Can Artificial Intelligence help to identify privacy paradox: case of CBDC*

Viktor Koziuk[1,†], Nataliia Dziubanovska[1,†], and Ivan Tsegelnyy[1,†]

[1] *West Ukrainian National University, 11 Lvivska Str., Ternopil, 46009, Ukraine*

Abstract

This study explores the potential role of Artificial Intelligence (AI) in identifying the privacy paradox in the design of Central Bank Digital Currencies (CBDCs). The privacy paradox refers to the discrepancy between individuals' stated preferences for privacy and their actual behavior, which can have significant implications for CBDC design, particularly regarding privacy and functionality. The research employs a two-step approach, utilizing AI language models and association rule analysis to interpret survey results from respondents in four countries – Zimbabwe, Uzbekistan, Nigeria, and Ukraine. The analysis revealed significant signs of the privacy paradox, where respondents express concern about privacy but continue to trust central banks and use technologies that could compromise their anonymity. The study shows that AI models provide more unambiguous conclusions than traditional statistical methods, highlighting complex relationships between privacy preferences, trust in central banks, and CBDC design choices. This paper offers valuable insights for policymakers in designing CBDCs that balance privacy and functionality while addressing the emerging privacy paradox.

Keywords

Privacy paradox, Artificial Intelligence, Central banks, Central Bank Digital Currency, CBDC design, Privacy, Trust, Anonymity, AI models, Apriori algorithm.

1. Introduction

The crypto revolution has generated considerable enthusiasm about how digitalisation can transform modern money. The expectation that the spread of cryptocurrencies will have a strong impact on monetary systems has triggered a "defensive" reaction from central banks. Central bank digital currency (CBDC) projects continue to be considered as one of the options for responding to the challenges of digitalisation. Preserving monetary sovereignty, promoting digital technologies and fintech, and addressing the payment needs and habits of the next generation of payment service consumers are the main arguments why central banks pay so much attention to CBDCs [1], [2], [3], [4], [5], [6].

However, despite significant progress in discussions on how CBDC could be an option to respond to the challenges to modern money posed by digitalisation, the actual steps to implement CBDC have slowed down. On the one hand, the very fact of CBDC is viewed critically, either because of the crypto industry's exaggeration of the risks to payment services or because of the market niche that central banks' digital money will occupy [7]. On the other hand, the perception of the revolutionary design and transformative power of CBDCs has proven to be clearly inadequate compared to the requirements that central banks have faced in terms of the institutional and technological format of their digital money [8]. The privacy of the consumer of payment services, their anonymity and, ultimately, the traceability of transactions are directly at the intersection of the problem of social values, political freedoms, the balance between rights and obligations, and the requirements of financial monitoring legislation. In all historical forms of money, the anonymity and untraceability

The Second International Conference of Young Scientists on Artificial Intelligence for Sustainable Development (YAISD), May 8-9, 2025, Ternopil, Ukraine

* Corresponding author.

† These authors contributed equally.

viktorkoziuk@wunu.edu.ua (V. Koziuk); n.dziubanovska@wunu.edu.ua (N. Dziubanovska); i.tsehelnyi@st.wunu.edu.ua (I. Tsegelnyy)

0000-0002-5715-2983 (V. Koziuk); 0000-0002-8441-5216 (N. Dziubanovska); 0009-0000-0798-4311 (I. Tsegelnyy)

of transactions were mechanically guaranteed. In the digital world, however, the situation is changing. Privacy/anonymity can be guaranteed technologically, which in turn requires an institutional format. And the choice of a particular format for guaranteeing transaction privacy/anonymity is influenced by a significant number of institutional factors.

When a central bank introduces a CBDC, the question of the role of privacy in the design is almost a starting point, as everything else will depend on it. The European Central Bank has openly demonstrated its commitment to the idea of ensuring the privacy of e-euro users [3], [4], [5], [6]. At the same time, ensuring the privacy of CBDCs is a complex technical challenge with many implementation options, depending on the policy towards digital money and expectations about the role it will play in the relationship between public institutions and individuals [3], [9], [10], [11]. Assuming that demand for CBDCs will determine their success, and that demand will depend on the proposed design of CBDCs, research attention naturally focuses on how much economic agents value privacy/anonymity versus functional benefits in their daily transactions. The validity of this contrast stems from the very nature of digital money and competition for customers in the digital world, where the popularity of a payment service is determined by its functionality and design. In the context of CBDCs, this problem is exacerbated as economic agents have to choose among many available options to meet their payment needs while maintaining trust in the central bank, in its technological solutions and institutional capacity [12].

An equally important concern is whether central banks are overemphasising choice in favour of privacy. As shown in the Kantar Public Survey of Payment Service Consumer Preferences and Demands (2022) [13] privacy is not an obvious priority. Koziuk and Ivashuk (2022) [14] show that when economic agents distrust public institutions, their preferences shift from anonymity to functionality. Such a view of the problem raises the question of whether the well-known phenomenon of the privacy paradox applies to CBDCs [15], [16], [17], [18].

The applying of traditional empirical analysis methods leaves some uncertainty about how to interpret the resulting quantitative relationships between variables characterising privacy preferences or binary variables denoting a choice between CBDC design alternatives. Economic agents show signs of both preference sequences and deviation from such sequences as the class of phenomena to which a particular choice alternative belongs changes [12], [19]. This raises the question of whether traditional quantitative methods adequately capture the complexity of heterogeneous relationships. It also raises the question of the role of a particular theoretical shift in the interpretation of results. Artificial intelligence technologies allow us to better identify non-linear patterns of relationships between variables representing different classes of phenomena. Artificial intelligence technologies also allow us to obtain an “interpretation” of the obtained dependencies.

This article aims to apply AI capabilities to interpret respondents’ preferences in terms of whether they fall under the privacy paradox. Based on a survey of respondents, quantitative values are obtained for the general propensity for privacy, the propensity for privacy in the digital environment, and the propensity for privacy in the financial environment. The obtained results are compared with each other and combined with three binary choices regarding the preference for anonymity over functionality in the design of CBDCs, trust in the central bank as a guarantor of the anonymity of CBDC transactions, and trust in the independence of the central bank as a precondition for the ability to guarantee the anonymity of transactions (for more details on the methodology, see [12], [19]). The obtained results on respondents’ preferences are analysed using eight AI language models for the presence of signs of the privacy paradox in respondents’ answers. In the context of the eight models, the consistency of the responses is traced with different emphasis on individual nuances. The interpretations obtained from the linguistic models are compared with the results of applying the associative rules method using the Apriori algorithm in Python. In the case of both language models and the associative rule method, the results confirming the privacy paradox in respondents’ preferences for CBDC design are more unambiguous than those obtained using traditional methods. This suggests that AI technologies make it possible to identify complex relationships between variables representing different classes of phenomena in a more comprehensive way. At the same time, the development of AI technologies raises the question of how much human bias can be replaced by AI bias in the interpretation of quantitative research results.

2. Literature review

The literature on CBDCs is actively updated with research on design issues. Very often, however, the design of CBDC issues are more focused on the implications for the financial system [8], [20], [21], [22]. The privacy issue is most often considered in the context of the extent to which a central bank is committed to a particular version of anonymity in line with the preferences of society and policymakers [23], [24]. The approaches of the ECB [3], [4], [5], [6] and the People's Bank of China [9] show significant differences. It is clear that the more central banks try to simultaneously guarantee privacy and maintain KYC policies and high standards of financial monitoring, the more complex the design of CBDCs becomes and the more difficult it is to understand the overall configuration of the interaction between the central bank, the financial sector and the consumer of financial services. Auer et al. show that absolute anonymity of transactions does not correspond to the social optimum. There is currently no clear technological solution to ensure that these priorities are reconciled [25]. It is possible that this technological uncertainty affects the demand function for CBDCs.

The theoretical evidence on the relationship between money and privacy on the one hand, and privacy preferences on the other, is broadly consistent. For example, Kahn et al. (2005) [26] show that privacy is a property of money that creates a specific value relative to alternative means of payment. This value has been confirmed in behavioural experiments [27]. However, privacy is not an exclusive virtue of money, and therefore may be subject to trade-offs when economic agents receive additional incentives in the case of more complex alternatives (trade-offs) [28]. The lack of trust in the provision of such privacy, which is compensated by better functionality, may be a similar incentive [14]. When it comes to empirical analysis of privacy preferences in the context of studying the demand for CBDCs, researchers are generally in agreement. Abramova et al. (2022) [29] and Bijlsma et al. (2021) [30] confirm through surveys that economic agents value transaction privacy; their expectations of CBDCs are mostly based on privacy guarantees; trust in digital money issued by central banks is higher; trust in central banks is higher than in technological companies. Choi et al. (2023) [31], using a more sophisticated methodology that combines surveys with elements of a behavioral experiment, confirm, based on an analysis of randomised groups, that the preference for privacy is dominant, but that it is strongly amplified in certain contextual cases. These findings are somewhat at odds with, but do not negate, the results of Kantar Public (2022) [13], Koziuk and Ivashuk (2022) [14], Koziuk et al. (2024a,b) [12], [19].

Of course, when using surveys with direct questions and determining stated preferences, the result may not be consistent with the conclusions drawn from the research methodology, which a priori takes into account the possibility of the privacy paradox. In a broad sense, the privacy paradox can be defined as the discrepancy between the stated preferences for privacy and the actual behavior of economic agents. This phenomenon has been actively studied in the context of the proliferation of social media and the growing role of the data economy (Blank et al. (2014) [32] provide an overview of the development of the debate on privacy in the digital world and controversial actions related to its proliferation). At the same time, the privacy paradox has wider implications than just the issue of social media. A privacy as a money virtue is an example.

Research on the privacy paradox confirms that there are significant differences between stated preferences and actual behavior [15], [16], [17], [18]. Other studies have considered much more nuance. For example, Athey et al. (2017) [33] suggest that economic agents do not value privacy and that the incentives for efforts to protect it must be significant. This view takes into account the fact that economic agents can perform a cost-benefit analysis on the basis of which they make decisions. In other words, the "privacy calculus" [34] softens the rigid definition of the privacy paradox. The privacy calculus approach opens the way to incorporating the problem of context into the analysis. Indeed, it is important to understand the context in which economic agents compare losses and benefits. In other words, losses in the form of something are compared to benefits in the form of something. Barth et al. (2017) [35], Chen et al, (2021) [36], Hirschprung (2023) [37], argue that context matters because privacy is understood in a specific sense that is determined by the social nature of interactions. Kokolakis (2017) [38], Solove (2021) [39], express scepticism about the privacy paradox, suggesting that it is a matter of interpretation rather than behavior. Adorjan and Ricciardelli (2019) [40], offer an alternative argument. Privacy is being eroded in the minds of the younger generation. The "nothing to hide" behavior pattern dominates the value of privacy, and therefore discrepancies

between stated preferences and actual behavior may not be of functional importance. Nevertheless, Adorjan and Ricciardelli (2019) [40], conclude that the privacy paradox is undergoing a mutation, reflecting an adaptation to everyday coexistence with online technologies.

In the context of digital finance, empirical research findings are still much closer to the fact that the privacy paradox exists in one form or another. For example, risk appetite, choices under complex conditions of uncertainty or specific user experiences create specific contexts for using financial applications, where respondents demonstrate more complex behavioral algorithms, weighing the costs and benefits of sharing information about themselves and preferences for certain functionalities [41], [42], [43]. In contrast to these findings, Barth et al. (2019) [44] point to an apparent privacy paradox. The sample included technologically savvy respondents. Their stated privacy preferences differed from their actual choices when it came to the functionality of financial applications. These findings are consistent with those of Koziuk and Ivashuk (2022) [14], who focus on the issue of trust. However, in both cases, functionality is an important factor that can challenge privacy preferences, which is also consistent with the findings on payment instrument functionality requirements in Kantar Public (2022) [13].

Therefore, stated preferences may differ from actual behavior. This is confirmed in the context of digital finance [44]. On the other hand, respondents tend to trust central banks and choose privacy as an element of CBDC design [29], [30], [31]. This raises the additional question of how privacy preferences correlate with the choice of anonymity or functionality in CBDC design and with trust in the central bank as the institution responsible for CBDC design, which will determine how well the chosen design will meet users' needs and preferences. Koziuk et al. (2024) [12], [19], based on a survey and quantification of individual privacy preferences in the general context, in the digital context and in the financial context, show that respondents may show consistency of preferences in some cases and not in others when the context changes or when the choice is between alternatives belonging to different classes of phenomena. The feature of this approach is that it does not use answers to questions about privacy preferences. Instead, based on the questions in the Likert scale, the propensity for privacy in the three contexts is quantified. These quantitative values are compared with each other and also with binary choices regarding preference for anonymity over CBDC functionality, confidence in the central bank's ability to guarantee anonymity of transactions, and confidence in the central bank's independence as a precondition for implementing such guarantees. The conclusions are interpreted as a mild form of the privacy paradox, based on results obtained using traditional statistical methods.

The question arises whether AI tools can help to interpret the results of the surveys in [12], [19] more unambiguously. Taking into account the considerable amount of literature that contains both confirmations and denials of the privacy paradox, AI can choose an option that allows the results of this survey to be correlated with the amount of information available to AI. The results are then compared with the use of a more formal algorithm of the Apriori associative rule method in Python. The results show that 8 different models of generative AI are unambiguous in interpreting the survey data as a manifestation of the privacy paradox; the responses in the context of the 8 models have some specific emphases, but there is consistency between them; the associative rule method based on the Apriori algorithm also confirmed the existence of the privacy paradox. The results of this study demonstrate that AI can reach more unambiguous conclusions when analysing complex forms of relationships than traditional statistical methods. In terms of CBDC policy, this means that central banks may overestimate the importance of privacy and that the stated privacy preferences of CBDCs may be subject to a trade-off with design functionality.

3. Methodology

The study uses a two-step approach to analyse the privacy paradox and its implications for attitudes towards central banks in the context of ensuring anonymity. The aim of this approach is to gain a deeper understanding of the privacy paradox by combining the analysis of responses using artificial intelligence (AI) language models and the use of association rule analysis.

The first stage focuses on the use of several AI language models to analyse survey results, while the second stage involves the use of association rule analysis to identify hidden relationships between different aspects of privacy.

Data for the study was collected through a comprehensive survey of respondents from four countries: Zimbabwe, Uzbekistan, Nigeria and Ukraine. The survey included questions on three indices of propensity toward privacy: general, digital and financial, as well as respondents' attitudes towards anonymity, functionality and trust in the ability of central banks to ensure anonymity. Respondents were asked to rate their propensity toward privacy in different contexts and to answer questions about their preferences for anonymity versus functionality and their trust in central banks to protect their data. This provided a rich dataset for a detailed analysis of the privacy paradox.

In the first phase of the study, the survey results were fed into various AI language models for analysis, including the most popular chatbots and virtual assistants with generative AI capabilities:

Claude 3.7 Sonnet – a language model developed by Anthropic. Claude focuses on deep contextual understanding, multidimensional responses and ensuring safer, more reasoned conversations. The model is designed to reduce bias and misinterpretation, making it highly useful for complex, multi-tasking queries. The stable release of Claude 3.7 Sonnet on 24 February 2025 not only generates answers, but also supports reasoning and explanation to improve understanding of context. The updated version of the model offers improved performance and accuracy in handling complex queries, making it an ideal tool for research and analysis of large amounts of information [45].

DeepSeek R1 – a model developed by DeepSeek that emphasises accuracy and query processing speed. It is known for providing clear and concise answers with deep analysis capabilities, allowing it to perform calculations and data analysis with high efficiency. Version R1, released on 10 January 2025, was a preliminary stable release that preceded version 3.7. It featured improved handling of complex queries and reduced bias, making it more effective for scientific and practical research. DeepSeek R1 is useful in scenarios where accuracy is paramount without overwhelming the user, particularly for fast answers to complex questions [46].

ChatGPT o3-mini – Developed by OpenAI, this model is optimised for rapid text generation and adaptation across a wide range of topics. It is known for supporting productive conversations, responding quickly to queries, and interpreting questions within the context of the conversation. On 31 January 2025, OpenAI released o3-mini to all ChatGPT users (including free tier users) and some API users. OpenAI describes o3-mini as a "specialised alternative" for "technical areas where accuracy and speed are required. It excels at providing high-quality answers and ensuring excellent adaptability, making it ideal for research that requires rapid processing of large amounts of data [47].

Gemini 2.0 Flash – Developed by Google DeepMind, this model is designed to generate detailed responses with in-depth, multi-step analysis. Released on 5 February 2025, Gemini 2.0 Flash became widely available to developers through APIs (Vertex AI, AI Studio) and the Gemini app for end users. It provides powerful intellectual analysis, particularly useful for complex tasks such as idea exploration or exploring multifactorial relationships in large datasets [48].

Mistral Small 3 – Developed by Mistral, this model specialises in providing concise yet accurate answers. Known for its efficient processing while maintaining maximum accuracy and logical coherence, Mistral is an excellent tool for fast and accurate responses in various scientific and practical contexts. The stable release of Mistral Small 3 on 25 January 2025 signalled its readiness for widespread use in various tasks [49].

Qwen 2.5 Max – Developed by Qwen, this model focuses on high efficiency and fast query understanding. It is suitable for scenarios that require both speed and accuracy in data processing. Qwen delivers excellent results when processing data from multiple sources, helping to answer complex questions quickly. The stable release of version 2.5-Max on 28 January 2025 demonstrates its readiness for integration into systems where fast information processing is critical. The model is capable of quickly interpreting complex queries, making it ideal for scenarios that require both accuracy and minimal delays in data processing [50].

Grok Grok 2 – Developed by xAI, Grok Grok 2 focuses on generating creative and unconventional answers. It can interpret complex questions and provide innovative and well-reasoned solutions, making it valuable for tasks where a non-standard approach to data analysis is important. The first release of Grok 2 was on 14 August 2024 [51].

Llama 3 (70B) – developed by Meta, Llama 3 is a large language model that uses deep learning to generate integrated, content-rich responses. With a large number of parameters, it is highly effective at handling large volumes of data, performing detailed analysis and generating responses that meet high standards of accuracy and depth. Llama 3 was released on 18 April 2024 in two versions: 8B and

70B parameters. Due to its different parameter sizes, Llama 3 offers high efficiency and flexibility, allowing it to be used for both simpler tasks and more complex tasks that require significant computing power and deeper contextual understanding [52].

These AI models, with different characteristics and capabilities, were used to analyse the survey results in order to identify the privacy paradox and correlations between respondents' views on confidentiality and their trust in institutions, in particular central banks.

The study used a specific prompt for the AI language models to interpret the survey results and assess the presence of the privacy paradox. The prompt was formulated to enable the models to analyse data collected from respondents in several countries (Zimbabwe, Uzbekistan, Nigeria, Ukraine), focusing on their privacy inclinations in general, digital and financial contexts.

Prompt: Analyse the results of the survey, which includes data from several countries (Zimbabwe, Uzbekistan, Nigeria, Ukraine). The table presents respondents' answers to questions about propensity toward privacy indices in different environments: general, digital and financial. The table also includes data on respondents' age, their responses to questions on anonymity and functionality, and their confidence in the central bank's ability to ensure anonymity. Tasks:

1. Analyze how the different propensity toward privacy indices change based on age, country, and other factors.
2. Draw conclusions about the relationship between trust in the central bank's ability to guarantee anonymity and the privacy ratings in different environments.
3. Determine if there are signs of the "privacy paradox" in the collected data. Assess whether there is a disconnect between the respondents' high propensity toward privacy and their trust in institutions like central banks that ensure anonymity.
4. Assess whether there is a disconnect between the respondents' general privacy inclination indices and their propensity toward privacy indices in digital and financial environments. Does this support or contradict the existence of the "privacy paradox"?
5. Compare the privacy ratings and trust in central banks between different countries. Use the data to identify potential trends and generate conclusions that could help understand the nuances of privacy perceptions among different respondent groups.

Responses from each model were compared to identify consistency or discrepancies in interpreting the privacy paradox.

The second stage of the study involved performing association rule analysis using the Apriori algorithm in Python. Association analysis is a method within data mining used to uncover hidden patterns or relationships between items in datasets, where certain events or elements frequently occur together. Association analysis is part of unsupervised learning, as it seeks patterns and relationships in the data without predefined class labels. It helps identify association rules that can be used to predict future events or improve processes such as marketing strategies, recommendation systems, and more.

Key concepts of association analysis:

Association Rule: A statement in the form of (A ⟶ B), indicating that if element A occurs, element B is likely to occur as well.

Metrics for evaluating associations:

- Support: The frequency with which two variables appear together in the dataset. It indicates how often elements A and B appear together.
- Confidence: The probability that element B will occur given that element A has already occurred.
- Lift: A measure of how strongly two elements are related compared to their independent occurrence.

The results of the association rule analysis provided additional insights into the factors contributing to the privacy paradox and confirmed the primary findings made using the AI models.

The final stage of the study involved synthesizing the results from both approaches – the AI model responses and the association rule analysis. The conclusions drawn offer a deeper understanding of the nature of the privacy paradox and provide recommendations for future research and security policies regarding personal data protection in the digital age.

4. Results

As a result of the survey, data were collected that allow for a deeper exploration of the relationships between various aspects of privacy, trust in central banks, and technological capabilities. Among the 155 respondents, a significant number of instances of the privacy paradox were identified: 63 instances of the privacy paradox for the general privacy index; 53 instances of the privacy paradox for the digital privacy index; 54 instances of the privacy paradox for the financial privacy index.

These data suggest that a significant portion of respondents express a high level of concern about privacy protection, yet simultaneously trust central banks or use technologies that could compromise their privacy. This situation exemplifies the classic privacy paradox, where theoretical beliefs about confidentiality do not always align with actual behaviors or choices.

To gain a deeper understanding of this phenomenon, it is crucial to utilize modern data analysis tools, among which AI plays a key role. Language models enable the efficient processing of large volumes of data, conducting comparisons between the results of different models, and importantly, automatically uncovering hidden patterns that may remain unnoticed in traditional analysis. After each model was tested with the given prompt, its responses regarding the privacy paradox were analyzed (Figure 1). The responses from different models showed variations in their approaches to interpreting privacy issues and trust in institutions.

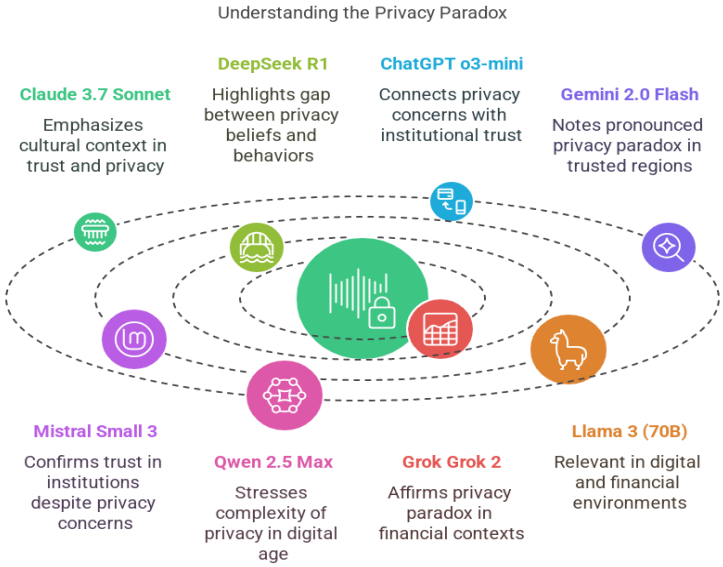

Figure 1: Comparison of Responses from Different AI Language Models

Each of these models interpreted the data and provided their conclusions based on the survey information, which allowed for comparing different approaches to analyzing the privacy paradox and identifying key trends and differences in the interpretation of the results. Key observations based on the models' responses:

Claude 3.7 Sonnet highlighted the importance of cultural and social contexts in respondents' attitudes towards trust and privacy. The model emphasized that although respondents express concern about protecting their personal data, they sometimes trust central institutions, such as central banks. It also noted that most respondents tend to trust institutions that guarantee anonymity, even in situations where there is high concern about confidentiality.

DeepSeek R1 focused on the significant gap between theoretical beliefs about confidentiality and respondents' actual actions. The model pointed out that even in countries with high trust in central banks, respondents do not always alter their actions, maintaining a high level of concern about digital privacy. Furthermore, this model identified a high level of inconsistency in the relationships between trust in institutions and reasoned attitudes towards anonymity.

ChatGPT o3-mini drew attention to the connection between high levels of concern about digital privacy and trust in institutions, requiring additional context for explanation. The model also emphasized that respondents in countries with high trust in institutions, such as central banks, often remain passive in their behavior towards personal data protection. This confirms the hypothesis of the privacy paradox, where respondents' expectations and behaviors do not always align.

Gemini 2.0 Flash determined that in countries with high levels of trust in institutions, the privacy paradox is particularly pronounced. Respondents show high levels of concern about privacy, yet continue to trust central banks and other institutions responsible for processing their data. The model highlighted the importance of this phenomenon for understanding attitudes towards institutional guarantees.

Mistral Small 3 confirmed that even with high levels of concern about digital privacy, respondents often demonstrate trust in institutions, especially central banks. The model also pointed out that while respondents express concerns about privacy protection, they do not always take the necessary steps to safeguard it, which is another classic example of the privacy paradox.

Qwen 2.5 Max revealed the presence of the privacy paradox, emphasizing that even with high levels of concern about confidentiality, respondents often trust institutions that may have access to their personal data. The model emphasized that this reflects the complexity of privacy in the digital age, where people, despite their concerns, either cannot or do not want to change their behavior.

Grok Grok 2 confirmed the existence of the privacy paradox in countries with high levels of trust in financial institutions. The model observed that even when respondents express concern about protecting their personal data, they are often willing to trust institutions that may collect it, if these institutions have control or regulation that provides a certain level of protection.

Llama 3 (70B) highlighted that the privacy paradox is relevant not only for digital privacy but also in financial environments. It also noted that high levels of concern about digital privacy do not always correlate with a corresponding change in respondents' behavior when it comes to trust in institutions or the use of technologies.

Thus, comparing the responses from the various language models, it can be concluded that all models confirmed the existence of the privacy paradox among the respondents, where they express a high level of concern about confidentiality but continue to trust institutions that might violate their privacy, especially in the context of central banks. The models' responses suggest that the level of trust in institutions, such as central banks, significantly impacts respondents' attitudes towards privacy. However, this relationship is not straightforward and varies depending on the country. Additionally, while the main trends are consistent, different models focus on different aspects of the analysis, such as the significance of cultural context (Claude), technological aspects (Mistral), or the depth of the paradox (Qwen).

The conclusions drawn are informative regarding the existence of the privacy paradox, but we do not have a clear understanding of how different factors, such as anonymity, trust in institutions, and technological aspects, interact with each other.

To gain a deeper understanding of the relationships between these variables and to uncover hidden patterns that may influence respondents' behavior, we applied association rule analysis. Searching for association rules expands the analytical capabilities by revealing not only general trends but also precise dependencies between different parameters that may not be apparent in general conclusions.

Association rule analysis, particularly the use of the Apriori algorithm, not only helps to confirm theoretical conclusions drawn from the AI model responses but also uncovers specific connections between various aspects of privacy, trust in banking institutions, and the relationship between the concepts of anonymity and functionality. This allows for a deeper understanding of the privacy paradox and the discovery of new, important interrelationships that may have gone unnoticed without the aid of data analysis methods (Figure 2).

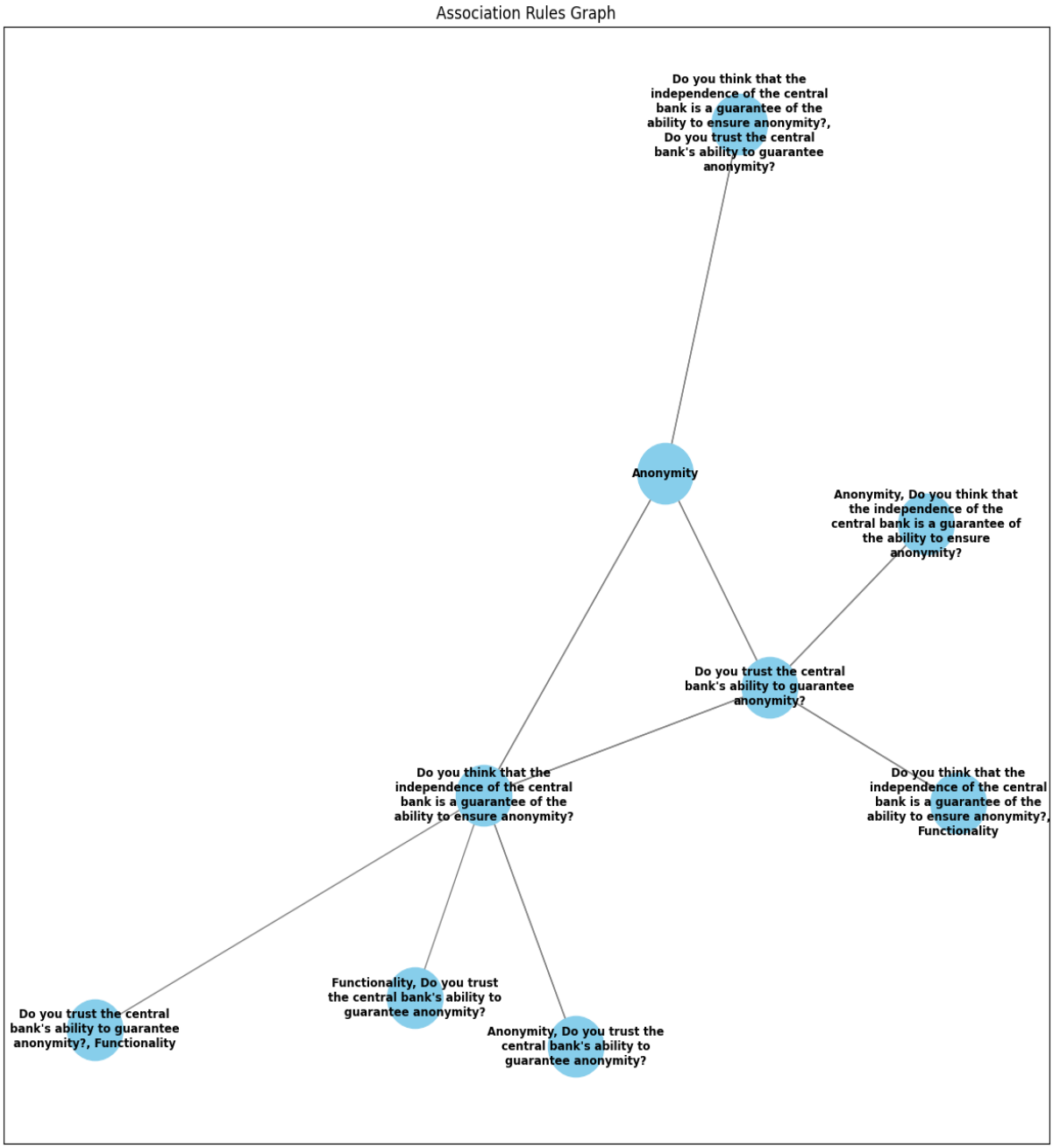

Figure 2: Association Rules Graph

As a result of the analysis, *16 association rules* were identified:

- average support value – 38.7%;
- average confidence value – 68.1%;
- average lift value – 1.145.

Some of the *association rules* (based on confidence):

(*Do you think that the independence of the central bank is a guarantee of the ability to ensure anonymity*? ⟶ *Do you trust the central bank's ability to guarantee anonymity*?):

- support – 25%;
- confidence – 95.12%;
- lift – 1.21.

This rule demonstrates a strong association between trust in the central bank and the belief that the independence of the central bank is a precondition to guaranty a privacy.

(*Do you think that the independence of the central bank is a guarantee of the ability to ensure anonymity*? ⟶ *Do you trust the central bank's ability to guarantee anonymity*?):

- support – 62.18%;
- confidence – 95.10%;
- lift – 1.21.

This rule also shows a high level of trust in the central bank concerning anonymity when the institution is independent.

(*Anonymity, Do you think that the independence of the central bank is a guarantee of the ability to ensure anonymity? ⟶ Do you trust the central bank's ability to guarantee anonymity?*):

- support – 37.18%;
- confidence – 95.08%;
- lift – 1.21.

This rule suggests that respondents who value both anonymity and the independence of the central bank are highly likely to trust the central bank.

(*Anonymity ⟶ Do you trust the central bank's ability to guarantee anonymity?*):

- support – 46.79%;
- confidence – 82.02%;
- lift – 1.04.

This rule also indicates a significant correlation between concerns about anonymity and trust in the central bank's ability to ensure it.

(*Anonymity, Do you trust the central bank's ability to guarantee anonymity? ⟶ Do you think that the independence of the central bank is a guarantee of the ability to ensure anonymity?*):

- support – 37.18%;
- confidence – 79.45%;
- lift – 1.22.

This rule shows how beliefs regarding anonymity and central bank independence are interconnected.

Overall, the results of the association rule analysis confirm that the most significant associations are related to trust in central banks and the belief that the independence of these institutions guarantees anonymity.

This suggests that respondents who consider anonymity important are largely also trusting that banks can provide such protection. Rules with high confidence and lift values indicate that the relationship between anonymity and trust in institutions is a key factor in shaping respondents' attitudes toward the privacy paradox.

The first approach, which involved the use of various AI generative language models to analyze respondents' answers, provided a deep understanding of general trends regarding privacy attitudes and trust in institutions such as central banks. The models confirmed the existence of the privacy paradox, where respondents express concerns about the confidentiality of their data but continue to trust institutions that could violate their privacy, especially in the context of financial institutions. This led to the conclusion about the importance of studying the relationship between privacy, trust in institutions, and technological aspects like anonymity, which also play a crucial role in shaping individuals' perceptions, influencing their willingness to share personal information and their confidence in the systems that manage and protect that data.

The second approach, involving association rule analysis, provided a more detailed exploration of hidden relationships between different variables. The use of association rule analysis with the Apriori algorithm revealed precise dependencies between the levels of trust in central banks, anonymity, and other aspects that may influence respondents' behavior. This approach enabled the identification of not only general trends but also specific patterns that were not obvious in the overall conclusions from the first stage.

Both approaches complement each other, allowing for a better understanding of the complex nature of the privacy paradox. The first approach helped identify general trends, while the second refined and confirmed these conclusions by revealing hidden connections. As a result, we were able to not only confirm the existence of the privacy paradox but also identify key factors that influence respondents' attitudes towards confidentiality and trust in institutions.

These results can serve as a foundation for further research and the development of policies aimed to improve personal data protection in the digital age.

5. Conclusions

The design of Central Bank Digital Currencies (CBDC) is largely influenced by how central banks address the priority of user privacy protection in payment services and the anonymity of transactions. At the same time, the very fact that economic agents value privacy is a matter of debate. Interaction with the digital world reveals many signs that stated preferences may not align with actual actions. Does the privacy paradox extend to CBDC?

In papers [12], [19], traditional statistical methods showed that respondents exhibit both consistency in preferences and contradictions in their choices, which were interpreted as a mild form of the privacy paradox. Through the application of AI, this interpretative uncertainty was significantly reduced. The use of 8 generative AI models demonstrated unanimous agreement in interpreting the survey results as a privacy paradox.

The association rule method based on the Apriori algorithm in Python also confirmed that respondents exhibit inconsistency in choosing between anonymity or functionality for CBDC, regardless of their overall, digital, or financial privacy inclination. Furthermore, consistency in trust towards central banks and their independence does not correspond with the prioritization of one aspect of CBDC design over the other. With the help of AI, it was possible to overcome the limitations of traditional statistical methods, which allow for a certain level of uncertainty and bias in interpretation.

The results indicate that AI tools allow for better identification of complex relationships between variables representing different classes of phenomena. Generative AI models allow for complementary interactions with ML and DL models. Comparing the results of both AI approaches enhances the overall interpretative picture.

Regarding CBDC policy, the results confirm a high likelihood of overestimating privacy as a design element. However, this does not mean that central banks should disregard privacy in the design process, justifying their choices based on the privacy paradox.

Declaration on Generative AI

During the preparation of this work, the authors used the generative AI models, such as Claude (3.7 Sonnet), DeepSeek (R1), ChatGPT (o3-mini), Gemini (2.0 Flash), Mistral (Small 3), Qwen (2.5 Max), Grok (Grok 2), and Llama (3 (70B)) in order to: Analyze survey results to identify the privacy paradox and explore the relationships between respondents' attitudes toward confidentiality and their trust in institutions, particularly central banks. Further, the authors used Napkin AI for figures 1 in order to: Generate images. After using these tools/services, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.
[6] 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.
[7] 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.
[8] Bindeisl U., Senner R. (2024). Macroeconomic modelling of CBDC: a critical review. ECB Working paper. №2978. pp. 1-47.
[9] 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/.
[10] 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-opportunitieschallenges-and-design-discussion-paper.
[11] 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.
[12] Koziuk V., Ivashuk Y., Hayda Y. (2024a). CBDC, Trust in the Central Bank and the Privacy Paradox. Economics – Innovative and Economics Research Journal. Vol. 12. Issue 2. Pp. 219-242. doi: 10.2478/eoik-2024-0025.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] 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.
[18] Barnes S.(2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). https://doi.org/10.5210/fm.v11i9.1394.
[19] Koziuk V., Ivashuk Y., Hayda Y. (2024b). CBDC and Trust in a Central Bank: Transitivity of Preferences vs Privacy Paradox. Financial Internet Quarterly 2024, vol. 20 / no. 4. pp. 32-47. DOI: https://doi.org/10.2478/fiqf-2024-0025.
[20] 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.
[21] 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.
[22] 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.
[23] Ahnert, T., Assenmacher, K., Hoffmann, P., Leonello, A., Monnet, C. & Porcellacchia D. (2022a). The economics of central bank digital currency. ECB Working Paper, 2713, 1-52.
[24] Ahnert, T., Hoffmann, P. & Monnet, C. (2022b). The digital economy, privacy, and CBDC. ECB Working Paper, 2662, 1-52.
[25] Auer R., Böhme R., Clark J., Demirag D. (2025). Privacy-enhancing technologies for digital payments: mapping the landscape. BIS Working Paper. №1242. pp. 1-27.
[26] 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.

[27] 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.
[28] 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.
[29] 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.
[30] 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.
[31] 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.
[32] Blank G., Bolsover G., Dubois E. (2014). A New Privacy Paradox: Young People and Privacy on Social Network Sites. SSRN Electronic Journal. April.
[33] 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.
[34] 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.
[35] 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.
[36] 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.
[37] Hirschprung R. (2023). Is the Privacy Paradox a Domain-Specific Phenomenon. Computers. 12. 156. 1-14. https://doi.org/10.3390/computers12080156.
[38] 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.
[39] 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.
[40] Adorjan M., Ricciardelli R. (2019). A New Privacy Paradox? Youth Agentic Practices of Privacy Management Despite "Nothing to Hide" Online. Canadian Review of Sociology. Vol. 56. Issue 1. pp. 8–29.
[41] 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.
[42] 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.
[43] 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.
[44] 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.
[45] Claude (language model). From Wikipedia. URL : https://en.wikipedia.org/wiki/Claude_(language_model).

[46] DeepSeek (AI). From Wikipedia. URL : https://en.wikipedia.org/wiki/DeepSeek_(AI).
[47] ChatGPT. From Wikipedia. URL : https://en.wikipedia.org/wiki/ChatGPT.
[48] Gemini (AI). From Wikipedia. URL : https://en.wikipedia.org/wiki/Gemini_(AI).
[49] Mistral (AI). From Wikipedia. URL : https://en.wikipedia.org/wiki/Mistral_(AI).
[50] Qwen (AI). From Wikipedia. URL : https://en.wikipedia.org/wiki/Qwen_(AI).
[51] Grok (AI). From Wikipedia. URL : https://en.wikipedia.org/wiki/Grok_(AI).
[52] LLaMA (language model). From Wikipedia. URL : https://en.wikipedia.org/wiki/LLaMA_(language_model).