilzadeh, P. (2020), "The impacts of the privacy policy on individual trust in health information exchanges (HIEs)", *Internet Research*, Emerald Publishing Limited, Vol. 30 No. 3, pp. 811–843, doi: 10.1108/INTR-01-2019-0003.

European Commission. (2023), "European Digital Identity", available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (accessed 2 June 2023).

European Commission's Digital Decade. (2025), "Digital Decade 2025: Country reports | Shaping Europe's digital future", available at: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-country-reports?utm_source=chatgpt.com (accessed 30 June 2026).

Fischer-Hbner, S. and Berthold, S. (2017), "Privacy-enhancing technologies", *Computer and Information Security Handbook*, Elsevier, pp. 759–778, doi: 10.1016/B978-0-12-803843-7.00053-3.

Fornell, C. and Bookstein, F.L. (1982), "Two structural equation models: LISREL and PLS applied to consumer exit-voice theory", *Journal of Marketing Research*, SAGE Publications Sage CA: Los Angeles, CA, Vol. 19 No. 4, pp. 440–452, doi: 10.1177/002224378201900406.

Journal of Enterprise Information Management

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Sage Publications Sage CA: Los Angeles, CA, Vol. 18 No. 1, pp. 39–50, doi: 10.1177/002224378101800104.

Fox, G. and James, T.L. (2021), "Toward an understanding of the antecedents to health information privacy concern: A mixed methods study", *Information Systems Frontiers*, Springer, Vol. 23 No. 6, pp. 1537–1562, doi: 10.1007/s10796-020-10053-0.

Fusch, P.I. and Ness, L.R. (2015), "Are we there yet? Data saturation in qualitative research", *The Qualitative Report*, Vol. 20 No. 9, pp. 1408–1416.

Gefen, D., Benbasat, I. and Pavlou, P.A. (2008), "A research agenda for trust in online environments", *Journal of Management Information Systems*, Vol. 24 No. 4, pp. 275–286, doi: 10.2753/MIS0742-1222240411.

Ghaiumy Anaraky, R., Li, Y., Cho, H., Huang, D.Y., Byrne, K.A., Knijnenburg, B. and Nov, O. (2024), "Personalizing privacy protection with individuals' regulatory focus: Would you preserve or enhance your information privacy?", *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pp. 1–17.

Gong, Z., Han, Z., Li, X., Yu, C. and Reinhardt, J.D. (2019), "Factors influencing the adoption of online health consultation services: The role of subjective norm, trust, perceived benefit, and offline habit", *Frontiers in Public Health*, Frontiers Media SA, Vol. 7, p. 286, doi: 10.3389/fpubh.2019.00286.

Goyal, S., Chauhan, S., Gajpal, Y. and Bhardwaj, A.K. (2023), "Examining consumers' continuance and sharing intention toward food delivery apps", *Journal of Enterprise Information Management*, Emerald Publishing Limited, Vol. 36 No. 6, pp. 1677–1707, doi: 10.1108/JEIM-01-2023-0006.

Habib, A., Alsmadi, D. and Prybutok, V.R. (2020), "Factors that determine residents' acceptance of smart city technologies", *Behaviour and Information Technology*, Taylor and Francis Ltd., Vol. 39 No. 6, pp. 610–623, doi: 10.1080/0144929X.2019.1693629.

Hair, J.F., Ringle, C.M. and Sarstedt, M. (2011), "PLS-SEM: Indeed a silver bullet", *Journal of Marketing Theory and Practice*, Taylor & Francis, Vol. 19 No. 2, pp. 139–152, doi: 10.2753/MTP1069-6679190202.

Hallem, A.P.Y., Abbes, A.P.I., Hikkerova, P.L. and Taga, M.P.N. (2021), "A trust model for collaborative redistribution platforms: A platform design issue", *Technological Forecasting and Social Change*, Elsevier Inc., Vol. 170, doi: 10.1016/j.techfore.2021.120943.

Hanif, M.S., Wang, M., Mumtaz, M.U., Ahmed, Z. and Zaki, W. (2022), "What attracts me or prevents me from mobile shopping? An adapted UTAUT2 model empirical research on behavioral intentions of aspirant young consumers in Pakistan", *Asia Pacific Journal of Marketing and Logistics*, Emerald Group Holdings Ltd., Vol. 34 No. 5, pp. 1031–1059, doi: 10.1108/APJML-09-2020-0659.

Harborth, D. and Pape, S. (2020), "How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor", *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, ACM New York, NY, USA, Vol. 51 No. 1, pp. 51–69, doi: 10.1145/3380799.3380805.

Henseler, J., Ringle, C.M. and Sarstedt, M. (2015), "A new criterion for assessing discriminant validity in variance-based structural equation modeling", *Journal of the Academy of Marketing Science*, Springer, Vol. 43 No. 1, pp. 115–135, doi: 10.1007/s11747-014-0403-8.

Hu, L.-T. and Bentler, P.M. (1998), "Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification", *Psychological Methods*, Vol. 3 No. 4, pp. 424–453.

Hua, C., Cole, S. and Xu, N. (2021), "Rethinking trust in tourism apps: The moderating effect of age", *Journal of Hospitality and Tourism Technology*, Emerald Group Holdings Ltd., Vol. 12 No. 3, pp. 548–562, doi: 10.1108/JHTT-01-2020-0013.

Journal of Enterprise Information Management

Jacob, F., Grosse, E.H., Morana, S. and König, C.J. (2023), "Picking with a robot colleague: A systematic literature review and evaluation of technology acceptance in human–robot collaborative warehouses", *Computers and Industrial Engineering*, Elsevier Ltd, Vol. 180, doi: 10.1016/j.cie.2023.109262.

Jørgensen, K.P. and Beck, R. (2022), "Universal wallets", *Business & Information Systems Engineering*, Springer, Vol. 64, pp. 115–125, doi: 10.1007/s12599-021-00736-6.

Kaaniche, N., Laurent, M. and Belguith, S. (2020), "Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey", *Journal of Network and Computer Applications*, Elsevier, Vol. 171, p. 102807, doi: 10.1016/j.jnca.2020.102807.

Kajol, K., Singh, R. and Paul, J. (2022), "Adoption of digital financial transactions: A review of literature and future research agenda", *Technological Forecasting and Social Change*, Elsevier Inc., Vol. 184, doi: 10.1016/j.techfore.2022.121991.

Keba, V., Oliveira, T. and Trabandt, M. (2025), "Exploring the association between cultural values and the intention to use digital data wallets", *International Journal of Information Management Data Insights*, Elsevier B.V., Vol. 5 No. 2, doi: 10.1016/j.jjimei.2025.100363.

Kim, M.J., Hall, C.M. and Kim, D.K. (2020), "Why do investors participate in tourism incentive crowdfunding? The effects of attribution and trust on willingness to fund", *Journal of Travel and Tourism Marketing*, Routledge, Vol. 37 No. 2, pp. 141–154, doi: 10.1080/10548408.2020.1722784.

Korir, M., Parkin, S. and Dunphy, P. (2022), "An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control", *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pp. 195–211.

Kuen, L., Schürmann, F., Westmattelmann, D., Hartwig, S., Tzafrir, S. and Schewe, G. (2023), "Trust transfer effects and associated risks in telemedicine adoption", *Electronic Markets*, Springer, Vol. 33 No. 1, p. 35.

Kuen, L., Westmattelmann, D., Bruckes, M. and Schewe, G. (2023), "Who earns trust in online environments? A meta-analysis of trust in technology and trust in provider for technology acceptance", *Electronic Markets*, Springer, Vol. 33 No. 1, p. 61, doi: 10.1007/s12525-023-00672-1.

Laatikainen, G., Mustak, M. and Hickman, N. (2025), "Self-sovereign identity adoption: Antecedents and potential outcomes", *Technology in Society*, Elsevier Ltd, Vol. 82, doi: 10.1016/j.techsoc.2025.102859.

Lee, G. and Xia, W. (2010), "Toward agile: An integrated analysis of quantitative and qualitative field data on software development agility", *MIS Quarterly*, JSTOR, Vol. 34 No. 1, pp. 87–114.

Lee, H.J. and Cha, M.K. (2022), "The relationship between anti-consumption lifestyle and the trust triangle in a ride-sharing platform: A cross-cultural study of U.S. and Indian consumers", *International Journal of Consumer Studies*, John Wiley and Sons Inc, Vol. 46 No. 1, pp. 279–294, doi: 10.1111/ijcs.12676.

Lee, M.K.O. and Turban, E. (2001), "A trust model for consumer internet shopping", *International Journal of Electronic Commerce*, Vol. 6 No. 1, pp. 75–91, doi: 10.1080/10864415.2001.11044227.

Lee, Z.W.Y., Chan, T.K.H., Balaji, M.S. and Chong, A.Y.L. (2018), "Why people participate in the sharing economy: An empirical investigation of Uber", *Internet Research*, Emerald Group Publishing Ltd., Vol. 28 No. 3, pp. 829–850, doi: 10.1108/IntR-01-2017-0037.

Lindell, M.K. and Whitney, D.J. (2001), "Accounting for common method variance in cross-sectional research designs.", *Journal of Applied Psychology*, American Psychological Association, Vol. 86 No. 1, p. 114, doi: 10.1037//0021-9010.86.1.114.

Journal of Enterprise Information Management

Liu, Y., Hu, B., Yan, W. and Lin, Z. (2023), "Can chatbots satisfy me? A mixed-method comparative study of satisfaction with task-oriented chatbots in mainland China and Hong Kong", *Computers in Human Behavior*, Elsevier, Vol. 143, p. 107716.

Lu, B., Wang, Z. and Zhang, S. (2021), "Platform-based mechanisms, institutional trust, and continuous use intention: The moderating role of perceived effectiveness of sharing economy institutional mechanisms", *Information and Management*, Elsevier B.V., Vol. 58 No. 7, doi: 10.1016/j.im.2021.103504.

Lucier, D.M., Howell, R.T., Okabe-Miyamoto, K., Durnell, E. and Zizi, M. (2023), "We make a nice pair: Pairing the mID with a NeuroTechnology privacy enhancing technology improves mID download intentions", *Computers in Human Behavior Reports*, Elsevier, Vol. 11, p. 100321, doi: 10.1016/j.chbr.2023.100321.

Lukkien, B., Bharosa, N. and de Reuver, M. (2023), "Barriers for developing and launching digital identity wallets", *Proceedings of the 24th Annual International Conference on Digital Government Research*, EasyChair, pp. 289–299, doi: 10.1145/3598469.3598501.

Mao, Z. (Eddie), Jones, M.F., Li, M., Wei, W. and Lyu, J. (2020), "Sleeping in a stranger's home: A trust formation model for Airbnb", *Journal of Hospitality and Tourism Management*, Elsevier Ltd, Vol. 42, pp. 67–76, doi: 10.1016/j.jhtm.2019.11.012.

Marriott, H.R. and Williams, M.D. (2018), "Exploring consumers perceived risk and trust for mobile shopping: A theoretical framework and empirical study", *Journal of Retailing and Consumer Services*, Elsevier Ltd, Vol. 42, pp. 133–146, doi: 10.1016/j.jretconser.2018.01.017.

Martínez-López, F.J., Li, Y., Feng, C. and López-López, D. (2021), "Buying through social platforms: Perceived risks and trust", *Journal of Organizational and End User Computing*, IGI Global, Vol. 33 No. 4, pp. 1–27, doi: 10.4018/JOEUC.20210701.oa4.

Mayer, R.C., Davis, J.H. and David Schoorman, F. (1995), "An integrative model of organizational trust", Vol. 20 No. 3, pp. 709–734.

Mayr, A., Stahmann, P., Nebel, M. and Janiesch, C. (2024), "Still doing it yourself? Investigating determinants for the adoption of intelligent process automation", *Electronic Markets*, Springer Science and Business Media Deutschland GmbH, Vol. 34 No. 1, doi: 10.1007/s12525-024-00737-9.

McKnight, D.H., Choudhury, V. and Kacmar, C. (2002), "The impact of initial consumer trust on intentions to transact with a web site: A trust building model", *The Journal of Strategic Information Systems*, Elsevier, Vol. 11 No. 3–4, pp. 297–323, doi: 10.1016/S0963-8687(02)00020-3.

Mensah, I.K., Dadson, G.E., Mwakapesa, D.S. and Ukolov, V.F. (2022), "The determinants of Mobile government services adoption: The moderating effect of perceived government support (PGS)", *Information Development*, SAGE Publications Sage UK: London, England, p. 02666669221089656.

Miles, M.B. (1994), "Qualitative data analysis: An expanded sourcebook", *Thousand Oaks*.

"Model Fit". (2026), , available at: https://www.smartpls.com/documentation/algorithms-and-techniques/model-fit (accessed 27 January 2026).

Mou, J. and Cohen, J. (2015), "Antecedents of trust in electronic-service providers: Results from a meta-analysis", *Pacific Asia Journal of the Association for Information Systems*, pp. 1–30, doi: 10.17705/1pais.07101.

Mou, J., Cui, Y. and Kurcz, K. (2020), "Trust, risk and alternative website quality in B-buyer acceptance of cross-border E-commerce", *Journal of Global Information Management*, IGI Global, Vol. 28 No. 1, pp. 167–188, doi: 10.4018/JGIM.2020010109.

Mou, J., Shin, D.-H. and Cohen, J.F. (2017), "Tracing college students' acceptance of online health services", *International Journal of Human–Computer Interaction*, Taylor & Francis, Vol. 33 No. 5, pp. 371–384, doi: 10.1080/10447318.2016.1244941.

Journal of Enterprise Information Management

Müller, L.S., Nohe, C., Reiners, S., Becker, J. and Hertel, G. (2024), "Adopting information systems at work: A longitudinal examination of trust dynamics, antecedents, and outcomes", *Behaviour and Information Technology*, Taylor and Francis Ltd., Vol. 43 No. 6, pp. 1096–1128, doi: 10.1080/0144929X.2023.2196598.

Nemeslaki, A., Aranyossy, M. and Sasvári, P. (2016), "Could on-line voting boost desire to vote?–Technology acceptance perceptions of young Hungarian citizens", *Government Information Quarterly*, Elsevier, Vol. 33 No. 4, pp. 705–714, doi: 10.1016/j.giq.2016.11.003.

Ngwenyama, O., Henriksen, H.Z. and Hardt, D. (2021), "Public management challenges in the digital risk society: A critical analysis of the public debate on implementation of the Danish NemID", *European Journal of Information Systems*, Taylor & Francis, Vol. 32 No. 3, pp. 108–126, doi: 10.1080/0960085X.2021.1907234.

Ngwenyama, O., Henriksen, H.Z. and Hardt, D. (2023), "Public management challenges in the digital risk society: A critical analysis of the public debate on implementation of the Danish NemID", *European Journal of Information Systems*, Taylor & Francis, Vol. 32 No. 2, pp. 108–126, doi: 10.1080/0960085X.2021.1907234.

Padma Kiran, K. and Vedala, N.S. (2025), "Exploring behavioral intentions of consumers towards different digital payment services through the interplay of perceived risks and adoption factors", *Humanities and Social Sciences Communications*, Springer Nature, Vol. 12 No. 1, doi: 10.1057/s41599-025-05468-6.

Podgorelec, B., Alber, L. and Zefferer, T. (2022), "What is a (digital) identity wallet? A systematic literature review", *Proceedings - 2022 IEEE 46th Annual Computers, Software, and Applications Conference, COMPSAC 2022*, Institute of Electrical and Electronics Engineers Inc., pp. 809–818, doi: 10.1109/COMPSAC54236.2022.00131.

Prakash, A.V. and Das, S. (2020), "Intelligent conversational agents in mental healthcare services: A thematic analysis of user perceptions", *Pacific Asia Journal of the Association for Information Systems*, Vol. 12 No. 2, p. 1.

Ringle, C.M., Wende, S. and Becker, J.M. (2022), "SmartPLS 4. Oststeinbek", SmartPLS.

Sarstedt, M., Ringle, C.M., Cheah, J.H., Ting, H., Moisescu, O.I. and Radomir, L. (2020), "Structural model robustness checks in PLS-SEM", *Tourism Economics*, SAGE Publications Inc., Vol. 26 No. 4, pp. 531–554, doi: 10.1177/1354816618823921.

Sauer, M., Becker, C., Oberweis, A., Pfeifer, S., Stark, A. and Sürmeli, J. (2025), "User Experience and Information Security Implications of Digital Identity Wallets", *ICICM 2024 - Proceedings of the 2024 14th International Conference on Information Communication and Management*, Association for Computing Machinery, Inc, pp. 36–45, doi: 10.1145/3711609.3711615.

Sedlmeir, J., Smethurst, R., Rieger, A. and Fridgen, G. (2021), "Digital identities and verifiable credentials", *Business & Information Systems Engineering*, Springer, Vol. 63 No. 5, pp. 603–613, doi: 10.1007/s12599-021-00722-y.

Shao, Z. and Yin, H. (2019), "Building customers' trust in the ridesharing platform with institutional mechanisms: An empirical study in China", *Internet Research*, Emerald Group Holdings Ltd., Vol. 29 No. 5, pp. 1040–1063, doi: 10.1108/INTR-02-2018-0086.

Shao, Z., Zhang, L., Brown, S.A. and Zhao, T. (2022), "Understanding users' trust transfer mechanism in a blockchain-enabled platform: A mixed methods study", *Decision Support Systems*, Elsevier, Vol. 155, p. 113716, doi: 10.1016/j.dss.2021.113716.

Shao, Z., Zhang, L., Li, X. and Guo, Y. (2019), "Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender", *Electronic Commerce Research and Applications*, Elsevier, Vol. 33, p. 100823, doi: 10.1016/j.elerap.2018.100823.

Silva, P., Gonçalves, C., Antunes, N., Curado, M. and Walek, B. (2022), "Privacy risk assessment and privacy-preserving data monitoring", *Expert Systems with Applications*, Elsevier, Vol. 200, p. 116867, doi: 10.1016/j.eswa.2022.116867.

Journal of Enterprise Information Management

Singh, P. and Malik, G. (2024), "Mixed method approach towards continuous use of chatbots in healthcare apps: An integration of humanizing experience theory", *Services Marketing Quarterly*, Routledge, Vol. 45 No. 3, pp. 225–255, doi: 10.1080/15332969.2024.2349342.

Sinha, N., Paul, J. and Singh, N. (2024), "Mobile payments for bottom of the pyramid: Towards a positive social change", *Technological Forecasting and Social Change*, Elsevier Inc., Vol. 202, doi: 10.1016/j.techfore.2024.123313.

Skalkos, A., Tsohou, A., Karyda, M. and Kokolakis, S. (2020), "Identifying the values associated with users' behavior towards anonymity tools through means-end analysis", *Computers in Human Behavior Reports*, Elsevier, Vol. 2, p. 100034, doi: 10.1016/j.chbr.2020.100034.

Söllner, M., Hoffmann, A. and Leimeister, J.M. (2016), "Why different trust relationships matter for information systems users", *European Journal of Information Systems*, Taylor & Francis, Vol. 25 No. 3, pp. 274–287, doi: 10.1057/ejis.2015.17.

SOTERIA. (2023), "SOTERIA, user-friendly secured personal data management platform", available at: https://www.soteria-h2020.eu/ (accessed 5 June 2023).

Srnicek, N. (2026), "Brazil's dWallet program will let citizens cash in on their data - Rest of World", available at: https://restofworld.org/2025/brazil-dwallet-user-data-pilot/ (accessed 3 February 2026).

Sun, S., Zhang, J., Zhu, Y., Jiang, M. and Chen, S. (2022), "Exploring users' willingness to disclose personal information in online healthcare communities: The role of satisfaction", *Technological Forecasting and Social Change*, Elsevier Inc., Vol. 178, doi: 10.1016/j.techfore.2022.121596.

Vaithilingam, S., Ong, C.S., Moisescu, O.I. and Nair, M.S. (2024), "Robustness checks in PLS-SEM: A review of recent practices and recommendations for future applications in business research", *Journal of Business Research*, Elsevier Inc., Vol. 173, doi: 10.1016/j.jbusres.2023.114465.

Venkatesh, V., Brown, S. and Sullivan, Y. (2023), *Conducting Mixed-Methods Research*, Virginia Tech Publishing.

Venkatesh, V., Brown, S.A. and Bala, H. (2013), *Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems*, *Source: MIS Quarterly*, Vol. 37.

Venkatesh, V., Brown, S.A. and Sullivan, Y.W. (2016), "Guidelines for conducting mixed-methods research: An extension and illustration", *Journal of the Association for Information Systems*, Vol. 17 No. 7, pp. 435–495, doi: 10.17705/1jais.00433.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, JSTOR, pp. 425–478, doi: 10.2307/30036540.

Venkatesh, V., Thong, J.Y.L. and Xu, X. (2012), "Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology", *MIS Quarterly*, JSTOR, Vol. 36, pp. 157–178, doi: 10.2307/41410412.

Vongvit, R., Maeng, K. and Chan Lee, S. (2024), "Effects of trust and customer perceived value on the acceptance of urban air mobility as public transportation", *Travel Behaviour and Society*, Elsevier Ltd, Vol. 36, doi: 10.1016/j.tbs.2024.100788.

Wang, C. (2014), "Antecedents and consequences of perceived value in mobile government continuance use: An empirical research in China", *Computers in Human Behavior*, Vol. 34, pp. 140–147, doi: 10.1016/j.chb.2014.01.034.

Wang, H., Meng, Y. and Wang, W. (2013), "The role of perceived interactivity in virtual communities: Building trust and increasing stickiness", *Connection Science*, Taylor & Francis, Vol. 25 No. 1, pp. 55–73, doi: 10.1080/09540091.2013.824407.

Journal of Enterprise Information Management

Wang, M., Kang, Y., Deng, B. and Lan, X. (2024), "Exploring college students' risk perception and acceptance intention of facial recognition technology in China", *Telematics and Informatics*, Elsevier Ltd, Vol. 95, doi: 10.1016/j.tele.2024.102193.

Xu, Z. (2019), "An empirical study of patients' privacy concerns for health informatics as a service", *Technological Forecasting and Social Change*, Elsevier, Vol. 143, pp. 297–306, doi: 10.1016/j.techfore.2019.01.018.

Yan, Z., Zhao, X., Liu, Y. and Luo, X.R. (2024), "Blockchain-driven decentralized identity management: An interdisciplinary review and research agenda", *Information & Management*, Elsevier, Vol. 61 No. 7, p. 104026, doi: 10.1016/j.im.2024.104026.

Yang, S., Song, Y., Chen, S. and Xia, X. (2017), "Why are customers loyal in sharing-economy services? A relational benefits perspective", *Journal of Services Marketing*, Emerald Publishing Limited, Vol. 31 No. 1, pp. 48–62, doi: 10.1108/JSM-01-2016-0042.

Zhai, M. and Chen, Y. (2023), "How do relational bonds affect user engagement in e-commerce livestreaming? The mediating role of trust", *Journal of Retailing and Consumer Services*, Elsevier Ltd, Vol. 71, doi: 10.1016/j.jretconser.2022.103239.

Zhang, H., Zheng, S. and Zhu, P. (2024), "Why are Indonesian consumers buying on live streaming platforms? Research on consumer perceived value theory", *Heliyon*, Elsevier Ltd, Vol. 10 No. 13, doi: 10.1016/j.heliyon.2024.e33518.

Zhang, T., Tao, D., Qu, X., Zhang, X., Zeng, J., Zhu, H. and Zhu, H. (2020), "Automated vehicle acceptance in China: Social influence and initial trust are key determinants", *Transportation Research Part C: Emerging Technologies*, Elsevier, Vol. 112, pp. 220–233, doi: 10.1016/j.trc.2020.01.027.

Zhao, H. and Khaliq, N. (2024), "In quest of perceived risk determinants affecting intention to use fintech: Moderating effects of situational factors", *Technological Forecasting and Social Change*, Elsevier Inc., Vol. 207, doi: 10.1016/j.techfore.2024.123599.

Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J. and Schaub, F. (2020), "Examining the adoption and abandonment of security, privacy, and identity theft protection practices", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–15, doi: 10.1145/3313831.3376570.

Journal of Enterprise Information Management

Journal of Enterprise Information Management

Appendix A

Table 10. Decision choice

Steps	Topic	Decision	Design
Appropriateness	Research questions	Mixed-method research	Qualitative: What are the antecedents of different trust targets? Quantitative: How do the antecedents influence the trust targets? What is the influence of risks on the relationship between antecedents and trust targets? Mixed-method: Do identified antecedents positively influence trust targets?
	Purpose	Qualitative study helps to develop hypotheses for quantitative study.	Developmental purpose: qualitative study developed the model and hypotheses, which were tested in the quantitative study.
	Epistemological perspective	Different epistemological assumptions	Multiple paradigm
	Paradigmatic assumptions	Different methodological approaches	Inductive qualitative study followed by a positivist quantitative study.
Research designs	Investigation strategy	Mixed-method strategy	Exploratory qualitative study followed by a confirmatory quantitative study
	Strands	Multiple stands	Multistrand design.
	Mixing strategy	The elements of the qualitative and quantitative studies were combined at the inferential stages.	Partially mixed methods
	Time orientation	Qualitative precedes quantitative	Sequential exploratory design
	Priority	Not equal	Dominant-less dominant design: qualitative–less dominant, quantitative-dominant.
Data collection and analysis	Sampling	Same population, different strategies	Purposive sample for qualitative study. Probability sample for quantitative study.
	Data collection	Separate data collection in each phase	Qualitative: the combination of open- and closed-ended questions (interviews); Quantitative: closed-ended questions (online questionnaire).
	Data analysis	Firstly, the qualitative data was analyzed, and secondly, the quantitative data.	Sequential design Qualitative: open coding, aggregation of categories into constructs. Quantitative: sample of 1800 answers, rsing PLS-SEM.
	Types of reasoning	The hypotheses were developed and then tested.	Inductive (qualitative) and deductive (quantitative).
	Interference quality	Quality standards addressed	Credibility, reliability, validity, and statistical assumptions were assessed to ensure robust findings.

Notes: adapted from (Venkatesh *et al.*, 2013).

Journal of Enterprise Information Management

Appendix B

Table 11. Interviewee details

Pseudonyms	Age	Employment	Gender	Country
I1	26	Student	Female	Austria
I2	21	Self-employed	Male	Austria
I3	27	Data protection	Female	Austria
I4	27	Financial controller	Female	Austria
I5	36	Consulting	Male	Austria
I6	26	Processing system manager	Female	Austria
I7	22	Student	Female	Austria
I8	25	Railway company	Male	Austria
I9	45	IT Consultant	Male	Austria
I10	36	Sales Director	Female	Austria
I11	30	Assistant Manager	Female	Romania
I12	39	Nurse	Female	Romania
I13	38	Lawyer	Male	Romania
I14	54	Teacher	Male	Romania
I15	49	Teacher	Female	Romania
I16	39	Unemployed	Female	Romania
I17	38	Public procurement expert	Female	Romania
I18	39	Tourism	Female	Romania
I19	39	Marketing Manager	Female	Romania
I20	32	Driver	Male	Romania
I21	26	Human resources	Female	Spain
I22	31	Business development	Male	Spain
I23	46	Professor	Male	Spain
I24	19	Student	Male	Spain
I25	37	Product Manager	Male	Spain
I26	20	Student	Female	Spain
I27	34	IT consultant	Male	Spain
I28	40	Professor	Female	Spain
I29	25	Pre-doctoral program	Female	Spain
I30	36	Computer engineer	Male	Spain

Journal of Enterprise Information Management

Appendix C

Interview Guide

1. How do you perceive the importance of data privacy in online transactions?
2. How would you describe your level of concern about data privacy when engaging in online activities?
3. What are your thoughts on the use of cookies in online environments?
4. Do you currently use any tools or methods to protect your online privacy?
   - **If yes:**
     - Which specific tools or methods do you use? Why?
   - **If no:**
     - Have you considered using such tools in the past? Why?

Explanation of digital data wallets

5. What do you think of digital data wallets? (benefits or drawbacks)
6. What features or requirements would you prioritize in digital data wallets?

Appendix D

Table 12. Survey items

Construct	Items	Source
Performance expectancy	PE1. I find that digital data wallets could be useful in my daily life.	Venkatesh et al. (2012)
	PE2. Using digital data wallets could increase my chances of achieving things that are important to me.	
	PE3. Using digital data wallets could help me accomplish things more quickly.	
	PE4. Using digital data wallets could increase my productivity.	
Transparency	Please specify the importance of the following items: T1. Whether digital data wallets would allow me to find out what information about me they keep in their databases.	Xu, (2019)
	T2. Whether digital data wallets will tell me how long they will retain information they collect from me.	
	T3. The purpose for which digital data wallets would want to collect data from me.	
Social influence	SI1. People who are important to me think that I should use digital data wallets.	Venkatesh et al. (2012)
	SI2. People who influence my behavior think that I should use digital data wallets.	
	SI3. People whose opinions I value prefer that I use digital data wallets.	
Safety	Saf1. Providing identification information using digital data wallets would make me feel safe.	Cheng et al. (2021)
	Saf2. Providing identification information using digital data wallet would make me less concerned about online crime issues. (1-strongly disagree, 7-strongly agree)	
	Saf3. To what extent would you provide identification information in digital data wallet due to the security issue? (1-very low, 7-very high)	
Trust in the information system (formative)	TIS1. I believe that digital data wallets could perform well.	Söllner et al. (2016)
	TIS2. It is important to understand the inner processes that digital data wallet uses to support me.	
	TIS3. I understand why digital data wallets were developed.	
Trust in the Internet (formative)	TIn1. I feel good about how things go when I do activities on the Internet.	
	TIn2. I feel assured that legal and technological structures adequately protect me from problems on the Internet.	
Trust in the community of Internet users (formative)	TCIU1. Information provided by other users of the Internet is valuable.	
	TCIU2. Other users of the Internet offer me help when I have questions.	
	TCIU3. In general, I can count on the information provided by other internet users.	
Trust in the provider (formative)	TP1. I expect that the digital wallet providers to do a good job.	
	TP2. I believe that digital data wallet providers will be willing to support me to achieve my goals as a user.	
	TP3. I believe I will be able to count on the statements of the digital wallet providers.	
Financial risks	FR1. Providing my identification information by using digital data wallets would make me lose money.	Cheng et al. (2021)
	FR2. Providing identification information by using digital data wallets would subject my bank account to potential fraud.	
	FR3. Providing my identification information by using digital data wallets would lead to a financial loss for me.	

Journal of Enterprise Information Management

Identity theft risks	ITR1. Providing identification information by using digital data wallets would make my identification information to be illegally used by others.
	ITR2. Providing identification information by using digital data wallets would lead to unauthorized charges on my bank or credit card account.
	ITR3. Somebody will use my identity for criminal purposes if I provide my identification information to a digital data wallet.

Journal of Enterprise Information Management

Journal of Enterprise Information Management

Appendix E

Table 13. Age and gender distribution

Country	Age/gender	Sample	Population	Chi-squared (p-value)
Austria	18-24	9.5%	9.5%	0.0017 (1.0000)
	25-47	41.0%	40.9%	
	48-64	26.5%	26.6%	
	65+	23.0%	23.0%	
	Male	49.0%	49.0%	0.1601 (0.6891)
	Female	51.0%	51.0%	
Romania	18-24	9.0%	9.0%	0.3408 (0.9522)
	25-47	43.3%	43.2%	
	48-64	24.5%	24.5%	
	65+	23.3%	23.3%	
	Male	49.0%	48.9%	0.1601 (0.6891)
	Female	51.0%	51.1%	
Spain	18-24	8.5%	8.5%	0.22284 (0.9729)
	25-47	42.3%	42.3%	
	48-64	25.5%	25.5%	
	65+	23.8%	23.8%	
	Male	49.3%	49.2%	0.1158 (0.7338)
	Female	50.8%	50.8%	

Notes: https://ec.europa.eu/eurostat/databrowser/view/demo_pjan/default/table?lang=en (EUROSTAT: Population on 1 January by age and sex. Extracted on 04.04.22. Latest update on 03.07.23).

Appendix F

Table 14. Heterotrait-Monotrait Ratio.

	PE	T	SI	Saf	FR	ITR
Performance expectancy (PE)						
Transparency (T)	0.25					
Social influence (SI)	0.75	0.09				
Safety (Saf)	0.68	0.10	0.69			
Financial risks (FR)	0.20	0.07	0.13	0.24		
Identity theft risks (ITR)	0.22	0.10	0.18	0.30	0.83	

Table 15. Loadings and cross-loadings.

	Performance expectancy (PE)	Transparency (T)	Social influence (SI)	Safety (Saf)	Financial risks (FR)	Identity theft risks (ITR)
PE1	**0.93**	0.26	0.63	0.58	-0.20	-0.22
PE2	**0.93**	0.18	0.71	0.62	-0.17	-0.19
PE3	**0.94**	0.28	0.61	0.54	-0.17	-0.19
PE4	**0.92**	0.19	0.71	0.61	-0.16	-0.17
T1	0.24	**0.95**	0.10	0.10	0.06	0.08
T2	0.24	**0.95**	0.09	0.09	0.05	0.08
T3	0.21	**0.94**	0.06	0.07	0.06	0.09
SI1	0.69	0.07	**0.96**	0.62	-0.12	-0.17
SI2	0.66	0.08	**0.96**	0.62	-0.10	-0.15
SI3	0.70	0.11	**0.97**	0.64	-0.13	-0.18
Saf1	0.60	0.11	0.61	**0.94**	-0.21	-0.28
Saf2	0.56	0.07	0.61	**0.92**	-0.17	-0.22
Saf3	0.58	0.08	0.58	**0.91**	-0.22	-0.27
FR1	-0.12	0.01	-0.02	-0.10	**0.90**	0.63
FR2	-0.20	0.13	-0.20	-0.30	**0.88**	0.71
FR3	-0.18	0.02	-0.10	-0.17	**0.93**	0.71
ITR1	-0.20	0.10	-0.18	-0.29	0.71	**0.94**
ITR2	-0.19	0.07	-0.15	-0.25	0.73	**0.95**
ITR3	-0.19	0.09	-0.16	-0.25	0.71	**0.95**

Journal of Enterprise Information Management

Appendix G

To ensure model robustness, three analyses were performed (Sarstedt *et al.*, 2020; Vaithilingam *et al.*, 2024). Firstly, the quadratic effect was assessed (Table 16). relationships were non-significant ($p > 0.05$), while Transparency → Trust in the Internet ($p < 0.001$), Safety → Trust in the provider ($p = 0.004$), and Trust in the community of Internet users → Trust in the information system ($p = 0.026$) showed significant negative quadric effects, indicating diminishing returns at higher levels.

Table 16. Quadratic effects

	Coefficients	P values
Non-linear relationships		
PE → TIS	0.011	0.592
T → TIn	-0.119	0.000
SI → TCIU	0.000	0.989
S → TP	-0.069	0.004
TIn → TCIU	0.012	0.619
TIn → TIS	0.029	0.247
TIn → TP	0.030	0.191
TCIU → TIS	-0.050	0.026
TP → TIS	-0.011	0.642
Linear relationship		
PE → TIS	0.287	0.000
T → TIn	0.063	0.077
SI → TCIU	0.280	0.000
S → TP	0.313	0.000
TIn → TCIU	0.523	0.000
TIn → TIS	0.518	0.000
TIn → TP	0.110	0.000
TCIU → TIS	0.182	0.000
TP → TIS	0.380	0.000

Notes: PE – performance expectancy, T – transparency, SI – social influence, Saf – safety, TIn - trust in the Internet, TCIU - trust in the community of Internet users, TP - trust in the provider, TIS - trust in the information system.

Second, Gaussian Copula analysis assessed endogeneity (Table 17; Sarstedt *et al.*, 2020). Significant endogeneity was found for Transparency → Trust in the Internet, Safety → Trust in the provider, and Trust in the community of Internet users → Trust in the information system. The remaining relationships showed no endogeneity issues. Although endogeneity attenuated these coefficients, their direction and significance remained unchanged.

Table 17. Gaussian Copula analysis

Gaussian Copula of the final model	Coefficients	P values
GC: PE → TIS	-0.010	0.519
GC: T → TIn	-0.672	0.000
GC: SI → TCIU	-0.051	0.359
GC: S → TP	-0.248	0.000
GC: TIn → TCIU	-0.046	0.398
GC: TIn → TIS	0.026	0.290
GC: TIn → TP	-0.232	0.000
GC: TCIU → TIS	-0.043	0.096
GC: TP → TIS	-0.029	0.171
PE → TIS	0.251	0.000

T → TIn	0.486	0.000
SI → TCIU	0.316	0.000
S → TP	0.525	0.000
TIn → TCIU	0.533	0.000
TIn → TIS	0.049	0.218
TIn → TP	0.563	0.000
TCIU → TIS	0.259	0.000
TP → TIS	0.425	0.000

Notes: GC - Gaussian Copula, PE – performance expectancy, T – transparency, SI – social influence, Saf – safety, TIn - trust in the Internet, TCIU - trust in the community of Internet users, TP - trust in the provider, TIS - trust in the information system.

Finally, unobserved heterogeneity was assessed using Finite Mixture PLS (Table 18). Model selection criteria suggest 4-14 segments, with no consistent optimal solution. Thus, unobserved heterogeneity was not considered critical.

Table 18. Fit indices for the one- to fourteen-segment solutions.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
AIC	11621.2	9856.5	8595.0	8272.3	7979.7	7779.3	7461.2	7249.5	7159.4	6949.2	6883.3	6760.6	6631.5	**6500.4**
AIC3	11646.2	9907.5	8672.0	8375.3	8108.7	7934.3	7642.2	7456.5	7392.4	7208.2	7168.3	7071.6	6968.5	**6863.4**
CAIC	11773.5	10167.1	9063.9	8899.6	8765.4	8723.3	8563.5	**8510.2**	8578.4	8526.5	8619.0	8654.7	8683.9	8711.1
AIC4	11671.2	9958.5	8749.0	8478.3	8237.7	8089.3	7823.2	7663.5	7625.4	7467.2	7453.3	7382.6	7305.5	**7226.4**
BIC	11748.5	10116.1	8986.9	8796.6	8636.4	8568.3	8382.5	8303.2	8345.4	**8267.5**	8334.0	8343.7	8346.9	8348.1
MDL5	12457.5	11562.5	11170.7	**11717.7**	12294.8	12964.1	13515.7	14173.8	14953.4	15612.9	16416.7	17163.7	17904.3	18642.9
EN	0.0	0.7	0.8	0.7	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8

Overall, the robustness analyses confirmed the model's stability. Minor non-linearity and endogeneity did not affect the main conclusions.

Journal of Enterprise Information Management