CENTRAL BANK DIGITAL CURRENCIES:

THE NEW BALANCE BETWEEN PRIVACY AND ACCESS IN THE DIGITAL ECONOMY

BOB CHEN

z5362361

I INTRODUCTION

Central Bank Digital Currencies (CBDCs) are a relatively novel economic concept which have materialised in response to the digitisation of global and domestic economies. As individual, corporate and government transactions are increasingly being conducted digitally and not through cash, it follows that central banks, as the sole issuers of money, should directly mint digital denominations of their currencies [1]. CBDCs are issued solely by national banks and are equivalent in value to cash [2]. CBDCs are however, not cryptocurrencies [2]. They are centrally managed with currency minting being at the discretion of the national central bank, in accordance monetary policy goals. The technology the central bank uses to maintain the currency ledger can be with traditional technologies, or with a modified distributed ledger. A majority of currently implemented and discussed strategies use centralised ledgers or a technology agnostic.

Whilst the existing banking system has a mature and evolved regulatory environment which demarcate the boundaries between private and government responsibilities, CBDCs present governments with the opportunity to reset these boundaries. This especially relates to the quantity and type of transaction information which financial institutions collect and market as a cost for their services. As proposed implementations show however, governments have not always taken a position to reduce private access and control based on underlying political philosophies.

A *Objective*

This essay recognises fundamentally that privacy is not the same as security. Of course, privacy depends on a secure technology framework, but it is about so much more. Since CBDCs are controlled currencies, central banks and institutions will always have significant visibility and control of the currency ledger. Thus, privacy concerns the attainment of regulatory assurance that sufficient technical and legal infrastructures exist to protect personal data against unsanctioned or coerced use.

To this end, this essay will first define the issues, scope, and context of its discussion. Then it will explore a variety of solution models across different technologies. Interestingly, because of the recency of research and trials, CBDC proposals between countries differ greatly between the technologies used, with most developed proposals currently technology agnostic with the option for distributed ledger implementation in the future. Accordingly, this essay will briefly examine the Swedish proposal, amongst others, which utilises distributed ledger technology, before undertaking a deeper study of the technologically agnostic Bank of England and the People's Bank of China proposals.

B *Privacy Issues*

As with new technological conceptions of the recent past, CBDCs raise several categories of privacy issues. One of those categories relates to government surveillance and elicit the following concerns.

- Will the central bank have access to individual balance and transaction data?
- Would state police and security services have access to personal contact and identifying information?
- Could individual access to currency be disrupted?

Another category relates to the private commercialisation of consumer data.

- Will banks and other financial institutions have access to balance and transaction data?
- Can banks and financial institutions commercialise such data?

And finally, there are implementation concerns which relate to privacy.

- Does the currency and the ledger on which it is built protect user details, user balances and transaction histories?
- Do both parties in a transaction have access to each other's personal contact and identifying information?
- Are the previous transaction histories for a unit of currency visible to its current holder?

There is no natural answer to each of these concerns. Instead, these questions represent choices and compromises central banks will need to make and explain as they design their CBDC.

C *Context*

The utopian and satisfying comfort of absolute data privacy can temporarily devalue the importance of access to data for the purposes of investigation and interception by civil and criminal investigators. Consideration of CBDC privacy should bear in mind the current privacy, regulatory and commercial environment.

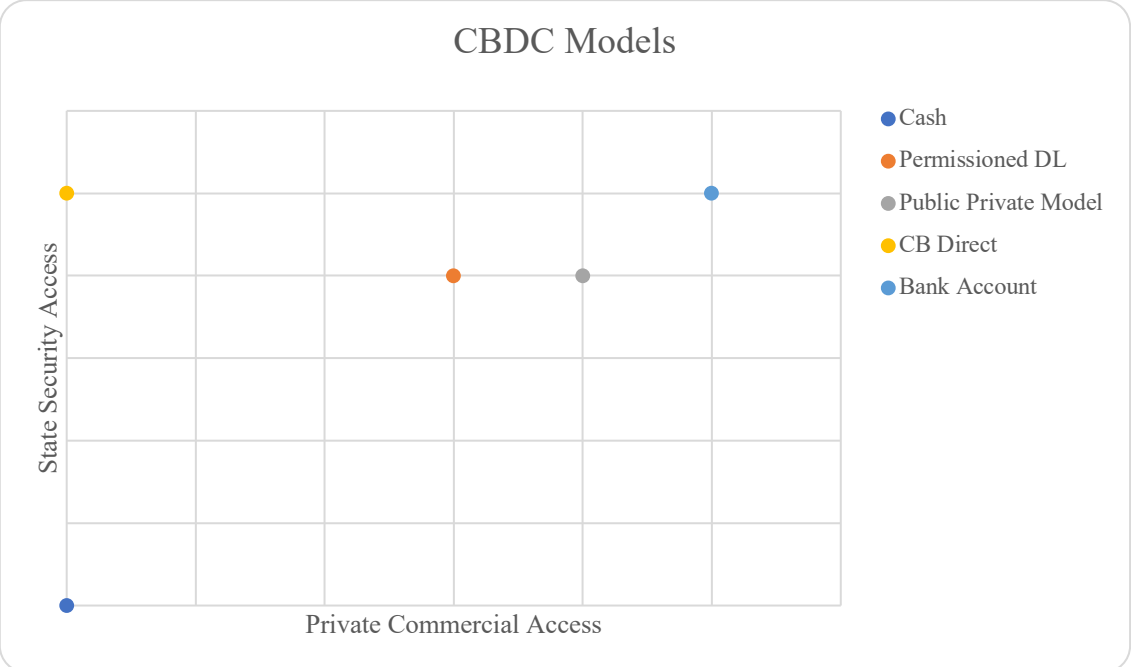
1. Financial institutions already collect significant know your customer (KYC) data and participate in anti-money laundering (AML) regulations as required by law. These

policies are the evolution of modern accountability policies which have been enabled through the digitisation of commerce [3]. They provide reasonable and needed safeguards against criminal activity and aid in the enforcement of laws. Thus, it is unlikely that central banks and governments will adopt a CBDC implementation which regresses from these achievements.

2. Central banks exist within enabling legal frameworks which regulate their independence and autonomy [4]. This essay will assume the autonomy and independence of central banks as per their enabling legislation [4]. Concerns of central bank collusion with police are political and not technical in nature. They are not an issue with CBDCs but rather the social infrastructure it exists in.
3. Under the general capitalistic model of most economies, companies are not motivated to act in their customers' best privacy interest if it is also not more profitable for them to do so. The terms of service for many card processors allow for the use of aggregate consumer transaction data. Consumers have no ability to decline this use other than to withdraw from using the product.

II SOLUTIONS

Privacy attributes of solutions can be compared through the modelling of two standards. These are the ability for the state to access transaction and account data and the ability for private entities to commercialise transaction and account data [5]. The underlying implementation of a CBDC can be a mix of or either a token or account-based system. Simplified, a token system records an owner for each asset whereas an account-based system records assets for each owner [6]. Either architecture relates to the integrity of the CBDC system by preventing double-spending. Whereas an account-based system can query the ledger for an account balance, a token system relies on the spending of a token possessing some sort of private key meaning the token can only be spent once [7].



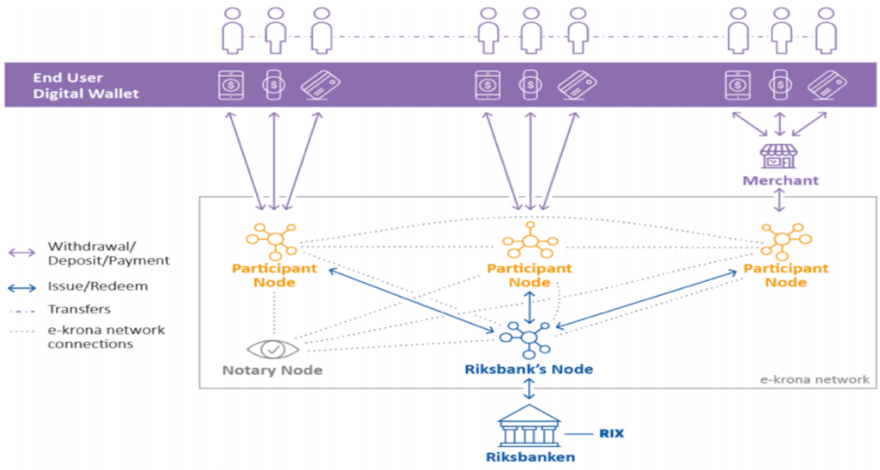
The two points of reference for this rough comparison are cash and bank accounts [8]. Cash is a token style system where ownership is attached to the token (note/coin). It has a low ability for the government to audit ownership and transaction histories [9]. It also has a low ability for financial institutions to collect balance and usage data for commercialisation [9]. Traditional bank accounts are an account-based system. They have a relatively high ability for government to access account and transaction data using legal subpoenas and search warrants. Financial institutions have visibility over customer data and can specify the use and commercialisation of such data in policies set forth by themselves. The attributes of potential CBDC models are set out below.

A *Permissioned Distributed Ledger*

A permissioned distributed ledger (PDL) CBDC is based on the research, experience, and learnings from traditional distributed ledger cryptocurrencies such as Bitcoin which has been publicly available since 2009. While their underlying architectures are similar, they differ in that PDLs require each party which interacts with the ledger to be authorised. The standard for authorisation is determined in advance and can vary from "anyone who requests can join" to "full KYC details need to be verified" [10]. The national reserve bank will set these requirements.

Since access to the ledger is permissioned, only the reserve bank and financial institutions will run full nodes of the ledger. Individual consumers will be serviced through wallets created and maintained by a permissioned financial institution. Beyond access to the ledger, transactions on the ledger can be permissioned as well. Whilst default transactions between two parties will appear on the ledger viewable to all other authorised participants, there is also the option to obscure transactions so that their existence is only viewable to a limited set of pre-determined parties.

Sweden has indicated their intention to create a CBDC of this structure via central bank whitepapers beginning 2017 [11].



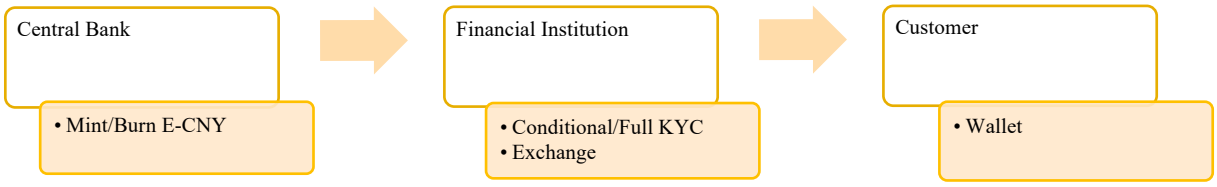
Source Accenture

The e-krona uses the Corda by R3 PDL [12]. It is intended to have a separate notary node which acts as the "miner" for e-krona transactions [12].

Under this model, the Riksbanken does not conduct its own KYC checks nor hold identifiable customer data. Banks continue to act as the intermediary for customer funds and are accountable to customers and to legislation mandating data disclosure. They can continue to set their own policies regarding the use of customer data for commercial purposes.

Perhaps more problematically is that where it has come to implementation, governments have relied on private companies contracted to design, deliver, and maintain PDL networks. These standards and agreements are enforced through contract and not legislation or constitutional guarantees and thus are a weak assurance to proper governance. The Corda framework is supervised by the Corda board of eleven directors, nine of whom are elected by participants in the Corda framework (financial institutions and central banks) [13]. Two seats on the Corda board are permanently reserved for R3 appointees, where R3 is a private company not accountable to public oversight nor shareholders [13]. Instead R3 is a for-profit corporation owned in large part by global banks. Further, as of 2021, the Corda board has handed the day-to-day running and power of legal contracting to R3 indefinitely [14]. Entanglement between the de-jure independent board and the for-profit company includes a litany of private interests which do not give assurance that a country's government will have full control over the underlying rules and practices of their currency. It risks countries which want to have more stringent policies towards AML or privacy to be required to negotiate with other operators from other currencies to enact changes to their underlying framework.

B *Digital Currency Electronic Payments*

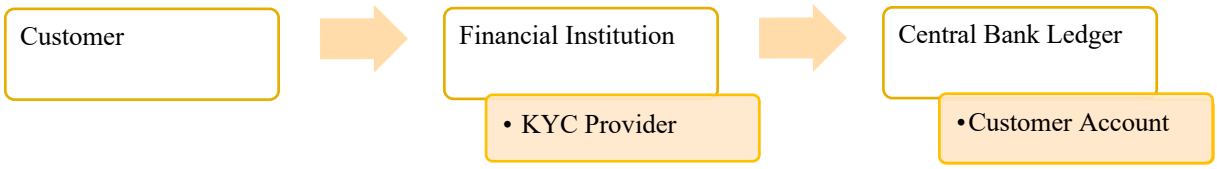


The People's Bank of China (PBOC) has, unlike Sweden, designed their own underlying framework which is technologically agnostic however can be stored as a PDL in the future. Research began in 2014 and China is currently the only developed nation with a mature testing regime for their CBDC [15]. The main difference with previously discussed PDL frameworks is the in-house nature of development which grants the PBOC discretion and initiative to shape the development of the currency standard. The conditional KYC feature of the digital yuan allows for small quantities of yuan to be held and used with minor KYC checks [16]. This reduces the number of personal details which are collected by financial institutions which can then be commercialised.

C *Public Private Model*

1 *Controlled Direct Liability*

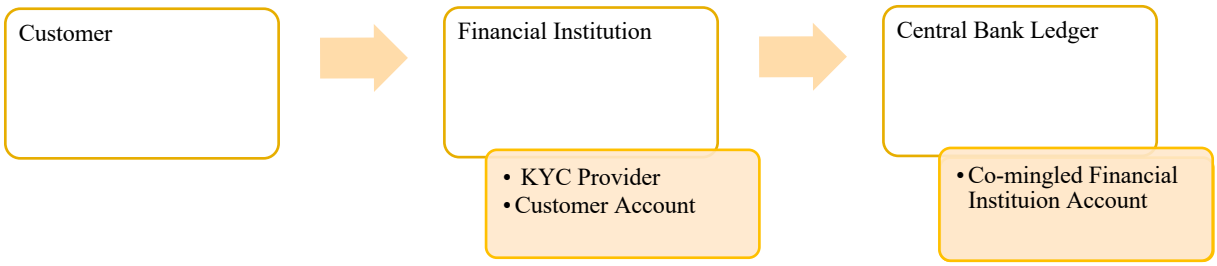
This form of public private partnership increases the function of the central bank in day-to-day banking. It is an account-based model where deposits are directly held at the central bank in individual accounts for each customer [17]. These deposits will be controlled by financial institutions who will perform KYC, customer interaction/instruction, onboarding, and support functions. These institutions will not own these deposits [17].



Countries such as the United Kingdom and Australia have been investigating this model of operation for their CBDCs however no concrete implementation has been selected [18]. This model reduces data that the bank needs to hold and be responsible for. Banks can still attain a similar degree of customer account and transaction data by recording requests and responses customers make to their CBDC account. The central bank ledger contains anonymised account information, so the central bank is unable to attain personal details of account holders without additional measures.

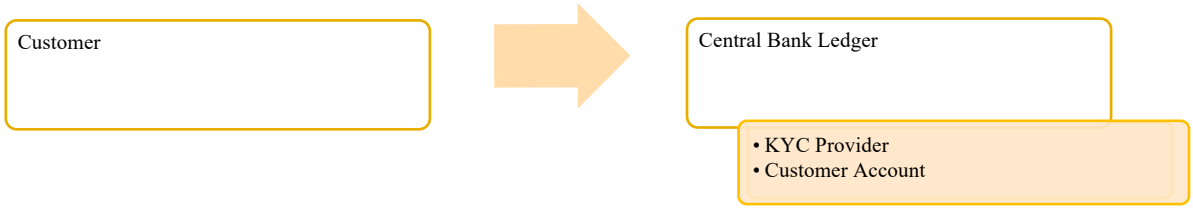
2 *Comingled Pools*

The comingled pool is the model which most preserves the current form of banking responsibilities and control. It is an account-based system where financial institutions will hold account entries at the central bank [17]. Customers will have their own accounts with their financial institutions which will continue to manage KYC and user interaction actions. Under this model, banks own the digital currency deposited with them and the central bank is unable to see the quantity, and individual account details of a bank's customers [17]. They can only see the macro pools of currency under management by banks. Banks will have equal access to account and transaction data as they do now.



D *Central Bank Direct*

The direct model for CBDCs is the model which most reduces the role of financial institutions in future financial transactions. It makes customers direct responsibilities of the central bank removing the need for commercial deposit taking institutions. The central bank will be responsible for KYC and AML supervision as well as day-to-day transactions.



No major economy has currently proposed this model of a CBDC because of concern that it will drastically affect the integrity, confidence and stability of existing deposit taking institutions as well as a mild population distrust of perceived direct government control of the banks.

III THE DIGITAL POUND

The Bank of England (BoE) has studied the potential for a CBDC since 2016. When the UK took the presidency of the G7 in 2021, they set public policy principles for CBDC development which includes standards relating to law, regulation, security, and monetary policy [19]. These standards are the basis of UK CBDC research and policy direction. In February 2023, the Bank of England released their white paper plan for the digital pound implementation and trial [20].

A *Implementation Architecture*

The architecture is proposed to be a centralised ledger being run by the BoE. The digital pound relies on a public private operation using either the aforementioned controlled direct liability model or the comingled pool model [20].

1. The BoE maintains a ledger for digital pound deposits. They are also the sole body with minting capability.
2. Financial institutions allow customers to create accounts with them. Financial institutions can create an account at the BoE ledger on behalf of the customer and henceforth act as an interface for the customer and the BoE ledger. Alternatively, they can create a large account where multiple customer deposits are held at the BoE and run their own ledger to distinguish between liabilities to each customer (more like a traditional bank).

The digital pound has a 20,000 GBP cap on any single balance to allow for daily transactions and salary deposits but not for larger sums of money to be accumulated [20]. This is to reduce the risk of money laundering and illicit activity.

All users of a digital pound account will need to undergo full KYC checks like opening a bank account. This requires details such as a name, and date of birth as well as ID to support these assertions.

Does the currency and the ledger on which it is built protect user details, user balances and transaction histories?

Yes. The BoE ledger does not contain any identifying information on customers [20]. Balances and transaction histories are stored by the ledger and are subject to regular risks associated with bank account security.

Do both parties in a transaction have access to each other's personal contact and identifying information?

No. Transactions between parties will rely on third parties such as banks and payment processors. Like current card payments and bank transfers, apart from account numbers, further information is not given. The BoE ledger cannot look up account details given a name or date of birth.

Are the previous transaction histories for a unit of currency visible to its current holder?

No. This is an account based CBDC and currency ownership history is not stored [21].

B *Commercial Access to Data*

Will banks and other financial institutions have access to balance and transaction data?

Yes. Banks and financial institutions have access to all balance and transaction data like existing bank accounts. The BoE ledger is simply the underlying infrastructure to which a bank adds a frontend to create a financial product for customers to use [20].

Customers can open accounts at multiple institutions to spread the information provided to institutions.

Can banks and financial institutions commercialise such data?

Yes. To the same extent that they can commercialise their existing bank data.

C *State Access to Data*

Will the central bank have access to individual balance and transaction data?

The central bank, through their ledger, can see account balances and transaction data. They cannot see any identifying details about each account, which is managed by the banks.

Would state police and security services have access to personal contact and identifying information?

Yes. Like existing processes with bank accounts, police can subpoena banks for personal and contact details identifying a BoE account since those banks would have needed to collect KYC details prior to opening an account. The BoE addresses this point directly in their white paper asserting that the need for law enforcement to conduct searches is imperative to controlling money laundering and illicit activities. It is not the bank's intention to create a payment system which completely anonymises its users.

Could individual access to currency be disrupted?

Yes. The Proceeds of Crime Act 2002 gives police the ability to apply to a court for an order to freeze an account containing assets of an individual involved in crime. Banks such as retail banks which provide UK customers with digital pound access will be required to comply with these orders.

IV THE DIGITAL YUAN

The People's Bank of China (PBOC) began digital yuan research in 2014 with the first pilot being deployed in 2020 and wider pilots being deployed across China during the 2022 Winter Olympics reaching over 10 major cities. It meets cash-like accessibility attributes such as a low barrier to usage, a low cost to usage and anonymity to a certain extent [22]. Participating financial institutions provide services to convert between digital yuan and renminbi bank deposits.

Cumulative digital yuan transactions currently sit at 87 billion RMB or 13.7 billion USD [23]. They currently represent 0.13% of the PBOC's cash reserves [24]. As of February 2022, 244 million individual accounts and 18 million business wallets have been opened.

A *Implementation Architecture*

The digital yuan has a multi-tier model of operation involving existing institutions [16].

1. The PBOC maintains a ledger for digital yuan deposits. They are the sole body with minting and burning capability [25].
2. Select financial institutions participating in the trial maintain customer services [26]. They provide a wallet for the customer to see and handle their digital yuan balances. This wallet is simply displaying a user's balance on the PBOC's ledger as that is where customers' digital yuan are stored. These financial institutions handle the dissemination of digital yuan via the acceptance of RMB bank deposits and vice versa for customers wishing to convert to cash.
3. A wider range of financial institutions provide payment services and financial products to customers with digital yuan facilitating purchases and P2P transfers [25].

The digital yuan uses a system of controlled anonymity where the amount of personal information required of consumers depends on their daily spend and total deposit amount [25]. The minimum information required to open an account is with a single phone number [27].

This minimum account affords the greatest privacy protections and has a 10,000 RMB balance limit, 2000 RMB per transaction limit and a 5000 RMB daily transaction limit [28]. Increased tiers of verification comparable with normal bank KYC checks will increase these limits [27]. Business accounts have increased limits to personal accounts.

Does the currency and the ledger on which it is built protect user details, user balances and transaction histories?

The central bank ledger stores only wallet balances, transaction histories and phone numbers [16]. Individual financial institutions which conduct KYC processes may store additional information on customers such as names, addresses and date of birth, the security of which would depend on the institution. Despite this, the storage of a phone number within the central bank's ledger is a significant piece of information which may help identify owners in the event of a breach.

Do both parties in a transaction have access to each other's personal contact and identifying information?

No. Parties are not able to know identifying and contact information of opposing parties to a transaction [16]. Transactions can be business to consumer via a payment processor or peer to peer via wallets or even via Bluetooth [25].

Are the previous transaction histories for a unit of currency visible to its current holder?

No. The digital yuan uses an account-based ledger. Transaction histories are tied to accounts and not units of currency [21].

B *Commercial Access to Data*

Will banks and other financial institutions have access to balance and transaction data?

Not exactly. A digital yuan wallet is a standalone app or hardware device. While select banks and financial institutions enrol users with wallets, they cannot then see the transaction data that occurs within a wallet. They provide users exchange services to convert RMB to digital yuan and they have a record of these conversions [16]. Users however have a choice in financial institutions meaning they can avoid any singular bank gaining an accurate image of their balance.

However, many financial institutions like Alipay and WeChat Pay provide integrated wallets within their existing apps [16]. These apps act as an additional interface between users and their wallets and consequently are privy to user requests to their wallets.

Finally, users can create child wallets tied to their original wallet which they can add to different payment providers and banks [28]. This allows users to operate multiple wallets which can obfuscate their activities to financial services providers.

Can banks and financial institutions commercialise such data?

Yes. To the extent that they can get the data, institutions can treat this data per their existing privacy policies and commercialise accordingly.

C *State Access to Data*

Will the central bank have access to individual balance and transaction data?

Yes. The central bank will have access to individual balance and transaction data tied to each wallet. They have minor details such as a phone number which they can use to identify that data via lookups for phone number ownership.

Would state police and security services have access to personal contact and identifying information?

Yes. Like bank accounts, law enforcement can use search warrants served either to financial institutions or the PBOC to gain a person's transaction history or personal details.

Could individual access to currency be disrupted?

As with bank accounts, police have the authority to freeze personal assets including bank accounts and digital yuan wallets if they suspect the person has committed a crime. Banks are required to cooperate with police to freeze accounts and financial services provided to individuals. It is likely that the PBOC will likewise comply with similar requests to freeze digital yuan wallets.

Applications to freeze assets must be approved by a court under Article 94 of the Criminal Procedure Law [29]. The Anti-Money Laundering Law likewise empowers police with these prerogatives.

V COMPARATIVE COMMENTARY

A *Implementation Architecture*

The BoE proposal for their CBDC places a strong emphasis on existing institutional participation. Although well intentioned, this emphasis on the private sector and fear of the central bank taking a greater role in the currency's implementation has resulted in the BoE essentially designing a common backend for banks to use. The government, through the central bank, should be wary of assuming private sector overheads without reducing institutions' control and access to data or internalising the costs of designing and operating such a system.

Access to an account relies on going through an existing financial institution with full KYC checks for any balance. This has the same accessibility issues as exist bank accounts and does not fulfill a CBDC goal of better serving the underbanked.

The PBOC design, like the BoE proposal, assigns a role to existing banking institutions, however, shifts a greater level of control and data away from the banks. It is representative of the central bank assuming greater operational control of its CBDC while leaving customer service to the private sector. It reduces institutions to mere providers of frontend services to a wallet which the user inherently owns. Users can change providers for their wallet, unlike with the BoE model which would require a user to close an account and open a new account with a different bank. The minimum requirement of a phone number, but no KYC is a reasonable entry point which increases accessibility beyond those with bank accounts. The requirement for a phone number allows for 2FA and acts as a limit to excessive accounts.

B *Commercial Access to Data*

The BoE model essentially is a banking backend which all banks can use to offer their products. Hence, they will largely have similar access and visibility to data which they can commercialise per their terms. Governments should be cautious of increasing for-profit corporation access to transaction data so unconditionally for its new currency. On the other hand, the digital yuan does not give institutions which create user wallets control over those deposits. Unless a user pays their yuan to a bank, they cannot earn interest. Hence, by default, banks will have reduced access to customer data, unless they are able to market an integrated application which persuades users to hold their currency with them.

C *State Access to Data*

The BoE model moderately increases data which the government (central bank) stores since a ledger is now being stored by the BoE and not by individual banks. The PBOC will now also have visibility of cash holdings in anonymised accounts and access to mobile phone numbers tied to each account. In both cases, the macro visibility of the money supply, be it M0, M1 or M2 is being increased reducing the privacy of financial institutions. This will aid regulatory regimes with increased transparency and decreased reliance on self-reported data.

VI CONCLUSIONS

An examination of a range of CBDC models reveals the intention of central banks is the standardisation of internet banking, making it state-sponsored, universally accessible and at no cost to the end consumer. The absolute anonymity of cash is dead. It is not being considered a feature to be fully preserved in CBDC design considering anti-money laundering and counter-terrorism needs [3]. Instead, designs differ over the level of default access corporations and government possess to financial data [30]. All proposed CBDC architectures can be abused by security services if that is their overwhelming will; just as all CBDC models can be abused by private institutions if a strict regulatory regime is not present. These attributes are not new, but merely duplicate to the existing financial banking system. But the bigger question for governments is whether they will use CBDC creation as an opportunity for a blank slate to redefine the role of public and private entities so as to improve privacy outcomes, or to merely rollover the same financial and regulatory landscape.

VII BIBLIOGRAPHY

[1] Cryptopedia, “Which Countries Have CBDCs?,” Cryptopedia, 15 March 2021. [Online]. Available: https://www.gemini.com/cryptopedia/cbdcs-digital-currency-us-china. [Accessed 17 April 2023].

[2] M. Bobinac, “CENTRAL BANK DIGITAL CURRENCIES,” Thales, 28 February 2023. [Online]. Available: https://cpl.thalesgroup.com/blog/identity-data-protection/central-bank-digital-currency-cbdc. [Accessed 17 April 2023].

[3] D. Ballaschk, “The public, the private and the secret: Thoughts on privacy in central bank digital currencies,” *Journal of Payments Strategy & Systems,* vol. 15, no. 3, pp. 277-286, 2021.

[4] C.-Y. Tsang, “Disciplining Central Banks: Addressing the Privacy Concerns of CBDCs and Central Bank Independence,” The FinReg Blog, 8 November 2022. [Online]. Available: https://sites.duke.edu/thefinregblog/2022/11/08/disciplining-central-banks-addressing-the-privacy-concerns-of-cbdcs-and-central-bank-independence/. [Accessed 17 April 2023].

[5] A. Kaushik, “Central Bank Digital Currency (CBDC) and Privacy,” Massachusetts Institute of Technology Media Lab’s Digital Currency Initiative Sloan School of Management, Boston, 2020.

[6] nChain, “Account vs token-based CBDC,” nChain, 26 October 2022. [Online]. Available: https://nchain.com/account-vs-token-based-cbdc/#:~:text=Put%20simply%2C%20the%20former%20means,tokens%2C%20which%20have%20key%20holders.. [Accessed 17 April 2023].

[7] E. Copic, “It’s Time to Abandon the “Token vs. Account” Discussion,” LinkedIn, 24 February 2022. [Online]. Available: https://www.linkedin.com/pulse/its-time-abandon-token-vs-account-discussion-ezechiel-copic/. [Accessed 17 April 2023].

[8] S. Darbha, “Privacy in CBDC technology,” Bank of Canada, 9 June 2020. [Online]. Available: https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/. [Accessed 17 April 2023].

[9] N. Sridhar, “Should Central Banks Offer the Public Token-Based Digital Currencies?,” Discourse, 8 June 2021. [Online]. Available: https://www.discoursemagazine.com/economics/2021/06/08/should-central-banks-offer-the-public-token-based-digital-currencies/. [Accessed 17 April 2023].

[10] Digital Currency Governance Consortium White Paper Series, “Privacy and Confidentiality Options for Central Bank Digital Currency,” World Economic Forum, 2021.

[11] SVERIGES RIKSBANK, “E-krona,” Riksbank, 4 April 2023. [Online]. Available: https://www.riksbank.se/en-gb/payments--cash/e-krona/. [Accessed 17 April 2023].

[12] Binance Research, “Sweden’s Public Digital Cash: E-Krona,” Binance, 4 March 2020. [Online]. Available: https://research.binance.com/en/analysis/e-krona. [Accessed 17 April 2023].

[13] Corda, “By-Laws,” Corda Network, [Online]. Available: https://corda.network/corda-network-foundation/by-laws/. [Accessed 17 April 2023].

[14] Corda, “About the Foundation,” Corda Network, [Online]. Available: https://corda.network/corda-network-foundation/about-the-foundation/. [Accessed 17 April 2023].

[15] R. P. Buckley, “China’s Central Bank Digital Currency Will Transform the International Monetary and Financial Systems,” Oxford Business Law Blog, 18 November 2022. [Online]. Available: https://blogs.law.ox.ac.uk/blog-post/2022/11/chinas-central-bank-digital-currency-will-transform-international-monetary-and. [Accessed 17 April 2023].

[16] H. Wang, “China’s Approach to Central Bank Digital Currency,” Herbert Smith Freehills China International Business and Economic Law (CIBEL) Centre, Sydney, 2022.

[17] DFCRC, “Australian CBDC Pilot for Digital Finance Innovation,” RBA, 2022.

[18] DFCRC, “Australian Central Bank Digital Currency Pilot Project,” DFCRC, 26 September 2022. [Online]. Available: https://dfcrc.com.au/cbdc/. [Accessed 17 April 2023].

[19] G7, “Public Policy Principles for Retail Central Bank Digital Currencies,” G7, Cornwall, 2021.

[20] Bank of England, “The digital pound: a new form of money for households and businesses?,” Bank of England, London, 2023.

[21] R. Garratt, “Token- or Account-Based? A Digital Currency Can Be Both,” Federal Reserve Bank of New York, 12 August 2020. [Online]. Available: https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/. [Accessed 17 April 2023].

[22] P. Cheng, “Decoding the rise of Central Bank Digital Currency in China: designs, problems, and prospects,” Nature Public Health Emergency Collection , Singapore, 2022.

[23] E. Cheng, “China’s digital yuan notches $8.3 billion in transactions in 6 months, taking a tiny share of payments,” CNBC, 18 January 2022. [Online]. Available: https://www.cnbc.com/2022/01/18/chinas-digital-yuan-notches-8point3-billion-transactions-in-half-a-year.html. [Accessed 17 April 2023].

[24] A. Singh, “China Includes Digital Yuan in Cash Circulation Data for First Time,” CoinDesk, 12 January 2023. [Online]. Available: https://www.coindesk.com/policy/2023/01/11/china-includes-digital-yuan-in-cash-circulation-data-for-first-time/. [Accessed 17 April 2023].

[25] Working Group on E-CNY Research Research Research Research and Development Development Development Development of the People's People's People's People's Bank of China, “Progress Progress Progress Progress of Research Research Research Research & Development Development Development Development of E-CNY in China,” People's People's People's Bank of China, Beijing, 2021.

[26] Deutsche Bank, “Digital yuan: what is it and how does it work?,” Deutsche Bank, 14 July 2021. [Online]. Available: https://www.db.com/news/detail/20210714-digital-yuan-what-is-it-and-how-does-it-work. [Accessed 17 April 2023].

[27] A. Kumar, “A Report Card on China’s Central Bank Digital Currency: the e-CNY,” Atlantic Council, 1 March 2022. [Online]. Available: https://www.atlanticcouncil.org/blogs/econographics/a-report-card-on-chinas-central-bank-digital-currency-the-e-cny/. [Accessed 17 April 2023].

[28] Ledger Insights, “Details about the digital yuan wallet officially disclosed,” Ledger Insights, 11 June 2021. [Online]. Available: https://www.ledgerinsights.com/blockchain-mineral-traceability-firm-circulor-raises-14-million/. [Accessed 17 April 2023].

[29] *REGULATIONS OF THE PEOPLE'S REPUBLIC OF CHINA ON ARREST AND DETENTION,* 1979.

[30] C. Wagner, “CBDCs and Privacy Are Not Mutually Exclusive: ConsenSys Exec,” Blockworks, 4 March 2023. [Online]. Available: https://blockworks.co/news/cbdcs-privacy-not-mutually-exclusive. [Accessed 17 April 2023].

[31] B. SMITH-MEYER, “Democracy at stake if digital currencies trample over privacy, says ex-central banker,” POLITICO, 25 August 2022. [Online]. Available: https://www.politico.eu/article/democracy-at-stake-if-digital-currencies-trample-over-privacy-warns-ex-central-banker/. [Accessed 17 April 2023].