sciendo

NS global economics

ECONOMICS
Innovative and Economics Research Journal
Volume 12, No. 2, 2024
www.economicsrs.com

CBDC, TRUST IN THE CENTRAL BANK AND THE PRIVACY PARADOX

Viktor Koziuk[1], Yurii Ivashuk[1], Yurii Hayda[1]

Received 10.02.2024. | Sent to review 03.03.2024. | Accepted 13.07.2024.

Original article

CC BY NC ND

[1] West Ukrainian National University, Ternopil, Ukraine

Corresponding Author:
Viktor Koziuk

Email: victorkozyuk@ukr.net

JEL Classification: E41, E42, E51, E58, G20

Doi: 10.2478/eoik-2024-0025

UDK: 334.753:336.763.3(4-672EU))

ABSTRACT

Privacy/anonymity of digital transactions is an issue that potentially may affect demand for central bank digital currency. Does discussions about privacy paradox related to CBDC? In this paper, basing on the respondent's survey, we construct indexes of privacy preferences (in general, in digital and financial environment) to identify relations between stated preferences in different contexts and between choice toward anonymity vs functionality of CBDC, trust to central bank as CBDC issuer and its independence as a precondition to guaranty anonymity of transactions. We find that generally respondents demonstrate consequence of preferences in terms of, what we call, general privacy, privacy in digital and financial environment. Distribution of obtained 3 indexes demonstrates some differences. Probit model also demonstrates that relation between choice toward anonymity over functionality of CBDC and level of 3 indexes is modest. Where is no correspondence between choice toward anonymity over functionality and trust in central bank and its independence. However, respondents demonstrate high level of trust in central bank ability to guaranty anonymity of transactions and view independence as supporting it even opting functionality over anonymity. We reach a conclusion that some weak form of privacy paradox is exist, central banks, promoting CBDC, should stress on functionality of it. However, privacy should not be ignored. It is better to have it as "nice bonus" to functionality of CBDC.

Keywords: *central bank digital currency, digital money, anonymity of transactions, CBDC design, privacy paradox*

1. INTRODUCTION

Digital transformation approaches are very close to changing the nature of money. Some of its virtues, so invisible in the past, are becoming a real subject for discussion in the present. The new possibilities of money digitalisation give rise to the problem of policy choice by central banks and challenge how certain social constructs are interpreted. Privacy is one example of how the virtues inherent in traditional money (Kahn et al., 2005) have become a dilemma in the development of digital money. Why should economic agents prefer alternatives to cash or payment services available today? And why central banks, entering into competition with cryptocurrencies for reasons of ensuring national monetary sovereignty (Brooks, 2021), pay so much attention to the problem of CBDC design, probably the main debatable element of

which is the privacy/anonymity of transactions (Agut et al., 2021, Fanti, 2022, Eichengreen, 2022, Soderberg et al., 2023, UK Parliament, 2023)? At the same time, the very subject area of privacy in the digital world is far from a final scientific consensus. As shown in many works (Solove, 2021, Kokolakis, 2017, Athey et al., 2017), research on behaviour regarding privacy often provides the basis for relatively polar conclusions. How can the discussion about the nature of privacy in the digital world be useful for CBDC design development?

Empirical research on CBDC design preferences does not ignore the importance of privacy and trust in central banks among the factors that may influence what the demand for a central bank digital currency will be (Kantar Public, 2022, Bijlsma et al., 2021, Abramova et al., 2022). At the same time, in most cases, surveys with direct questions about privacy preference (Bijlsma et al., 2021, Abramova et al., 2022, Jiand, 2020) or the use of the experimental approach elements with randomised groups of respondents (Choi et al., 2023) risk being targeted in the context of discussions about whether the stated preference for privacy reflects the actual behaviour of economic agents, that is, in the context of discussions about the privacy paradox. In Koziuk and Ivashuk, 2022, it is shown that economic agents may accept a lower level of privacy if it is compensated by better functionality of the CBDC, while there are trust issues in the institutional environment in which privacy should be guaranteed. In light of this, it is fundamentally important to identify a propensity for privacy in a way that is distinct from the traditional privacy preference question and to consider the context in which economic agents do or do not demonstrate such a propensity.

Based on a survey of respondents from 4 countries, this article identifies the general propensity for privacy in digital and financial environments based on calculating the relevant individual indices. This made it possible to mitigate the problem of context, which is often cited as an argument in criticism of the privacy paradox approach. Quantitative values of the three indices that were obtained were used to test the probability of a positive answer to the question about the preference of CBDC anonymity over functionality. Based on empirical analysis, it has been shown that, in general, economic agents behave consistently with a certain bias towards the privacy paradox. However, the choice between anonymity and functionality may appear to be an autonomous factor that does not always follow from the stated preference for privacy. With trust in the central bank as a guarantor of anonymity, privacy will be a “nice bonus” of functionality. A policy recommendation emerges from this research – trust in central banks as CBDC issuers weighs more than the formal opposition of anonymity and functionality.

2. LITERATURE REVIEW

The literature on the optimal forms of interaction between economic agents in the digital environment is actively growing. Privacy is increasingly articulately becoming a central topic of research, as access to big data is already a competitive advantage, and new technological possibilities for the traceability of transactions raise concerns about the balance of power between the private individual and the state. This article is at the intersection of several research areas: theoretical analysis of the nature of money in the digital environment, identification of the CBDC optimal design, in particular the role of privacy as well as how and to what extent it should be guaranteed, the study of privacy preferences and the privacy paradox, which testifies to the differences in the stated preferences and the actual behaviour of economic agents, study of the relationships between trust in central banks, their status, and prospects for the privacy of monetary transactions. In this article, privacy is considered from the standpoint of an individual’s ability to control information about themselves, while anonymity in the sense of transactional anonymity will be a special case of such privacy, due to which they are often used as synonyms.

Digitization is changing money. The emergence of the blockchain has strengthened those theoretical positions, which emphasize that money has memory features (Kocherlakota, 1998). And therefore, cryptocurrencies are money, even despite the inefficiency of performing the functions of money in their structural integrity. Brunnermeier et al., 2019, point to the possibility of unbundling the structural integrity of the money functions thanks to modern technologies. This will affect the competition between services that will be able to meet the needs of economic agents in certain functions of money separately. The new technological possibilities of tracking transactions are reflected in the fact that traditional money has an immanent virtue, imperceptible outside the process of digitization - the ability to guarantee the anonymity of transactions, thereby ensuring privacy. Kahn et al., 2005 provide theoretical arguments for why privacy is immanent in money. Borgonovo et al., 2021 prove, based on a behavioural experiment, that economic agents value privacy in money. Although the level of reward and liquidity conditions influence the virtue of money that will prevail (Masciandaro, 2018). That is, it is impossible to neglect the privacy factor in the design of digital money, regardless of how economic agents value it. Competition between different forms of digital and fiat money will increase, influencing what the optimal design of CBDC should be.

The idea of CBDC as a response to the challenge of competitive pressure from private cryptocurrencies (Brunnermeier et al., 2019) immediately raised questions about design. It is a natural subject of discussion due to wide variations on the topic of technological basis, functionality, method of distribution among users, interface, use-case, limits on transactions, etc. (Mancini-Griffoli, 2018). The reason for this is obvious. The chosen design will affect the effectiveness of the central bank in ensuring price and financial stability (Brunnermeier and Niepelt, 2019, Andolfatto, 2020, Agur, 2022, Williamson, 2022). Along with this, the issue of privacy as an aspect of design is no less important, as it will directly determine the demand and trust in the central bank's digital currency.

The ECB is quite unequivocal that privacy must be guaranteed at the design level of the digital euro. This corresponds to the preferences of economic agents in the Eurozone (ECB, 2019, 2021, Panetta, 2023, Hernandez de Cos, 2023). Surveys on the role of privacy in CBDC design demonstrate that it is important (Bijlsma et al., 2021, Abramova et al., 2022, Jiand, 2020, Choi et al., 2023). However, there is space for discussion about this.

Firstly, surveys conducted in European countries have shown that respondents do not think about whether the privacy of their transactions is protected (Kantar Public, 2022). Privacy is an important feature of money expected from CBDC, but not exclusive and not of primary importance along with Universal acceptance, ant, contactless and open person-to-person payments, one-stop-solution, Easy to use, secure, reliable and fast: biometric authentication, Cost-efficiency, etc. Also, for the respondents, the main thing is the functionality of the services, not their provider. Although Europeans prefer it to be either a bank, a central bank, or a European agency rather than a big tech company (Kantar Public, 2022). Trust in the central bank is higher than in technology companies, according to surveys conducted in South Korea (Choi et al., 2023), Austria (Abramova et al., 2022) and the Netherlands (Bijlsma et al., 2021). Koziuk and Ivashuk, 2022 argue that privacy can be a compromise in favour of functionality, and this phenomenon is not always clearly linked to cultural attitudes but rather to institutional factors.

Secondly, combining blockchain with transaction anonymity is a technical challenge by definition. Its solution requires a decision at the level of political choice of digital currency design. As shown in ECB, 2019, Bank of England, 2020, Garratt and van Oordt, 2021, Radukić et al., 2019, ensuring a certain politically acceptable level of privacy requires quite complex technical and procedural solutions. Pfister and de Seze, 2023 analyse the digital yuan's approach to privacy and point to the potential risks to personal freedom from the side of the option chosen

by the People's Bank of China. Fanti, 2022 and WEF, 2021 highlight that there are problems with technological compatibility between one way of guaranteeing privacy or another and the chosen digital currency design.

That is, public demand for CBDC to guarantee privacy puts central banks before a difficult choice. The high level of technological complexity of such solutions gives rise to the problem of information asymmetry, adequacy of request perception and expectations regarding privacy and, accordingly, trusts. This brings the subject area of this article closer to research on privacy in the digital environment.

Discussions about the differences between stated privacy preferences (attitudes) and choice (behaviour) of economic agents postulate the existence of a privacy paradox. In the most general form, it boils down to the fact that the behaviour of economic agents in the digital environment indicates a much lower importance of privacy compared to the stated preferences for it. As demonstrated by Acquisti, 2004, Acquisti and Grossklags, 2005, Norberg et al., 2007, Barnes, 2006, there is a clear discrepancy between the stated propensity for privacy and actual behaviour. Actual preference-contradictory behaviour involves significantly more self-disclosure, willingness to self-disclose in response to minor incentives, unwillingness to exert effort to maintain privacy, etc.

Athey et al., 2017, with the help of a well-known behavioural experiment, confirm the extremely low value of the gain for which economic agents are willing to exchange information about themselves and the significant value of the incentives that should motivate actions to ensure privacy. Chen et al., 2021, based on a large amount of Alipay customer data, support the idea of the relevance of the privacy paradox but do not rule out that it arises because of the specific case of human interaction with digital applications. Kokolakis, 2017, Barth et al., 2017 and Gerber et al., 2018 review the literature on this issue and structure theoretical approaches to its explanation. Criticisms of the privacy paradox (Solove, 2021) and studies that have largely attempted to explain it (Barth et al., 2017) emphasise that context matters. For instance, Hirschprung, 2023 shows data from an experiment where 437 respondents showed differences in their stated preferences for privacy and actions related to it. However, such differences vary significantly depending on the situational domain.

Differences in stated privacy preferences should not be correlated with behaviour or choice in an artificially simulated experiment (Solove, 2021, Kokolakis, 2017). More important is the tracking of preferences and behaviour in contextually determined situations that are understandable to economic agents. Also, the complexity of the information environment and the context's specificity do not exclude the fact that economic agents behave by the privacy calculus (Culnan and Armstrong, 1999). That is, they rationally weigh the losses and benefits regarding actions or refrain from actions that affect their privacy. The idea of privacy calculus is based on the rational choice theory. It takes into account various caveats of behavioural economics regarding the nature of choice in an informationally complex environment with a high level of uncertainty (Kokolakis, 2017, Barth et al., 2017, Gerber et al., 2018). Also, implicitly, the issue of context is taken into account here. Economic agents take into consideration that the context conditions losses and gains. They need to take actions related to privacy in it. Brits and Jonker, 2023 prove this with the example of a survey on attitudes towards financial applications. Van der Cruijsen, 2020 supports the idea of the context importance. In her research, the willingness of payment services users to share data depends on who it will be and for what purpose. Rosati et al., 2022 add the importance of the expected outcome of data sharing and also point to an inverse relationship between propensity for risk and willingness to share data. That is, willingness to share data is determined by trust and financial incentives. In other words, apart from purely theoretical arguments in favour of explaining the privacy paradox (Barth et al., 2017, Gerber et

al., 2018) or its denial (Solove, 2021), surveys support the idea that this paradox fits into more complex patterns of behaviour. However, Barth et al., 2019 prove the existence of the privacy paradox on the example of an experiment with technically knowledgeable respondents. Such respondents demonstrated a greater importance of functionality than privacy when choosing financial applications, regardless of the initial stated attitude towards privacy. Brits and Jonker, 2023, in turn, emphasize the dominance of privacy calculus-style behaviour.

The results of Barth et al., 2019 correspond with the findings of Koziuk and Ivashuk, 2022 that the discrepancy between the stated propensity for privacy and the choice in favour of functionality is due to how institutions affect trust. Even if cultural factors determine the degree of privacy preference, they lose their effectiveness where respondents are faced with a choice between the anonymity of transactions and the functionality of applications. At the same time, CBDC demand research tests trust in central banks, banks and financial institutions. Most of them are unambiguous. Respondents are more likely to agree to use CBDC because they trust their issuer (Bijlsma et al., 2021, Abramova et al., 2022, Jiand, 2020, Choi et al., 2023). However, a clarification should be made here. In these studies, the independent variable is a binary variable denoting trust or distrust in the central bank, the importance or unimportance of cash for the anonymity of payments, trust in the financial institution as such, whether it will share data with third parties or not. In other words, the results of such surveys will be subject to criticism from the side of privacy paradox, even if they are constructed according to a complex experimental algorithm, as in the case of Choi et al., 2023.

However, investigation of trust in the CBDC issuer is important. Koziuk, 2021a demonstrates that when the age factor of digital money preference dominates, the degree of trust in the central bank is more sensitive to past inflationary experience. This could potentially undermine the prospects of CBDC in a number of developed countries with negative demographics. For instance, Abramova et al., 2022 on the example of Austria testifies to a restrained pessimism about the bright prospects of the central bank digital currency. Instead, Bijlsma et al., 2021 on the example of the Netherlands are cautiously optimistic. In both studies, the relationship between willingness to use CBDC and trust in the central bank is positive. At the same time, the role of the central bank status in matters of digital transformation of money is insufficiently studied. Koziuk, 2021a, 2022 notes that central bank independence plays an important role in creating an environment of trust in digital currency, and institutional distortions in monetary processes affect the popularity of private cryptocurrencies. At the same time, Koziuk, 2021b shows that the progress of CBDC implementation is more likely related to the average level of central banks independence, and the political regime matters in terms of the extent to which transaction traceability can become a tool of political control and social selection. Pfister and de Seze, 2023 also make similar caveats based on an analysis of e-yuan design. Tsang et al., 2023 analyse different CBDC design options and indicate that regardless of the chosen option, central bank independence plays a critical role. It is the status of the CBDC issuer that will determine whether users' privacy will be ensured or not, as various variations on the topic of technical and institutional ways of guaranteeing privacy may not be sufficient if the central bank is not adequately institutionally protected (Tsang et al., 2023).

According to the conducted analysis of literary sources, it is possible to form several prerequisites for formulating the research agenda of the article. Firstly, the design of the CBDC and the ways to guarantee the anonymity of transactions are technically complex. Therefore, economic agents may not have all the necessary information to make a welfare-maximizing decision. Secondly, the behaviour of economic agents in the digital environment often falls under the privacy paradox, which, in turn, does not exclude more complex patterns of behaviour in which choices will be made under the influence of a specific context and with an analysis of losses

and benefits. Thirdly, suppose the stated propensity for privacy may be overstated. In that case, the choice in favour of functionality may appear natural the more it is reinforced by additional institutional factors, such as those related to trust. Fourthly, the difficulty with assessing the central bank's true ability to guarantee the anonymity of transactions means that an economic agent will use trust if the relation "privacy preference - trust in the issuer as a guarantor of privacy" dominates for him/her. Otherwise, he/she has enough functionality, especially if the ability to guarantee privacy is already distrusted.

3. AIM OF THE RESEARCH

This article puts forward an initial agnostic assumption about some uncertainty about the choice between the advantage of transaction anonymity and the advantage of the payment services functionality. By determining individual indices of the propensity for privacy in general, digital and financial environments, an assessment is made of whether there is a correlation between these three indices across the entire sample of respondents or whether the value of such indices affects the choice between anonymity and functionality. If individual indices of the propensity for privacy have a positive relationship with the preference for anonymity over functionality, this will mean that economic agents behave consistently. If the relationship is reversed, it will mean the privacy paradox. If there is no relationship, it will mean that the choice between anonymity and functionality does not depend so strongly on propensity or non-propensity for privacy.

Based on the survey of 156 respondents from 4 countries, it has been found that there is a correlation between three indices of individual propensity for privacy, however, it is weaker in the case of general privacy and privacy in the financial environment, which indicates signs of the privacy paradox; there is a relationship between individual propensity for privacy (across three indices) and the choice between anonymity and CBDC, so the fact that it is statistically weak indicates that such a choice may not depend on this propensity but be an autonomous fact; there is a clear and statistically significant relationship between trust in the central bank and trust in its independence as a guarantee of transaction anonymity. That is, respondents may trust the CBDC issuer's ability to guarantee transaction anonymity even when such anonymity is not constitutive to them. This leads to an important conclusion for central bank policies. The functionality of the CBDC design is constitutive for the success of this project. Ensuring the privacy of CBDC users looks like a "nice bonus", which, however, should not be neglected. On the contrary, the institutional status of central banks should be strengthened in response to the challenges of digital transformation, even in the face of an unpredictable relationship between stated preferences, identified propensities, and actual behaviour in the digital world.

4. METHODS

Methodologically, this study consists of several stages: developing a questionnaire, conducting an online survey and data processing (156 responses have been received from 4 countries: Ukraine, Uzbekistan, Nigeria, and Zimbabwe). The questionnaire consists of two parts. In the first part, respondents give answers to determine the index of their individual propensity for privacy in 3 options. In the second one, they answer questions about the preference for anonymity or functionality in CBDC design, as well as whether they trust the ability of the central bank to ensure the anonymity of transactions and whether they trust that the independence of the central bank is a guarantee of its ability to ensure the anonymity of transactions.

At the heart of the survey design idea is the assumption that a direct question about the preference for privacy/anonymity of transactions is subject to criticism from the side of the privacy

paradox approach. Moreover, such criticism can be twofold. A direct question and the resulting binary variable for privacy preference, when regressed with a variable indicating a preference for one or another aspect of the CBDC design, will be a very simple test. The result can be interpreted too arbitrarily in the categories of confirmation or refutation of the privacy paradox. Solove, 2021 criticises this approach. Also, such an approach will not take into account context, which is important because privacy behaviour can vary significantly depending on the circumstances, as shown, for instance, in Hirschprung, 2023 or Cloos et al., 2019. Therefore, in contrast to a direct answer about privacy preference (Bijlsma et al., 2021, Abramova et al., 2022, Jiand, 2020, Choi et al., 2023), we construct the questions in such a way that answers to them allow assessing the privacy preference, rather than obtaining a response about privacy preference directly. Cloos et al., 2019 use this approach to complicate experimental design to assess the privacy paradox. Accordingly, we suggest that respondents first be surveyed to determine privacy preference, and then the resulting quantitative value of such preference is used for further analysis.

Considering the importance of context in matters of privacy, the general propensity for privacy is determined based on responses to a series of general questions. The propensity for privacy in the digital environment is separately assessed based on more contextual questions. The propensity for privacy in the financial environment is also separately determined based on respondents' answers to questions articulately defined by the context. The assessment of some aspects of individual propensity for all three types of privacy, which are reflected in the content of individual questions, is determined on a 5-point Likert scale (see Appendix A). By integrating these estimates, three individual indices are calculated for each respondent: the index of the general propensity for privacy (GPP), the index of the propensity for privacy in the digital environment (DEP), the index of the propensity for privacy in the financial environment (FEP). The value of these indices can range from 10.0 to 50.0. The nature of the relationship between these three indices will indicate how consistent respondents are in their reported propensity preferences for privacy in general and specific contexts. A strong positive relationship will indicate a lack of dominance of the privacy paradox, consistency of preferences and vice versa. The nature of the distribution of these indices values, illustrated by several descriptive statistics, may reflect both similarities and certain differences in economic subjects' attitude to privacy types.

Further, the obtained individual indices of the propensity for privacy are used as independent variables in assessing their relationship with the dependent binary variable, which reflects respondents' preferences when choosing between anonymity and functionality. A one-factor Probit model is used for this. Additionally, the influence of the respondents' age on their choice between anonymity and functionality is tested. The age of respondents in most empirical studies inversely corresponds to the propensity for privacy or the propensity to use fintech products (Koziuk, 2021a, Frost, 2020, Bijlsma et al., 2021, Abramova et al., 2022, Choi et al., 2023). The dependent variable is modelled according to the following principle: if the respondent chooses the former between the preferences of anonymity or functionality, the variable is assigned the value 1, and otherwise, 0. In the case of a sequence of respondents between the choice in favour of anonymity and the values of individual indices of propensity for privacy, a direct positive relationship should be observed. Otherwise, it will indicate the existence of a privacy paradox. In the event that one or the other direction of the relationship is statistically insignificant, it can be assumed that the individual propensity for privacy and the choice among CBDC design elements appear as separate phenomena.

A cross-tabulation analysis (contingency table analysis) is used to assess the significance, direction, and density of the relationship between responses regarding the benefits of anonymity or CBDC design functionality, trust in the central bank as a guarantor of transaction anonymity,

and trust in the independence of the central bank as a prerequisite for the ability to guarantee such anonymity. Exceeding the current value of the $\chi 2$ test over the critical one will indicate the truth of the alternative hypothesis that the relationship between the categorical variables, which reflect the binary answers of the respondents, exists and is statistically significant. The Phi Coefficient is used to estimate the density of such a relationship. Computationally, Phi is the square root of chi-square divided by the sample size. This method allows us to construct the equivalent of the correlation matrix but for binary variables. That is, the variables are modelled according to the principle following: if the respondent in the question about the preference for anonymity of transactions with the help of CBDC or the functionality of CBDC design chooses the first, the variable is assigned the value 1, and in the other case – 0. The affirmative answer is assigned 1 in the other two questions, and the negative answer is 0. This analysis is designed to reveal how holistically the respondents perceive the role of the central bank in ensuring the anonymity of transactions and how this correlates with their preference for the analysed aspects of CBDC design.

5. RESULTS

5. 1. INDIVIDUAL INDICES OF PROPENSITY FOR PRIVACY

A survey of respondents (the survey is presented in Appendix A) was used to obtain results on general privacy in digital and financial environments. Each of the three indices is calculated based on the number of points corresponding to the respondents' answers to each of the 10 questions. Table 1 presents descriptive statistics for the three obtained indices.

Table 1. Descriptive statistics of propensity for privacy indices

Indicators of descriptive statistics	Index of general propensity for privacy (GPP)	Index of propensity for privacy in the digital environment (DEP)	Index of propensity for privacy in the financial environment (FEP)
Mean	32.0	33.1	27.5
Confidence -95%	31.1	32.4	26.9
Confidence 95%	32.8	33.9	28.2
Median	32.0	34.0	28.0
Mode	31.0	35.0	28.0
Frequency of mode	20	17	21
Min	15	18	17
Max	46	44	38
St.Dev.	5.31	4.71	4.01
Coefficient of Variation	16.6	14.2	14.6
Standard Error	0.42	0.38	0.32
Skewness	-0.49	-0.55	-0.19
Kurtosis	0.79	0.79	-0.18

Source: Authors calculations.

Analysis of descriptive statistics shows that the distribution of individual values of three indices is slightly different. That is, there are differences in the average parameters, the degree of variability, and the nature of the distribution of the integral estimates of respondents' propensity for general privacy and propensity for privacy in the digital and financial environments. Firstly, the sample of individual evaluations by GPP is the most variable. The largest difference between the minimum and maximum value, the highest standard deviation and coefficient of variation are observed. The sample by DEP is less variable, compared to the GPP, but more variable

than the sample by FEP. That is, the distribution of FEP values indicates that the index of propensity for privacy in the financial environment is the most homogeneous. This is a testament to the importance of context. Secondly, there is a difference in the average values of the three indices. GPP shows the highest maximum and the lowest minimum value. DEP has the largest arithmetic mean value, and FEP - the smallest one (the difference between them is statistically significant - Student's t-test is 8.52 at t0.05 = 1.96). This may suggest a manifestation of the privacy paradox. Thirdly, the distribution of all three indices is characterised by left-tailed asymmetry (negative Skewness values). At the same time, DEP has the longest left tail with a Skewness indicator of -0.55, and the distribution of FEP values is closer to normal (Skewness -0.19). There are differences in the shape of the distribution curve peak. Kurtosis-positive values, which occur in the case of GPP and DEP, indicate pronounced heavy tails and a distinct peak of the distribution, that is, the presence of large deviations. In the case of FEP, Kurtosis is negative at -0.18 level, indicating less pronounced tails and less likelihood of large deviations. As can be seen, in all three cases, the lower levels of the index values vary much more than the higher ones. However, the FEP varies more in the average range of values, with a higher overall homogeneity. At the same time, the DEP has a higher peak but a longer left-sided tail. Such differences like the distribution indicate that respondents' propensity for general, digital and financial privacy are not identical. In general, it can be assumed that context reduces the spread of values.

5. 2. ANALYSIS OF RELATIONSHIPS BETWEEN INDIVIDUAL INDICES OF PROPENSITY FOR PRIVACY

The results of the correlation analysis of the relationship between three indices allow us to state that, despite the differences in the distribution's nature, the respondents demonstrate a certain sequence of preferences (table 2).

Table 2. Correlation matrix of relationships between individual indices of propensity for privacy

Propensity for privacy	DEP	FEP
GPP	0.446 p = 0.000	0.427 p = 0.000
DEP		0.350 p = 0.000

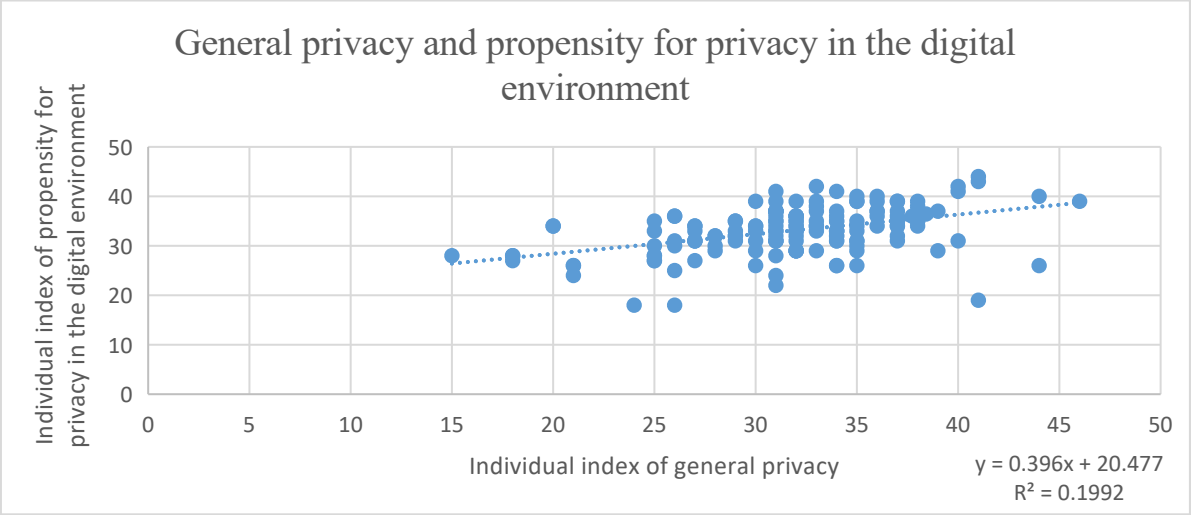
Source: Authors calculations.

As can be seen from Table 2, the pairwise correlation coefficients are statistically significant, although the density of the relationship according to the Chaddock scale is moderate. The positive value of the correlation coefficient in all three cases indicates the consistency of preferences for privacy in all analysed contexts. In other words, a high propensity for general privacy means that the respondent prefers a high propensity for privacy in both digital and financial environments. However, the correlation slightly decreases when comparing the pairs of variables GPP-DEP and GPP-FEP from 0.446 to 0.427. And in the case of DEP-FEP, it is even lower - 0.35. That is, context matters. The weakening of the correlation in couples with FEP may indicate that in financial matters, the distance between the stated preferences and preferences for privacy in the financial environment is the greatest.

Regression analysis (Fig. 1-3.) allows us to clarify the results obtained based on correlation analysis. All constructed models adequately describe the relationship between independent and dependent variables – the Fisher's F criterion is respectively 38.3, 34.4, and 21.5, significantly

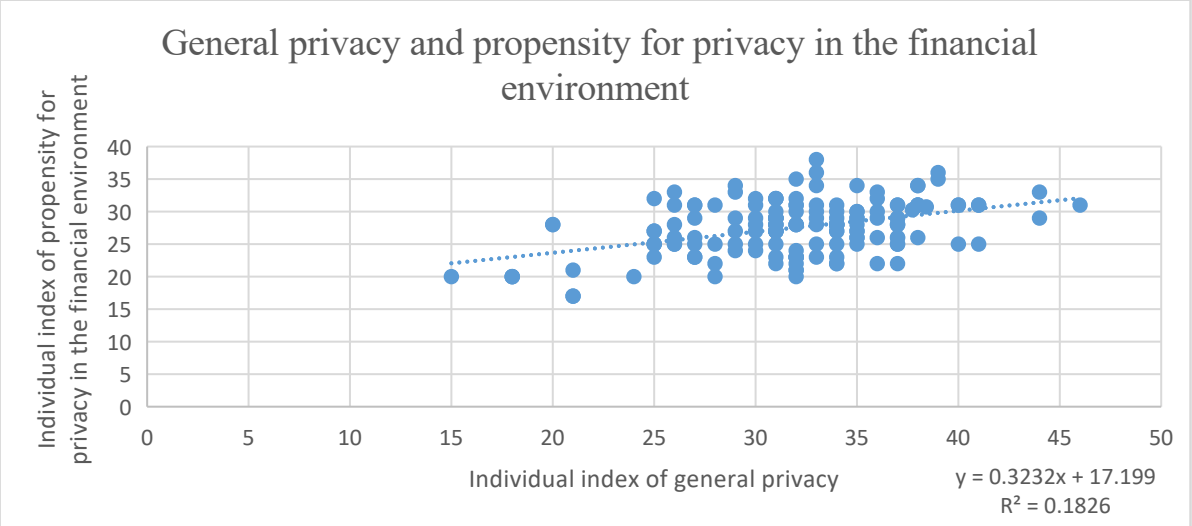
exceeding the tabulated F0.01 = 6.81. All intercepts and regression coefficients are statistically significant, the distribution of residuals is close to normal, and Durbin-Watson statistics are close to 2 (1.90, 1.60, and 1.56 respectively), indicating weak autocorrelation of residuals. As can be seen from the configuration of regression lines and analytical forms of regression models, there is an unambiguous direct relationship between all three indicators. The slope angle of regression lines and regression coefficients decrease from the highest in the pair of variables GPP-DEP to the lowest in DEP-FEP. This suggests that the influence of the propensity for general privacy for respondents on digital and financial privacy is consistently traced. The effect of the propensity for digital privacy on the propensity for financial privacy is even smaller.

Figure 1. Graph of a one-factor linear regression model (dependent variable – DEP, independent – GPP)



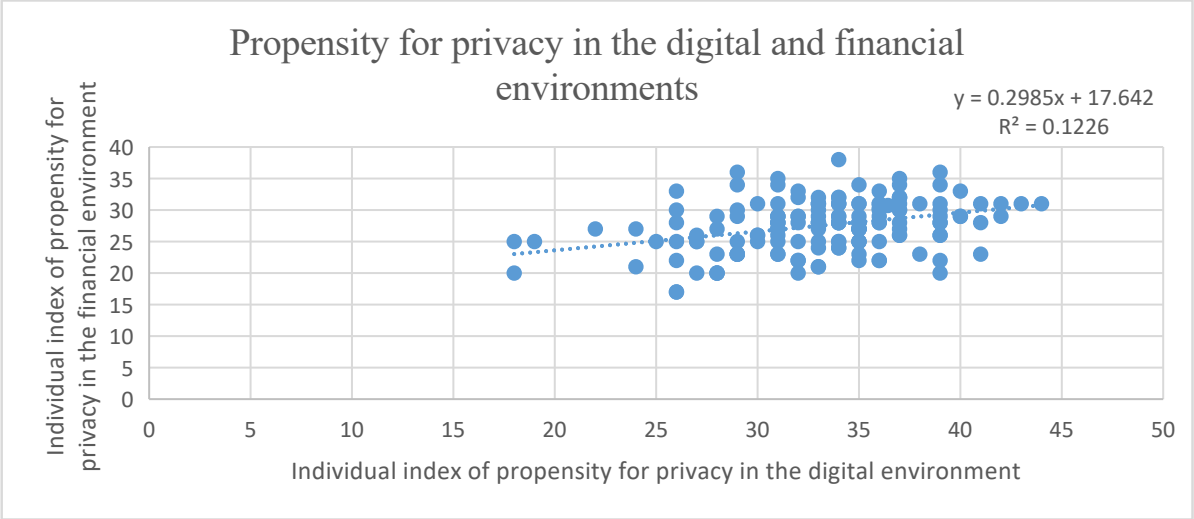
Source: Built by authors.

Figure 2. Graph of a one-factor linear regression model (dependent variable – FEP, independent – GPP)



Source: Built by authors.

Figure 3. Graph of a one-factor linear regression model (dependent variable – FEP, independent – DEP)



Source: Built by authors.

From an empirical point of view, it is obvious that the differences in the distribution nature of individual assessments of the propensity for privacy across three indices, the form and density of the correlation between them do not give grounds for asserting that the differences in preferences in three cases are very big. Discussing this as another example of the privacy paradox is impossible. However, the obtained empirical results can be interpreted as a manifestation of the importance of context and the importance of privacy paradox in a weak form.

Equally important is that the propensity for privacy in the financial environment is the lowest among the three cases. This seems quite surprising in light of the analysis of payment preferences, where respondents prefer anonymity when purchasing sensitive goods (Choi et al., 2023). On the other hand, this does not rule out that economic agents behave more by the privacy calculus hypothesis (Brits and Jonker, 2023, Van der Cruijsen, 2020). In finance, they can demonstrate a higher level of information transparency, even though one might intuitively expect the opposite.

5. 3. PROBIT ANALYSIS OF RELATIONSHIPS BETWEEN INDIVIDUAL PROPENSITY FOR PRIVACY INDICES AND PREFERENCES FOR CBDC DESIGN

Empirical works are quite unambiguous about the fact that individuals who declare a high value of privacy will tend to choose CBDC if the latter guarantees a higher level of transaction anonymity (Bijlsma et al., 2021, Abramova et al., 2022, Choi et al., 2023). However, this formulation is mostly associated with the alternative “more privacy - less privacy”. In the case of a choice between privacy and other aspects of payment services that maximise customer value, the situation does not look so compelling (Kantar Public, 2022). The choice between the alternatives of transaction anonymity and functionality of payment services can be influenced by institutional distortions regarding trust in financial institutions (Koziuk and Ivashuk, 2022). Equally important is that functionality may play a more significant role in light of the privacy paradox and the importance of the context in which such a choice is made (Barth et al., 2019).

Probit regression was applied to investigate the relationships between the variables reflecting the preferences of the economic subjects of CBDC design and individual indices of the propensity for privacy. Probit analysis models a binary response - in our case, the dependent variable

takes the value 1 if the respondent prefers the anonymity of CBDC transactions over functionality, and the response takes the value 0 if functionality is prioritised.

The general appearance of the Probit model is as follows:

$$P(Yi|X) = f(Xi), \qquad (1) - \text{ordinal numbers of the formula}$$

$$Yi = \begin{cases} 1, & Y^* > 0 \\ 0, & Y^* < 0, \end{cases} \qquad (2) - \text{ordinal numbers of the formula}$$

Yi* - A > F in the sense of anonymity priority over functionality,

Xi: Yi* = Xi*β + ε, where Xi* are individual indices of the propensity for privacy for each respondent (GPP, DEP and FEP) depending on the specification and age of the respondents.

The results of the Probit regression application are presented in Table 3.

Table 3. Results of Probit analysis of respondents' survey data

	Value of β1 in the models			
	(1)	(2)	(3)	(4)
GPP	0.015068			
DEP		0.016499		
FEP			0.041963	
Age				-0.004002
Chi2	0.6263	0.5868	2.7935	0.0711
P	0.4287	0.4437	0.0947	0.7897

Source: Authors calculations.

Results presented in Table 3 do not allow us to come to an unequivocal conclusion about whether there is a stable relationship between survey-based privacy and the preference for transaction anonymity over design functionality. Thus, the positive values of the coefficients at the independent variables in specifications (1-3) indicate that there is a logical relationship between higher values of individual propensity for privacy and the priority of anonymity. The negative value of the corresponding coefficient in the specification (4) indicates that the greater the age, the more likely the choice favours anonymity. Younger respondents are ready to choose in favour of functionality, which corresponds to other results (Barth et al., 2019).

At the same time, in models 1-2 and 4, the statistical significance of the relationship is insufficient. In model 3, it closely approaches statistical significance. Such a difference in statistical significance is intuitively understandable. A higher level of propensity for financial privacy prompts a choice in favour of anonymity over functionality. However, the FEP distribution is characterised by lower levels with shorter tail skewness. That is, better statistical significance values in the Probit model, specifically for financial privacy, can be explained not so much by the propensity level but by the intensity of choice as a group.

The obtained results do not give reason to believe that the relationships in the format of the privacy paradox are traced in a strong form. However, the logical sequence of the respondents' choice is also violated because, at the intuitively correct direction of communication, its density remains insignificant. It follows that respondents may make behavioural errors when it comes to decision-making in the context of two distinct classes of phenomena (anonymity vs function-

ality), or in the case when the respondents distinguish differences in the class of phenomena, they begin to be guided by additional factors. And therefore, their choice falls under the privacy calculus.

The latter raises the question of the theoretical consistency between the identified distinct values and distributions of individual propensity for privacy indices, as well as how such values correspond to the choice in favour of transaction anonymity. A lower level of propensity for financial privacy compared to general propensity does not contradict the choice in favour of anonymity over functionality in the categories of the privacy calculus, even if it confirms certain signs of the privacy paradox. This option may result from the structure of the questionnaire regarding the determination of propensity for privacy individual indices. In the case of FEP, issues related to trust in financial institutions, state regulators of digital money, and client identification procedures have a significant specific weight. Due to this, the FEP can shift downward, compared to the GPP, under the influence of trust or another institutional factor. As a result, a respondent with a lower level of FEP, compared to GPP or DEP, may prefer the anonymity of transactions because he/she perceives it in the relevant context.

5. 4. CBDC AND TRUST IN THE CENTRAL BANK

As already mentioned, in several works, respondents' probability of choosing a CBDC was positively correlated with trust in the central bank (Abramova et al., 2022, Choi et al., 2023). Also notable is the attention to the issue of central bank independence and CBDC design, the agreement between design and the ability to enforce control over society (Koziuk, 2021b, Pfister and de Seze, 2023, Tsang et al., 2023). An extremely important institutional conclusion emerges from the literature on the functional efficiency of central banks. Their independence matters. That is why this test includes the question of whether respondents consistently perceive trust in the central bank and its status as a reason for their trust in it to have a rational basis formed in the real political process. The importance of the question of the central bank independence is determined by the fact that its institutional capacity will determine the proposal of a socially optimal design of digital money, a guarantee that the personal data of users will not be used for profit, minimisation of the political interference likelihood in the payment histories of economic agents.

Confidence in the central bank is important in whether there will be sufficient demand for its digital currency. If respondents prefer some aspect of CBDC design but do not trust the central bank's ability to ensure its privacy promises, demand is likely to be weak. Economic agents should have sufficient incentive to choose CBDC over other forms of money. Since all variables in this test are binary, cross-tabulation analysis is used as an empirical tool, the results of which are shown in Table 4.

Table 4. Results of cross-tabulation analysis of respondents' answers to questions about CBDC design and trust in the central bank

	Confidence that the central bank will guarantee the anonymity of transactions	Trust that the central bank's independence will allow it to guarantee anonymity
Preference of anonymity over functionality	$\chi^2 = 1.253$ p = 0.263 Phi = 0.090	$\chi^2 = 0.911$ p = 0.339 Phi = 0.076
Confidence that the central bank will guarantee the anonymity of transactions		$\chi^2 = 46.662$ p = 0.000 Phi = 0.547

Source: Authors calculations.

As can be seen from Table 4, there is no connection between the choice in favour of anonymity and trust in the central bank. That is, as in the previous cases, respondents most likely perceive CBDC design attributes and the status of their issuer as separate classes of phenomena. A high statistical correlation of answers to questions about trust indicates an obvious consistency among respondents. If they trust the central bank as a guarantor of anonymity, they trust that its independence is the basis of this.

Several conclusions emerge from the cross-tabulation analysis. Firstly, trust in the central bank and its independence is perceived by respondents as a holistic phenomenon, which is not the same as a choice between design options for digital money. Secondly, this may play a greater role in the demand for CBDC than formally opposes particular design elements, especially if there is an information asymmetry or a barrier of understanding regarding them. Thirdly, even if social choice regarding CBDC design elements may reflect a divergence between stated priorities and actual demand, the latter will be highly sensitive to how the functionality creates a "nice bonus of privacy assurance" derived from the central bank's institutional position. Fourthly, the nature of the relationship between privacy/anonymity preferences and trust in the central bank as an embodiment of authority requires further study.

6. DISCUSSION

The privacy paradox turned out to be a rather complex behavioural phenomenon. Conceptual discussions about its nature (Solove, 2021, Kokolakis, 2017, Barth et al., 2017, Gerber et al., 2018) indicate that an initial interpretation of what is the difference in stated preferences and actual actions is important. On the other hand, if context is crucial (Barth et al., 2019, Brits and Jonker, 2023, Van der Cruijsen, 2020), it opens the way for each individual case of human-digital interaction to be analysed for the subject of preferences consistency as well as coincidence of preferences and behaviour. As can be seen from this study, CBDC is not an exception. Moreover, in the case of CBDC, it is of fundamental importance, since the demand for it and the authority of the central bank as a regulator and guarantor of macro-financial stability will depend on the socially acceptable design of the digital currency.

Privacy is seen as a policy priority (ECB, 2019) and an important design component of central bank digital currency (Choi et al., 2023). At the same time, according to the results of our research, the priority of transaction anonymity over functionality, which is evidence of the high value of privacy in the stated preferences, is not a hard fact. This is evident from the nature of the relationships between the individual indices of general digital and financial privacy, the lack of statistical significance between the level of these indices, and the affirmative response regarding the preference for anonymity over functionality. This conclusion is close to the results, which emphasise the privacy calculus and the fact that in certain contexts, functionality is crucial (Kantar Public, 2022, Barth et al., 2019, Brits and Jonker, 2023, Van der Cruijsen, 2020). The results presented in this work regarding the trust in the central bank as a CBDC issuer are similar to those obtained in (Bijlsma et al., 2021, Abramova et al., 2022, Choi et al., 2023). However, there are some differences.

The empirical testing results of the nature of respondents' answers proved that the issue of the privacy paradox will continue to be debated, along with the discovery of some new patterns of relationships not yet described in the literature.

According to our research, respondents perceive the fact of trust in the central bank as a separate phenomenon from the fact of privacy preferences. This is indicated by the weak relationship between the answers to the question about the preference for anonymity of transactions over the functionality of the design and by the trust in the ability of the central bank to guarantee ano-

nymity. That is, the choice regarding the anonymity of transactions or the functionality of their implementation in respondents' perception does not depend on how they trust the central bank's ability to guarantee such anonymity. It follows that the positioning of CBDC design exclusively in the categories of high privacy protection standards should not be perceived as an imperative. Moreover, if you adjust for the age of the potential target audience, for which the priority of privacy is not high, a better approach to CBDC design and the corresponding positioning of a central bank digital currency would be an emphasis on functionality (some aspects of such an approach are presented in Panetta (2023)), with privacy as a "nice bonus".

7. CONCLUSIONS

The privacy paradox has long generated discussions about the nature of human behaviour in the digital world and the optimal choice of personal data protection algorithms. For central banks, this raised the question of how transaction anonymity should be placed in the framework of CBDC design, taking into account the technological possibilities of tracing transactions, competition with traditional fiat money, which by its very nature guarantees privacy, the right of citizens to privacy and financial monitoring standards. It is already clear from existing policies regarding CBDC design that central banks can take quite different paths. China relies on the doctrine of limited privacy, while the ECB insists that the privacy of the digital euro should be a cornerstone of its design.

In light of the prospects for the CBDC proliferation and the importance central banks attach to their optimal design, the study of the privacy paradox is of considerable practical interest. However, the final results are still up for debate. This is related to both the theoretical issues of understanding the content of the privacy paradox and the relevant empirical method of its diagnosis. Although most surveys on CBDC design start from prioritising privacy for economic agents, the preference for transaction anonymity over functionality is not dominant in the context of payment services, payment habits, etc.

In contrast to a direct survey about the preference for privacy or the design of choosing respondents from among alternatives, the article proposes to determine the propensity for privacy in an indirect way. This also made it possible to reinforce the role of context and remove the privacy paradox approach direct caveat about differences in stated preferences and actual actions. Determining individual indices of the propensity for privacy (indices of general privacy, privacy in the digital and financial environments) based on a survey and comparing the levels of these indices with answers to questions about the preference for anonymity of transactions over functionality have not shown convincing results to confirm or deny the privacy paradox. Despite this, respondents show a consistency of preferences for general privacy and privacy in the digital and financial environments. However, the distribution nature of the calculated three indices indicates certain differences that can be qualified as a weak form of the privacy paradox. Considering the weak relationship between the level of individual privacy preference indices and the choice between anonymity and functionality and the strong relationship between trust in the central bank as a guarantor of anonymity and trust in its independence, it is clear that CBDC design policy can be specified. It seems more optimal to focus on CBDC functionality, where transactional data privacy would be a "nice bonus". At the same time, the significant role of trust in the central bank in the success of CBDC points to the need to maintain their independence in light of the new challenges of the digital age.

REFERENCES

Abramova, S., Böhme, R., Elsinger, H., Stix, H., and Summer, M. (2022). What can CBDC designers learn from asking potential users? Results from a survey of Austrian residents. *Oesterreichische Nationalbank Working Paper 241*. https://ideas.repec.org/p/onb/oenbwp/241.html

Acquisti A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In: *EC '04 Proceedings of the 5th ACM Conference on Electronic Commerce*, USA, 21-29. https://doi.org/10.1145/988772.988777

Acquisti A., Grossklags J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 2, 24-30. https://doi.org/:10.1109/MSP.2005.22

Acquisti, A, Taylor, C., and Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 52(2), 442-492. http://dx.doi.org/10.2139/ssrn.2580411

Agur, I., A. Ari, and G. Dell'Ariccia (2022): Designing central bank digital currencies, *Journal of Monetary Economics*, 125, 62–79. https://doi.org/10.5089/9781513519883.001

Andolfatto, D. (2020). Assessing the Impact of Central Bank Digital Currency on Private Banks, *The Economic Journal*, 131, 525–540. https://doi.org/10.20955/wp.2018.026

Athey, S., Catalini, C. and Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk. *NBER Working Paper 23488*. https://www.nber.org/system/files/working_papers/w23488/w23488.pdf

Bank of England (2020). Central Bank Digital Currency: Opportunities, Challenges, and Designs, *Bank of England Discussion Paper*. https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

Barnes S.(2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). https://doi.org/10.5210/fm.v11i9.1394

Barth S., Menno D., de Jong T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*. 34. pp. 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Barth, S., De Jong, M.D.T., Junger, M., Hartel, P.H. and Roppelt, J.C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematic and Informatics*, 41, 55-69. https://doi.org/10.1016/j.tele.2019.03.003

Bijlsma M., van der Cruijsen C., Jonker N., Reijerink J. (2021). What triggers consumer adoption of CBDC? *De Nederlandsche Bank Working Paper 709*. pp. 1-33. https://doi.org/10.2139/ssrn.3839477

Borgonovo E., Caselli S., Cillo A., Masciandaro D., Rabitti G. (2021). Money, Privacy, Anonymity: What Do Experiments Tell Us? *Journal of Financial Stability*. Vol. 56. https://doi.org/10.1016/j.jfs.2021.100934

Brits H., Jonker N. (2023). The Use of Financial Apps: Privacy Paradox or Privacy Calculus? *De Nederlandsche Bank Working Paper No. 794*. pp. 1-46. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4624569

Brooks S. (2021). Revisiting the Monetary Sovereignty Rationale for CBDCs. *Bank of Canada Staff Discussion Paper*. — 2021-17. pp. 1-29. https://doi.org/10.34989/sdp-2021-17

Brunnermeier M., James H., Landau J.P. (2019). The Digitalization of Money. *NBER Working Paper №26300*. P. 1-32. http://dx.doi.org/10.3386/w26300

Brunnermeier M., Niepelt D. (2019). On the Equivalence of Private and Public Money. *Journal of Monetary Economics*. 106. pp. 27-41. https://doi.org/10.1016/j.jmoneco.2019.07.004

Chen, L., Huang, Y., Ouyang, S., and Xiong, W. (2021). The data privacy paradox and digital demand. *NBER Working Paper 28854*. https://www.nber.org/system/files/working_papers/w28854/w28854.pdf

Choi S., Kim B., Kim Y.-S., Kwon O. (2023). Central Bank Digital Currency and Privacy: A Randomized Survey Experiment. *BIS Working Paper № 1147*. pp. 1-61. http://dx.doi.org/10.2139/ssrn.4204110

Cloos J., Frank B., Kampenhuber L., Karam S., Luong N., Moller D., Monge-Larrain M., Tan Dat N., Nilgen M., Rossler Ch. (2019). Is Your Privacy for Sale? An Experiment on the Willingness to Reveal Sensitive Information. *Games*. 10, 28. pp. 2-15. https://doi.org/10.3390/g10030028

Cruijsen C. van der (2020). Payments data: do consumers want banks to keep them in a safe or turn them into gold? *Applied Economics*. 52(6), 609 – 622. https://doi.org/10.1080/00036846.2019.1659493

Culnan M., Armstrong P. (1999). Infromation privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organizational Science*. 10 (1), 340-347. https://doi.org/10.1287/orsc.10.1.104

ECB. Digital euro: Experimentation, scope and key learnings. *Technical report, European Central Bank*, April 2021(b). https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf

ECB. Eurosystem report on the public consultation on a digital euro. *Consultation report, European Central Bank*, April 2021(a). https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

Eichengreen B. (2022). The Trilemma of Central Bank Digital Currencies. *Project Syndicate*. November 9. https://www.project-syndicate.org/commentary/flawed-assumptions-driving-race-for-cbdcs-by-barry-eichengreen-2022-11

European Central Bank (2019). Exploring Anonymity in Central Bank Digital Currencies. *ECB. In Focus* №4. 1-11. https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.mipinfocus191217.da.pdf

European Central Bank (2021). Eurosystem report on the public consultation on a digital euro. April 2021. https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

Fanti G. (2022). An Apparent Trilemma for Cross Border Central Bank Digital Currencies. *Harward National Security Journal*. Vol. 14, 75-86. https://harvardnsj.org/wp-content/uploads/2022/12/Fanti_14-Harv.-Natl-Sec.-J.-75-2022.pdf

Frost J. (2020). The economic forces driving fintech adoption across countries. *BIS Working Paper № 838*, 1-16. https://www.bis.org/publ/work838.htm

Garratt, R. J. and van Oordt, M. R. C. (2021). Privacy as a Public Good: A Case for Electronic Cash. *Journal of Political Economy*, 129 (7), 2157–2180. https://doi.org/10.1086/714133

Gerber N., Gerber P., Volkamer M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security*. 77. 226-261. https://doi.org/10.1016/j.cose.2018.04.002

Gimpel, H., Kleindienst, D. and Waldmann, D. (2018). The disclosure of private data: measuring the privacy paradox in digital services. *Electronic Markets*, 28, 475-490. https://doi.org/10.1007/s12525-018-0303-8

Goldfarb A., Que V. (2023). The Economics of Digital Privacy. *Annual Review of Economics*. 15, 267-86. https://doi.org/10.1146/annurev-economics-082322-014346

Hernandez de Cos P. (2023). The Digital Euro Project – A New Milestone. Speech by Mr Pablo Hernández de Cos, Governor of the Bank of Spain, at the Annual Convention of the Asociación de Mercados Financieros, Madrid, 20 November 2023. https://www.bis.org/review/r231121i.pdf

Hess T., Becker M., Klausinn S. (2019). Uncovering the Privacy Paradox: The Influence of Distraction on Data Disclosure Decisions. *Conference: Proceedings of the 27th European Conference on Information Systems (ECIS 2019)*. At: Stockholm & Uppsala, Sweden, 1-14. https://salo.li/9B26ecf

Hirschprung R. (2023). Is the Privacy Paradox a Domain-Specific Phenomenon. *Computers*. 12. 156. 1-14. https://doi.org/10.3390/computers12080156

Jiang J. (2020). CBDC adoption and usage: some insights from field and laboratory experiments. *Bank of Canda Staff Analytical Note*, 12,1-12. https://doi.org/10.34989/san-2020-12

Kahn Ch., McAndrews J., Roberds W. (2005). Money is Privacy. *International Economic Review*. 46. (2), 377-399. https://doi.org/10.1111/j.1468-2354.2005.00323.x

Kantar Public. Study on new digital payment methods. *Kantar Public - commissioned by the European Central Bank*, 2022. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.dedocs220330_annex_summary.en.pdf

Kocherlakota, N. (1998). Money is Memory. *Journal of Economic Theory, 81(2),* 232-251. https://doi.org/10.1006/jeth.1997.2357

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: *A review of current research on the privacy paradox phenomenon. Computer & Security*, 64, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Koziuk V. (2021a). Confidence in digital money: Are central banks more trusted than age is matter? *Investment Management and Financial Innovations, 18 (1),* 12-32. https://doi.org/10.21511/imfi.18(1).2021.02

Koziuk V. (2021b). Willingness to adopt digital currency: whether central bank independence is important. *Finance of Ukraine*, 3, 7-22. https://doi.org/10.33763/finukr2021.03.007

Koziuk V. (2022). What do cross-country Bitcoin holdings tell us? *Monetary and institutional discontent vs financial development, 19 (1),* 168-185. https://doi.org/10.21511/imfi.19(1).2022.13

Koziuk V., Ivashuk Y. (2022). Does it Matter for CBDC Design? Privacy-Anonymity Preferences from the Side of Hierarchies and Egalitarian Cultural Patterns. *ECONOMICS - Innovative and Economics Research Journal,* 10 (1), 35-53. https://doi.org/10.2478/eoik-2022-0008

Mancini-Griffoli, T., Martinez Peria, M. S., Agur, I., Ari, A., Kiff, J., Popescu, A., &Rochon, C. (2018). *Casting Light on Central Bank Digital Currency* (IMF Staff Discussion Notes No. 18/08). https://doi.org/10.5089/9781484384572.006

Masciandaro D. (2018). Central Bank Digital Cash and Cryptocurrencies: Insights from Baumol-Friedman Demand for Money. *Australia Economic Review*. 51. pp. 1-11. https://doi.org/10.1111/1467-8462.12304

Norberg P., Horne D., Horne D. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Paneta F. (2023). The cost of not issuing a digital euro. CEPR-ECB Conference The macroeconomic implications of central bank digital currencies. Frankfurt am Main, 23 November 2023. https://www.ecb.europa.eu/press/conferences/shared/pdf/20231123_cepr_ecb/Panetta_speech.ga.pdf

Pfister Ch., de Seze N. (2023). Who Needs an e-Yuan?. *SUERF Policy Brief No 716*, 1-7. https://www.suerf.org/publications/suerf-policy-notes-and-briefs/who-needs-an-e-yuan/

Radukić S., Mastilo Z., Kostić Z. (2019) Effects of Digital Transformation and Network Externalities in the Telecommunication Markets. *ECONOMICS - Innovative and Economics Research Journal,* 7(2). https://doi.org/10.2478/eoik-2019-0019

Rosati P., Fox G., Cummins M., Lynn T. (2022). Perceived Risk as a Determinant of Propemsity to Adopt Account Information Servcies under the EU Payment Services Directive. *Journal of Theoretical and Applied Electronic Commerce Research*, 17, 493 – 506. https://doi.org/10.3390/jtaer17020026

Schomakers, E.-V., Lidynia, C., and Ziefle, M. (2019). A typology of online privacy personalities. *Journal of Grid Computing*, 17, 727-747. https://doi.org/10.1007/s10723-019-09500-3

Soderberg G., Kiff J., Tourpe H., Bechara M., Forte S., Kao K., Lannquist A., Sun T., Yoshinaga A. (2023). How Should Central Banks Explore Central Bank Digital Currency? *FinTech Note 008*, 1-43. http://surl.li/ulcah

Solove, D.J. (2021). The myth of the privacy paradox. *George Washington Law Review*, 89(1), 1-51. http://dx.doi.org/10.2139/ssrn.3536265

Syngjoo Choi, Bongseob Kim, Young-Sik Kim, Ohik Kwon. (2023). Central Bank Digital Currency and Privacy: A Randomized Survey Experiment. *BIS Working Papers No 1147*, 1-61. https://www.bis.org/publ/work1147.htm

Tsang Ch.-U., Yang A., Chen P.-K. (2023). Disciplining CBDC: Addressing the Privacy Aspects and Central Bank Independence. *Northwestern Journal of International Law and Business*, 43 (3), 235-289. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4253888

UK Parliament. (2023). Central Bank Digital Currency: Solution in Search of a Problem. House of Lord. Economic Affairs Committee. 3rd Report on Session 2021-2022. 52 p. https://publications.parliament.uk/pa/ld5802/ldselect/ldeconaf/131/13102.htm

Williamson, S. (2022). Central Bank Digital Currency: Welfare and Policy Implications. *Journal of Political Economy,* 130 (11), 2829-2861. https://doi.org/10.1086/720457

World Economic Forum (2021). Privacy and Confidentiality of Central Bank Digital Currency. *White Paper*. 1-21. https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf

Appendix A

Structure of the questionnaire for determining indices of individual propensity for privacy: general, in the digital and financial environments

Questionnaire related to privacy

General attitude to privacy

Question	Answer option	Points
Are you in comfort about to disclose information about your wealth (property, cash) on a claim	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you think that to disclose information about wealth helps to improve the public services	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you think that to disclose information about wealth helps to improve private services	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you prefer to meet with friends at your home	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you think that it is not necessary for kids to have separate room	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
While living in hostel will you prefer bigger number of neighbors	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Are you ready to share your personal hygiene things	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2

Question	Answer option	Points
	In any case	1
Do you often tell about events from your life during a long trip	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Is it appropriate to you to discuss sharp political or social issues with little known people	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Is it appropriate to you to share emotions or experiences from your private life with colleagues or not close friends	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1

Attitude to privacy in the digital environment

Question	Answer option	Points
Are you active in social media	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you think that it is better when a social media profile (account) is open	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you share information about your private life events (traveling, visiting interest place / events, meeting with friends) in social media	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you try to fulfill information in your social media profile (account) properly and timely	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2

Question	Answer option	**Points**
	In any case	1
Are you in comfort to fulfill a columns during on-line polls or registrations	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you fulfill information about you in on-line polls or registrations when it is possible not to do	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you agree that it is appropriate to trace web-sights visitors personal data	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you allow to trace your personal data while visiting web-sights	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you think that digital services activity regulations are proper guaranty against commercial use of your personal data	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Is it appropriate for you that your personal data could be in commercial use without your permission even when it's help with quality of services that you can potentially consume	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1

Attitude to privacy in case of money and finance in an institutional environment

Question	Answer option	Points
Do you prefer digital (arm-length) form of money transactions even when it is require initial client identification	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you think that digital transactions guaranty the same level of anonymity as a paper money	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Are you in comfort with client identification procedure in financial institutions	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you think that information about you as a client is better protected in state-owned financial institutions than in privately-owned	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you presume that financial institutions must share information about you as a client on a claim of relevant authorities	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you presume that financial institutions invest considerable efforts (funds) to protect your personal data	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you think that financial authorities guaranty protection of your personal data (client information) against abuse of other authorities	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2

Question	Answer option	Points
	In any case	1
Do you think that financial authorities accumulate and proceed information about personal transactions only for better regulations	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Do you agree that to share personal data is more risky when it's required by financial institution with monopolistic power	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1
Is it appropriate for you to think that traceability of money (financial) transactions will be a social norm in a society	In no case	5
	Rather not	4
	I don't know	3
	Rather yes	2
	In any case	1