Privacy in Payment in the Age of Central Bank Digital Currency

Frédéric Tronnier

Privacy in Payment in the Age of Central Bank Digital Currency

Frédéric Tronnier

Goethe Universität Frankfurt, Frankfurt am Main, Germany
frederic.tronnier@m-chair.de

In academia and at central banks, central bank digital currency (CBDC) is increasingly being researched due to the continuous decline in cash payments and the emergence of private stablecoins such as Libra. While CBDC offers various advantages for central banks, sensitive transaction and holdings data of individuals and users need to be protected. This paper analyses how privacy in payment is being discussed in CBDC related literature and pilot projects of central banks. Central banks rarely identify privacy as a key requirement in the development and implementation of a CBDC. Instead, anonymity is seen as one possible feature of a CBDC that could hinder know-your-customer (KYC) and anti-money laundering (AML) compliance of banks. In pilot projects, different techniques and solutions have been proposed to achieve varying levels of privacy for users. A comprehensive framework on how best to achieve privacy in retail CBDC is needed. Such a framework should consider the differing underlying design aspects of a CBDC and the use cases for which the CBDC is to be developed.

Keywords: Privacy, Payment, Central Bank Digital Currency, CBDC, Cryptocurrency

1 Introduction

Payment systems and currencies have been subject to a multitude of significant changes over the last millennia, from shells to coins to banknotes, cheques to the current digital payment in ever-changing currencies. Today, electronic and mobile payment systems are challenging cash-based payments. For the last 400 years [1], central banks have been responsible for issuing legal tender to the population of their respective country or empire. Cash, to this day the only form of legal tender that may be owned by individuals and is issued directly through a central bank [2], grants the holder the option to carry out transactions with a high degree of privacy. With the decrease in cash payments in many parts of the world [3] and particularly in countries like Sweden [4], economies are shifting towards electronic, online, and mobile payment.

Through the introduction of Bitcoin by Nakamoto [5], cryptocurrencies were established with the intention to provide new and decentralized means of payment, units of account, and stores of value. Although cryptocurrencies have not -yet - lived up to their self-set expectations, organizations such as Facebook have started working on

their own cryptocurrencies or tokens to offer their customers a new means of transactions to increase their market dominance [6].

With the rise in cryptocurrency prices and attention towards it, the decrease in cash use, and the increased efforts of global corporations aiming to enter the currency market, the questions of whether and how central banks are going to react to these developments have arisen naturally given their central role in managing the money supply of a country. As a result, central banks worldwide have started piloting projects on central bank digital currency (CBDC), most notably in Sweden [7], China [8], South Africa [9] and the whole European Union (EU) [10]. These central bank-issued digital currencies could potentially offer central banks the possibility to effectively and efficiently oversee, track and analyse holdings and transactions much better than with cash [11]. Protecting sensitive financial and non-financial personal data in payment is therefore essential and needs to be researched in academia.

2 Aim of this paper

"Currency cannot be private, money is a public good of sovereignty..."
- Francois Villeroy de Galhau, Governor of the Bank of France [12]

The quote by the Governor of the Bank of France, the French central bank, highlights the ongoing discussion by CBs about the introduction of a CBDC in response to decentralized or private cryptocurrencies and the need for a digital alternative to cash for individuals. Currently, CBDC as a new form of payment is discussed worldwide in academia and by central banks through research papers as well as first pilot tests and proofs-of-concepts (PoC).

However it was shown that CBDC is discussed mainly through papers that provide a general introduction to the topic, as well as work on the possible economic and monetary effects that a CBDC would have on the banking industry and the economy as a whole, while literature on the societal impact, or stakeholders who might be impacted by CBDC, is scarce [13]. Scientific papers and reports published by central banks focus on discussing the general underlying technical concept, the potential design options, and their (dis)advantages of CBDC [13]. Work with a main focus on privacy in CBDC has only been issued by the Bank of Canada[14] and the European Central Bank [15]. In this paper, information privacy follows the notion of Clarke [16] that data of individuals should not be available to other entities and that the individual must be able to execute "… a substantial degree of control over that data and its use." [16, p.60]. Garratt and van Oordt [17] analyzed privacy in payment and argued that privacy can be viewed as a public good. The inability or failure of individuals to preserve their payment information impose a negative externality on others as it can be used for price discrimination of other individuals and therefore leads to socially suboptimal results. Privacy concerns of individuals and users have also been researched for newer payment systems such as online [18] and mobile payment [19]. In electronic payments, various methods and solutions for anonymous payment systems have been introduced in the past, from hardware tokens [20] to protocols [21] and various cryptocurrencies [22, 23].

Naturally research in CBDC, often conducted by central banks, focuses on CBDC from the perspective of a central bank. A notable exception is the work of, Leinonen [24] who highlights the requirements for a CBDC from an end-user perspective. He states that a CBDC should have more in common with currently used private (digital) payment services than with traditional cash, and mentions the possibility of market turbulence in the payments sector caused by introducing/issuing a CBDC, and suggests that this CBDC should serve as a basic payment instrument.

While currency may be a public good, the information that are generated while paying and transacting in a currency should not be public and are protected through regulation such as the General Data Protection Regulation (GDPR). Therefore, this paper aims to contribute to the growing body of literature on CBDC by exploring privacy in CBDC payments for the first time through the analysis of existing research and information published by central banks. Pilot projects from central banks and developed PoC will be examined to gain a thorough understanding of the potential impact of CBDC on users' privacy. Thus, this paper aims to assess how central banks address the topic of privacy in CBDC both theoretically, in published information, and practically, in pilot projects that implemented CBDC.

3 Central Bank Digital Currency

In order to define CBDC it is advisable to define money itself first. Greco and Thomas [25] provide the practical definition that money "… is anything that is generally accepted as a means of payment." [25, p.27]. Money provides several functions. The three most important ones are to act as a medium of exchange, as a unit of account, and as a store of value. The concept of the Money Flower is introduced in [26], which distinguishes between different forms of money through four key properties: issuer (central bank or private institutions), form (digital or physical), accessibility (available to the general public or limited to banks), and technology (account- or token/value-based). Currently, only banknotes and coins are issued by central banks as legal tender for the general population. Bank deposits, although denominated in the same monetary unit as cash, are issued by private commercial banks and not central banks. These commercial banks also have access to central bank digital money in the form of reserves and settlement accounts, which are not accessible for the general population. Cryptocurrencies like Bitcoin and other forms of digital tokens, on the other hand, can either be widely accessible or wholesale only, but are not private and not central bank-issued. Cryptocurrencies may be defined as a virtual type of currency that "… rely on the transmission of digital information, utilizing cryptographic methods to ensure legitimate, unique transactions" [27, p.3]. Within this framework, stablecoins form a special category. Stablecoins are private, digital tokens that are often backed by a basket of established currencies, cryptocurrencies, or other assets with the goal to generate and maintain a stable price of the coin. Libra, the proposed token of the eponymous project initiated by Facebook and other organizations [28] is one example of a stablecoin that could potentially function similarly to a CBDC.

Based on [26] and [29], three major categories of CBDC can be identified: general-purpose accounts, general-purpose tokens and wholesale tokens. While general-purpose accounts only expand on the existing reserves and settlement account systems of central banks, tokens are based on blockchain or distributed ledger technology (DLT) that may be accessible for the general public or limited to financial institutions. In this context, a token represents a digital and identifiable unit of currency that is transferred as a means of payment. This stands in contrast to an account-based model in which the owner of an account is identified, rather than the means of payment [30].

For this paper, CBDC are defined as digital, central bank-issued currencies, excluding existing central bank reserves and settlement accounts. The underlying technology, account-based CBDC or token, also called blockchain or DLT-based, may differ between the investigated research and the different pilot projects of central banks. Similarly, the use cases of central banks with a CBDC differ between general-purpose and wholesale CBDC. While a general-purpose CBDC may be used by the general public with cash-like features, a wholesale CBDC is not accessible by the general public and is used for interbank payment settlements [31]. As this paper analyses the privacy implications of a CBDC for individuals, the focus is on general-purpose CBDC.

For central banks, CBDC offers various potential advantages, including a greater market power and the ability of stronger control over monetary policy [see 22–24]. However, a CBDC also offers central banks the general possibility to effectively and efficiently oversee, track and analyze transactions much better than before, depending on the design and technical features of the CBDC. This represents a strong potential threat to user privacy and data protection [35]. Both academia and central banks themselves published various papers and articles on CBDC. Tronnier, Recker and Hamm [13] showed that the majority of research is focused on providing an initial overview of the topic, followed by research on the monetary and economic implications of a CBDC. However, research on other factors such as societal and legal implications has been scarce. Issues on privacy and anonymity of transactions in CBDC have thus far been researched only superficially. In [26] it is argued that a CBDC could have the same level of privacy as cash but note that the property of privacy in cash emerged over time out of convenience. In CBDC, the decision for anonymity as a feature would nowadays become a conscious one. Wandhöfer [11] argues that anonymity is a key property of cash and proposes to equip CBDC with a comparable level of anonymity, for instance through the identification of users at the point of conversion, without linkage to cryptographic transaction information. The author also highlights the importance of anonymous payment solutions to protect citizens against surveillance. In [36] it is argued that anonymity in CBDC would be of even greater importance in the future, should cash use continue to decline or eventually be completely replaced by CBDC. Then, a CBDC would act as the only anonymous payment method for individuals.

The close collaboration of central banks with all stakeholders in the development of a CBDC is important [31]. Although central banks already collaborate with technology service providers, financial institutions and other central banks, we argue that for retail CBDC, the end-users, the general population, is equally important for the success and adoption of a CBDC. Thus, this paper evaluates how central banks consider privacy

and its importance for individuals. Several central banks are in different stages of piloting first projects on CBDC to test their hypotheses and the underlying technology of the CBDC. These pilot projects are a stark contrast to the majority of theoretical papers on the subject as first solutions are implemented and evaluated by the manufacturing central bank.

4 Methodology

To evaluate how privacy and privacy concerns are currently being discussed and considered, published research and pilot projects have to be identified first. A first literature review is provided in [13], where the authors evaluate both academic works as well as published literature by the central banks and finding that central bank papers have been published in academic journals in the past. Furthermore, the authors search multiple scientific databases, among others Web of Science, AIS eLibrary, EBSCOhost and IEEE Xplore, for the term Central Bank Digital Currency, finding 19 articles on the topic. However, their work does not encompass all central banks but only the five main central banks that issue the most important currencies worldwide by number of users and overall economic importance.

In this paper, we adapt the process of a systematic academic literature review by [37] to websites of various central banks to identify papers of academic quality and pilot projects. Additionally, a simplistic google based search is used to identify information that could not be found directly through a central banks' website. The focus hereby lies in research and pilot projects on retail CBDC, acting as a cash equivalent, as privacy is of particular importance for individuals and end-users. While privacy can and should also be considered in wholesale CBDC, the number of stakeholders, different banks, and payment service providers is significantly lower than the number of people that would use a CBDC as a cash equivalent in everyday payments.

The work of several other authors is also used to provide a starting point in identifying pilot projects and central bank activities. The authors of [38] provide not only a comprehensive overview of CBDC but also a first list of central bank pilot projects. The authors analyze 17 retail CBDC projects from 17 countries based on the design choices architecture, infrastructure, access, and state the motivation and result of each project. In a paper provided by Bank of International Settlement [29] 63 central banks are surveyed on whether and how they are investigating CBDC. A similar survey was conducted in 2020 with 66 central banks [39]. Another very recent work also provides a comprehensive list of CBDC projects and activities of central banks [31]. The authors focus on wholesale CBDC projects for interbank settlement and payment and the underlying DLT. Political, legal and societal implications are explicitly stated to be outside of the scope of their work.

Based on the work of [13, 29, 31, 38] we identified a total of 78 CBs for initial consideration. These CBs have all participated in the surveys by the Bank of International Settlement or were previously identified to conduct research on CBDC by [31] or [38]. All CBs are listed in table 1 and table 2 of this work. The website of each CB was then searched for the keywords "CBDC", "Central Bank Digital Currency" and

"digital currency". Only complete research publications in English that have been published by the specific central bank have been considered as "Final Hits". Several keyword hits are due to speeches, talks and news on this topic, which have not been counted in the final hits. Hits have been reviewed using the title and/or the abstract to assess their relevance to this study by covering the topic of CBDC in general.

Additionally, a google keyword search was conducted for the keywords stated above in combination with the country of each central bank to obtain supplementary information that has or has not been published by the central banks themselves. This was especially helpful to obtain information on pilot projects of central banks, as the search engine on most central bank websites demonstrated to be less effective and expedient than expected.

5 Results of the literature review

Table 1 demonstrates the result of the systematic literature review on central bank websites. Due to page limitations, only findings that demonstrated hits are included. All final hits have been read and analysed to gather information on whether and how the central bank covers privacy and data protection in their analysis of CBDC.

It can be seen that for 38 (48,7%) central banks no hits could be found, while for an additional 13 central banks, no final hits were found, leaving 27 central banks for consideration. From the ones that published information on CBDC, data protection and privacy was often covered only superficially. Only the European Central Bank (ECB) and the Bank of Canada published research specifically dedicated to the topic of privacy. Table 1 covers all central banks that exhibited findings while table 2, in the appendix, lists the central banks for which no hits could be reported through the literature review, as well as on how detailed information on privacy have been provided by the banks. As the search function provided on many central banks' websites proofed to be ineffective, an additional google search was conducted to verify the results and obtain additional information where possible. Hereby, the official name of the central bank, along with the term CBDC were used as keywords, using the Google News search mask. Supplementary information could be found particularly on the pilot projects of central banks, provided by various newspapers. In the following, selected findings will be reviewed to establish the focus of different publications and central banks.

Table 1. Hits of the Literature Review on Central Bank Websites

Central Bank	Search	Coverage	Hits	Final Hits	Privacy consideration level*
Bank Indonesia	All Results	No option	10	1	1
Bank Negara Malaysia	All results	No option	9	1	1
Bank of Canada	All Content Typs	No option	36	16	4
Bank of England	Publications	All	4	4	2

Bank of France	Publications	All	5	3	3
Bank of Israel	No option	No option	10	2	2
Bank of Italy	Full site	No option	8	2	4
Bank of Japan	Contained in page	No option	22	4	1
Bank of Korea	All	No option	1	1	1
Bank of Lithuania	All	No option	5	2	2
Bank of Spain	All	No option	27	1	3
Bank of Thailand	No option	No option	77	5	3
Central Bank of Brazil	All Categories	All	3	1	1
Central Bank of Iceland	All Categories	All	1	1	1
Danmarks Nationalbank	No option	No option	6	2	3
De Nederlandsche Bank	No option	No option	13	3	3
European Central Bank (ECB)	No option	No option	30	5	4
Federal Reserve	Entire Site	No option	2	1	1
Hong Kong Monetary Authority	Data, Publications and Research	No option	4	1	1
Monetary Authority of Singapore	All	All	2378	2	4
Mongolbank	No option	No option	1	1	1
National Bank of Belgium	No option	No option	10	1	1
Norges Bank	Publications	No option	2	2	2
Reserve Bank of India	All	All	1	1	1
Reserve Bank of New Zealand	No option	No option	4	1	1
Sveriges Riksbank	PDF	No option	29	13	2
Swiss National Bank	Any Result Type	Any Modified Date	13	1	1
*1:not mentioned, 2:privacy mentioned superficially, 3:privacy discussed, 4:privacy as core design element or requirement					

Table 1 provides the official name of the respective central bank, used search options as well as the number of hits and final hits for the keywords “CBDC” and “Central Bank Digital Currency”. Additionally, a privacy consideration level is provided, depending on how much work CBs provide on privacy in CBDC. A lower score indicates that privacy issues have not, or only superficially, been discussed. This

demonstrates that final hits in table 1 may discuss CBDC without even mentioning privacy considerations or data protection. CBs with a higher score provided chapters specifically on privacy and data protection in their work, or published dedicated work with privacy as its sole focus.

Although various central banks published information and research on CBDC, many central banks covered privacy only superficially. As a possible explanation for this, the Bank of England argues that that privacy considerations do not fall directly into the area of business of a central bank but must be nonetheless taken into account [40].

The Central Bank of France discusses privacy in more detail and conducted a taskforce to document the potential benefits, issues and risks of a CBDC, taking an operational perspective on the topic [41]. Privacy and anonymity are discussed with regards to anti-money-laundering (AML) and the combating financing of terrorism (CFT) requirements as well as international legislation on privacy. The bank states that the "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data ..." must be applied when creating and implementing a CBDC. Furthermore, the bank states that the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services (PSD2) excludes central banks from being payment service providers, resulting in the question whether a central bank is legally allowed to issue a CBDC. Concerning AML/CFT requirements, the bank notes that the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (amended in 2018 by Directive (EU) 2018/843) defines virtual currencies as "a digital representation of value that is not issued or guaranteed by a central bank…", wherefore a CBDC would not be treated as a virtual currency in the AML/CFT regulation. However, the central bank may be defined as a financial institution under the Directive 2013/36/EU and would, therefore, have to object to AML/CFT regulation [41].

The Bank of Japan reviews anonymity as both, a possible advantage or a disadvantage of CBDC. While anonymity ensures privacy protection in payments, cash is also used for illicit activities, money laundering and tax evasion. The authors reference the Peoples Bank of China that pointed out the prevention of such activities as one possible advantage of a CBDC [42]. Similarly, the Bank of Spain focuses on the (dis)advantages of an anonymous CBDC. The authors note that, even if a CBDC would be non-anonymous, money laundering and illicit activities would still be conducted, only using other currencies, gold, or cryptocurrencies. As a further disadvantage, a non-anonymous CBDC would require the central bank to invest heavily in IT-infrastructure to secure such a system and validate transactions [43]. According to the authors, the adaption of a decentralized validation mechanism of cryptocurrencies to a CBDC might be problematic. This would add costs and could pose a security threat if the system turns out to not be robust. However, it has to be noted that these arguments are only applicable to a token-based CBDC.

In a report for the central bank of the Netherlands, the authors of [44] note that, depending on the design of the CBDC, personal information could be obtained by non-banking operators, whereby surveys indicate that households trust non-banking

operators less with their data than they trust financial institutions. As privacy is a key objective for CBDC, the authors would choose a design in which the central bank does not obtain balances and transaction information if the CBDC is used for commercial purposes. Figure 1 demonstrates the degree of privacy for users for different payment systems as evaluated by [44].

Fig. 1. *Degree of privacy for users by payment system* [34, p.33]

The authors argue that a CBDC would provide a higher degree of privacy than commercial bank money and private digital currencies like Libra because the CB does not have commercial incentive to use payment data. Nonetheless, a CB might need to provide, undefined, supervisory authorities with access to payment data to investigate illegal activities such as money-laundering or the financing of terrorism. Furthermore, the authors argue that intermediaries might only need access to transaction data to initiate payments, balances could only be visible to the CB. However, Fig.1 provides only a subjective scale and no further information on possible attack models are given.

The author of [45] from the Bank of Italy analyses the demand for CBDC and introduces a novel specification for money, the notion of money as a store of information. Here, the existence of privacy cost is assumed and linked to the demand for trustlessness [37–38 as cited by 36]. The loss of trust in public institutions is speculated to be one driver in the adoption of cryptocurrencies. In an economic, computer-based experiment with 80 students as participants, the author tested for design features of money that are valued by participants. The participants had to create portfolios consisting of different shares of the four currency types E-Currency -the CBDC of the experiment-, paper currency, banking currency and cryptocurrency [48]. The currency types differed on their safeness, store of value and anonymity, whereby the CBDC was chosen to be non-anonymous. The features and the building of the portfolio were described to the participants beforehand and 1440 responses were collected from the 80 participants. The preliminary results indicated that participants value liquidity and expected return in currencies while anonymity as a feature was valued less.

The Norges Bank, the central bank of Norway, discusses privacy as an aspect of consumer protection [49]. The bank notes that the country is working on incorporating the General Data Protection Regulation (GDPR) into their national legislation and state that it would be beneficial to consider guidelines on data protection by default and by design in the development of a CBDC. Further legislation that affects privacy are EEA agreements for the free flow of transactions and capital as well as the Financial Contracts Act that regulates the misuse of payments, for instance, if an authorized payment has been made by another entity than the customer. A CBDC must comply with these rules, which affects data protection.

The Bank of Canada published an analytical note on privacy in CBDC in June 2020 and provided one of the very few papers with a specific focus on privacy. The authors provide a framework to compare different retail payment solutions regarding their privacy profiles for holdings and transactions. They differentiate between stakeholders such as the government, banks or money service business (MSB) that can either act on behalf of the payee(Pe) or the payer(Pr), or other users [14]. MSB hereby legally defines non-bank financial institutions, that offer money transfers, the issuing money orders or the exchange and transfer of digital currencies to the public [50].

Figure 2 displays the results of the different payment technologies for the different stakeholders, whereby higher values indicate a higher level of privacy.

Fig. 2. Privacy profiles of payment technologies [14] of the Bank of Canada

Solution	Government					Payer MSB					Payee MSB					Payee	Payment providers					Public (other users)				
	H		T			H		T			H		T			T	H		T			H		T		
	O	B	Pr	Pe	A	O	B	Pr	Pe	A	O	B	Pr	Pe	A	Pr	O	B	Pr	Pe	A	O	B	Pr	Pe	A
Credit card (stripe)	3	3	1	1	0	0	0	0	0	0	2	3	2	0	0	0	1	3	1	0	0	3	3	3	3	3
Credit card (EMV)	3	3	1	1	0	0	0	0	0	0	2	3	2	0	0	2	1	3	1	1	0	3	3	3	3	3
E-transfer	3	3	1	1	0	0	0	0	1	0	1	3	1	0	0	2	1	3	1	1	0	3	3	3	3	3
Debit card	3	3	1	1	0	0	0	0	0	0	1	3	1	0	0	1	1	3	1	1	0	3	3	3	3	3
Permissioned DLT	1	0	1	1	0	0	0	0	1	0	1	3	1	0	0	1	1	0	1	1	0	3	3	3	3	3
Bitcoin custodial	2	3	2	2	0	0	0	0	2	0	2	3	2	0	0	2	2	3	2	2	0	2	3	2	2	0
Bitcoin pro	3	3	2	2	0	3	3	2	2	0	3	3	2	2	0	2	3	3	2	2	0	3	3	2	2	0
Tiered ledgers	1	0	1	1	0	0	0	0	1	0	2	3	2	0	0	1	3	3	3	3	3	3	3	3	3	3
Device-based (KYC, non-transferable)	0	2	2	0	2	0	2	2	0	2	0	2	2	0	2	1	2	3	3	3	3	3	3	3	3	3
Device-based (non-KYC, transferable)	3	3	2	0	2	3	3	2	0	2	3	3	2	0	2	1	2	3	3	3	3	3	3	3	3	3
Cash	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3

It can be seen that DLT-based solutions provide anonymity only to certain stakeholders for specific data categories. For instance, a custodial Bitcoin payment offers a relatively high level of anonymity, as stated by the authors, for holdings data, that is information on the owner (O) and the balance (B) of a wallet. However, the transaction (T) amount (A) is always visible for all entities in all columns. A permissioned DLT, a solution that is favored by many central banks, would provide a high level of anonymity from other users or the general public. The central bank as well as the banks or non-bank financial institutions that are executing such a transaction on behalf of payer and payee have however access to most data types using such a solution. Overall, the authors demonstrate that the level of privacy a payment solution provides depends on the type of data and differs between stakeholders that may or may not view and access payments information.

The authors therefore note that a CBDCs privacy system depends on several questions that need to be considered first. Should all transactions be disclosed to the government? How much and what kind of information is necessary for merchants, banks, MSBs and law enforcement? Should Know-your-customer (KYC) regulations apply at all times? Both KYC and AML/CFT requirements need to be met, which could impact the

maximum level of achievable privacy. Lastly, it is concluded that nuanced and fine-grained solutions are possible in designing a CBDC. Hereby privacy by design and several privacy-enhancing techniques such as zero-knowledge proofs, multi-party computation and differential privacy are mentioned. These concepts and techniques could be applied to a CBDC.

6 Pilot projects on CBDC

Several findings of the literature review included not only theoretical work by the central banks but also information on pilot projects and PoCs of central banks in CBDC.

A country that has already introduced CBDC as legal tender are the Marshall Islands. As one of the smallest countries in the world, with a population of about 50.000 living on more than 1000 islands, the traditional payment system is not suitable for the geographic conditions of the country, leading to high transaction fees [51]. Thus, the country introduced the Marshallese Sovereign (SOV) in 2018, a blockchain-based cash equivalent and declared it as legal tender through the Sovereign Currency Act 2018. The declaration requires all users of the SOV to undergo KYC procedures. User data is not kept on the blockchain, and users can choose between different accredited verifiers that then issue the user a cryptographically signed ID. Additionally, users can create multiple IDs by verifying multiple accounts through multiple verifiers, thereby increasing the level of privacy. Verifiers, however, are not only responsible for IDs but analyse and monitor transactions with the ability to report suspicious activities and blacklist users [52].

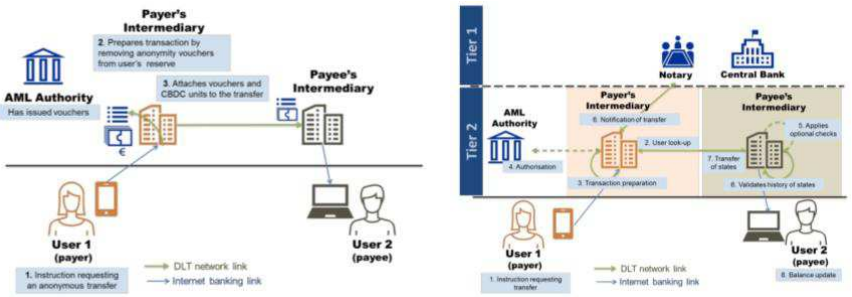
The Sand Dollar of the Central Bank of the Bahamas was introduced in a whitepaper in 2019 and is being piloted on several islands of the country. The project uses an account-based solution where transactions and holdings are not anonymous but confidential. The CBDC is meant to act as both, a cash equivalent for the general population as well as a payment method for wholesale applications such as interbank settlements [53]. A key requirement for the project has been that transactions are non-anonymous while still protecting user confidentiality. The central bank itself will maintain a KYC register and monitor transactions. In the whitepaper, additional information on the KYC requirements is provided. The requirements vary for low- and medium-value personal accounts and high-value accounts for businesses. Limits are set for the maximum holding amount as well as for a maximum transaction limit per month. Depending on the account, account holders are required to provide only basic information like name and address or use official documents to activate an account. Apart from that, the project differs from other findings as stakeholder research has been conducted to assess the willingness of the country's inhabitants to adopt digital financial services. The survey, conducted among 519 randomly chosen residents of the district of Exuma, did however only assess the respondents' use of online and mobile payment behavior and did not question privacy concerns with regard to the respective technologies [53].

Sweden started working on a CBDC as early as 2017 and is one of the countries most often mentioned when it comes to digital currencies in general. The country, due

to the strong decrease in cash use among its citizens, is evaluating a digital cash equivalent, the e-krona. In its second report, the central bank states that payment with e-krona will be traceable, as, regardless of whether the currency will be account- or token-based, a central register for transactions will exist [54]. The bank notes that transaction and user data can be identified, although the bank will comply with all applying regulations and ensure data protection. Interestingly, the bank mentions a prepaid e-krona card, which could be exchanged physically between users and thus would allow for anonymous transactions. Such prepaid cards, with token-based e-krona already stored on, could be anonymously bought and would comply with the respective AML regulation. This would not be possible with an account-based e-krona.

The ECB of the EU represents the only central bank that provided a document exclusively dedicated to privacy and anonymity in the PoC of a retail CBDC. In their Issue no 4/2019, titled "Exploring anonymity in central bank digital currencies" [15], they report the results of a PoC that provides users with some degree of privacy. The PoC, developed by the European System of Central Bank's (ESCB) EUROchain research network, is based on the Corda network, an open-source distributed ledger technology (DLT) platform. The solution uses "anonymity vouchers" that are issued by an AML authority at regular intervals towards users. This entity performs anti-money laundering checks, authorizes transactions and verifies users' identities. The ECB does not act as the AML authority in the PoC. Instead, the ECB itself is responsible for issuing and removing CBDC from circulation. Users can then spend anonymity vouchers, one voucher per one unit of CBDC, for anonymous transactions. The vouchers are not transferable and the amount of vouchers per user in a specific timeframe is specified by the AML authority. Figure 4 describes the transfer of CBDC with anonymity vouchers, as compared to the transfer using AML checks. The ECB itself is not involved in transfers using anonymity vouchers. The payer sends CBDC stating the amount, payee information, and the wish for an anonymous transaction to its intermediary. The payer's intermediary then checks if the payer has enough anonymity vouchers. Using the DLT network, the intermediary attaches the vouchers and CBDC to the transfer to prove to the payee's intermediary that the transaction can occur anonymously. If enough anonymity vouchers are provided, the payer's intermediary does not need approval by the AML authority, creating an anonymous transaction as the payee's intermediary does not have to validate the transaction with further checks.

Fig. 4. CBDC transfer with (left) and without (right) anonymity vouchers [15]



If no or not enough vouchers, are used, the AML authority has to authorize the transaction while a notary node maintains a registry of transactions and states, without specific transaction value data or user information. The ECB concludes that it's PoC CBDC payment system can ensure users' privacy for low-value payments while still ensuring AML/CFT compliance for higher-value transactions. Nonetheless, several issues are noted that can be improved in the future. Regarding privacy preservation, intermediaries need to view past transactions to validate new transactions, which could be used to create a knowledge graph over time in the current PoC. This issue could be solved through chain snipping, meaning that the transaction history of users will be reset. Privacy-enhancing techniques and technologies such as rotating public keys, zero-knowledge proof, and enclave computing may be added to increase user privacy.

7 Discussion

The systematic literature review demonstrated that privacy plays only a minor role in the information provided by central banks on CBDC. Several banks either published no information on CBDC at all or did not discuss privacy, trust, and anonymity of transactions in their work. Others discussed these topics only superficially. By investigating the literature and pilot projects of central banks directly, more information on privacy as a feature or design element of the prototypes could be found. The approach towards privacy has not been standardized and differs between the findings. In the theoretical findings, privacy is often seen as one design feature that a CBDC might possess. The advantages and disadvantages of anonymous CBDC are outlined for individuals and the central bank. For individuals, it is assumed that anonymity is a desired characteristic in a currency, although individuals attitudes towards privacy in CBDC have only been researched directly in [48]. Apart from that, only the Central Bank of the Bahamas interacted with users directly by surveying respondents on financial inclusion as a prerequisite for the introduction of a CBDC [53]. In [48], the preliminary results even indicated that anonymity seems to play a weaker role for individuals than what could reasonably be expected. Thus, additional research is necessary to establish the importance of anonymity and possible privacy concerns of individuals for novel payment methods. The concept of trust is closely connected to privacy concerns and was found to also be examined only lightly. The authors of [44]

state that households trust financial institutions more with their data than non-banking operators. Such findings need to be incorporated in the design of a CBDC to ensure that only trusted entities can access privacy-sensitive information in CBDC payments and holdings.

For central banks, anonymity is not seen as a desirable feature as this could hinder compliance with AML/CFT regulation and KYC requirements and could enable illicit activities. It is noted, however, that such activities would still be possible through other (crypto)currencies even if a CBDC were to be completely non-anonymous. Additional disadvantages for the central bank would be increasing costs due to the required investments in the IT-infrastructure as well as substantial research and labor costs to create and manage such a system and to validate transactions. The concepts of privacy-by-design and privacy-by-default are only mentioned in findings that focus specifically on privacy. Similarly, privacy-enhancing technologies (PETs), such as zero-knowledge proof or other techniques that could be applied to token-based CBDC, are not discussed but merely mentioned for future research. Since the publication of the corresponding papers, blockchain platforms such as Corda have adapted such technologies, potentially changing the evaluation result of central banks of such platforms.

While CBs often cite existing regulation and the prevention of illegal activities as reasons to limit privacy in CBDC, it fails to consider regulation that requires the provision of privacy of information for individuals in a similar matter. Financial and personal information that would be stored, exchanged and created by using a CBDC is defined as personal data in Art. 4 GDPR. As this personal data would be processed, defined as the performance of operations on the data (Art. 4(2) GDPR) by CBs and other payment service providers, the GDPR would regulate and restrict how exactly personal data can be used and processed in CBDC payments. Thus, CBs need to consider how privacy can be established in CBDC payments and should not only look for compliance that is focusing on the prevention on illegal activities. The European Data Protection Board (EDPB) has recently published guidelines on the interplay of the GDPR and PSD2 [55] and reiterates the need for data protection and compliance with the GDPR in electronic payments.

The Bank of Canada [14] provides the work with the strongest focus on privacy in CBDC exhibited in this literature review. Although the authors provide an overview of privacy profiles of different payment technologies and rate these technologies on their level of privacy, distinguishing between the possible stakeholders involved, these ratings are not explained in detail. It is, for instance, unclear how the scale in this rating is derived and how exactly it was determined how well a certain technology scored. Furthermore, as was shown in the pilot projects of other central banks, different privacy-enhancing technologies and techniques can substantially improve the possible level of privacy in DLT based payment systems. Therefore, information is missing on the underlying assumptions for the payment systems and how certain technologies could affect the possible level of privacy.

The ECB used a DLT-based solution in its pilot project. The use of “anonymity vouchers” offers a solution that could potentially be independent of the underlying Corda platform solution. In this regard, it is comparable with the use of prepaid cards already loaded with CBDC, an idea introduced by the Central Bank of Sweden [54].

Although neither can function without an underlying technical solution, be it token- or account-based, both possibly provide an interesting workaround to ensure privacy for individuals, without the need for extensive technological research that is required to ensure privacy on the ledger level. Privacy is therefore not only discussed theoretically in various papers of central banks, but also in pilot projects on a technical level. As no finding provided a list or overview of the possible levels on which privacy could be applied or ensured, it is concluded that a comprehensive overview of this subject is still missing.

8 Conclusion and Future Work

This paper evaluates both, the current theoretical work and pilot projects on central bank digital currency concerning privacy and anonymity in payments. Although privacy is a fundamental right and payment and transaction data classify as sensitive information, privacy is discussed often superficially and with no real consideration towards the user or individual. Instead, privacy is discussed as a feature that could hinder central banks' obligations to comply with KYC/AML requirements. Therefore, legal requirements and possible disadvantages of an anonymous CBDC are predominantly discussed. Possible privacy concerns of users are discussed only superficially, similarly to possible technical solutions to ensure privacy. Upon further investigation, it could be shown that several pilot projects of central banks discuss privacy in CBDC in more detail and provide first solutions to foster privacy in retail CBDC.

The current work of central banks is lacking a comprehensive overview of the possible solutions to achieve privacy, grouped by different use cases and desired design choices. The analyzed papers demonstrated that several solutions exist, from de-identification techniques that can be integrated into token-based CBDC to the use of anonymity vouchers or prepaid cards that are loaded with CBDC for both, token- and account-based CBDC. Future work could furthermore focus on individuals' privacy concerns, the desire for anonymity and trust in CBDC, and the involved stakeholders in such a payment system. Existing research on privacy concerns in established payment systems could be adapted and repeated with CBDC as a new payment system. Privacy concerns and trust issues could be researched as potential factors that might influence the adoption of CBDC by the people. Privacy should not only be seen as a feature or option but rather as a requirement that needs to be met.

9 Limitations and Contributions

This paper comes with several limitations. Concerning the review of central bank activities in this domain, not every central bank worldwide has been evaluated. Additionally, not all central banks provide information or search interfaces in English, making a review of their publications and work difficult. The search engines themselves proved to be less effective than expected. As central banks are not obliged to publish their work it is also possible that significant work on CBDC has been done internally

that was not communicated to the general public. By using a simple Google and Google News search we tried to mitigate these issues and obtained more information on pilot projects of central banks. Additionally, only information on retail CBDC has been discussed. Through the literature research, it became apparent that various central banks provide information on wholesale CBDC, for interbank payment and settlement, for which privacy should also be considered.

The paper contributes to the scientific body of knowledge of both privacy and payment systems through the identification of research gaps in those domains. The under-researched topic of CBDC, in general, was discussed with a particular focus on privacy. It was shown that privacy as a key design aspect of a CDBC has only been researched scarcely, which is surprising given the impact that the introduction of a CBDC in a country would likely have on individuals. Further research on how to protect sensitive transaction and holdings information in CBDC payments is necessary. As a managerial contribution, it was shown that a multitude of options exist to create a privacy friendly CBDC. Different central banks used different techniques, both in theory and practice, to tackle the existing issue of designing a CBDC that meets both AML/CFT requirements and the fundamental rights of individuals.

References

1. Quinn S, Roberds W (2007) The Bank of Amsterdam and the leap to central bank money. Am Econ Rev 97:262–265. https://doi.org/10.1257/aer.97.2.262
2. European Commission (2010) COMMISSION RECOMMENDATION of 22 March 2010 on the scope and effects of legal tender of euro banknotes and coins. Off J Eur Union
3. Doidge F, Bright I (2017) All aboard for the cashless society
4. Sveriges Riksbank (2018) The Riksbank's E-Krona Project Report 2
5. Nakamoto S (2008) Bitcoin: A Peer-to-Peer Electronic Cash System
6. Vasudevan R (2020) Libra and Facebook's Money Illusion. https://doi.org/10.1080/05775132.2019.1684662
7. Skingsley C (2016) Should the Riksbank issue e-krona? speech FinTech Stock 16:
8. The Economist (2020) China aims to launch the world's first official digital currency
9. South African Reserve Bank (2019) South African Reserve Bank Procurement Division - Expression of Interest
10. ECB (2020) Central bank group to assess potential cases for central bank digital currencies
11. Wandhöfer R (2017) The future of digital retail payments in Europe: A place for digital cash? J Payments Strateg Syst
12. Phillips D (2020) "Digital currency cannot be private," warns Bank of France Governor
13. Tronnier F, Recker M, Hamm P (2020) AIS Electronic Library (AISeL) Towards Central Bank Digital Currency – A Systematic Literature Review Towards Central Bank Digital Currency – A Systematic Literature Review
14. Darbha S, Arora R (2020) Privacy in CBDC technology. https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/#table1
15. ECB (2019) Exploring anonymity in central bank digital currencies. Focus

December:1–11
16. Clarke R (1999) Internet Privacy Concerns Confirm the Case for Intervention. Commun ACM 42:60–67
17. Garratt RJ, van Oordt MRC (2019) Privacy as a Public Good: A Case for Electronic Cash. Work Pap. https://doi.org/10.1017/CBO9781316658888.004
18. El Haddad G, Aimeur E, Hage H (2018) Understanding Trust, Privacy and Financial Fears in Online Payment. Proc - 17th IEEE Int Conf Trust Secur Priv Comput Commun 12th IEEE Int Conf Big Data Sci Eng Trust 2018 28–36. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00015
19. Sahnoune Z, Aimeur E, El Haddad G, Sokoudjou R (2015) Watch your mobile payment: An empirical study of privacy disclosure. Proc - 14th IEEE Int Conf Trust Secur Priv Comput Commun Trust 2015 1:934–941. https://doi.org/10.1109/Trustcom.2015.467
20. Mars A, Adi W (2019) Fair exchange and anonymous e-commerce by deploying clone-resistant tokens. 2019 42nd Int Conv Inf Commun Technol Electron Microelectron MIPRO 2019 - Proc 1226–1231. https://doi.org/10.23919/MIPRO.2019.8756734
21. Sekhar VC, Mrudula S (2012) A complete secure customer centric anonymous payment in a digital ecosystem. 2012 Int Conf Comput Electron Electr Technol ICCEET 2012 1049–1054. https://doi.org/10.1109/ICCEET.2012.6203889
22. Ben-Sasson E, Chiesa A, Garman C, et al (2014) Zerocash: Decentralized anonymous payments from bitcoin. Proc - IEEE Symp Secur Priv 459–474. https://doi.org/10.1109/SP.2014.36
23. Jayasinghe D, Markantonakis K, Mayes K (2014) Optimistic fair-exchange with anonymity for bitcoin users. Proc - 11th IEEE Int Conf E-bus Eng ICEBE 2014 - Incl 10th Work Serv Appl Integr Collab SOAIC 2014 1st Work E-Commerce Eng ECE 2014 44–51. https://doi.org/10.1109/ICEBE.2014.20
24. Leinonen H (2019) Electronic central bank cash: To be or not to be? J Payments Strateg Syst 13:20–31
25. Greco J, Thomas H (2001) Money. Understanding and Creating Alternatives to Legal Tender. Chelsea Green Publishing Company
26. Bech ML, Garratt R (2017) Central bank cryptocurrencies
27. Farell R (2015) An Analysis of the Cryptocurrency Industry. Whart Res Sch Journal Pap 130:1–23
28. Libra Association (2020) Cover Letter - White Paper v2.0. 1–29
29. Barontini C, Holden H (2019) Proceeding with caution - a survey on central bank digital currency
30. Kahn CM, Rivadeneyra F, Wong R (2018) Should the Central Bank Issue E-Money? SSRN Electron J. https://doi.org/10.2139/ssrn.3271654
31. Opare EA, Kim K (2020) A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures. IEEE Access 8:110810–110847. https://doi.org/10.1109/access.2020.3001970
32. Bordo M, Levin AT (2019) U.S. Digital Cash: Principles & Practical Steps. 1–31
33. Nabilou H, Prüm A (2019) Central Banks and Regulation of Cryptocurrencies. Rochester, NY
34. Hampl M, Havranek T (2019) Central Bank Equity as an Instrument of Monetary Policy. Comp Econ Stud. https://doi.org/10.1057/s41294-019-00092-1

35. Lannquist A (World EF (2019) Central Banks and Distributed Ledger Technology: How are Central Banks Exploring Blockchain Today? World Econ Forum
36. Bordo M, Levin A (2017) Central Bank Digital Currency and the Future of Monetary Policy. Univ Nusant PGRI Kediri
37. Vom Brocke J, Simons A, Niehaves B, et al (2009) Reconstructing the giant: On the importance of rigour in documenting the literature search process. In: 17th European Conference on Information Systems, ECIS 2009
38. Auer R, Böhme R (2020) The technology of retail central bank digital currency. BIS Q Rev 85–100
39. Boar C, Holden H, Wadsworth A (2020) Impending arrival - a sequel to the survey on central bank digital currency. BIS Pap 19
40. Bank of England (2020) Central Bank Digital Currency, Opportunities, challenges and design
41. Banque de France (2020) Central Bank Digital Currency
42. Yanagawa N, Yamaoka H (2019) Digital Innovation, Data Revolution and Central Bank Digital Currency. 1–20
43. Nuño G (2018) Monetary policy implications of central bank-issued digital currency. Econ Bull
44. Wierts P, Boven H (2020) Central Bank Digital Currency. Amsterdam, The Netherlands, The Netherlands
45. Masciandaro D (2018) Central Bank Digital Cash and Cryptocurrencies: Insights from a New Baumol–Friedman Demand for Money. Aust Econ Rev 51:. https://doi.org/10.1111/1467-8462.12304
46. Pagnotta E, Buraschi A (2018) An Equilibrium Valuation of Bitcoin and Decentralized Network Assets. SSRN Electron J. https://doi.org/10.2139/ssrn.3142022
47. Kahn CM (2018) Payment Systems and Privacy. Fed Reserv Bank St Louis Rev 100:337–344. https://doi.org/10.20955/r.100.337-44
48. Borgonovo E, Cillo A, Caselli S, Masciandaro D (2018) Between Cash, Deposit and Bitcoin: Would We Like a Central Bank Digital Currency? Money Demand and Experimental Economics. SSRN Electron J. https://doi.org/10.2139/ssrn.3160752
49. BANK N (2018) NORGES BANK PAPERS Central bank digital currencies
50. Financial Transactions and Reports Analysis Centre of Canada (2020) Money services businesses (MSBs). https://www.fintrac-canafe.gc.ca/msb-esm/msb-eng. Accessed 26 Nov 2020
51. SOV Development Foundation (2019) The Marshall Islands. https://sov.foundation/marshall-islands
52. Foundation SD (2019) The Marshallese Sovereign (SOV): Fair, Sustainable Money. https://docsend.com/view/nvi59vw
53. Central Bank of the Bahamas (2019) Project Sand Dollar :
54. Sveriges Riksbank (2018) The Riksbank's e-krona project
55. European Data Protection Board (2020) Guidelines 06 / 2020 on the interplay of the Second Payment Services Directive and the GDPR. 1–23

Appendix

Table 2. List of Central Banks and monetary authorities for which no hits could be reported

Central Bank of Azerbaijan	Central Bank of Ecuador	Central Bank of Tunisia	Central Bank of Montenegro
National Bank of Serbia	Central Bank of Egypt	National Bank of Ukraine	Central Bank of the Islamic State of the Iran
Central Bank of Bahrain	Bank of Estonia	Banco Central de Venzuela	Banco Central del Paraguay
Bangladesh Bank	Central Bank of Eswatini	Central Reserve Bank of El Salvador	The Central Bank of the Bahamas
Central Bank of Iraq	Bank Al-Maghrib (Morocco)	National Bank of Georgia	Monetary Brunei Darussalam
National Bank of Cambodia	Central Bank of Kenya	Central Bank of Hungary	Banco Central de la Republica Dominica
Banco de Cabo Verde	Central Bank of Kuwait	Central Bank of Sri Lanka Authority	Central Bank of West African States
Cayman Islands Monetary Authority	Marshall Islands Government	Saudi Arabian Monetary Authority	National Reserve Bank of Tonga
Peoples Bank of China	Central Bank of Jordan	State Bank of Vietnam	Central Bank of the Republic of Kosovo
		Bank of Jamaica	Bank of Zambia