Dujam Kovač
University of Split
Faculty of Economics,
Business and Tourism
21000 Split, Croatia
dujam.kovac@efst.hr

Antea Jovanović
University of Split
Faculty of Economics,
Business and Tourism
21000 Split, Croatia
ajovan00@live.efst.hr

Mario Pečarić
University of Split / University of Rijeka
Faculty of Economics, Business
and Tourism / Faculty of
Economics and Business
21000 Split / 51000 Rijeka, Croatia
mario.pecaric@efst.hr

JEL: E42, G21, O33
Original scientific article
https://doi.org/10.51680/ev.38.2.8

Received: June 18, 2025
Revision received: September 1, 2025
Accepted for publishing: September 5, 2025

DETERMINANTS OF DIGITAL EURO ACCEPTANCE AMONG STUDENTS: THE ROLE OF PRIVACY CONCERNS AND THE LIMITATIONS OF SECURITY MEASURES

Abstract

Purpose: The research examines the factors influencing university students' intention to use the digital euro, problematising the role of privacy concerns and the effectiveness of security measures

Methodology: The research is based on survey data from 150 students at the Faculty of Economics, Business and Tourism, University of Split, Croatia. Binary logistic regression, ROC curve analysis and chi-square independence tests were used.

Results: The results show that privacy concerns compared to other payment methods, preference for cash payments, belief in lower transaction cost, and familiarity with the digital euro significantly influence students' intention to adopt this digital currency. In particular, it was found that a high concern about privacy and a strong preference for cash had a negative impact on the intention to adopt the digital euro. On the other hand, a higher level of belief in lower transaction costs and better familiarity with the digital euro had a positive effect on their willingness to adopt. Additionally, the analysis showed that technical security measures, such as a digital signature, biometrics, encryption and pseudonymisation, did not significantly mitigate students' privacy concerns.

Conclusion: The research highlights the need to tackle privacy issues and strengthen trust in institutions and the legal framework, indicating that technical solutions alone are not enough to encourage adoption of the digital euro. Implementation of the digital euro as a means of payment requires broad strategies that pair technological progress with strong institutional protection, thereby reducing privacy risks and increasing trust of the digital euro as a payment instrument.

Keywords: Digital euro, adoption intention, privacy concerns, security measures, fintech, institutional trust

1. Introduction

The development of fintech has enabled the conceptual development and introduction of central bank digital currencies (CBDCs). Recent research has focused in particular on the digital euro as a form of digital money and complement to cash in the liabilities of the Eurosystem. Extensive discussions and comprehensive progress reports (Deutsche Bundesbank, 2024; European Central Bank, 2024; Tronnier et al., 2022) have highlighted numerous benefits but also a number of potential drawbacks, among which privacy and security concerns related to the use of the digital euro are particularly emphasised (Jabbar et al., 2023; Hamm et al., 2023; Mashatan et al., 2022). The importance of protecting privacy and security is fundamental and was already taken into account in the initial development phases as part of the "privacy by design" approach. In addition to technical aspects, security-related and institutional aspects of implementation, which have received less attention in the literature, are also becoming significant. Even in the case of possible technical deficiencies and shortcomings, the development of a suitable institutional security infrastructure ensures security and the repair of damage. It is also a fundamental link in the adoption of the digital euro, as it strengthens trust and accountability.

This article has two main objectives: first, to examine the factors influencing the intention to use the digital euro and to determine the role of privacy concerns; and second, to determine the importance of security measures in mitigating privacy concerns. These objectives were achieved through a survey of students from the Faculty of Economics, Business and Tourism, University of Split. The sample size was appropriate for the methodological framework and methods used. Binary logistic regression, ROC analysis and chi-square independence tests were used in statistical analyses to investigate the factors influencing the intention to use the digital euro, as well as the role of privacy perceptions and security measures. The analysis showed that students recognise the potential benefits of the digital euro but also stress privacy and the continued importance of cash for payments. This finding raises several questions, one of which is how well they understand the concept of the digital euro itself. The analysis also confirms that technical security solutions do little to ease privacy worries, implying the need to study security measures at the institutional level, specifically, how effectively legislation is implemented.

The paper consists of six sections. After the introduction, Section 2, which deals with theoretical and conceptual background, defines the importance of privacy and security in the development of the digital euro. The third section presents the research methodology, while the fourth section analyses the research results. The fifth section develops the discussion, reviews the paper's contribution, and provides directions for further research. Finally, the concluding considerations are presented in Section 6.

2. Theoretical and conceptual background

The discussion about central bank digital currencies (CBDCs) is becoming increasingly important. The digital euro, which was developed by the European Central Bank as a complement to cash to improve the efficiency of the payment system, financial integration and monetary sovereignty of the eurozone, occupies an important place in recent discussions and research. Despite numerous advantages such as speed, convenience and efficiency of transactions, the digital euro brings with it various challenges, with privacy protection being particularly emphasised.

The perception of risk in relation to the introduction of the digital euro, in particular the potential loss of privacy, is a decisive factor in the adoption of new technologies (Deutsche Bundesbank 2024, 2021; De Nederlandsche Bank 2021). This becomes clear when users realise that by paying with the digital euro, they are making their personal financial data (spending habits) accessible within the system. In line with the "privacy by design" approach, privacy protection is a core element of the architecture of the digital euro, which emphasises the anonymity of offline transactions. Nevertheless, the literature highlights challenges posed by centralised infrastructures that are vulnerable to cyber-attacks and regulatory abuse (Kramcsák et al., 2024), which exacerbates users' privacy concerns.

The literature review focuses on two areas: firstly, analysis of previous research on privacy concerns with a focus on the digital euro, and secondly, analysis of the literature on perceptions of the effectiveness of security measures and their influence on technology adoption.

In the fintech industry, privacy refers to the right of users to control access to their personal financial data, while risk refers to the possibility of adverse consequences when using certain technologies or

services (Karwatzki et al., 2022). In addition to traditional financial risks such as loss of money, fintech is increasingly faced with threats related to loss of privacy, security of digital identity and misuse of data (Mashatan et al., 2022). Digital currencies, especially the digital euro as a prime example of a CBDC, can increase the perceived risk and fear for privacy as transaction data is transparent (Borgonovo et al., 2019; Herskind et al., 2020). Hamm et al. (2023) confirm that privacy concerns significantly influence the intention to adopt digital currencies. According to Jabbar et al. (2023), users weigh the benefits against the risks and are willing to sacrifice some privacy if practical benefits such as ease of use justify it. The "digital privacy paradox" is notable as users claim to value privacy but often jeopardise it for relatively small benefits (Athey et al., 2017). Privacy concerns are shaped by the transparency of data use, the risk of data breaches and the demographic, psychological and cultural characteristics of users (Tronnier et al., 2022; Voskobojnikov et al., 2020; Gao et al., 2016).

In addition to privacy risks, the general perception of risk significantly influences users' attitudes towards digital currencies (Chen & Farkas, 2019). In addition to privacy concerns, users evaluate several other risk dimensions, such as financial and operational risks (Abramova & Böhme, 2016; Mashatan et al., 2022). To understand how these perceptions determine users' intentions and behaviour, researchers rely on established theoretical models. Frameworks such as the Technology Acceptance Model (TAM) and the Theory of Planned Behaviour (TPB) are commonly used to explain how perceived risks influence technology adoption (Tronnier et al., 2022; Marriott et al., 2017).

Although privacy concerns and risk perceptions dominate discussions about digital currency adoption, perceptions of security measures significantly influence users' trust in financial technologies. According to Zaghloul et al. (2020) and Krombholz et al. (2016), typical security technologies such as digital signatures, biometrics, encryption and pseudonymisation are generally perceived positively by users, yet they are often accompanied by unrealistic expectations regarding their effectiveness. Even though biometrics and pseudonymisation can mitigate privacy concerns to a certain extent, research shows that their implementation is often not enough to significantly reduce users' fears (Mashatan et al., 2022; Jabbar et al., 2023). There is therefore a noticeable gap between user expectations and the actual technical capabilities of these measures, which means that a high level of perceived risk remains despite advanced security technologies (Herskind et al., 2020).

3. Methodology

3.1 Description of the sample and operationalisation of the key variables

The study was conducted using survey data collected between July and September 2024. The target population consisted of students from the Faculty of Economics, Business and Tourism, University of Split, selected for their relevance as potential future users of the digital euro and assumed to be more familiar with the concept of the digital euro compared to the wider population. A non-random sample was used, targeting accessible and willing participants within this population. Surveys were distributed through personal invitations within faculty channels (student mailing lists). The total sample size was 150 respondents, which was appropriate for the exploratory nature of the study and the statistical methods used (binary logistic regression and chi-square tests). The data were collected using electronic surveys via Google Forms, which ensure anonymity and easy access. While this sampling frame is not representative of the entire Croatian or EU student population, it allowed for targeted insights into a subgroup with greater familiarity with economic concepts, payment systems, and the (digital) euro.

The questionnaire consisted of closed questions to operationalise the variables of interest, primarily on a Likert scale from 1 to 5. However, the main dependent variable, intention to use the digital euro, was measured using a categorical scale with four distinct options to capture nuanced attitudes towards adoption. This scale was chosen to reflect realistic decision-making stages rather than a standard agreement continuum. The independent variables included perceptions and attitudes (*privacy concerns, sense of security, familiarity with the concept, importance of cash*) and socio-demographic characteristics, including gender and year of study (see Table 1). The variables were dichotomised to simplify the analysis and provide clearer insights into the differences between groups of respondents and to ensure consistency of statisti-

cal processing. This approach maintains analytical relevance while promoting interpretative clarity of the results.

Within the sample, 70% of respondents were female (n=105), while 30% were male (n=45). In addition, the distribution of respondents by their year of study was as follows: 12.7% were first-year students (n=19), 7.3% second-year (n=11), 27.3% third-year (n=41), 18.7% fourth-year (n=28), and 34.0% fifth-year students (n=51). This structure indicates that the majority of participants were in the more advanced stages of their studies, which may have influenced their familiarity with economic and financial concepts, and consequently their ability to evaluate the potential introduction of the digital euro.

Table 1 Definition and operationalisation of key variables

Variable status	Variable name	Original measurement scale	Recoding
Dependent variable	Intention to use Dig_EUR	{1, Yes, immediately}; {2, Yes, after some time}; {3, No}; {4, Not sure}	Dichotomous variable - {1,2, Intention to use}; {3,4, No intention to use}
Independent variable	Privacy concerns	{1, Not at all concerned}; {2, Slightly concerned}; {3, Moderately concerned}; {4, Concerned}; {5, Very concerned}	Dichotomous variable - {1,2,3, Low to moderate concern}; {4,5, High concern}
Independent variable	Belief in lower transaction cost	{1, Do not believe at all}; {2, Slightly believe}; {3, Neutral}; {4, Believe}; {5, Strongly believe}	Dichotomous variable - {1,2,3, Low to moderate belief}; {4,5, High belief}
Independent variable	Belief in greater security compared to cryptocurrencies	{1, Do not believe at all}; {2, Slightly believe}; {3, Neutral}; {4, Believe}; {5, Strongly believe}	Dichotomous variable - {1,2,3, Low to moderate belief}; {4,5, High belief}
Independent variable	Belief in complexity of use	{1, Don't believe at all}; {2, Believe a little}; {3, Neutral}; {4, Believe}; {5, Strongly believe}	Dichotomous variable - {1,2,3, Low to moderate belief}; {4,5, High belief}
Independent variable	Familiarity with Dig_EUR	{1, Not at all familiar}; {2, Slightly familiar}; {3, Somewhat familiar}; {4, Well familiar}; {5, Very well familiar}	Dichotomous variable - {1,2,3, Low to moderate familiarity}; {4,5, High familiarity}
Independent variable	Use of financial technology	{1, Never}; {2, Rarely}; {3, Sometimes}; {4, Often}; {5, Almost always}	Dichotomous variable - {1,2,3, Rare or moderate use}; {4,5, Frequent or intensive use}
Independent variable	Importance of cash	{1, Not at all important}; {2, Slightly important}; {3, Moderately important}; {4, Very important}; {5, Extremely important}	Dichotomous variable - {1,2,3, Low to moderate importance}; {4,5, High importance}
Independent variable	Source of information	{1, Faculty}; {2, Media}; {3, Internet}; {4, Social networks}; {5, Personal contact}; {6, Professional publications}; {7, Banks}; {8, Other}	Categorical variable - {1,6, Faculty and professional publications}; {2,3,4,5,7,8, Other}
Independent variable	Gender	{1, Female}; {2, Male}	Categorical variable - {1, Female}; {2, Male}
Independent variable	Year of study	{1, First year}; {2, Second year}; {3, Third year}; {4, Fourth year}; {5, Fifth year}	Dichotomous variable - {1,2,3, Undergraduate level}; {4,5, Graduate level}

Variable status	Variable name	Original measurement scale	Recoding
Independent / **Dependent variable**	Belief in privacy concerns compared to other payment methods	{1, No impact}; {2, Low impact}; {3, Moderate impact}; {4, Significant impact}; {5, Complete threat to privacy}	Dichotomous variable - {1,2,3, Low to moderate perceived threat}; {4,5, High perceived threat}
Independent variable	Measure - Digital signature	{1, Not at all important}; {2, Slightly important}; {3, Moderately important}; {4, Very important}; {5, Extremely important}	Dichotomous variable - {1,2,3, Low to moderate importance}; {4,5, High importance}
Independent variable	Measure - Biometrics	{1, Not at all important}; {2, Slightly important}; {3, Moderately important}; {4, Very important}; {5, Extremely important}	Dichotomous variable - {1,2,3, Low to moderate importance}; {4,5, High importance}
Independent variable	Measure - Authorisation control	{1, Not at all important}; {2, Slightly important}; {3, Moderately important}; {4, Very important}; {5, Extremely important}	Dichotomous variable - {1,2,3, Low to moderate importance}; {4,5, High importance}
Independent variable	Measure - Encryption	{1, Not at all important}; {2, Slightly important}; {3, Moderately important}; {4, Very important}; {5, Extremely important}	Dichotomous variable - {1,2,3, Low to moderate importance}; {4,5, High importance}
Independent variable	Measure - Pseudonymisation	{1, Not at all important}; {2, Slightly important}; {3, Moderately important}; {4, Very important}; {5, Extremely important}	Dichotomous variable - {1,2,3, Low to moderate importance}; {4,5, High importance}

Note: Questionnaire items were adapted for research purposes based on the following sources: Deutsche Bundesbank (2024); Tronnier et al. (2022); Deutsche Bundesbank (2021).

Source: Compiled by the authors

The descriptive statistics of the variables indicate several key characteristics of the respondents. The variables related to the use of financial technology have the highest value (M=4.20, SD=0.867), indicating frequent use by the respondents. Security measures, in particular authorisation control (M=4.17, SD=1.096), encryption (M=4.16, SD=1.106), and biometric authentication (M=4.15, SD=1.110), were rated highly, indicating a high level of sensitivity to the security aspects of the digital euro. The variables describing the perceived complexity of using the digital euro (M=2.27, SD=1.028) and familiarity with the concept of the digital euro (M=2.50, SD=1.008) had the lowest mean scores, indicating a relatively low perceived complexity but also limited familiarity with the concept itself. The analysis of distribution asymmetry shows a predominant negative asymmetry for variables relating to security measures and the use of fintech, indicating that most respondents rate these aspects highly. Conversely, a positive asymmetry was found for the intention to use the digital euro (skewness=0.690), indicating significant reservations about immediate adoption. Most of the variables showed a slightly negative kurtosis, which indicates a slightly larger dispersion compared to the normal distribution.

The descriptive analysis shows an intriguing pattern: respondents express major concerns about privacy protection while at the same time being in favour of technical security measures such as authorisation control, encryption and biometric authentication. In the context of the digital euro, this paradox suggests that technical solutions alone are not enough to gain the trust of users.

Table 2 Descriptive statistics

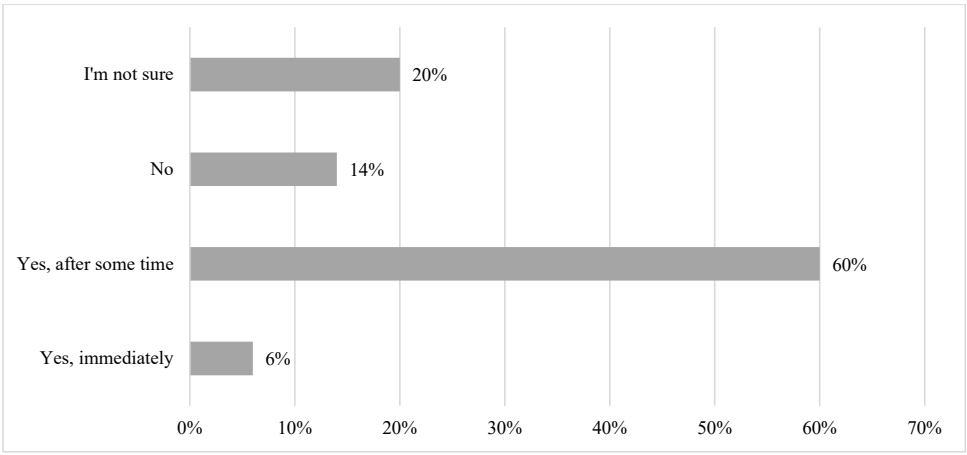
Variable	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Intention to use Dig_EUR	150	1	4	2.48	.880	.690	.198	-.621	.394
Privacy concern	150	1	5	2.97	1.223	.064	.198	-.863	.394
Belief in lower transaction cost	150	1	5	2.90	1.122	-.176	.198	-.806	.394
Belief in greater security compared to cryptocurrencies	150	1	5	3.29	1.051	-.633	.198	.044	.394
Belief in complexity of use	150	1	5	2.27	1.028	.384	.198	-.512	.394
Familiarity with Dig_EUR	150	1	5	2.50	1.008	.299	.198	-.261	.394
Use of financial technology	150	2	5	4.20	.867	-1.027	.198	.520	.394
Importance of cash	150	1	5	3.33	1.028	-.106	.198	-.393	.394
Year of study	150	1	5	3.54	1.359	-.532	.198	-.831	.394
Belief in privacy concerns compared to other payment methods	150	1	5	2.95	.992	-.240	.198	-.158	.394
Measure - Digital signature	150	1	5	3.98	1.261	-.980	.198	-.151	.394
Measure - Biometrics	150	1	5	4.15	1.110	-1.085	.198	.177	.394
Measure - Authorisation control	150	1	5	4.17	1.096	-1.082	.198	.103	.394
Measure - Encryption	150	1	5	4.16	1.106	-1.107	.198	.243	.394
Measure - Pseudonymisation	150	1	5	3.85	1.167	-.687	.198	-.384	.394

Source: Compiled by the authors

The distribution of responses for the main dependent variables of the study, which provide an insight into the attitudes and perceptions of students of the Faculty of Economics, Business and Tourism, University of Split, with regard to the digital euro. The analysis focuses on two main variables: the intention to use the digital euro and the belief that the use of the digital euro is associated with privacy risks.

According to the survey results, 60% of respondents stated that they would use the digital euro, but only after some time. A smaller proportion, 6%, stated that they would use the digital euro as soon as it is available, indicating a degree of confidence in this new technology and digital currency. Conversely, 14% of respondents indicated that they would not use the digital euro, while 20% remained unclear about its use.

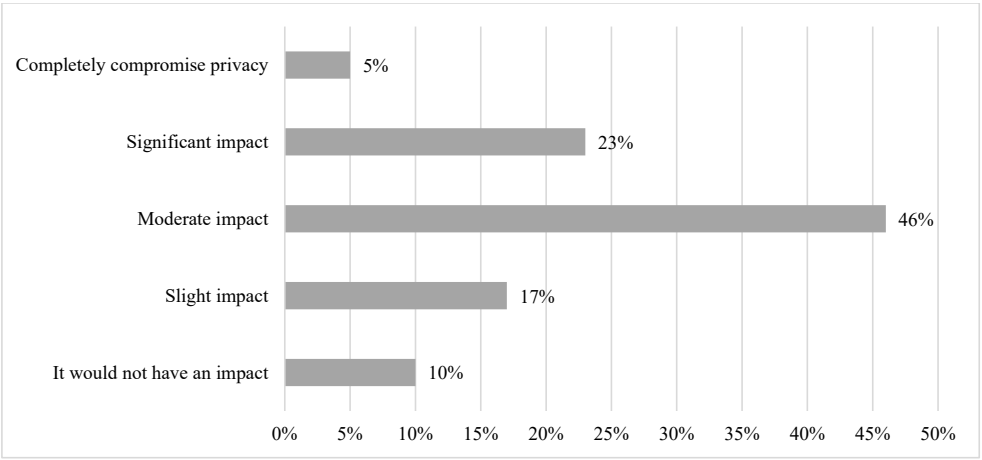
Figure 1 Distribution of responses regarding the intention to use the digital euro



Source: Compiled by the authors

Respondents believe that the digital euro could jeopardise their privacy and see it as a potential risk to the protection of personal data, which could be an obstacle to wider adoption. According to the data collected, 73.4% of respondents believe that the use of the digital euro could moderately, significantly or completely compromise or threaten their privacy. Conversely, only 26.7% believe that this impact would be negligible or non-existent.

Figure 2 Distribution of responses regarding the belief in a threat to privacy from the use of the digital euro compared to other means of payment



Source: Compiled by the authors

3.2 Methods of data analysis

In this study, several statistical methods were used to analyse the collected data. Binary logistic regression was used to identify the main determinants influencing students' intention to use the digital euro. Logistic regression is particularly well suited for modelling dichotomous (binary) outcomes and allows the assessment of relationships between mul-

tiple independent variables and a binary dependent variable through odds ratios, which indicate the probability of an outcome based on changes in the predictor variables (Strzelecka et al., 2020; Szafraniec-Siluta et al., 2022).

A stepwise forward likelihood ratio method was applied, with variables entered sequentially according to the significance criteria ($p < 0.05$ for inclusion and $p > 0.10$ for exclusion). The discriminatory power of the logistic regression model was assessed using a receiver operating characteristics (ROC) analysis, focusing on the ROC-AUC (area under the curve) indicator. AUC values above 0.5 signal good model performance (Strzelecka et al., 2020; Szafraniec-Siluta et al., 2022).

In order to provide additional confirmation of the estimates, chi-square tests were performed to analyse the statistical significance of the relationship between the intention to use the digital euro and the independent variables. All statistical analyses were conducted in IBM SPSS Statistics, version 29.0.

4. Research findings

4.1 Determinants of digital euro acceptance

The first model, which is tested by a binary logistic regression analysis, contains the following variables in addition to those shown in Table 3: *Privacy concerns, Belief that the digital euro is more secure than cryptocurrencies, Perceived complexity of use, Use of financial technology, Year of study, Sources of information (university courses or professional publications)* and *Gender*, that are excluded by the forward stepwise method.

Table 3 Omnibus test of the model

Step	Variables in the model	-2 Log likelihood	Cox & Snell R^2	Nagelkerke R^2	χ^2	p-value
1	Belief in privacy concerns compared to other payment methods	174.612	0.111	0.154	17.699	< 0.001
2	Importance of cash	163.993	0.172	0.238	28.317	< 0.001
3	Belief in lower transaction cost	154.189	0.224	0.311	38.122	< 0.001
4	Familiarity with the digital euro	148.351	0.254	0.352	43.960	< 0.001

Source: Compiled by the authors

Table 4 Final regression model parameters

Predictor	Description	β	S.E.	Wald	df	Sig.	Exp(β)	95% C.I. for Exp(β)
X_1	Belief in privacy concerns compared to other payment methods	1.627	0.447	13.258	1	<0.001	5.090	[2.120 - 12.223]
X_2	Importance of cash	1.542	0.424	13.242	1	<0.001	4.674	[2.037 - 10.726]
X_3	Belief in lower transaction cost	-1.375	0.486	8.000	1	0.005	0.253	[0.097 - 0.656]
X_4	Familiarity with the digital euro	-1.643	0.751	4.791	1	0.029	0.193	[0.044 - 0.842]
Constant		-1.448	1.146	1.594	1	0.207	0.235	/

Source: Compiled by the authors

The model explains between 25.4% (Cox and Snell R^2) and 35.2% (Nagelkerke R^2) of the variance in the intention to use the digital euro. The Hosmer-Lemeshow test confirms a good fit of the model to the data ($\chi^2 = 8.576$, df = 6, $p = 0.199$), according to Hosmer et al. (1997), as the model is considered a good fit if the p-value is greater than 0.05, indicating that there are no significant discrepancies

between predicted and observed values within the prediction deciles. The classification accuracy of the model is 76%, the specificity is 80.8%, and the sensitivity is 66.7%.

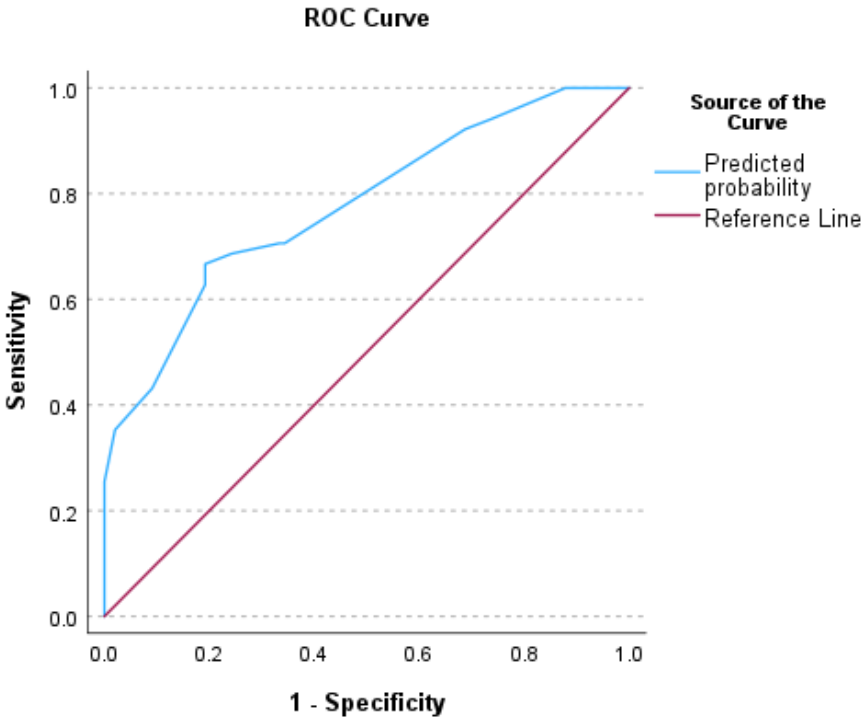
The theoretical logistic regression model is expressed as follows:

$$\text{logit}(p) = -1.448 + 1.627X1 + 1.542X2 - 1.375X3 - 1.643X4.$$

Respondents who perceive a high threat to privacy from the digital euro compared to other means of payment are 5 times more likely not to use it than respondents who perceive a low to medium threat [β=1.627, Exp(β)=5.090, p<0.001]. Respondents for whom cash is very important are 4.7 times more likely not to use the digital euro [β=1.542, Exp(β)=4.674, p<0.001] than respondents who consider cash less important. The model suggests that the threat to privacy and the importance of cash are the biggest barriers to the adoption of the digital euro. Conversely, belief in the efficiency of transactions and familiarity with the digital euro are facilitating factors. Individuals who believe that the digital euro reduces transaction costs are 74.7% less likely to reject it [β=-1.375, Exp(β)=0.253, p=0.005], and individuals who are better informed about the digital euro are 80.7% less likely to reject it [β=-1.643, Exp(β)=0.193, p=0.029].

Additional confirmation of the model quality was obtained by the ROC analysis. The area under the curve (AUC) was 0.777 ≈ 0.8 (SE = 0.041; p < 0.001; CI95% = [0.696 - 0.857]), indicating a very good discriminatory ability of the model according to Fawcett (2006) and Hosmer et al. (2013), which accurately distinguishes between students who intend to use the digital euro and those who do not.

Figure 3 ROC curve for predicting the intention to use the digital euro



Source: Compiled by the authors

To further examine the robustness of the binary logistic regression results, chi-square tests for independence were performed to examine bivariate relationships between the dependent variable, intention to use the digital euro, and individual predictor variables. In contrast to logistic re-

gression, which simultaneously controls for the effects of multiple predictors, chi-square tests allow the identification of potentially significant relationships at the level of individual variables, independent of others. This provides a more comprehensive insight into the data patterns and confirms the results obtained with the multidimensional model.

Table 5 Chi-square test results for associations with the intention to use the digital euro

Variable	X^2 value	p-value	Confirmed by binary logistic regression
Belief in privacy concerns compared to other payment methods	18.297	< 0.001	Yes
Importance of cash	14.61	< 0.001	Yes
Belief in lower transaction cost	6.551	0.01	Yes
Familiarity with the digital euro	4.229	0.04	Yes
Privacy concerns	14.441	< 0.001	No
Perceived complexity of use	9.638	0.002	No
Opposition to digital money	9.037	0.003	No
Perceived security (digital euro is more secure)	6.805	0.009	No
Belief in security compared to cryptocurrencies	4.015	0.045	No

Source: Compiled by the authors

4.2 Concerns about privacy and the limits of security measures

Having established that privacy concerns are the most important predictor of the intention to adopt a digital euro, in this analysis we investigated whether technical security measures that can provide greater privacy protection can effectively mitigate these concerns. A binary logistic regression using a forward stepwise method (likelihood ratio) examined the effects of security measures on students' concerns about using the digital euro. The measures were the digital signature, biometrics, authorisation control, encryption and pseudonymisation.

The logistic regression results showed that none of the security measures made statistically significant contributions to the model ($p > 0.05$).

Table 6 First selection results for security variables in logistic regression

Variable	Score	df	p-value
Measure - Digital signature	0.743	1	0.389
Measure - Biometrics	1.112	1	0.292
Measure - Authorisation control	0.135	1	0.713
Measure - Encryption	0.024	1	0.878
Measure - Pseudonymisation	0.944	1	0.331

Source: Compiled by the authors

Chi-square tests confirmed these results and also showed no statistically significant correlations between the technical measures mentioned and privacy concerns.

These results indicate that the perception of privacy is not significantly influenced by the available technical security measures, confirming the paradox identified earlier: Although technical security measures are highly rated, these measures do not adequately address privacy concerns. This emphasises the need for further research on other potential factors influencing privacy concerns, such as institutional trust and regulatory assurances, which are crucial for overcoming perceived risks among potential users of the digital euro.

Table 7 Chi-square test results for the relationship between security measures and privacy concerns

Variable	χ^2 value	p-value	Confirmed by binary logistic regression
Measure - Digital signature	0.743	0.389	No
Measure - Biometrics	1.112	0.292	No
Measure - Authorisation control	0.135	0.713	No
Measure - Encryption	0.024	0.878	No
Measure - Pseudonymisation	0.944	0.331	No

Source: Compiled by the authors

The results indicate that students' perception of privacy is not significantly influenced by the available technical security measures. These results support the previously identified paradox from the analysis: Although students express a high degree of importance regarding technical security measures, these measures do not explain their privacy concerns.

5. Discussion

The research results confirm the original assumptions. Students recognised the potential benefits of the digital euro, such as faster and cheaper transactions, but at the same time viewed risks to privacy as a major barrier. The logistic regression analysis revealed that perceived privacy threat, importance of cash, confidence in transaction security, and familiarity with the digital euro were significant predictors of adoption. The ROC analysis also confirms the strong discriminatory power of the model (AUC = 0.777), with concern for privacy proving to be the most significant predictor compared to other payment methods. The results of this study are consistent with the Deutsche Bundesbank (2024) and the European Data Protection Board (2023), both of which emphasised data protection as a key factor for the introduction of the digital euro.

The results also indicate that technical security measures such as biometric authentication, digital signatures, encryption and pseudonymisation do not significantly reduce privacy concerns. This suggests that technical protection measures alone are not sufficient to improve the acceptance of the digital euro (Jabbar et al., 2023; Lee et al., 2021). Concerns about surveillance and misuse of personal data cannot be addressed by technology alone, but point to the need for stronger institutional data control. In this respect, the findings support previous work by the European Data Protection Board (2023) and Panetta (2021), emphasising that institutional safeguards and oversight mechanisms are essential for the public acceptance of central bank digital currencies.

Another important result concerns the role of familiarity. Students reported relatively low levels of knowledge about the digital euro (mean score 2.5 on a five-point scale). Our analysis shows that greater familiarity is associated with a higher likelihood of adoption, highlighting that privacy sensitivity is partly shaped by knowledge gaps. This is consistent with earlier findings, which underline the need for education (Horváth, 2023) and transparent communication of institutional safeguards to build user trust (Bijlsman et al., 2023).

The model analysed also takes into account the characteristics of the sample. While gender is not statistically significant in the regression model, it may still be important to understand the observed strong sensitivity to privacy, as 70% of respondents were female. According to van der Cruijsen and Broekhoff (2024), women tend to be more afraid

of the digital world and have less knowledge about payment fraud. In contrast, men are more inclined to adopt new digital payment instruments. In terms of their year of study, the majority of participants were in their senior year of study (the third to fifth year of study, 80%). Although gender and year of study do not have a statistically significant influence on the intention to use the digital euro, this structure may have influenced perceptions, as students who are more familiar with economic and financial concepts may be better able to assess the impact of the digital euro, especially when weighing up its benefits and risks.

The results support the view that the adoption of the digital euro depends precisely on the confidence that its implementation avoids privacy concerns, and that this cannot be achieved through technical design solutions alone. From a theoretical perspective, acceptance depends on the integration of institutional, legal and social safeguards that address privacy issues, combined with education and communication strategies that support the adoption of the digital euro. The interplay of institutional trust and public understanding therefore proves to be a key prerequisite for the acceptance of central bank digital currencies. From a theoretical perspective, the results support the notion that the implementation of the digital euro must not only provide technical solutions, but also institutional, legal and societal guarantees for the protection of privacy.

5.1 Policy and practical implications

In line with the research results, the implementation of the digital euro must prioritise strengthening user trust. This requires embedding data protection principles into its architecture. Such an approach includes enabling anonymous transactions for smaller amounts, establishing strict limits on data collection and access, and ensuring independent oversight. Beyond technical design, transparent communication with citizens on both the legal and institutional safeguards, as well as the broader benefits of introducing the digital euro, is of critical importance.

Both the European Union and Croatia are already moving in this direction. At the European level, the digital euro project is in its active preparation phase (November 2023 - October 2025) and represents the central framework for national strategies, including Croatia's. This process explicitly emphasises "privacy by design" principles, with ongoing consultation on the appropriate level of transaction anonymity, proportionality of data use, and institutional supervision (European Data Protection Board, 2023). In the Croatian context, alignment with these standards will be crucial, but national authorities must also ensure that European-level guarantees are communicated in an accessible and locally relevant manner.

The findings of this study further suggest that familiarity with the digital euro is important. Therefore, public communication (educational campaigns) coordinated at the EU level should be implemented locally. Such campaigns should clearly explain who has access to transaction data, under which legal basis, and what protections are available. Communication strategies should not only highlight technological safeguards but also underline legal protections and institutional guarantees against the misuse of personal data. In Croatia, the Croatian National Bank (HNB) should take a leading role in carrying out public communication efforts aimed at improving familiarity with the digital euro.

Finally, evidence-based pilot projects and systematic reporting practices are necessary to complement the existing technical and legal infrastructure for the digital euro. Public reporting of pilot outcomes, covering adoption rates, privacy-related incidents, and user comprehension, would build trust through verifiable evidence rather than abstract assurances. Such an integrated approach to policies and measures directly responds to the insights from this study, according to which trust and familiarity with the digital euro emerge as decisive conditions for wider acceptance.

5.2 Limitations of the research and future research directions

Despite its contributions, this study has several limitations that should be acknowledged. First, the research was conducted on a student population of economics majors. While this group is relevant given their potential role as future users of the digital euro and their relatively high level of financial literacy, the results cannot be fully generalised to the wider population. Older citizens or those with lower levels of digital literacy, different payment habits, and less confidence in using new technologies may perceive the risks and benefits of the digital euro differently, and ultimately display different levels of willingness to adopt it. Future research should therefore aim to broaden the sample to include other age, educational, and socio-economic groups, thereby allowing for more meaningful comparisons.

Second, the role of broader socio-psychological factors, such as institutional trust, risk aversion, and overall digital literacy, requires deeper investigation, as these may be closely linked to intentions to adopt the digital euro. The introduction of the digital euro represents not only a technological, but also an institutional and societal change. Future studies should therefore explore how different dimensions of trust, whether in central banks or in technological solutions, shape attitudes towards adoption.

Third, longitudinal and cross-country comparative research would be particularly valuable for tracing how perceptions of privacy and acceptance of the digital euro evolve over time. Such studies could provide insight into the dynamics of public trust and user attitudes under the influence of institutional and regulatory developments.

Finally, further research should also assess the effectiveness of public communication strategies aimed at familiarising citizens with the concept and functions of the digital euro. An open question remains whether such communication can lead to behavioural change and long-term acceptance. Addressing this issue would allow for a more precise evaluation of which combination of regulatory measures, institutional guarantees, and educational approaches most effectively builds trust in the digital euro.

6. Conclusion

This study focused on the analysis of the factors influencing the acceptance of the digital euro among students, with particular attention to privacy concerns and perceptions of security measures. The results of the binary logistic regression model indicate that perceived risk to privacy, importance of cash, confidence in the security of transactions and familiarity with the concept of the digital euro significantly influence attitudes towards its adoption. At the same time, the proposed security technologies showed no significant impact on reducing privacy concerns, indicating a limited understanding of technical security solutions.

Students who reported higher levels of familiarity were substantially more likely to express an intention to adopt the digital euro. Given that the research population consisted of economics students, many of whom were in advanced stages of study, this finding suggests that exposure to financial and economic concepts can enhance understanding and lower perceived barriers to adoption. At the same time, the results indicate that even within a population expected to possess relatively high financial literacy, average familiarity with the digital euro was only moderate. This signals a gap between general economic knowledge and awareness of specific financial innovations, a gap that may be even wider in the general population.

The second model showed that no single technical solution has a statistically significant effect on privacy concerns related to the intention to use the digital euro. Even more advanced technical measures failed to lessen concerns of privacy. Thus, alongside understanding and overcoming the limits of technical fixes, the institutional-regulatory framework plays an important role in encouraging the adoption of the digital euro by lowering the perceived privacy risk.

The acceptance of the digital euro does not depend solely on addressing privacy concerns through institutional and regulatory frameworks, but also on building knowledge about the currency itself. Among economics students, familiarity with the digital euro emerged as a one of the key factors facilitating adoption. Public communication and the dissemination of information aimed at increasing awareness of its functions and benefits are therefore indispensable components of a successful introduction strategy. For policymakers, this underscores the need for a holistic approach: combining legal and institutional guarantees for privacy with sustained efforts to raise public awareness and understanding of the digital euro as a complement to cash and a reliable means of payment.

Although this study provides valuable insights into the attitudes of economics students towards the adoption of the digital euro, several limitations should be acknowledged. The reliance on a student population limits the generalisability of the findings, as older groups or those with lower levels of digital and financial literacy may perceive risks and benefits differently, and ultimately display varying intentions to adopt the digital euro. Future research should therefore include more diverse demographic and socio-economic samples and track changes in attitudes over time, particularly as the ECB moves closer to potential issuance. In addition, broader factors such as institutional trust, digital literacy, and the effectiveness of educational interventions deserve closer examination in order to understand how they shape the long-term acceptance of the digital euro.

References

1. Abramova, S. & Böhme, R. (2016). Perceived Benefit and Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study. In *Proceedings of the 37th International Conference on Interaction Sciences (ICIS 2016).* Dublin: Association for Information Systems. https://doi.org/10.3386/w23488
2. Athey, S., Catalini, C. & Tucker, C. (2017). *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* (NBER Working Paper No. w23488). Cambridge, MA: National Bureau of Economic Research.
3. Bijlsma, M., van der Cruijsen, C., Jonker, N. & Reijerink, J. (2024). What Triggers Consumer Adoption of Central Bank Digital Currency?. *Journal of Financial Services Research*, *65*(1), 1-40. https://doi.org/10.1007/s10693-023-00420-8
4. Borgonovo, E., Caselli, S., Cillo, A., Masciandaro, D. & Rabitti, G. (2019). *Privacy and Money: It Matters* (Working Paper No. 108). Milan: Bocconi University. https://dx.doi.org/10.2139/ssrn.3330494
5. Chen, L. C. & Farkas, D. (2019). Individual Risk Perception and Choice using Cryptocurrency for Transactions. In *Proceedings of the 40th International Conference on Interaction Sciences (ICIS 2019).* Munich: Association for Information Systems.
6. De Nederlandsche Bank (2021). *DNB survey finds 49% of respondents ready to use digital euro*. https://www.centralbanking.com/fintech/cbdc/7825796/dnb-survey-finds-49-of-respondents-ready-to-use-digital-euro
7. Deutsche Bundesbank (2021). *What do households in Germany think about the digital euro? First results from surveys and interviews*. https://www.bundesbank.de/resource/blob/879312/807018037068359550e1d89a5dc366fe/mL/2021-10-digitaler-euro-private-haushalte-data.pdf
8. Deutsche Bundesbank (2024). *Bundesbank survey: Widespread acceptance of digital euro among general public*. https://www.bundesbank.de/en/press/press-releases/bundesbank-survey-widespread-acceptance-of-digital-euro-among-general-public--933322
9. European Central Bank (2024). *Progress on the preparation phase of a digital euro - Second progress report*. https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202412.en.html#toc2
10. European Data Protection Board (2023). *Digital euro: Ensuring the highest data protection and privacy standards*. https://www.edpb.europa.eu/news/news/2023/digital-euro-ensuring-highest-data-protection-and-privacy-standards_en
11. Gao, X., Clark, G. D. & Lindqvist, J. (2016). Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 1656-1668). San Jose, CA: ACM. https://doi.org/10.1145/2858036.2858049
12. Hamm, P., Pape, S. & Rannenberg, K. (2023, June). The Influence of Privacy Concerns on Cryptocurrency Acceptance. In *IFIP International Conference on ICT Systems Security and Privacy Protection* (pp. 45-58). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56326-3_4
13. Herskind, L., Katsikouli, P. & Dragoni, N. (2020). Privacy and Cryptocurrencies - A Systematic Literature Review. *IEEE Access*, *8*, 54044-54059. https://doi.org/10.1109/ACCESS.2020.2980950
14. Horváth, D. (2023). Money in the digital age: Exploring the potential of central bank digital currency with a focus on social adaptation and education. *Sustainable Futures*, *6*, 100136. https://doi.org/10.1016/j.sftr.2023.100136
15. Jabbar, A., Geebren, A., Hussain, Z., Dani, S. & Ul-Durar, S. (2023). Investigating individual privacy within CBDC: A privacy calculus perspective. *Research in International Business and Finance*, *64*, 101826. https://doi.org/10.1016/j.ribaf.2022.101826
16. Karwatzki, S., Trenz, M. & Veit, D. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. *Information Systems Journal*, *32*(6), 1126-1157. https://doi.org/10.1111/isj.12386

17. Kramcsák, P. T., Penedo, A. C., Van den Poel, M. & Ortalda, A. (2024). *Untangling Digital Euro's Personal Data Protection Challenges: An Exploration of Data Processing Activities and Latent Privacy Risks*. https://www.researchgate.net/publication/385513252

18. Krombholz, K., Judmayer, A., Gusenbauer, M. & Weippl, E. (2016). The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. In *International Conference on Financial Cryptography and Data Security* (pp. 555-580). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-54970-4_33

19. Lee, Y., Son, B., Park, S., Lee, J. & Jang, H. (2021). A Survey on Security and Privacy in Blockchain-based Central Bank Digital Currencies. *Journal of Internet Services and Information Security*, *11*(3), 16-29. https://doi.org/10.22667/JISIS.2021.08.31.016

20. Marriott, H. R., Williams, M. D. & Dwivedi, Y. K. (2017). Risk, privacy and security concerns in digital retail. *The Marketing Review*, *17*(3), 337-365. https://doi.org/10.1362/146934717X14909733966254

21. Mashatan, A., Sangari, M. S. & Dehghani, M. (2022). How perceptions of information privacy and security impact consumer trust in crypto-payment: an empirical study. *IEEE Access*, *10*, 69441-69454. https://doi.org/10.1109/ACCESS.2022.3186786

22. Panetta, F. (2021). *Central bank digital currencies: a monetary anchor for digital innovation*. European Central Bank. https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211105~08781cb638.en.html

23. Strzelecka, A., Kurdyś-Kujawska, A. & Zawadzka, D. (2020). Application of logistic regression models to assess household financial decisions regarding debt. *Procedia Computer Science*, *176*, 3418-3427. https://doi.org/10.1016/j.procs.2020.09.055

24. Szafraniec-Siluta, E., Zawadzka, D. & Strzelecka, A. (2022). Application of the logistic regression model to assess the likelihood of making tangible investments by agricultural enterprises. *Procedia Computer Science*, *207*, 3894-3903. https://doi.org/10.1016/j.procs.2022.09.451

25. Tronnier, F., Harborth, D. & Hamm, P. (2022). Investigating privacy concerns and trust in the digital Euro in Germany. *Electronic Commerce Research and Applications*, *53*, 101158. https://doi.org/10.1016/j.elerap.2022.101158

26. van der Cruijsen, C. & Broekhoff, M. C. (2024). Gender gaps in the world of payments (De Nederlandsche Bank Working Paper No. 805). Amsterdam: De Nederlandsche Bank. https://dx.doi.org/10.2139/ssrn.4752532

27. Voskobojnikov, A., Obada-Obieh, B., Huang, Y. & Beznosov, K. (2020). Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users. In *International Conference on Financial Cryptography and Data Security* (pp. 595-614). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-51280-4_32

28. Zaghloul, E., Li, T., Mutka, M. W. & Ren, J. (2020). Bitcoin and Blockchain: Security and Privacy. *IEEE Internet of Things Journal*, *7*(10), 10288-10313. https://doi.org/10.1109/JIOT.2020.3004273