Quantitative Finance and Economics

QFE, 8(1): 126–152.
DOI: 10.3934/QFE.2024006
Received: 02 November 2023
Revised: 11 February 2024
Accepted: 01 March 2024
Published: 11 March 2024

https://www.aimspress.com/journal/QFE

Research article

How do privacy concerns impact actual adoption of central bank digital currency? An investigation using the e-CNY in China

Frédéric Tronnier* and Weihua Qiu

Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt am Main, Hesse, Germany

* **Correspondence:** Email: frederic.tronnier@m-chair.de.

Abstract: Central Bank Digital Currencies (CBDC) are being researched in academia and piloted by central banks around the world. Initial research highlights the importance of privacy concerns on adoption intention in CBDC. We took one step further and investigated the link between privacy concerns and adoption using the Chinese CBDC and digitalized version of the Yuan, the e-CNY. We integrated and applied the established Antecedent Privacy Concerns and Outcomes (APCO) model with the Task-Technology Fit model in a quantitative online-questionnaire with 682 Chinese participants to study the influence of privacy concerns on CBDC usage. The data was analyzed using partial least squares structural equation modeling (PLS-SEM) to identify significant path coefficients and effects in the developed model. The findings demonstrated that several antecedents significantly influenced privacy concerns, which in turn influenced e-CNY usage. In particular, perceived vulnerabilities impacted privacy concerns, while soft and hart trust factors were found to neither impact concerns or usage. When compared to prior research, the distinction between intention to use and usage of CBDC, under consideration of privacy concerns, seemed to be negligible. The often discussed 'privacy-paradox' could not be observed for CBDC. Observed differences in antecedents and other factors may have been due to cultural, political, and demographic factors, as well as different CBDC design choices. For practitioners, the results further emphasized the need for a privacy-friendly implementation of retail CBDC, which efficiently communicated user benefits while rebutting perceived vulnerabilities.

Keywords: central bank digital currency; CBDC; privacy concerns; adoption; digital money; e-CNY; DCEP

JEL Codes: E42, E58, G41, O33, C83

Abbreviations: APCO: Antecedent Privacy Concerns and Outcome; BIS: Bank for International Settlements; CB-SEM: covariance-based structural equation modeling; CBDC: Central Bank Digital Currency; CFIP: concern for information privacy; DCEP: Digital currency electronic payment; DLT: Distributed ledger technology; e-CNY: Electronic Chinese yuan; GIPC: global information privacy concern; HTMT: heterotrait-monotrait ratio; IUIPC: Internet Users' Information Privacy Concerns; PLS-SEM: partial least squares structural equation modeling; PBoC: People's Bank of China; TAM: technology acceptance model; TRA: theory of reasoned action; TTF: Task-Technology-Fit; UTAUT: unified theory of acceptance and use of technology; VIF: variance inflation factor

1. Introduction

In recent years, academic research on Central Bank Digital Currency (CBDC) is growing steadily, as more and more central banks worldwide are in various stages of investigating, piloting, or establishing CBDC. The bank of international settlements (BIS) states that, as of 2023, 93% of all central banks are actively researching the topic (Kosse & Mattei, 2023), with numerous pilot projects being deployed. Different types of CBDC are envisioned, for either wholesale or retail purposes. In the contemporary financial landscape, the emergence of digital currencies in general has not only the potential to reshape monetary systems (Sauer, 2016) but also comes with new challenges (Raymaekers, 2015). Such challenges for instance include the protection of information privacy (Goodell et al., 2021) and trust in technology and institutions (Zarifis et al., 2015).

The People's Bank of China (PBoC) was one of the first to research and actually issue a CBDC, the Electronic Yuan (e-CNY) through a dedicated system, the Digital Currency Electronic Payment (DCEP) system (People's Bank of China, 2021). The e-CNY acts as legal tender for retail purposes (Cheng, 2023), and was implemented due to the rapidly changing digital economy, the decline in cash usage, and the emergence of new digital cryptocurrencies such as Bitcoin. The overall objective has been to meet the changing demand of individuals for digital payments. It acts as a "digital version of fiat currency issued by the PBOC", with all the basic functions of money (People's Bank of China, 2021). A two-tier model is used, in which the central bank issues e-CNY to authorized commercial institutions that then circulate e-CNY to the public.

Numerous objectives or potential advantages for issuing CBDC have been discussed, ranging from an increase in financial inclusion, to more control over monetary policy (Yang & Zhou, 2022), to offering a digital complement for the physical legal tender, cash (European Central Bank, 2022). However, achieving such goals is contingent on citizens actually adopting CBDC for retail payments and transactions in their daily life.

Studying the adoption of new technologies, such as digital currencies, including CBDC, is a focus area in various research domains and one of the objectives of this work. In the past, central banks and academic research has focused on adoption intention as a proxy for actual adoption of CBDC, given

its unavailability to be used by citizens among several countries and regions (Bijlsma et al., 2021; Solberg Söilen & Benhayoun, 2022; Tronnier et al., 2022). Privacy concerns have been identified as potentially the most important factor for citizens in the development of a CBDC in Europe (European Central Bank, 2021). These concerns are often being researched in academia from a technical (Gross et al., 2021) or regulatory (Pocher & Veneris, 2021) point of view. Moreover, initial research on the link between privacy concerns of individuals and the intention to adopt a CBDC has already been conducted (Tronnier et al., 2022), demonstrating the negative influence of privacy concerns on the intention to adopt a digital euro.

In this work, we aim to study this link in more detail by focusing not only on adoption intention but on actual adoption, or usage behavior. While adoption intention is sometimes seen as the closest indicator for actual adoption, there is conflicting research that indicates that the two are not necessarily similar indicating an "intention-behavior gap" (Sheeran & Webb, 2016). What is more, differences in CBDC, as well as citizens' cultural and behavioral differences between countries, limits the generalizability of existing findings that were mainly conducted in a European context (Bijlsma et al., 2021; Solberg Söilen & Benhayoun, 2022; Tronnier et al., 2022). Thus, the e-CNY is chosen to study actual end-user usage and its link to privacy concerns for CBDC. The objective of this work is therefore to study the link between possible privacy concerns and usage behavior and to compare these findings with existing research that focused on behavioral intention.

The research questions (RQ) of this work are therefore as follows:

RQ1: Which antecedents and factors influence privacy concerns in e-CNY users?

RQ2: How do privacy concerns usage behavior for the e-CNY?

RQ3: Are there differences in privacy concerns and adoption (intention) for different CBDC and countries?

To answer these research questions, we conduct a quantitative questionnaire among Chinese citizens to obtain 682 final respondents. We follow and adapt the research model for CBDC by Tronnier et al. (2022) that is based on the antecedents-privacy concerns- and outcomes (APCO) model by Smith et al. (2011) and combine it with the Task-Technology-Fit (TTF) model (Goodhue & Thompson, 1995). The data sample is analyzed using partial least squares structural equation modelling (PLS-SEM) in accordance with Hair et al. (2011).

The results verify the significant negative influence of privacy concerns on adoption of the e-CNY. The antecedents prior privacy victim experience, perceived vulnerability, and self-efficacy are found to significantly influence privacy concerns. Notably, soft and hard trust factors are found to influence neither privacy concerns nor e-CNY usage. By comparing our results to existing work that studied the influence of privacy concerns on adoption intention, the theoretical contribution of this work addresses the intention-behavior gap (Sheeran & Webb, 2016). For CBDC, this work acts as first evidence that behavioral intentions and actual behavior could indeed be similar. As a practical contribution, this work emphasizes the importance of privacy in CBDC payments, as a privacy-friendly solution could encourage future adoption.

This work is structured as follows: The second chapter provides the scientific background of this work, introduces CBDC, and discusses related work and scientific models on privacy concerns and adoption behavior both in general and in the context of this work. Chapter 3 describes the methodology applied and develops the hypotheses of this work. The results are then presented in chapter 4, covering

measurement and structural model assessments. Chapter 4 discusses the results obtained in chapter 3 and points out limitations and opportunities for future work. The conclusion of this work is presented in chapter 5.

2. Related work and scientific background

2.1. Related Work on central bank digital currency

Commonly, money is described through its attributes, to serve as a unit of account, act as a medium of exchange, and retain value as a store of value (Brunner et al., 1971). Moreover, money can then be categorized based on four key properties: issuer, form, accessibility, and technology employed (Bech & Garratt, 2017). The only form of legal tender that is directly available to citizens, the public, is cash in the form of coins (and banknotes) (Bossu et al., 2021), while digital reserves are only used for interbank settlements. Central banks now aim to create and issue an additional legal tender, CBDC.

CBDC may be defined as a digital currency created by a central bank, designed either for wholesale interbank purposes or as a retail solution for public use. From a technological perspective, blockchain and account-based solutions are being researched and piloted (Bech & Garratt, 2017). Given this broad definition, we focus exclusively on retail CBDC, and the e-CNY implemented by the PBoC. The e-CNY, as first envisioned in 2016 and piloted in the subsequent years in specific Chinese regions, is the first active CBDC of a major economy. As legal tender (Cheng, 2023), to be used for retail purposes, it was proposed to counter emerging threats by cryptocurrencies and the declining cash use, as well as the overall trend towards digital payments and payment solutions (People's Bank of China, 2021). The e-CNY is sometimes referred to as the Digital Currency Electronic Payment (DCEP) system (Huang & Li, 2023). In contrast to other central banks, such as the European Central Bank (ECB), the PBOC specifically states that e-CNY is to act as a substitute for cash (People's Bank of China, 2021). Users are able to fill digital wallets with e-CNY and use them for online and offline transactions. There exist four different categories that are classified based on the balance of e-CNY that the wallet can hold and the possible number of transactions per day and year. These limits depend on the level of identification of users, as users that registered a wallet with only a mobile phone number (category 1) are allowed fewer transactions and a lower balance than users that registered using a valid ID and linked their wallet to a bank account (category 2 and 3) (Cheng, 2023; Xu, 2022). Transactions with e-CNY can be made in either a dedicated e-CNY application or through existing payment service provider solutions.

As of 2023, the overwhelming majority of central banks, surveyed by the bank for international settlements (BIS), are currently researching CBDC (Kosse & Mattei, 2023). The authors find work on retail CBDC to be more advanced than the work on wholesale CBDC, with cryptocurrencies and stablecoins as competitors rarely used for digital payments. There exists plentiful research, by academia and from central banks, on the motives, potential benefits, and drawbacks of the introduction of CBDC (Auer et al., 2021). Advantages include the potential for enhanced payment efficiency, financial stability, financial inclusion, and improved anti-money laundering capabilities (Schueffel, 2023). These advantages might differ depending on the CBDC design and vary in their usefulness depending on the economic status of a country and the objectives of the respective central bank (Auer et al., 2020).

However, for citizens, the benefits of CBDC may be less evident, particularly due to concerns for privacy and the potential of surveillance on an individual and societal level (Schueffel, 2023). An in-depth analysis on CBDC in Asia is performed by Lee et al. (2023).The authors focus on analyzing potential benefits and risks of CBDC and discuss regulatory and technological aspects. Environmental friendliness of CBDC was analyzed by Alonso (2023) using a sample of 34 countries. The author finds that countries in the Eurozone could launch a higher percentage of green CBDC, although environmental impact will ultimately depend on the design choices taken in the development of CBDC.

Initial research on CBDC adoption intention suggests that established factors such as performance expectations, social recommendations, facilitation conditions (Solberg Söilen & Benhayoun, 2022), trust, and privacy protection (Tronnier et al., 2022) play crucial roles. Recent research also underscores the interplay between CBDC and other payment methods from the perspective of users (Tronnier et al., 2023). Attitudes towards unfamiliar CBDCs are influenced by the perceived similarity to existing, familiar payment methods.

Given the actual availability of the e-CNY, first research on the subject already exists. Technical research for instance focused on the auditability of the e-CNY (Wang et al., 2022). Other researchers utilize a quantitative survey to study adoption factors for the Chinese CBDC (Wu et al., 2022). The authors combine the established model of the unified theory of acceptance and use of technology (UTAUT) with push-pull-mooring theory. The results indicate that all factors of the existing model, such as habit, social influence or perceived risk, significantly influence CBDC usage. The overall model results in an R2 of 0.359. Other work focuses on how the FinTech sector responds to CBDC signals by central banks, finding that response intensity is weakening over time (Li et al., 2022).

The study by Xia et al. (2023) can be seen as the one closest to this work. The authors study adoptions intention for e-CNY in China, using the previously mentioned push-pull-mooring model and combining it with the task-technology-fit (TTF) model. The authors also include privacy concerns in their model and find that they, as well as the majority of other factors, influence usage intention. However, the study differs from this work in two crucial aspects. First, the authors study adoption intention, not actual adoption. Second, the authors study general privacy concerns and not privacy concerns in relation to CBDC specifically. In other models, such general privacy concerns are sometimes modeled as a moderator or antecedent (Tronnier et al., 2022) for privacy concerns that relate to a specific context or technology. In this work, we focus on privacy concerns in e-CNY as both a dependent variable for several antecedents and an independent variable that influences usage behavior.

2.2. Scientific background on privacy concerns and technology adoption

The adoption of new technologies has been a major field of academic research with researchers studying the adoption of other payment-related technologies such as ATMs (Sharma, 1991), digital payment solutions such as mobile banking (Bhatiasevi, 2016; Chin et al., 2022; Zhou et al., 2010), or in-store banking (de Kerviler et al., 2016). The adoption of cryptocurrencies (Al-Amri et al., 2019; Alzahrani & Daim, 2019; Esmaeilzadeh et al., 2019; Sohaib et al., 2020) and stablecoins (Kimmerl, 2020) has similarly been studied using systematic literature reviews, qualitative interviews and quantitative surveys. The scientific basis builds on top of several established models and theories, such as the technology adoption model (TAM) (Davis, 1989), the theory of reasoned action (TRA) (Ajzen

& Fishbein, 1980) and the theory of planned behavior (Ajzen, 1991). These theories and models later lead to the development of further models such as the widely used unified theory of acceptance and use of technology, (UTAUT and UTAUT2) (Venkatesh et al., 2003, 2012; Venkatesh & Davis, 2000). Many of these models have been applied towards the payment context to study the adoption of digital payment solutions, for instance by adding additional factors such as trust in the mobile commerce context (Lin et al., 2011), security (Ramos-de-Luna et al., 2016) or privacy concerns (Su et al., 2018). Older models, such as TAM, enjoy continued usage and are being adapted to be applied to new technologies or in new contexts (Huang et al., 2023). A close link has been established between attitudes towards technology and their adoption (Ajzen & Fishbein, 1980), which were also assessed, for instance for facial recognition technology in payments (Dang et al., 2022). For CBDC, it has been observed that attitudes towards existing payment solutions shape attitudes towards not-yet-exiting CBDC in European respondents (Tronnier et al., 2023).

Most recently, the existing models for technology adoption have also been adapted towards CBDC. Solberg Söilen & Benhayoun (2022) study intention to adopt CBDC using the UTAUT by adding trust in the currency system to the existing models. The authors find that the factors performance and social recommendations significantly influence adoption intention. Similarly, Bai (2020) was, to our knowledge, the first to study centralized digital currency adoption intention for the Chinese market utilizing a quantitative approach. The author combines UTAUT2 and TPB and find established factors such as performance and effort expectancy, but also facilitating conditions and hedonic motivation, to be factors that significantly influence intention to use. A further approach, using UTAUT has been conducted using the additional factors of national identity and fairness by Wu et al. (2022).

Privacy is found to be an incremental factor that influences technology adoption. There exist countless definitions for the intangible concept of privacy, ranging from the “right to be left alone” (Warren & Brandeis, 1890) to a subjective view of fairness in processing personal data (Malhotra et al., 2004). Contextual integrity theory (Nissenbaum, 2010) argues that privacy is context-dependent and that flow of information are perceived as acceptable, or a violation of privacy, based on the specific factors of sender, recipient, information type, transmission principle and data subject. Similarly, Smith et al. (2011) argued that, due to these different perceptions, privacy cannot be measured directly. Subsequently, privacy concerns are used as a surrogate to measure privacy (Smith et al., 2011). On the topic, several comprehensive reviews of academic literature exist (Malhotra et al., 2004; Smith et al., 2011), with a wide variety of different models having been developed to measure privacy concerns. For instance, the internet users’ information privacy concerns (IUIPC) model (Malhotra et al., 2004) extends existing theory on privacy concerns by focusing on the digital context. The resulting model is found to explain a significant amount of variance in behavioral intention. Older established models, such as the global information privacy concern (GIPC) and the concern for information privacy (CFIP) (Smith et al., 1996) scale focus on the offline or organizational context and are therefore not transferable to this work. The APCO model by Smith et al. (2011) studies antecedents, privacy concerns and outcomes in the digital world and has been applied and adapted to differing contexts, such as augmented reality (Harborth & Pape, 2021) or CBDC (Tronnier et al., 2022).

With the exponential growth in CBDC research, privacy has become a prominent topic of interest among central banks and academics, as digital transactions create and process a diverse range of data. For instance, transaction data is routinely processed to comply with regulations, including anti-money

laundering (AML) and know-your-customer (KYC) requirements (Dogan & Bicakci, 2023), which are likely to apply to CBDC transactions as well (Wadsworth, 2018). As a result, personal data could potentially be exposed during the transfer of CBDC transaction-level financial information (Auer & Böhme, 2020), posing the risk of CBDC becoming a digital entity that threatens privacy and erodes civil liberties (Baronchelli et al., 2022). For CBDC transactions, data processing typically falls into two categories: identity-related and transaction-related information (Allen et al., 2020; Lee et al., 2021). As an example, the proposed regulation on the digital euro, the European CBDC, identifies multiple types of data that would be transferred in digital euro transactions, such as transaction amounts, wallet amounts or data recipients (European Commission, 2023). Sun and Rizaldy (2023) review learnings from other e-money solutions in Asia, including China, and argue that privacy-preserving data-sharing arrangements for CBDC are possible.

Auer et al. (2023) provide a mapping of the privacy landscape for CBDC, while Lee et al. (2021) offer a taxonomy of technical approaches to privacy in blockchain-based CBDCs. Technologies, such as zero-knowledge-proofs, are used to demonstrate that privacy-friendly CBDC solutions can indeed retain regulatory compliance (Gross et al., 2021). From an econometric standpoint, Fang et al. (2023) model the need for a balanced approach to privacy protection and regulation, coupled with user education on the subject, using game theory. Other research delves into privacy calculus theory, assessing the trade-off between privacy concerns and benefits associated with information disclosure in CBDC (Jabbar et al., 2023) or studying the factors influencing privacy concerns in CBDC (Tronnier & Biker, 2022).

Overall, it can be seen that existing models to study technology adoption have already been applied towards CBDC. However, the key factor of privacy concerns has not yet been studied for actual CBDC usage, but solely for behavioral intention to use, for a hypothetical CBDC. We argue that this constitutes as a gap in academic literature on the subject of CBDC, due to the significant difference between intention and actual behavior (Sheeran & Webb, 2016). This is particularly relevant when it comes to privacy and privacy concerns (Gerber et al., 2018; Kokolakis, 2017). Both, intention-behavior gap and the so called "privacy-paradox" state that communicated or intended behavior does not equal actual behavior, in particular if the socially desirable protection of privacy is involved. This difference has been observed for other socially desired actions such as ethical consumption (Hassan et al., 2016). It can be explained through the different weightings that individuals give concrete actions now, in contrast to potential future impacts to privacy breaches in the distant future (Hallam & Zanella, 2017).

In this work, we aim to close this gap in literature on CBDC by investigating CBDC adoption and its link to privacy concerns. To this end, we employ a dedicated research model to study the influence and antecedents of privacy concerns in CBDC, as outlined in the following.

3. Methodology

With the overall aim to study the influence of privacy concerns on adoption behavior of Chinese citizens for the e-CNY, we adapt and combine two established models from the information systems (IS) research domain. We specifically follow the call from Tronnier et al. (2022) for more research on privacy concerns in non-European CBDC payments and adapt their model towards the e-CNY. The Antecedents-Privacy Concerns and Outcomes (APCO) model by Smith et al. (2011) is augmented with the Task-Technology-Fit (TTF) model to better suit the news of the innovative context of CBDC.

Additionally, a specific focus is given to the dimension of trust, that is identified as a crucial antecedent of privacy concerns (Dinev et al., 2006). All constructs are adapted from established literature to maintain reliability and validity. The research questions are addressed through in total 14 hypotheses that are outlined in the following.

3.1. Antecedents of privacy concerns

The factor of *Awareness* has been extensively examined in various contexts. Westin (1967) initially proposed that heightened awareness from exposure to privacy-related media coverage could intensify privacy concerns. This perspective was expanded by Culnan (1993) who argued that personal experiences could contribute to awareness, thus providing a broader understanding of this construct. Smith et al. (1996) reinforced this notion, demonstrating the correlation between privacy awareness and the level of privacy concern (Benamati et al., 2017). Applying these findings to digital currencies such as the e-CNY, it is reasonable to surmise that increased awareness of a CBDC influences privacy concerns. Understanding of the underpinning technology, knowledge of privacy safeguards, and awareness of potential risks and benefits can all play pivotal roles in shaping privacy concerns. Thus, the following hypotheses is proposed:

H1: Awareness of the e-CNY is negatively associated with privacy concerns regarding the e-CNY.

Privacy victim experiences have been recognized in the literature as having significant influence on privacy concerns. The works of Smith et al. (1996, 2011) revealed that individuals who have been exposed to, or been victims of, personal information abuses express stronger concerns regarding information privacy. This is found to hold true in both institutional and peer contexts, suggesting that past negative experiences, even with a limited number of entities, can generalize to shape individuals' privacy concerns in broader contexts (Ozdemir et al., 2017). The idea that privacy experiences impact privacy concerns is further substantiated by Pavlou and Gefen (2005). The authors find that negative prior experiences in an online marketplace led to increased privacy concerns, demonstrating the influence of past experiences on future privacy-related perceptions. Applying these insights to the context of e-CNY, one could hypothesize that individuals' experiences related to privacy violations could shape their privacy concerns related to e-CNY usage. Based on the aforementioned literature, we therefore hypothesize:

H2: Privacy victim experiences of individuals are positively associated with privacy concerns regarding the e-CNY.

Perceived control refers to an individual's belief about the degree to which one can influence a situation or outcome. Research suggests that individuals with higher perceived control over their personal information are likely to have lower privacy concerns (Hajli & Lin, 2016). This concept aligns with privacy calculus theory, which argues that individuals weigh perceived potential benefits against perceived possible privacy risks associated with personal information sharing (Culnan & Armstrong, 1999; Dinev & Hart, 2004). If individuals perceive they have more control over their information, they may assess the privacy risk as lower, thereby reducing their privacy concerns (Ozdemir et al., 2017; Smith et al., 2011). A user who feels to possess control over e-CNY transactions, including the sharing and usage of personal information, may be more likely to have reduced privacy concerns. Such perceived control might stem from transparency in transaction processes, the ability to opt-in or opt-out of specific data sharing, and

awareness of the privacy safeguards in place. One concrete example could be the different options for signing on for e-CNY wallets, that provide different levels of pseudonymity (Cheng, 2023; Xu, 2022).

H3: Perceived control over the e-CNY is negatively associated with privacy concerns regarding the e-CNY.

A further antecedent that was found to positively influence privacy concerns (Smith et al., 1996, 2011; Tronnier et al., 2022) is *perceived vulnerability*. Perceived vulnerability denotes an individual's perceived susceptibility to harm or loss. A high level of perceived vulnerability often leads to an increase in privacy concerns and is also linked to previous negative experiences, such as falling prey to a hacker or phishing attack (Miltgen & Peyrat-Guillard, 2014). In the context of CBDCs, the perceived vulnerability may arise from concerns related to the security of the technology, the potential misuse of personal information, and the risk of financial losses. We therefore hypothesize:

H4: Perceived vulnerability is positively associated with privacy concerns regarding the e-CNY.

Self-efficacy relates to an individual's belief in their capability to complete specific tasks, for instance when interacting with technology (Compeau & Higgins, 1995). Prior research highlights the inverse relationship between self-efficacy and privacy concerns (Maddux & Rogers, 1983). More recent works (Alashoor et al., 2017; Tsai et al., 2016), reinforce this relationship, showing that individuals that exhibit higher self-efficacy demonstrate lower privacy concerns. In the context of the e-CNY, self-efficacy could play a significant role in shaping privacy concerns. Users with high self-efficacy may feel more confident in their ability to use e-CNY securely and manage the associated privacy risks, thus reducing their privacy concerns. This may include understanding the privacy settings and safeguards, managing personal information related to transactions, and responding to potential privacy threats. We therefore propose the following hypothesis:

H5: Self-efficacy is negatively associated with privacy concerns in the e-CNY.

3.2. Privacy concerns and related factors

The emergence of CBDC, such as the e-CNY, marks a significant shift in the financial landscape. CBDC could potentially offer increased efficiency, accessibility, and foster financial inclusion (Auer et al., 2020). However, we argue that adoption, and the tangible positive effects CBDC could have, depend on the perceived fit between the technology characteristics of the CBDC and the task characteristics of financial transactions, that are the transactions that are to be conducted using CBDC.

The Task-Technology Fit model (TTF) model by Goodhue and Thompson (1995) states that information technology is likely to have a positive impact on individual performance and usage when the capabilities of the IT match the tasks that the user must perform. In the context of CBDCs like e-CNY, the technology-task fit could refer to how well the features of the DCEP system align with the users' financial transaction needs. This could include factors such as security features, ease of transactions, accessibility, and transaction speed. If the DCEP system is perceived to meet these needs effectively, the likelihood of its use could increase. The significant influence of TTF on adoption could be observed for technologies such as enterprise resource planning systems (Abugabah et al., 2015), e-learning solutions (Lin & Wang, 2012), and has also been researched for CBDC specifically (Xia et al., 2023). Therefore, we propose:

H6: The Task-technology fit is positively associated with the usage of the DCEP system in e-CNY.

Privacy concerns are at the center of the APCO model, with the antecedents introduced above influencing privacy concerns, while privacy concerns in turn influence a specific outcome. This outcome would be the adoption of a technology, acting as an independent variable in the second part of the model. Privacy concerns refer to individuals' apprehensions about the potential loss of control over personal information (Smith et al., 2011) and have been shown to negatively influence technology acceptance, information disclosure, or usage behavior (Dinev and Hart, 2004). For the digital euro, privacy concerns were found to significantly negatively influence intention to use the CBDC (Tronnier et al., 2022), although the "privacy paradox" (Barnes, 2006) argues that there exists a gap between intention and actual behavior with respect to privacy. Privacy was further found to be a major factor for individuals with respect to CBDC in research by central banks (European Central Bank, 2022) and researchers frequently discuss the potential negative implications of CBDC on citizens' privacy (Baronchelli et al., 2022). Thus, we propose:

H7: Privacy concerns in e-CNY are negatively associated with the usage of e-CNY.

Trust is a multifaceted construct and ensuring trust in the respective currency is one of the major objectives of each central bank (European Central Bank, 2020). Moreover, it is crucial for central banks in ensuring that monetary policy can be applied successfully (Angino et al., 2021), with trust levels in central banks, by citizens, differing significantly between countries (Bursian & Fürth, 2015). Trust in central banks and their policies is influenced by factors such as education, political leaning and specific events (Angino et al., 2021). Trust in digital currency solutions is also found to influence intention to use CBDC in prior research (Solberg Söilen & Benhayoun, 2022). When discussing trust outside the money-context, the factor is found to positively influence behavioral intention and usage (Dinev & Hart, 2006), for instance for purchasing behavior (Pavlou & Fygenson, 2006).

As trust is often modeled in different fashions (Smith et al., 2011), we follow the approach by Tronnier et al. (2022) and Wonneberger and Mieg (2011) that measure soft and hard trust factors for money specifically. Hard trust factors hereby relate to the main functions of money, such as acting as medium of exchange and store of value. Soft trust factors facilitate the functioning of money, for instance through the perceived image or security of it. These trust factors, including system security and credibility, are found to significantly impact technology adoption and use (Featherman et al., 2010). In the work of Tronnier et al. (2022), especially soft trust factors impact privacy concerns and the intention to adopt a European CBDC for European respondents. Based on these results, we propose the following hypotheses:

H8: Soft trust factors are negatively associated with privacy concerns for the e-CNY.

H9: Hard trust factors are negatively associated with privacy concerns for the e-CNY.

H10: Soft trust factors are positively associated with the usage of e-CNY.

H11: Hard trust factors are positively associated with the usage of e-CNY.

The role of *perceived risk* in shaping trust and influencing the adoption and usage of technology-based systems is well-documented in the literature. Perceived risk refers to the potential for loss in the pursuit of a desired outcome and is considered a major barrier to the acceptance and use of new technologies (Featherman and Pavlou, 2003). For the e-CNY, perceived risk can stem from several sources, including potential financial losses, data breaches, and uncertainty about the system's reliability (Smith et al., 2011). Various studies have established the negative influence of perceived risk on trust.

For instance, Pavlou (2003) found that as perceived risk increases, trust in the online vendor decreases, which subsequently reduces the intention to transact. We therefore argue:

H12: Perceived risk is negatively associated with the usage of the DCEP system in e-CNY.

Government involvement is a vital factor in shaping public trust, particularly when it comes to financial systems and new forms of currency like e-CNY. In the broader context, government involvement often includes regulation, supervision, and sometimes direct operation or support of a system, all of which can influence public perceptions of trust. The concept of government involvement fostering trust has been supported by existing literature (Akkaya et al., 2010; Bélanger & Crossler, 2011; Li, 2011; Patton & Jøsang, 2004).

However, the specific impact of government involvement on trust in the context of CBDCs such as e-CNY is unexplored. Given its importance and potential impact, this study proposes to be the first to examine this relationship. We therefore argue that government involvement is not only positively linked to trust factors but extends beyond trust (Stoica et al., 2005). We hypothesize that it directly influences usage behavior in e-CNY, as the Chinese government plays a pivotal role in directing economic trends and is actively promoting and incentivizing e-CNY usage for citizens:

H13: Government involvement is positively associated with soft trust factors in e-CNY.

H14: Government involvement is positively associated with hard trust factors in e-CNY.

H15: Government involvement is positively associated with the usage of the DCEP system in e-CNY.

3.3. Questionnaire design

All items and their wording were adapted from prior research, as outlined above, and items are depicted in Appendix Table A.1, including mean and standard deviation values. Upon agreement on the exact phrasing of each item in English by the authors, all items were translated to Mandarin by a native speaker. Another researcher verified the translations using digital translation solutions by transferring them back to English. These were then discussed until agreement on all items was reached. 5-point Likert scales were used for answers wherever applicable, ranging from "Strongly disagree" to "Strongly agree". A pilot survey was conducted to test item design and verify whether respondents' answers, obtained through a market research institution, are usable. Following this preliminary phase, several items were augmented, to account for differences in meaning through the translation from English to Mandarin. The questionnaire commenced with an introductory section on the intended objective of the survey, to obtain consent for the purpose of academic research. Next, the e-CNY was introduced, following the information provided by the central bank of China. Upon these introductory information, items for the general model as well as demographic questions were provided to respondents.

3.4. Sample collection

In total, 800 respondents were surveyed, of which 692 respondents are included in the final sample, accounting for failed control questions, suspicious answer behavior or too quickly completed questionnaires.

Participants were recruited by one researcher through word-of-mouth and digital distribution as well as through a market research institution, "Credamo.com". Participants were compensated for their work

through the market research institution, and consent was obtained to use responses for academic purposes. A checklist, provided by the ethics board of the authors' university suggested that an official ethical approval was not necessary. Only IP-addresses of respondents were collected as personal data during the survey to avoid multiple responses by the same individual. This data was deleted upon verification.

The valid sample consisted of 303 males and 389 females, with a substantial majority (50.29%) in the age bracket of 18–29 years. This indicates a skew towards younger respondents, reflecting a possible interest in or inclination towards digital financial technologies among younger demographics. The sample represented a broad cross-section of educational backgrounds, with a significant 72.54% holding at least a Bachelor's degree. The high proportion of highly-educated participants suggests that the results will reflect the perspectives of a demographic that may be more familiar with the concept and potential implications of CBDC. Only 32 individuals stated to never have used e-CNY at least once, nor to have interacted with the underlying DCEP system in any way. We also surveyed usage for offline and online payments using DCEP, finding that the system is used much less frequently for offline transactions, for instance to pay in physical stores, and much more often for online transactions.

4. Results

The research model and its hypotheses, developed in the prior section, is assessed using structural equation modeling (SEM). In contrast to earlier methods such as multiple regression analysis, SEM offers the possibility to analyze causal chains, such as "Factor A impacts Factor B, impacts Factor C". PLS uses path models, diagrams, to display the relationships between variables. The path model consists of an inner (structural) model, that links constructs and depicts the relationships, and outer (measurement) models, which display the relationship between constructs and indicator variables (Sarstedt et al., 2017). According to Hair et al. (2011), there exist two main approaches for SEM, partial least squares SEM (PLS-SEM) and covariance-based SEM (CB-SEM). SEM is seen as an extension of modeling techniques such as multiple regression analysis and may be defined as the simultaneous combination of factor analyses and multiple regression analyses (Dash & Paul, 2021). CB-SEM is based on covariance, and PLS-SEM is based on variance or partial least squares (Dash & Paul, 2021). The result is a sophisticated model that depicts the dependence and interdependence of relationships between constructs in the model. Recent work that compared the effectiveness of both methods for technology forecasting found that both methods are equally effective in analyzing structural relationships (Dash & Paul, 2021). While CB-SEM is seen as more suitable to verify existing theories, for "theory development as well as prediction purposes, PLS-SEM is better." (Dash & Paul, 2021). Due to the exploratory nature in studying e-CNY usage, we therefore opt for PLS-SEM, in line with the research by Tronnier et al. (2022), which we aim to compare our work with. The structural model is created and tested using SmartPLS version 4. We perform computations with the path weighting scheme, allowing for a maximum of 300 iterations and a stop criterion of 10^{-7}. Bootstrapping incorporated 5000 bootstrap subsamples, opting for no sign changes as the method for handling sign changes during iterations.

4.1. Measurement model assessment

The first-order constructs in our measurement model are reflective. Therefore, we analyze internal consistency reliability, convergent validity and discriminant validity for these constructs (Hair et al., 2011). Cronbach's α and Composite reliability (rho_a) are used to assess reliability, Average Variance Extracted (AVE) is used to measure construct validity. The results for our items are depicted in Table 1.

Table 1. ICR and AVE of the constructs.

	Cronbach's alpha	Composite reliability (rho_a)	AVE
Awareness of the e-CNY	0.496	0.507	0.392
Credibility	0.551	0.551	0.690
Fungibility	0.563	0.567	0.695
Government involvement	0.713	0.714	0.777
Hard factor	0.771	0.775	0.468
Image	0.535	0.535	0.683
Liquidity	0.640	0.641	0.735
Perceived control	0.678	0.654	0.555
Perceived risk	0.913	0.928	0.794
Perceived vulnerability	0.930	0.932	0.827
Privacy concerns in the e-CNY	0.921	0.921	0.863
Security	0.611	0.611	0.720
Self-efficacy	0.791	0.791	0.827
Soft factor	0.818	0.820	0.524
Stability	0.511	0.517	0.671
Task-Technology Fit	0.681	0.737	0.511
Usage of e-CNY	0.868	0.867	0.723

Cronbach's α and composite reliability score of above 0.7 are generally deemed satisfactory, implying that the items within a construct cohere together well and reliably measure the same underlying concept (Tavakol & Dennick, 2011). We observed a distinct range of scores across the constructs. All constructs except for the constructs *Awareness of the e-CNY*, *Credibility*, *Fungibility*, *Image*, and *Stability* met this benchmark. These lower scores could potentially be attributed to the complexity of these constructs, which may not be adequately captured by the items included in the survey. It could also be that these constructs are interpreted differently by the respondents, resulting in less consistency in the responses.

When assessing construct validity, an AVE score > 0.5 is considered adequate, implying that more than half of the variance of the items is due to the construct they are supposed to be measuring (Hair et al., 2011). All constructs except for *Awareness of the e-CNY*, *Perceived control* and *TTF* did meet this criterion. The low AVE scores could be due to the items not adequately capturing the breadth of these constructs or the constructs not being well-defined, resulting in a lower shared variance among the items. In the process of assessing the construct reliability and validity for "Government Involvement", a critical evaluation was undertaken on the constituent items. Notably, out of the four items, two (question 2 and 4) were identified as potentially detrimental to the construct's internal

consistency. Thus, we removed those items, resulting in a more robust Alpha, increasing from 0.635 to 0.714. The removed items are nonetheless depicted in the appendix but are marked as *redacted*, as they were not used in the structural model assessment later on.

Future research may benefit from revisiting the constructs with lower reliability and validity scores, refining the measures, and conducting additional pilot testing. Additionally, the incorporation of qualitative methods could further shed light on the nuances of these constructs that were possibly missed in the survey design.

Next, we assess discriminant validity for our constructs. Discriminant validity refers to the degree to which constructs that are theoretically different are also empirically different (Henseler et al., 2015). It reflects the uniqueness or distinctness of a construct and ensures that a construct is not highly correlated with other constructs from which it is supposed to differ (Hair et al., 2011). The heterotrait-monotrait ratio (HTMT) has been suggested as a reliable criterion to assess discriminant validity (Henseler et al., 2015). Values of HTMT lower than 0.85 demonstrate that the constructs possess adequate discriminant validity (Henseler et al., 2015). HTMT values for the main model paths are displayed in Table A.2 in the appendix. For our variables, HTMT ratios for most pairs of constructs were less than 0.85, supporting the discriminant validity of these constructs. For instance, the constructs "Perceived control" and "Awareness of the e-CNY" showed a HTMT value of 0.254, far below the threshold, which suggests that they are distinctly different.

However, certain pairs of constructs such as "*Hard trust factor*" and "*Fungibility*" (1.228), and "*Image*" and "*Credibility*" (1.194) had HTMT values exceeding the threshold of 0.85, raising concerns about discriminant validity. "*Hard trust factor*" is a higher-order construct composed of "*Liquidity*", "*Fungibility*", and "*Stability*", while "*Soft trust factor*" is composed of "*Security*", "*Credibility*", and "*Image*". The high correlation might therefore be due to their inherent interrelatedness, as these constructs share some underlying components. As we adapted these items and their phrasing from existing research (Tronnier et al., 2022; Wonneberger & Mieg, 2011), we decided to keep them in the model. Nonetheless, these results highlight the importance to refine the trust constructs in the future.

4.2. Structural model assessment

In multivariate analysis, collinearity statistics, particularly the Variance Inflation Factor (VIF), are vital for evaluating the structural model. VIF indicates the level of multicollinearity, with VIF values > 5 usually depicting concerning levels of multicollinearity (Hair et al., 2011). VIF values for the inner model are depicted in Table A.3 in the appendix and for all items of the questionnaire in the outer model in Table A.2.

The collinearity statistics derived from the survey data exhibit VIF values below the threshold of 5, suggesting that the model does not suffer from severe multicollinearity issues. This supports the validity of the regression models underpinning the construct of the structural model.

However, three constructs, namely *Perceived vulnerability* (item 4), *Usage of e-CNY* (item 2,3) as shown Table A.1, demonstrate VIF > 4, indicating potential multicollinearity. These high VIF values suggest these constructs may not be entirely independent but are interrelated with other constructs of the model. This interdependence could impact interpretability and reliability of the regression coefficients. To mitigate these issues, it might be worth reconsidering the model in the future by

excluding these constructs to evaluate if their removal improves the model's overall performance. Alternatively, refining the questionnaire by modifying the wording or context of these questions in future studies might help reduce their collinearity. It is noted that trust factors did demonstrate similar issues in the work of Tronnier et al. (2022), but not in the original work by Wonnerberger and Mieg (2011). A possible explanation could be the low number of items per construct.

Finally, Figure 1. depicts the overall research model of this work as well as the corresponding path coefficients. p-values are indicated through asterisks (***p < 0.001, **p < 0.01, *p < 0.05). The path estimates for both dependent variables are shown in Table 2. Adjusted R^2 values are 0.821 for *privacy concerns of e-CNY* and 0.567 for *Usage of e-CNY.*

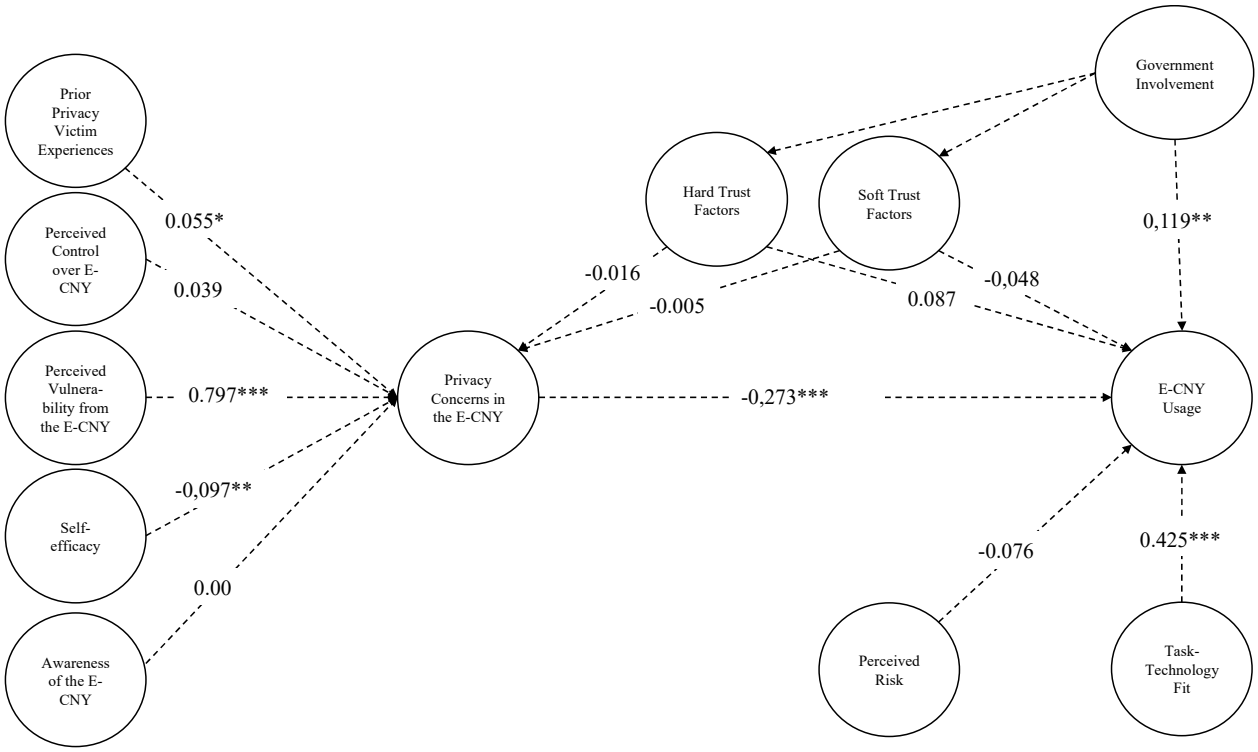

Figure 1. Final research model and path coefficients (Statistical significance: *0.05, **0.01, ***0.001).

Table 2. Path estimates (Statistical significance: *0.05, **0.01, ***0.001).

Variable	Path	Coefficient
	DV: Privacy Concerns	DV: e−CNY Usage
Adjusted R2	0.821	0.567
Privacy Victim Experience	0.055*	
Perceived Control	0.039(*)	
Perceived Risk		−0.076
Perceived Vulnerability	0.797***	
Self−Efficacy	−0.097**	
Awareness of e−CNY	0.000	
Privacy Concerns for e−CNY		−0.273***
Task−Technology−Fit (TTF)		0.425***
Government Involvement		0.119**
Soft Trust Factors	−0.005	−0,048
Hard Trust Factors	−0.016	0.087

Last, we report the total effects, that are the direct and indirect effects of variables on the indirect variables. The resulting effects are depicted in Table 3 and all results discussed in the following section.

Table 3. Total effects.

Total Effect	Effect Size	P-Value
Perceived risk → Usage of e−CNY	−0.076	0.149
Awareness of the e−CNY → Usage of e−CNY	0.000	1.000
Hard factor → Usage of e−CNY	0.092	0.066
Perceived vulnerability → Usage of e−CNY	−0.218	0.000
Privacy concerns in the e−CNY → Usage of e−CNY	−0.273	0.000
Privacy victim experience → Usage of e−CNY	−0.015	0.035
Soft factor → Usage of e−CNY	−0.047	0.373
Self−efficacy → Usage of e−CNY	0.027	0.008
Task−Technology Fit → Usage of e−CNY	0.425	0.000
Government Involvement → Usage of e−CNY	0.119	0.002

5. Discussion

The findings described in the prior chapter enable us to answer the posed research questions. *RQ1* aimed to uncover factors that influence privacy concerns with respect to the e-CNY. We found support for the hypotheses *H2* to *H5* but could not confirm *H1*. Therefore, the factors *Privacy Victim Experiences*, *Perceived Control over e-CNY*, *Perceived Vulnerability from e-CNY* and *Self-Efficacy* are all found to significantly influence *Privacy Concerns in e-CNY* while *Awareness of e-CNY* does not. In particular, *Perceived Vulnerability from e-CNY* demonstrates a very strong influence, with the other effects, although significant, demonstrating lower values. A possible explanation for the lack of influence through awareness could be the fact that all items that measure awareness, depict mean

values > 4 on a 5-point Likert scale. This could indicate that most respondents are clearly aware of the existence and aspects of the e-CNY. Given that the overwhelming majority of respondents are rather young and have conducted transactions using e-CNY at least once, these high values are plausible.

With regard to the different dimensions and factors for trust, the results indicate that both, *Soft* and *Hard Trust Factors*, do not influence privacy concerns significantly (H8, H9 not confirmed), nor do they influence e-CNY usage (H10, H11 not confirmed). Moreover, we find that *Government Involvement* is not able to influence either of the two (H13, H14 not confirmed) but does positively influence adoption (H15 confirmed). This might suggest that while government backing bolsters the overall adoption of the system, its influence on trust facets is less straightforward. Thus, the government's role in financial technologies remains a pivotal area for future research, especially in contexts like China where government participation is pronounced and e-CNY usage greatly encouraged.

The main construct of this research model, *Privacy Concerns in e-CNY*, is significantly negatively influencing adoption (H7 confirmed) as does *Task-Technology-Fit* (H6 confirmed) but not *Perceived Risk* (H12 not confirmed). The lack of influence of perceived risk is in contrast to the results depicted by Wu et al. (2022) that also surveyed actual usage using Chinese respondents. Conventional wisdom also holds that increased perceived risk results in decreased adoption of new technologies (Featherman & Pavlou, 2003). Low mean values of all perceived risk items indicate that the usage of the e-CNY is generally seen as not risky, which might be due to governmental assurances in the deployment of the CBDC, or socially desirable responses.

Nonetheless, with regard to *RQ2*, it can be observed that privacy concerns are indeed able to negatively influence adoption in CBDC, which further accentuates the need for central banks that have not yet actually deployed a CBDC to consider this factor.

Last, and to answer *RQ3*, the findings in *RQ2*, need to be compared to existing work that surveyed the influence of privacy concerns on adoption intention in CBDC (Tronnier et al., 2022; Xia et al., 2023). It can be observed that there are notable differences as well as similarities when comparing the results to those of the work of Tronnier et al. (2022) that surveyed adoption intention in a digital euro in Germany. R^2 values for privacy concerns and adoption observed in this work are notably higher than in the existing work that focused on behavioral intention. On the one hand, the antecedents that perceived vulnerability and self-efficacy are found to both significantly positively (negatively) influence privacy concerns in the respective CBDC. Path coefficients for self-efficacy are almost identical (−0.113/−0.115) for both CBDC (e-CNY/digital euro), while path coefficients for perceived vulnerability are the highest among all factors surveyed for both CBDC. This indicates the great importance of this factor among individuals of different cultural and geographic backgrounds. Both studies observe the significant negative influence of privacy concerns on CBDC, although the path coefficient for e-CNY (−0.280) is higher than for the digital euro (−0.122). Hard trust factors are found to not significantly influence privacy concerns for both CBDC. Similarly, awareness is found to neither influence privacy concerns in the digital euro, nor in the e-CNY. Awareness could potentially influence privacy concerns negatively or positively (Tronnier et al., 2022). An explanation for the lack of influence could be that assumptions about CBDC are being made by individuals even before becoming aware of the specifics such as features and design options of a CBDC. By deriving attitudes based on experiences with similar technology or existing digital payment solutions (Tronnier et al., 2023), respondents could form attitudes without the need for specific awareness on the specifics of CBDC. A

noteworthy distinction lies in the reliability of the "Awareness" scales, where a Cronbach's alpha of 0.513 for the e-CNY contrasts starkly with the solid 0.917 for the digital euro. This could suggest shortcomings in scale translation and applicability between technologies that respondents have already used, and those that are only conceptual at the time of the survey.

On the other hand, soft trust factors are found to significantly influence privacy concerns (negatively) and adoption intention (positively) in the digital euro, but are found to be not significant for e-CNY. Tronnier et al. (2022) emphasized the primacy of soft trust factors in a digital euro, arguing that they held a stronger sway over individuals than hard trust factors when it came to privacy concerns and potential use. Such findings resonate with the sentiment that while the digital euro remains conceptual, trust's intangible dimensions, like central banks' credibility, become paramount. Another possible explanation could lie in the cultural, demographical and political differences between Chinese and German participants. Trust dimensions with regard to financial organizations and central banks are found to be somewhat comparable among western countries (Bursian & Fürth, 2015).However, comparisons with Chinese data is not possible as established scholars on trust reject existing data due to a lack of reliability (Berggren et al., 2014). The authors analyzed trust in central banks in 149 countries and had to exclude Iran and China from that comparison, as prior research demonstrated trust levels in these countries more than two standard deviations higher than what could be expected (Berggren et al., 2014, p.430).

Prior privacy victim experiences and perceived control are found to be significant for e-CNY, albeit only at a 0.05 level, while they are not significant for the digital euro at all. A possible explanation could again originate from the different maturity levels of the two CBDC. For the e-CNY, there exists documentation that different types of personal data are processed, depending on the verification method with which an individual first registers for e-CNY usage. This shows that it is indeed possible to, somewhat, control the level of personal data sharing. For the digital euro, such information was not available at the time of the survey. However, following the survey, the European Central Bank issued a legislative proposal on the digital euro that details the type of data that is to be shared, depending on the transaction type (European Commission, 2023). Here, offline transactions are depicted as offering a much higher level of anonymity, which could alter the influence of the perceived control factor in future research. When comparing the results to those of Xia et al. (2023), we find that TTF significantly influences adoption intention of e-CNY as well as actual usage in our work. We argue that this alignment of CBDC features with users' tasks, the payment processes they conduct, is more insightful than simply surveying potential perceived benefits of CBDC, as demonstrated for the digital euro (Goodhue & Thompson, 1995). Similarly, government involvement, or government support, is found to be positively associated with intention or usage. Most notably, the authors find a positive relationship between privacy concerns and intention, which they attribute to a lack of understanding of the subject by respondents. The negative relationship observed in this work nonetheless has been established for other technologies as well as for intention in other CBDC (Tronnier et al., 2022).

Overall, it can be observed that existing research, studying adoption intention and privacy concerns in CBDC, depicts comparable results to those of this work, in which actual usage is surveyed. Thus, we argue that differences that have been observed, i.e., for specific antecedents of privacy concerns, might emanate from other factors than the intention-behavior gap. Potential explanation factors are differences in the specific design and availability of a CBDC as well as differences in

respondents' culture and demographics. For instance, as the digital euro in Europe has not been implemented yet, the e-CNY has undergone various stages of pilot testing in China, providing familiarity and showcasing its functionalities. Notably, usage of e-CNY was also encouraged through monetary incentives by providing a fixed sum of money for newly set-up wallets.

Nonetheless, this study is not without limitations, which correspond to the differences observed between different works on privacy and adoption in CBDC. The results of this work need to be considered with the political and cultural landscape of Chinese respondents in mind. The seemingly negligible influence of trust factors on privacy concerns and e-CNY usage are in contrast to Western studies. Such differences can, in parts, be explained through socially and politically desirable answer behavior, as mean values for trust factors and other antecedents are consistently high. High values are also observed in other research with Chinese respondents (Xia et al., 2023), which complicates adequate comparisons for trust dimensions across cultural and political system (Berggren et al., 2014). Socially and politically desirable responses could therefore lead to high trust levels in central banks in this work, while other factors are found to be largely comparable to prior research in the Western context. It has been well-documented that cultural nuances significantly influence individuals' perceptions and behaviors, especially in the domain of technology adoption (Lee et al., 2013). The results further underscore this, suggesting that findings from one cultural context may not always be generalizable to another, although the significant association between usage and privacy concerns is now observed across different regions. The sample of this work, although substantial, consists of rather young and educated Chinese individuals. Results might therefore not be transferable to other demographics, a limitation that is also noted in other user studies on CBDC given the recent topic of CBDC (Tronnier et al., 2022; Xia et al., 2023). From a methodological perspective, in particular trust constructs demonstrated low Cronbach's Alpha values, that suggest the necessity for the development of suitable trust scales for digital currencies.

Last, the rapidly evolving landscape of CBDC implies that perceptions and task-technology alignments could shift over time. This study therefore serves as a snapshot within a specific timeframe, and subsequent studies should consider longitudinal approaches to capture these evolving dynamics. During the conduction of this work, it was noticed that e-CNY transactions could now be conducted using third-party applications, which proves that CBDC are likely to be incorporated into a broader financial ecosystem. This increases the need for additional research on the topic, with a particular focus of context-dependent factors such as specific transaction types, payment channels and the specific data that can or is transferred during CBDC transactions.

6. Conclusions

Central Bank Digital Currencies are posed to be the future of digital payment solutions, envisioned and developed by central banks around the world. In this work, we studied actual end-user CBDC adoption and privacy concerns, using a sample of 692 Chinese survey participants, as the e-CNY, implemented by the People's Bank of China, is available for retail user purposes since the end of 2022. To this end, an adapted version of the Antecedents, Privacy Concerns and Outcomes (APCO) model by Smith et al. (2011) is augmented with trust factors and task-technology-fit constructs. The objective is to compare actual CBDC usage in this work with prior research on behavioral intention to use. PLS-SEM

analysis demonstrated the significant negative influence of privacy concerns on e-CNY usage, as well as the impact of several antecedents on privacy concerns themselves. The results suggest that particularly perceived vulnerability acts as an antecedent that significantly negatively impacts privacy concerns in e-CNY. Soft and hard trust factors are found to neither significantly influence privacy concerns nor adoption in e-CNY, a finding that contrasts to prior research on intention to use CBDC.

As a theoretical contribution, this work adds to the basis of research on the "intention-behavior gap" (Sheeran & Webb, 2016), that has not been considered for CBDC as of now, due to the limited availability of "active" CBDC. We find that existing research on the influence of privacy concerns in CBDC on behavioral intention are also found for actual use behavior. We further verify the importance of the task-technology-fit for CBDC, a factor that is largely overlooked in existing models that study technology adoption.

For practitioners, such as central banks that are currently developing CBDC, the findings of this work further emphasize the need to consider privacy in CBDC transactions, as privacy concerns negatively influence intention as well as usage among different CBDC. In particular, perceived vulnerabilities of users need to be considered. While prior research in other CBDC argues that fostering trust may help in overcoming privacy concerns, this work finds trust to be an insignificant factor for Chinese individuals. Instead, central banks should consider a user-centric approach with the goal to develop CBDC features that match end users' objectives and needs in online and offline transactions. By understanding the cognitive constructs in the decision-making processes of individuals, policymakers and CBDC developers can also craft more effective communication strategies, address concerns, and showcase benefits in a manner that resonates with the public, to foster future CBDC adoption.

Use of AI tools declaration

The authors affirm that no artificial intelligence (AI) tools were used in the creation of this work.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

Abugabah A, Sanzogni L, Alfarraj O (2015) Evaluating the impact of ERP systems in higher education. *Int J Inf Learn Technol* 32: 45–64. https://doi.org/10.1108/IJILT-10-2013-0058

Ajzen I (1991) The theory of planned behavior. *Organ Behav Hum Dec.* https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen I, Fishbein M (1980) Understanding attitudes and predicting social behaviour. New Jersey: Prentice-Hall. *Englewood Cliffs,* 50.

Akkaya C, Wolf P, Krcmar H (2010) The Role of Trust in E-Government Adoption: A Literature Review. *AMCIS 2010 Proceedings*. Available from: https://aisel.aisnet.org/amcis2010/297.

Al-Amri R, Zakaria NH, Habbal A, et al. (2019) Cryptocurrency adoption: current stage, opportunities, and open challenges. *Int J Adv Comp Res* 9: 293–307. https://doi.org:10.19101/IJACR.PID43

Alashoor T, Han S, Joseph RC (2017) Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Commun Assoc Inf Sys* 41: 62–96. https://doi.org/10.17705/1cais.04104

Allen S, Čapkun S, Zhang F, et al. (2020) Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. *NBER WORKING PAPER SERIES*.

Alonso SLN (2023) Can Central Bank Digital Currencies be green and sustainable? *Green Financ* 5: 603–623. https://doi.org/10.3934/GF.2023023

Alzahrani S, Daim TU (2019) Analysis of the cryptocurrency adoption decision: Literature review. *PICMET 2019 - Portland International Conference on Management of Engineering and Technology: Technology Management in the World of Intelligent Systems, Proceedings*. https://doi.org/10.23919/PICMET.2019.8893819

Angino S, Ferrara FM, Secola S (2021) The cultural origins of institutional trust: The case of the European Central Bank. *Eur Union Politics*. https://doi.org/10.1177/14651165211048325

Auer R, Böhme R (2020) The technology of retail central bank digital currency. *BIS Q Rev*, 85–100.

Auer R, Böhme R, Clark J, et al. (2023) Mapping the Privacy Landscape for Central Bank Digital Currencies. *Commun ACM* 66: 46–53. https://doi.org/10.1145/3579316

Auer R, Cornelli G, Frost J (2020) Rise of the central bank digital currencies: drivers, approaches and technologies. *BIS Working Papers* 880.

Auer R, Frost J, Gambacorta L, et al. (2021) Central Bank Digital Currencies: Motives, Economic Implications and the Research Frontier. *Ann Rev Econ*. https://doi.org/10.2139/SSRN.3922836

Bai X (2020) *Examining factors influencing behavioral intention to adopt centralized digital currencies (CDC): An empirical study based on the integrated model of UTAUT2 and TPB*.

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

Baronchelli A, Halaburda H, Teytelboym A (2022) Central bank digital currencies risk becoming a digital Leviathan. *Nature Hum Behav* 6: 907–909. https://doi.org/10.1038/s41562-022-01404-9

Bech M, Garratt R (2017) Central bank cryptocurrencies. *BIS Q Rev,* 55–70.

Bélanger F, Crossler RE (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Q* 35. https://doi.org/10.2307/41409971

Benamati JH, Ozdemir ZD, Smith HJ (2017) An empirical test of an Antecedents - Privacy Concerns - Outcomes model. *J Inf Sci* 43: 583–600. https://doi.org/10.1177/0165551516653590

Berggren N, Daunfeldt SO, Hellström J (2014) Social trust and central-bank independence. *Eur J Polit Econ* 34: 425–439. https://doi.org/10.1016/J.EJPOLECO.2013.10.002

Bhatiasevi V (2016) An extended UTAUT model to explain the adoption of mobile banking. *Inf Dev* 32: 799–814. https://doi.org/10.1177/0266666915570764

Bijlsma M, van der Cruijsen C, Jonker N, et al. (2021) What triggers consumer adoption of CBDC? *SSRN Electronic J,* 709. https://doi.org/10.2139/ssrn.3836440

Bossu W, Itatani M, Margulis C, et al. (2021) *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations*. https://doi.org/10.2139/ssrn.3758088

Brunner K, Meltzer A, Brunner K, et al. (1971) The Uses of Money: Money in the Theory of an Exchange Economy. *Am Econ Rev* 61: 784–805.

Bursian D, Fürth S (2015) Trust Me! I am a European Central Banker. *J Money Credit Bank* 47: 1503–1530. https://doi.org/10.1111/jmcb.12282

Cheng P (2023) Decoding the rise of Central Bank Digital Currency in China: designs, problems, and prospects. *J Bank Regul* 24: 156–170. https://doi.org/10.1057/S41261-022-00193-5

Chin AG, Harris MA, Brookshire R (2022) An Empirical Investigation of Intent to Adopt Mobile Payment Systems Using a Trust-based Extended Valence Framework. *Inf Sys Front* 24: 329–347. https://doi.org/10.1007/s10796-020-10080-x

Compeau DR, Higgins CA (1995) Computer self-efficacy: Development of a measure and initial test. *MIS Q: Manage Inf Sys* 19: 189–210. https://doi.org/10.2307/249688

Culnan MJ (1993) "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Q: Manage Inf Sys* 17: 341–361. https://doi.org/10.2307/249775

Culnan MJ, Armstrong PK (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organ Sci* 10: 104–115. https://doi.org/10.1287/orsc.10.1.104

Dang VT, Nguyen N, Nguyen HV, et al. (2022) Consumer attitudes toward facial recognition payment: an examination of antecedents and *outcomes. Int J Bank Mark* 40: 511–535. https://doi.org/10.1108/IJBM-04-2021-0135

Dash G, Paul J (2021) CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technol Forecast Social Change* 173. https://doi.org/10.1016/J.TECHFORE.2021.121092

Davis F (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Q* 13: 319. https://doi.org/10.2307/249008

De Kerviler G, Demoulin NTM, Zidda P (2016) Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers? *J Retail Consum Serv* 31: 334–344. https://doi.org/10.1016/j.jretconser.2016.04.011

Dinev T, Hart P (2004) Internet privacy concerns and their antecedents -measurement validity and a regression model. *Behav Inf Technol* 23: 413–422. https://doi.org/10.1080/01449290410001715723

Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Inf Syst Res* 17: 61–80. https://doi.org/10.1287/isre.1060.0080

Dinev T, Hart P, Dinev T, et al. (2006) *An Extended Privacy Calculus Model for E-Commerce Transactions an Extended Privacy Calculus Model for E-Commerce Transactions*. https://doi.org/10.1287/isre.1060.0080

Dogan A, Bicakci K (2023) KAIME : Central Bank Digital Currency with Realistic and Modular Privacy. *Cryptology EPrint Archive*. https://doi.org/10.5220/0012308600003648

Esmaeilzadeh P, Subramanian H, Cousins K (2019) Individuals' Cryptocurrency Adoption: A Proposed Moderated-Mediation Model. *Americas Conference on Information Systems (AMCIS)*, *25th*. Available from: https://aisel.aisnet.org/amcis2019/adoption_diffusion_IT/adoption_diffusion_IT/1/

European Central Bank (2020) *Report on a digital euro* (Issue October). Available from: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

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

European Central Bank (2022) *Progress on the investigation phase of a digital euro*.

European Commission (2023) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of the digital euro. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0369.

Fang W, Liu N, Pan Q, et al. (2023) The trilateral game of privacy perception, financial regulation and central bank digital currency issuance. *J Account Bus Financ Res* 16: 44–52. https://doi.org/10.55217/102.v16i2.644

Featherman MS, Miyazaki AD, Sprott DE (2010) Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. *J Serv Mark* 24: 219–229. https://doi.org/10.1108/08876041011040622

Featherman MS, Pavlou PA (2003) Predicting e-services adoption: A perceived risk facets perspective. *Int J Hum Comput Stud* 59: 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3

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

Goodell G, Al-Nakib H, Tasca P (2021) A digital currency architecture for privacy and owner custodianship. *Future Int* 13: 130. https://doi.org/10.3390/fi13050130

Goodhue DL, Thompson RL (1995) Task-technology fit and individual performance. *MIS Q Manage Inf Syst* 19: 213–233. https://doi.org/10.2307/249689

Gross J, Sedlmeir J, Babel M, et al. (2021) Designing a Central Bank Digital Currency with Support for Cash-Like Privacy. *SSRN Electron J*. https://doi.org/10.2139/ssrn.3891121

Hair J, Ringle CM, Sarstedt M (2011) PLS-SEM: Indeed a Silver Bullet. *J Market Theory Pract* 19: 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hajli N, Lin X (2016) Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *J Bus Ethics* 133: 111–123. https://doi.org/10.1007/S10551-014-2346-X

Hallam C, Zanella G (2017) Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Comput Hu Behav* 68: 217–227. https://doi.org/10.1016/J.CHB.2016.11.033

Harborth D, Pape S (2021) Investigating Privacy Concerns Related to Mobile Augmented Reality Apps – A Vignette Based Online Experiment. *Comput Hum Behav* 122: 106833. https://doi.org/10.1016/j.chb.2021.106833.

Hassan LM, Shiu E, Shaw D (2016) Who Says There is an Intention–Behaviour Gap? Assessing the Empirical Evidence of an Intention–Behaviour Gap in Ethical Consumption. *J Bus Ethics* 136: 219–236. https://doi.org/10.1007/S10551-014-2440-0

Henseler J, Ringle CM, Sarstedt M (2015) A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J Acade Market Sci* 43: 115–135. https://doi.org/10.1007/s11747-014-0403-8

Huang H, Li X (2023) China's Pursuit of Central Bank Digital Currency: Reasons, Prospects and Implications. *Bank Financ Law Rev* 39. https://papers.ssrn.com/abstract=4566641

Huang M, Ren Y, Wang X, et al. (2023) What affects the use of smartphones by the elderly? A hybrid survey from China. *National Account Rev* 5: 245–260. https://doi.org/10.3934/NAR.2023015

Jabbar A, Geebren A, Hussain Z, et al. (2023) Investigating individual privacy within CBDC: A privacy calculus perspective. *Res Int Bus Financ* 64: 101826. https://doi.org/10.1016/j.ribaf.2022.101826

Kimmerl J (2020) Understanding Users' Perception on the Adoption of Stablecoins - The Libra Case. *PACIS 2020 Proceedings*. Available from: https://aisel.aisnet.org/pacis2020/187

Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput Security* 64: 122–134. https://doi.org/10.1016/J.COSE.2015.07.002

Kosse A, Mattei I (2023) *Making headway - Results of the 2022 BIS survey on central bank digital currencies and crypto*. https://www.bis.org.

Lee DKC, Shih CM, Zheng J, et al. (2023) Asian CBDCs on the rise: An in-depth analysis of developments and implications. *Quant Financ Econ* 7: 665–696. https://doi.org/10.3934/QFE.2023032

Lee DKC, Yan L, Wang Y (2021) A global perspective on central bank digital currency. *China Econ J* 14: 52–66. https://doi.org/10.1080/17538963.2020.1870279

Lee SG, Trimi S, Kim C (2013) The impact of cultural differences on technology adoption. *J World Bus* 48: 20–29. https://doi.org/10.1016/J.JWB.2012.06.003

Lee Y, Son B, Park S, et al. (2021) A survey on security and privacy in blockchain-based central bank digital currencies. *J Int Serv Inf Secur* 11: 16–29. https://doi.org/10.22667/JISIS.2021.08.31.016

Li Y (2011) Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Commun Assoc Inf Syst* 28. https://doi.org/10.17705/1CAIS.02828

Li Z, Yang C, Huang Z (2022) How does the fintech sector react to signals from central bank digital currencies? *Financ Res Lett* 50: 103308. https://doi.org/10.1016/J.FRL.2022.103308

Lin J, Lu Y, Wang B, et al. (2011) The role of inter-channel trust transfer in establishing mobile commerce trust. *Electron Comm Res Appl* 10: 615–625. https://doi.org/10.1016/j.elerap.2011.07.008

Lin WS, Wang CH (2012) Antecedences to continued intentions of adopting e-learning system in blended learning instruction: A contingency framework based on models of information system success and task-technology fit. *Comput Edu* 58: 88–99. https://doi.org/10.1016/J.COMPEDU.2011.07.008

Maddux JE, Rogers RW (1983) Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *J Exp Social Psychology* 19: 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Inf Syst Res* 15: 336–355. https://doi.org/10.1287/isre.1040.0032

Miltgen CL, Peyrat-Guillard D (2014) Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *Eur J Inf Syst* 23: 103–125. https://doi.org/10.1057/ejis.2013.17

Nissenbaum H (2010) *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford University Pres.

Ozdemir ZD, Jeff Smith H, Benamati JH (2017) Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *Eur J Inf Syst* 26: 642–660. https://doi.org/10.1057/s41303-017-0056-z

Patton MA, Jøsang A (2004) Technologies for Trust in Electronic Commerce. *Electron Comm Res* 4: 9–21. https://doi.org/10.1023/B:ELEC.0000009279.89570.27

Pavlou PA (2003) Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *Int J Electron Comm* 7: 101–134. https://doi.org/10.1080/10864415.2003.11044275

Pavlou PA, Fygenson M (2006) Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Q Manage Inf Syst* 30: 115–143. https://doi.org/10.2307/25148720

Pavlou PA, Gefen D (2005) Psychological Contract Violation in Online Marketplaces: Antecedents, Consequences, and Moderating Role. 16: 372–399. https://doi.org/10.1287/ISRE.1050.0065

People's Bank of China (2021) *Progress of e-CNY in China*.

Pocher N, Veneris A (2021) Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme. *SSRN Electron J,* 1–9. https://doi.org/10.2139/ssrn.3759144

Ramos-de-Luna I, Montoro-Ríos F, Liébana-Cabanillas F (2016) Determinants of the intention to use NFC technology as a payment system: an acceptance model approach. *Inf Syst E-Bus Manage* 14: 293–314. https://doi.org/10.1007/s10257-015-0284-5

Raymaekers W (2015) Cryptocurrency Bitcoin: Disruption, challenges and opportunities. *J Payments Strat Syst* 9: 30–46.

Sarstedt M, Ringle CM, Hair JF (2017) Partial Least Squares Structural Equation Modeling. *Handbook Market Res,* 1–40. https://doi.org/10.1007/978-3-319-05542-8_15-1

Sauer B (2016) Virtual currencies, the money market, and monetary policy. *Int Adv Econ Res* 22: 117–130. https://doi.org/10.1007/s11294-016-9576-x

Schueffel P (2023) CBDCs: Pros and Cons - A Comprehensive List and Discussion of the Advantages and Disadvantages of Central Bank Digital Currency. *SSRN Electron J*. https://doi.org/10.2139/SSRN.4398748

Sharma S (1991) *Behind the Diffusion Curve: An Analysis of ATM ADoption*.

Sheeran P, Webb TL (2016) The Intention-Behavior Gap. *Social Pers Psychology Compass* 10: 503–518. https://doi.org/10.1111/SPC3.12265

Smith HJ, Dinev T, Xu H (2011) *Information privacy research: an interdisciplinary review. MIS Q,* 989–1015. https://doi.org/10.2307/41409970

Smith HJ, Milberg SJ, Burke SJ (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Q,* 167–196. https://doi.org/10.2307/249477

Sohaib O, Hussain W, Asif M, et al. (2020) A PLS-SEM Neural Network Approach for Understanding Cryptocurrency Adoption. *IEEE Access* 8: 13138–13150. https://doi.org/10.1109/ACCESS.2019.2960083

Solberg Söilen K, Benhayoun L (2022) Household acceptance of central bank digital currency: the role of institutional trust. *Int J Bank Mark* 40: 172–196. https://doi.org/10.1108/IJBM-04-2021-0156

Stoica M, Miller DW, Stotlar D (2005) New Technology Adoption, Business Strategy and Government Involvement: The Case of Mobile Commerce. *J Nonprofit Public Sector Mark* 13: 213–232. https://doi.org/10.1300/J054V13N01_12

Su P, Wang L, Yan J (2018) How users' Internet experience affects the adoption of mobile payment: a mediation model. *Technol Anal Strat Manage* 30: 186–197. https://doi.org/10.1080/09537325.2017.1297788

Sun T, Rizaldy R (2023) Some Lessons from Asian E-Money Schemes for the Adoption of Central Bank Digital Currency. *IMF Working Paper* 2023/123. https://doi.org/10.5089/9798400245565.001

Tavakol M, Dennick R (2011) Making sense of Cronbach's alpha. *Int J Medical Edu* 53. https://doi.org/10.5116/IJME.4DFB.8DFD

Tronnier F, Biker P (2022) A Framework and Qualitative Evaluation of Privacy Concerns in the Digital Euro. *PACIS 2022 Proceedings*. Available from: https://aisel.aisnet.org/pacis2022/63.

Tronnier F, Harborth D, Biker P (2023) Applying the extended attitude formation theory to central bank digital currencies. *Electron Mark* 33: 1–21. https://doi.org/10.1007/S12525-023-00638-3

Tronnier F, Harborth D, Hamm P (2022) Investigating privacy concerns and trust in the digital Euro in Germany. *Electron Comm Res Appl* 53: 101158. https://doi.org/https://doi.org/10.1016/j.elerap.2022.101158

Tsai HYS, Jiang M, Alhabash S, et al. (2016) Understanding online safety behaviors: A protection motivation theory perspective. *Comput Security* 59: 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Venkatesh V, Davis FD (2000) A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Manage Sci* 46: 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh V, Morris M, Davis G, et al. (2003) User acceptance of information technology: Toward a unified view. *MIS Q Manage Inf Syst* 27. https://doi.org/10.2307/30036540

Venkatesh V, Thong JYL, Yu X (2012) Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology1. *MIS Q Manage Inf Syst* 36. https://doi.org/10.1088/1751-8113/44/8/085201

Wadsworth A (2018) The pros and cons of issuing a central bank digital currency. *Reserve Bank New Zealand Bull* 81: 1–21.

Wang YR, Ma CQ, Ren YS (2022) A model for CBDC audits based on blockchain technology: Learning from the DCEP. *Res Int Bus Financ*, 101781. https://doi.org/10.1016/j.ribaf.2022.101781

Warren SD, Brandeis LD (1890) The Right to Privacy. *Harvard Law Rev* 4: 193. https://doi.org/10.2307/1321160

Westin AF (1967) *Privacy and Freedom*. Antheneum.

Wonneberger ET, Mieg HA (2011) Trust in money: hard, soft and idealistic factors in Euro, gold and German community currencies. *J Sust Financ Invest* 1: 230–240. https://doi.org/10.1080/20430795.2012.655891

Wu B, An X, Wang C, et al. (2022) Extending UTAUT with national identity and fairness to understand user adoption of DCEP in China. *Sci Report* 12: 1–11. https://doi.org/10.1038/s41598-022-10927-0

Xia H, Gao Y, Zhang JZ (2023) Understanding the adoption context of China's digital currency electronic payment. Financial *Innovation* 9: 1–27. https://doi.org/10.1186/S40854-023-00467-5

Xu J (2022) Developments and Implications of Central Bank Digital Currency: The Case of China e-CNY. *Asian Econ Policy Rev* 17: 235–250. https://doi.org/10.1111/AEPR.12396

Yang J, Zhou G (2022) A study on the influence mechanism of CBDC on monetary policy: An analysis based on e-CNY. *PLOS ONE* 17. https://doi.org/10.1371/JOURNAL.PONE.0268471

Zarifis A, Cheng X, Dimitriou S, Efthymiou L (2015) Trust in Digital Currency Enabled Transactions Model. *MCIS 2015 Proceedings*.

Zhou T, Lu Y, Wang, B. (2010) Integrating TTF and UTAUT to explain mobile banking user adoption. *Comput Hum Behav* 26: 760–767. https://doi.org/10.1016/j.chb.2010.01.013

AIMS Press