NOVA IMS Information Management School

MGI

Master Degree Program in

Information Management

Adoption of Digital Data Wallets

UTAUT2 Encounters Privacy Calculus

Maureen Rachel Tibbe

Dissertation

presented as partial requirement for obtaining the Master's Degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

ADOPTION OF DIGITAL DATA WALLETS:
UTAUT2 ENCOUNTERS PRIVACY CALCULUS

by

Maureen Rachel Tibbe

Master Thesis presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Knowledge Management and Business Intelligence.

Supervisor: Ph.D. Tiago Oliveira

July 2023

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration. I further declare that I have fully acknowledge the Rules of Conduct and Code of Honor from the NOVA Information Management School.

Maureen Rachel Tibbe

Munich, July 07, 2023

ABSTRACT

Headlines about data leaks, stolen identities, and privacy breaches are no rarity, providing an opportunity for decentralized identity management systems to gain increasing attention. The underlying solution involve digital data wallets (DDWs), which allow users to verify themselves for various services by securely storing their own data - from university certificates to ID cards to health records. Accordingly, it is critical to understand what factors influence the expected use of DDWs along with the extent to which privacy concerns affect their adoption. Therefore, this study provides a holistic approach by proposing a model consisting of variables from the unified theory of acceptance and use of technology (UTAUT2) as well as variables from the privacy calculus model fused into a distinct model. The model was estimated using the partial least squares method and survey data from 400 respondents. It revealed that perceived benefits as well as perceived value play a vital role in the expected use of DDWs. Contrarily, perceived risks were found to influence perceived value, but not expected use. Overall, the model resulted in 11 out of 18 hypotheses being supported. These results help to understand how users will adopt DDWs and are important in encouraging citizens to engage with this new technology.

KEYWORDS

Digital Data Wallet; Adoption; Acceptance; UTAUT2; Privacy calculus

Sustainable Development Goals (SGD)

INDEX

1. Introduction 1
2. Theoretical Background 2
    2.1. Concept of Digital Data Wallets 2
    2.2. Technology Adoption 3
        2.2.1. Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) 4
        2.2.2. Privacy Calculus 5
3. Conceptual Model 7
4. Research Methodology 12
5. Results 13
    5.1. Measurement Model 13
    5.2. Structural Model and Hypothesis Testing 14
6. Discussion 16
    6.1. Theoretical Implications 16
    6.2. Practical Implications 19
    6.3. Limitations and Recommendations for Future Research 19
7. Conclusion 20
Bibliographical References 21
Appendix 29

LIST OF FIGURES

Figure 1 – Conceptual Model 8
Figure 2 – Conceptual Model including results. Notes: ***p<0.001, **p<0.01, *p<0.05 15
Figure 3 – Moderating effect of FC between perceived benefits and expected use 17
Figure 4 – Moderating effect of FC between perceived risks and expected use 18
Figure 5 – Moderating effect of FC between perceived value and expected use..... 18

LIST OF TABLES

Table 1 – UTAUT2 studies overview 4
Table 2 – Privacy calculus studies overview 6
Table 3 – Demographic profile of questionnaire's respondents..... 12
Table 4 – Fornell-Larcker criterion..... 14
Table 5 – Variance inflation factor. Notes: **<0.001, *p<0.01..... 14
Table 6 – Hypotheses conclusion..... 16

LIST OF ABBREVIATIONS AND ACRONYMS

DDW	Digital Data Wallet
UTAUT2	Unified Theory of Acceptance and Use of Technology
VC	Verifiable Credentials
IS	Information Systems
TAM	Technology Acceptance Model
PLS-SEM	Partial Least Squares Structural Equation Modelling
AVE	Average Variance Extracted
HTMT	Heterotrait-Monotrait ratio
VIF	Variance Inflation Factor

1. INTRODUCTION

In recent years, as the Internet continues to evolve alongside the emerging trend of digitized services, headlines about existing data leaks, successful hacker attacks on central data repositories, and misuse of user data by various popular service providers have been mounting – ultimately leading current identity management systems to face repeated criticism. However, these issues create an opportunity for decentralized identity management systems to gain attention, whereby a unified, secure authentication process with full user control throughout the entire process is expected to become the standard. At the heart of these identity management systems lies a digital data wallet (DDW), which is stored on a user's smartphone and allows them to store their personal data, ranging from driver's licenses to health records, in order to digitally verify their eligibility for various services.

With the strong growth in technological advances, research regarding DDWs is still in its infancy. Despite several studies focusing on mobile wallets, electronic wallets, and digital wallets, few have focused on DDWs, which are characterized by having the ability to store all of the user's personal identity-based data in one place, rather than just covering financial prospects or occasionally identity documents as is often the case. In addition, while earlier research has covered the topic of digital wallets (Alkhowaiter, 2020), there is limited empirical work which focuses on the privacy concerns associated with the adoption of digital data wallets, specifically in today's world of technology where individuals' digital footprint has been expanded exponentially. With a massive drive around the globe to go digital in all aspects of life, the need for optimum privacy and security is increasingly becoming a priority. The risk factors associated with digitization are not surprising, as users are often defrauded and hacked to access their personal and financial data. In this regard, Shaw et al. (2022) observe an abundance of privacy and security differences among individuals when it comes to adopting digital wallets. These concerns could be based on individuals' past experiences or future concerns, but hold a strong place in determining their adoption behavior, specifically for technological products, which are commonly considered more vulnerable in terms of privacy and security (Quach et al., 2022). Accordingly, researchers need to include the aspect of privacy concerns in their studies investigating the adoption of digital products (Jaspers & Pearson, 2022). Therefore, to fill this gap in literature, this study examines the acceptance of DDWs and integrates, in addition to general factors, users' privacy concerns that prevent them from using DDWs in their everyday lives. Accordingly, this study highlights the following research objectives: 1) examination of factors influencing the consumers' adoption of digital data wallets, 2) exploration of the associated risks, challenges as well as concerns consumers encounter when engaging with digital data wallets.

The contribution of this study is twofold. First, the current study examines the factors that affect users' adoption of digital wallets using variables from UTAUT2, a wide-ranged model, typically used to predict technology adoption as well as usage behavior. Second, the study examines users' risks and concerns about the use of digital data exchanges in terms of privacy and security of their personal information using the privacy calculus model, which is limited to perceived risks and benefits and is typically used to predict users' willingness to disclose their personal information. Accordingly, this study combines variables from the UTAUT2 model with variables from the privacy calculus model and merges them into a single model to provide a comprehensive outlook on the adoption of DDWs. The findings of this study could help professionals to increase the adoption of DDWs by improving their core functions and

enhancing the privacy of users' data. In addition, the study urges practitioners to promote their measures to protect the privacy of users' identity-based data among the masses.

The paper is structured as follows. As a theoretical basis and orientation to the topic, following the introduction in the theoretical part, the concept of DDWs as well as essential models for the subsequent conceptual model designed for this paper are presented. Following, section 3 introduces the conceptualized model along with the research hypotheses to be tested. The next section focuses on the description of the methodological approach. In this respect, the research method underlying this work is presented. Subsequently, the main obtained results are analyzed in the fifth thematic section. Furthermore, limitations are highlighted and implications for science and practice are crystallized in section 6. The final conclusion in section 7 summarizes the principal outcomes of this research.

2. THEORETICAL BACKGROUND

2.1. CONCEPT OF DIGITAL DATA WALLETS

The term digital data wallet has per se become the buzzword in a world of authentication, (social) platforms and digital transformation – argued to be key to the future. Notwithstanding the reality that most people consider themselves familiar with the term DDW, a Google search for this term yields 133 million results, none of which actually refer to DDWs, but instead solely address digital wallets, indicating the importance of defining a common understanding in respect of this paper. Searching literature results in the conclusion of a diverse range of definitions and interpretations of the term DDW.

With the march of time and the impulse to eradicate all existing loopholes in prevailing identity models, a new model - decentralized identity - inspired by blockchain technology first surfaced in 2015 (Preukschat & Reed, 2021). Over the past years, significant advancements have shaped a new number of innovations in decentralized identity management along with cryptography. In simplistic terms, DDWs are reasonably similar to physical wallets, with the difference that DDWs require software to translate binary data into readable data.

Ironically, this model in fact involves a well-known and intuitive procedure, considering that exactly such a process is applied as a standard in the real world to verify one’s identity (Preukschat & Reed, 2021; Sedlmeir et al., 2021). Instead of a physical wallet, a prerequisite for taking advantage of this identity model is a universal DDW stored on the user’s own smartphone which contains various credentials issued by trusted parties analogous to the plastic cards in a physical wallet. In fact, the difference lies in the use of DDWs, digital credentials, and digital connections (Preukschat & Reed, 2021). In this regard, the independence of a user from a central identity provider forms the core of this method, implying that users retain full control over their personal data at all times (Sedlmeir et al., 2021). Besides the user, two additional parties appear in this model - the issuer and the verifier. Generally, the issuer is responsible for the accurate and trustworthy creation of verifiable credentials (VC) (Sedlmeir et al., 2021; Sporny et al., 2019). Put in simplified matter, the term credential refers to the plastic cards in one’s physical wallet to prove one’s identity, e.g. credit cards, driver licenses, identity (ID) cards, and many more. Alongside the typical plastic cards, testimonials, diplomas, certificates and health data for example, are also referred to as credentials. Generally, VCs adapt the

basic principle of daily used physical documents and can therefore be divided into different parts. The core of a VC consists of one or more claims about the subject of the VC. Those claims can reveal anything about the subject, such as attributes (age, height, eye color, etc.), relationships (employer, citizenship, mother, etc.) or entitlements (membership rewards, legal rights, medical benefits, etc.), and are usually created by a single authority (city government, national agency or certification body), which in this case is the issuer of the credential (Preukschat & Reed, 2021; Sedlmeir et al., 2021; Sporny et al., 2019). Another crucial component is the summary of metadata about certain information such as issuer, type and date as well as other data fields describing the VC. These are usually signed by the issuer using common signature procedures including mathematical methods to ensure the authenticity of digital messages and thereby provide a higher level of trust (Sporny et al., 2019). This can be obtained for example on the basis of a concept that has been known for decades, namely public/private key cryptography (Preukschat & Reed, 2021). While the owner of a private key uses it to sign messages, any other person can prove this signature using the owner's respective private key (Preukschat & Reed, 2021). Fundamentally, the basic concept of DDWs involves the holder requesting a specific document from a specific issuer, which the issuer then issues in form of a VC (Sporny et al., 2019). The holder stores this VC in a DDW and therefore has permanent access to the stored document (Preukschat & Reed, 2021). Subsequently, the holder is able to use this document to identify him-/herself to a specific verifier (Preukschat & Reed, 2021; Sedlmeir et al., 2021; Sporny et al., 2019). Once a holder intends to register with a service offered by a verifier, for example, the verifier requests a verifiable presentation, which may consist of one or more credentials (Sporny et al., 2019). However, the verifier only receives it in case the holder confirms the verifiable presentation (Preukschat & Reed, 2021). Alternatively, it is possible to share only certain attributes of a credential instead of the entire document (Ruff, 2018). Often all the information on a document is superfluous information for a verifier. For instance, a verifier does not necessarily need to know when exactly the holder was born, it could be sufficient for the verifier to know that the holder's age is above a certain threshold. Subsequently, the verifier is able to track who the issuer of the presented document(s) is and whether they are trustworthy (Preukschat & Reed, 2021).

2.2. TECHNOLOGY ADOPTION

Over the past decades, various technology adoption models have guided information systems (IS) research to identify what factors influence technology adoption at organizational, group, and individual levels, both positively as well as negatively. Their relevance is predicated on the underlying assumption that only a widespread and utilized technology, employed by an entire ecosystem, can have a significant impact on the digitization of our society (Ain et al., 2016; Oliveira & Martins, 2011). Therefore, models are constantly being revised, along with emerging models providing new insights to improve the understanding of new technology acceptance. However, Oliveira (2011) further suggests examining a technology under study from multiple adaptation perspectives by combining variables from different models to advance comprehension of determinants associated with technology adoption. After extensive research, the two models relevant to this paper identified are UTAUT2 (Venkatesh et al., 2012) and privacy calculus (Laufer & Wolfe, 1977). The reason is that UTAUT2, as one of the most well-known models, provides an excellent basic foundation for explaining technology adoption with its variables due to its comprehensive framework and predictive power. However, to create a more context specific model, applying only UTAUT2 would not cover certain specific domains. Since this technology is primarily dealing with user data, variables related to data privacy and security

are of great importance. The following sections discuss the models individually and highlight their importance in previous research.

2.2.1. Unified Theory of Acceptance and Use of Technology 2 (UTAUT2)

The UTAUT builds on the technology acceptance model (TAM) (Davis, 1989), which is originally based on Ajzen & Fishbein's (1980) Theory of Reasoned Action and its further development, the Theory of Planned Behavior (Ajzen, 1985), but outperforms both in predicting user acceptance (Legris et al., 2003; Rahman et al., 2017). Unlike previous approaches, the TAM (Davis, 1989) does not initially rely on general attitudes toward technology, instead measuring behavioral intention toward a technology. Intention is based on the primary construct usefulness and the secondary construct ease of use. Subsequently, the UTAUT (Venkatesh et al., 2003) and the UTAUT2 (Venkatesh et al., 2012) amplify this in the direction of a universal theory, ultimately involving twelve variables. These act on intention to use and actual use while being moderated by socio-demographic variables such as age, gender, and experience. Although the UTAUT model achieves high variance elucidation, it is limited by the fact that it was predominantly developed for the organizational context resulting in limited, if any, applicability in other domains of life. In an attempt to understand how consumers behave when integrating new technologies during or before consumption, Venkatesh et al. (2012) elaborated on the UTAUT as a follow-up model, the UTAUT2. Against this background, the UTAUT2 model was extended to include three factors: hedonic motivation, price value and habit (Venkatesh et al., 2012). The following variables have remained identical from the original UTAUT model: performance expectancy, effort expectancy, social influence and facilitating conditions (Venkatesh et al., 2003). In addition, gender, age, experience, and voluntariness in the use of technology proved to be significant moderators for the initial UTAUT model (Venkatesh et al., 2003). However, in the further development towards the UTAUT2 model, voluntariness was removed from the model as a moderating variable, since utilization in private environments is generally a voluntary behavior (Venkatesh et al., 2012).

UTAUT2 has been applied, integrated and extended within a wide range of domains which can be roughly classified as different types of: 1) users, 2) organization, 3) technology, 4) task types, 5) times, 6) places (Tamilmani et al., 2021). Considering that previous studies on the topic of technology types are of particular interest to this study, Table 1 provides a brief overview of various studies that have applied UTAUT2 in the context of different technologies to explore the breadth of the model and how the different variables are applied in diverse settings.

Table 1 – UTAUT2 studies overview

Title	Authors	Year	Overall topic	Constructs	Findings
Factors influencing the adoption of e-Government services in Mauritius	Lallmahomed et al.	2017	E-government	Performance expectancy, effort expectancy, social influence, facilitating conditons, perceived price value, perceived awareness, computer self efficacy, trust, resistance to change, behaviroal intention	Performance expectancy and facilitating conditions positively influence behavioural intention whereas resistance to change and computer self-efficacy have a negative significant relationship with intention to use e-government services.
Surfing the social networks	Robin et al.	2016	Social network service (SNS)	Subjective norm, perceived playfulness, perceived ease of use, perceived usefulness, intention to use	Perceived playfulness is the best determinant when prediciting the intention to use Facebook, Twitter, Instagram, whereas perceived usefulness was the best determinant for LinkedIn.

Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology	Oliveira et al.	2016	Mobile payment	Performance expectancy, effort expectancy, social influence, facilitating conditons, hedonic motivation, price value, compatibility, innovativeness, perceived technology security, behavioral intention to adopt, behavioral intention to recommend	Compatibility, perceived technology security, performance expectations, innovativenss and social influence have significant direct and indirect effects on mobile payment adoption and intention to recommend the technology. The relevance of customers' intention to recommend was also confirmed.
An empirical study of wearable technology acceptance in healthcare	Gao et al.	2015	Wearable health technology	Performance expectancy, social influence, effort expectancy, hedonic motivation, functional congruence, perceived vulnerability, perceived privacy risk, behavioral intention	Medical wearable users pay more attention to factors such as perceived expectancy, effort expectancy, self-efficacy, and perceived severity when choosing a medical wearable.
Extending UTAUT2 to explore pervasive information systems	Segura & Thiesse	2015	Pervasive information systems	Ubiquity, unobtrusiveness, context awareness, performance expectancy, effort expectancy, social influence, hedonic motivation, price value, behaviroal intention	Awareness appears to be the most significant feature for potential consumers of a pervasive technology. Ubiquity and unobtrusiveness can be regarded as important for performance expectancy and effort expectancy, while unobtrusiveness also exhibits a positive effect on hedonic motivation. Social influence has the strongest direct effect on behavioral intention.
An empirical analysis of mobile Internet acceptance in Chile	Ramírez-Correa et al.	2014	Mobile Internet	Performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, habit, behvioural intention, use behaviour	Increase of mobile Internet usage is explained by habit, facilitating conditions, hedonic motivation, performance expectancy, price value and social influence. Only effort expectancy did not influence the dependent variable.

All these studies prove how versatile the UTAUT2 model is and how flexibly it can be combined with other variables. Especially for new technologies, which are not yet so well researched, it offers a first-class possibility to get an overall view of the adoption.

2.2.2. Privacy Calculus

Originally referred to as the "behavioral calculus“, the privacy calculus theory states that users make decisions about whether to disclose personal information based on a risk-benefit calculus, suggesting that individuals think about the future consequences of their behavioral actions (Laufer & Wolfe, 1977). In a nutshell, individuals weigh the associated risks against perceived benefits before deciding whether to disclose personal information. The perceived privacy risk is delineated as potential opportunistic behavior by the recipient that may emerge when an individual discloses their personal information, resulting in a potential loss of control over their personal information (Dinev & Hart, 2006). Among common benefits of disclosing private data are financial perks (e.g., loyalty programs), greater comfort (e.g., storing credit card information with an online retailer), or social benefits (e.g., social networks and messengers) (Sun et al., 2015; Wilson & Valacich, 2012). In contrast, the costs of data disclosure are not as explicit and encompass a full spectrum of potential hazards and negative consequences (e.g., security risks, identity theft, unintended use by third parties, or social criticism and humiliation) (Warshaw et al., 2015). Therefore, based on this model, a user is expected to willingly share one’s data if the expected benefits of disclosure outweigh the risks (Lee & Kwon, 2015).

However, individuals may still raise concerns about the loss of their data, leading to an observed misalignment between their stated worries versus their actual actions (Gerber et al., 2018).

Overall, privacy calculus has been extensively studied in various contexts, such as e-commerce (Dinev & Hart, 2006), mobile apps (Xu et al., 2009), and social network usage (Krasnova et al., 2010; Wilson et al., 2014). For instance, Dinev and Hart (2006) present an extended privacy calculus for online transactions. In the context of personalization, Chellappa and Sin (2005) propose a research model that predicts the use of online personalization by the compatibility between the value for personalization and privacy concerns. Another strand of the privacy calculus literature focuses on social networks. For example, Krasnova et al. (2012) examined the role of culture in the decision to disclose personal information on social networks. Sipior et al. (2013) extended Dinev and Hart's (2006) calculus model and adapted it to the social network context. Table 2 provides a brief overview of studies published in top journals that have applied the privacy calculus theory in different contexts.

Table 2 – Privacy calculus studies overview

Title	Authors	Year	Overall topic	Theories used	Included constructs	Findings
Unfolding the popularity of video conferencing apps – A privacy calculus perspective	Sandhu et al.	2022	Popularity of video conferencing apps	Privacy calculus	Perceived benefits, perceived risks, perceived value, continuance intentions, trust, social presence, techniciality, ubiquity (time savings, spatial flexibility, portability, ommediacy, continuity), MUIPC (perceived surveillance, perceived intrusion, secondary use of personal information)	The study provides insights into the trade-offs professionals are willing to undertake regarding privacy concerns related to VC apps, and sheds light on promoting privacy at the enterprise level, by leveraging control mechanisms that encourage employees to engage in privacy behaviors.
Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective	Jozani et al.	2020	Engagement with social media enabled apps	Privacy calculus	Perceived benefits (efficiency, social, enjoyment), privacy risk, privacy control information sensitivity, institutionaly privacy concerns, social privacy concerns, engagement	The effect of information sensitivity positively influences institutional privacy concerns, while privacy risk has a positive effect and privacy control has a negative effect on social privacy concerns. In addition, institutional and social privacy concerns have a negative influence on user engagement. Meanwhile, the effects of social benefit and enjoyment are significant and positive, but efficiency benefit has a negative effect on user engagement.
A cross-cultural perspective on the privacy calculus	Trepte et al.	2017	Disclosure on social network sites	Privacy calculus combined with Hofstede's culutral dimensions	Individualism, uncertainty avoidance, risks, benefits, willingness for disclosure	People from collectivist-oriented countries attach greater importance to privacy risks. Also, uncertainty avoidance was found to be a cultural dimension that shapes perceptions of SNS risks and benefits. Individuals from cultures with high uncertainty avoidance consider privacy risks more important in their privacy disclosure decisions. Simultaneously, these participants place less importance on social satisfactions as social encounters are seen as less controllable in the social media context.
Intention to disclose personal information via mobile applications: A privacy calculus perspective	Wang et al.	2015	Consumer intention to disclose personal information via apps.	Privacy calculus	Perceived benefits, perceived risks, intention to disclose via mobile apps, personalized service, self-presentation, perceived severity, perceived control	The study found that self-presentation and personalized services positively affect perceived benefits. This positive perception, influences users' intention to disclose personal information. Yet, perceived risks, directly shaped by the level of perceived severity and perceived control, have a negative influence on consumers' willingness to disclose personal information. Compared to perceived risks, perceived benefits have a greater effect on the intention to disclose personal information.

Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective	Li et al.	2015	Consumers' adoption of healthcare wearable devices	Privacy calculus	Perceived privacy risk (information sensitivity, personal innovativeness, legislative protection, perceived prestige, perceived informativeness), perceived benefits (perceived informativeness, functional congruence), adoption intention, actual adoption	When an individual perceives the benefits of a device to be greater than the potential risks to their privacy, they are more inclined to embrace its use. The perceived privacy risk of individuals is influenced by factors such as the sensitivity of health information, personal innovativeness, legislative protection, and the perceived prestige associated with the device. Conversely, the perceived benefits of individuals are shaped by their perception of informativeness and how well the device aligns with their functional needs.
Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior	Keith et al.	2013	Information disclosure on mobile devices	Privacy calculus	Perceived privacy risks (privacy risk awareness, privacy concern), perceived benefirs, intent to disclose, employment	The study found that an increase in perceived privacy risk from a new mobile app significantly decreased a person's intention to disclose information about the app, while perceived benefits increased that intention. Perceived privacy risks play a larger role than perceived benefits in determining intent to disclose information; consumers who intended to disclose information actually did not do so. Finally, perceived benefits of disclosing information do not affect the extent to which consumers register, while they do lead consumers to choose riskier privacy settings.
An extended privacy calculus model for e-commerce transactions	Dinev et al.	2006	Internet privacy concerns for e-commerce transactions	Privacy calculus	Perceived Internet privacy risk, Internet privacy concerns, Internet trust, personal Internet interest, willingness to provide personal information to transact on the Internet	While concerns regarding Internet privacy can hinder e-commerce transactions, the combined impact of Internet trust and personal interest in the online medium are significant factors that can override perceptions of privacy risks. These factors play a crucial role in determining whether individuals choose to disclose personal information when utilizing the Internet.

All these studies reveal that privacy in general will continue to grow in importance in today's digital world with a rising number of digital services, implying the importance of paying closer attention to this issue as new technologies emerge. Individuals react varyingly to privacy concerns with different technologies, which may, however, be related to the perceived benefits of a technology and should therefore be explored.

3. CONCEPTUAL MODEL

DDWs as described above are a relatively new concept, although it is reasonable to assume that the underlying logic is not too foreign to users due to the adoption of mobile wallets such as the well-known Apple Wallet. Nevertheless, data privacy and security of the user's data play a major role, as these issues have gained increasing attention in recent years. Hence, it was decided to build a holistic picture by joining variables from the UTAUT2 model as well as variables from the privacy calculus theory and ultimately merging them into a distinct model. Conclusively, this results in an integrated conceptual model designed specifically to forecast consumer usage, reflecting upon a broad range of relevant factors (see Figure 1). However, in order to thoroughly harmonize the two individual models, some adjustments were undertaken, which will be explained in the following.

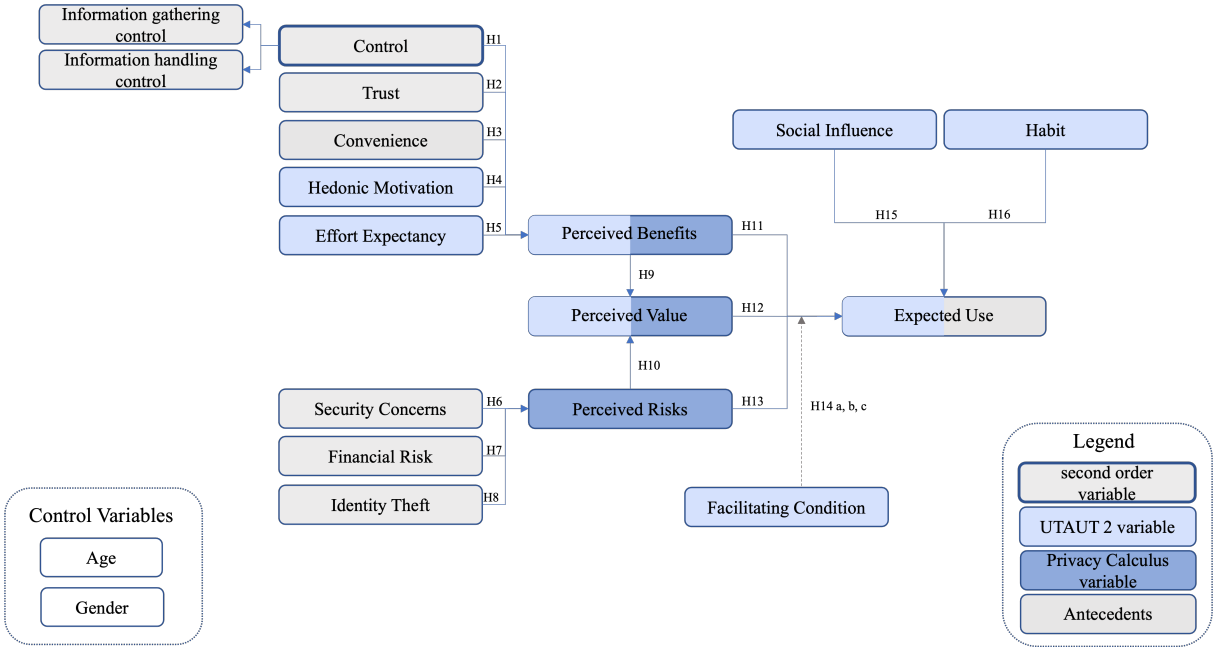

Figure 1 – Conceptual Model

At the heart of the model resides the core privacy calculus construct, primarily consisting of perceived benefits and risks, which in turn influence the variable perceived value. Consequently, a first step was to analyze which variables from UTAUT2 may influence either perceived benefits or perceived risks. It was determined at the outset that the variables performance expectancy and perceived benefits can, by definition, be superimposed and pursue roughly the identical meaning. Underlying the privacy calculus is the idea that a person who anticipates high benefits in a given situation is more likely to self-disclose in that setting given that those benefits outweigh the risks (Dinev & Hart, 2006). In comparison, Venkatesh et al. (2012) defines the performance expectancy variable as the extent to which the use of a technology benefits consumers in undertaking certain activities. Accordingly, the two variables mentioned are merged into one, which retains the label perceived benefits from the privacy calculus model. To this end, the variables hedonic motivation and effort expectancy from the UTAUT2 construct, as well as three additional antecedents involving control, trust, and convenience, were identified to constitute perceived benefits. Conversely, in the case of perceived risks, no variables from the UTAUT2 model were identified, leaving only three antecedents influencing this variable, namely security concerns, financial risk, and identity theft. Still at the core of the model lies another variable, perceived value, also derived from a variable in the UTAUT 2 construct as well as the privacy calculus model. When adjusting UTAUT for consumer context, Venkatesh et al. (2012) included the variable price value to capture "the cognitive tradeoff between the perceived benefits of applications and the monetary costs of their use" (Venkatesh et al., 2012, p. 161), as cost has the potential to significantly affect consumers' adoption of technology (Venkatesh et al., 2012). In some contexts, however, this variable could become obsolete, especially if the technology is available to the end user free of charge (Shaw & Sergueeva, 2019). Nevertheless, although no real costs are associated with the use of the DDWs, consumers are "burdened" by disclosing personal data. Consequently, in this model, the price value construct from UTAUT2 is replaced by the perceived value variable from privacy calculus, reflecting consumers' cognitive trade-off weighed by the benefits of disclosing personal information compared to the perceived risk of losing privacy (Shaw & Sergueeva, 2016, 2019; Weinhard et al., 2017). Further, given that the technology is not yet commercially available, the

dependent variable expected use derives to some extent from the UTAUT2 construct, but has been slightly renamed to measure only anticipated adoption, thereby simultaneously accounting for the willingness to disclose personal information from the privacy calculus model. Moreover, the variables social influence and habit from the UTAUT 2 construct influence the dependent variable, whereas facilitating conditions act as a moderator between the heart of the model (perceived benefits, value, risks) and the dependent variable. Finally, it should be noted that in the developed model the control variable experience is excluded due to the fact that DDWs are perceived a rather new technology with limited likelihood of prior exposure. Based on the above foundation, the following hypotheses are proposed:

The variable privacy control is presented in Figure 1 with a slightly thicker frame, due to the fact of being a second-order variable resulting from the variables information gathering control as well as information handling control. In a nutshell, the concept of this variable encompasses two different facets of information control: firstly, how much control a person perceives they have over the acquisition of their personal information (collection and storage) and secondly, how much control a person perceives they have over the handling of that information (use and dissemination) (Alge et al., 2006; Cheng et al., 2021). Providing users with the ability to control their privacy is a powerful tool for improving positive perceptions while reducing negative perceptions, which in turn may impact the expected use of DDWs. Based on these arguments, privacy control is expected to have a positive impact on perceived benefits, which increases the use of a DDW (Alge et al., 2006; Cheng et al., 2021).

H1: *Privacy control positively influences perceived benefits.*

Based on Ross and LaCroix (1996), trust can arise from predictability. Put in simplified matter, once individuals are able to predict future activities of certain objects by expecting those objects to function reliably, they are likely to develop trust in those objects (X. Wang et al., 2021). Benamati et al. (2017) even takes this a step further and defines trust as the extent to which people are willing to expose themselves to the actions of a third party including for example the willingness to disclose personal information as a condition of using DDWs (Duan & Deng, 2022). Consequently, by trusting the use of certain technologies, individuals tend to be confident that technology providers will protect personal data from unauthorized access as well as misuse (Duan & Deng, 2022). As a result, it can be concluded that people who are willing to trust the technology provider are conversely less concerned about data privacy, which studies have underscored (Duan & Deng, 2022; Morosan & DeFranco, 2015; X. Wang et al., 2021).

H2: *Trust positively influences perceived benefits.*

Convenience in the sense of timesaving or reduced workload resulting from the disclosure of personal data and subsequently making use of it when using various digital services is perceived as an ongoing barrier that encourages or discourages future intentions (Cheng et al., 2021; Collier & Kimes, 2013). Accordingly, it can be assumed that convenience influences perceived benefits, which is also supported by the study of Kim et al. (2023), revealing that convenience influences perceived benefits when it comes to customers' self-service technology choices.

H3: *Convenience positively influences perceived benefits.*

Hedonic motivation, conceptualized as perceived enjoyment, is defined as the amusement or pleasure experienced as a result of using a technology, has proven to exert a direct effect on technology adoption as well as use (Venkatesh et al., 2012). Against this background, it is hypothesized that people who generally find pleasure in using DDWs will perceive the technology positively.

H4: *Hedonic Motivation positively influences perceived benefits.*

Effort expectancy is defined by Venkatesh et al. (2003, 2012) as the degree to which a technology offers ease of use for consumers. Based thereon, it can be deduced a technology is perceived more positively the easier it is to use (Utomo et al., 2021).

H5: *Effort expectancy positively influences perceived benefits.*

New technologies in particular inevitably raise a number of concerns among users, some of which are not unjustified and ultimately have a negative impact on the acceptance of the technology. In peculiar, a DDW that concentrates a person's most valuable information in one location provides a significant target for attacks (Cichy et al., 2021). In addition, a lack of technical understanding associated with a technology that is not yet backed by decades of research and implementation audits is another factor contributing to these security concerns (Sartor et al., 2022). Overall, the term security addresses the protection of data from unauthorized access as well as from damage based on certain objectives: ensuring integrity, authenticity and confidentiality (Cichy et al., 2021). Conclusively, skepticism is especially high toward decentralized identity management in general (Sartor et al., 2022) and, according to Cichy et al.'s (2021) study, major security concerns significantly influence the privacy concerns. Beyond security concerns, new technologies are often associated with various other privacy invasion concerns, such as financial risk and identity theft. Numerous studies on privacy concerns have sought to analyze individuals' privacy perceptions and behaviors across myriad dimensions, such as the consequences of privacy concerns, the importance of privacy control, in addition to the link between privacy and self-disclosure or purchase intentions (Cheng et al., 2021; Jordan et al., 2018; Xu et al., 2011; Yang et al., 2015). Identity theft as well as financial risks are both deemed as invasion of privacy; therefore the associated potential to be vulnerable to exposure leads to the conclusion that the higher the fear of these issues, the greater the negative perception of the technology (Cheng et al., 2021; Jordan et al., 2018; Yang et al., 2015).

H6: *Security concerns positively influence perceived risks.*

H7: *Financial risk positively influences perceived risks.*

H8: *Identity theft positively influences perceived risks.*

Considering that perceived value reflects consumers' cognitive trade-offs between the benefits of disclosing personal information and the perceived risk of losing privacy, it can be argued that this variable is positively influenced by perceived benefits while being negatively influenced by perceived risks (Shaw & Sergueeva, 2016, 2019; Yang et al., 2015).

H9: *Perceived benefits positively influence perceived value.*

H10: *Perceived risks negatively influence perceived value.*

In general, individuals base decisions on their subjective value, which is derived from perceived benefits and risks (Yang et al., 2015). To this effect, prior studies have identified a strong relationship between perceived value and intention to use mobile Internet, mobile payment or service adoption (H.-W. Kim et al., 2007; Kleijnen et al., 2007; Yang et al., 2015). Consequently, it can be assumed that perceived value, together with perceived benefits and risks, significantly influence consumers' intention to adopt DDWs and, consequently, its expected usage.

H11: *Perceived benefits positively influence consumers' expected use.*

H12: *Perceived value positively influences consumers' expected use.*

H13: *Perceived risks negatively influence consumers' expected use.*

By definition, facilitating conditions represent how consumers perceive the resources and support available to execute a specific behavior (Venkatesh et al., 2012). Previous information systems research has identified mixed influences of facilitating conditions on behavioral intention and actual use, leading Limayem and Hirt (2003) to propose a moderating effect of facilitating conditions on the relationship between behavioral intention and actual use. Hossain et al. (2017) tested this proposal in their study on location-based services in which the moderating effect of facilitating conditions was confirmed. On reflection, this is eminently logical, as facilitating conditions may be more relevant to some users than to others, e.g., due to differences in technical affinity, and therefore often do not have a direct impact on actual use. Applying this to the present study, facilitating conditions are assumed to have a moderating effect on the relationships between perceived benefits and expected use, perceived value and expected use, as well as perceived risks and expected use.

H14 a, b, c: *Facilitating conditions moderate the relationship between a) perceived benefits and expected use, b) perceived value and expected use, c) perceived risks and expected use.*

In fact, a technology like DDWs can only genuinely thrive in an ecosystem, meaning when many people choose to use it. Therefore, social influence, in other words, the degree to which consumers feel that significant others believe that they should use a particular technology (Venkatesh et al., 2012), is of tremendous importance for technology adoption (Chávez Herting et al., 2020; Nikou & Bouwman, 2013). Therefore, social influence may affect the expected use of DDWs.

H15: *Social influence positively influences consumers' expected use.*

The phenomenon referred to as habit refers to a repeated pattern of behavior that emerges without conscious awareness; accordingly, these repeated behaviors may result in habitual behaviors (Nikou & Bouwman, 2013). Once a behavior has been repeated more frequently in the past, subsequent behaviors can be assumed to occur automatically (Nikou & Bouwman, 2013; Venkatesh et al., 2012). Above all, habit plays an integral role in the adoption to new technologies (Chávez Herting et al., 2020; Venkatesh et al., 2012), which is supported by Jung and Lee's (2020) study on the use of open educational resource repositories, indicating that habit is the variable that had the greatest influence on the their adoption. Consequently, it can be inferred that the more people would become habituated to using a DDW, the higher the predicted use will be.

H16: *Habit positively influences consumers' expected use.*

4. RESEARCH METHODOLOGY

With the aim of empirically investigating the research model described above, a standardized questionnaire was created containing specific questions about each variable and hypothesis to be examined. Originally, the questionnaire was drafted in English, whereas the final version was translated into German by a professional translator, given the fact that the questionnaire was distributed solely in Austria. With the assistance of a market research company, the questionnaire was distributed between May and April 2022 and yielded 400 valid responses. Prior to distribution of the questionnaire, a pilot was conducted to identify any ambiguities, refine certain questions, and obtain additional feedback on content and structure. Moreover, for the purpose of providing respondents with a basic understanding of DDWs, the questionnaire is preceded by a short informational video. The content of this video provides a brief outline of how the technology functions as well as potential use cases in an approachable format.

Generally, all measures were adopted from literature with slight modifications - the items for UTAUT2 data constructs were adopted from Venkatesh et al. (2003, 2012) whereas items for the privacy calculus data constructs were inherited from Kehr et al. (2015) and Wang et al. (2004) while items for the additional antecedents were derived from Cheng et al. (2021), Alge et al. (2006) as well as Cichy et al. (2021). The items for all constructs are included in Appendix A. Most items were measured using a seven-point Likert scale ranging from 1 (strongly agree) to 7 (strongly disagree) in order to be able to quantify as well as finally transfer the answers into a structural equation model. Likert scales with seven response options were chosen in order to provide respondents with the option of not answering a question unambiguously compared to a scale with an even number of response options. However, to evaluate the expected use of DDWs, one item measures the expected frequency of DDW use in relation to various credentials (e.g., ID card, credit card, university certificate, …) on a slightly different range from 1 (never) to 7 (every time I would need it). Moreover, the questionnaire includes demographic questions about age and gender, as well as general information concerning education and occupation. While age is measured in age ranges, gender is measured in form of dummy variables, with 1 representing men. Table 3 displays the demographic profile of the questionnaire's respondents.

Table 3 – Demographic profile of questionnaire's respondents

Demographic measures		Sample (n=400)	Frequency (%)
Gender	Male	196	49%
	Female	204	51%
Age	18-24	40	10%
	25-47	160	40%
	48-64	108	27%
	≥65	92	23%
Occupation	Student	20	5%
	Employed	196	49%
	Self-employed	36	9%
	Unemployed / Retired	148	37%
Education	School degree	132	33%
	Apprenticeship	164	41%
	Bachelor's degree	44	11%
	Master's degree	52	13%
	Doctoral degree	8	2%

5. RESULTS

The current study has utilized partial least squares structural equation modelling (PLS-SEM) for data analysis which has garnered an abundance of interest from methodological and application researchers across a variety of fields (Becker et al., 2023). Many researchers find the PLS-SEM method to be particularly intriguing since it allows them to estimate complicated models with a large number of constructs, marker variables, and structural paths without putting distributional presumptions on the data (Hair et al., 2019). Studies that have been published in business management as well as information systems over the past decades have increasingly used PLS-SEM to estimate and empirically support theoretically established models with constructs (Guenther et al., 2023). The findings obtained from the data analysis were reported and interpreted according to the recommendations of Hair et al. (2019), which were supplemented by guidance on reporting Smart PLS results from one of the program's co-founders.

5.1. MEASUREMENT MODEL

Analyzing the indicator loadings is the first stage in the evaluation of the measurement model. For adequate item reliability, loadings above 0.708 are advised (Hair et al., 2019). Accordingly, items IGC1, IHC1 and H2 were deleted to establish significant item reliability. Subsequently, the evaluation of the reliability of internal consistency is performed. The genuine reliability of the construct is often assumed to lie between two extremes, with Cronbach's alpha possibly being too conservative and the composite reliability possibly being too liberal (Hair et al., 2019). Accordingly, Hair et al. (2019) recommend ρ_A, which typically falls between Cronbach's alpha and the composite reliability, as an approximate measure of construct reliability. The results of this study demonstrate significant ρ_A values which present that all the variables are within the acceptable range of reliability (see Appendix B).

Thereafter, the convergent validity of each construct measure is examined in the third step of the reflective measurement model assessment. The average variance extracted (AVE) for all items on each construct is the statistic used to assess a concept's convergent validity. When the AVE is 0.50 or above, the construct is considered acceptable, because it accounts for at least 50% of the variation of its item (Hair et al., 2019). All the AVE values are above 0.50 which demonstrate that all the variables share more than 50% variation among them (see Appendix B).

The extent to which a construct is empirically different from other constructs in the structural model is measured by discriminant validity, which is the fourth phase (Hair et al., 2019). The Fornell-Larcker criterion performs poorly, particularly when the indicator loadings on a construct deviate just marginally, therefore, Henseler et al. (2015) suggested the heterotrait-monotrait (HTMT) ratio of the correlations as a suitable substitute. For structural models with constructs that are theoretically extremely similar, a threshold value of 0.90 is recommended (Hair et al., 2019; Henseler et al., 2015). As per the results, all the HTMT values are in the acceptable range except one, namely IHC (see Appendix C), which is negligible given that an additional inferential statistics test was performed rejecting hypothesis HTMT = 1. All values were below 1 in this case. Despite recent findings in research, the values of the Fornell-Larcker criterion was additionally analyzed, according to which the square root of the AVE must be greater than the correlation between the variables (Hair et al., 2019). These results indicated that the square root of the AVE, diagonally distributed, was higher than the correlation coefficient between the constructs (see Table 4). Therefore, said results indicate that all the constructs are empirically distinct from one another and totally suitable for further analysis.

Additionally, all loadings are greater than the cross loadings (see Appendix C), which also argues for discriminant validity (Chin, 1998).

Table 4 – Fornell-Larcker criterion

Variables	Mean	SD	Con	DS	EE	FC	FR	H	HM	IGC	IHC	IT	PB	PR	SI	Tr	Val
Convenience	4.134	1.771	0.956														
Security Concerns	5.061	1.495	-0.285	0.883													
Effort Expectancy	4.776	1.609	0.567	-0.162	0.906												
Facilitating Condition	4.440	1.744	0.580	-0.206	0.758	0.916											
Financial Risk	4.110	1.413	-0.275	0.475	-0.293	-0.229	0.863										
Habit	3.722	1.742	0.705	-0.327	0.620	0.640	-0.244	0.898									
Hedonic Motivation	3.965	1.693	0.641	-0.295	0.601	0.594	-0.249	0.773	0.917								
Info Gathering Control	3.460	1.764	0.539	-0.319	0.385	0.403	-0.313	0.559	0.543	0.922							
Info Handling Control	3.519	1.766	0.621	-0.351	0.459	0.483	-0.337	0.644	0.629	0.810	0.955						
Identity Theft	4.357	1.514	-0.205	0.542	-0.219	-0.201	0.730	-0.216	-0.173	-0.215	-0.260	0.931					
Perceived Benefits	3.448	1.639	0.665	-0.362	0.394	0.481	-0.353	0.621	0.523	0.566	0.594	-0.308	0.938				
Perceived Risk	5.161	1.498	-0.300	0.667	-0.165	-0.233	0.559	-0.345	-0.314	-0.343	-0.396	0.586	-0.454	0.937			
Social Influence	2.877	1.731	0.408	-0.354	0.323	0.411	-0.187	0.543	0.582	0.468	0.515	-0.184	0.416	-0.393	0.957		
Trust	3.474	1.655	0.638	-0.520	0.460	0.496	-0.453	0.679	0.623	0.631	0.688	-0.403	0.727	-0.570	0.525	0.908	
Perceived Value	3.838	1.765	0.740	-0.372	0.545	0.541	-0.362	0.757	0.693	0.598	0.680	-0.297	0.701	-0.420	0.452	0.810	0.954

Following the confirmation of all mandatory criteria for the evaluation of the measurement model for the reflective construct, the evaluation for the formative construct was performed. Therefore, the variance inflation factor (VIF) was assessed to verify multicollinearity along with the statistical significance of the weights of each indicator. The acceptable value for the VIF, as suggested by Hair et al. (2019), should be less than 5. The result of the collinearity diagnostic indicated that all VIF values remained below the acceptable value and hence fulfilled the criteria, indicating that there was no multicollinearity among the indicators of the formative construct (see Table 5). Although the outer weights of indicators EU1 and EU3-5 are not statistically significant, they were retained considering that their loadings are above 0.5.

Table 5 – Variance inflation factor. Notes: **<0.001, *p<0.01

Items	VIF	Outer weights	Outer loadings
EU1	3.829	0.142	0.871
EU2	3.497	0.348**	0.906
EU3	4.091	0.022	0.836
EU4	3.559	0.124	0.856
EU5	3.311	0.012	0.800
EU6	1.746	0.229**	0.693
EU7	2.198	0.330*	0.814

5.2. STRUCTURAL MODEL AND HYPOTHESIS TESTING

For the purpose of collinearity analysis, the inner VIF between the predictors and the outcome variables must be assessed. As a matter of fact, this procedure is executed in a similar way as the evaluation of formative measurement model, except that the latent variable values of the predictor constructs are used in a partial regression to calculate the VIF values. Thus, as a rule of thumb, VIF values above 5 reflect likely collinearity problems between the predictor constructs (Hair et al., 2019). Based on the results of the current study, all values of the internal VIF fall below the acceptable value of 5, ranging from 1.265 to 3.092.

The results of hypothesis testing are measured in terms of magnitude and value of path coefficients and their respective p-values which are considered significant at less than 0.05 (Hair et al., 2019). By applying the bootstrapping method with 5000 replicate samples, the significance levels of the constructs in the conceptual model were assessed. Figure 2 summarizes the findings.

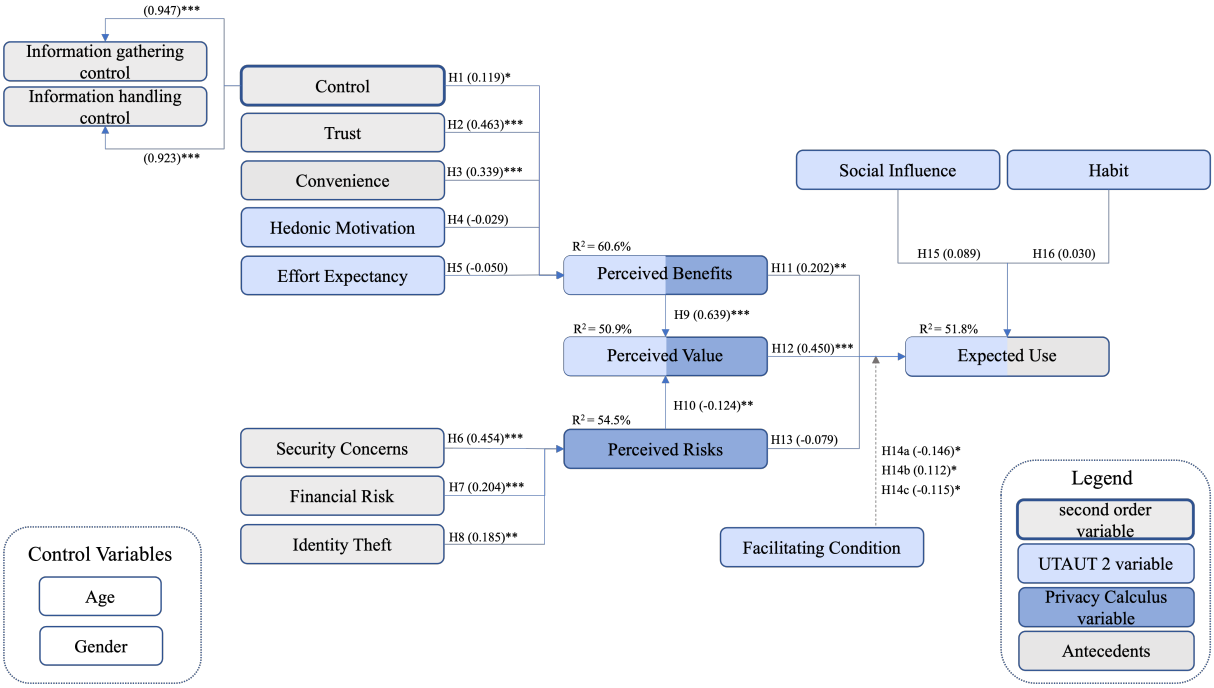

Figure 2 – Conceptual Model including results. Notes: ***p<0.001, **p<0.01, *p<0.05

The present model explains 51.8% of the variation in the expected use of DDWs. Perceived benefits ($\hat{\beta}$= 0.202, p<0.01) and perceived value ($\hat{\beta}$= 0.450, p<0.001) are statistically significant for predicting expected use. Conversely, perceived risk ($\hat{\beta}$= -0.079, p>0.05), social influence ($\hat{\beta}$= 0.089, p>0.05) as well as habit ($\hat{\beta}$= 0.030, p>0.10) are not statistically significant measures of expected use. Therefore, H11 and H12 are supported, while H13, H15 and H16 are not. The moderation effect of facilitating conditions on expected use is statistically significant in all cases: with perceived benefits ($\hat{\beta}$= -0.146, p<0.05), perceived value ($\hat{\beta}$= 0.112, p<0.05) and perceived risks ($\hat{\beta}$= -0.115, p<0.05). However, although all cases are statistically significance, the moderation effects of facilitating conditions between perceived benefits and expected use as well as between perceived risks and expected use occur differently than hypothesized, namely negatively instead of positively. Consequently, only H14b is supported, while H14a and H14c are rejected. Moreover, the model explains 60.6% of the variation associated with perceived benefits of using DDWs. On the one hand, privacy control ($\hat{\beta}$= 0.119, p<0.05), trust ($\hat{\beta}$= 0.463, p<0.001) as well as convenience ($\hat{\beta}$= 0.339, p<0.001) are statistically significant for perceived benefits supporting H1, H2, and H3. On the other hand, hedonic motivation ($\hat{\beta}$= -0.029, p>0.10) and effort expectancy ($\hat{\beta}$= -0.050, p>0.10) were found not to be statistically significant, therefore H4 and H5 are rejected. Concerning the perceived value of using DDWs, the model explains 50.9% of the variation. In this context, both perceived benefits ($\hat{\beta}$= 0.639, p<0.001) and perceived risks ($\hat{\beta}$= -0.124, p<0.01) were measured as statistically significant, providing evidence to confirm hypotheses H9 and H10. In terms of perceived risks associated with DDW use, the model explains 54.5% of the variation, with all variables contributing statistical significance, including security concerns ($\hat{\beta}$= 0.454, p<0.001), financial risk ($\hat{\beta}$= 0.204, p<0.001), and identity theft ($\hat{\beta}$= 0.185, p<0.01).

Accordingly, hypotheses H6, H7, and H8 are validated. Finally, regarding the control construct of the model, it proved to be a second-order composite control variable, with both variables (control of information processing and control of information acquisition) demonstrating relevance to control based on reaching statistical significance. Overall, of the 18 hypotheses, 11 hypotheses are confirmed, and 7 hypotheses are rejected.

The defined control variables age and gender are predominantly not statistically significant ($p>0.05$ or even $p>0.10$), except for age influencing perceived risks. Therefore, it can be inferred that gender has no significant impact on the dependent variable and thus is not related to the expected use of DDWs. With respect to the control variable age, it can be deduced that this variable is likewise to gender inconsequential to the expected use of DDWs, since perceived risks also do not influence the dependent variable. For clarity, all results are also displayed in the table below.

Table 6 – Hypotheses conclusion

Hypotheses	Independent V.	Dependent V.	Sign suggested	Findings	Result	Conclusion
H1	Control	Perceived Benefits	Positive	ß= 0.119, p<0.05	Positive and statistically sign.	Supported
H2	Trust	Perceived Benefits	Positive	ß= 0.463, p<0.001	Positive and statistically sign.	Supported
H3	Convenience	Perceived Benefits	Positive	ß= 0.339, p<0.001	Positive and statistically sign.	Supported
H4	Hedonic Motivation	Perceived Benefits	Positive	ß= -0.029, p>0.10	Negative and statistically insign.	Rejected
H5	Effort Expectancy	Perceived Benefits	Positive	ß= -0.050, p>0.10	Negative and statistically insign.	Rejected
H6	Security Concerns	Perceived Risks	Positive	ß= 0.454, p<0.001	Positive and statistically sign.	Supported
H7	Financial Risk	Perceived Risks	Positive	ß= 0.204, p<0.001	Positive and statistically sign.	Supported
H8	Identity Theft	Perceived Risks	Positive	ß= 0.185, p<0.01	Positive and statistically sign.	Supported
H9	Perceived Benefits	Perceived Value	Positive	ß= 0.639, p<0.001	Positive and statistically sign.	Supported
H10	Perceived Risks	Perceived Value	Negative	ß= -0.124, p<0.01	Negative and statistically sign.	Supported
H11	Perceived Benefits	Expected Use	Positive	ß= 0.202, p<0.01	Positive and statistically sign.	Supported
H12	Perceived Value	Expected Use	Positive	ß= 0.450, p<0.001	Positive and statistically sign.	Supported
H13	Perceived Risks	Expected Use	Negative	ß= -0.079, p>0.05	Negative and statistically insign.	Rejected
H14a	Facilitating Conditions	PB x Expected Use	Moderation	ß= -0.146, p<0.05	Negative and statistically sign.	Rejected
H14b	Facilitating Conditions	PV x Expected Use	Moderation	ß= 0.112, p<0.05	Positive and statistically sign.	Supported
H14c	Facilitating Conditions	PR x Expected Use	Moderation	ß= -0115, p<0.05	Negtaive and statistically sign.	Rejected
H15	Social Influence	Expected Use	Positive	ß= 0.089, p>0.05	Positive and statistically insign.	Rejected
H16	Habit	Expected Use	Positive	ß= 0.030, p>0.10	Positive and statistically insign.	Rejected

6. DISCUSSION

6.1. THEORETICAL IMPLICATIONS

Overall, the studied model explains 51.8% variance in the expected use of DDWs. The present research concludes that regardless of privacy control, trust and convenience significantly increasing the perceived benefits of DDWs, hedonic motivation and effort expectancy have no significant impact on the perceived benefits of DDWs. Moreover, it was found that three antecedents of risks (security concerns, financial risks and identity theft) associated with the usage of DDWs significantly increase the perceived risks which is in line with the extant literature where Cheng et al. (2021) viewed them as invasions of privacy. Therefore, the possibility of being exposed as a result of stated privacy concerns results in the conclusion that individuals' perceptions of technology are more negatively affected by them.

Findings of the study also established a significant positive relationship of perceived benefits with perceived value and expected use. Moreover, perceived risks associated with DDWs have been found to decrease the perceived value of the stated technology which is justified as per the findings of Shaw

& Sergueeva (2019). Whereas, in terms of expected use, findings related to perceived risks were insignificant. In fact, as many studies have revealed, individuals often act contrarily to their attitudes toward their own information privacy when deciding to use a product (Gerber et al., 2018; Kokolakis, 2017). In other words, individuals may have very strong privacy concerns, but do not modify their privacy settings or refrain from using a certain webpage/app. Causes of the so-called privacy paradox are manifold, often based on network effects, convenience, or information asymmetry and are difficult to metatheorize with a single human behavioral theory (Gerber et al., 2018; Kokolakis, 2017).

Furthermore, the study presented that perceived value substantially contributes to the expected use of DDWs, which is in line with the previous literature by Yang et al. (2015). In addition, social influence and habit did not influence the expected use of DDWs regardless of their extensive relationship in the extant literature. These findings could have resulted from the fact that the product is not yet available on the market for customers and respondents experienced difficulty in assessing the questions about habit and social influence without a real foundation.

Moreover, the study included three moderations that tested the moderating role of facilitating conditions between perceived benefits, perceived risks and perceived value, and expected use. Figure 3 indicates that the relationship between perceived benefits of DDWs and expected use is stronger with low facilitating conditions.

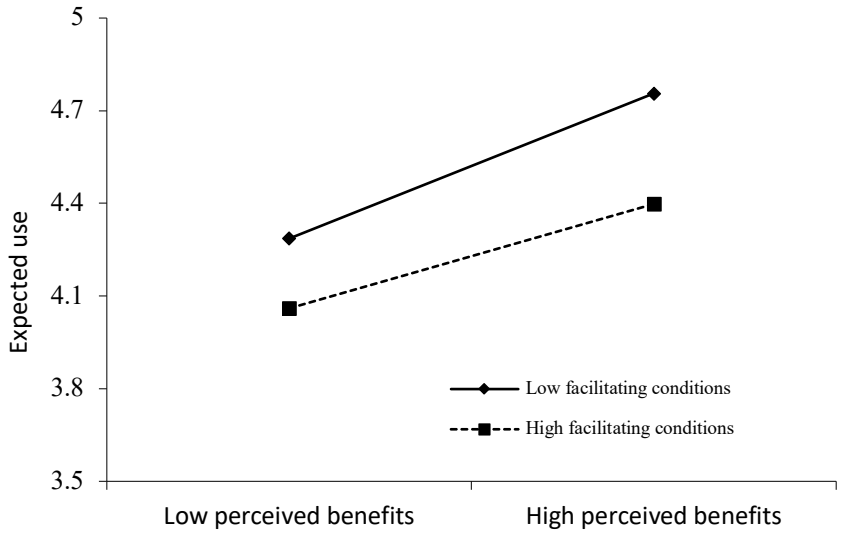

Figure 3 – Moderating effect of FC between perceived benefits and expected use

As can be observed in Figure 4, the same applies to the relationship between perceived risks and expected use.

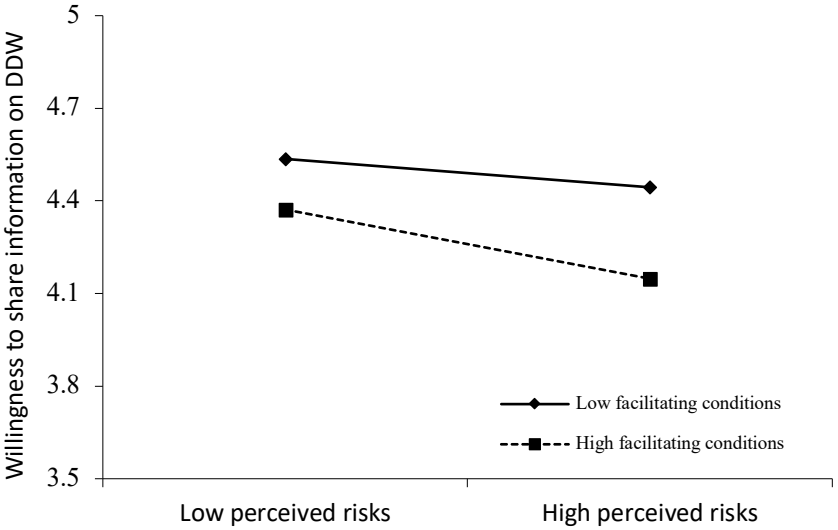

Figure 4 – Moderating effect of FC between perceived risks and expected use

Only the relationship between perceived value and expected use behaves differently for the facilitating conditions moderation: A high level of facilitating conditions increases the effect of perceived value on expected use even more dramatically (Figure 5).

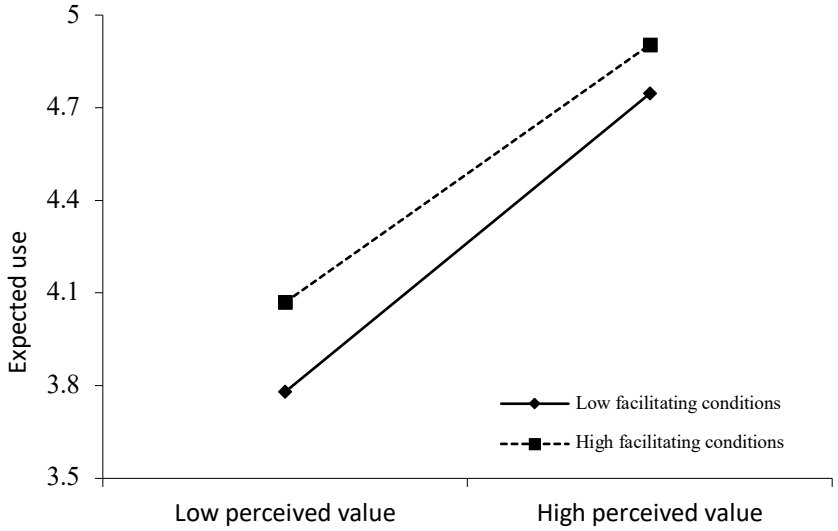

Figure 5 – Moderating effect of FC between perceived value and expected use

Interestingly, the results are contrary to hypothesized expectations, as the facilitating conditions moderator was expected to have a positive effect on the relationships in all three cases. However, in two out of three cases the expected use is higher with lower facilitating conditions. This could be explained by the fact that facilitating conditions mainly rely on other contextual variables such as compatibility and behavioral control, which should not be ignored while interpreting the relevant results (Ghazizadeh et al., 2012).

Overall, this research model extends the existing literature on the adoption of digital data sharing. In particular, the study provides a conceptual model that assesses the expected use of DDWS under the influence of various factors, especially perceived benefits and risks. Theoretically, the proposed model integrates variables from the UTAUT2 model with variables from the privacy calculus model and fuses them into a single model to better understand end users' usage intentions of DDWs in conjunction with their underlying privacy concerns along with the resulting actual behavior. This study provides clear implications for the design and communication of future DDWs based on the privacy aspect by illuminating its statistically significant expected use by a wide range of population in terms of age, gender, education and socio-economic background.

6.2. Practical Implications

The stated findings have practical implications which imply that the strategies to uphold DDWs should augment the users' interest in the usage of DDWs through mass promotion of their advantages. In this regard, authorities should advertise the ways to avoid security risks and hazards among potential users, in order to enhance wide-scale adoption of DDWs. They should also prevent users' concerns regarding privacy through active simulation of DDWs usage and functionality of security systems work to safeguard the data as well as privacy of users. Most people are intimidated at first when it comes to new, digital technologies and above all do not acquire the knowledge about such topics themselves. However, the underlying reason why it is extremely important to invest into gaining technological understanding among the population, because otherwise the entire concept of DDWs will not succeed. This technology depends on its ecosystem, in other words, only once a sufficient number of issuers who issue credentials is reached along with an even larger amount of verifiers who offer use cases, will users take advantage of it. Even if perceived risks do not directly influence the expected use of DDWs, they do influence perceived value, which in turn influences expected use. Therefore, it is of great importance to raise people's awareness regarding the fact that this technology is more secure than anything we currently know when it comes to identity management systems.

6.3. Limitations and Recommendations for Future Research

Regardless of the noteworthy contribution of the study and its implications, the study is subject to certain limitations which could serve as potential research arenas for future researchers in the similar field. First, the study has been constrained in terms of its geographical location since it has been conducted in a small country, specifically Austria. Future researchers could extend a similar model and research context in other geographical areas in order to test the generalizability of the presented results. Second, a mono-method quantitative research methodology has been adopted in the study in order to address the core research questions. However, qualitative approaches solely or in amalgamation with quantitative ones could offer rich data and additionally useful insights in order to study the presented research issue. Therefore, future researchers are recommended to include exploratory aspects in a similar context to address the research questions in a subjective as well as comprehensive manner. Third, given the geographic profile of study respondents, the findings of the study could have been skewed considering that a vast majority of respondents were middle aged (ages 25 – 47), unemployed or lacking higher education such as bachelor's degree and above. There is a plausible assertion that average population might hold distinct perceptions and behaviors regarding the adoption of digital data wallets which might result in diverse findings of the study. Further research could be extended upon the research issue with the data collection from a target audience which is

employed and highly educated. Last, as addressed above, up to now no definite explanation for the privacy paradox has been found. Nevertheless, a multitude of possible explanations, whether theoretical or the development of comprehensive models, that shed more light on the dichotomy between privacy attitudes, concerns, or perceived risk and privacy behaviors. Therefore, further research could explore the explicit cause of the presented privacy paradox for this study.

7. CONCLUSION

The main focus of this paper is to examine the key factors influencing the expected adoption of DDWs, with an emphasis on exploring general elements that influence customer adoption of DDWs, as well as the risks, challenges, and concerns associated with the use of these decentralized identity management systems. For the sake of providing the most holistic possible understanding, variables from the UTAUT2 model as well as variables from the privacy calculus theory were joined and merged into a single model. In order to address the research objectives, a quantitative research study has been conducted where the primary data has been assessed in terms of partial least squares structural equation modelling. The research sought to understand the antecedents of digital data wallets adoption in Austria as well as the associated privacy concerns of potential users. Findings of the study signified the privacy concerns of study participants in terms of security concerns, financial risks and identity theft associated with DDWs. Most of the research findings have been found in line with the extant literature. However, some rejected relationships were identified, which, in the case of the influence of perceived risks on expected use, may be explained by the so-called privacy paradox and would require further investigation. In other cases, such as social influence and habit, it is likely that the respondents encountered difficulties in assessing the questions since they had no previous exposure to the technology. In a nutshell, the research highlighted the sensitivity of privacy concerns, interestingly not halting the adoption of DDWs as well as antecedents of perceived benefits and value which enhance the expected use of DDWs.

BIBLIOGRAPHICAL REFERENCES

Ain, N., Kaur, K., & Waheed, M. (2016). The influence of learning value on learning management system use: An extension of UTAUT2. *Information Development*, *32*(5), 1306–1321. https://doi.org/10.1177/0266666915597546

Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: Empowering creative and extrarole performance. *Journal of Applied Psychology*, *91*(1), 221–232.

Alkhowaiter, W. A. (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review. *International Journal of Information Management*, *53*.

Becker, J.-M., Cheah, J.-H., Gholamzade, R., Ringle, C. M., & Sarstedt, M. (2023). PLS-SEM's most wanted guidance. *International Journal of Contemporary Hospitality Management*, *35*(1), 321–346.

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an antecedents–privacy concerns–outcomes model. *Journal of Information Science*, *43*(5), 583–600.

Chávez Herting, D., Cladellas Pros, R., & Castelló Tarrida, A. (2020). Habit and social influence as determinants of PowerPoint use in higher education: A study from a technology acceptance approach. *Interactive Learning Environments*, *31*(1), 497–513.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*, 181–202.

Cheng, X., Su, L., Luo, X., Benitez, J., & 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*, *31*(3), 339–363.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly*, *22*(1), 1–8.

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy concerns and data sharing in the internet of things: Mixed methods evidence from connected cars. *MIS Quarterly*, *45*(4), 1863–1891.

Collier, J. E., & Kimes, S. E. (2013). Only if it is convenient: Understanding how convenience influences self-service technology evaluation. *Journal of Service Research*, *16*(1), 39–51.

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

Duan, S. X., & Deng, H. (2022). Exploring privacy paradox in contact tracing apps adoption. *Internet Research*, *32*(5), 1725–1750.

Fernández Robin, C., McCoy, S., & Yáñez, D. (2016). Surfing the social networks. *Social Computing and Social Media*, *8*, 279–286.

Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, *115*(9), 1704–1723.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261.

Ghazizadeh, M., Lee, J. D., & Boyle, L. N. (2012). Extending the technology acceptance model to assess automation. *Cognition, Technology & Work*, *14*, 39–49.

Guenther, P., Guenther, M., Ringle, C. M., Zaefarian, G., & Cartwright, S. (2023). Improving PLS-SEM use for business marketing research. *Industrial Marketing Management*, *111*, 127–142.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*, 115–135.

Hossain, M. A., Hasan, M. I., Chan, C., Ahmed, J. U., & others. (2017). Predicting user acceptance and continuance behaviour towards location-based services: The moderating effect of facilitating

conditions on behavioural intention and actual use. *Australasian Journal of Information Systems*, *21*.

Jaspers, E. D., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research*, *142*, 255–265.

Jordan, G., Leskovar, R., & Marič, M. (2018). Impact of fear of identity theft and perceived risk on online purchase intention. *Organizacija*, *51*(2), 146–155.

Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, *107*.

Jung, I., & Lee, J. (2020). A cross-cultural approach to the adoption of open educational resources in higher education. *British Journal of Educational Technology*, *51*(1), 263–280.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173.

Kim, H.-W., Chan, H. C., & Gupta, S. (2007). Value-based adoption of mobile internet: An empirical investigation. *Decision Support Systems*, *43*(1), 111–126.

Kim, M., Kim, Y., & Lee, G. (2023). Effect of situational factors (control, convenience, time pressure, and order complexity) on customers' self-service technology choices. *Journal of Hospitality Marketing & Management*, *32*(5), 649–669.

Kleijnen, M., De Ruyter, K., & Wetzels, M. (2007). An assessment of value creation in mobile service delivery and the moderating role of time consciousness. *Journal of Retailing*, *83*(1), 33–46.

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

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Die Rolle der Kultur in der Selbstoffenbarung und Privatsphäre in sozialen Onlinenetzwerken. *Wirtschaftsinformatik*, 1–11.

Lallmahomed, M. Z., Lallmahomed, N., & Lallmahomed, G. M. (2017). Factors influencing the adoption of e-Government services in Mauritius. *Telematics and Informatics*, *34*(4), 57–72.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42.

Lee, N., & Kwon, O. (2015). A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. *Expert Systems with Applications*, *42*(5), 2764–2771.

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, *88*, 8–17.

Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems*, *4*(1), 65–97.

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, *47*, 120–130.

Nikou, S., & Bouwman, H. (2013). The diffusion of mobile social network service in China: The role of habit and social influence. *2013 46th Hawaii International Conference on System Sciences*, 1073–1081.

Oliveira, T., & Martins, M. F. (2011). Information technology adoption models at firm level. *The Electronic Journal Information Systems Evaluation*, *14*(1), 110–121.

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, *61*, 404–414.

Preukschat, A., & Reed, D. (2021). *Self-sovereign identity: Decentralized digital idenentity and verifiable credentials*. Manning Publications.

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299–1323.

Ramírez-Correa, P. E., Rondán-Cataluña, F. J., & Arenas-Gaitán, J. (2014). An empirical analysis of mobile Internet acceptance in Chile. *Information Research*, *19*(3), 19–3.

Ross, W., & LaCroix, J. (1996). Multiple meanings of trust in negotiation theory and research: A literature review and integrative model. *International Journal of Conflict Management*, *7*(4), 314–360.

Ruff, T. (2018). *The three models of digital identity relationships*. Evernym. https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186

Sandhu, R. K., Vasconcelos-Gomes, J., Thomas, M. A., & Oliveira, T. (2023). Unfolding the popularity of video conferencing apps – A privacy calculus perspective. *International Journal of Information Management*, *68*. https://doi.org/10.1016/j.ijinfomgt.2022.102569

Sartor, S., Sedlmeir, J., & Rieger, A. (2022). *Love at first sight? A user experience study of self-sovereign identity wallets*. Thirtieth European Conference on Information Systems.

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, *63*(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y

Segura, A. S., & Thiesse, F. (2015). Extending UTAUT2 to explore pervasive information systems. *European Conference on Information Systems*, *23*.

Shaw, N., Eschenbrenner, B., & Brand, B. M. (2022). Towards a mobile app diffusion of innovations model: A multinational study of mobile wallet adoption. *Journal of Retailing and Consumer Services*, *64*.

Shaw, N., & Sergueeva, K. (2016). Convenient or useful? Consumer adoption of smartphones for mobile commerce. *Diffusion Interest Group in Information Technology*.

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management*, *45*, 44–55.

Sipior, J. C., Ward, B. T., Connolly, R., & MacGabhann, L. (2013). Privacy in online social networking: Applying a privacy calculus model. *Pacific Asia Conference on Information Systems (PACIS)*.

Sporny, M., Longely, D., & Chadwick, D. (2019). Verifiable credentials data model 1.0: Expressing verifiable information on the web. *World Wide Web Consortium (W3C)*. https://www.w3.org/TR/2019/REC-vc-data-model-20191119/

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278–292.

Tamilmani, K., Rana, N. P., Wamba, S. F., & Dwivedi, R. (2021). The extended unified theory of acceptance and use of technology (UTAUT2): A systematic literature review and theory evaluation. *International Journal of Information Management*, *57*. https://www.sciencedirect.com/science/article/pii/S0268401220314687

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society*, *3*(1), 1–13.

Utomo, P., Kurniasari, F., & Purnamaningsih, P. (2021). The effects of performance expectancy, effort expectancy, facilitating condition, and habit on behavior intention in using mobile healthcare application. *International Journal of Community Service & Engagement*, *2*(4), 183–197.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.2307/41410412

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531–542.

Wang, X., Wang, Y., Lin, X., & Abdullat, A. (2021). The dual concept of consumer value in social media brand community: A trust transfer perspective. *International Journal of Information Management*, *59*, 102319.

Wang, Y., Lo, H.-P., & Yang, Y. (2004). An integrated framework for service quality, customer value, satisfaction: Evidence from China's telecommunication industry. *Information Systems Frontiers*, *6*(4), 325–340.

Warshaw, J., Matthews, T., Whittaker, S., Kau, C., & Bengualid, M. (2015). Can an algorithm know the "real you"?: Understanding people's reactions to hyper-personal analytics systems. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 797–806.

Weinhard, A., Hauser, M., & Thiesse, F. (2017). Explaining adoption of pervasive retail systems with a model based on UTAUT2 and the extended privacy calculus. *PACIS 2017 Proceedings*, *217*.

Wilson, D., Proudfoot, J., & Valacich, J. (2014). Saving face on Facebook: Privacy concerns, social benefits, and impression management. *Behaviour & Information Technology*, *37*(1), 16–37.

Wilson, D., & Valacich, J. (2012). *Unpacking the privacy paradox: Irrational decision-making within the privacy calculus*. Thirty Third International Conference on Information Systems.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*(3), 135–174.

Yang, Y., Liu, Y., Li, H., & Yu, B. (2015). Understanding perceived risks in mobile payment acceptance. *Industrial Management & Data Systems*, *115*(2), 253–269.

APPENDIX

APPENDIX A – ITEMS

Construct		Item	Author
Performance Expectancy		PE1. I find that digital data wallet could be useful in my daily life.	(Venkatesh et al., 2012)
		PE2. Using digital data wallet could increase my chances of achieving things that are important to me.	
		PE3. Using digital data wallet could help me accomplish things more quickly.	
		PE4. Using digital data wallet could increase my productivity.	
Effort Expectancy		EE1. Learning how to use digital data wallet could be easy for me.	(Venkatesh et al., 2012)
		EE2. My interaction with digital data wallet could be clear and understandable.	
		EE3. I find digital data wallet could be easy to use.	
		EE4. It could be easy for me to become skillful at using digital data wallet.	
Social Influence		SI1. People who are important to me think that I should use digital data wallet.	(Venkatesh et al., 2012)
		SI2. People who influence my behavior think that I should use digital data wallet.	
		SI3. People whose opinions I value prefer that I use digital data wallet.	
Hedonic Motivation		HM1. Using digital data wallet could be fun.	(Venkatesh et al., 2012)
		HM2. Using digital data wallet could be enjoyable.	
		HM3. Using digital data wallet could be very entertaining.	
Facilitating Conditions		FC1. I have the resources necessary to use digital data wallet.	(Venkatesh et al., 2012)
		FC2. I have the knowledge necessary to use digital data wallet.	
		FC3. Digital data wallet would be compatible with other technologies I use.	
		FC4. I could get help from others when I have difficulties using digital data wallet.	
Price Value		PV1. Digital data wallet could be reasonably priced.	(Venkatesh et al., 2012)
		PV2. Digital data wallet could be a good value for the money.	
		PV3. Digital data wallet could provide a good value.	
Habit		HT1. The use of digital data wallet could become a habit for me.	(Venkatesh et al., 2012)
		HT2. I could become addicted to using digital data wallet.	
		HT3. I must use digital data wallet in the future.	
		HT4. Using digital data wallet could become natural to me.	
Privacy Control (second order)	Information gathering control	IGC1. I would be comfortable if digital data wallet collects my personal information that I would like to keep private.	(Cheng et al., 2021)
		IGC2. I believe that the digital data wallet will allow me to determine the type of information it stores about me.	
		IGC3. I believe I will be able to prevent digital data wallet from collecting personal information about me that I want to keep from them.	(Alge et al., 2006)
	Information handling control	IHC1. Digital data wallet will respect my right to control who can see my personal information.	(Cheng et al., 2021)
		IHC2. Digital data wallet will allow me to decide how my personal information can be released to others.	
		IHC3. I believe I will be able to control how digital data wallet uses my personal information.	
Data security		DS1. I am critical about how data security will be embedded in digital data wallet.	(Cichy et al., 2021)
		DS2. I believe that hackers may easily access personal data from digital data wallet.	
		DS3. I doubt that personal data could be secured from unauthorized access in digital data wallet.	
		DS4. I believe that digital data wallet will pose a real risk to the protection of personal data.	
Convenience		Con1. Providing identification information by using digital data wallet would allow me to save time.	(Cheng et al., 2021)
		Con2. Providing identification information by using digital data wallet would be convenient for me.	
		Con3. Providing identification information by using digital data wallet would give me a convenient way to travel, shopping, paying taxes, etc.	
Financial risks		FR1. Providing my identification information by using digital data wallet would make me lose money.	(Cheng et al., 2021)
		FR2. Providing identification information by using digital data wallet would subject my bank account to potential fraud.	
		FR3. Providing my identification information by using digital data wallet would lead to a financial loss for me.	
Identity theft		IdT1. Providing identification information by using digital data wallet would make my identification information to be illegally used by others.	(Cheng et al., 2021)
		IdT2. Providing identification information by using digital data wallet would lead to unauthorized charges on my bank or credit card account.	
		IdT3. Somebody will use my identity for criminal purposes if I provide my identification information to digital data wallet.	
Perceived Benefits		PB1. Providing my personal information to digital data wallet would entail benefits for me.	(Kehr et al., 2015)
		PB2. Revealing my personal information to digital data wallet would help me obtain the services I want.	
		PB3. I believe that as a result of my personal information disclosure, I would benefit from saving time.	

Perceived Risks	PR1. It would be risky to give personal information to digital data wallet.	(Kehr et al., 2015)
	PR2. There would be high potential for privacy loss associated with giving personal information to digital data wallet.	
	PR3. Personal information could be inappropriately used by using digital data wallet.	
	PR4. Providing the digital data wallet with my personal information could involve many unexpected problems.	
Overall Trust	Tr1. Digital data wallet could represent a secure system.	(Duan & Deng, 2022)
	Tr2. I would feel secure providing personal information	
	to digital data wallet.	
	Tr3. I would not worry about the information being used by digital data wallet.	
	Tr4. I trust that digital data wallet would keep my best interests in mind when dealing with (my information).	(Lin et al., 2021)
	Tr5. I believe that digital data wallet will be predictable and consistent regarding the usage of (my information).	
Value	Val.1 Overall, digital data wallets could be value for money.	(Wang et al., 2004)
	Val.2 Digital data wallet could be worth what is given up such as time, energy and effort.	
	Val3. Digital data wallets could be a good choice.	
Expected Use	Please choose your expected usage frequency of the digital data wallet as (Note: Frequency ranged from "never" to "always that I need"):	(Venkatesh et al., 2012)
	a) Passport	
	b) National identification card	
	c) Driver's license	
	d) National health system card	
	e) Certificate of car ownership	
	f) Certificate from university	
	g) Bank account number /credit card	

APPENDIX B – ρ_A and AVE results

Constructs		**Loadings**	**ρA**	**AVE**
Convenience	Con 1	0.956	0.954	0.914
	Con 2	0.955		
	Con 3	0.958		
Security Concerns	DS1	0.873	0.909	0.779
	DS2	0.905		
	DS3	0.854		
	DS4	0.897		
Effort Expectancy	EE1	0.915	0.934	0.821
	EE2	0.937		
	EE3	0.838		
	EE4	0.929		
Facilitating Conditions	FC1	0.925	0.923	0.839
	FC2	0.901		
	FC3	0.921		
Financial Risk	FR1	0.831	0.869	0.744
	FR2	0.873		
	FR3	0.883		
Habit	H1	0.915	0.888	0.689
	H3	0.831		
	H4	0.944		
Hedonic Motivation	HM1	0.947	0.911	0.841
	HM2	0.917		
	HM3	0.886		
Information Gathering Control	IGC2	0.920	0.829	0.741
	IGC3	0.923		
Information Handling Control	IHC2	0.956	0.925	0.869
	IHC3	0.954		
Identity Theft	IT1	0.935	0.925	0.866
	IT2	0.916		
	IT3	0.941		
Perceived Benefits	PB1	0.939	0.931	0.879
	PB2	0.944		

	PB3	0.931		
	PR1	0.939		
Perceived Risks	PR2	0.958	0.955	0.877
	PR3	0.924		
	PR4	0.925		
	SI1	0.954		
Social Influence	SI2	0.957	0.955	0.917
	SI3	0.961		
	Trust1	0.895		
	Trust2	0.924		
Trust	Trust3	0.867	0.947	0.824
	Trust4	0.928		
	Trust5	0.922		
	Val1	0.945		
Perceived Value	Val2	0.959	0.54	0.911
	Val3	0.959		

APPENDIX C – Heterotrait-Monotrait ratio

Variables	Con	DS	EE	FC	FR	H	HM	IGC	IHC	IT	PB	PR	SI	Tr	Val
Convenience															
Security Concerns	0.305														
Effort Expectancy	0.603	0.172													
Facilitating Condition	0.619	0.227	0.824												
Financial Risk	0.307	0.522	0.334	0.255											
Habit	0.766	0.369	0.678	0.707	0.275										
Hedonic Motivation	0.687	0.327	0.652	0.644	0.282	0.861									
Info Gathering Control	0.610	0.370	0.442	0.462	0.373	0.658	0.628								
Info Handling Control	0.669	0.389	0.500	0.528	0.378	0.724	0.696	0.939							
Identity Theft	0.218	0.591	0.235	0.219	0.825	0.238	0.190	0.246	0.284						
Perceived Benefits	0.705	0.393	0.422	0.519	0.390	0.685	0.567	0.646	0.647	0.332					
Perceived Risk	0.313	0.715	0.174	0.249	0.606	0.380	0.340	0.388	0.427	0.623	0.481				
Social Influence	0.427	0.379	0.340	0.436	0.194	0.599	0.628	0.528	0.554	0.195	0.441	0.413			
Trust	0.669	0.561	0.488	0.531	0.495	0.743	0.671	0.715	0.743	0.431	0.774	0.600	0.552		
Perceived Value	0.777	0.399	0.580	0.577	0.402	0.827	0.746	0.675	0.733	0.316	0.743	0.440	0.473	0.851	