

Association for Information Systems

AIS Electronic Library (AISeL)

AMCIS 2024 Proceedings

Americas Conference on Information Systems
(AMCIS)

August 2024

What Makes You Trust Digital Data Wallets? The Role of Platform Mechanisms on Trust Formation

Varvara Keba

Universidade NOVA de Lisboa, vkeba@novaims.unl.pt

Gurpreet Dhillon

IT and Decision Sciences, gurpreet.dhillon@unt.edu

Tiago Oliveira

NOVA Information Management School (NOVA IMS), toliveira@novaims.unl.pt

Ronnie Das

Audencia Business School, rdas@audencia.com

Melanie Trabandt

Audencia Business School, mtrabandt@audencia.com

Follow this and additional works at: <https://aisel.aisnet.org/amcis2024>

Recommended Citation

Keba, Varvara; Dhillon, Gurpreet; Oliveira, Tiago; Das, Ronnie; and Trabandt, Melanie, "What Makes You Trust Digital Data Wallets? The Role of Platform Mechanisms on Trust Formation" (2024). *AMCIS 2024 Proceedings*. 10.

<https://aisel.aisnet.org/amcis2024/adoptdiff/adoptdiff/10>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2024 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

What Makes You Trust Digital Data Wallets? The Role of Platform Mechanisms on Trust Formation

Emergent Research Forum (ERF) Paper

Varvara Keba

NOVA Information Management
School, Universidade NOVA de Lisboa
vkeba@novaims.unl.pt

Gurpreet Dhillon

University of North Texas
gurpreet.dhillon@unt.edu

Tiago Oliveira

NOVA Information Management
School, Universidade NOVA de Lisboa
toliveira@novaims.unl.pt

Ronnie Das

Department of Marketing, Audencia
Business School
rdas@audencia.com

Mélanie Trabant

Department of Marketing, Audencia Business School
mtrabant@audencia.com

Abstract

Digital data wallets are user-centric platforms that enable users to control their privacy online. The relationship between trust and digital data wallets remains unclear. This study aims to examine factors that influence different trust targets. We constructed the research model based on a mixed methods approach. The qualitative study is used to identify antecedents of each trust target. We built the research model based on the network of trust model and the qualitative study results. The model will then be tested with data from three European countries - Austria, Romania, and Spain.

Keywords

Digital data wallet, privacy-enhancing technology, trust network, mixed-methods approach.

Introduction

Obtaining personal information has become easier because of the perpetual burgeoning of tools, services, and apps that require increasing volumes of personally identifiable information (Silva et al. 2022). A recent survey found that it is too difficult for 79% of worldwide consumers to understand how companies use their data (CISCO 2022). Consequently, the aggregation of personal information online raises numerous privacy concerns (Davidson et al. 2023). Nevertheless, there still remains a low level of adoption of privacy-enhancing technologies and practices (Zou et al. 2020).

Digital data wallets are user-centric personal data management platforms that enable users to control their privacy online (European Commission 2023; SOTERIA 2023). Digital data wallets are a relatively new technological advancement. Therefore, understanding how people form their initial trust is critical for developing trustworthy technologies. Additionally, the requirements of potential users are often overlooked in privacy-enhancing technology development (Bélanger and Crossler 2011). Therefore, the study seeks to answer the following questions: what are the antecedents of different trust targets and how do the antecedents influence the trust targets?

To answer the research questions, we developed the research model based on the network of trust model (Söllner et al. 2016) and the qualitative study. The qualitative study is used to identify the antecedents of different trust targets, which are integrated into the model. The quantitative study will be used to test the research model. The presented research model is not complete. The quantitative study is in progress.

The contributions of the study are fourfold. Firstly, the study contributes to trust literature by identifying the mechanism of trust formation in digital data wallets. Secondly, the study extends the application of the network of trust model in the context of privacy-enhancing technology adoption, specifically digital data wallet adoption. Thirdly, a mixed methods approach is adopted following Venkatesh et al, (2023), allowing the building of a comprehensive framework for forming trust mechanisms in digital data wallets. Finally, the study findings can be used to build reliable relationships with digital data wallet users and providers.

Theoretical background

Privacy-enhancing technologies

Privacy-enhancing technologies are technologies that are designed to reduce unnecessary processing of personal information by limiting information disclosure (Fischer-Hbner and Berthold 2017). Digital data wallets are user-centric personal data management platforms that enable users to control their privacy online while accessing different electronic services (European Commission 2023; SOTERIA 2023). Individuals consider advanced privacy-enhancing technologies and practices complex and untrustworthy (Bracamonte et al. 2022). Lack of trust in privacy-enhancing technologies is regarded as one of the main barriers to adoption (Coopamootoo 2020). Harborth et al, (2020) indicated that trust in privacy-enhancing technologies is the most important factor in explaining behavioral intention. Nevertheless, the relationship between trust and privacy-enhancing technology, like digital data wallets, remains unclear.

Trust

Trust is a psychological state characterized by the readiness to accept vulnerability in exchange for positive expectations (McKnight et al. 2002). Söllner et al, (2016) developed a network of trust model to examine the various trust relationships, which includes five different targets of trust, specifically the user, the information system, the internet, the provider, and the community of internet users. Different trust targets have been examined in the literature in various contexts. Although different trust targets are studied in the literature, most research focuses on the mediation role of trust targets or considers them the antecedents of behavioral intention (e.g. Shao et al. 2022, Kuen et al. 2023, Gan and Lau 2024). Since trust is one of the key predictors of technology use (Li et al. 2008), the main focus of the study is to explore trust formation in digital data wallets by examining the antecedents of different trust targets.

Mixed methods design approach

To answer the research questions, the mixed methods approach is adopted (Venkatesh et al. 2023). The purpose of the study is developmental. Hence, the qualitative study is used to identify antecedents to different trust targets, and the quantitative study will be used to test the research model and hypotheses.

Qualitative Study

The goal of the qualitative study is to identify antecedents of trust targets. The qualitative study enabled us to analyze the requirements of potential users. Thirty interviews were conducted in three European countries, specifically Austria (Central), Romania (Eastern), and Spain (Western Europe), representing the sample of a European Union. The interviews were conducted in the participant's native language. Interviews were conducted until conceptual themes began to repeat, achieving data saturation (Fusch and Ness 2015). We followed an open coding methodology to analyze the data, segmenting data for quotes and associating it with categories.

The qualitative study identified three antecedents of trust targets, specifically transparency, social influence, and safety. Table 1 presents representative quotations. Transparency refers to providing

information about the types of data a company has acquired about them and how that data will be utilized (Dinev et al. 2013). When individuals talk about transparency, they often mention how important it is for websites and online services to operate transparently in general. Transparency empowers individuals to make informed decisions about their online activities. Hence, we consider transparency as an antecedent of trust in the internet. Social influence is defined as the individuals' perception of how important others, such as friends and family, believe that they use the technology (Venkatesh et al. 2012). People tend to trust technology more if other users recommend using it. Nevertheless, a positive recommendation from a close social circle is considered more reliable than a general recommendation regarding new technologies, such as digital data wallets. Safety is the relief from worry over potential crimes or injuries (Yang et al. 2017). Prioritizing safety allows providers to clearly show their commitment to protecting users and earning their trust. To increase trust in the provider, potential users expect that they will offer some safety guarantees.

Categories	Quotes
Transparency	<i>"I think transparency goes together with trustworthiness. To be able to trust, I also want to understand how my data is handled." (Interviewee 21); "because of the transparency, I can have an influence over what happens with it, and I can control it. (Interviewee 24)"; "Well, with many websites, it is not clear what happens with the data; there is no transparency. And it is not clear what kind of data is being processed, and that doesn't provide a comfortable feeling." (Interviewee 28).</i>
Social influence	<i>"I would for sure look for reviews and experiences of others regarding this platform. I would read more about it on the internet." (Interviewee 8); "If they [DDW providers] have very good reviews from other people, I may give it a go and try" (Interviewee 19); "If my friends or parents or someone told me that it was very good, I would use it the truth." (Interviewee 14).</i>
Safety	<i>"I would definitely before giving any money to that company, I would need to do my research, is it safe, is it reliable, is it a scam, or not." (Interviewee 2); "I am unsure if I would use something like this, just because I am missing the security and guarantee that it is safe." (Interviewee 11); "Although at the same time you are aware that more and more attacks to big companies are becoming more and more present and therefore the possibility that your data or your information is not safe there is greater." (Interviewee 18).</i>

Table 1. Representative quotations

Research Model and Hypotheses Development

Figure 1 presents the research model. The model is built based on the qualitative study results and the network of trust model. The presented model is not complete and will be tested in the quantitative study.

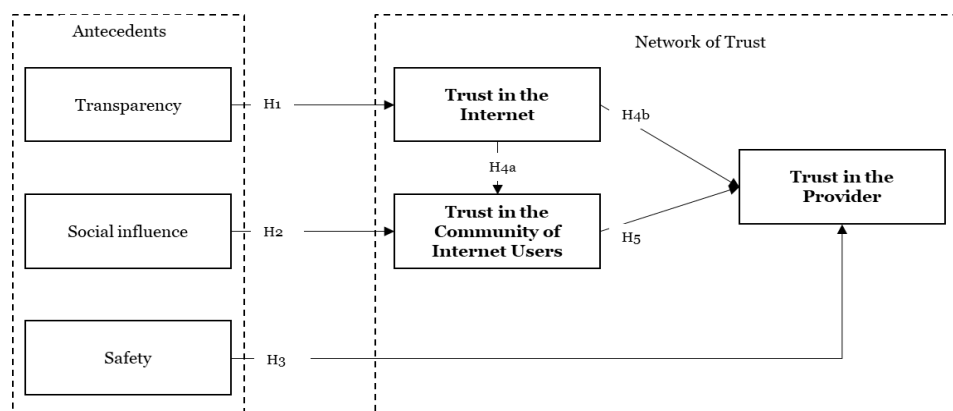


Figure 1. Research model

Previous literature suggests that transparency increases trust (Esmaeilzadeh 2020). Trust in the internet refers to users' perception that the internet is a safe environment (Söllner et al. 2016). We argue that if digital data wallets transparently inform their users about handling information online, individuals will consider the digital environment safer and increase their trust in the internet. One respondent affirms the argument: *"I think transparency goes together with trustworthiness. To be able to trust, I also want to understand how my data is handled."* (Interviewee 21). Therefore, it is hypothesized:

H1: Transparency will positively influence trust in the internet.

Social influence is a significant factor in explaining both initial trust formation and technology adoption (Zhang et al. 2020; Venkatesh et al. 2012). Trust in the community of the internet users refers to the ability to rely on suggestions from other online users (Söllner et al. 2016). Since digital data wallets are innovative technologies, recommendations from close social circles can enhance the recommendations of other users. One respondent emphasized: *"If my friends or parents or someone told me that it was very good, I would use it the truth."* (Interviewee 14). Therefore, it is hypothesized:

H2: Social influence will positively influence trust in the community of internet users.

Safety is often considered a priority by users (Cheng et al. 2021). Trust in a provider refers to the confidence placed in individuals or organizations responsible for the usefulness of an information system (Söllner et al. 2016). We argue that if digital data wallets protect personal information and provide a safe environment for information sharing, users' trust in the provider will increase. One respondent affirms the argument: *"I would definitely before giving any money to that company, I would need to do my research, is it safe, is it reliable, is it a scam, or not."* (Interviewee 2). Therefore, it is hypothesized:

H3: Safety will positively influence trust in the provider.

According to Söllner et al, (2016), if individuals trust in the internet as the environment, they will be more likely to consider other targets trustworthy, including trust in the community of internet users and trust in the provider. We also argue that if potential users trust recommendations from the internet community, their trust in the provider will also increase. Therefore, it is hypothesized:

H4a (b): Trust in the internet will positively influence trust in the community of internet users (trust in the provider).

H5: Trust in the community of internet users will positively influence trust in the provider.

Acknowledgements

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

REFERENCES

- Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35), JSTOR, pp. 1017–1041.
- Bracamonte, V., Pape, S., and Loebner, S. 2022. "All Apps Do This': Comparing Privacy Concerns towards Privacy Tools and Non-Privacy Tools for Social Media Content," *Proceedings on Privacy Enhancing Technologies* (3), pp. 57–78.
- Cheng, X., Su, L., Luo, X., Benitez, J., and Cai, S. 2021. "The Good, the Bad, and the Ugly: Impact of Analytics and Artificial Intelligence-Enabled Personal Information Collection on Privacy and Participation in Ridesharing," *European Journal of Information Systems* (31:3), Taylor & Francis, pp. 1–25.
- CISCO. 2022. "Data Transparency's Essential Role in Building Customer Trust." (https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf).
- Coopamootoo, K. P. L. 2020. "Usage Patterns of Privacy-Enhancing Technologies," in *Proceedings of the*

- 2020 ACM SIGSAC Conference on Computer and Communications Security, pp. 1371–1390.
- Davidson, E., Wessel, L., Winter, J. S., and Winter, S. 2023. “Future Directions for Scholarship on Data Governance, Digital Innovation, and Grand Challenges,” *Information and Organization* (33:1), Elsevier, p. 100454.
- Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. “Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts,” *European Journal of Information Systems* (22:3), Springer, pp. 295–316.
- Esmaeilzadeh, P. 2020. “The Impacts of the Privacy Policy on Individual Trust in Health Information Exchanges (HIEs),” *Internet Research* (30:3), Emerald Publishing Limited, pp. 811–843.
- European Commission. 2023. “European Digital Identity.” (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en, accessed June 2, 2023).
- Fischer-Hbner, S., and Berthold, S. 2017. “Privacy-Enhancing Technologies,” in *Computer and Information Security Handbook*, Elsevier, pp. 759–778.
- Fusch, P. I., and Ness, L. R. 2015. “Are We There yet? Data Saturation in Qualitative Research,” *The Qualitative Report* (20:9), pp. 1408–1416.
- Gan, Q., and Lau, R. Y. K. 2024. “Trust in a ‘Trust-Free’ System: Blockchain Acceptance in the Banking and Finance Sector,” *Technological Forecasting and Social Change* (199), Elsevier, p. 123050.
- Harborth, D., Pape, S., and Rannenberg, K. 2020. “Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym,” *Proceedings on Privacy Enhancing Technologies* (202:2), pp. 111–128.
- Kuen, L., Westmattmann, D., Bruckes, M., and Schewe, G. 2023. “Who Earns Trust in Online Environments? A Meta-Analysis of Trust in Technology and Trust in Provider for Technology Acceptance,” *Electronic Markets* (33:1), Springer, p. 61.
- Li, X., Hess, T. J., and Valacich, J. S. 2008. “Why Do We Trust New Technology? A Study of Initial Trust Formation with Organizational Information Systems,” *The Journal of Strategic Information Systems* (17:1), Elsevier, pp. 39–71.
- McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. “The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model,” *The Journal of Strategic Information Systems* (11:3–4), Elsevier, pp. 297–323.
- Shao, Z., Zhang, L., Brown, S. A., and Zhao, T. 2022. “Understanding Users’ Trust Transfer Mechanism in a Blockchain-Enabled Platform: A Mixed Methods Study,” *Decision Support Systems* (155), Elsevier, p. 113716.
- Silva, P., Gonçalves, C., Antunes, N., Curado, M., and Walek, B. 2022. “Privacy Risk Assessment and Privacy-Preserving Data Monitoring,” *Expert Systems with Applications* (200), Elsevier, p. 116867.
- Söllner, M., Hoffmann, A., and Leimeister, J. M. 2016. “Why Different Trust Relationships Matter for Information Systems Users,” *European Journal of Information Systems* (25:3), Taylor & Francis, pp. 274–287.
- SOTERIA. 2023. “SOTERIA, User-Friendly Secured Personal Data Management Platform.” (<https://www.soteria-h2020.eu/>, accessed June 5, 2023).
- Venkatesh, V., Brown, S., and Sullivan, Y. 2023. *Conducting Mixed-Methods Research*, Virginia Tech Publishing.
- Venkatesh, V., Thong, J. Y. L., and Xu, X. 2012. “Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology,” *MIS Quarterly* (36), JSTOR, pp. 157–178.
- Zhang, T., Tao, D., Qu, X., Zhang, X., Zeng, J., Zhu, Haoyu, and Zhu, Han. 2020. “Automated Vehicle Acceptance in China: Social Influence and Initial Trust Are Key Determinants,” *Transportation Research Part C: Emerging Technologies* (112), Elsevier, pp. 220–233.
- Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., and Schaub, F. 2020. “Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices,” in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–15.