Central bank digital currencies risk becoming a digital Leviathan[1]

Andrea Baronchelli
Department of Mathematics, City University of London, London, UK. The Alan Turing Institute, London, UK. UCL Centre for Blockchain Technologies, University College London, London, UK. ✉e-mail: abaronchelli@turing.ac.uk

Hanna Halaburda
Stern School of Business, New York University, New York, NY, USA. ✉e-mail: hh66@stern.nyu.edu

Alexander Teytelboym
Department of Economics, University of Oxford, Oxford, UK. St Catherine's College, University of Oxford, Oxford, UK. Institute for New Economic Thinking at the Oxford Martin School, Oxford, UK. ✉e-mail: alexander.teytelboym@economics.ox.ac.uk

Central bank digital currencies (CBDCs) already exist in several countries, with many more on the way. But although CBDCs can promote financial inclusivity by offering convenience and low transaction costs, their adoption must not lead to the loss of privacy and erosion of civil liberties.

Until recently, digital money was issued by commercial banks via credit or debit cards, while central banks were the only source of printed or minted money. But in October 2020, the Central Bank of the Bahamas launched the Sand Dollar — the world's first central bank digital currency (CBDC), a digital currency issued directly by a central bank.

Since then, seven countries in the Eastern Caribbean as well as Nigeria have officially launched their own CBDCs, 14 countries are piloting them and more than 50 have announced that they are in the research and development stage. There are many reasons for this flurry of activity. First, CBDCs are touted as a tool for financial inclusivity, giving more people access to banking services. Second, CBDCs are supposed to lower settlement costs and reduce frictions and fees associated with digital payments. Third, and perhaps most importantly, after Facebook's aborted attempt at launching the Libra/Diem currency, there is growing concern among central banks that private players could issue a global currency free from political control.

A CBDC is a digital substitute for cash. But even if CBDCs do not replace cash, their wide adoption will create a dramatic change in how much data are generated by innocuous day-to-day transactions. Today, using cash, you can go to a shop and buy yourself as much chocolate as you like without anyone (except, perhaps, the shop assistant) knowing about it. But if you had to pay using a CBDC, the central bank could immediately trace your transaction. What might it do with that data? Perhaps it could

[1] Preprint version of: **Baronchelli, A., Halaburda, H., & Teytelboym, A. (2022). Central bank digital currencies risk becoming a digital Leviathan. *Nature Human Behaviour*, *6*(7), 907-909.**

allow your health insurer to find out about your unhealthy eating habits. Or maybe it could let the government social security department know about this so your benefits could be docked as a punishment for your gluttony.

In order to collect taxes and keep order, states typically want to know who we are and how much money we earn. But, so far, states have not engaged in a systematic and legitimate effort to trace how we spend our money. Public ledger cryptocurrencies, such as Bitcoin, have flipped this relationship on its head: they store all transactions on an accessible ledger, but can hide the identities of their users. If CBDCs are implemented properly, they could deliver the best of both worlds: privacy for small transactions and genuine financial inclusion as well as a reduction in crime that uses vast quantities of cash alongside the current electronic payment system. Plenty of digital currency technologies are already being tested, and new ones appear every month. However, if we pick the wrong technologies, we risk heading towards the worst of both worlds: a state — even a democratic one — that knows your identity, your income and your transactions, holding even more power over your life.

State of CBDCs

Financial inclusion is a global development challenge. There are 1.7 billion people around the world who are unbanked — they don't have access to a bank account or a mobile phone. For example, from 71% of the population in Morocco to 51% in Argentina, 7% in the US and 4% in the UK are unbanked. The effects of financial inclusion can be dramatic. Nepali women who were offered a bank account managed to increase their assets by 16%, and an increase in bank branches in rural areas helped to cut rural poverty in India by up to 17 percentage points.

As CBDCs are supposed to make it easier to open a digital payment account and have lower transaction fees, they are widely promoted as a means to foster greater financial inclusion. For example, the Nigerian e-Naira seemingly offers a Tier Zero account, supposedly for "customers without existing bank account and without verified national insurance number." However, when we tried to open an e-Naira account in February 2022, we were asked to provide the details of our bank account. What's even worse is that we were also required to provide biometric details, which makes the e-Naira less accessible and more intrusive than a standard bank account. When we checked The Bahamian Sand Dollar Tier I account in February 2022, we were told that "government-issued identification is not an enrolment requirement," but then we were invited to "choose and contact your preferred Sand Dollar enabled authorised financial institution (AFI)," thus making any enrollees subject to bank-level (know-your-customer; KYC) identity checks.

Currently, the most important CBDC pilot is the digital renminbi issued by the People's Bank of China, with over 260 million users and US $13.8bn of transactions so far. Originally opened only to bank account holders, China allowed foreign athletes and tourists to use the CBDC during the 2022 Winter Olympics. China says that the digital renminbi provides 'controllable anonymity', but it is vague on details. Many commentators suspect that virtually any digital renminbi transaction would be

traceable and that the Chinese Communist Party is using the CBDC as another tool of political control.

Virtual anonymity

Currently, CBDCs are not much more accessible than traditional bank accounts, so they are hardly living up to their promises of financial inclusion. Indeed, there is a clear trade-off between the lower barriers to account access that would foster financial inclusion and greater anonymity, which might encourage illicit CBDC use. But already banked consumers and retailers might nevertheless be attracted to CBDCs by the lower transaction fees. If network effects take off, we could see wide adoption within some countries with the central banks sitting on more data than they had ever collected before.

Why should we worry that the central bank might collect data on all our transactions? After all, any electronic payment between commercial banks via a credit card or by direct transfer can already be checked and stopped (privacy is often even worse for some mobile phone payment systems). However, in order to trace a particular transaction or account (for example, to prevent tax evasion), the government needs to request information from banks. In the UK, for example, this is done by issuing a 'third-party notice' to the banks. These can take time and end up involving the courts. CBDCs could potentially offer a frictionless way for the state to systematically monitor all transactions.

It is hard to underestimate the temptation for states — even democratic ones — to increase their surveillance powers. As Edward Snowden revealed, the US government rolled out an unprecedented surveillance programme called PRISM in 2007, which collects internet communications from various US internet companies. In 2016, a court ruled that UK security agencies unlawfully tracked individual phone and web use and other confidential personal information, without adequate safeguards or supervision, for 17 years. China has a surveillance programme in place in Xinjiang, which reportedly includes all-encompassing monitoring based on identity cards, checkpoints, facial recognition and the collection of DNA from millions of individuals.

State-owned transaction data bring about a number of possible risks. First, the central bank might have the ability to make a CBDC non-fungible. This would allow it to directly control how the money of specific individuals can and cannot be spent. Second, the government could use the collected data for personalized pricing of public services or targeted punishment. For example, public medical services could carry a penalty for those who buy cigarettes. Indeed, transaction surveillance might incentivise people to make certain purchases in order to 'please' the government. Third, even if governments do not use the data themselves, they might be tempted to sell the data to private companies. For example, an e-commerce platform could find out your entire spending history and be much better at targeting products to you. There are precedents of states giving away troves of personal data without obtaining proper consent. In the UK, for example, the National Health Service shared details of more than one million patient records with Google's spinoff DeepMind without obtaining the patients' consent.

CBDCs that serve people

To avoid CBDCs further eroding our privacy, the public needs to encourage policymakers to make good design decisions as early as possible — before bad features become institutionally entrenched.

No central bank would allow its CBDC to be completely anonymous. Complete anonymity creates incentives for illicit activities, such as money laundering, drug trafficking and terrorism financing. However, current CBDCs offer no obvious privacy protection whatsoever.

We should distinguish between two types of privacy that are relevant to users of CBDCs. First is the anonymity of the wallet or account. Wallets cannot be fully anonymous because any restrictions placed on them can be circumvented by creating multiple wallets. However, in order to foster financial inclusion, it should be possible to create an account with minimal identity verification. In some countries, it might be enough to register using a mobile phone, a (temporary) residential address or a landline number. In particular, one should not require an existing bank account in order to open a CBDC account.

The second type of privacy is the anonymity of the transactions. Distributed ledger cryptocurrencies offer various levels of transaction anonymity: from the pseudonymity of Bitcoin to an essentially anonymous Monero. Different CBDCs already use different technologies, from conventional transaction architectures in Nigeria to Hyperledger Fabric, a flexible distributed ledger technology (DLT) used by the Eastern Caribbean CBDC. As a result, the CBDCs, which are almost certain to be permissioned (maintained by a set of pre-approved validators), can benefit from the designs that work well even in permissionless systems (in which anyone could become a validator). For example, CBDCs can draw on a two-tiered payment and minting infrastructure. It is technically possible to make it very difficult to trace someone's transactions by designing a 'layered' blockchain (for example, Avalanche). In this way, the central bank can issue money on a private and permissioned blockchain, and then have transactions occur over a public and permissionless blockchain. Another promising proposal from the European Central Bank using the Corda DLT suggests anonymity for small transactions (which can more generally be ensured with 'smart contracts') and greater visibility for larger transactions. Finally, transactions for which anonymity cannot be guaranteed should not be stored indefinitely. In other words, people should have the right to have all their transactions forgotten in a reasonable time.

We need to talk about CBDCs

It is deeply concerning that there is no public debate about the privacy of CBDCs. And it is crucial that the parameters of this debate are set as soon as possible. The technological properties of CBDCs, such as whether the CBDC is on a distributed or centralized ledger (that may or may not even make the CDBC more convenient), are second-order issues for society's choices of digital cash use. Instead, the public and

their lawmakers must decide on the features of CBDCs that minimize the violation of privacy and human rights in pursuit of greater convenience. Therefore, we encourage the public debate to consider (i) which features of CBDCs would actually promote financial inclusion; (ii) how CBDCs can ensure a reasonable level of account and transaction anonymity; and (iii) how the vast data that will be generated by CBDC use will be processed, stored and eventually destroyed. We hope that this public debate will force the issue to become a top priority of central banks that are considering CBDC launches.

It would be disastrous to neglect the privacy debate around CBDCs in the same way as regulators ignored privacy concerns posed by social media platforms. For years, the tech giants have been left to hoover up, store and process vast amounts of data. And while data and privacy regulations are slowly catching up, many citizens are still happy to give up an extraordinary amount of privacy for the convenience of receiving 'surprisingly good recommendations'.

The rush to issue CBDCs and the absence of a well-informed debate could drastically erode the little individual privacy that still remains in open societies. Choices about payment systems are path-dependent and sticky, and we are in a unique position to make them early. Without a democratic debate on the features of digital cash now, we may inherit a future in which we succumb to the digital Leviathan.

Acknowledgements
The authors acknowledge helpful discussions with, and research assistance from, I. Abba, J.-W. Chang and J. Le Cornu.

Competing interests
The authors declare no competing interests.

References
1. Bharathan, V. Central Bank Digital Currency: the first nationwide CBDC in the world has been launched by The Bahamas. Forbes. 21 October 2020.
2. Central Bank Digital Currency Tracker (Atlantic Council, 2021).
3. Auer, R. et al. Central Bank Digital Currencies: Motives, Economic Implications Working Papers No. 976 (Bank for International Settlements, 2021).
4. Farrow, R. How democracies spy on their citizens. The New Yorker. 18 April 2022.
5. Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S. & Hess, J. The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution (World Bank Group, 2017).
6. Klapper, L. Financial inclusion has a big role to play in reaching the SDGs. World Bank Blogs. 15 September 2016.
7. Liao, R. China's digital yuan wallet now has 260 million individual users. TechCrunch. 18 January 2022.
8. Kynge, J. & Yu, S. Virtual control: the agenda behind China's new digital currency. Financial Times. 17 February 2021.
9. Travis, A. UK security agencies unlawfully collected data for 17 years, court rules. The Guardian. 17 October 2016.

10. Rogin, J. Ethnic cleansing makes a comeback – in China. Washington Post. 2 August 2018.
11. Allen, S. et al. Design Choices for Central Bank Digital Currency: Policy and Technical Considerations No. w27634 (National Bureau of Economic Research, 2020).
12. Google DeepMind NHS app test broke UK privacy law. BBC News. 3 July 2017.
13. Exploring anonymity in central bank digital currencies. In Focus issue 4 (European Central Bank, 2019).