The Influence of Privacy Concerns on Cryptocurrency Acceptance

Peter Hamm[1[0000−0003−3501−3525]], Sebastian Pape[1[0000−0002−0893−7856]], and Kai Rannenberg[1]

Goethe University Frankfurt, Frankfurt, Germany peter.hamm@m-chair.de

Abstract. Despite the hype, cryptocurrencies have to far failed to establish themselves as a means of payment for everyday transactions, spawning a wealth of research into acceptance factors and obstacles for cryptocurrency adoption. Our paper adds to this literature by investigating the role of organizational privacy concerns and risk perceptions on cryptocurrency acceptance. Employing a representative survey of German e-commerce users with 257 respondents we find that while risk perceptions and concerns about data collection do affect adoption willingness for cryptocurrencies, neither are useful for predicting actual adoption behavior. This is especially notable since the lack of central counterparties that may steal funds or personal data was one of the original motivations for the creation of the first cryptocurrencies. Our results provide insight into the nature of cryptocurrency adoption and highlights a discrepancy between intention and behavior.

Keywords: Cryptocurrencies · Technology adoption · Concern for information privacy.

1 Introduction

When first appearing on the scene, cryptocurrencies such as Bitcoin were hailed as a revolutionary technology that could transform the financial industry by obviating the need for trusted central counterparties [46]. However, in spite of the hype, Bitcoin and other cryptocurrencies have so far failed to establish themselves as a tool for everyday payments [26], with most use limited to investment purposes [17], as well as some for illicit activities [16]. The extant literature identified perceived risk, trust, as well as lack of self-efficacy as core reasons for this [1, 33, 48, 49]. This is notable, since an important part of the original justification for Bitcoin and other cryptocurrencies was the lack of central counterparties that one would need to trust [36]. Against this backdrop, we want to investigate how privacy concerns specifically towards online entities affect cryptocurrency adoption as a payment system, due to these concerns being a raison d'être for cryptocurrencies in the first place. These concerns have received little attention in the cryptocurrency adoption literature, even though they have been shown to be of high importance for similar technologies such as electronic [35, 37] and mobile payments [34, 54], as well as for the burgeoning area of central bank digital currencies [44]. We aim help closing this research gap by answering the following research questions:

RQ1 How do risk perception and organizational privacy concerns affect the adoption willingness for cryptocurrencies?
RQ2 How do risk perception and organizational privacy concerns affect the adoption behavior for cryptocurrencies?

2 Background

2.1 Privacy Concerns

Privacy has long been a topic of discussion and research, with a myriad of definitions given. As far back as 1890, Brandeis and Warren [6] defined privacy as an inherent “right to be left alone”. Later, Westin [51] defined privacy more narrowly as the right to prevent the disclosure of personal information, and identified the issue of privacy concerns. Due to privacy itself being a multifaceted variable that may be impossible to measure directly, privacy concerns offer a useful proxy for privacy issues, and have emerged as the central construct in most empirical research work on the topic [41], although other terms such as “privacy beliefs” or “privacy attitudes” are sometimes used as well [53]. The importance of privacy concerns in e-commerce and internet services is well established [11, 28, 45, 50].

Probably the first very popular instrument to measure privacy concerns in an e-commerce setting was the *Concern for Information Privacy (CFIP)* construct [42], which focuses on organizational information privacy practices and has proven itself as a reliable measure of individual privacy concerns in past studies [43]. The instrument employs four sub-scales: *collection*, which covers concerns about the scale of data collected and stored, *unauthorized secondary use*, which covers use of the data for purposes not originally intended and agreed for, *errors* covering concerns about intentional or unintentional errors in the stored data, and *improper access*, which encapsulates the concern that individuals not authorized to view the data may still access it [42]. A further development is the *Internet Users' Information Privacy Concerns (IUIPC)* [30], which is a more complex second-order construct that has found use for modelling human factors in privacy enhancing technologies [18, 22]. More recently, the *Antecedents. Privacy Concerns, Outcomes* or *APCO* model [41] introduced a full causal model incorporating a number of antecedents as well as outcome variables such as trust and behavioral reactions.

Due to the organizational focus of our research question, we will employ the *CFIP* as we consider it to be the most appropriate measure for our study.

2.2 Acceptance of Cryptocurrencies

The adoption of technologies has long been a lively area of research [10, 15, 47], and found successful application in areas such as e-commerce and mobile payments [7, 8]. In the area of cryptocurrencies, prior work applied the Technology Acceptance Model (TAM) [10] on Bitcoin, adapting the model by including perceived risks and perceived benefits, finding that the effect of perceived risks on Bitcoin use behavior had both a higher effect size as well as higher statistical significance compared to perceived benefits [1]. Another approach using the TAM but adding perceived trust also found a significant effect of perceived risk on the intention to use cryptocurrencies for C2C e-commerce applications, albeit with a smaller effect size than perceived trust or perceived usefulness [33]. This is in contrast to another study by Arias-Oliva et al. [2], who integrate perceived risk into the UTAUT model [47], but do not find find it to be a statistically significant factor predicting cryptocurrency adoption intention [2]. However, it should be noted that for both aforementioned studies, the operationalization of perceived risk did not consider privacy risk directly. Looking specifically at payment transactions with cryptocurrencies Mashatan et al. found perceived information privacy risk, anonymity, and traceability to significantly affect trust, which in turn had a significant effect on the intention to use crypto-payments, while no significant evidence was found for a role of perceived information security fraud risk [32].

On the influence of privacy perceptions, previous research has found that existing users of Bitcoin tend to rate their concerns as either low or medium [14].

A related topic that has more recently attracted significant attention are central bank digital currencies (CBDC). These currencies, that would enable households to hold central bank money directly without participation of the private financial sector, were first seriously discussed in the form of cryptocurrencies issued by central banks [4], although researchers quickly argued that these currencies will not be true decentralized cryptocurrencies [5]. One large empirical study with more than 1000 respondents concerning a potential digital Euro found that privacy concerns exhibit a negative effect on the willingness to use this currency [44]. The study found a strong effect of soft trust factors (i.e. credibility, image, and security) on both privacy concerns as well as the willingness to use the currency; other significant antecedents of privacy concerns in the digital Euro were perceived vulnerability from the currency, self-efficacy, and general information privacy concerns. Another paper employing the privacy-calculus found evidence that privacy concerns do have a negative influence on the willingness of customers to use a CBDC and thus disclose personal information, although they may still be willing to do so if the offered benefits of this technology outweigh these concerns [24].

3 Methodology

In this section, we briefly cover the development of the questionnaire, the data collection and the research model. We estimate how concerns for information privacy, as defined by the CFIP construct, as well as risk perceptions, affect the willingness to use cryptocurrencies as a means of payment.

3.1 Questionnaire, Data Collection and Ethical Considerations

The data was collected with the support of a panel provider in Germany (certified following the ISO 20252 norm). The survey was implemented with the software LimeSurvey [39] and hosted on a university server. We sampled the participants in a way to achieve a sample representative of German e-commerce users. For that purpose, we set quotas to end up with approximately 50% females and 50% males in the sample as well as a distribution of age following the EUROSTAT2018 census [13]. The Questionnaire was in German. The English translation can be found in the appendix.

The German translation of the concerns for information privacy (CFIP) [42] construct was taken from the work by Harborth and Pape [21], who employed two independent verified translators and verified the validity and reliability of the translation.To measure risk perception, we consider risk to be composed of four items each representing a form of risk identified in previous literature: legal risk [12, 49], market risk [12, 49], counterparty risk [32], and operational risk [29]. We aggregate these by taking the average of the responses. Finally, to gauge adoption willingness, we asked participants if they have made a purchase with Bitcoin or another cryptocurrency in the past, to which they could reply that they have done so, that they have not done so but that they have considered it, or that they did not even consider it.

The participants were informed about the purpose of the study, the storage location and that they stay anonymous unless they reveal their identity within the free texts. Minors were not allowed to participate. This was ensured by our panel provider and an additional information text before our survey. Participants agreed that their data is used for research and consequent publications. The user study was evaluated by the university's ethics board and has been classified as "ethically acceptable".

3.2 Research Model and Hypotheses

To distinguish between *adoption willingness* and *adoption behavior*, we consider the former to include individuals that at least considered using cryptocurrencies in the past, while the latter only includes individuals who have actually done so.

$$\text{adoption willingness} = \begin{cases} 1, & \text{if respondent says they have used} \\ & \quad \text{cryptocurrencies in the past} \\ 1, & \text{if respondent says they have considered} \\ & \quad \text{using cryptocurrencies in the past} \\ 0, & \text{otherwise} \end{cases}$$

$$\text{adoption behavior} = \begin{cases} 1, & \text{if respondent says they have used} \\ & \quad \text{cryptocurrencies in the past} \\ 0, & \text{otherwise} \end{cases}$$

The independent variables are *risk perception (RP)*, and the four CFIP subscales *collection (CO)*, *errors (ER)*, *unauthorized secondary use (US)*, and *improper access (IA)*. As the dependent variables in our dataset are binary, we employ a logistic regression. This type of regression estimates the odds of a random variable being equal to one given a set of independent predictor variables [52, pp. 584–595]. Our general research model is as follows:

$$AW_i = \beta_0 + \beta_1 RP_i + \beta_2 CO_i + \beta_3 ER_i + \beta_4 US_i + \beta_5 IA_i$$
$$AB_i = \beta_0 + \beta_1 RP_i + \beta_2 CO_i + \beta_3 ER_i + \beta_4 US_i + \beta_5 IA_i$$

Where AW_1 are the log-odds, i.e. the logarithm of the odds ratio, for the respondent i to be willing to use cryptocurrencies, and AB_i the corresponding log-odds for them already using the currencies. We further investigate models where we only look at one CFIP-subscale to gauge the importance of the other items on the result.

Risk perception measures the perceived risk of using cryptocurrencies, consisting of legal, market, counterparty and operational risk. The established literature finds strong evidence that perceived risk is a significant obstacle to cryptocurrency adoption [1, 33], thus we hypothesize:

H1a: *Risk perception (RP)* has a negative effect on the likelihood of *adoption willingness* concerning cryptocurrencies.
H1b: *Risk perception (RP)* has a negative effect on the likelihood of *adoption behavior* concerning cryptocurrencies.

The privacy concerns are not directly worded in reference to cryptocurrencies in themselves. That is because decentralized cryptocurrencies are operated algorithmically and at least theoretically do not depend on any specific player who has access to personal data. Thus, we are considering how the perception of privacy risk with online entities influences cryptocurrency adoption. These entities may include players in the cryptocurrency ecosystem such as exchanges, as well as merchants or other entities. As the declared original goal of cryptocurrencies was to obviate the need for trusted third parties [36], privacy concerns should make cryptocurrencies more attractive by removing the need to engage with central counterparties and disclose personal information to them. However, some papers have found positive associations between trust in entities like banks and trust in cryptocurrencies [3], indicating that concerns towards the behavior of involved companies may have a different effect on cryptocurrencies than assumed. Still, as the original justification is theoretically sound and has not consistently been disproven, we hypothesize that:

H2a: Concerns about data collection (CO) have a positive effect on the likelihood of *adoption willingness* concerning cryptocurrencies.
H2b: Concerns about data collection (CO) have a positive effect on the likelihood of *adoption behavior* concerning cryptocurrencies.

H3a: Concerns about *data errors (ER)* have a positive effect on the likelihood of *adoption willingness* concerning cryptocurrencies.

H3b: Concerns about *data errors (ER)* have a positive effect on the likelihood of *adoption behavior* concerning cryptocurrencies.

H4a: Concerns about *unauthorized secondary use (US)* of the data have a positive effect on the likelihood of *adoption willingness* concerning cryptocurrencies.

H4b: Concerns about *unauthorized secondary use (US)* of the data have a positive effect on the likelihood of *adoption behavior* concerning cryptocurrencies.

H5a: Concerns about *improper access (IA)* have a positive effect on the likelihood of *adoption willingness* concerning cryptocurrencies.

H5b: Concerns about *improper access (IA)* have a positive effect on the likelihood of *adoption behavior* concerning cryptocurrencies.

4 Results

This section will describe the statistical results of our analysis. Overall, 257 individuals completed the survey, of which 7 had already used cryptocurrencies, while a further 26 stated that they had at least considered it in the past, leaving 224 individuals who have not even considered doing so. The sample demographics are given in Table 1. The variables *Risk Perception*, *Collection*, *Errors*, *Unauthorized Secondary Use*, and *Improper Access* were computed by taking the average of their corresponding items. None of the resulting variables are normally distributed according to the Shapiro-Wilk-Test [40], with each variable achieving a significance level below 0.0001. Internal consistency was evaluated by employing Cronbach's alpha [9], as shown in table 2. All values are higher than the lower limit of 0.7, thus indicating that the individual items measure the same construct, and below the upper limit of 0.95, indicating that none of the items are redundant [19].

The first step of our analysis was to consider whether risk perception or any of the CFIP items were valued significantly different between demographic groups. For age, we divided the sample according to the median age, which was 41 in our

Table 1: Demographics of our Sample

Education	N	Percent
Lower secondary education (Hauptschulabschluss)	10	3.8%
Secondary school (Realschulabschluss)	70	27.2%
University entrance qualification (Abitur)	79	30.7%
Bachelors' degree	38	14.8%
Masters' degree and equivalent	51	19.8%
PhD and higher	9	3.5%

Age	N	Percent
18 – 29	60	22.3%
30 – 41	71	27.6%
42 – 53	69	26.8%
54 – 65	52	20.2%
66 and older	5	1.9%

Gender	N	Percent
Male	132	51.3%
Female	125	48.6%

Table 2: Internal consistency and Mann–Whitney U tests for population differences

	Cronbach's	Mann–Whitney U tests		
Variable	alpha	Age	Gender	Education
Risk Perception	0.8505	**0.0020**	0.2713	0.3564
Collection	0.8738	**0.0019**	0.5126	0.6527
Errors	0.8969	**0.0380**	0.8674	0.0888
Unauthorized Secondary Use	0.9382	**0.0004**	0.1635	**0.0478**
Improper Access	0.9236	**0.0045**	**0.0065**	0.0580

p - values, bold for $p < 0.05$

sample. Gender distinguished between male and female respondents, while for education we drew a line between respondents holding at least a Bachelor's degree and those that did not. We evaluated this by employing the Mann-Whitney U test, a nonparametric test that evaluates whether the distribution of one random variable is larger than another [31]. The results of this evaluation are given in Table 2.

The results show that respondents younger than the median age of 41 were significantly more concerned about cryptocurrencies, but at the same time significantly less concerned about each of the CFIP subscales. In the case of gender, female respondents exhibited more concern about *Improper Access*, while we see no statistically significant differences otherwise. As for education, respondents without university education were significantly more worried about *Unauthorized Secondary Use*, albeit with a significance level barely below 5%, with *Improper Access* barely missing this threshold, and again with respondents without university education scoring higher on the measure on average.

Finally, we want to consider whether Risk Perception or any of the CFIP scales influence the willingness or the actual decision to adopt cryptocurrencies as payment systems. We first use each concern variable separately before employing a model with all variables together.

The results for the willingness to use cryptocurrencies are given in Table 3. We find a negative effect of *Risk Perception* across all models with a stable coefficient, indicating support for hypothesis *H1a*, i.e. higher risk perceptions lower the odds that a respondent did consider using cryptocurrencies for payments. Among the items indicating privacy concerns, only data *Collection* exhibited statistically significant values in the corresponding simple as well as the full model with the expected positive sign, so we can confirm hypothesis *H2a*, indicating that individuals worried about undue collection of their data by online companies are more likely to consider using cryptocurrencies for payment. We did not find support for an effect for data *Errors*, *Unauthorized Secondary Use*, or *Improper Access* of the data, thus we cannot confirm hypotheses *H3a, H4a*, or *H5a.*

The regression results for actual use behavior are given in Table 4. Here, only *Unauthorized Secondary Use* is statistically significant in the full model. However, it is not significant in the partial models, i.e. those without the other

Table 3: Adoption Willingness on CFIP Subscales and Risk Perception

variable	simple models					full model
const	-0.384	**-2.679***	-1.982	-0.259	0.357	-2.101
	(0.551)	(0.025)	(0.07)	(0.843)	(0.779)	(0.172)
RP	**-0.316***	**-0.361****	**-0.337***	**-0.315***	**-0.311***	**-0.390****
	(0.017)	(0.007)	(0.011)	(0.018)	(0.02)	(0.005)
CO		**0.473***				**0.591***
		(0.017)				(0.012)
ER			0.343			0.37
			(0.069)			(0.073)
US				-0.02		-0.047
				(0.913)		(0.889)
IA					-0.123	-0.422
					(0.502)	(0.186)

$*p < 0.05$, $**p < 0.01$, $***p < 0.001$, p-values in parentheses.

CFIP factors, and the sign is negative, meaning that high concerns about unauthorized secondary use by online companies make it less likely that individuals use cryptocurrencies. Thus, even though the coefficient may be statistically significant, we cannot confirm hypothesis *H4b*. Furthermore, *Risk Perception*, which played a significant role for willingness, does not in turn predict actual use of cryptocurrencies. We thus find no support for hypotheses *H1b, H2b, H3b* or *H5b*.

5 Discussion

Concerning our first research question, we find strong evidence that risk perception towards cryptocurrencies has a significant influence on adoption willingness across all models, indicating that perceived risk stops individuals from even considering to use cryptocurrencies for payments. As for privacy concerns, only worries about data *collection* had a significant influence on adoption willingness, showing that individuals who think that online companies collect too much data are more interested in using cryptocurrencies. Among the other factors, only concerns about data *errors* had the expected positive effect on willingness on average, but the significance level barely missed the cutoff value of 5%. We found no evidence for an effect of *unauthorized secondary use* or *improper access*.

We do not find support for any of our hypotheses concerning the second research question. Risk perceptions seems to play no role for the actual adoption of cryptocurrencies, with the effect on adoption behavior actually being positive on average (albeit statistically insignificant). This finding adds to the picture developed in prior research that found no effect of risk perception on actual behavior for cryptocurrencies [48], even though an effect on intention was found in a number of earlier studies [1, 33].

Concerning privacy risk, the only variable exhibiting a significant effect on use behavior is *unauthorized secondary use*. However, it is only significant if

Table 4: Adoption Behavior on CFIP Subscales and Risk Perception

variable	simple models					full model
const	**-4.197***	**-6.206***	**-7.030****	-2.551	-5.274	**-8.168***
	(0.012)	(0.021)	(0.005)	(0.281)	(0.1)	(0.022)
RP	0.121	0.063	0.053	0.184	0.101	0.066
	(0.696)	(0.832)	(0.855)	(0.585)	(0.740)	(0.838)
CO		0.428				0.725
		(0.31)				(0.183)
ER			0.614			0.681
			(0.126)			(0.168)
US				-0.316		**-1.881***
				(0.354)		(0.012)
IA					0.185	1.335
					(0.689)	(0.098)

$*p < 0.05$, $**p < 0.01$, $***p < 0.001$, p-values in parentheses.

we include every other CFIP variable, and even then the results indicate that individuals worried about unauthorized secondary use of their data by online-companies are in fact less likely to use cryptocurrencies. This may be explained by existing users identifying cryptocurrency exchanges or other market players under the umbrella term “online companies”, where non-users may apply the term to merchants due to their lack of familiarity with the cryptocurrency ecosystem. Furthermore, the sample of actual users with only seven responses is very small. Thus, further research is needed to investigate to which degree the results can be generalized.

The observed discrepancy between stated intentions and actual behavior is a well known phenomenon in privacy-related areas, where is it generally referred to as the privacy paradox [27].

6 Limitations and Future Research

An obvious limitation of our study is that we used privacy concerns towards e-commerce companies to gauge privacy concerns, which may not be equivalent to concerns about cryptocurrencies in themselves. Previous research found that trust in cryptocurrencies is associated with trust in other entities, notably the government [3] and interpersonal trust in general [25], and more research could shed light on the connection between privacy concerns towards entities in the e-commerce and the cryptocurrency ecosystems and the currencies themselves. We further focused on privacy concerns and risk perception, leaving out factors such as perceived ease of use and perceived usefulness [10], cost-effectiveness [20], or self-efficacy [48]. We did this to afford ourselves the possibility to look at facets of privacy concerns without the risk of overfitting the model, but future research should still consider these factors and how they interact with privacy concerns. Us employing a representative sample of German users of e-commerce meant that even though we reached 257 respondents, only seven of these had already used cryptocurrencies, which means a low representation for actual users as in individuals who have used these for payment purposes. While we believe using this type of sample was necessary to ensure that the results are applicable to the German population overall, future research may repeat this type of study with a larger focus on existing users. Finally, our study only asks German respondents, which may limit our studies applicability to other countries, as significant differences in privacy concerns and perceptions are well-founded in the literature [23, 38]. Future research may replicate our study for different countries or cultures.

7 Conclusion

In this study, we contribute to the literature by investigating the effect of risk perceptions and privacy concerns towards online companies on whether individuals are willing to use cryptocurrencies, as well as their actual behavior. We find that perceived risk as well as worries about the collection of personal data exert a significant influence on whether individuals would consider using cryptocurrencies. However, neither variable was useful for explaining actual use behavior. This is consistent with the extant literature on cryptocurrency adoption [48]. Our results add to that picture, and open avenues to further research as to why perceived risk seems to play a major role for intention, but not behavior when it comes to cryptocurrency usage.

Acknowledgements

This work was supported by the German Federal Ministry of Education and Research's (BMBF) program "Datenschutz: selbstbestimmt in der digitalen Welt" via the SIOC project.

Bibliography

[1] Abramova, S., Böhme, R.: Perceived benefit and risk as multidimensional determinants of bitcoin use: A quantitative exploratory study. ICIS 2016 Proceedings (2016)

[2] Arias-Oliva, M., Pelegrín-Borondo, J., Matías-Clavero, G.: Variables influencing cryptocurrency use: a technology acceptance model in spain. Frontiers in psychology 10, 475 (2019)

[3] Arli, D., van Esch, P., Bakpayev, M., Laurence, A.: Do consumers really trust cryptocurrencies? MIP 39(1), 74–90 (2021)

[4] Bech, M.L., Garratt, R.: Central bank cryptocurrencies. BIS Quarterly Review September (2017)

[5] Berentsen, A., Schär, F.: The case for central bank electronic money and the non-case for central bank cryptocurrencies. Federal Reserve Bank of St. Louis Review, Second Quarter 2018 pp. 97–106 (2018)

[6] Brandeis, L., Warren, S.: The right to privacy. Harvard law review 4(5), 193–220 (1890)

[7] Chen, L.d.: A model of consumer acceptance of mobile payment. International Journal of Mobile Communications 6(1), 32–52 (2008)

[8] Chen, L.D., Tan, J.: Technology adaptation in e-commerce:: key determinants of virtual stores acceptance. EMJ 22(1), 74–86 (2004)

[9] Cronbach, L.J.: Coefficient alpha and the internal structure of tests. psychometrika 16(3), 297–334 (1951)

[10] Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly pp. 319–340 (1989)

[11] Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., Colautti, C.: Privacy calculus model in e-commerce–a study of italy and the united states. European Journal of Information Systems 15(4), 389–402 (2006)

[12] Esmaeilzadeh, P., Hemang, S., Cousins, K.: Individuals' cryptocurrency adoption: A proposed moderated-mediation model. AMCIS 2019 (2019)

[13] EUROSTAT: EUROSTAT 2018. https://ec.europa.eu/eurostat/de/home (2021)

[14] Fabian, B., Ermakova, T., Sander, U.: Anonymity in bitcoin?–the users' perspective. ICIS 2016 Proceedings (2016)

[15] Fishbein, M.: A theory of reasoned action: some applications and implications. (1979)

[16] Foley, S., Karlsen, J.R., Putniņš, T.J.: Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies 32(5), 1798–1853 (2019)

[17] Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M.C., Siering, M.: Bitcoin-asset or currency? revealing users' hidden intentions. ECIS 2014 (2014)

[18] Groß, T.: Validity and reliability of the scale internet users' information privacy concerns (IUIPC). PoPETS 2021 (2021)

[19] Hair Jr, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M.: A primer on partial least squares structural equation modeling (PLS-SEM). Sage (2021)

[20] Hamm, P.: Acceptance factors for cryptocurrencies as payment systems. In: HICSS 2022 (2022)

[21] Harborth, D., Pape, S.: German translation of the concerns for information privacy (CFIP) construct. Tech. rep., SSRN (01 2018)

[22] Harborth, D., Pape, S.: How privacy concerns and trust and risk beliefs influence users' intentions to use privacy-enhancing technologies – the case of tor. In: HICSS 2019. pp. 4851–4860 (01 2019)

[23] Ilhan, A., Fietkiewicz, K.J.: Data privacy-related behavior and concerns of activity tracking technology users from germany and the usa. Aslib Journal of Information Management 73(2), 180–200 (2021)

[24] Jabbar, A., Geebren, A., Hussain, Z., Dani, S., Ul-Durar, S.: Investigating individual privacy within cbdc: A privacy calculus perspective. Research in International Business and Finance 64, 101826 (2023)

[25] Jalan, A., Matkovskyy, R., Urquhart, A., Yarovaya, L.: The role of interpersonal trust in cryptocurrency adoption. Journal of International Financial Markets, Institutions and Money 83 (2023)

[26] Jonker, N.: What drives the adoption of crypto-payments by online retailers? Electronic Commerce Research and Applications 35, 100848 (2019)

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

[28] Li, Y.: Empirical studies on online information privacy concerns: Literature review and an integrative framework. Communications of the Association for Information Systems 28(1), 28 (2011)

[29] Lustig, C., Nardi, B.: Algorithmic authority: The case of bitcoin. In: HICSS 2015. pp. 743–752 (2015)

[30] Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. ISR 15(4), 336–355 (2004)

[31] Mann, H.B., Whitney, D.R.: On a test of whether one of two random variables is stochastically larger than the other. The annals of mathematical statistics pp. 50–60 (1947)

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

[33] Mendoza-Tello, J.C., Mora, H., Pujol-López, F.A., Lytras, M.D.: Disruptive innovation of cryptocurrencies in consumer acceptance and trust. Information Systems and e-Business Management 17, 195–222 (2019)

[34] Merhi, M., Hone, K., Tarhini, A.: A cross-cultural study of the intention to use mobile banking between lebanese and british consumers: Extending UTAUT2 with security, privacy and trust. Technology in Society 59 (2019)

[35] Muñoz-Leiva, F., Luque-Martínez, T., Sánchez-Fernández, J.: How to improve trust toward electronic banking. Online Information Review 34(6), 907–934 (2010)

[36] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized business review p. 21260 (2008)

[37] Poon, W.C.: Users' adoption of e-banking services: the malaysian perspective. Journal of business & industrial marketing 23(1), 59–69 (2008)

[38] Schallehn, F., Valogianni, K.: Sustainability awareness and smart meter privacy concerns: The cases of us and germany. Energy Policy 161, 112756 (2022)

[39] Schmitz, C., et al.: Limesurvey: An open source survey tool. LimeSurvey Project Hamburg, Germany (2023), http://www.limesurvey.org

[40] Shapiro, S.S., Wilk, M.B.: An analysis of variance test for normality (complete samples). Biometrika 52(3/4), 591–611 (1965)

[41] Smith, H.J., Dinev, T., Xu, H.: Information privacy research: an interdisciplinary review. MIS quarterly pp. 989–1015 (2011)

[42] Smith, H.J., Milberg, S.J., Burke, S.J.: Information privacy: Measuring individuals' concerns about organizational practices. MIS quarterly pp. 167–196 (1996)

[43] Stewart, K.A., Segars, A.H.: An empirical examination of the concern for information privacy instrument. ISR 13(1), 36–49 (2002)

[44] Tronnier, F., Harborth, D., Hamm, P.: Investigating privacy concerns and trust in the digital euro in germany. Electronic Commerce Research and Applications 53, 101158 (2022)

[45] Udo, G.J.: Privacy and security concerns as major barriers for e-commerce: a survey study. Information management & computer security (2001)

[46] Undheim, T.: Why banks fear bitcoin. `https://web.archive.org/web/20180424095311/https://fortune.com/2014/11/20/why-banks-fear-bitcoin/` (2014)

[47] Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: Toward a unified view. MIS quarterly pp. 425–478 (2003)

[48] Voskobojnikov, A., Abramova, S., Beznosov, K., Böhme, R.: Non-adoption of crypto-assets: Exploring the role of trust, self-efficacy, and risk. In: ECIS (2021)

[49] Voskobojnikov, A., Obada-Obieh, B., Huang, Y., Beznosov, K.: Surviving the cryptojungle: Perception and management of risk among north american cryptocurrency (non) users. In: FC 2020. pp. 595–614. Springer (2020)

[50] Wang, H., Lee, M.K., Wang, C.: Consumer privacy concerns about internet marketing. Communications of the ACM 41(3), 63–70 (1998)

[51] Westin, A.F.: Privacy and freedom. Washington and Lee Law Review 25(1), 166 (1968)

[52] Wooldridge, J.M.: Introductory econometrics: A modern approach. Cengage learning (2015)

[53] Xu, H., Dinev, T., Smith, J., Hart, P.: Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems 12(12), 1 (2011)

[54] Zhang, T., Lu, C., Kizildag, M.: Banking "on-the-go": examining consumers' adoption of mobile banking services. International Journal of Quality and Service Sciences 10(3), 279–295 (2018)

All URLs have been last accessed on March 11, 2023.

Questionnaire

Demographics We asked for the following demographics, answer options are listed in brackets: age ($> 18, 18, \dots, 65, > 65$), gender (female, male) and education (cf. Tab. 1).

Adoption Willingness / Behavior[1]

Have you made a purchase with bitcoin or another cryptocurrency in the past?

[1] Yes; No, but I have considered it before; No, I haven't considered it yet either.

Risk Perception[2]

RP1 When I use cryptocurrency, I worry about the risk of fraud because of the lack of legal regulations.

RP2 When I pay with cryptocurrencies, I worry about the value of my money because of the volatility of these currencies.

RP3 When I pay with cryptocurrencies I do not feel absolutely protected from illegal attacks and activities.

RP4 When I pay with cryptocurrencies, I worry about my electronic devices not working well due to cryptographic errors and the payment not being recorded correctly.

Collection[2]

CO1 It usually bothers me when companies ask me for personal information.

CO2 When companies ask me for personal information, I sometimes think twice before providing it.

CO3 It bothers me to give personal information to so many companies. CO4. I am concerned that companies are collecting too much personal information about me.

Errors[2]

ER1 All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.

ER2 Companies should take more steps to make sure that the personal information in their files is accurate.

ER3 Companies should have better procedures to correct errors in personal information.

ER4 Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.

Unauthorized Secondary Use[2]

US1 Companies should not use personal information for any purposes unless it has been authorized by the individuals who provided the information.

US2 When people give personal information to a company for some reason, the company should never use the information for any other reason.

US3 Companies should never sell the personal information in their computer databases to other companies.

US4 Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

Improper Access[2]

IA1 Companies should devote more time and effort to preventing unauthorized access to personal information.

IA2 Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.

IA3 Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

[2] seven-point Likert scale from “strongly disagree” (1) to “strongly agree” (7).