Nicola Bilotta

Chapter 8: CBDCs and Stablecoins: The Scramble for (Controllable) Anonymity

In an increasingly digitalized society, citizen–consumers create an enormous volume of data, enabling the empowerment of new business opportunities produced by data aggregation and analysis. This unprecedented megatrend has already raised several questions around data governance, concerning the rules that frame availability, management, accessibility, security and usability of data. These concerns are heightened when considering the accumulation of financial data, which is experiencing a remarkable growth in both volume and quality, due to the increasing digitalisation of payments. Cash – in the form of banknotes and coins – has the unique feature of full anonymity. Someone can pay for goods or services without disclosing one's identity or personal/financial information. This is something that credit/debit cards and mobile payment apps do not have. Whenever a transaction is intermediated by a third-party, the latter gathers and stores data on that transaction. Cash then reduces the information asymmetry between governments and private corporations, and citizens.

On the one hand, a progressively cashless society can help mitigate the risks of tax evasion and money laundering, as regulators would be able more easily to monitor and keep track of citizens' transactions. On the other hand, the existing digital payment solutions are developed and owned by private actors – incumbent financial institutions, big technology companies and non-banking actors – enabling these players to establish an intermediary function between governments and public money. Furthermore, these private players can collect valuable data that can empower their models of behavioural profiles. This is particularly relevant for big tech and non-bank actors that will be able to develop a more comprehensive profile of consumers through a cross-sources analysis, combing through information on what consumers like, desire, buy and can afford. Financial data is valuable because it provides an accurate picture of consumer's habits and financial situation. The growing public policy concerns on the effects of this payment disintermediation increase if private non-banking actors are also seeking to launch private digital currencies that could potentially create parallel money systems, operating on a new architecture rather than on traditional infrastructures and networks.

Governments are worried that, if this trend of cashless payments keeps expanding, private actors would dominate the digital payment market, producing risks related to data aggregation and accumulation. To strengthen the role of central bank money as a relevant unit of account in a digital society, central banks are exploring the development of domestic general purpose central bank digital currencies (CBDCs). Despite CBDCs being a public-issued form of money, they also produce risks around how much information central governments can retain from consumer's transactions. This makes it challenging to find and establish a balance between controllable anonymity and compliance with the current anti-money laundering (AML) rules. Apparently, CBDCs could be technically designed to blind or regulate states' supervision to allow users some degree of privacy and anonymity.[1] Yet the equilibrium of the degree of anonymity in relation to efficiency and security in a CBDC system appears to primarily be a political decision rather than a technical and design issue. The underlying infrastructure is determined by a conscious choice. Most of the current literature and discussion on privacy/anonymity and CBDCs has been focused on the possible technical solutions to guarantee security and to limit accessibility.[2] Those engaged in this discussion should however take a step back first and focus on which degree of privacy/anonymity monetary systems should guarantee to citizens. In terms of their different natures and the risks they produce, both CBDCs and private-owned stablecoins raise concerns on anonymity, data aggregation and balance of power: how much privacy should be available, and from whom, are key public policy issues. Nevertheless, whereas the debate on stablecoins at the multilateral level appears to have recognized the political dimension of this innovation, the discussion on CBDCs seems to lack a political approach to anonymity.

8.1 Anonymity in CBDCs and privately owned stablecoins

One often hears the common – and yet simplistic and misconceived – argument that the only people who care about anonymous payment systems are

1 European Central Bank (ECB), 'Exploring Anonymity in Central Bank Digital Currencies', *In Focus Papers*, No. 4 (December 2019), https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf.

2 Ibid.; Committee on Payments and Market Infrastructures, 'Central Bank Digital Currencies', in *CPMI Papers*, No. 174 (March 2018), https://www.bis.org/cpmi/publ/d174.htm.

those who are violating the law.[3] This has been an extremely popular reasoning to stigmatize the development of untraceable means of digital payment – such as Bitcoins – as a sort of anarcho-utopian project. However, in the book *Privacy and Freedom*, published in 1967, Alan Westin asserted that privacy is an individual freedom: 'the claim of individuals […] to determine for themselves when, how, and [to] what extent information about them [citizens] is communicated to others'.[4] That commercial payment platforms monetize data is no secret. They either sell data to third parties for cross-source aggregation or use payment data to cluster users and sell these consumer profiles to third parties. Google, for instance, bought data on millions of card transactions from Mastercard. The deal aimed at tracking when and whether the online advertisements powered by Google resulted in a sale in physical shops.[5] Although both Google and Mastercard guaranteed the privacy and the safety of the financial data, Google has started offering a service called 'Store Sales Measurement', which allows it to anonymously match ads and actual store sales.[6] Clients have, however, not been informed that their banking data has been sold and shared with a third party. Similarly, in China, the flow of data in Alibaba's various activities has been feeding and empowering its large ecosystem, such as with the transfer of data from Alibaba's e-commerce stores and Alipay to MyBank to assess creditworthiness, or from Alipay to Sesame Credit.[7] This market is still underdeveloped, and it is likely to grow very fast, driven by the increasing scale of data accumulation and by the advancement of prediction tools.

Whether (controllable) anonymity is a right or an individual freedom in the realm of payments is arguable, but the digitalisation of payments is de facto altering the equilibrium between privacy and security that has endured for centuries in the relationship of citizen–consumers, governments and private

3 Felix Salmon, 'Why Payments Won't Ever Be Anonymous', in *Reuters*, 16 December 2011, http://reut.rs/1pjAtfX.

4 Alan F. Westin, *Privacy and Freedom*, New York, Atheneum, 1967, p. 7.

5 Mark Bergen and Jennifer Surane, 'Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales', in *Bloomberg*, 30 August 2018, https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales.

6 Sridhar Ramaswamy, 'Powering Ads and Analytics Innovations with Machine Learning', in *Google Blog,* 23 May 2017, https://blog.google/products/marketingplatform/360/powering-ads-analytics-innovations-with-machine-learning-xp.

7 John Gapper, 'Alibaba's Social Credit Rating Is a Risky Game', in *Financial Times*, 21 February 2018, https://www.ft.com/content/99165d7a-1646-11e8-9376-4a6390addb44.

companies. With the traceability produced by digital payments, several questions can be raised. How is the financial data collected used? Could 'financial surveillance' be a threat? In that case, can that threat be mitigated? Could digital currencies affect the balance of power in the relationship of individuals with state and private corporations? This range of questions is more relevant now than ever, considering a future society in which digital currencies are widely used, increasing risks of misbehaviour in data exploitation by private corporations as well as by public authorities.

The development of private-owned stablecoins within a larger ecosystem could be a turning point in monetary systems as this form of digital money could reach scale very quickly. The first intrinsic advantage of stablecoins is that they can assure a less volatile asset to users, providing these digital currencies with a potential function of medium of exchange and of store of value. Nevertheless, the attractiveness of these initiatives is causally linked to two factors that affect money circulation. First, the credibility of the issuer. Consumers need to trust that they can convert their digital tokens into fiat money anytime they like, and that the value of the stablecoin is indeed stable and backed by reserves. Second, the degree of acceptance. Users could be incentivized to adopt a stablecoin that is backed by a corporation that has a pre-existing relationship with a large consumer base and has high brand recognition, as this could mitigate the perceived risks related to its governance and, at the same time, it could empower an ecosystem of services and products accessible through this digital currency, exploiting network effects. Such characteristics could allow both diffusion of information and adoption, reducing the common entry barriers to traditional currency.[8]

If the intermediation of private players is already dominating electronic and mobile payments, stablecoins could provide large private tech corporations with the opportunity to generate and record unique data on transactions directly on their independent infrastructure, facilitating the empowerment of faster, cheaper and more efficient solutions for data predictive analysis and tools. Network externalities are stronger when an ecosystem offers an integrated platform of services and products, creating value through knowledge. Digital payment solutions then become a tool to strengthen the business models of these players, which aim at building an 'aggregator of mutually complementary activities'.

8 Tobias Adrian and Tommaso Mancini-Griffoli, 'Digital Currencies: The Rise of Stablecoins', in *IMF Blog*, 19 September 2019, https://blogs.imf.org/?p=27149.

A further consolidation of digital payment solutions through stablecoins developed by private players could lead to a deeper concentration of cross-sources data aggregation, creating far-reaching implications for how data will be used within the ecosystem or shared with third parties.[9] Even though both established e-wallets (such as Google Pay or Apple Pay) and stablecoin's pivotal projects (such as Libra - recently renamed Diem -) have given assurances that they will not share or monetize financial data, these intermediaries could anyway ultimately access and gather information to empower their ecosystem. For example, if users integrate Calibra, Facebook's e-wallet, with their Messenger or WhatsApp accounts, Facebook will be able to track basic information, such as with whom or at which shop users have started a transaction, without needing specific approval by users themselves. Furthermore, in the name of convenience, large tech corporations are likely to encourage users to allow the free flow of information within their ecosystem's activities with the promise of rewards.

Despite private banking and non-banking players claiming that personal data is only used in an anonymized form, data is normally only protected by pseudonymized keys. To highlight how weak the system is, some experts were able to correctly track names or card numbers of 90 per cent of 1.1 million credit card holders only based on their 'anonymized' card transactions made over three months.[10] In addition to a set of technical concerns related to data protection, the aggregation of financial data could produce newer risks of anti-competitive use of data. Exploiting network effects and market dominance, big tech companies could be incentivized to engage in price discrimination (charging consumers different prices for the same product) due to the increasing information asymmetry between consumers and companies.[11] Think about Uber's 'route-based pricing'. This system uses various factors to set rates based on a prediction that evaluates how much a user will be willing to spend. Or consider the petition filed

9 G7 Working Group on Stablecoins, 'Investigating the Impact of Global Stablecoins', in *CPMI Papers*, No. 187 (18 October 2019), p. 15, https://www.bis.org/cpmi/publ/d187.htm.

10 Heike Mai, 'Cash Empowers the Individual Through Data Protection', in *Talking Point*, 2 July 2019, https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000495958/Cash_empowers_the_individual_through_data_protecti.xhtml.

11 Bank for International Settlements (BIS), 'Big Tech in Finance: Opportunities and Risks', in *Annual Economic Report 2019*, June 2019, p. 67, https://www.bis.org/publ/arpdf/ar2019e3.htm. See google patent: https://pdfpiw.uspto.gov/.piw?docid=08260657.

by Consumer Education Foundation with the Federal Trade Commission on Walmart's online shop. The former found that users could purchase a set of basic goods at different prices. Anonymous users were offered lower prices.[12] In this sense, aggregating financial data would radically increase the potential of predictive analysis models, maximizing the efficiency of their ecosystems. Therefore, to accurately assess and understand the possible effects of stablecoins connected to pre-existing ecosystems, the framework under which financial data is regulated in these ecosystems needs to be analysed in the wider context of a data-driven economy and of the competitive use of data, as showed by several studies carried out by international supervisory bodies.[13]

CBDCs could however mitigate the abovementioned issues by providing 'what the private sector cannot: privacy in payments'.[14] Thus, CBDCs could aim at counterbalancing the current dominance of private players in the mobile payment market.[15] Central banks are not profit-driven. They do not monetize the data they gather. Instead, their main aim is to ensure a robust and safe monetary system. By being able to track CBDC data more efficiently, central banks could better monitor the status of their domestic economy, reducing the existing information asymmetry when deciding on a monetary policy intervention. Data aggregation for central banks makes a lot of sense. A tighter control on transaction histories could improve their ability to fight money laundering and tax evasion, at the same time reducing the size of the informal economy.

While all this is true, central banks would also be able to access and collect information unavailable before, empowering a newer and deeper identification of users and payment flows. Beyond spending habits, it would enable location tracking and the accumulation of sensitive personal data. If misused, CBDCs could adversely foster an unprecedented centralisation of information in the government's hands. It is not a matter of predicting an Orwellian

12 REPRESENT project, *Secret Surveillance Scoring: Urgent Request for Investigation and Enforcement Action*, 24 June 2019, https://www.representconsumers.org/wp-content/uploads/2019/06/2019.06.24-FTC-Letter-Surveillance-Scores.pdf.

13 Maurice E. Stucke, 'Should We Be Concerned About Data-opolies?', in *Georgetown Law Technology Review*, Vol 2, No. 2 (2018), p. 275–324, https://wp.me/p8IxBy-zh.

14 Christine Lagarde, 'Winds of Change. The Case for New Digital Currency', in *IMF Speeches*, January 2019, p. 5, http://dx.doi.org/10.5089/9781484389171.076.

15 Alexander Kriwoluzky and Chi Hyun Kim, 'Public or Private? The Future of Money', in *Monetary Dialogue Papers*, December 2019, https://doi.org/10.2861/880099.

scenario, but of assessing potential risks related to a rise of public visibility into a financial system, altering the relation of power between citizens and governments. If financial transactions are fully traceable, public authorities may be incentivized to abuse data and, in some cases, it may facilitate political surveillance in domestic markets. Moreover, if retail and corporate consumers use a foreign CBDC, foreign governments may be able to directly gather data on those transactions (such as in projects for cross-border interbank settlement, migrant remittance, or in case of tourists or business travellers). If a domestic CBDC has different customer data privacy policies and safeguards, then foreign user data may be vulnerable when people use those CBDCs. For example, in 2018, the Office of the Privacy Commissioner of Canada advised its citizens to buy legal cannabis using cash, fearing that some countries could deny consumers entry if they find out that those consumers have purchased legal cannabis.[16]

These concerns are amplified in authoritarian regimes, where governments could drastically increase the efficiency of their surveillance and repression tools. For instance, if a citizen attends a political protest, the central bank could immediately freeze their CBDC account. Even in democratic countries governed by the rule of law, an extreme centralisation of payment history data could produce risks. Democracy is more fragile than many realize. The reduction of the information asymmetry would provide public authorities with additional power over citizens. There is a big difference between trusting a government to not misuse transaction data and trusting it to develop a system that is built to protect information.[17] Therefore, to mitigate risk, CBDCs should have privacy safeguards with compliance measures included in their design from the outset. This approach could ensure a more secure functional design. If, instead, privacy and compliance are added at a second stage, it could leave in loopholes.[18]

16 Canada's Office of the Privacy Commissioner (OPC), *Protecting Personal Information: Cannabis Transactions*, December 2018, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_can_201812.

17 Charles Kahn, 'Payment Systems and Privacy', in *Federal Reserve Bank of St. Louis Review*, Vol. 100, No. 4 (Fourth Quarter 2018), p. 337–344. https://doi.org/10.20955/r.100.337-44.

18 Ann Cavoukian, *Privacy by Design. The 7 Foundational Principles*, updated January 2011, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

8.2 Why is anonymity not a design issue?

Most of the current research underlines that a system can seek counterparty anonymity and/or third-party anonymity in payments. The former implies that payers do not reveal their identities to recipients. The latter instead implies that the true identities of payers and recipients are not accessible to parties not directly involved in the transaction. Whereas counterparty anonymity seems to be less controversial, third-party anonymity has remarkable implications as it directly affects the efficiency of AML procedures.[19] While it is easier to consciously blind counterparties – such as blinding merchants from accessing the true identity and transaction history of the payer – hiding this information from the government could be more complicated. These concerns drive the discussion over the choice between a token-based or account-based CBDC (see Chapter 1 in this volume). The former could provide better privacy for users by default, offering the opportunity to establish varying degrees of anonymity. This system would however increase risks related to financial integrity. The latter would, despite varying degrees of anonymity shaped by its design, resemble a model similar to deposits.[20] The two systems could also co-exist, exploiting their comparative advantages. In a recent paper, the Bank of Canada proposed an architecture in which larger transactions would be carried out through an account-based CBDC, while smaller-value transactions could use anonymous token-based options.[21] Where to set the cap for the token-account transactions or the amount at which AML rules would come into play is yet to be decided.[22]

In the vibrant research on possible design to protect users' privacy in CBDC's systems, the European Central Bank has developed an interesting proposal. The

19 Morten Linnemann Bech and Rodney Garratt, 'Central Bank Cryptocurrencies', in *BIS Quarterly Review*, September 2017, p. 55–70, https://www.bis.org/publ/qtrpdf/r_qt1709f.htm.

20 Santiago Fernández de Lis and Pablo Urbiola, 'Retail Central Bank Digital Currencies: Means of Payment vs Store of Value', in *SUERF Policy Notes*, No. 183 (July 2020), https://www.suerf.org/policynotes/15609/retail-central-bank-digital-currencies-means-of-payment-vs-store-of-value; Raphael Auer and Rainer Böhmep, 'The Technology of Retail Central Bank Digital Currency', in *BIS Quarterly Review*, March 2020, p. 93, https://www.bis.org/publ/qtrpdf/r_qt2003j.htm.

21 John Miedema et al., 'Designing a CBDC for Universal Access', in *Bank of Canada Staff Analytical Notes*, No. 2020–10 (June 2020), https://www.bankofcanada.ca/?p=212517.

22 Raphael Auer, Giulio Cornelli and Jon Frost, 'Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies', in *BIS Working Papers*, No. 880 (August 2020), https://www.bis.org/publ/work880.htm.

ECB acknowledged that 'the payments ecosystem needs to find an answer to an issue that concerns all citizens: the question of how to allow some degree of privacy in electronic payments, while still ensuring compliance with AML/CFT regulations.'[23] The technical solution proposed is to develop 'anonymity vouchers' for low-value transactions, while high-value transactions would be subjects to standard AML checks. Users would be granted time- and quantity-limited vouchers monthly, regardless of their account balances. These vouchers would not be transferable to other users and their value would be one voucher per one unit of CBDC. In the scenario described, the CBDC system would have four main features: (i) balances are not remunerated; (ii) it would be a two tier system; (iii) the ECB would be the only authorized issuer of CBDC units; and (iv) an ad hoc AML authority would monitor the parties involved in high value transactions. A two-tier system requires an intermediary to provide a user with a pseudonymous identity to be used as a network address for CBDC transactions. In case a transaction is carried out without an anonymity voucher, the intermediary will initiate the transfer via the AML authority, which will ultimately authorize or reject the transaction.[24]

In addition to a set of technical areas of improvement, a key question that could be raised in this scenario is of which factors the ECB will use to decide the limits of anonymity vouchers accessible to users. This will be a political decision rather than a technical one.

8.3 Multilateralism for (controllable) anonymity in CBDCs

If technical solutions exist to selectively blind governments and private corporations in digital currency systems,[25] the key questions are where the boundaries between anonymity and security are, and how to ensure that those boundaries are respected.[26] Full anonymity in digital currency systems is not desirable, as it could potentially ease illegal transactions and undermine compliance with regulations (KYC and AML). Similarly, no anonymity at all would

23 ECB, 'Exploring Anonymity in Central Bank Digital Currencies', cit., p. 3.

24 Ibid., p. 8.

25 Sarah Allen et al., 'Design Choices for Central Bank Digital Currency: Policy and Technical Considerations', in *NBER Working Papers*, No. 27634 (August 2020), https://www.nber.org/papers/w27634.

26 Sriram Darbha and Rakesh Arora, 'Privacy in CBDC Technology', in *Bank of Canada Staff Analytical Notes*, No. 2020–9 (June 2020), https://www.bankofcanada.ca/?p=212142.

produce unnecessary risk. Despite raising different sets of concerns on the effects of data visibility, both CBDCs and privately owned stablecoins would require a set of common rules to establish international standards on the degree of anonymity and privacy these systems should guarantee. On the one hand, the awareness has rapidly emerged that stablecoin's financial data accumulation is first a political matter, fostering an extensive debate on how to regulate identity and management of transaction data to mitigate the risks of moral hazard.[27] Although the international dialogue on this matter is not easy, several international organisations are collaborating to set global responses to the challenges produced by stablecoins.[28] Setting aside mitigation of money laundering and tax evasion risks and interoperability,[29] the political dimension of anonymity in CBDCs has been reduced to a discussion on design and technical solutions. While this is true, the answer lies in the technological infrastructure of a CBDC. However, the shape that an infrastructure takes is the result of an ex ante political decision, as clearly acknowledged by the IMF in a recent study.[30]

Moreover, the effects of the varying degrees of anonymity blur the boundaries of a domestic market. As fiat money operates in a globalized and interconnected world economy, national/regional CBDCs, being also accessed by foreign retail and corporate customers, could produce adverse effects both domestically and internationally. Therefore, to avoid potential misuse of data and ensure fair and transparent systems, international supervisory bodies should promote a

27 Financial Action Task Force (FATF), *FATF Report to G20 on So-called Stablecoins*, June 2020, http://www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html; G7 Working Group on Stablecoins, 'Investigating the Impact of Global Stablecoins', cit.; Financial Stability Board (FSB), *Addressing the Regulatory, Supervisory and Oversight Challenges Raised by "Global Stablecoin" Arrangements*, 14 April 2020, https://www.fsb.org/?p=20011.

28 Such as: Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the International Organization of Securities Commissions (IOSCO), the Financial Action Task Force (FATF), the Organization for Economic Co-operation and Development (OECD) and the Financial Stability Board (FSB).

29 FATF website: *Regulation of Virtual Assets*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html; and, *Public Consultation on FATF Draft Guidance on Digital Identity*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html.

30 John Kiffet al., 'A Survey of Research on Retail Central Bank Digital Currency', in *IMF Working Papers*, No. 20/104 (2020), p. 31, https://www.imf.org/en/Publications/WP/Issues/2020/06/26/A-Survey-of-Research-on-Retail-Central-Bank-Digital-Currency-49517.

multilateral effort to specifically discuss and establish the level of privacy that a CBDC system should provide. Even though anonymity and privacy concerns radically differ across countries due to diverse cultural, socio-economic and political contexts, a multilateral policy compromise could help achieve not an optimal solution, but basic shared pillars on how much privacy CBDC infrastructure should be designed to guarantee. This effort should be led by central banks and international organisations together with civil society, governments and private financial intermediaries. By this, citizens would be incentivized to trust CBDCs in domestic and foreign markets.

Finding a consensus on as highly sensitive and core subject as the rules for a national digital sovereign currency would be extremely complicated. Some countries would refuse to comply with any global standards. As in the current situation in the broader multilateral governance of digital space, where the major powers (the United States, China, and the EU) have different approaches and tend to pursue divergent interests, a multilateral dialogue on the degree of anonymity in CBDCs is likely to hit roadblocks. However, the establishment of a few common pillars adopted by a club of countries could guide more national legislations through spill-over effects. As highlighted by Hathaway and Shapiro, most current international laws have been shaped by this approach of 'shared interests and decentralized enforcement'.[31] Following Buchanan's economic theory of clubs, this 'club' of countries could influence the development of standards in other jurisdictions by cutting off access to their network of CBDCs to nations that do not comply with their rules. Partial or full exclusion from a shared network would undermine the economic benefits of the CBDC, incentivizing membership to gain the potential advantages of being in the club.[32]

Conclusion

Cash has created an information asymmetry among citizens, governments and private players, ensuring a degree of anonymity in transactions. The development of digital currencies, particularly CBDCs and privately owned stablecoins, could radically transform this equilibrium, allowing great visibility into financial data transactions. Whereas the implications of private corporations' data accumulation have raised several concerns among international and national

31 Oona Hathaway and Scott J. Shapiro, 'Welcome to the Post-Leader World', in *Foreign Policy*, 4 July 2020, https://foreignpolicy.com/2020/07/04/after-hegemony.

32 James M. Buchanan, 'An Economic Theory of Clubs', in *Economica*, New Series, Vol. 32, No. 125 (February 1965), p. 1–14.

policymakers, the discussion on the political dimension of anonymity in CBDCs appears to have been marginalized. Nevertheless, if the technological solutions to consciously blind governments exist, the degree of anonymity designed into the system must be determined by an ex ante political choice.

No anonymity produces privacy risks for users, ultimately threating individual freedom. It is therefore widely acknowledged that CBDCs need to guarantee some privacy to their users. However, there is no consensus in on which the degree of privacy. To avoid moral hazard and the political misuse of visibility in transaction data, a multilateral effort is needed to set the limits of anonymity that CBDCs should provide. CBDCs being a matter of sovereignty, it would be extremely difficult to find a global consensus on the issue. A solution could be to promote shared standards and boundaries on guaranteed privacy within a club of countries. Membership in such a network would foster economic advantages related to full interoperability, while non-members would have only partial or no access to the network.

This is the time to start such a discussion. In this period of intense research and development, before individual countries launch national CBDCs, countries should develop a common framework in which the boundaries of privacy and anonymity are set. As it is essential that privacy and anonymity by designed into the infrastructure at the very onset, this multilateral exercise must take place before it is too late.

References

Tobias Adrian and Tommaso Mancini-Griffoli, 'Digital Currencies: The Rise of Stablecoins', in *IMF Blog*, 19 September 2019, https://blogs.imf.org/?p=27149

Sarah Allen et al., 'Design Choices for Central Bank Digital Currency: Policy and Technical Considerations', in *NBER Working Papers*, No. 27634 (August 2020), https://www.nber.org/papers/w27634

Raphael Auer and Rainer Böhmep, 'The Technology of Retail Central Bank Digital Currency', in *BIS Quarterly Review*, March 2020, p. 85–100, https://www.bis.org/publ/qtrpdf/r_qt2003j.htm

Raphael Auer, Giulio Cornelli and Jon Frost, 'Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies', in *BIS Working Papers*, No. 880 (August 2020), https://www.bis.org/publ/work880.htm

Bank for International Settlements (BIS), 'Big Tech in Finance: Opportunities and Risks', in *Annual Economic Report 2019*, June 2019, p. 55–79, https://www.bis.org/publ/arpdf/ar2019e3.htm

Mark Bergen and Jennifer Surane, 'Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales', in *Bloomberg*, 30 August 2018, https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales

James M. Buchanan, 'An Economic Theory of Clubs', in *Economica*, New Series, Vol. 32, No. 125 (February 1965), p. 1–14

Canada's Office of the Privacy Commissioner (OPC), *Protecting Personal Information: Cannabis Transactions*, December 2018, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_can_201812

Ann Cavoukian, *Privacy by Design. The 7 Foundational Principles*, updated January 2011, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Committee on Payments and Market Infrastructures, 'Central Bank Digital Currencies', in *CPMI Papers*, No. 174 (March 2018), https://www.bis.org/cpmi/publ/d174.htm

Sriram Darbha and Rakesh Arora, 'Privacy in CBDC Technology', in *Bank of Canada Staff Analytical Notes*, No. 2020–9 (June 2020), https://www.bankofcanada.ca/?p=212142

European Central Bank (ECB), 'Exploring Anonymity in Central Bank Digital Currencies', *In Focus Papers*, No. 4 (December 2019), https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

Santiago Fernández de Lis and Pablo Urbiola, 'Retail Central Bank Digital Currencies: Means of Payment vs Store of Value', in *SUERF Policy Notes*, No. 183 (July 2020), https://www.suerf.org/policynotes/15609/retail-central-bank-digital-currencies-means-of-payment-vs-store-of-value

Financial Action Task Force (FATF), *FATF Report to G20 on So-called Stablecoins*, June 2020, http://www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html

Financial Stability Board (FSB), *Addressing the Regulatory, Supervisory and Oversight Challenges Raised by "Global Stablecoin" Arrangements*, 14 April 2020, https://www.fsb.org/?p=20011

G7 Working Group on Stablecoins, 'Investigating the Impact of Global Stablecoins', in *CPMI Papers*, No. 187 (18 October 2019), https://www.bis.org/cpmi/publ/d187.htm

John Gapper, 'Alibaba's Social Credit Rating Is a Risky Game', in *Financial Times*, 21 February 2018, https://www.ft.com/content/99165d7a-1646-11e8-9376-4a6390addb44

Oona Hathaway and Scott J. Shapiro, 'Welcome to the Post-Leader World', in *Foreign Policy*, 4 July 2020, https://foreignpolicy.com/2020/07/04/after-hegemony

Charles Kahn, 'Payment Systems and Privacy', in *Federal Reserve Bank of St. Louis Review*, Vol. 100, No. 4 (Fourth Quarter 2018), p. 337–344. https://doi.org/10.20955/r.100.337-44

John Kiff et al., 'A Survey of Research on Retail Central Bank Digital Currency', in *IMF Working Papers*, No. 20/104 (2020), https://www.imf.org/en/Publications/WP/Issues/2020/06/26/A-Survey-of-Research-on-Retail-Central-Bank-Digital-Currency-49517

Alexander Kriwoluzky and Chi Hyun Kim, 'Public or Private? The Future of Money', in *Monetary Dialogue Papers*, December 2019, https://doi.org/10.2861/880099

Christine Lagarde, 'Winds of Change. The Case for New Digital Currency', in *IMF Speeches*, January 2019, http://dx.doi.org/10.5089/9781484389171.076

Steven Levy and Gregory Barber, 'The Ambitious Plan Behind Facebook's Cryptocurrency, Libra', in *Wired*, 18 June 2019, https://www.wired.com/story/ambitious-plan-behind-facebooks-cryptocurrency-libra

Morten Linnemann Bech and Rodney Garratt, 'Central Bank Cryptocurrencies', in *BIS Quarterly Review*, September 2017, p. 55–70, https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

Heike Mai, 'Cash Empowers the Individual Through Data Protection', in *Talking Point*, 2 July 2019, https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000495958/Cash_empowers_the_individual_through_data_protecti.xhtml

John Miedema et al., 'Designing a CBDC for Universal Access', in *Bank of Canada Staff Analytical Notes*, No. 2020–10 (June 2020), https://www.bankofcanada.ca/?p=212517

Sridhar Ramaswamy, 'Powering Ads and Analytics Innovations with Machine Learning', in *Google Blog,* 23 May 2017, https://blog.google/products/marketingplatform/360/powering-ads-analytics-innovations-with-machine-learning-xp

REPRESENT project, *Secret Surveillance Scoring: Urgent Request for Investigation and Enforcement Action*, 24 June 2019, https://www.representconsumers.org/wp-content/uploads/2019/06/2019.06.24-FTC-Letter-Surveillance-Scores.pdf

Felix Salmon, 'Why Payments Won't Ever Be Anonymous', in *Reuters*, 16 December 2011, http://reut.rs/1pjAtfX

Maurice E. Stucke, 'Should We Be Concerned About Data-opolies?', in *Georgetown Law Technology Review*, Vol 2, No. 2 (2018), p. 275–324, https://wp.me/p8IxBy-zh

Alan F. Westin, *Privacy and Freedom*, New York, Atheneum, 1967

Nicola Bilotta and Fabrizio Botti - 9783034342926
Downloaded from PubFactory at 08/09/2021 11:57:01AM
via free access