Massachusetts Institute of Technology
Media Lab's Digital Currency Initiative
Sloan School of Management

Central Bank Digital Currency (CBDC) and Privacy

Authors: Aayushi Kaushik, Joseph Wyatt, Tianyang Xi

Keywords: Central Banks, CBDC, Privacy

Blockchain Lab Program
2019-2020 Working Groups Cycle
Taught by N. Narula, G. Gensler, and S. Johnson
Member Company: Boston Consulting Group
Project Group: CBDC and Privacy

CBDC & Privacy

1. Executive Summary

Central Bank Digital Currency (CBDC) is the fiat money in the digital format, which is established by government regulation, monetary authority or law. With the transitions of different formats that currency were used, from metal to banknotes to credit card then mobile payment, and the legality or activities of cryptocurrency have been banned by multiple countries[1], CBDC started to get more attention in late 2017[2]. Unlike the Bitcoin or other cryptocurrency that are decentralized and used globally, CBDC shares the similar characteristics as "money" that are backed by a government. Digitalization of payment has been more widely discussed since the COVID-19 pandemic[3]. While other central banks are talking about CBDC while acting towards the pandemic crisis, the People's Bank of China (PBC), the central bank for China, is already testing its toolkit in April 2020[4].

Privacy has been a huge concern in different aspects of the digital world, so is the case in the digitalization of currency. Paying with cash is the ultimate in anonymity whereas the administrator of CBDC can potentially access personal transactions. The two essential questions have been how to protect personal data at the same time enable the compliance with unconventional transaction regulations. Certain criteria need to be evaluated while designing the implementation of CBDC based on different economic and political conditions.

---

[1] Legality of bitcoin by country or territory
https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

[2] Bjerg, Ole (June 13, 2017). "Designing New Money - The Policy Trilemma of Central Bank Digital Currency". Rochester, NY. SSRN 2985381.

[3] Covid-19 could accelerate CBDC development – BIS economists
https://www.centralbanking.com/fintech/cbdc/7521206/covid-19-could-accelerate-cbdc-development-bis-economists

[4]The Economist (April 23,2020). "China aims to launch the world's first official digital currency" https://www.economist.com/finance-and-economics/2020/04/23/china-aims-to-launch-the-worlds-first-official-digital-currency

The Bank of England (BoE) is the first central bank to raise the concept of a CBDC in its 2015 research agenda[5]. The U.K. follows the General Data Protection Regulation (GDPR), that essentially gives users ownership rights over their own personal data. Therefore, BoE is still in the position of actively weighing pros and cons of CBDC[6].

Established by European Parliament and Council of the European Union, GDPR also limits the actions of European Central Bank (ECB). After evaluating the anonymity of CBDC[7], ECB released its progress of designing tiered CBDC and the financial system[8].

Discussions of a digital currency and cheaper and easier means of transferring money electronically were moving very slowly in the U.S.[9] until 2 developments 1) Facebook proposal for Libra and 2) realization China was far ahead. This has jump-started more serious work in the US with a fascinating debate on who can regulate this and whether it would be better for a US company, instead of the US government or the Federal Reserve (Fed), in the lead.

The leading position of mobile payment has put China in a better shape when coming to the talk of digital currency. China first started evaluating the CBDC implementation as early as 2014[10] and later named its digital currency Digital Currency Electronic Payment (DCEP). While DCEP has not been officially announced, Director of the Digital Currency Research Institute of the PBC, Changchun Mu has already talked about the philosophy of some settings of DCEP in his personal online classes. The Chinese approach, as one of the solutions addressing the privacy

[5] One Bank Research Agenda https://www.bankofengland.co.uk/-/media/boe/files/research/one-bank-research-agenda---summary.pdf?la=en&hash=B2C820FBF6A960C4A625C2DAB5B5B6CE4FEDF120
[6] Central Bank Digital Currency: opportunities, challenges and design https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper
[7] https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf
[8] https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf
[9] The Digitalization of Payments and Currency: Some Issues for Consideration https://www.federalreserve.gov/newsevents/speech/brainard20200205a.htm
[10] Changchun Mu (September, 2019) Libra & the Future of Digital Currency

concerns, has been, for now, the most well-demonstrated implementation of CBDC. This gave a positive sign of the possibility of a more widely implementation of CBDCs. In the current test of DCEP, we can see some assumptions have been realized, including no network signal required for transactions.

Central banks from some emerging markets, like Uruguay[11] and Organisation of Eastern Caribbean States (OECS)[12] are also in the process of actively pursuing different solutions to implement their own CBDC.

In this paper, we examine different means of financial transactions with respect to the level of privacy they afford to their users. Specifically, this paper aims to study the extent of privacy that a Central Bank Digital Currency (CBDC) can afford for its citizens.

2. Defining Privacy

To that extent, the first thing that needs to be concretized is the definition of Privacy that this paper assumes. Within the context of this paper, **Privacy** is defined as the state in which an individual's piece of information is known only to the individual themselves, and is not shared with anyone else without the individual's consent to do so. With respect to financial transactions, the pieces of information that are intended to be private include the following:

1. Individual's Identity

   This includes identifying data such as name, address, a unique identifier such as a Social Security Number (SSN) or Social Insurance Number (SIN), passport number, etcetera.

2. Individual's Transaction History

[11] Uruguayan central bank to test digital currency - Agencia EFE, 20 September 2017
[12] ECCB to Issue World's First Blockchain-based Digital Currency https://www.eccb-centralbank.org/news/view/eccb-to-issue-worldas-first-blockchain-based-digital-currency

As title. This includes information about all financial transactions that have been made to date since enrollment on the financial transaction platform.

3. Metadata associated with the Transaction

   Depending on the means of transaction, metadata associated with the transaction can assume multiple forms. For instance, a credit-card based transaction metadata can include time of transaction, name of the transactors, specifics of the goods exchanged within the transaction, location of the transactors, etcetera.

The reason why defining Privacy as above is important is because with a CBDC implementation that will be technology based, the Central Bank's (and by extension, other governmental agencies') access to the aforementioned fields becomes much easier than it is presently. Tying an individual's financial information to their identity, in turn, allows the government to surveil the public closely.

In addition to the aforementioned definition of Privacy, this paper assumes that a CBDC implementation would result in complete removal of fiat currency, thus making the quandary about Privacy possible. Additionally, for the purposes of this paper, the Central Bank adopts a 'retail CBDC' model. Defined more in detail by Auer and Bohme 2020, a key aspect of the retail CBDC model is that the Central Bank is the entity that generates and dispenses CBDC to the citizens.

3. Privacy issues from User perspective and Policy Perspective around data driven CBDC

Different from traditional banknotes, CBDC has the nature of allowing payment instruments to obtain various information and data attached to payments and transactions[13].The privacy issues

[13] Noriyuki Y. and Hiromi Y., Digital innovation, data revolution and Central Bank Digital Currency, Bank of Japan Working Paper Series, 2019.

of the data driven CBDC could be decreased by applying technologies such as the blockchain. On the other hand, there are also lots of voices that implementing CBDC would allow the law department to have more approaches to solve problems such as money laundering and tax evasion. For instance, the recently issued Chinese CBDC has considered the prevention of tax evasion as one of the advantages of CBDC[14]. Consequently, to demonstrate and clarify privacy issues of CBDC, which would involve the manipulation of big data attached with the digital currency, there are several aspects we should put into consideration first for further insights. Here, we analyze and present privacy issues of CBDC from three different perspectives consisting of the stakeholders, the users, and the policy.

3a. Stakeholders

The implementation of a central bank digital currency would impact several different parties, each with their own preferences and needs when it comes to digital transactions. Given this paper's focus on privacy, as part of our framework we sought to delineate who these stakeholders are and outline their preferences from a privacy perspective. Our recommendation requires understanding and accommodating the preferences of the various stakeholders involved. We seek to recommend the best possible implementation of a CBDC from a privacy perspective, or at least more deeply understand the key tradeoffs being made and at which stakeholder's expense.

We identify five primary stakeholders whose privacy preferences to consider:

1. User (Citizen)
2. Issuer (Central Bank)
3. Law Enforcement (AML/CFT agencies)

[14] https://voxeu.org/article/benefits-central-bank-digital-currency, May 10th, 2020 accessed.

4. Bank or PSP (Administrator)
5. Receiver (another user or merchant)

We will now delve into them individually.

3a. 1. User

The user is the individual who operates the digital wallet and owns the monies within. As stated previously we believe the user is generally focused on protecting his/her financial data as much as possible. Citizen privacy preferences may vary by country and citizens have become as accustomed to trading some privacy for access, convenience, or innovation depending on the product in question. In general, we assume the ideal solution would be akin to digital cash where value is transferred easily without any of the user's personal or financial information being disclosed.

3a. 2. Issuer

The issuer is the entity that creates the liability that the user has a claim against. In the case of a CBDC this is ostensibly the central bank issuing the currency. The privacy preferences of a central bank can vary depending on the country, mandate, degree of independence, legal framework of the central bank, whether it has control of the payment system of a country, etc.

In order to have more clarity on this point the authors of this paper are in the process of interviewing various central bankers to hear their perspective more directly. However, in the absence of these interviews we make a few underlying assumptions on central banks' privacy preferences. We acknowledge that the main priority is keeping the sovereign currency central to the financial system, carrying out its mandate, and maintaining financial stability. We assume the central bank is open to as private CBDC implementation as possible to the extent that it does not interfere with these key priorities.

Therefore, how other stakeholders respond may influence the central bank's approach to privacy to the extent it disrupts its obligations in other key priorities. For example, if citizens don't view the CBDC as private enough they may turn to a corporate or crypto currency, detracting from the priority of keeping the sovereign currency central. While monitoring the flow of money across the economy can better inform a central bank's monetary policy actions and timing to carry out its mandates, it could also invite encroachment on central banker independence by law enforcement agencies—impairing a central bank's ability to effect its mandate. If a private CBDC housed a central bank proves too popular it could disrupt financial stability if commercial banks experience bank runs. Ultimately our assumption is the central bank errs on the side of citizen privacy with a few caveats.

3a. 3. Law Enforcement

Law enforcement includes government agencies responsible for anti-money laundering, countering terrorist finance, as well as collecting taxes. In the United States this would be the Justice Department, Department of Defense, and Internal Revenue Service. Given the history of cases pertaining to individual privacy outlined above from a policy perspective we assume these agencies would gravitate toward any data source which augments their ability to carry out their responsibilities. Thus, they have a natural preference for less citizen privacy. Accordingly, the type of data a potential CBDC collects, who owns the data, and the legal framework surrounding it is critical for determining the degree of privacy from government surveillance a user would have.

3a. 4. Bank of PSP

This category includes the owners and managers of payment systems. This includes a vast array of companies beyond banks and payments service providers, but also credit card companies and the SWIFT network. While all these companies provide different types of services with respect

to payments we can align into a single category because they agree when it comes to user privacy in our view. Personal financial data is essential for conducting their primary business functions and cybersecurity, but they also either sell data or make their user available for targeted marketing by third parties. Therefore, we believe banks et. al. would be interested in managing CBDC accounts similarly to the way they manage existing accounts.[15] We rely on the 2016 study looking at US banks privacy practices around customer data to inform us on how users' financial data is utilized for cross-selling and third-party marketing which is beyond what the primary services the bank offers its customers.

3a. 5. Receiver

The receiver is the person or entity at the other end of the initiated transaction, likely a friend or merchant. In the case of the merchant the business model relies on customer study and targeting which is not possible if no identifying information is gathered from a customer upon purchase. Thus, we believe the merchant is similarly aligned with the bank in preferring access to useful customer information for future targeting, unlike with a cash transaction when no information about the customer is available.

In sum we evaluate each of the various conceivable CBDC implementations through the lens of the various stakeholders in reaching our recommendation. We consider how the various features accompanying each implementation impacts the preference of the stakeholders above.

3b. User Perspective on Privacy

Based on a survey conducted by BCG (Boston Consulting Group)[16], 30% of users across all the countries surveyed including Spain, France, Italy, UK, Germany, and US, believe that

[15] Cranor, Lorrie Faith, et al. "A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices." *ACM Transactions on the Web*, vol. 10, no. 3, 2016, pp. 1–33., doi:10.1145/2911988.
[16] John R., Alexander L., Elias B., Bridging the trust gap in personal data, The Boston Consulting Group, 2018.

companies aren't honest about data use. The users' concern on data misuse is obvious even in organizations related to financial, technological, and government services. Consequently, the adoption of CBDC would bring more concerns around data privacy to users since its data driven nature compared with traditional banknotes and cash. Moreover, further discussion on how to prevent data misuse for a possible CBDC scheme is extremely required.

Furthermore, users also need more intrusions on data policy, how their data will be used based on the CBDC scheme and related policy. Through methods such as regular emails and regular phone calls, users are allowed to achieve more transparency of their private data's use. Users should be informed of the latest metrics timely when perceptions of other entities have been adjusted.

On the other hand, personal data sharing to some extent would allow the law department, the central bank and other entities to have resources to track down any malicious behavior, thus protecting users' data privacy as well as achieving an optimal balance of the safety of the CBDC's payment instruments and effective use of data.

3c. Policy Perspective

The last important piece to cover is how the three different branches of the government have dealt with Privacy in the past, since this is an indicator of future actions. To that extent, we looked at examples of how the Judiciary has ruled when dealing with the executive branch's demand for user data from private companies. Secondly, we look at how the legislative branch has ruled when it comes to collection of citizen data. For the purposes of this paper, we focus on the US government.

With respect to the Judicial system's stance, there are two landmark cases that come to light. The first dispute is between Apple and FBI, wherein the latter has repeatedly asked Apple to help unlock a device that is protected by Apple's encryption[17]. Whereas within the San Bernardino case FBI withdrew its request; in a separate case a judge also ruled that the All Writs Act could not be used as valid ground to force Apple to unlock the device [17].

In the second dispute of *United States v New York Telephone Co.*, however, Supreme Courts cited the All Writs Act to "give courts the power to demand reasonable technical assistance from the phone company in accessing phone call records" [17], ruling against private companies and citizen privacy.

Secondly, with respect to the legislative branch, we can look at the Foreign Intelligence Surveillance Act as an example. Effective since 2008 and initially intended to expire in 2012, the act has since been extended twice, under two different administrations. Note that this act has been the legal basis for surveillance programs such as PRISM[18].

Overall, the important result that we gleaned after researching the US government's stance on accessing citizens' privacy data is that the government errs on the side of having as much data as possible, 'for the sake of homeland security'. While the intention is valid, this creates a tension between citizens who are privacy conscious and the government.

4. Framework used to assess CBDC Implementations

4a. Criteria within the Framework and best possible values of these criteria

[17] FBI-apple Encryption Dispute https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute

[18] Foreign Intelligence Surveillance Act Of 1978 Amendments Act Of 2000 https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978_Amendments_Act_of_2008#Legislative_history

To assess various CBDC implementations from a privacy perspective, we used a predetermined list of criteria that was extracted from the definition of privacy used within this paper. Additionally, this list of criteria was informed by features of a CBDC implementation. The following paragraphs delve into the list of criteria and the best possible values for these criteria from a privacy perspective.

1. Who issues this currency?

By definition, the currency would have to be issued by the Central Bank for it to qualify as Central Bank Digital Currency.

2. Who is the Account Administrator?

The Account Administrator would be the entity in charge of running the individual accounts that citizens own. From a privacy perspective, we believe that the best entity to be the Account Administrator would be the Central Bank itself. This limits the number of entities that have access to the Users'/citizens' data.

3. Who is the Infrastructure Administrator?

The Infrastructure Administrator would be the entity that is responsible for maintaining the technical implementation (software, hardware, and networking components). Similar to the reasoning for Account Administrator, we recommend that the Central Bank be responsible for Infrastructure Administration.

4. Who owns the User Identity Data?

From a privacy perspective, we recommend that three entities be allowed access to the user data. By default, the User has access to their own Identity data. Additionally, due to KYC and AML compliance, the Central Bank would also need access to the User Identity Data to be able to establish the User account. Lastly, the third entity that *may* be allowed access to the User Identity Data would be Law Enforcement. This data access should occur only if a transaction within a user account or the account itself is flagged as a result of KYC and AML laws.

5. Which entities are User Balance and Transaction History visible to?

We recommend that the User be the only entity that the User Balance and Transaction History are visible to. However, similar to User Identity Data, User Balance and Transaction History may be shared with the Central Bank and Law Enforcement agencies in case of an issue flagged under KYC and AML.

6. Who collects, stores, and examines the Metadata?

As established within the section that examines government surveillance policies and stances, the best form of ensuring privacy of data would be to avoid collection in the first place. As a result, from a privacy perspective, we recommend that metadata not be collected in the first place unless it is required to be collected by laws and policies currently in place.

7. Is the User anonymous to the receiver?

To be able to keep the same privacy level as afforded by fiat currency, we recommend that this decision be dependent on the nature of the transaction. Unless revealing the identity is crucial for the transaction to process, the User should get to decide whether they would like to disclose their identity.

8. Does the Central Bank (or Infrastructure Administrator) have the right to share User data with a third-party entity?

From a privacy perspective, we recommend that no right is afforded to the Central Bank or the Infrastructure Administrator to share User data with a third-party entity.

9. Will the data allow for targeted marketing/ads?

Similar to the previous criterion, we recommend that targeting Users for marketing/ads based on User data be disallowed.

4b. Enumeration of all possible values for criteria and selection on the basis of 4a

The following figure enumerates different possible versions of CBDC (and non-CBDC) implementations, as well as the values that the list of criteria can assume.

	Options for Transferring Value																			
Privacy Spectrum	Respected by default and all circumstances								Respected by default, except in case of legal requirements											Full Transparency
CBDC?				CBDC	CBDC	CBDC	CBDC	CBDC	CBDC	CBDC	CBDC	CBDC	CBDC	CBDC	CBDC	CBDC				CBDC
Currency issuer	Central Bank	Permissionless	Permissionless	Central Bank	Central Bank	Central Bank	Central Bank	Central Bank	Central Bank	Central Bank	Central Bank	Central Bank	Central Bank	Central Bank	Central Bank	Bank of Kenya	Facebook & Co.	Central Bank	Central Bank
Account Administrator	User	Varies	Varies	User	User	User	User	Central Bank	Central Bank	Central Bank	Central Bank	Central Bank	Bank or PSP	Bank or PSP	Bank or PSP	Safaricom	Facebook & Co.	Bank or PSP	Central Bank
Infrastructure Admin	n/a	Varies	Varies	Central Bank	Bank or PSP	Central Bank	Bank or PSP	Central Bank	Central Bank	Central Bank	Central Bank	Bank or PSP	Bank or PSP	Bank or PSP	Bank or PSP	Safaricom	Facebook & Co.	Bank or PSP	Central Bank
	Cash (physical notes)	Monero and Zcash	Bitcoin	Full anonymity (direct + tokenized)	Full anonymity (indirect + tokenized)	Full anonymity (direct + tokenized + AML/CFT compliant)	Full anonymity (indirect + tokenized + AML/CFT compliant)	CB retail account (Direct + account)	CB retail account (Direct + account)	CB retail account (Direct + account)	CB retail account (Direct + account)	Hybrid infrastructure (Indirect + Account)	Typical retail infrastructure w/o mktg (Indirect + Account)	Typical retail infrastructure w/ mktg option (Indirect + Account)	Typical retail infrastructure (Indirect + Account)	MPesa (B = Safaricom)	Libra (B = Facebook)	Normal bank retail account	Direct CBDC; full transparency
Feasible or not? (Reason)				no (no AML/CFT)	no (no AML/CFT)	yes	yes	yes	yes	yes	yes	yes	no (finance special interest)	yes	yes				no (citizens won't tolerate/adopt)
List of data types																			
User Identity (i.e. KYC)	U only	U only	U only	U only	U only	U, L*	U, L*	U, CB, L*	U, CB, L*	U, CB, L*	U, CB, L*	U, CB, L*	U, B, L*	U, B, L*	U, B, L*, M	U, B, L*,	U, B, L*, M	U, B, L*, M	U, CB, L, M
All user transaction and balances	U only	U only	U only	U only	U only	U only	U only	U only	U, CB	U, CB, L	U, CB, L	U, CB	U, B	U, B	U, B	U, B	U, B	U, B	U, CB, L
AML and CFT flag transactions						L	L	L	CB, L	CB, L	CB, L	CB, L	B, L	B, L	B, L	B, L	B, L	B, L	CB, L
Metadata											CB			B	B	B	B	B	CB
Anonymous to receiver (U = user consent required)	yes	yes	yes	yes	yes	yes	yes	no	no	no	no	no	no	no	no	no	no	no	no
Data sharing option (U = user consent required)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	no	no	no	U		no	U	yes	yes	yes	yes	yes
Target mktg for 3rd parties	n/a	n/a	n/a	n/a	n/a	n/a	n/a	no	no	no	CB, M		no	B, M	B, M	B, M	B, M	B, M	CB, M

The table on the previous page represents the various enumerations of the listed criteria. These enumerations decreasingly favor User privacy as the table columns are traversed from left to right. Additionally, there are a few implementations that as a result of the enumerations values are disqualified as CBDCs.

On the basis of our list of criteria and their best possible values, we recommend the darkest green column, which would be a Central Bank run Direct User Account. In such an implementation, the Central Bank is responsible for building and administering the technical infrastructure. Additionally, the only entity other than the Central Bank and the User who may access User Identity Data would be the Law Enforcement agencies. Such an access would happen if a transaction or account gets flagged under KYC/AML laws.

4c. Evaluation of ongoing CBDC projects

Given our recommendation for the CBDC implementation which best serves the privacy of the user we can infer the privacy priorities of various countries from the status of their plans around CBDC. A March 2020 paper written by Raphael Auer and Rainer Böhme of the BIS explaining the potential structure of a CBDC explored how 24 countries could classify their ongoing projects and research.[19] We will inspect these 24 countries and a few others through our privacy framework lens.

Firstly, we concede that the details of an individual countries' implementation are not entirely clear and where a country is leaning with respect to privacy in its research is also not without ambiguity. Our hope is that the privacy framework offers a different perspective on this

[19] Auer, Raphael, and Rainer Böhme. "The Technology of Retail Central Bank Digital Currency." *BIS Quarterly Review*, Mar. 2020.

ongoing process and potentially becomes another layer through which CBDC progress is evaluated even though the process remains far off despite efforts being catalyzed by China's leadership in launching a CBDC and the Covid-19 pandemic putting the prospects of a CBDC more center-stage. Our CBDC privacy evaluation broadly places countries into four distinct groups:

1. Soft Rejectors: countries which have for the time being decided against moving forward with a CBDC
2. Active Researchers: countries whose plans remain unclear and are actively evaluating a whole range of potential CBDC implementations.
3. Active implementers: countries who are currently piloting or have piloted a CBDC
4. China: as the current lead in the CBDC implementation field, China has been allotted its own category at this time

We now delve into the distinct groups.

1. Soft Rejectors

This list currently includes Australia[20], New Zealand[21], Denmark[22], Switzerland[23], and Israel[24]. These countries may still take part in research to some degree, but have clearly stated that they view the risk as outweighing the benefits and have little to no interest in launching a CBDC

[20] Cook, S., 2020. *Australia Disapproves Idea Of CBDC*. [online] CryptoNewsZ. Available at: <https://www.cryptonewsz.com/australia-discards-the-idea-of-central-bank-cryptocurrency/> [Accessed 11 May 2020].
[21] Bascand, Geoff. "The Point Conference." The Point Conference. 11 May 2020, Auckland.
[22] Gürtler, Kristen, et al. "Central Bank Digital Currency in Denmark?" *DANMARKS NATIONALBANK*, https://www.nationalbanken.dk/en/publications/Pages/2017/12/Central-bank-digital-currency-in-Denmark.aspx.
[23] Aki, J., 2020. *Swiss Government To Take A Cautioned Approach To CBDC - Insidebitcoins.Com*. [online] InsideBitcoins.com. Available at: <https://insidebitcoins.com/news/swiss-government-to-take-a-cautioned-approach-to-cbdc/244218> [Accessed 11 May 2020].
[24] Ullah, S., 2020. *Bank Of Israel Rejects Central Digital Currency*. [online] The Tradable. Available at: <https://thetradable.com/bank-of-israel-rejects-central-digital-currency/> [Accessed 11 May 2020].

any time soon. These are generally smaller and homogeneous countries with an advanced financial infrastructure and under-banked populations. The citizens have no demand for a CBDC as the current system serves them sufficiently. In our view the decision to reject a CBDC implicitly chooses for citizens to remain subject to the financial surveillance endemic to private enterprise offerings as cash continues to fall out of favor.

2. Active Researchers

This list houses the vast majority of countries and for example includes Sweden, ECB countries, the United States, Brazil, Norway, Canada, England, Japan, and India. Again, the statement of public officials here has generally been mixed (with some like Sweden and Japan potentially qualifying for soft rejectors), but these countries are actively engaged in individual or collaborative research on the topic. Given all the various types of implementations are in play it is too early to say where this group falls from a privacy perspective.

3. Active Implementers

These countries have implemented a live project or pilot, thereby revealing their positions regarding privacy to some degree. The group includes Cambodia[25], The Bahamas[26], The Eastern Caribbean Currency Union[27], Ecuador, South Africa[28], and Uruguay[29]. Generally, these countries

[25] Ledger Insights - enterprise blockchain. 2020. *Cambodia To Launch Digital Currency, DLT Based Interbank Payments - Ledger Insights - Enterprise Blockchain*. [online] Available at: <https://www.ledgerinsights.com/cambodia-central-bank-digital-currency-dlt-payments/> [Accessed 11 May 2020].
[26] Thebahamasinvestor.com. 2020. *Interest Growing In Sand Dollar Project - Video | The Bahamas Investor*. [online] Available at: <http://www.thebahamasinvestor.com/2020/interest-growing-in-sand-dollar-project-video/> [Accessed 11 May 2020].
[27] 2020. [online] Available at: <https://www.eccb-centralbank.org/news/view/eccb-to-issue-worldas-first-blockchain-based-digital-currency> [Accessed 11 May 2020].
[28] Ashar, J., 2020. *South Africa Reserve Bank Wants To Test CBDC Based On Native Currency - The Global Treasurer*. [online] The Global Treasurer. Available at: <https://www.theglobaltreasurer.com/SARB-wants-to-test-CBDC-based-on-native-currency> [Accessed 11 May 2020].
[29] Bergara, Mario, and Jorge Ponce. "Central Bank Digital Currency: The Uruguayan E-Peso Case."

had greater incentive to launch a CBDC as an effort to make their own sovereign currencies more central to their financial systems. In many cases these countries have experienced dollarization.

Additionally, in many cases these are cash-based economies for which private enterprise has not offered a digital solution so the government has chosen to enter that space. Despite this underlying rationale, there are relative clear privacy decisions made with the choice of either a direct or indirect implementation.

Ecuador, South Africa, the Bahamas, and Uruguay all opted for a direct solution while the ECCB and Cambodia have chosen to go indirect. While information is limited Ecuador, South Africa, and the Bahamas seem to allow for a lot of visibility of transactions for the central government. In fact, citizens' lack of trust of the Ecuadorian government likely contributed to the failure of its 2014 pilot[30]. Cambodia's and the Eastern Caribbean Countries' decision to collaborate with financial institutions may be suboptimal from a privacy perspective, but could still be effective implementations for those countries.

4. China

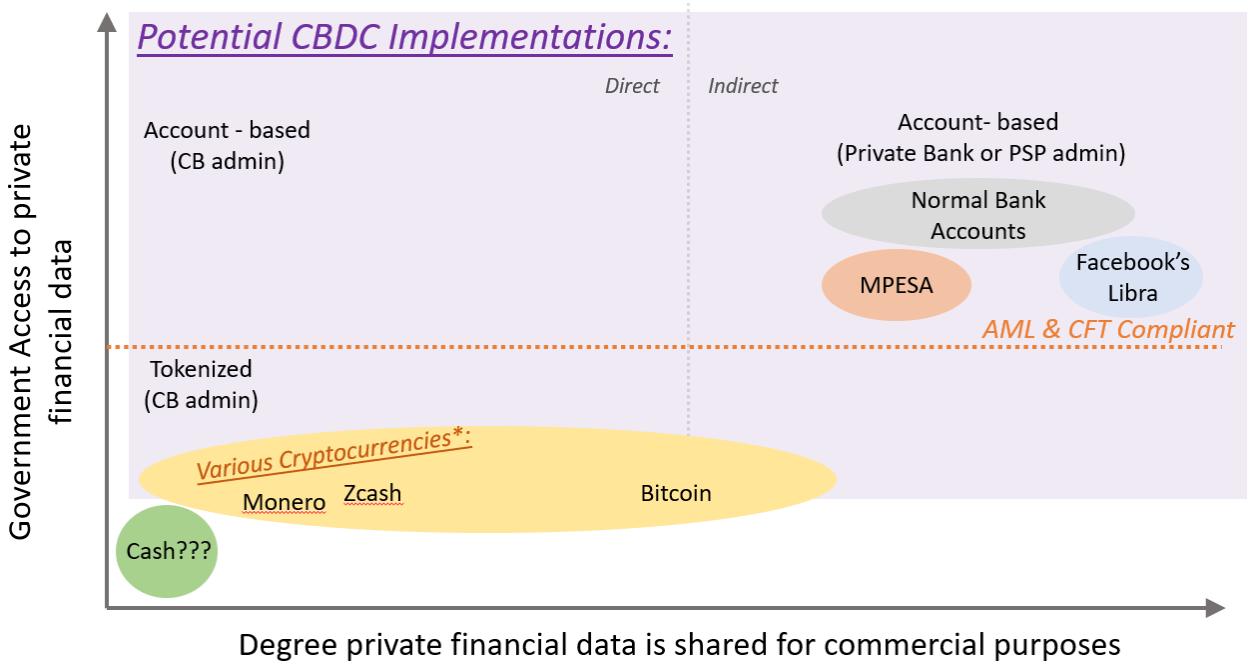
China is the leader with plans to test run it's CBDC DCEP in four cities[31]. Unlike the other countries in the third category it's already very advanced in digital payments with WeChat and Alipay. The official stated reason for offering a CBDC is for the population to have non-cash options outside of Alipay or WeChat, essentially competition for private enterprise as physical cash falls out of favor. Also, China's intention to carve more space for itself as a future reserve currency is well known. China claims to have two types of DCEP wallets[10]. One is through a bank

[30] White, L., 2020. *The World's First Central Bank Electronic Money Has Come - And Gone: Ecuador, 2014-2018 - Alt-M*. [online] Alt-M. Available at: <https://www.alt-m.org/2018/03/29/the-worlds-first-central-bank-electronic-money-has-come-and-gone-ecuador-2014-2018/> [Accessed 11 May 2020].
[31] Jia, C., 2020. *Digital Currency Trials Are Underway*. [online] English.gov.cn. Available at: <http://english.www.gov.cn/statecouncil/ministries/202004/21/content_WS5e9e4e02c6d0b3f0e949603f.html> [Accessed 11 May 2020].

and the other is through one's phone. The second may be anonymous for the bank, but neither is anonymous from a government perspective. The Chinese DCEP offers both an indirect and direct option, but neither are particularly private from the government though the direct one is more private from commercial interest as our framework suggests.

5. Privacy Spectrum used to assess CBDC Implementations

5a. Plotting implementations from a User Perspective



Our definition of privacy looks at protecting personal financial data. We have attempted to simplify our spectrum of potential CBDC implementation through representing the landscape of privacy graphically. Of the two axes, the x-axis represents the degree to which an individual's financial data is available for use by commercial interest in areas other than why the user provided the data in the first place (e.g. third-party marketing). The y-axis is the degree to which the

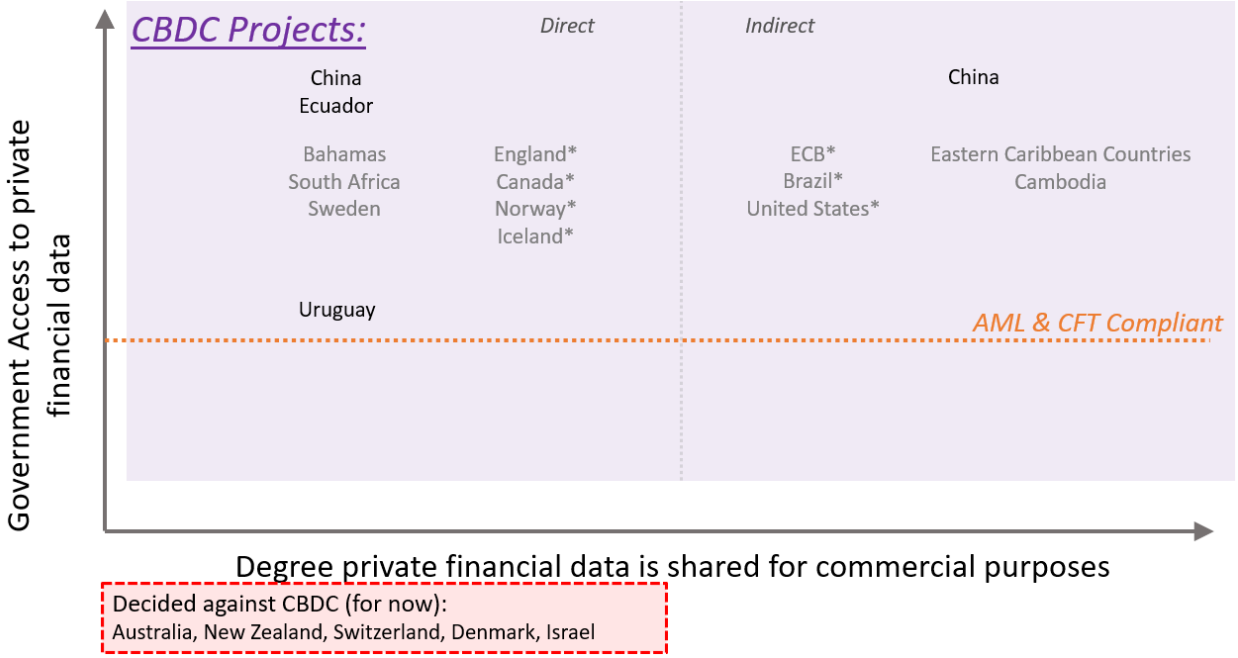
government can monitor individuals' personal financial life. Notably in the middle of the y-axis we have the AML & CFT threshold where an individual's identity is made available for legal reasons to combat money laundering and terrorist financing.

On this chart we have placed various forms of holding and transferring value and have made general determinations on where these stand privacy-wise. At the origin we have physical cash, the original bearer instrument where no identifying information or metadata is created if two parties choose to transact. Next to cash we have the various forms of cryptocurrency which have varying degrees of privacy depending on how they are accessed. We note that in general monero and zcash are less traceable than Bitcoin. On the right side and above the AML & CFT threshold we have normal bank accounts, Safaricom's MPESA, and potentially Facebook's Libra. All of these accounts provided by third parties require the user to provide their identity and allow their transaction data to be monitored by the company offering the service. This convenience comes with a price of user data likely being made available for marketing purposes.

The purple box represents the entire spectrum of possible CBDC implementations. We highlight three main categories. We have the account-based indirect option where the user's CBDC wallet is essentially managed by a bank or PSP much like the existing digital banking options. On the left we have the direct option where the user banks with the central direction. Below the AML & CFT line we have the token-based options. This option would be the most anonymous, but unlikely to be implemented given it would not require identity in order to transact and therefore likely not legally feasible, though worth highlighting.[32]

[32] Culligan, A., 2020. *Token Or Account Based CBDC? - SETL Blog*. [online] SETL Blog. Available at: <https://setl.io/blog/token-or-account-based-cbdc/> [Accessed 11 May 2020].

5b. Plotting specific country projects on the Privacy Spectrum



As detailed above, the privacy specifics of various countries' CBDC research and projects remain fairly unspecified. Despite this we believe it is useful to attempt to plot where countries currently sit when it comes to privacy and their potential and existing CBDC implementations. We expect that further research (including but not limited to our pending central banker interviews) will add clarity to this question.

We have a rough sketch of where countries generally fall on the privacy spectrum based on our current research. Countries in black font are those where we feel we have higher degree of certainty vs the many in grey. As discussed previously the first criteria we look at in determining privacy is the degree that a user's financial data is protected from commercial interest and exploitation. Based on this logic we view a direct implementation as more private from commercial interest by definition and therefore we place countries that are leaning towards a direct implementation on the left side of the graph and indirect leaning countries on that right and further

along the x-axis. When it comes to government access, we assume every country has implemented or would implement a CBDC structure that achieves the baseline level of AML & CFT compliance, however the degree of government surveillance beyond that is unclear. This explains why many countries remain grey because the level and ease of government access to private financial data is opaque at this time.

We do note that Ecuador's 2014 project gave the government substantial visibility into private citizens' financial lives which is why it is plotted further north. Also the description of China's DCEP also appears to afford the government extremely effective monitoring capabilities whether the citizen chooses the "controlled anonymous" option linked to a cell phone or chooses to link the wallet directly to their bank account. We have Uruguay close to the AML & CFT line and thus assume a higher level of anonymity for citizens given the model country used in the 2017 e-Peso pilot.

6. Recommendations

After evaluating the ongoing CBDCs, let's go back to our framework. To address the privacy concerns, we give the following recommendations. As a fiat currency, CBDC should be able to serve the compliance of AML and KYC.

One of the first ways to filter is allowing target marketing for 3rd parties. Depending on whether this is a world where the infrastructure is a retail CBDC model, wherein the Central Bank issues currency directly to citizens with no other banks or PSPs being present in the architecture), this problem becomes easier to resolve. Allowing other banks to remain allows the current banking infrastructure to have some presence in the future and removes the onus of delving into direct to customer banking from the Central Bank. However, at the same time, it also removes the benefits that CBDC has to offer, such as helicopter money. Central bankers

raised concerns about taking on the burden of dealing with citizens directly as compared to keeping the current infrastructure10. A large country like China has a large population, and the economic development, resource endowment, and population base of each place are quite different. Introducing the 3rd party adds more flexibility to the system and avoids the central bank to face all consumers in the country. It also gives the Central Banks more control over fiscal policy. From the privacy perspective, a direct to consumer model allows a more efficient and transparent structure in place that removes third party marketing and data scraping opportunities. The public perception of whether their data is safe from surveillance of certain parts of the law and whether it really matters as the legislation of the government surveillance ex-post a direct CBDC implementation matter. From only the privacy perspective, we are now focusing on retail CBDC that does not allow third party data collection or sharing.

The next filter that can be applied is the AML and CFT flag transactions. This row details who can access the account details and the flagged info in case of an alert. Central banks should be aware and involved in handing over the information to law services, as opposed to them having complete access to the identification data) to avoid any possible data abuse and privacy breach. In case of multiple accounts, this also allows central banks to deal with other accounts. If data is to be exposed, more oversight would be better than just one entity, in the sake of law enforcement, dealing with the data. This also allows an inbuilt data ‘protector’/ ‘checker’ to exist in the form of the central bank.

The third filter to apply would be information about specific transactions and balances. Only the user should be allowed to see their transactions and balances. We have lived in the current system where the central bank has been functioning well without seeing user level

account data, unless it is flagged. From a privacy perspective, only the user needs to know their account balance and transactions.

The last distinction happens within the implementation should be a retail or a hybrid infrastructure. Assuming that the hybrid infrastructure ownership does not lie with a third party, the two options are identical from a privacy perspective. As in our framework, the dark-green columns are our recommendations.

6. Conclusion

With the digitalization of traditional financial approaches, the CBDC (Central Bank Digital Currency) is attracting more and more attention. However, accompanied by the implementation of CBDC, the data driven nature of it brings about more considerations on data privacy before a secure and feasible solution could be reached. Besides, the advancement of information technologies with respect to decentralized data such as blockchain and cybersecurity[33] is considered to bring more resilience for future CBDC implementations.

In this research, first we demonstrate the definition of privacy, which is related to various types of private data. Then as we discussed above, CBDC allows easier access to users' identity tied with individuals' financial information, on the other hand, allowing the government law department to have more resources to surveil the public closely. Moreover, privacy issues possibly caused by the CBDC are presented from three different perspectives including the stakeholders, the users, and the policy. A framework based on a list of criteria which is informed by features of a CBDC implementation is adopted for evaluating each implementation option. Furthermore, with respect to countries who are already actively implementing the CBDC, we analyzed these specific

[33] Yuwei Sun, Hideya Ochiai, Hiroshi Esaki. Intrusion Detection with Segmented Federated Learning for Large-Scale Multiple LANs. IEEE World Congress on Computational Intelligence (WCCI), 2020.

country projects using a privacy spectrum, showing the extent of government access to private financial data and the extent of these data being shared for commercial purposes. Besides, countries with various opinions on the implementation of CBDC have been given out for further understanding of the feasibility of it.

At last, we proposed our recommendations for possible CBDC implementation of a retail or hybrid CBDC model that meets the compliance of AML and KYC, enables AML and CFT flag transactions but limits the access to specific transactions and balances and forbids third party data collection or sharing .For future research, an evaluation based on questionnaire and interviews with central bankers and other experts could be considered, by which we could achieve more insights on the feasibility and robustness of our implementation.

Appendix

Resource Report

We'd like the thank the thoughtful contributions of Prof. Simon Johnson, Prof. Gary Gensler, Neha Nerula, Prof Athanasios Orphanides, and Robleh Ali

Auer, Raphael, and Rainer Böhme. "The Technology of Retail Central Bank Digital Currency." *BIS Quarterly Review*, Mar. 2020.

Cranor, Lorrie Faith, et al. "A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices." *ACM Transactions on the Web*, vol. 10, no. 3, 2016, pp. 1–33., doi:10.1145/2911988.

Cook, S., 2020. *Australia Disapproves Idea Of CBDC*. [online] CryptoNewsZ. Available at: <https://www.cryptonewsz.com/australia-discards-the-idea-of-central-bank-cryptocurrency/> [Accessed 11 May 2020].

Bascand, Geoff. "The Point Conference." The Point Conference. 11 May 2020, Auckland.

Gürtler, Kristen, et al. "Central Bank Digital Currency in Denmark?" *DANMARKS NATIONALBANK*, https://www.nationalbanken.dk/en/publications/Pages/2017/12/Central-bank-digital-currency-in-Denmark.aspx.

Aki, J., 2020. *Swiss Government To Take A Cautioned Approach To CBDC - Insidebitcoins.Com*. [online] InsideBitcoins.com. Available at: <https://insidebitcoins.com/news/swiss-government-to-take-a-cautioned-approach-to-cbdc/244218> [Accessed 11 May 2020].

Ullah, S., 2020. *Bank Of Israel Rejects Central Digital Currency*. [online] The Tradable. Available at: <https://thetradable.com/bank-of-israel-rejects-central-digital-currency/> [Accessed 11 May 2020].

Ledger Insights - enterprise blockchain. 2020. *Cambodia To Launch Digital Currency, DLT Based Interbank Payments - Ledger Insights - Enterprise Blockchain*. [online] Available at: <https://www.ledgerinsights.com/cambodia-central-bank-digital-currency-dlt-payments/> [Accessed 11 May 2020].

Thebahamasinvestor.com. 2020. *Interest Growing In Sand Dollar Project - Video | The Bahamas Investor*. [online] Available at: <http://www.thebahamasinvestor.com/2020/interest-growing-in-sand-dollar-project-video/> [Accessed 11 May 2020].

2020. [online] Available at: <https://www.eccb-centralbank.org/news/view/eccb-to-issue-worldas-first-blockchain-based-digital-currency> [Accessed 11 May 2020].

Ashar, J., 2020. *South Africa Reserve Bank Wants To Test CBDC Based On Native Currency - The Global Treasurer*. [online] The Global Treasurer. Available at: <https://www.theglobaltreasurer.com/SARB-wants-to-test-CBDC-based-on-native-currency> [Accessed 11 May 2020].

Bergara, Mario, and Jorge Ponce. "Central Bank Digital Currency: The Uruguayan E-Peso Case."

White, L., 2020. *The World's First Central Bank Electronic Money Has Come - And Gone: Ecuador, 2014-2018 - Alt-M*. [online] Alt-M. Available at: <https://www.alt-m.org/2018/03/29/the-worlds-first-central-bank-electronic-money-has-come-and-gone-ecuador-2014-2018/> [Accessed 11 May 2020].

Culligan, A., 2020. *Token Or Account Based CBDC? - SETL Blog*. [online] SETL Blog. Available at: <https://setl.io/blog/token-or-account-based-cbdc/> [Accessed 11 May 2020].

Brainard, Lael. "Symposium on the Future of Payments." Symposium on the Future of Payments. 12 May 2020, Stanford.

Jerome Powell Senate Testimony February 2020

Cœuré, Benoît, and Jacqueline Loh. "Committee on Payments and Market Infrastructures." *Bank for International Settlements*, Mar. 2018.

"Central Bank Digital Currencies." *Wikipedia*, Wikimedia Foundation, 19 Apr. 2020, www.wikipedia.org/.

Alexandre, Ana. "Private Payment System for Central Bank Digital Currency Possible, Says ECB." *Cointelegraph*, Cointelegraph, 17 Dec. 2019, cointelegraph.com/news/private-payment-system-for-central-bank-digital-currency-possible-says-ecb.

Ward, Orla, and Sabrina Rochemont. "Understanding Central Bank Digital Currencies (CBDC)." *Institute and Faculty of Actuaries*, Mar. 2009, https://www.actuaries.org.uk/system/files/field/document/Understanding CBDCs Final - disc.pdf.

Harper, Jim. "Jim Harper." *Cayman Financial Review*, 24 May 2016, www.caymanfinancialreview.com/2016/05/23/security-vs-security-the-trade-offs-in-financial-surveillance/.

"Central Bank Digital Currency: Opportunities, Challenges and Design." *Bank of England*, 28 Feb. 2020, www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper.

"Contingency Planning for a Central Bank Digital Currency." *Bank of Canada*, www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency/#Scenario-2-Private-digital-currencies.

Adam, David, et al. "CENTRAL BANK DIGITAL CURRENCY." *Banque De France*, https://publications.banque-france.fr/sites/default/files/media/2020/02/04/central-bank-digital-currency_cbdc_2020_02_03.pdf.

Koning, JP. "Approaches to a Central Bank Digital Currency in Brazil." *R3 Reports*, 18 Oct. 2018, https://www.r3.com/wp-content/uploads/2018/11/CBDC_Brazil_R3.pdf.

"Exploring Anonymity in Central Bank Digital Currencies." *European Central Bank Eurosystem: In Focus*, no. 4, Dec. 2019, https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf.

"Central Bank Digital Currencies." *Norges Bank Papers*, vol. 2, 2019.

Nelson, Danny. "Sweden's Central Bank Finally Embraces DLT, but Only in Simulation Mode." *CoinDesk*, CoinDesk, 6 May 2020, www.coindesk.com/swedens-central-bank-finally-embraces-dlt-but-only-in-simulation-mode.