



BIS Working Papers
No 1147

Central Bank Digital
Currency and Privacy: A
Randomized Survey
Experiment

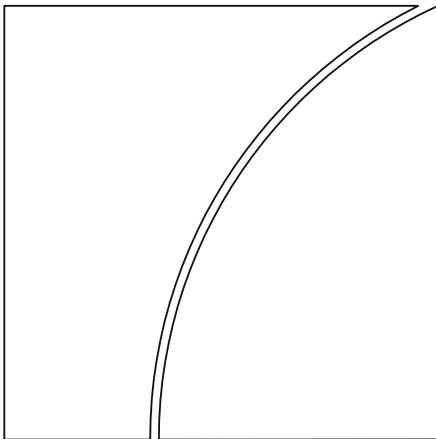
by Syngjoo Choi, Bongseob Kim, Young-Sik Kim, Ohik
Kwon

Monetary and Economic Department

November 2023

JEL classification: E40, E50, C90

Keywords: central bank digital currency (CBDC), privacy,
randomized online survey experiment



BIS Working Papers are written by members of the Monetary and Economic Department of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS.

This publication is available on the BIS website (www.bis.org).

© *Bank for International Settlements 2023. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.*

ISSN 1020-0959 (print)
ISSN 1682-7678 (online)

Central Bank Digital Currency and Privacy: A Randomized Survey Experiment*

Syngjoo Choi[†] Bongseop Kim[‡] Young Sik Kim[§] Ohik Kwon[¶]

November 9, 2023

Abstract

Privacy protection is among the key features to consider in the design of central bank digital currency (CBDC). Using a nationally representative sample of over 3,500 participants, we conduct a randomized online survey experiment to examine how the willingness to use CBDC as a means of payment varies with the degree of privacy protection and information provision on the privacy benefits of using CBDC. We find that both factors significantly increase participants' willingness to use CBDC by up to 60% when purchasing privacy-sensitive products. Our findings provide useful insights regarding the design and the public's adoption of CBDC.

Keywords: central bank digital currency (CBDC), privacy, randomized online survey experiment

JEL classification numbers: E40, E50, C90

*We wish to thank two anonymous reviewers, an associate editor, and an editor for their comments which have helped us improve the paper substantially. We also gratefully acknowledge valuable inputs provided by In Do Hwang, Hwan Koo Kang, Dongsup Kim, Kyeongtae Lee, Suk Won Lee, Yang Su Park, Byoung-ki Kim, Sung Guan Yun, Jaevin Park and participants in the 2023 Asia-Pacific Economic Science Association Meeting at Seoul National University. This study was supported by the Bank of Korea and the Creative-Pioneering Researchers Program through Seoul National University. We received the IRB approval from Seoul National University (IRB No.2109/002-023). This study is registered at the AEA Registry (AEARCTR-0008059). The views expressed in this paper are those of authors and may not necessarily reflect the official views of the Bank of Korea or the Bank for International Settlements. All errors are our own.

[†]Department of Economics, Seoul National University. Email: syngjooc@snu.ac.kr

[‡]Department of Economics, Seoul National University. Email: bongseop@snu.ac.kr

[§]Department of Economics & SIRFE, Seoul National University. Email: kimy@snu.ac.kr

[¶]Economic Research Institute, Bank of Korea; Bank for International Settlements. Email: okwon@bok.or.kr; ohik.kwon@bis.org

1 Introduction

Central bank digital currency (CBDC) refers to money issued in digital form by the central bank for use either among financial institutions only (i.e. wholesale CBDC) or by the general public including households and non-bank businesses (i.e. retail CBDC). It is denominated in the national unit of account and is a direct liability of the central bank, similar to physical cash. A main departure of retail CBDC from physical cash is limited anonymity due to the electronic form it takes. Privacy protection emerges as an important issue because there is a possibility that personal identity information and transaction data are concentrated in the central bank when it provides a CBDC account or a digital wallet to individuals and businesses for their use of CBDC as a means of payment and a store of value ([Bank for International Settlement, 2021](#)). In what follows CBDC will refer to retail CBDC only.

As the demand for anonymous payment methods is expected to continue in order to protect user data and secure the right to be forgotten, there have been discussions about how much anonymity should be provided by the central bank (e.g. [Kahn, 2018](#)). For cash, anonymity and privacy are essentially protected. However, for CBDC, the degree of anonymity and privacy protection is determined by the policy judgment of the central bank. Even if CBDC is designed in a way that protects a high level of privacy, it must comply with anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations. Therefore, there is a possibility of privacy being invaded to a degree that exceeds what consumers are willing to tolerate. The lack of privacy protection can be costly for consumers, from tangible costs such as identity theft or discrimination to less tangible ones such as stigma or psychological discomfort ([Acquisti et al., 2016](#)). The costs associated with inadequate privacy protection are substantial, as evidenced by the fact that in 2021, around 15 million consumers in the United States were impacted by identity theft, causing losses of approximately 24 billion USD ([Javelin, 2022](#)).

According to the results of a recent online survey by the European Central Bank, the largest majority of respondents (41%) chose privacy protection as the most important characteristic to consider when issuing a CBDC ([European Central Bank, 2021](#)). The Federal Reserve is also exploring privacy as one of the key issues for a potential U.S. CBDC ([Board of Governors of the Federal Reserve System, 2022](#)). As noted by [Goldfarb and Tucker \(2012\)](#), privacy concerns are increasing over time, making it even more important to consider privacy in the context of CBDC.

Since the public's willingness to use CBDC may vary with the degree of restrictions on anonymity or the degree of privacy protection when using CBDC, a careful investigation

is required as to how the different extent of privacy protection affects the potential choice of using CBDC. In addition, it is necessary to analyze the choice of CBDC as a means of payment due to its potential privacy benefits compared to the existing private electronic payment methods. Noting that CBDC is not currently in use, the intention to use it when issued in the future can be investigated through a survey of the general public who are presented with hypothetical design choices for CBDC.

In this paper we conduct a randomized survey experiment to measure how the willingness to use CBDC changes with the degree of anonymity and privacy protection offered, and the provision of information on the potential privacy benefits of using CBDC such as preventing the commercial use of personal identity information and transaction data. Our study takes into account the main issues discussed in the literature regarding the design choices of CBDC concerning privacy protection and data governance. First, CBDC could be designed to protect privacy and give its users control over whom they share data with while meeting AML and CFT regulations. This would essentially require the separation of a user's personal identity information from transaction data as proposed in the platform CBDC model by the [Bank of England \(2020\)](#). Since the central bank would have no access to user's personal data, privacy concerns due to holding personal identity information by the central bank would be practically eliminated, but AML and/or CFT requirements could still be fulfilled. Second, as properly noted by [Garratt and van Oordt \(2021\)](#), the introduction of CBDC could allow for privacy-enhancing techniques that shield the personal identity and characteristics of its users from commercial parties (e.g. BigTech). Finally, the CBDC design could include "anonymity vouchers" to ensure the anonymity of small value purchases of privacy-sensitive products without the AML authority seeing transaction data ([European Central Bank, 2019](#)).

Our randomized online survey experiment was conducted with a nationally representative sample of over 3,500 participants born in South Korea. We designed the survey experiment to identify the causal impact of the following on the willingness to use CBDC as a means of payment: (1) CBDC design for the preservation of privacy and (2) information on the potential privacy benefits of using CBDC in the sense that it can prevent the use of personal identity information and transaction data by commercial parties such as financial institutions and BigTech companies.

The first arm of the randomization process provides participants with one of the three versions of the CBDC design that differ in the extent to which privacy is preserved upon using CBDC as a means of payment. Specifically, a *combined repository* (CR) stores both personal identity information and transaction data in a single institution, which can be combined arbitrarily to identify an individual who pays for the associated transaction using CBDC. In contrast, a *separate repository* (SR) stores personal identity information

and transaction data separately in two different institutions, which makes it practically impossible to combine them for individual identification. A *small-amount CBDC Voucher* (Voucher) allows its users to have cash-like anonymity for small-amount transactions without revealing neither personal identity information nor transaction data to the AML authority. In the second arm of the randomization, half of the participants are provided with the information that CBDC can *prevent the commercial use* (PCU) of its users' personal identity information and transaction data by private financial institutions and BigTech companies. This information is not provided to the other half of the survey participants.

As a result, our randomized experiment has a three-by-two factorial design with six equally sized homogeneous treatment groups, each consisting of about 590 participants and referred to as CR, CR & PCU, SR, SR & PCU, Voucher, and Voucher & PCU. Participants in each treatment group are asked identical questions about their choice of payment methods for offline and online transactions out of credit and/or debit cards, mobile fast payment, cash (not available online), and CBDC when purchasing privacy-sensitive and privacy-insensitive products, respectively. By comparing the differences in the responses to these questions across groups, we aim to estimate the causal effects of different CBDC schemes with regard to the preservation of privacy and the privacy benefits of using CBDC on the willingness to choose CBDC as a means of payment.

The main results of the paper are as follows. First, we find significant effects of the privacy preserving variations of the CBDC design on the willingness to use CBDC when respondents purchase privacy-sensitive products (e.g., psychiatric services, adult products). Compared to the CR treatment as a baseline, the SR treatment and the Voucher treatment increase the willingness to use CBDC by 7 and 5 percentage points, respectively, in offline purchasing situations. The impacts of the CBDC privacy-preserving design appear to be even larger in online purchasing situations; the SR design and the Voucher design raise the likelihood of choosing CBDC by about 11 and 9 percentage points, respectively. Considering the average frequency of choosing CBDC in the CR treatment, the magnitudes of the effects of the privacy-preserving variations (i.e. SR and Voucher) in the CBDC design range between 19% and 29%. Using multinomial logit analysis, we find that the increase in the willingness to use CBDC due to the privacy-preserving variations of the CBDC design is mostly accompanied by decreases in the usage of cash and credit and/or debit cards, but not in the demand for mobile fast payment. When purchasing privacy-insensitive products (e.g., food, office supplies), we find negligible treatment effects in both offline and online purchasing situations.

Second, we find that the willingness to use CBDC increases significantly with the provision of information about the privacy benefits of using it. The PCU treatment increases the willingness to use CBDC by about 6 percentage points in the offline purchasing of privacy-

sensitive products, amounting to a 20% increase relative to the usage of CBDC in the baseline treatment (CR), and by 4 percentage points in online purchasing, amounting to a 9% increase relative to the baseline treatment. When purchasing privacy-insensitive products, the PCU treatment has weak effects on respondents' willingness to choose CBDC.

Third, compared to the baseline treatment, when respondents are provided with the privacy preservation of the CBDC design and the PCU information jointly, their willingness to choose CBDC increases by 14 percentage points in the SR & PCU treatment in both offline and online purchases, amounting to a 60% increase relative to the baseline treatment. In the Voucher & PCU treatment, willingness to choose CBDC also increases by 11 and 12 percentage points in offline and online purchases, respectively.

Furthermore, we find that the treatment effects are larger for those who are more responsive to privacy protection activity by using cash in offline purchases, and for those who show less concern over privacy invasion by government or private institutions such as traditional financial institutions and BigTech companies. In addition, we find heterogeneous treatment effects across demographic characteristics; for example, females are more responsive to the extent of privacy preservation associated with using CBDC and the provision of PCU information than males.

Our paper contributes to the literature regarding monetary economics that emphasizes the role of money in providing transaction privacy. [Kahn et al. \(2005\)](#) argue that anonymous physical cash can be in constant demand in transactions requiring privacy (e.g. medications for mental illness) because it protects the transaction parties from potential risks due to identity exposure, unlike electronic payment methods such as credit cards. More recently, [Garratt and van Oordt \(2021\)](#) claim that CBDC can contribute to enhancing consumer welfare as a public good which not only protects consumer privacy, but also prevents financial institutions and BigTech companies from monopolizing information. These foregoing studies theoretically explore the possibility that people demand monies (cash or CBDC) issued by central banks because they can preserve transaction privacy. Our paper complements this literature by providing empirical evidence on theoretical results.

We also contribute to the recent literature which empirically investigates the relationship between privacy concerns and consumers' willingness to use CBDC.¹ First, [Abramova et al. \(2022\)](#) and [Bijlsma et al. \(2021\)](#) surveyed participants about their willingness to use CBDC and conducted a partial correlation analysis of these responses with individual at-

¹This literature investigates more broadly what would be the impact of CBDC issuance on the household's demand for payment instruments and liquid assets. In the literature regarding correlational studies including [Abramova et al. \(2022\)](#) and [Bijlsma et al. \(2021\)](#), [Fujiki \(2021\)](#) found, using Japanese survey data, that the survey respondents value the shorter transaction time associated with CBDC.

titudes toward privacy. Our paper differs in that we randomly vary the degree of CBDC privacy protection design and information provision on the privacy benefits of using CBDC and report their causal impacts on participants’ willingness to use it. Second, [Huynh et al. \(2020\)](#) and [Li \(2022\)](#) used a household survey about the usage of existing payment methods – cash, debit, and credit cards – and estimated the influences of their attributes as well as individual characteristics on the demands for existing payment methods. Based on the estimation results and structural assumptions, they predicted the demand for CBDC whose design characteristics vary from cash-like to debit-like when it is introduced. This structural analysis leads to the prediction of the impacts of CBDC design attributes such as anonymity and security on its demand. Our paper complements these studies by conducting a randomized survey experiment with a representative adult sample and evaluating the causal impacts on participants’ willingness to use CBDC. Third, using discrete choice experiments, [Choi et al. \(2023\)](#) examined individual respondents’ preferences for the relevant attributes of payment methods and used the estimated preferences to predict the payment preference for CBDC characterized as a collection of payment attributes. Preferences for the privacy-protection attribute in terms of disclosure of information type are shown to have a significant but modest effect in the general context of payment method choices. Our paper focuses more on the details of the privacy protection design of CBDC and their impacts on CBDC demand, suggesting how to design the privacy protection details of CBDC.

There have been several empirical and experimental studies on the desirable features of CBDC and the associated impact on the payment system. For instance, the experimental studies of [Camera et al. \(2003\)](#) and [Camera \(2020\)](#) found that an interest-bearing CBDC could induce hoarding, thereby disrupting the payment system. Another experimental study by [Borgonovo et al. \(2021\)](#) showed that anonymity matters for money demand. Based on the previous episodes and experimental studies, [Jiang \(2020\)](#) found that CBDC could have a clear niche as “enhanced cash” in the sense that it reduces carrying costs and enables electronic transfers, while retaining its distinctive desirable features including a high degree of privacy. None of the existing studies in this literature evaluate the role of CBDC in privacy protection. To the best of our knowledge, our paper is the first attempt to examine the effects of the privacy-preserving design of CBDC and the information about its privacy benefits on the public’s willingness to use CBDC as a means of payment.²

Our paper is also related to the literature regarding economics of privacy, namely, the

²As a related study, [Alvarez et al. \(2022\)](#) conducted a national face-to-face survey in El Salvador which adopted Bitcoin as legal tender in September 2021. They found that it was not well accepted as a medium of exchange for daily transactions, despite a large incentive being offered by the government.

cost-benefit perspective of protecting or sharing personal data (see [Acquisti et al. \(2015\)](#) and [Acquisti et al. \(2016\)](#) for a review of this literature). A growing list of studies uses experimental methods to understand privacy-related decision making ([Acquisti et al., 2013](#), [Tsai et al., 2011](#), [Feri et al., 2016](#), [Athey et al., 2017](#), [Prince and Wallsten, 2022](#)). For instance, [Tsai et al. \(2011\)](#) found that a privacy protection policy affects consumer’s online purchasing decisions. [Feri et al. \(2016\)](#) also found that risk perceptions of personal data leakage determine an individual’s intent to provide sensitive personal information to firms. [Prince and Wallsten \(2022\)](#) found that people especially value privacy for financial (bank balance) information which reflects their transaction records. Following the traditional economic analysis of privacy, our paper contributes to this literature by showing that the privacy-preserving variations of the CBDC design and the information about its privacy benefits are instrumental in individuals’ willingness to use CBDC.

Finally, this paper is related to recent macroeconomic studies using randomized controlled trials to investigate how people learn and respond to information about monetary policy, fiscal policy, or financial stability. For instance, [Coibion et al. \(2022\)](#) examine how different forms of inflation information, such as the Federal Open Market Committee (FOMC) statement, inflation target, or news articles on FOMC meetings, influence inflation expectations in a randomized controlled trial using a sample of nearly 20,000 individuals in the US. Other works using a similar methodology include [Brouwer and de Haan \(2022\)](#), [Galati et al. \(2022\)](#), [Beutel et al. \(2021\)](#), [Coibion et al. \(2021\)](#), and [Grosse-Steffen \(2021\)](#).

The rest of the paper is organized as follows. Section 2 describes the online survey and the experimental design based on discussions in the literature on the CBDC design choices with regard to the preservation of privacy. It also presents sample characteristics and balance checks. Section 3 discusses the conceptual and empirical frameworks followed by the estimation results in Section 4 about the causal effects of different degrees of privacy preservation and the potential privacy benefits of CBDC on its choice as a means of payment. Section 5 presents the concluding remarks.

2 Survey and Experimental Design

We begin with a description of how we designed the online survey and randomized experiments based on the discussions in the literature concerning the CBDC design features for privacy protection. We also present the sample characteristics of the online survey and balance checks across treatment groups participating in the randomized experiments.

2.1 Survey Design

In November 2021, we conducted an online survey via Hankook Research, a professional survey company, using a nationally representative sample of 3,561 participants, born in South Korea and aged 19 years and above.³ For data quality, participants with a response time of less than four minutes were excluded.⁴ Therefore, the analysis was conducted on the remaining 3,514 participants. Each participant received a participation fee of KRW 2,000 (US\$1.68, as of January 11, 2022) upon completing the survey. Figure 1 shows the survey flow which consists of five modules.⁵ The full survey questionnaire (the original Korean version as well as its English translation) and screenshots of the randomization module for CBDC and privacy by treatment status are available in the online Appendix.

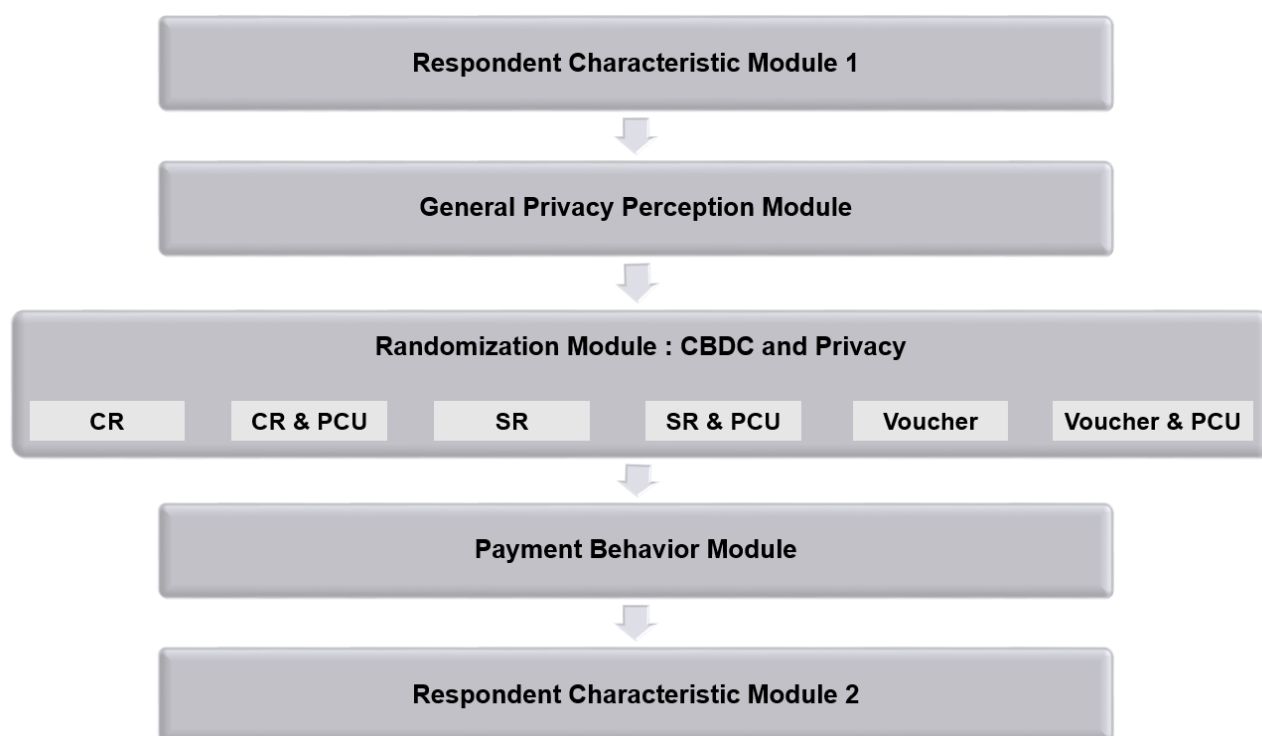


Figure 1: Survey Flow

³The socio-demographics of the survey sample correspond well to the underlying population. However, noting that the respondents are filling out an online survey which includes questions on their payment behavior as well as their financial situation, the sample is possibly balanced towards consumers who have below average privacy concerns. If it happened, this would strengthen the findings of this paper since the average treatment effects we find would be lower bound estimates for a representative population sample.

⁴We set this time following the comments of Hankook Research. The main results are not affected when these outliers are included.

⁵We conducted a very brief survey module before the randomization module. In addition, after the randomization module, we implemented another randomization module regarding financial stability and a survey module on preferences over payment methods specialized for conjoint analysis. We report the results of these omitted modules in a companion paper. The details are available upon request.

Respondent Characteristics: In the first and last modules, we collect information about respondents' characteristics including gender, age, education, marital status, employment status, household income and wealth.

General Privacy Perception: In the second module, we measure respondents' attitudes toward privacy, their past behavior with respect to the protection of personal identity information, and their knowledge of privacy. In particular, we measure perceptions about privacy in various situations, using questions adopted from previous surveys such as those used by the [Pew Research Center \(2014, 2019\)](#), and [Korea Information Society Development Institute \(2020\)](#) as well as those created by us. Participants are asked about how much they are concerned about the leakage of confidential information, how sensitive they are to the exposure of individual information to others, and how much they value the right to privacy. In particular, regarding the protection of individual privacy rights, we assess participants' trust in the government and public institutions, private financial institutions, and IT or BigTech companies, respectively. The general privacy perception measurements from all of the respondents will be used to examine how the willingness to use CBDC as a means of payment, by those randomly assigned to each treatment group, varies with the heterogeneity of privacy perception.

CBDC and Privacy Experiment: In the third module, we conduct a randomized survey experiment to estimate the willingness to use CBDC depending on the degree of privacy protection and the provision of information on the potential privacy benefits of using it as a means of payment. This module starts with a quick CBDC tutorial that illustrates its features and how to use it. This information is provided in plain language using pictures and lasts for 30 seconds. Participants are then asked to solve two quiz questions to check their understanding of the tutorial. After confirming the correct answers to these questions, they are allowed to proceed to the next pages of the experimental survey. The details of the experimental design are described in [Section 2.3](#).

Payment Behaviors: In this module, participants are asked about their purchase and payment behaviors, including where they usually make purchases (offline/online) and which payment method they usually use (e.g., cash, credit/debit cards, mobile fast payment). They are also asked about how much cash they carry on average and whether they have experience with cryptocurrency.

2.2 Experimental Design: Background

There have been active discussions in both policy circles and academia with regard to the design choices of retail CBDC and the associated implications for privacy and data gov-

ernance. In general, effective identification is crucial to the payment system's safety and integrity by preventing fraud as well as complying with AML and/or CFT regulations. Hence, identification at some level is central to the design of CBDCs, which calls for an account-based CBDC, but with safeguards on data privacy ([Bank for International Settlement, 2021](#)). It is therefore essential to consider how privacy is respected and data is protected when designing a CBDC system.

First, CBDC compliance with AML and/or CFT regulations would rule out truly anonymous payments. However, CBDC could be designed to protect privacy and give users control over who they share data with. For example, users may want to make payments to a BigTech without sharing their personal identity information, concerned that this would allow a BigTech to use it for commercial purposes. In this way, the payer could have anonymity with other users, but not with law enforcement. Specifically, the [Bank of England \(2020\)](#) proposes that the core ledger only stores pseudonymous accounts and balances, but that each account in the core ledger is linked to a separate payment interface provider who knows the personal identity information of each user and applies AML checks to users. This arrangement would essentially allow for the separation of a user's personal identity information from transaction data, reducing the privacy concerns that could arise from the central bank holding the personal data of CBDC users.

Second, as properly noted by [Garratt and van Oordt \(2021\)](#) and [Ahnert et al. \(2022\)](#), there is a strong incentive for commercial platforms (e.g. BigTech) to monetize the transaction data of their users. That is, payment data revealed by one person can be used to make inferences about the purchasing habits of other individuals. Consumers' privacy protection has a positive externality in the sense that it can prevent the commercial use of their transaction data by commercial platforms to infer other consumers' purchasing behavior. An electronic form of cash such as CBDC could duplicate the properties of physical cash by introducing a privacy-enhancing technique that shields personal identity information and the transaction data of its users from commercial use by private financial institutions and BigTech.

Finally, a new concept of "anonymity vouchers" has been proposed by the [European Central Bank \(2019\)](#) to enforce AML and/or CFT limits on the amount that a user can spend without the AML authority seeing the transaction data. The AML authority issues these additional, time limited vouchers to every CBDC user at regular intervals. If users want to transfer CBDC without revealing personal identity information to the AML authority, they need to spend these vouchers. Thus, the amount of CBDC that can be spent anonymously is limited by the number of vouchers that the AML authority provides to each user. In short, anonymity vouchers would ensure the anonymity of small-amount transactions using CBDC without leaving any transaction data, thereby protecting users'

privacy.

2.3 Randomized Experiments

Participants are randomly assigned to one of the three experimental conditions that differ in the design of CBDC regarding how personal identity information and transaction data are stored when it is used for transactions. Subsequently, all the participants are further randomly assigned to one of the two experimental conditions regarding the provision of information that the use of CBDC, instead of credit and/or debit cards or mobile fast payment, can prevent private financial institutions and BigTech companies from using personal identity information and transaction data for commercial purposes.

Each participant is then asked which payment method is preferred, for offline and online transactions, out of CBDC, cash (not available online), credit and/or debit card, and mobile fast payment in purchasing privacy-sensitive and privacy-insensitive commodities, respectively. We take examples of commodities regarding privacy sensitivity from [Tsai et al. \(2011\)](#). It is important to distinguish between privacy-sensitive and privacy-insensitive commodities, as the level of reluctance to expose purchase information about a particular commodity varies depending on the commodity type. For example, [Goldfarb and Tucker \(2012\)](#) found that consumers were especially privacy-protective in contexts where they were answering personal questions about health and financial products and such concerns have risen over time partly due to broadening perspectives of the contexts in which privacy is relevant [see also [Acquisti et al. \(2016\)](#)]. Thus, it is an empirical question whether the context-dependent privacy concerns transfer to the choice of payment methods in a context-dependent manner. In addition, the economy-wide significance of the data economy, particularly relying on the data collected from the consumption of privacy-sensitive commodities, becomes more relevant as privacy-related sectors including healthcare, financial, and retail industries go through a digital revolution with the growing data economy at their core. Hence, we believe this distinction of commodities regarding privacy sensitivity is economically meaningful, and central banks may place weight on context-dependent matters of privacy issues in the CBDC design.

Hence, we have a total of six experimental treatments groups based on how personal identity information and transaction data are stored upon the use of CBDC for transactions, and the provision of information that the use of CBDC can prevent the commercial use of personal identity information and transaction data. We employ a three-by-two factorial design to identify the causal impact of the following on the willingness to use CBDC as a means of payment: (1) the protection of privacy and anonymity in the CBDC design and (2) the provision of information on the privacy benefits of CBDC because it can pre-

vent the commercial use of customer information and data by financial institutions and BigTech companies.

Specifically, in the first arm of randomization, participants are shown one of the following three versions of the CBDC design that differ in how personal identity information and transaction data are stored when CBDC is used.

A combined repository (CR): *Personal identity information and transaction data are stored jointly in a single public institution. It may be possible to identify an individual by arbitrarily combining personal identity information and transaction data.*

A separate repository (SR): *Personal identity information and transaction data are stored separately in two different public institutions. It is essentially impossible to identify an individual by combining the two pieces of information.*

A small-amount anonymity voucher (Voucher): *For small amount transactions, one can use CBDC with an anonymity voucher which, like cash, does not leave behind any personal identity information and transaction data trails even for AML and /or CFT checks.*

Information on each CBDC design version and implied protection of privacy is provided in texts and graphics in the survey questionnaire, along with information about the extent to which each of the existing payment instruments (i.e., cash, credit/debit cards, mobile fast payment) protects the privacy and anonymity of its user.

In the second arm of randomization, a half subsample of the participants are shown information on the potential privacy benefits of CBDC, as detailed below, and the other half are not.

Preventing commercial use(PCU): *By using CBDC, people can prevent private financial institutions and companies such as BigTech from using their personal identity information and transaction data for commercial purposes.*

As a result, there are six equally sized groups: CR, CR & PCU, SR, SR & PCU, Voucher, and Voucher & PCU. Figure 2 presents screenshots of sample graphics shown to respondents in the SR and SR & PCU groups, respectively. The information screenshots that were provided to the respondents in all the treatments are presented in Section B.4 in the online Appendix.

All groups are then asked which payment method they would use out of CBDC, cash, credit and/or debit cards, and mobile fast payment when buying privacy-sensitive and privacy-insensitive products, respectively, in offline and online transactions. The distinction between offline and online refers to the availability of cash as a means of payment for

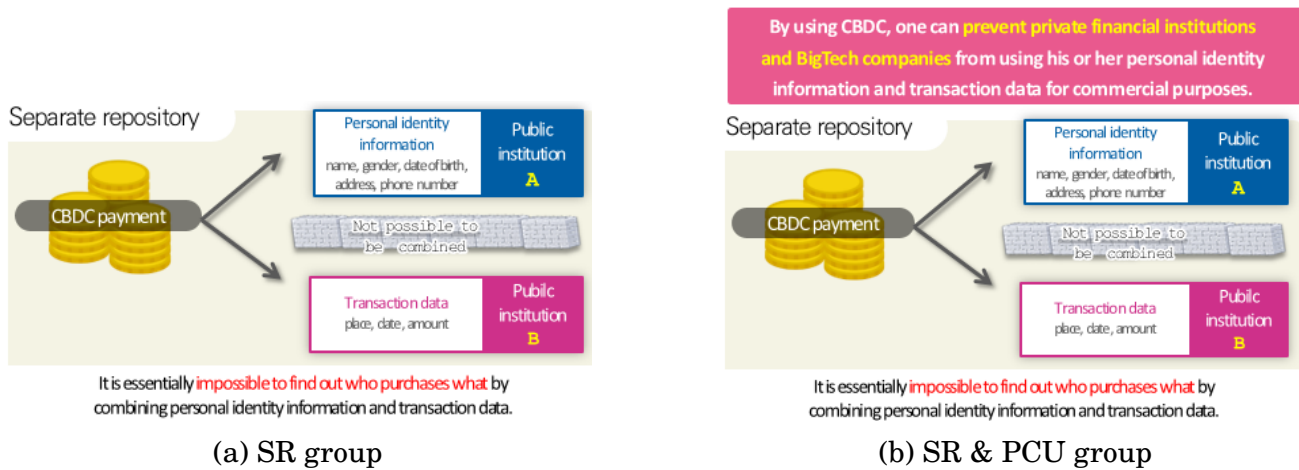


Figure 2: CBDC information screenshots

offline (or in-store) purchases only.⁶ Specifically, the respondents in each group are asked sequential questions as below.

*Suppose you want to buy (1) **privacy-sensitive goods or services (e.g., psychiatric services, adult products, plastic surgery, etc.)** / (2) **privacy-insensitive goods or services (e.g., food, office supplies, electronic goods, etc.)** in (a) **offline** / (b) **online transactions**. If CBDC is available as a means of payment, which payment method would you choose? Please make your choice carefully weighing between privacy exposure risk and convenience yield.*

By comparing the different outcomes of interest across the six groups, we aim to estimate how CBDCs with different privacy protection and provision of information on the potential privacy benefits of using CBDC can affect the willingness to use CBDC as a means of payment.

It is worth noting that our randomized experiments are likely unsusceptible to potential experimenter demand effects by which respondents infer the experimenter's objective and change their behaviors (Charness and Kuhn, 2012). First, we implement between-subject designs in which respondents are exposed to only one treatment. This would make it difficult for respondents to guess which parts of the experimental environment are varied. Second, we use an online survey method which does not allow for interaction between respondents and the experimenter, while guaranteeing respondents' anonymity using an anonymized ID. Finally, de Quidt et al. (2018) provide evidence that experimenter demand effects tend to be small in typical experiments.

⁶As an aspect of the CBDC design, offline functionality often refers to whether it is possible to make payments without internet connections, which is not the case here.

2.4 Sample Characteristics and Balance Checks

Table A1 in the online Appendix provides summary statistics for all respondents (column 1), along with comparing balances of samples between the control group (CR) and the treatment groups. Table A2 in the online Appendix shows that our samples are representative of the South Korean population regarding key individual characteristics when compared with the South Korean Demographic Statistics and the Korean Labor Income Panel Study. To ensure the internal validity of our causal inference, we also conduct tests of equality across the treatment arms in each of the individual characteristics. Columns (2)-(7) of Table A1 report respectively the mean of the control group and the mean differences between the treatment groups and the control group across individual characteristics, indicating no evidence that the treatment groups are systematically different from the control group. In sum, the results confirm that treatments are randomly assigned to participants.

We report simple statistics of the basic variables that will be used in data analysis. First, Table 1 shows distributions of survey outcomes that measure the willingness to use CBDC compared to other payment methods. These outcome variables will be used as dependent variables in our empirical analysis in Section 3.2. The first and second rows show which payment methods respondents want to use when purchasing privacy-sensitive products, while the third and fourth rows show respondents' choices of payment methods when purchasing privacy-insensitive products. For offline purchases, when CBDC is not available in the purchase of privacy-sensitive products, respondents choose cash (39.0%), credit and/or debit cards (34.2%), and mobile fast payment (8.4%) in order. Once CBDC is available, it is the most popular choice (30.0%), while the order of choice for the other payment methods remains the same. In the purchase of privacy-insensitive products, respondents choose credit and/or debit cards (46.5%), cash (13.6%), and mobile fast payment (12.7%) when CBDC is not available. Upon CBDC availability, respondents' choice of CBDC (27.3%) is next to their most preferred choice of credit and/or debit cards (31.3%). For online purchases, when CBDC is available, it is the most popular choice (42.0%) when purchasing privacy-sensitive products, and the second most popular choice (29.7%) when purchasing privacy-insensitive products (Table A3).

Table 1: Distribution of choosing payment methods in offline purchase

	(1)	(2)	(3)	(4)	(5)
	CBDC	Cash	Credit/Debit cards	Mobile fast payment	Don't care
CBDC is not available (Sensitive)		0.390	0.342	0.084	0.185
CBDC is available (Sensitive)	0.300	0.260	0.222	0.058	0.161
CBDC is not available (Insensitive)		0.136	0.465	0.127	0.272
CBDC is available (Insensitive)	0.273	0.090	0.313	0.075	0.250

Second, Table 2 shows the basic survey outcomes on respondents' knowledge about

CBDC and trust in public and private institutions regarding the protection of individual privacy rights. About 36% of the respondents have heard about CBDC and the lack of knowledge about CBDC is more prevalent in females and the age 19-29 group [column (1)].⁷ When it comes to trust in institutions, a substantial number of respondents express concerns over institutions potentially infringing on their individual privacy rights. In particular, the female and older age groups express more concerns than the male and younger age groups. Their concerns also vary with institutions [columns (2)-(4)]; the proportions of respondents who express concerns about financial institutions (67%) and BigTech companies (76%) are significantly higher than that about government (51%).

Table 2: Knowledge and trust in institutions

	(1)	(2)	(3)	(4)
	Heard about CBDC before	Concern about govt	Concern about FI	Concern about BigTech
All sample [3,514]	0.355	0.505	0.672	0.761
Male [1,727]	0.418	0.489	0.635	0.727
Female [1,787]	0.295	0.520	0.708	0.795
Age 19-29 [564]	0.257	0.330	0.573	0.667
Age 30-45 [925]	0.369	0.521	0.692	0.768
Age 46-59 [1,008]	0.361	0.563	0.726	0.794
Age above 60 [1,017]	0.392	0.530	0.655	0.776

Notes: The dependent variables are indicator variables equal to 1 in the following cases: *Heard about CBDC before*: a respondent has heard about CBDC before; *Concern about govt*: a respondent is concerned about government infringing privacy rights; *Concern about FI*: a respondent is concerned about financial institutions infringing privacy rights; *Concern about BigTech*: a respondent is concerned about BigTech companies infringing privacy rights. The number in brackets represents the number of respondents.

3 Conceptual Framework and Empirical Strategy

We provide a simple conceptual framework that is useful in understanding respondents' choice of CBDC as a means of payment in response to exposure to a randomly assigned treatment in this study. This leads us to state two hypotheses regarding the impacts of the degree of privacy protection of CBDC and information provision on the privacy benefits of using CBDC. We then proceed to empirical analysis to estimate the causal effects of the treatments.

⁷All the participants were also asked about their willingness to use CBDC after the survey experiments (and hence independent of the treatments that the respondents were subject to). About 81% answered in the positive. The respondents' choice to pay with CBDC (about 30% in Table 1) is the average of their choice to pay with CBDC in the survey experiments which allow for alternative payment methods (e.g., cash, credit and/or debit cards, mobile fast payment).

3.1 Conceptual Framework

We assume that an individual consumes goods or services q with expenditure m and chooses a means of payment $j \in \{\text{CBDC, cash, credit/debit cards, mobile fast payment}\}$. In general, utility from consumption $U(q)$ and expenditure m on goods or services purchased vary with their prices and quantities. In order to focus on how the choice of a payment method depends on its privacy attributes, we make a simplifying assumption that $U(q)$ and m are given as constant, regardless of the specific nature of the goods or services purchased. In addition to having utility from consumption net of expenditure $U(q) - m$, an individual i faces perceived costs of using a different means of payment. First, there is a cost of using cash, C_{ic} , including its carrying cost. Second, an individual i faces a potential cost due to loss of privacy by using a digital payment method such as CBDC, credit and/or debit cards, and mobile fast payment, $\eta(D_j)C_{ip}$ where C_{ip} is privacy cost and $\eta(\cdot) \geq 0$ with $\eta'(\cdot) < 0$ is a cost-adjusting parameter that depends on the degree of privacy protection of a payment method $D_j \in [0, 1]$. For instance, we assume $\eta(D_{cash}) = 0$ in that there is no loss of privacy by using anonymous cash. Privacy cost is discussed in [Kahn et al. \(2005\)](#) where the authors examine the role of cash in the provision of privacy. The use of cash leaves its user anonymous, whereas the use of credit requires the identification of its users and hence incurs privacy cost in the sense that they are exposed to the risk of identity theft. CBDC that is designed to enhance the privacy preservation of its users could have the effect of lowering privacy cost.

There is also a privacy benefit of using CBDC, $B_i > 0$, accrued by preventing private financial institutions and BigTech from accumulating and using the individual's personal information for commercial purposes. Furthermore, considering that the privacy benefit of using CBDC may not be immediately comprehensible to respondents, we introduce a parameter of the degree of attention on the privacy benefit $\theta(I)$ where I is an indicator variable equal to 1 when an individual receives information about the privacy benefit of using CBDC as a means of payment, and 0 otherwise. We assume that $\theta(1) > \theta(0) \geq 0$. The notion of a consumer's privacy benefit has been addressed in the recent literature. [Jones and Tonetti \(2020\)](#) discuss the benefit of data ownership by a consumer who can monetize transaction data by selling them to multiple organizations including financial institutions and BigTech. The selling price of consumers' transaction data reflects their perceived benefits from privacy in that it represents their valuation of privacy that makes them indifferent between selling and keeping it as privacy. The PCU feature of CBDC essentially gives its users ownership and control over transaction data, generating privacy benefits. Also, [Garratt and van Oordt \(2021\)](#) consider the costs associated with the use of privacy-enhancing electronic payment methods such as private cryptocurrencies. The use

of CBDC has privacy benefits in the sense that it provides a means of privacy-preserving payment at zero cost.

The utility function of an individual i , denoted V_i , is given as follows when consuming q with expenditure m using a means of payment $j \in \{\text{CBDC, cash, credit/debit cards, mobile fast payment}\}$ in offline transactions and $j \in \{\text{CBDC, credit/debit cards, mobile fast payment}\}$ in online transactions:

$$V_i = \begin{cases} U(q) - m - \eta(D_{CBDC}^k)C_{ip} + \theta(I)B_i & \text{if } j = \text{CBDC} \\ U(q) - m - C_{ic} & \text{if } j = \text{cash} \\ U(q) - m - \eta(D_{card})C_{ip} & \text{if } j = \text{credit/debit cards} \\ U(q) - m - \eta(D_{mobile})C_{ip} & \text{if } j = \text{mobile fast payment} \end{cases} \quad (3.1)$$

These utility functions differ in the costs and benefits associated with payment methods. With regard to CBDC, the value of parameter $\eta(D_{CBDC}^k)$, which captures the extent of privacy loss when using CBDC, varies across treatments concerning the degree of anonymity and privacy protection in CBDC design, denoted $k \in \{\text{CR, SR, Voucher}\}$. Because the Separate Repository (SR) or Voucher design preserves privacy more than the Combined Repository (CR), it is natural to assume that $\eta(D_{CBDC}^{SR})$ and $\eta(D_{CBDC}^{Voucher})$ are lower than $\eta(D_{CBDC}^{CR})$. Further, $\theta(I)B_i$ indicates the privacy benefit of using CBDC as explained above. When using cash, there is no loss of privacy, but instead there are carrying and transaction costs, denoted C_{ic} . Finally, concerning digital payment methods other than CBDC, the privacy cost of using credit and/or debit cards $\eta(D_{card})C_{ip}$ or mobile fast payment $\eta(D_{mobile})C_{ip}$ would have a different value from that of using CBDC $\eta(D_{CBDC}^k)C_{ip}$.

An individual i would be willing to use CBDC when the utility of using it is larger than that of using other means of payment. Thus, in offline transactions where cash is available, the individual would choose CBDC if

$$\eta(D_{CBDC}^k) \leq \min \left\{ \theta(I) \frac{B_i}{C_{ip}} + \frac{C_{ic}}{C_{ip}}, \theta(I) \frac{B_i}{C_{ip}} + \eta(D_{card}), \theta(I) \frac{B_i}{C_{ip}} + \eta(D_{mobile}) \right\} \quad (3.2)$$

and in online transactions where cash is not available, the individual would choose CBDC if

$$\eta(D_{CBDC}^k) \leq \min \left\{ \theta(I) \frac{B_i}{C_{ip}} + \eta(D_{card}), \theta(I) \frac{B_i}{C_{ip}} + \eta(D_{mobile}) \right\}. \quad (3.3)$$

We assume that the values of privacy costs and benefits, C_{ip} , C_{ic} , and B_i , are independently drawn from a joint probability distribution F across individuals. This distributional assumption leads us to discuss the relative ranking of the likelihood of choosing CBDC across

treatments.

The experimental variations regarding the degree of privacy protection in CBDC design and the provision of PCU information intend to change the parameter values of $\eta(D_{CBDC}^k)$ and $\theta(I)$ in conditions (3.2) and (3.3), and thus the likelihood of choosing CBDC as a preferred means of payment. We conjecture that the experimental variations are relevant in the situation of purchasing privacy-sensitive products, but irrelevant in the situation of purchasing privacy-insensitive products. Therefore, we state the following two hypotheses in the case of purchasing privacy-sensitive products.

Hypothesis 1 CBDC is more likely to be chosen as a means of payment in the Separate Repository (SR) or Voucher design of CBDC than in the Combined Repository (CR) design.

Hypothesis 2 CBDC is more likely to be chosen as a means of payment when individuals are informed of the privacy benefits of using CBDC in that it prevents financial institutions and BigTech companies from using their personal identity information and transaction data.

3.2 Empirical Strategy

We use the following regression specification to estimate the effects of treatments regarding privacy protection in the CBDC design and the provision of information about the privacy benefits of using CBDC on the choice of CBDC as a means of payment⁸

$$Y_i = \beta_0 + \sum_{k=1}^K \beta_k T_i^k + \gamma X_i + \epsilon_i \quad (3.4)$$

where Y_i denotes an outcome variable of interest for individual i . The main outcome variables are binary variables of whether to choose CBDC against other payment methods including cash, credit and/or debit cards, and mobile fast payments. Respondents are asked about their willingness to use CBDC against cash, credit and/or debit cards, and mobile fast payment in the offline purchasing situation and against credit and/or debit cards and mobile fast payment in the online buying situation. The same are asked for privacy-sensitive and privacy-insensitive products, respectively.

In the right-hand side of the regression, T_i^k is a binary indicator of the treatment group

⁸All the regressions are estimated using OLS for ease of interpretation, but basically the same results are obtained with binary logit models (online Appendix Table A5). In addition, we utilize a multinomial logit model to understand the substitution effects of each treatment on the willingness to use different payment methods (online Appendix Tables A6 ~ A11).

$k = 1, 2, \dots, K$ where K denotes the number of treatment groups, excluding the control group. In order to improve the statistical precision of the estimates of β_k 's, we consider a control vector X_i that includes individual socioeconomic characteristics such as gender, age, living in Seoul, marital status, education, employment status (all in dummy variables), and household income and wealth. It also includes an individual's privacy-related characteristics (e.g., privacy attitudes, knowledge of privacy, past behavior and experience with respect to privacy) and payment-related characteristics such as which payment method they usually use, whether they use mobile fast payment services, and where they usually make purchases (offline/online). Finally, a dummy variable is also included in the control vector, indicating whether a participant correctly solved the two quiz questions following the CBDC tutorial.⁹ Although our main specification includes all control variables, we also report and discuss results from regressions without control variables. For statistical inference, we use heteroskedasticity-robust standard errors.

4 Results

We report estimation results with emphasis on the average treatment effects of the different degrees of privacy preservation in the CBDC design and information about the potential privacy benefits of using CBDC on its choice as a means of payment. We also examine heterogeneous treatment effects on CBDC choice to understand who is more responsive to the privacy-preserving variations in CBDC design and the information provision of privacy benefits from the use of CBDC.

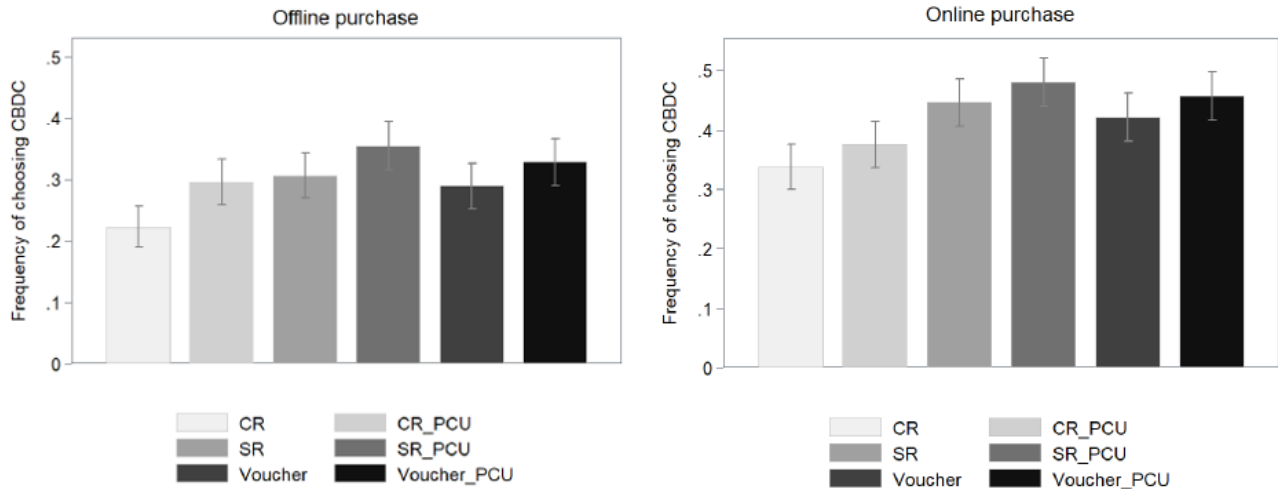
4.1 Average Treatment Effects

We begin with comparing the frequencies of choosing CBDC against other payment methods across treatments. Figure 3 presents the average frequencies of choosing CBDC in purchasing privacy-sensitive products offline (the left panel) and online (the right panel) across six treatment groups with 95 percent confidence intervals. Figure A1 in the Appendix reports corresponding figures for privacy-insensitive products offline and online.

For offline purchases, 22% of the respondents choose CBDC in the CR treatment group, 30% in the CR & PCU treatment group, 31% in the SR treatment group, 36% in the SR & PCU treatment group, 29% in the Voucher treatment group, and 33% in the Voucher & PCU treatment group. CBDC is expected to be chosen more frequently in online purchases because cash is not available. Indeed, 34% of the respondents choose CBDC in the CR

⁹The proportion of participants who solved the two questions correctly is 0.647.

Figure 3: Frequencies of choosing CBDC in purchasing privacy-sensitive products



Notes: Caps represent upper and lower bounds of the 95 percent confidence intervals.

group, 38% in the CR & PCU group, 45% in the SR group, 48% in the SR & PCU group, 42% in the Voucher group, and 46% in the Voucher & PCU group.

The empirical patterns shown in Figure 3 appear to be in line with the two hypotheses formulated in Section 3.1. Below we examine in detail how the SR and Voucher designs of CBDC affect its use as a means of payment relative to the CR design. We then investigate how the provision of PCU information about using CBDC affects its use as a means of payment. We also examine the combined effects of CR & PCU, SR & PCU, and Voucher & PCU treatments on the choice of CBDC as a means of payment.

Privacy Design of CBDC: We begin with examining the impact of the CBDC design variations with regard to privacy protection on the respondents' willingness to use CBDC in purchase behavior. In order to focus on the effects of the privacy-preserving variations in the CBDC design, we pool the data over the PCU variations.

Tables 3a and 3b report the regression results of estimating the average treatment effects of the privacy-preserving variations in the CBDC design on the choice of CBDC against other means of payment in purchasing privacy-sensitive and privacy-insensitive products, respectively. Columns (1)-(2) and (3)-(4) in each table report estimation results in the offline and online purchasing situation, respectively. Columns (1) and (3) are estimation results without the control vector X_i in the regression (3.4), whereas columns (2) and (4) are with the control vector X_i . The baseline treatment group is the Combined Repository (CR) group which consists of respondents assigned to the CR and CR & PCU treatments. While the controls improve the overall performance of the empirical model as

specified in (3.4), they have no notable impact on the average treatment effect estimates. This is to be expected given that the covariates are balanced due to randomization as reported in Table A1.

Table 3: Effects of the Privacy Design on CBDC Choice

(a) Privacy-sensitive goods				
	(1)	(2)	(3)	(4)
	Offline purchase		Online purchase	
SR	0.071***	0.075***	0.106***	0.105***
	(0.019)	(0.018)	(0.020)	(0.019)
Voucher	0.049***	0.050***	0.083***	0.082***
	(0.019)	(0.019)	(0.020)	(0.019)
Observations	3,514	3,514	3,514	3,514
R-squared	0.004	0.051	0.009	0.143
Base.Dep.Var.Mean	0.260	0.260	0.357	0.357
Socioeconomic	No	Yes	No	Yes
Privacy & Payment	No	Yes	No	Yes

(b) Privacy-insensitive goods				
	(1)	(2)	(3)	(4)
	Offline purchase		Online purchase	
SR	0.018	0.020	0.021	0.025
	(0.019)	(0.018)	(0.019)	(0.018)
Voucher	-0.003	-0.003	0.032*	0.031*
	(0.018)	(0.018)	(0.019)	(0.018)
Observations	3,514	3,514	3,514	3,514
R-squared	0.000	0.064	0.001	0.093
Base.Dep.Var.Mean	0.268	0.268	0.280	0.280
Socioeconomic	No	Yes	No	Yes
Privacy & Payment	No	Yes	No	Yes

Notes: The dependent variable is an indicator variable equal to 1 if a respondent chooses CBDC. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, and household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much respondents are concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much they value the right to privacy), knowledge of privacy, past behavior with respect to the protection of personal information, and past experience of personal information leakage. Payment-related control variables are where they usually buy products (offline/online), which payment method they usually use, whether they use mobile payment services, and whether they have experience with cryptocurrency. The control vector also includes whether they correctly solved the two quiz questions. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Firstly, in the purchase of privacy-sensitive products, the privacy-preserving variations in the CBDC design have significant effects on the willingness to use CBDC. Relative to the CR design, the SR design and the Voucher design increase the willingness to use CBDC as a means of payment by about 7.5 and 5 percentage points, respectively, when purchasing privacy-sensitive products offline. Considering that the frequency of using CBDC in the

baseline group is 0.26, these treatment effects respectively amount to a 29% and 19% increase in choosing CBDC in the offline purchase of privacy-sensitive products. The impact of the CBDC privacy design becomes somewhat larger in online purchases probably because cash is not available as an alternative means of payment.¹⁰ The SR design and the Voucher design raise the likelihood of choosing CBDC by about 10.5 and 8.2 percentage points respectively, amounting to a 29% and 23% increase relative to the baseline CR treatment. According to the conceptual framework behind respondents' choice of CBDC as laid out in Section 3.1, these results imply that loss of privacy when using CBDC, $\eta(D_{CBDC}^k)$, varies with the degrees of privacy preservation in the CBDC design $k \in \{\text{CR, SR, Voucher}\}$ such that $\eta(D_{CBDC}^{SR})$ and $\eta(D_{CBDC}^{Voucher})$ are significantly lower than $\eta(D_{CBDC}^{CR})$. These findings confirm Hypothesis 1 regarding the effects of the privacy-preserving variations in the CBDC design on the choice of CBDC as a means of payment. Secondly, in contrast to the purchase of privacy-sensitive products, Table 3b shows that for privacy-insensitive products, there are basically no significant effects of the privacy-preserving variations in the CBDC design on the use of CBDC as a means of payment in both offline and online purchasing scenarios.

In order to understand the substitution effects of the CBDC's various privacy protection treatments on the demands for different means of payment, we report multinomial logistic regression results of estimating the average marginal effects of each treatment on the willingness to use different payment methods, as shown in Tables A6 and A7, when purchasing privacy-sensitive and privacy-insensitive products, respectively. Specifically, when purchasing privacy-sensitive products offline, the SR treatment effect on the willingness to use CBDC, which exhibits a 7.6 percentage point increase (shown in Table A6a), is accompanied by decreases in the willingness to use cash and credit and/or debit cards by 4.4 and 3.4 percentage points, respectively. With the Voucher treatment, an increase in the willingness to use CBDC by 5 percentage points is accompanied by a decrease in the willingness to use cash by 3 percentage points. That is, an increase in the willingness to use CBDC due to either the SR or the Voucher privacy design crowds out the willingness to use cash more. The crowding-out effect of CBDC on cash can also be estimated by the decrease in the choice of cash payment before and after the availability of CBDC for each treatment group. Table A12 shows that in the CR group, the proportion of respondents choosing cash decreases by 26.6% (from 38.3 to 28.1 percentage points) with the availability of CBDC. In the SR and Voucher treatment groups, the availability of CBDC has the greater crowding-out effect on cash in that the choice of cash decreases by 38.3% and 34.9%, respectively.

¹⁰The coefficient of the treatment effect is statistically different between offline and online transactions at around the 10 percent significance level; that is, the χ^2 -statistics in the SR and Voucher design between offline and online transactions are 2.68 with a p -value of 0.101 and 2.97 with a p -value of 0.085, respectively.

In online purchases where cash is not available, the SR treatment effect on CBDC choice shows a 10.4 percentage point increase (as shown in Table A6b) and is accompanied by decreases in both the number of individuals using credit and/or debit cards by 4.9 percentage points, and by 4 percentage points for those indifferent about particular payment instruments. The Voucher treatment effect on CBDC choice, which results in an 8.1 percentage point increase, arises from decreases in the usage of both credit and/or debit cards and mobile fast payments by 4.2 and 3.1 percentage points, respectively. In short, an increase in the willingness to use CBDC due to its privacy treatments mostly substitutes away from cash and credit and/or debit cards. We do not find any significant substitution effects when purchasing privacy-insensitive products.

Information on Preventing Commercial Use: We next examine the impact of information about the potential privacy benefits of using CBDC because it can prevent private financial institutions and BigTech companies from using consumers’ personal identity information and transaction data for commercial purposes. Tables 4a and 4b report the regression results of estimating the average treatment effects of preventing commercial use (PCU) information on the choice of CBDC in purchasing privacy-sensitive and privacy-insensitive products. In Table 3, columns (1)-(2) and (3)-(4) in each table report estimation results for offline and online purchases, respectively. Columns (1) and (3) differ from columns (2) and (4) in the inclusion of the control variables in the regression.

Consistent with Hypothesis 2, the PCU information treatment has significant effects on respondents’ willingness to use CBDC against other means of payment in the scenario of purchasing privacy-sensitive goods. Providing PCU information on the privacy benefits of CBDC increases the likelihood of choosing CBDC by about 5.8 percentage points in offline purchases, amounting to a 21% increase relative to the use of CBDC in the baseline treatment without PCU information, and by about 3.9 percentage points in online purchases, amounting to a 10% increase relative to the baseline treatment without PCU information.¹¹ According to the conceptual framework of the respondents’ choice of CBDC as laid out in Section 3.1, these results imply that the privacy benefit of using CBDC due to PCU information, $\theta(I)B_i$, plays a significant role in the choice of CBDC as a means of payment for purchasing privacy-sensitive goods.

Furthermore, it is under the weak privacy conditions of CBDC, such as the CR treatment, that the PCU information treatment has a significant effect on the CBDC choice. Under the SR and Voucher conditions, the PCU treatment does not significantly add to the privacy of the consumer as shown in Table A13. This means that PCU information

¹¹We tested to see if the coefficient of treatment is different between offline and online transactions. The coefficient of PCU treatment does not differ significantly; the χ^2 -statistic was 1.59 with a p -value of 0.207.

Table 4: Effects of Preventing Commercial Use Information on CBDC Choice

(a) Privacy-sensitive goods				
	(1)	(2)	(3)	(4)
	Offline purchase		Online purchase	
PCU	0.053***	0.058***	0.036**	0.039**
	(0.015)	(0.015)	(0.017)	(0.016)
Observations	3,514	3,514	3,514	3,514
R-squared	0.003	0.050	0.001	0.136
Base.Dep.Var.Mean	0.273	0.273	0.402	0.402
Socioeconomic	No	Yes	No	Yes
Privacy & Payment	No	Yes	No	Yes

(b) Privacy-insensitive goods				
	(1)	(2)	(3)	(4)
	Offline purchase		Online purchase	
PCU	0.028*	0.027*	0.032**	0.029*
	(0.015)	(0.015)	(0.015)	(0.015)
Observations	3,514	3,514	3,514	3,514
R-squared	0.001	0.065	0.001	0.093
Base.Dep.Var.Mean	0.259	0.259	0.281	0.281
Socioeconomic	No	Yes	No	Yes
Privacy & Payment	No	Yes	No	Yes

Notes: The dependent variable is an indicator variable equal to 1 if a respondent chooses CBDC. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, and household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much respondents are concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much they value the right to privacy), knowledge of privacy, past behavior with respect to the protection of personal information, and past experience of personal information leakage. Payment-related control variables are where they usually buy products (offline/online), which payment method they usually use, whether they use mobile payment services, and whether they have experience with cryptocurrency. The control vector also includes whether they correctly solved the two quiz questions. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

has stronger effects on the CBDC choice when the privacy protection in the CBDC design is relatively weak. These results suggest that even if privacy is not well ensured in the CBDC design, the willingness to use CBDC could increase as long as people perceive the privacy benefits of CBDC compared to other payment methods.

In the scenario of purchasing privacy-insensitive products, the PCU treatment has weak effects on respondents' willingness to use CBDC. It increases the choice of CBDC by about 3 percentage points in both offline and online purchases. With the full set of controls, however, the effects of the PCU treatment are only significant at the 10% level.

In short, the average adoption of CBDC is higher for online purchases of privacy-sensitive products than for offline purchases as shown in Figure 3. The treatment effects

of CBDC's privacy attributes (i.e., SR, Voucher, PCU) are significant for both online and offline purchases as reported in Tables 3 and 4. In particular, the higher treatment effects for online purchases may not be surprising since our distinction between offline and online refers to the availability of cash as a means of payment for offline purchases only. It is worth noting that consumers' privacy here is not against the transaction party (e.g., the merchant), but against unknown third parties, which depends on the use of payment instruments. Hence, consumers are concerned about the type of privacy that is related to the payment method. Since cash is not available online as a payment instrument that protects privacy against third parties, the treatment effects of CBDC's privacy attributes are higher for online purchases.¹²

Tables A8 and A9 in the Appendix report the multinomial logistic regression results of estimating the average marginal effects of the PCU treatment on the choice of payment instruments. When purchasing privacy-sensitive products offline, the PCU treatment effect on the willingness to use CBDC (a 5.4 percentage point increase) is accompanied with decreases in both the number of individuals using cash by 2.3 percentage points and those indifferent about particular payment instruments by 2.2 percentage points. In the online purchases of privacy-sensitive products, the PCU treatment effect on CBDC demand (a 3.7 percentage point increase) is accompanied by a decrease in the number of individuals who are indifferent about particular payment methods by 2.4 percentage points.

Combined Treatment Effects: Because the survey experiment was implemented with the combination of privacy-preserving variations in the CBDC design (CR, SR, Voucher) and information on the privacy benefits of CBDC (PCU), we can also examine the combined effects of these experimental variations. Tables A4a and A4b in the online Appendix present the regression results where the CR treatment without the PCU information is set as a baseline treatment.¹³ As shown in Figure 3, 22.3% of the respondents in the offline purchasing situation and 33.8% in the online purchasing situation choose CBDC against other means of payment in this baseline treatment.

For privacy-sensitive products, most of the treatments have statistically significant effects. In offline purchases, compared to the baseline treatment, the likelihood of choosing CBDC is higher by about 7.5 percentage points in the CR & PCU treatment group (34% increase), 8.3 percentage points in the SR treatment group (37% increase), 14.2 percentage points in the SR & PCU treatment group (63% increase), 6.8 percentage points in

¹²In addition to online purchases which leave electronic trails with the merchant, offline purchases also generally leave trails with the merchant, regardless of the payment methods, i.e., electronic or cash. For instance, cash payment for visiting a doctor's office will leave a trail at the office. Hence, it is not whether trails are left behind with the merchant that distinguishes between online and offline purchases.

¹³Multinomial logistic regression results are presented in Tables A10 and A11 in online Appendix.

the Voucher treatment group (30% increase), and 10.6 percentage points in the Voucher & PCU treatment group (49 % increase). All the treatment effects are statistically significant at the 1% level. For online purchases, compared to the baseline treatment, CBDC is chosen more frequently by about 3.9 percentage points in the CR & PCU group (12% increase), 10 percentage points in the SR group (30% increase), 15 percentage points in the SR & PCU group (44% increase), 8.8 percentage points in the Voucher group (26% increase), and 11.6 percentage points in the Voucher & PCU group (36% increase). All the treatments except for the CR & PCU treatment have significant effects at the 1% level. These combined treatment effects corroborate the separate treatment effects reported in Tables 3a and 4a.

In contrast, most of the treatments have insignificant effects in the scenario of purchasing privacy-insensitive products. In the offline purchase scenario, relative to the CR treatment, the CR & PCU treatment and the SR & PCU treatment increase CBDC choice by 5.7 and 5.4 percentage points at the 5% and 10% levels, respectively. In the online purchase scenario, the SR & PCU treatment and the Voucher & PCU treatment raise the likelihood of the CBDC choice by 5.3 and 6 percentage points at the 5% significance level, respectively, which are overall consistent with the separate treatment effects reported in Tables 3b and 4b.

4.2 Heterogeneous Treatment Effects

We report the heterogeneity analysis of the treatment effects on CBDC choice across subgroups to understand who is more responsive to the privacy-preserving variations in the CBDC design and PCU information provision.

Privacy Concerns: We start by examining whether the treatment effects are different depending on the degree of respondents' privacy concern. We consider two different ways of categorizing the respondents. First, we divide the sample into two groups according to whether they choose to use cash when CBDC is not available when purchasing privacy-sensitive products. Respondents are asked this question just before being exposed to a randomly assigned treatment. Because using cash is the only way of preserving anonymity and protecting privacy in that situation, we assume that respondents who are more concerned about privacy are more likely to choose cash than other means of payment. Second, using the survey questions regarding respondents' general concern that their privacy rights might be violated by public (e.g. government) and private (e.g. financial institutions and BigTech companies) institutions, we divide the sample into these two groups. We compare treatment effects in each of the subgroups from the regression analysis with the full

set of controls.

Figure 4: Heterogeneous CBDC Design Treatment Effects for Privacy-Sensitive Products

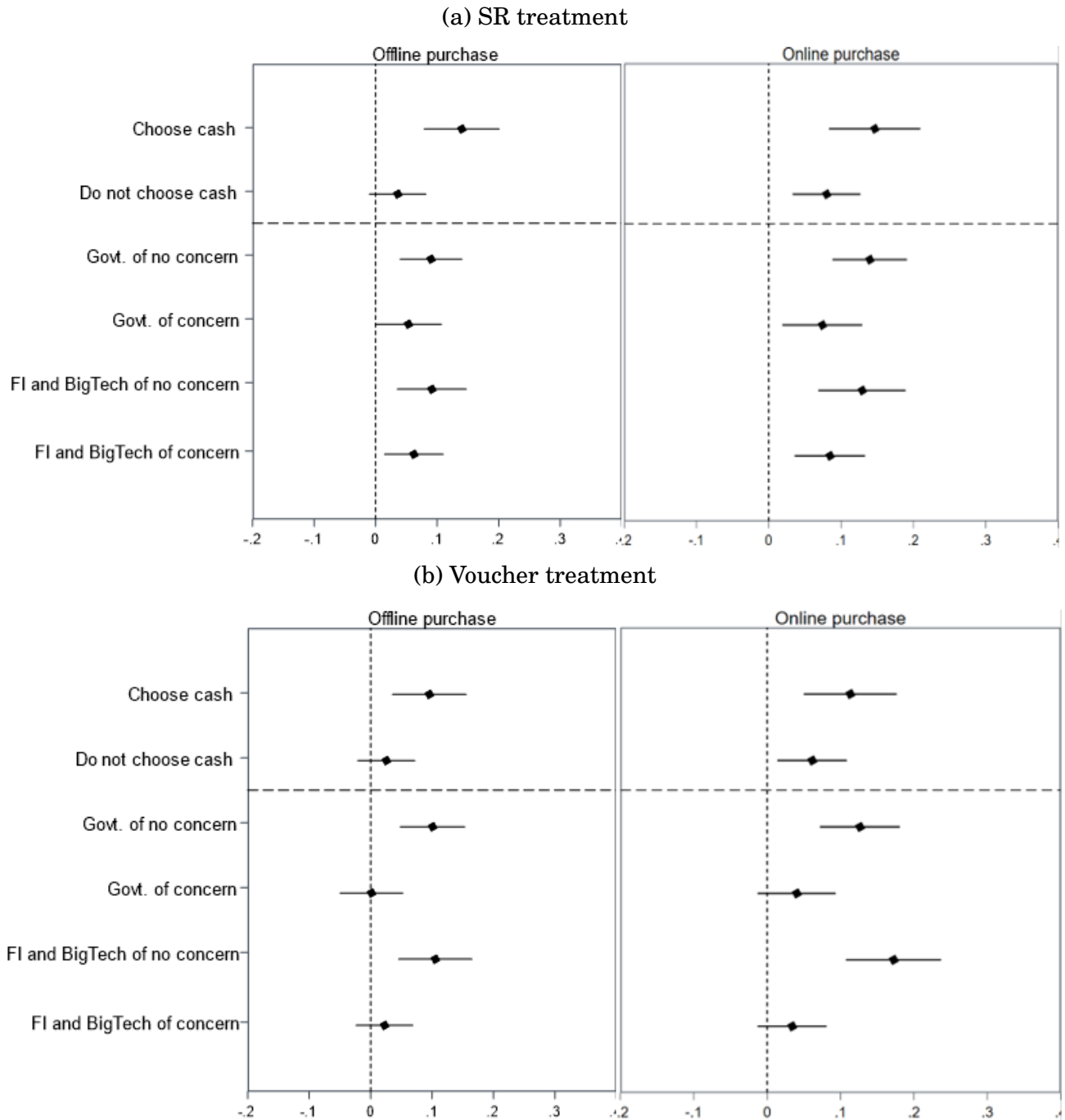


Figure 4 presents the heterogeneous treatment effects of the privacy-preserving CBDC designs between subgroups that differ in the choice of cash in the absence of CBDC. Respondents who choose cash when CBDC is not available are more responsive to the privacy-preserving treatment of the CBDC design. Specifically, as shown in Figure 4(a), for those who choose cash when CBDC is not available, the SR treatment increases the choice of

CBDC by about 14 and 14.6 percentage points in offline and online purchases, respectively. For those who do not choose cash when CBDC is unavailable, the SR treatment increases the use of CBDC by about 3.6 and 8 percentage points in offline and online purchases, respectively. We find the same patterns for the Voucher treatment as shown in Figure 4(b).

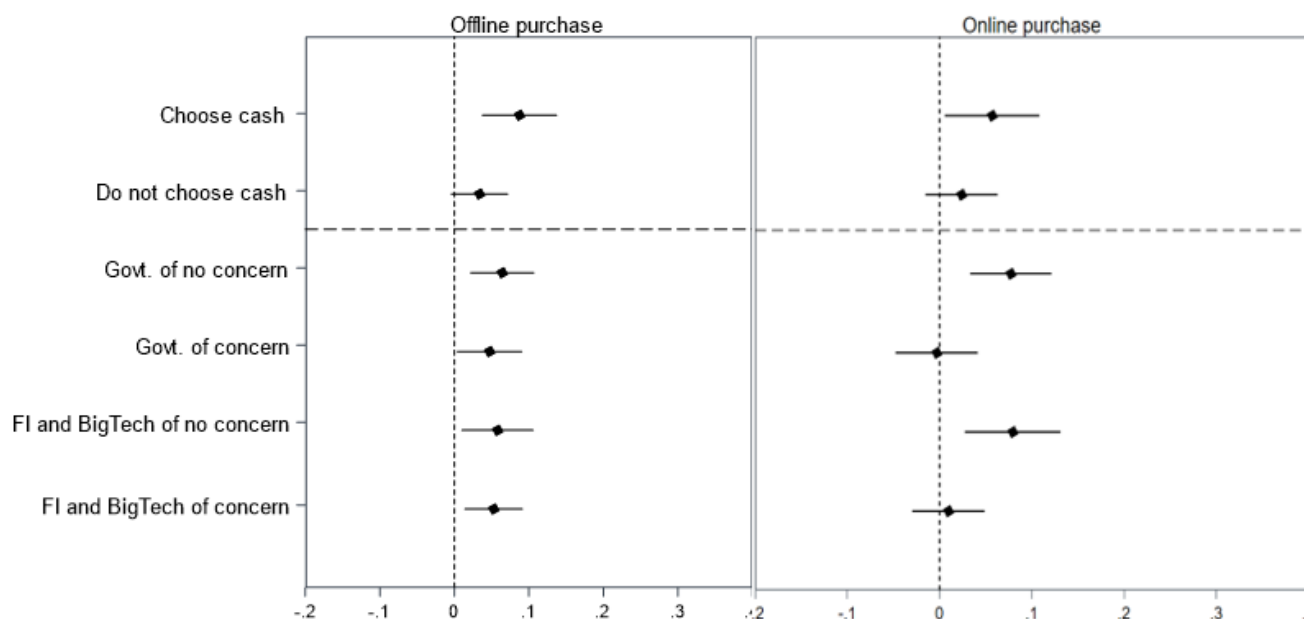
We turn to the second categorization of respondents based on their concern that individual privacy rights might be violated by the government, financial institutions, or BigTech companies. As shown in Figures 4(a) and (b), those who are not concerned about privacy violations by the government, financial institutions, or BigTech companies are more positively responsive to the SR and Voucher treatments than those who are concerned about privacy violations. The difference in treatment effects between these two groups appears to be larger in the Voucher treatment than in the SR treatment.

Next, Figure 5 shows the heterogeneous treatment effects of PCU information across subgroups regarding privacy concerns. While not as prominent as in the CBDC privacy design treatments, respondents who are not concerned about privacy violations by the government or private institutions are more responsive to the PCU treatment in online purchases. We do not see clear heterogeneous patterns in offline purchases.

In summary, the treatment effects of the privacy-preserving CBDC design are stronger for those who are more willing to use cash for privacy protection and for those who are not concerned about the possibility of privacy violations by the government or private institutions (e.g. financial institutions, BigTech companies). This suggests that the willingness to use CBDC by the public as a means of payment is likely to be related to their trust in the government or private institutions regarding privacy protection.

Socio-demographic Characteristics: We also examine whether the treatment effects are different depending on social and demographic factors. The results are presented in Tables A14 and A15 in the online Appendix. First, the female and unemployment groups are more responsive to the CBDC privacy design treatment and the PCU information provision treatment in both offline and online purchases. Second, different age groups show different responses to offline and online purchases. Older groups are more responsive to the treatments in offline purchases, whereas younger groups (especially between 20 and 29) are more responsive to the treatments in online purchases. These patterns seem to reflect the different frequency of offline and online purchases depending on age groups. Finally, the highly educated group with a college degree and lower wealth group are more responsive to the treatments.

Figure 5: Heterogeneous PCU Treatment Effects for Privacy-Sensitive Products



5 Concluding Remarks

Privacy protection has been regarded as the most important characteristic to consider in the issuance of CBDC. In this paper, we have designed and conducted a large-scale randomized online survey experiment to investigate the impact of CBDC design choices regarding the preservation of privacy on the willingness to use CBDC as a means of payment. The survey experiment also examines how the willingness to use CBDC is affected by information on the potential privacy benefits of using CBDC in the sense that it can prevent the commercial use of personal identity information and transaction data by financial institutions and BigTech companies.

We find that when privacy-sensitive products are purchased in both offline and online transactions, the willingness to use CBDC increases substantially when it is designed to preserve the privacy of its users by storing their personal identity information and transaction data separately in two different institutions and when the potential privacy benefits of using CBDC are informed. Our findings from the survey experiment with a nationally representative sample of over 3,500 participants provide useful insights into the specific features of CBDC concerning anonymity and privacy protection that can facilitate the choice of CBDC by the general public as a means of payment.

To the extent that our survey experiment reflects the main issues discussed in both policy circles around the world (e.g., Bank for International Settlement, European Central Bank, Bank of England) and the academic literature on the design choices of CBDC con-

cerning privacy protection and data governance, the results are relevant across countries which have considered introducing CBDC. However, some caution is required in generalizing our findings over time and across countries with different institutional settings and political climates. For instance, with regard to which institution is to safeguard personal data, trust in institutions varies with countries. According to a US survey ([Armantier et al., 2021](#)), American consumers have more trust in traditional financial institutions than government agencies and BigTech companies, whereas the respondents in our survey experiment show more trust in the government than financial institutions and BigTech companies.

Finally, our findings imply that as long as CBDC is designed to provide sufficient anonymity and protect privacy while meeting the AML and/or CFT regulations, it is more likely to substitute the existing payment instruments provided by the private sector, including commercial banks' demand deposits. This means that CBDC could enhance the public-good role of money in providing anonymity and protecting privacy in the digital age, but at the expense of credit intermediation. It would be interesting to investigate quantitatively how the degree of anonymity associated with using CBDC as a means of payment affects credit creation by banks, including the optimal degree of CBDC anonymity.

References

- Abramova, S., Böhme, R., Elsinger, H., Stix, H., and Summer, M. (2022). What can CBDC designers learn from asking potential users? Results from a survey of Austrian residents. *Oesterreichische Nationalbank Working Paper 241*.
- Acquisti, A., Brandmiarte, L., and Hancock, J. (2022). How privacy's past may shape its future. *Science*, 375(6578):270–272.
- Acquisti, A., Brandmiarte, L., and Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221):509–514.
- Acquisti, A. and Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy*, 3(1):26–33.
- Acquisti, A., John, L. K., and Loewenstein, G. (2013). What is privacy worth? *Journal of Legal Studies*, 42(2):249–274.
- Acquisti, A., Taylor, C., and Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2):442–492.
- Ahnert, T., Hoffmann, P., and Monnet, C. (2022). The Digital Economy, Privacy, and CBDC, European Central Bank, Working Paper Series No. 2662.
- Alvarez, F., Argente, D., and Van Patten, D. (2022). Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador, University of Chicago, Becker Friedman Institute for Economics Working Paper No. 2022-54.
- Armantier, O., Doerr, S., Fuster, A., and Shue, K. (2021). Whom do consumers trust with their data? us survey evidence. *BIS Bulletins 42*.
- Athey, S., Catalini, C., and Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk. *NBER Working Paper*.
- Bank for International Settlement (2021). CBDCs: an opportunity for the monetary system, Bank for International Settlement Annual Economic Report.
- Bank of England (2020). Central Bank Digital Currency: Opportunities, Challenges, and Designs, Bank of England Discussion Paper.
- Beutel, J., Metiu, N., and Stockerl, V. (2021). Toothless tiger with claws? financial stability communication, expectations, and risk-taking. *Journal of Monetary Economics*, 120:53–69.
- Bijlsma, M., van der Cruijssen, C., Jonker, N., and Reijerink, J. (2021). What triggers consumer adoption of CBDC? *De Nederlandsche Bank Working Paper 709*.

- Board of Governors of the Federal Reserve System (2022). Money and Payments: The U.S. Dollar in the Age of Digital Transformation, Research & Analysis.
- Borgonovo, E., Caselli, S., Cillo, A., Masciandaro, D., and Rabitti, G. (2021). Money, privacy, anonymity: What do experiments tell us? *Journal of Financial Stability*, 56:100934.
- Brouwer, N. and de Haan, J. (2022). The Impact of Providing Information about the ECB's Instruments on Inflation Expectations and Trust in the ECB: Experimental Evidence. *Journal of Macroeconomics*, 73.
- Camera, G. (2020). Introducing new forms of digital money: Evidence from the laboratory.
- Camera, G., Noussair, C., and Tucker, S. (2003). Rate-of-return dominance and efficiency in an experimental economy. *Economic Theory*, 22(3):629–660.
- Charness, G., G. U. and Kuhn, M. A. (2012). Experimental methods: Between-subject and within-subject design. *Journal of Economic Behavior and Organization*, 81:1–8.
- Choi, S., Kim, B., Kim, Y. S., Kwon, O., and Park, S. (2023). Predicting the Payment Preference for CBDC: A Survey Experiment Analysis, mimeo.
- Coibion, O., Gorodnichenko, Y., and Weber, M. (2021). Fiscal Policy and Households' Inflation Expectations: Evidence from a Randomized Control Trial, NBER Working Paper No. 28485.
- Coibion, O., Gorodnichenko, Y., and Weber, M. (2022). Monetary policy communications and their effects on household inflation expectations. *Journal of Political Economy*, 130(6):1537–1584.
- de Quidt, J., Haushofer, J., and Roth, C. (2018). Measuring and bounding experimenter demand. *American Economic Review*, 108(11):3266–3302.
- Dyson, B. and Hodgson, G. (2016). Why Central Banks Should Start Issuing Electronic Money, *Positive Money*.
- European Central Bank (2019). Exploring Anonymity in Central Bank Digital Currency. *In focus*, (4).
- European Central Bank (2021). ECB Digital Euro Consultation Ends with Record Level of Public Feedback, Press Release.
- Feri, F., Giannetti, C., and Jentzsch, N. (2016). Disclosure of personal information under risk of privacy shocks. *Journal of Economic Behavior and Organization*, 123:138–148.
- Fujiki, H. (2021). Attributes needed for Japan's central bank digital currency. *Japanese Economic Review*.

- Galati, G., Moessner, R., and van Rooij, M. (2022). Reactions of Household Inflation Expectations to a Symmetric Inflation Target and High Inflation, De Nederlandsche Bank, Working Paper No. 743.
- 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.
- Gellman, R. (2002). Privacy, Consumers, and Costs - How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete, The Digital Media Forum, Washington, D.C.
- Goldfarb, A. and Tucker, C. E. (2012). Shifts in privacy concerns. *American Economic Review: Papers & Proceedings*, 102(3):349–353.
- Grosse-Steffen, C. (2021). Anchoring of Inflation Expectation: Do Inflation Target Formulations Matter?, Banque de France, Working Paper No. 852.
- Huynh, K., Molnar, J., Shcherbakov, O., and Yu, Q. (2020). Demand for payment services and consumer welfare: The introduction of a central bank digital currency, Staff Working Papers 20-7, Bank of Canada.
- Javelin (2022). 2022 identity fraud study: The virtual battleground, Press Release.
- Jiang, J. (2020). CBDC adoption and usage: some insights from field and laboratory experiments, Bank of Canada Staff Analytical Note 2020-12.
- Jones, C. I. and Tonetti, C. (2020). Nonrivalry and the economics of data. *American Economic Review*, 110(9):2819–58.
- Kahn, C. M. (2018). Payment Systems and Privacy. *Federal Reserve Bank of St. Louis Review*, 100(4):337–344.
- Kahn, C. M., McAndrews, J., and Roberds, W. (2005). Money Is Privacy. *International Economic Review*, 46(2):377–399.
- Kim, Y. S. and Kwon, O. (2022). Central Bank Digital Currency, Credit Supply, and Financial Stability. *Journal of Money, Credit and Banking*, Forthcoming.
- Korea Information Society Development Institute (2020). The Korean Media Panel Survey.
- Li, J. (2022). Predicting the demand for central bank digital currency: A structural analysis with survey data, Staff Working Papers 21-65, Bank of Canada.
- Marreiros, H., Tonin, M., Vlassopoulos, M., and Schraefel, M. (2017). Now that you mention it: A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior and Organization*, 140:1–17.

- Pew Research Center (2014). Public Perceptions of Privacy and Security in the Post-Snowden Era, Press Release.
- Pew Research Center (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over their Personal Information, Press Release.
- Phelps, J., Nowak, G., and Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1):27–41.
- Prince, J. T. and Wallsten, S. (2022). How much is privacy worth around the world and across platforms? *Journal of Economics & Management Strategy*, 31(4):841–861.
- Skingsley, C. (2016). Should the Riksbank Issue e-krona?, Speech at FinTech Stockholm.
- Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2):254–268.

Appendices

A Tables and Figures

Table A1: Sample Characteristics and Balance Checks

	(1) All sample	(2) CR (Control Group)	(3) CR & PCU	(4) SR	(5) SR & PCU	(6) Voucher	(7) Voucher & PCU	Prob >F
Female	0.509	0.505 (0.021)	0.015 (0.029)	-0.005 (0.029)	0.008 (0.029)	0.004 (0.029)	-0.002 (0.029)	0.987
Age								
19~29	0.161	0.160 (0.015)	0.001 (0.021)	-0.012 (0.021)	0.016 (0.022)	-0.006 (0.021)	0.001 (0.021)	0.882
30~45	0.263	0.267 (0.018)	0.001 (0.026)	-0.008 (0.026)	-0.016 (0.025)	0.003 (0.026)	-0.002 (0.026)	0.975
46~59	0.287	0.287 (0.020)	-0.004 (0.026)	0.015 (0.027)	0.000 (0.026)	-0.010 (0.026)	-0.003 (0.026)	0.963
Above 60	0.289	0.285 (0.019)	0.003 (0.026)	0.005 (0.027)	0.000 (0.026)	0.012 (0.027)	0.004 (0.026)	0.998
Living in Seoul	0.179	0.181 (0.016)	0.002 (0.022)	-0.002 (0.023)	-0.005 (0.022)	-0.005 (0.022)	0.000 (0.022)	0.999
Married	0.616	0.615 (0.020)	-0.006 (0.028)	0.008 (0.029)	-0.026 (0.028)	0.019 (0.028)	0.016 (0.028)	0.646
Education								
Above College degree	0.470	0.476 (0.021)	0.012 (0.029)	-0.001 (0.029)	-0.008 (0.029)	-0.024 (0.029)	-0.015 (0.029)	0.870
Employment								
Employed	0.499	0.522 (0.021)	-0.044 (0.029)	-0.029 (0.029)	-0.043 (0.029)	-0.011 (0.029)	-0.010 (0.029)	0.539
Self-employed	0.101	0.098 (0.012)	0.004 (0.017)	0.000 (0.017)	0.002 (0.017)	-0.005 (0.017)	0.018 (0.018)	0.875
Not-employed	0.400	0.380 (0.020)	0.040 (0.029)	0.029 (0.029)	0.041 (0.028)	0.016 (0.028)	-0.008 (0.028)	0.388
Income								
Below 3 mil	0.381	0.385 (0.020)	-0.007 (0.028)	-0.006 (0.029)	-0.013 (0.028)	0.012 (0.029)	-0.009 (0.028)	0.963
3 mil – 5 mil	0.324	0.336 (0.020)	-0.023 (0.027)	-0.018 (0.028)	0.016 (0.028)	-0.042 (0.027)	-0.006 (0.027)	0.375
Above 5 mil	0.295	0.279 (0.018)	0.030 (0.027)	0.024 (0.027)	-0.003 (0.026)	0.029 (0.027)	0.016 (0.026)	0.704
Wealth								
Below 50 mil	0.334	0.360 (0.020)	-0.041 (0.028)	-0.010 (0.028)	-0.018 (0.028)	-0.059*** (0.027)	-0.028 (0.028)	0.298
50 mil-300 mil	0.386	0.383 (0.020)	0.023 (0.028)	-0.037 (0.028)	-0.008 (0.028)	0.035 (0.029)	0.001 (0.028)	0.166
Above 300 mil	0.280	0.257 (0.018)	0.018 (0.026)	0.047** (0.026)	0.026 (0.026)	0.024 (0.026)	0.027 (0.026)	0.638
# of obs.	3514	592	591	590	572	581	588	

Notes: In columns (3)-(7), Mean differences between Treatment Groups and Control Group are reported. Heteroskedacity-robust standard errors are reported in parantheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table A2: Sample Characteristics

	This Survey	South Korea population
Female	0.51	0.50
Age		
19~29	0.16	0.15
30~45	0.26	0.25
46~59	0.29	0.30
Above 60	0.29	0.30
Living in Seoul	0.18	0.18
Married	0.62	0.60
Education		
Above College degree	0.47	0.47
Employment		
Employed	0.50	0.40
Self-employed	0.10	0.15
Not-employed	0.40	0.45

Notes: This table displays statistics for the overall South Korea population and compares it to the characteristics of the sample of surveys. National statics on gender, age, place of residence are from the South Korea Demographic Statistics December 2021. Marriage, education are from the South Korea Population Census 2015, and Employment is from the 2019 Korea Labor Income Panel Study(KLIPS).

Table A3: Distribution of choosing payment methods in online purchase

	(1)	(2)	(3)	(4)
	CBDC	Credit/Debit cards	Mobile fast payment	Don't care
CBDC is available (Sensitive)	0.420	0.280	0.098	0.202
CBDC is available (Insensitive)	0.297	0.318	0.108	0.277

Table A4: Combined Effects on CBDC Choice

(a) Privacy-sensitive goods

	(1)	(2)	(3)	(4)
	Offline purchase		Online purchase	
CR & PCU	0.073*** (0.025)	0.075*** (0.025)	0.038 (0.028)	0.039 (0.027)
SR	0.084*** (0.026)	0.083*** (0.025)	0.108*** (0.028)	0.100*** (0.027)
SR & PCU	0.132*** (0.026)	0.142*** (0.026)	0.143*** (0.029)	0.150*** (0.027)
Voucher	0.066*** (0.025)	0.068*** (0.026)	0.084*** (0.028)	0.088*** (0.027)
Voucher & PCU	0.105*** (0.026)	0.106*** (0.026)	0.120*** (0.028)	0.116*** (0.027)
Observations	3,514	3,514	3,514	3,514
R-squared	0.008	0.055	0.010	0.145
Base.Dep.Var.Mean	0.223	0.223	0.338	0.338
Socioeconomic	No	Yes	No	Yes
Payment	No	Yes	No	Yes

(b) Privacy-insensitive goods

	(1)	(2)	(3)	(4)
	Offline purchase		Online purchase	
CR & PCU	0.056** (0.026)	0.057** (0.025)	0.029 (0.026)	0.027 (0.025)
SR	0.042 (0.026)	0.043 (0.025)	0.020 (0.026)	0.025 (0.025)
SR & PCU	0.050* (0.026)	0.054** (0.025)	0.053** (0.027)	0.053** (0.026)
Voucher	0.017 (0.025)	0.018 (0.025)	0.029 (0.026)	0.028 (0.025)
Voucher & PCU	0.034 (0.025)	0.032 (0.025)	0.063** (0.027)	0.060** (0.026)
Observations	3,514	3,514	3,514	3,514
R-squared	0.002	0.066	0.002	0.094
Base.Dep.Var.Mean	0.240	0.240	0.265	0.265
Socioeconomic	No	Yes	No	Yes
Privacy & Payment	No	Yes	No	Yes

Notes: The dependent variable is an indicator variable equal to 1 if a respondent chooses CBDC. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. The control vector also includes whether she solved correctly the two quiz questions on CBDC. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table A5: Logit model: Marginal Effects of the Privacy Design on CBDC Choice

(a) privacy-sensitive goods

	(1)	(2)
	Offline purchase	Online purchase
CR & PCU	0.082*** (0.030)	0.038 (0.028)
SR	0.091*** (0.029)	0.101*** (0.028)
SR & PCU	0.152*** (0.030)	0.149*** (0.027)
Voucher	0.076*** (0.030)	0.089*** (0.028)
Voucher & PCU	0.115*** (0.030)	0.116*** (0.028)
Observations	3,514	3,514
Pseudo R-squared	0.032	0.089
Base.Dep.Var.Mean	0.223	0.338
Socioeconomic	Yes	Yes
Privacy & Payment	Yes	Yes

(b) privacy-insensitive goods

	(1)	(2)
	Offline purchase	Online purchase
CR & PCU	0.058** (0.026)	0.026 (0.027)
SR	0.043 (0.027)	0.025 (0.026)
SR & PCU	0.054* (0.028)	0.052* (0.028)
Voucher	0.019 (0.027)	0.029 (0.027)
Voucher & PCU	0.033 (0.015)	0.060* (0.016)
Observations	3,514	3,514
Pseudo R-squared	0.045	0.068
Base.Dep.Var.Mean	0.240	0.265
Socioeconomic	Yes	Yes
Privacy & Payment	Yes	Yes

Notes: Average marginal effects are calculated for discrete changes from zero to one. The dependent variable is an indicator variable equal to 1 if a respondent chooses CBDC. Heteroskedasticity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. The control vector also includes whether she solved correctly the two quiz questions on CBDC. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table A6: Multinomial logit model: Marginal Effects of the Privacy Design on Payment Choice for Privacy-Sensitive Products

(a) Offline purchase

	(1)	(2)	(3)	(4)	(5)
	CBDC	Cash	Credit/Debit cards	Mobile fast payments	Don't care
SR	0.076*** (0.019)	-0.044*** (0.014)	-0.034** (0.016)	0.012 (0.009)	-0.011 (0.014)
Voucher	0.050*** (0.018)	-0.030** (0.014)	-0.017 (0.016)	0.002 (0.009)	-0.005 (0.014)
Observations	3,514	3,514	3,514	3,514	3,514
Base.Dep.Var.Mean	0.260	0.281	0.240	0.053	0.167
Socioeconomic	Yes	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes	Yes

(b) Online purchase

	(1)	(2)	(3)	(4)
	CBDC	Credit/Debit cards	Mobile fast payments	Don't care
SR	0.104*** (0.019)	-0.049*** (0.018)	-0.015 (0.012)	-0.040** (0.016)
Voucher	0.081*** (0.019)	-0.042** (0.018)	-0.031** (0.012)	-0.008 (0.017)
Observations	3,514	3,514	3,514	3,514
Base.Dep.Var.Mean	0.357	0.311	0.112	0.220
Socioeconomic	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes

Notes: Average marginal effects are calculated for discrete changes from zero to one in the treatment. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. The control vector also includes whether she solved correctly the two quiz questions on CBDC. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table A7: Multinomial logit model: Marginal Effects of the Privacy Design on Payment Choice for Privacy-Insensitive Products

(a) Offline purchase

	(1)	(2)	(3)	(4)	(5)
	CBDC	Cash	Credit/Debit cards	Mobile fast payments	Don't care
SR	0.019 (0.018)	0.003 (0.009)	-0.009 (0.019)	0.003 (0.010)	-0.016 (0.017)
Voucher	-0.005 (0.018)	0.005 (0.009)	0.004 (0.019)	-0.001 (0.010)	-0.003 (0.017)
Observations	3,514	3,514	3,514	3,514	3,514
Base.Dep.Var.Mean	0.268	0.088	0.313	0.074	0.257
Socioeconomic	Yes	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes	Yes

(b) Online purchase

	(1)	(2)	(3)	(4)
	CBDC	Credit/Debit cards	Mobile fast payments	Don't care
SR	0.025 (0.018)	-0.019 (0.019)	0.005 (0.124)	-0.011 (0.018)
Voucher	0.030 (0.018)	-0.017 (0.019)	-0.006 (0.012)	-0.008 (0.018)
Observations	3,514	3,514	3,514	3,514
Base.Dep.Var.Mean	0.280	0.329	0.110	0.283
Socioeconomic	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes

Notes: Average marginal effects are calculated for discrete changes from zero to one in the treatment. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. The control vector also includes whether she solved correctly the two quiz questions on CBDC. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table A8: Multinomial logit model: Marginal Effects of Preventing Commercial Use Information on Payment Choice for Privacy-Sensitive Products

(a) Offline purchase

	(1)	(2)	(3)	(4)	(5)
	CBDC	Cash	Credit/Debit cards	Mobile fast payments	Don't care
PCU	0.054*** (0.015)	-0.023** (0.012)	-0.008 (0.013)	-0.009 (0.008)	-0.022* (0.012)
Observations	3,514	3,514	3,514	3,514	3,514
Base.Dep.Var.Mean	0.273	0.268	0.223	0.058	0.173
Socioeconomic	Yes	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes	Yes

(b) Online purchase

	(1)	(2)	(3)	(4)
	CBDC	Credit/Debit cards	Mobile fast payments	Don't care
PCU	0.037** (0.016)	-0.006 (0.015)	-0.007 (0.010)	-0.024* (0.013)
Observations	3,514	3,514	3,514	3,514
Base.Dep.Var.Mean	0.402	0.282	0.102	0.215
Socioeconomic	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes

Notes: Average marginal effects are calculated for discrete changes from zero to one in the treatment. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. The control vector also includes whether she solved correctly the two quiz questions on CBDC. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table A9: Multinomial logit model: Marginal Effects of Preventing Commercial Use Information on Payment Choice for Privacy-Insensitive Products

(a) Offline purchase

	(1)	(2)	(3)	(4)	(5)
	CBDC	Cash	Credit/Debit cards	Mobile fast payments	Don't care
PCU	0.026*	0.006	0.000	-0.004	-0.027**
	(0.015)	(0.008)	(0.015)	(0.009)	(0.014)
Observations	3,514	3,514	3,514	3,514	3,514
Base.Dep.Var.Mean	0.259	0.085	0.313	0.2077	0.266
Socioeconomic	Yes	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes	Yes

(b) Online purchase

	(1)	(2)	(3)	(4)
	CBDC	Credit/Debit cards	Mobile fast payments	Don't care
PCU	0.027*	-0.000	0.013	-0.040***
	(0.015)	(0.015)	(0.010)	(0.015)
Observations	3,514	3,514	3,514	3,514
Base.Dep.Var.Mean	0.281	0.318	0.102	0.299
Socioeconomic	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes

Notes: Average marginal effects are calculated for discrete changes from zero to one in the treatment. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. The control vector also includes whether she solved correctly the two quiz questions on CBDC. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table A10: Multinomial logit model: Marginal Effects of the Treatments on Payment Choice for Privacy-Sensitive Products

(a) Offline purchase

	(1)	(2)	(3)	(4)	(5)
	CBDC	Cash	Credit/Debit cards	Mobile fast payments	Don't care
CR & PCU	0.076*** (0.027)	-0.047** (0.020)	-0.027 (0.022)	-0.004 (0.014)	0.003 (0.020)
SR	0.090*** (0.027)	-0.061*** (0.020)	-0.037* (0.022)	0.013 (0.013)	-0.005 (0.020)
SR & PCU	0.142*** (0.026)	-0.075*** (0.020)	-0.059*** (0.023)	0.006 (0.013)	-0.015 (0.020)
Voucher	0.073*** (0.027)	-0.050** (0.021)	-0.043* (0.022)	-0.005 (0.014)	0.024 (0.020)
Voucher & PCU	0.110*** (0.027)	-0.058*** (0.020)	-0.017 (0.022)	0.004 (0.013)	-0.038* (0.021)
Observations	3,514	3,514	3,515	3,514	3,514
Base.Dep.Var.Mean	0.223	0.301	0.257	0.056	0.164
Socioeconomic	Yes	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes	Yes

(b) Online purchase

	(1)	(2)	(3)	(4)
	CBDC	Credit/Debit cards	Mobile fast payments	Don't care
CR & PCU	0.038 (0.028)	-0.024 (0.025)	-0.076 (0.016)	-0.006 (0.022)
SR	0.100*** (0.027)	-0.042* (0.025)	-0.018 (0.016)	-0.041* (0.023)
SR & PCU	0.147*** (0.027)	-0.080*** (0.026)	-0.019 (0.016)	-0.048** (0.023)
Voucher	0.089*** (0.028)	-0.076*** (0.025)	-0.029* (0.017)	0.015 (0.022)
Voucher & PCU	0.115*** (0.027)	-0.032 (0.025)	-0.040** (0.017)	-0.043** (0.023)
Observations	3,514	3,514	3,515	3,514
Base.Dep.Var.Mean	0.338	0.323	0.118	0.221
Socioeconomic	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes

Notes: Average marginal effects are calculated for discrete changes from zero to one in the treatment. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. The control vector also includes whether she solved correctly the two quiz questions on CBDC. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table A11: Multinomial logit model: Marginal Effects of the Treatments on Payment Choice for Privacy-Insensitive Products

(a) Offline purchase

	(1)	(2)	(3)	(4)	(5)
	CBDC	Cash	Credit/Debit cards	Mobile fast payments	Don't care
CR & PCU	0.053**	0.010	-0.026	-0.006	-0.031
	(0.025)	(0.013)	(0.026)	(0.015)	(0.024)
SR	0.042	0.008	-0.031	0.006	-0.026
	(0.026)	(0.013)	(0.026)	(0.014)	(0.024)
SR & PCU	0.050*	0.009	-0.014	-0.008	-0.037
	(0.026)	(0.013)	(0.026)	(0.015)	(0.025)
Voucher	0.015	0.006	-0.013	-0.009	0.001
	(0.026)	(0.013)	(0.026)	(0.015)	(0.024)
Voucher & PCU	0.030	0.013	-0.005	0.001	-0.039
	(0.026)	(0.013)	(0.026)	(0.014)	(0.024)
Observations	3,514	3,514	3,515	3,514	3,514
Base.Dep.Var.Mean	0.240	0.081	0.328	0.079	0.272
Socioeconomic	Yes	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes	Yes

(b) Online purchase

	(1)	(2)	(3)	(4)
	CBDC	Credit/Debit cards	Mobile fast payments	Don't care
CR & PCU	0.053**	0.010	-0.026	-0.006
	(0.025)	(0.013)	(0.026)	(0.015)
SR	0.042	0.008	-0.031	0.006
	(0.026)	(0.013)	(0.026)	(0.014)
SR & PCU	0.050**	0.009	-0.014	-0.008
	(0.026)	(0.013)	(0.026)	(0.015)
Voucher	0.015	0.006	-0.013	-0.009
	(0.026)	(0.013)	(0.026)	(0.015)
Voucher & PCU	0.030	0.013	-0.005	0.001
	(0.026)	(0.013)	(0.026)	(0.014)
Observations	3,514	3,514	3,515	3,514
Base.Dep.Var.Mean	0.265	0.335	0.112	0.289
Socioeconomic	Yes	Yes	Yes	Yes
Privacy & Payment	Yes	Yes	Yes	Yes

Notes: Average marginal effects are calculated for discrete changes from zero to one in the treatment. Heteroskedasticity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. The control vector also includes whether she solved correctly the two quiz questions on CBDC. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table A12: Distribution of Payment Choice for Offline Privacy-Sensitive Products by Privacy Design Treatment Groups

		(1)	(2)	(3)	(4)	(5)
		CBDC	Cash	Credit/Debit cards	Mobile fast payment	Don't care
CR	CBDC is not available		0.383	0.344	0.085	0.189
	CBDC is available	0.260	0.281	0.240	0.053	0.167
SR	CBDC is not available		0.392	0.332	0.090	0.186
	CBDC is available	0.331	0.242	0.203	0.067	0.158
Voucher	CBDC is not available		0.393	0.349	0.078	0.180
	CBDC is available	0.301	0.256	0.223	0.054	0.158

Table A13: Effects of Preventing Commercial Use Information on CBDC Choice

(a) CR design				
	(1)	(2)	(3)	(4)
	Offline purchase		Online purchase	
PCU	0.073***	0.078***	0.038	0.039
	(0.025)	(0.025)	(0.028)	(0.027)
Observations	1,183	1,183	1,183	1,183
R-squared	0.007	0.035	0.002	0.126
Base.Dep.Var.Mean	0.223	0.223	0.338	0.338
Socioeconomic	No	Yes	No	Yes
Payment	No	Yes	No	Yes

(b) SR design				
	(1)	(2)	(3)	(4)
	Offline purchase		Online purchase	
PCU	0.048*	0.055**	0.035	0.048
	(0.027)	(0.027)	(0.029)	(0.028)
Observations	1,162	1,162	1,162	1,162
R-squared	0.003	0.073	0.001	0.149
Base.Dep.Var.Mean	0.307	0.307	0.446	0.446
Socioeconomic	No	Yes	No	Yes
Privacy & Payment	No	Yes	No	Yes

(c) Voucher design				
	(1)	(2)	(3)	(4)
	Offline purchase		Online purchase	
PCU	0.039	0.035	0.036	0.024
	(0.027)	(0.027)	(0.029)	(0.028)
Observations	1,169	1,169	1,169	1,169
R-squared	0.002	0.046	0.001	0.126
Base.Dep.Var.Mean	0.289	0.289	0.421	0.421
Socioeconomic	No	Yes	No	Yes
Privacy & Payment	No	Yes	No	Yes

Notes: The dependent variable is an indicator variable equal to 1 if a respondent chooses CBDC. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. The control vector also includes whether she solved correctly the two quiz questions on CBDC. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table A14: Heterogeneous CBDC Design Treatment Effects for Privacy-Sensitive Products

(a) Offline purchase

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Male	Female	19-29	30-45	46-59	Above 60	No college degree	College degree	Employed	Not employed	Low wealth	High wealth
SR	0.0395 (0.0271)	0.106*** (0.0257)	0.0576 (0.0476)	0.0469 (0.0371)	0.0885** (0.0351)	0.0984*** (0.0360)	0.0497** (0.0250)	0.0103*** (0.0281)	0.0500* (0.0269)	0.122*** (0.0289)	0.0252 (0.0262)	0.120*** (0.0266)
Voucher	0.0111 (0.0270)	0.0934*** (0.0260)	0.127*** (0.0480)	0.0129 (0.0366)	0.0968*** (0.0359)	0.00465*** (0.0350)	0.0518** (0.0253)	0.0470* (0.0279)	0.0533** (0.0270)	0.0654** (0.0290)	0.0164 (0.0266)	0.0825*** (0.0265)
Base.Dep.Var.Mean	0.289	0.231	0.231	0.275	0.244	0.278	0.244	0.277	0.274	0.224	0.262	0.257
Observations	1727	1787	564	925	1008	1017	1861	1653	1754	1405	1792	1722

(b) Online purchase

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Male	Female	19-29	30-45	46-59	Above 60	No college degree	College degree	Employed	Not employed	Low wealth	High wealth
SR	0.0831*** (0.0284)	0.130*** (0.0277)	0.170*** (0.0478)	0.118*** (0.0387)	0.0570 (0.0379)	0.118*** (0.0375)	0.0966*** (0.0272)	0.116*** (0.0292)	0.0620** (0.0282)	0.182*** (0.0308)	0.101*** (0.0281)	0.108*** (0.0282)
Voucher	0.0126 (0.0285)	0.161*** (0.0278)	0.297*** (0.0480)	0.0463 (0.0382)	0.0487 (0.0382)	0.0547 (0.0379)	0.0749*** (0.0272)	0.0916*** (0.0297)	0.0509* (0.0282)	0.150*** (0.0316)	0.0695** (0.0285)	0.103*** (0.0283)
Base.Dep.Var.Mean	0.387	0.327	0.256	0.346	0.400	0.382	0.322	0.395	0.392	0.293	0.332	0.382
Observations	1727	1787	564	925	1008	1017	1861	1653	1754	1405	1792	1722

Table A15: Heterogeneous PCU Treatment Effects for Privacy-Sensitive Products

(a) Offline purchase

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Male	Female	19-29	30-45	46-59	Above 60	No college degree	College degree	Employed	Not employed	Low wealth	High wealth
PCU	0.0478** (0.0221)	0.0611*** (0.0215)	0.0486 (0.0390)	0.0505 (0.0309)	0.112*** (0.0288)	0.0048 (0.0291)	0.0372* (0.0206)	0.0727*** (0.0232)	0.0726*** (0.0221)	0.0432* (0.0240)	0.0609*** (0.0215)	0.0509** (0.0222)
Base.Dep.Var.Mean	0.279	0.267	0.261	0.271	0.247	0.307	0.256	0.292	0.273	0.263	0.249	0.296
Observations	1727	1787	564	925	1008	1017	1861	1653	1754	1405	1792	1722

(b) Online purchase

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	Male	Female	19-29	30-45	46-59	Above 60	No college degree	College degree	Employed	Not employed	Low wealth	High wealth
PCU	0.00256 (0.0234)	0.0716*** (0.0230)	0.00724 (0.0411)	0.0456 (0.0324)	0.0732** (0.0305)	0.0278 (0.0311)	0.0558** (0.0222)	0.0210 (0.0243)	0.0417* (0.0233)	0.0382 (0.0259)	0.00149 (0.0233)	0.0726*** (0.0232)
Base.Dep.Var.Mean	0.415	0.389	0.386	0.381	0.404	0.428	0.352	0.457	0.407	0.388	0.390	0.412
Observations	1727	1787	564	925	1008	1017	1861	1653	1754	1405	1792	1722

Table A16: Effects of the Privacy Design on CBDC + Cash Choice

(a) Privacy-sensitive goods		
	(1)	(2)
	Offline purchase	
SR	0.032	0.030*
	(0.021)	(0.017)
Voucher	0.024	0.020
	(0.020)	(0.017)
Observations	3,514	3,514
R-squared	0.001	0.348
Base.Dep.Var.Mean	0.524	0.524
Socioeconomic	No	Yes
Privacy & Payment	No	Yes

(b) Privacy-insensitive goods		
	(1)	(2)
	Offline purchase	
SR	0.018	0.020
	(0.020)	(0.018)
Voucher	0.003	0.001
	(0.020)	(0.018)
Observations	3,514	3,514
R-squared	0.000	0.217
Base.Dep.Var.Mean	0.321	0.321
Socioeconomic	No	Yes
Privacy & Payment	No	Yes

Notes: The dependent variable is an indicator variable equal to 1 if a respondent chooses CBDC or cash. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

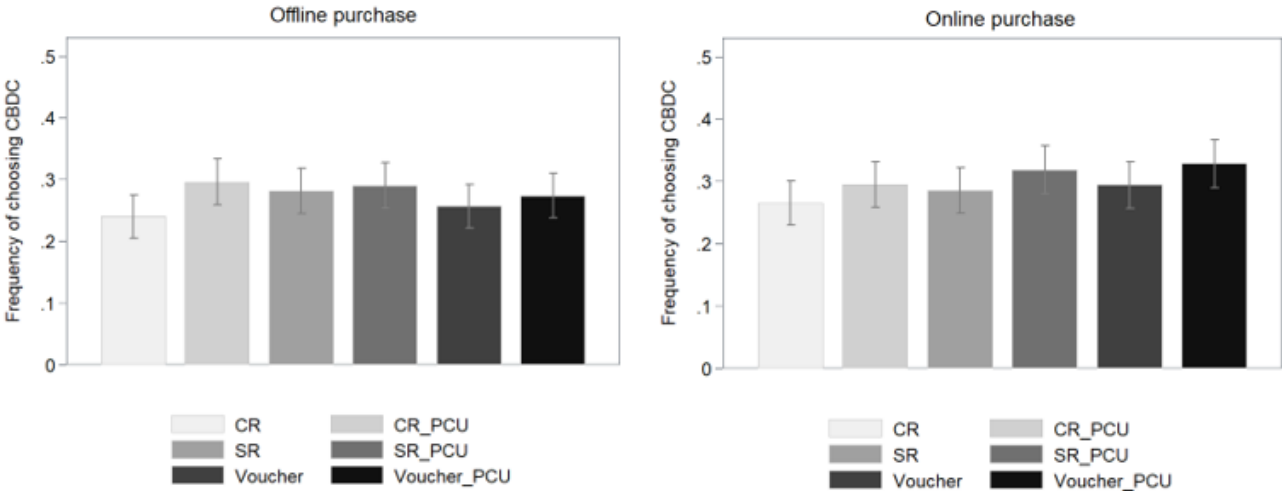
Table A17: Effects of Preventing Commercial Use Information on CBDC + Cash Choice

(a) Privacy-sensitive goods		
	(1)	(2)
	Offline purchase	
PCU	0.036**	0.033**
	(0.020)	(0.014)
Observations	3,514	3,514
R-squared	0.001	0.348
Base.Dep.Var.Mean	0.524	0.524
Socioeconomic	No	Yes
Privacy & Payment	No	Yes

(b) Privacy-insensitive goods		
	(1)	(2)
	Offline purchase	
PCU	0.038**	0.031**
	(0.016)	(0.015)
Observations	3,514	3,514
R-squared	0.002	0.218
Base.Dep.Var.Mean	0.321	0.321
Socioeconomic	No	Yes
Privacy & Payment	No	Yes

Notes: The dependent variable is an indicator variable equal to 1 if a respondent chooses CBDC or cash. Heteroskedacity-robust standard errors are reported in parentheses. Socioeconomic control variables are a respondent's gender, age, living in Seoul, marital status, education, employment status, household income and wealth. Privacy-related control variables are privacy attitudes (e.g., how much she is concerned about the leakage of confidential information, about the risk of privacy leakage by each institution, how much she values the right to privacy), knowledge of privacy, past behavior with respect to protection of personal information, past experience of personal information leakage. Payment-related control variables are where she usually buys products (offline/online), which payment method she usually uses, whether she uses mobile payment services, whether she has experience with cryptocurrency. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Figure A1: Frequencies of choosing CBDC in purchasing privacy-insensitive products



Notes: Caps represent upper and lower bounds of the 95 percent confidence intervals.

B Questionnaire and Screenshots

B.1 Korean Version

The original survey questionnaire in Korean is available in the following link:

[Questionnaire-Korean Version](#)

B.2 English Version

The translated survey questionnaire in English is available in the following link:

[Questionnaire-English Version](#)

B.3 Quizzes about CBDC

1. Which of the following statements about the characteristics of central bank digital currency (CBDC) is not true?
 - (a) It can be used and exchanged for the same value as cash.
 - (b) The value of central bank digital currency is stable, whereas private cryptocurrencies such as Bitcoin and Ethereum are subject to price fluctuations, making their value unstable.
 - (c) It is issued by private parties such as commercial banks and fintech companies.
 - (d) It is a digital form of fiat currency issued by a central bank.

The answer is (c). CBDC is a currency issued by a central bank.

2. Which of the following statements about the use of central bank digital currency (CBDC) is not true?
 - (a) It is a type of digital cash that can be used in face-to-face and online (digital) transactions where cash is not available.
 - (b) It can be used in a similar way to cash even when the internet is not available.
 - (c) Like debit cards and credit cards provided by private financial institutions such as commercial banks and card companies, annual fees and commissions must be paid.
 - (d) It can be used by anyone in the country, including individuals and businesses, for everyday transactions.

The answer is (c). CBDC can be used at no additional cost.

B.4 Screenshots of the CBDC and Privacy Experiment Module's Page by Treatment Status

D4-2. Suppose you want to buy **privacy-sensitive goods or services (e.g., psychiatric services, adult products, etc.)** in **offline** transactions. If **CBDC is available** as a means of payment, which payment method would you choose? Please make your choice carefully weighing between privacy exposure risk and convenience yield.

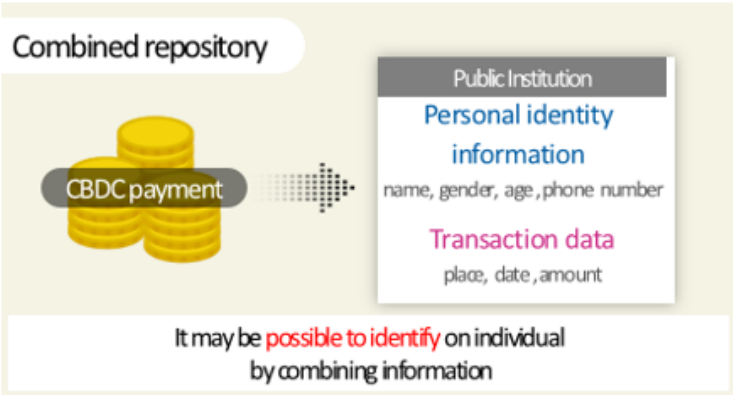
<p>CBDC</p>	 <p>In order to prevent illegal activities such as money laundering and financing for terrorism, personal identity information and transaction data are recorded. Both are stored jointly in a single public institution, so that it may be possible to find out who purchases what by arbitrarily combining personal identity information and transaction data.</p>
<p>Cash</p>	<p>Personal identity information and transaction data are not recorded.</p>
<p>Credit/Debit cards</p>	<p>Personal identity information and transaction data are recorded. Private financial institutions can use them for commercial purposes.</p>
<p>Mobile fast payment</p>	<p>Personal identity information and transaction data are recorded. BigTech companies can combine and analyze these information with consumer's online activities (e.g. search, SNS, shopping) for commercial purposes.</p>

Figure B2: CR Group

D4-2. Suppose you want to buy **privacy-sensitive goods or services (e.g., psychiatric services, adult products, etc.)** in **offline** transactions. If **CBDC** is available as a means of payment, which payment method would you choose? Please make your choice carefully weighing between privacy exposure risk and convenience yield.

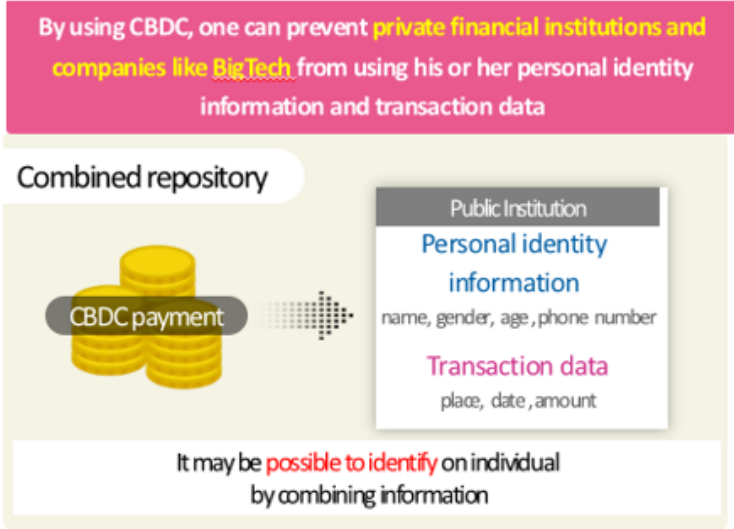
<p>CBDC</p>	 <p>By using CBDC, one can prevent private financial institutions and companies like BigTech from using his or her personal identity information and transaction data</p> <p>Combined repository</p> <p>Public Institution</p> <p>Personal identity information name, gender, age, phone number</p> <p>Transaction data place, date, amount</p> <p>It may be possible to identify on individual by combining information</p> <p>In order to prevent illegal activities such as money laundering and financing for terrorism, personal identity information and transaction data are recorded. Both are stored jointly in a single public institution, so that it may be possible to find out who purchases what by arbitrarily combining personal identity information and transaction data. The use of CBDC can prevent private financial institutions and BigTech companies from using personal identity information and transaction data for commercial purposes.</p>
<p>Cash</p>	<p>Personal identity information and transaction data are not recorded.</p>
<p>Credit/Debit cards</p>	<p>Personal identity information and transaction data are recorded. Private financial institutions can use them for commercial purposes.</p>
<p>Mobile fast payment</p>	<p>Personal identity information and transaction data are recorded. BigTech companies can combine and analyze these information with consumer's online activities (e.g. search, SNS, shopping) for commercial purposes.</p>

Figure B3: CR PCU Group

D4-2. Suppose you want to buy **privacy-sensitive goods or services (e.g., psychiatric services, adult products, etc.)** in **offline** transactions. If **CBDC is available** as a means of payment, which payment method would you choose? Please make your choice carefully weighing between privacy exposure risk and convenience yield.

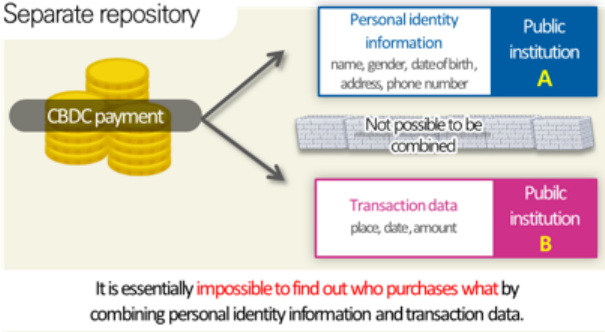
<p>CBDC</p>	 <p>Separate repository</p> <p>CBDC payment</p> <p>Personal identity information name, gender, date of birth, address, phone number</p> <p>Public institution A</p> <p>Not possible to be combined</p> <p>Transaction data place, date, amount</p> <p>Public institution B</p> <p>It is essentially impossible to find out who purchases what by combining personal identity information and transaction data.</p> <p>In order to prevent illegal activities such as money laundering and financing for terrorism, personal identity information and transaction data are recorded. They are stored separately in two different public institutions, so that it is essentially impossible to find out who purchases what by combining personal identity information and transaction data.</p>
<p>Cash</p>	<p>Personal identity information and transaction data are not recorded.</p>
<p>Credit/Debit cards</p>	<p>Personal identity information and transaction data are recorded. Private financial institutions can use them for commercial purposes.</p>
<p>Mobile fast payment</p>	<p>Personal identity information and transaction data are recorded. BigTech companies can combine and analyze these information with consumer's online activities (e.g. search, SNS, shopping) for commercial purposes.</p>

Figure B4: SR Group

D4-2. Suppose you want to buy **privacy-sensitive goods or services (e.g., psychiatric services, adult products, etc.)** in **offline** transactions. If **CBDC is available** as a means of payment, which payment method would you choose? Please make your choice carefully weighing between privacy exposure risk and convenience yield.

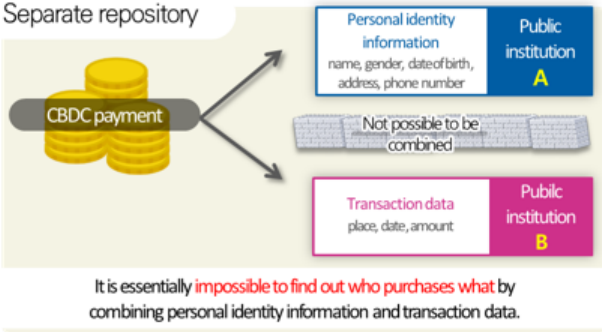
<p>CBDC</p>	<p>By using CBDC, one can prevent private financial institutions and BigTech companies from using his or her personal identity information and transaction data for commercial purposes.</p>  <p>In order to prevent illegal activities such as money laundering and financing for terrorism, personal identity information and transaction data are recorded. They are stored separately in two different public institutions, so that it is essentially impossible to find out who purchases what by combining personal identity information and transaction data. The use of CBDC can prevent private financial institutions and BigTech companies from using personal identity information and transaction data for commercial purposes.</p>
<p>Cash</p>	<p>Personal identity information and transaction data are not recorded.</p>
<p>Credit/Debit cards</p>	<p>Personal identity information and transaction data are recorded. Private financial institutions can use them for commercial purposes.</p>
<p>Mobile fast payment</p>	<p>Personal identity information and transaction data are recorded. BigTech companies can combine and analyze these information with consumer's online activities (e.g. search, SNS, shopping) for commercial purposes.</p>

Figure B5: SR & PCU Group

D4-2. Suppose you want to buy **privacy-sensitive goods or services (e.g., psychiatric services, adult products, etc.)** in **offline** transactions. If **CBDC is available** as a means of payment, which payment method would you choose? Please make your choice carefully weighing between privacy exposure risk and convenience yield.

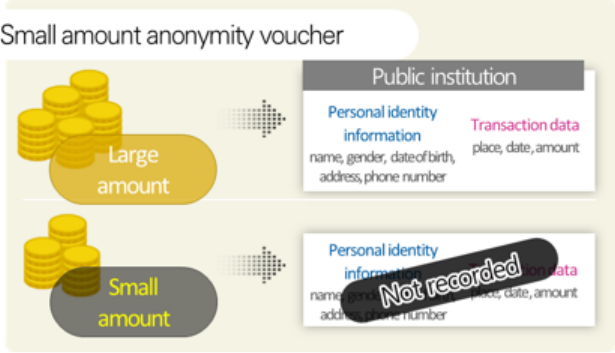
<p>CBDC</p>	 <p>In order to prevent illegal activities such as money laundering and financing for terrorism, personal identity information and transaction data are recorded. For small amount transactions, one can use CBDC as an anonymity voucher in the sense that it does not leave behind any trail of his or her personal identity information and transaction data.</p>
<p>Cash</p>	<p>Personal identity information and transaction data are not recorded.</p>
<p>Credit/Debit cards</p>	<p>Personal identity information and transaction data are recorded. Private financial institutions can use them for commercial purposes.</p>
<p>Mobile fast payment</p>	<p>Personal identity information and transaction data are recorded. BigTech companies can combine and analyze these information with consumer's online activities (e.g. search, SNS, shopping) for commercial purposes.</p>

Figure B6: Voucher Group

D4-2. Suppose you want to buy **privacy-sensitive goods or services (e.g., psychiatric services, adult products, etc.)** in **offline** transactions. If **CBDC is available** as a means of payment, which payment method would you choose? Please make your choice carefully weighing between privacy exposure risk and convenience yield.

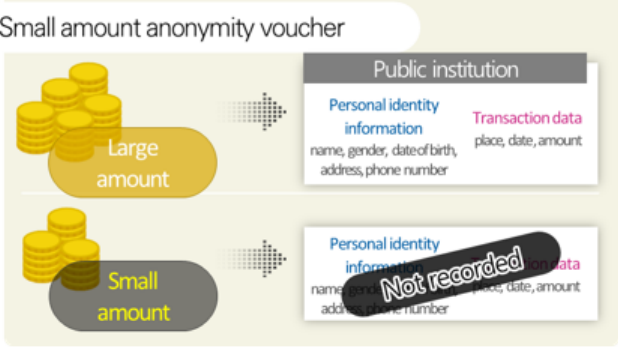
<p>CBDC</p>	<p>By using CBDC, one can prevent private financial institutions and BigTech companies from using his or her personal identity information and transaction data for commercial purposes.</p>  <p>Small amount anonymity voucher</p> <p>Large amount</p> <p>Small amount</p> <p>Public institution</p> <p>Personal identity information name, gender, date of birth, address, phone number</p> <p>Transaction data place, date, amount</p> <p>Personal identity information name, gender, date of birth, address, phone number</p> <p>Transaction data place, date, amount</p> <p>Not recorded</p> <p>In order to prevent illegal activities such as money laundering and financing for terrorism, personal identity information and transaction data are recorded. For small amount transactions, one can use CBDC as an anonymity voucher in the sense that it does not leave behind any trail of his or her personal identity information and transaction data. The use of CBDC can prevent private financial institutions and BigTech companies from using personal identity information and transaction data for commercial purposes.</p>
<p>Cash</p>	<p>Personal identity information and transaction data are not recorded.</p>
<p>Credit/Debit cards</p>	<p>Personal identity information and transaction data are recorded. Private financial institutions can use them for commercial purposes.</p>
<p>Mobile fast payment</p>	<p>Personal identity information and transaction data are recorded. BigTech companies can combine and analyze these information with consumer's online activities (e.g. search, SNS, shopping) for commercial purposes.</p>

Figure B7: Voucher & PCU Group

Previous volumes in this series

1146 November	On par: A Money View of stablecoins	Iñaki Aldasoro, Perry Mehrling, Daniel H. Neilson
1145 November	Dollar and Government Bond Liquidity: Evidence from Korea	Jieun Lee
1144 November	Profitability, valuation and resilience of global banks – a tight link	John Caparusso, Ulf Lewrick and Nikola Tarashev
1143 November	Do banks practice what they preach? Brown lending and environmental disclosure in the euro area	Leonardo Gambacorta, Salvatore Polizzi, Alessio Reghezza, Enzo Scannella
1142 November	Platform lending and innovation	Leonardo Gambacorta, Leonardo Madio and Bruno M Parigi
1141 November	Is high debt constraining monetary policy? Evidence from inflation expectations	Luis Brandao-Marques, Marco Casiraghi, Gaston Gelos, Olamide Harrison and Gunes Kamber
1140 November 2023	Relationship discounts in corporate bond trading	Simon Jurkatis, Andreas Schrimpf, Karamfil Todorov, Nicholas Vause
1139 October 2023	A journal ranking based on central bank citations	Raphael Auer, Giulio Cornelli and Christian Zimmermann
1138 October 2023	Dealer capacity and US Treasury market functionality	Darrell Duffie
1137 October 2023	International portfolio frictions	Wenxin Du
1136 October 2023	Expectations and the neutrality of interest rates	John Cochrane
1135 October 2023	Artificial intelligence, services globalisation and income inequality	Giulio Cornelli, Jon Frost and Saurabh Mishra
1134 October 2023	Bank competition, cost of credit and economic activity: evidence from Brazil	Gustavo Joaquim, Bernardus van Doornik and José Renato Haas Ornelas

All volumes are available on our website www.bis.org.