The public, the private and the secret: Thoughts on privacy in central bank digital currencies

Received (in revised form): 16th June, 2021

David Ballaschk*
Senior Expert, Deutsche Bundesbank, Germany

Jan Paulick**
Principal Expert, Deutsche Bundesbank, Germany

David Ballaschk *is a senior payment expert for the Deutsche Bundesbank, where his work mainly focuses on cross-border and real-time payments. He is a member of various European working groups and has represented the Bundesbank in both the Cross-border Retail Payments Working Group and the Cross-border Payments Task Force. He has an MSc in economics from Martin-Luther University Halle-Wittenberg.*

Jan Paulick *is a principal expert in the Strategy, Policy and Oversight division in the Deutsche Bundesbank's Directorate General Payments and Settlement Systems. His work focuses on quantitative analysis of financial market infrastructures as well as the implications of digital money and blockchain technology. He holds an MA in international economics from the University of Göttingen; he has also studied at UC Santa Cruz and Delhi School of Economics.*

Abstract

This paper discusses the issues surrounding privacy and anonymity in the context of central bank digital currency (CBDC). Most notably, central banks calibrating the design criteria for CBDC must strike a balance between data protection and the individual's right to privacy on the one hand, and the prevention of financial crime on the other. In this regard, there are — from a technical and governance point of view — a number of possible solutions. By way of illustration, this paper constructs three exemplary and simplified privacy scenarios. The paper also describes the need for standards to ensure the responsible treatment of data, and clear rules guaranteeing that access is restricted to public authorities fulfilling their mandates. When it comes to protecting user privacy in a CBDC system, this paper argues that independent central banks are ideally positioned to serve as an honest broker. In this respect, gaining the public's trust and acceptance will be a key challenge for central banks.

Keywords: central bank digital currency (CBDC), privacy, anonymity, retail payments, central banks

INTRODUCTION

The digital age has posed new challenges to privacy. Digital services are becoming ever more commonplace in people's day-to-day lives. Apps are used for shopping, banking and connecting with people — particularly during the coronavirus pandemic, when physical interactions were limited by lockdowns. However, even before the onset of COVID-19, electronic data had already become an essential component in companies' marketing strategies, as well as a surveillance tool for governments.

People are willing to surrender some of their privacy in exchange for using digital services, often for free. This may be a conscious choice or an unwanted side effect of a platform economy. But what happens with personal data? How much information are

David Ballaschk

Jan Paulick

**Deutsche Bundesbank, Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main, Germany*
E-mail: david.ballaschk@bundesbank.de

***Deutsche Bundesbank, Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main, Germany*
E-mail: jan.paulick@bundesbank.de

Journal of Payments Strategy & Systems
Vol. 15, No. 3 2021, pp. 277–286

people willing to give up in order to use online services? Which actors can access said data? Experience suggests that people do not always like the answers to these questions. Data breaches can undermine trust in the ability of companies and public entities to protect people's data and may result in an overall loss of trust in digital privacy arrangements.

In most democratic states, privacy is regarded as a valuable asset that may only be restricted if there is an overriding public interest. In payments, privacy is vital to ensure a trusting relationship between customers and the parties handling their payments. Banks and other providers of payment services protect confidential information. However, with the entrance of new, more data-driven market actors, changes in payment behaviour, an increasingly digitised economy, and discussions around the world regarding the introduction of central bank digital currency (CBDC), the issue of privacy warrants closer investigation.

The role of cash in everyday transactions has been declining over the last years, and this trend is likely to continue.[1] At the same time, digital payments data offer valuable insights into people's personal lives. This prompts a number of questions. Can public authorities leave the issue of privacy to the private sector and regulation? Do people have a need, or even a right, to transact anonymously using CBDC? What safeguards must be put in place to protect personal data from misuse? Answering these fundamental questions is certainly beyond the scope of this paper, but there are a couple of anchoring points and issues in the context of CBDC that merit discussion.

When it comes to privacy in cashless payments, there is a risk that users may opt for too little privacy in their payment choices due to a public good aspect of privacy.[2] For this reason, the protection of personal data must be taken into account when designing a CBDC. Henceforth, this paper will focus on retail CBDC, which would be available to consumers and households. Nevertheless, the considerations also apply, to some degree, to wholesale CBDC, access to which is more restricted — mostly, to banks and a few other actors.

Any CBDC design must comply with the data protection requirements of the respective jurisdiction,[3] while at the same time providing authorities with the information necessary to conduct, for example, anti money-laundering (AML) or know-your-customer (KYC) checks. In such circumstances, the need to conduct due diligence trumps the need to protect privacy. Essentially, users should have control over who is using and sharing their personal data and how. Privacy is one of the most complex issues in the CBDC discussion and the issue that probably sparks the most heated debates in the public domain. By way of example, the recent public consultation by the European Central Bank (ECB) found that respondents rank privacy as the most important feature of a potential digital euro.[4]

PRIVACY AND ANONYMITY IN ELECTRONIC PAYMENTS

Privacy and anonymity are terms that are often used interchangeably, but actually represent different facets of confidentiality.[5] Furthermore, both aspects come with different layers, adding complexity to the question of confidentiality. While anonymity in a payments context means that the parties involved remain unknown, privacy means that the content of the communication remains hidden to everyone but the actors involved in the payment transaction. Both aspects are interlinked: anonymity may help guarantee some form of privacy, as the data are harder to attribute to a specific person. On the flipside, anonymity efforts may be in vain if the message content is not kept private and contains sufficient information to identify the users.

Discussions on preserving privacy or anonymity in electronic payments have become more of a pressing issue as the use of cash as a settlement medium is declining in many countries, with the COVID-19 pandemic accelerating this dynamic. With the entrance of new actors into the retail space, privacy in electronic systems could experience a paradigm shift.

While the anonymity and privacy of cash is a by-product of its physical nature, the privacy of cashless payments must be ensured either through governance rules and legal arrangements, or through the design of the system itself (ie 'privacy by design'), or, better yet, both.[6] There have been multiple ideas on designing electronic payment systems that enable users to transact anonymously, or that at least ensure privacy. The best-known example is Bitcoin, which enables pseudo-anonymous transactions where random addresses are visible in the network, but the identity of users is unknown. One recently proposed solution in the context of CBDC is the use of blind signatures.[7] However, electronic payments leave digital footprints that make the preservation of privacy difficult or impossible to achieve in some settings, especially in settings where other policy considerations and regulatory compliance take precedence. The underlying reason is that, even in the absence of an intermediary, there must still be a ledger of some kind to prevent double-spending.[8] In addition, regulatory requirements oblige service providers to store certain user information and share it under certain circumstances to support public interests like preventing money laundering and combating the financing of illicit activities.

THE ROLE OF PRIVACY IN THE PAYMENTS MARKET

For reasons both good and bad, people value their privacy, and cash is used the world over by those who want their payments to remain private or who want to remain anonynymous. Moreover, in many jurisdictions the right to privacy is codified in law (eg the Charter of Fundamental Rights of the European Union and the EU General Data Protection Regulation) as well as in Article 12 of the Universal Declaration of Human Rights.[9,10]

With most central banks having no desire to abolish cash if and when they introduce a CBDC, an anonymous payment instruments will therefore continue to exist. However, even in countries where cash has the status of legal tender and its acceptance is mandated, there may be a stigma associated with its use. For example, cash payers could be seen as unbanked or having something to hide. Recently too, fear of coronavirus transmission may have added to (unwarranted) stigma surrounding the use of cash.[11] Furthermore, in increasingly digitised economies cash acceptance may decline to a point where some users are unable to use cash for transactions they want to keep private (if merchants accept cashless payments exclusively, this may be viewed as discriminatory practice[12]). Such developments prompt the question whether central banks should step in to provide a form of digital money that offers higher levels of privacy than private solutions.

Some users may wish to retain the anonymity of cash for their CBDC transactions. The properties of cash are inherent to its nature, but not fully transferable into a digital context. Certain aspects of CBDC — mainly its digital nature — make it significantly harder to achieve a similar level of anonymity and privacy as cash. Furthermore, a comparable degree of anonymity is not possible because a fully confidential digital means of payment could facilitate money laundering and the financing of criminal activities. For central banks, as the governing entities of such platforms, this would entail reputational risks. At the same time, the use of cash is often restricted via

upper limits, reporting requirements and other measures for combating money laundering and the financing of terrorism. The issue often lies in enforcing restrictions. One could argue that as long as cash continues to exist as a complement to CBDC and there is still sufficient cash acceptance on the merchant side, people will always have a fallback option for anonymous and private payments.

Privacy in this context refers to the payment process. Traditional actors do not appear to heavily leverage payment data for unintended purposes. However, issues of privacy most often do not lie in the treatment of payments data. Users often exhibit some ambivalence in their behaviour or appear to be willing to surrender personal information voluntarily. For example, consumers who shop online or use cashback programmes transfer data to third parties, with payments data typically benefiting from safeguards concerning, among other things, the transfer of identity data to merchants. CBDC will most likely not affect the use of cashback programmes, but might affect the availability of payments data to different actors in the marketplace.

Payments constitute some of the most private information about individuals and represent valuable data in terms of revealing true preferences, connections and whereabouts. Compared with survey data, payments constitute unbiased information based on actual transactions. The increasing uptake of cashless payments and influx of new actors into the market therefore highlight a general tendency that poses new challenges to public authorities. In combination with limited consumer choice, private enterprises or governments could economically exploit consumer data, with negative implications for society as a whole.

Private enterprises involved in supplying payments are often inherently interested in gathering data on users. The advent of big tech firms could adversely affect the issue of privacy as consumers implicitly pay with their data for payment services.[13] Furthermore, data are an increasingly valuable part of business models in the digital economy. The pressure on traditional actors to leverage customer data may increase in tandem.

As central banks consider issuing CBDCs that would constitute a liability on their balance sheet, similar to cash, the issue of privacy could become a distinguishing feature. As payments often represent two-sided markets, a 'data-neutral' approach to CBDC could generate sufficient demand for a publicly owned retail payment infrastructure. Payment providers and users have different preferences and incentives for using different forms of payment instruments. Preferences among consumers also differ across demographic characteristics, countries and regions. Today's payment instruments differ quite substantially in terms of their privacy profiles.[14,15] Providing different levels of privacy thus offers choice to users. In this respect, a CBDC would be introduced with a specific privacy profile and could compete with private market solutions. Ensuring a level playing field, payment providers would have the right to introduce the same level of privacy for their payment services. However, the difference would lie in the offering institutions and the trust of users towards them.

CONFLICT BETWEEN PRIVACY, DATA PROTECTION AND AML/KYC REQUIREMENTS

Central banks calibrating the design criteria for a CBDC must strike a balance between data protection and the individual's right to privacy on the one hand, and the public interest in combating the financing of terrorism (CFT) and money laundering on the other. A fully anonymous electronic payment instrument would not be compatible

with the regulator's AML/CFT obligations. For example, it could increase the risks for law-abiding citizens, as it might lead to an increase in criminal activities such as ransom extraction crimes, which were an issue with Bitcoin. Regulatory compliance is therefore not a goal for its own sake. Central banks should not turn back the clock on progress regarding AML and CFT. At the other end of the spectrum, a partially or fully transparent CBDC could be misused as a surveillance instrument by governments. Furthermore, such a design choice does not seem compatible with the fundamental rights of data protection and privacy mentioned above.

For a CBDC to comply with the legal regulations and requirements under the AML and CFT rules, users must be authenticated by at least one institution and transactions must be monitored in some capacity. Possible authenticating entities would be the issuing authority, network participants in charge of onboarding users, operators, or a separate institution integrated into the network. As central banks do not typically engage directly with the general public, and authenticating a large number of users poses immense operational challenges, authentication is likely to lie in the realms of the private sector.

One central duty of care, in addition to identifying the contractual partner and, if applicable, the beneficiary, is the ongoing monitoring of business relationships and transactions. Currently, complex IT systems fulfil this purpose. These systems are designed to detect unusual or suspicious transactions, and their effectiveness and efficiency ultimately depend on the information available in the payment chain.

Widening the scope to cross-border CBDC use, the complexity of the issue increases further. The lack of harmonised KYC/AML rules has been identified as one of the main frictions of cross-border payments, and is currently being addressed by the G20 as part of its roadmap to enhance cross-border payments.[16,17] While CBDCs have the opportunity to start from a relatively clean slate technically, the business design still depends on the AML/KYC rules in the respective jurisdictions. One could say that form not only follows function, but must also follow the rules. Consequently, a global harmonisation of KYC/AML requirements might contribute positively to a technical harmonisation of the privacy aspect of CBDCs and may help to prevent regulatory arbitrage.

Furthermore, global coordination in CBDC design is ultimately necessary to ensure efficiency for cross-border payments. Other than the technical aspect of interlinking the platforms, the aspect of data-sharing across borders plays a major role. It must be ensured that only the minimum necessary data are shared and that the recipients of data in other countries store the data securely.

TECHNICAL FRAMEWORK AND PRIVACY SCENARIOS

To strike a balance between data protection requirements and the need for AML and CFT, there are multiple design options for a CBDC. Depending on the technical design, some participants in the network may be able to see some or all of a token's ownership history, while wallet holders see only the transactions they are involved in. Distributed ledger technology (DLT) applications can pose a challenge in terms of preserving privacy owing to their decentralised design. Certain technical solutions make it possible to conceal the transaction history for individual actors in order to achieve a higher degree of privacy. These include, for example, cryptographic methods for encrypting transaction data or methods for shortening the transaction history. There are also techniques for pseudo-anonymising user names so that the name of the end user is only made known to selected parties.

Chaum *et al.* describe a framework that emulates the cash cycle quite closely.[18] Commercial banks authenticate users and merchants, but only observe withdrawals of CBDC by users and incoming payments to merchants. This could enable them to perform sufficient AML and CFT checks while individual payment transactions remain private. However, whether such an arrangement would sufficiently and effectively ensure regulatory compliance is open to debate. The central bank would maintain an online ledger to prevent double-spending, but would observe neither user identities nor transaction contents.

From a technical point of view, configurations are highly flexible and seem to support almost any specification and level of privacy. This flexibility could also be used when applying different privacy models in a single CBDC design, eg by linking the privacy level to the amount or transaction history of a user.

CBDC models based on accounts or tokens have implications for privacy. Account-based models are inherently linked to identity, whereas token-based models (value-based) could offer higher levels of anonymity or privacy (the distinction is subject to some debate and may not be critical in the context of CBDC; important here is the level of privacy that different models could offer[19,20]). However, depending on their design, tokens can potentially carry the full history of ownership and allow all previous owners to be traced, while accounts could potentially be pseudonymous, with the identity behind the account number being stored at a different entity. Tracing money can offer improvements in the context of AML and CFT, but also have negative implications for users and their right to privacy. In addition, this might not align with existing regulations concerning the right to be forgotten, and safeguards could be circumvented by bad actors. The choice of technology may enable or prohibit certain privacy-by-design features. Interoperable technologies may make it possible to tailor a CBDC to the needs of its users. For example, a wholesale CBDC could be constructed based on a token model, while retail CBDC could rely on account balances.

Importantly, the question matters: privacy from whom? It is quite common for people to share personal data with private companies which then monetise that data. Therefore, it may seem conceivable for people to trust public authorities to have visibility on basic information to ensure compliance with AML and CFT regulations. But it may also be possible that people who share private information with companies would hesitate to do so with government bodies, given that the latter have stronger rights to intervene in the personal freedom of individuals.

Consumer trust differs across different counterparties. Survey data for the USA shows that consumers are most likely to trust traditional financial institutions with their data, followed by FinTech firms and government agencies, while big tech firms enjoy lower levels of trust.[21] However, trust in public offices has been declining in recent years, with only 45 per cent of citizens in Organisation for Economic Co-operation and Development member countries trusting their governments before the pandemic.[22] That said, central banks may benefit from a higher level of trust than the general government.

Regarding the privacy of CBDC users, a responsible *operator* should be in charge of fulfilling legal requirements and may grant *government agencies* access to data if there is a court order or legal mandate to do so. In this context, operators include all parties involved in the processing of payments and could include wallet providers, commercial banks and central banks, depending on the design choices. A certain level of anonymity and privacy may be maintained towards the

Table 1: Exemplary and simplified privacy scenarios

	Operator	*Government agencies*	*Third parties*
Low privacy	Data access	Data access	No data access
Baseline privacy	Data access	No data access (with exceptions for law enforcement)	No data access
High privacy	No data access (if technically feasible)	No data access	No data access

operator and could differ between the different operating parties, but must not interfere with operational requirements. Institutional separation of the operator from the executive bodies of government, which would be the case if an independent central bank were the provider of CBDC, may help generate additional levels of trust. Most importantly, the data must be protected from the unauthorised access of *third parties* in all scenarios to ensure public acceptance.

For the privacy level of a CBDC, there are a number of design choices that lie between full privacy and full transparency.[23] Central banks must clarify which actors get access to what data under which circumstances. Based on these aspects, three exemplary and simplified privacy scenarios are constructed as a basis for further discussion (Table 1).

Limited confidentiality/low privacy

It may be in the interest of governments to introduce a CBDC that is as transparent as possible. In such a low privacy scenario, both government agencies (which may include tax authorities, law enforcement and/or financial crime units) and the operator of the background infrastructure would have default access to the data generated by users. In this scenario, government agencies would not have to go through the operator to gain access to payment data, possibly paving the way for misuse. The identities of users may be known by both operators and government agencies taking part in the network. Other users and third parties not involved in the payment transaction would not have any visibility of identities and transaction contents. In this scenario, people who are sensitive at least to a small degree to data protection issues may refrain from using CBDC.

Controllable confidentiality/baseline privacy

A CBDC could be designed in such a way that transactions are transparent in principle for the operator of the network and all the parties involved in the respective transaction. Providers of CBDC services would be obliged to check the identity of users and monitor their activities in order to be able to report suspicious transactions to the responsible authorities. However, it would also be conceivable for the identity to be known only to a separate authority in the network (eg eID database administrators responsible for money laundering checks). Depending on the national legislation, payers do not necessarily have to reveal their identity to the recipient of the payment — for example, to a supermarket. In this respect, confidentiality towards unauthorised parties and recipients is guaranteed, while traceability could be provided for law enforcement authorities and supervision through data provided by the operator in certain circumstances. Transaction monitoring could be done even without knowing the identity of the user. User acceptance may depend on

the credibility and trust in the entity safeguarding the data.

Selective confidentiality/high privacy

If the identity of users is determined when they first gain access, different degrees of anonymity are conceivable. Selective anonymity could mean, for example, that payments below a specified threshold value could be anonymous, both to the payee and to the operator or the parties of the CBDC network. However, it is doubtful whether such a procedure would effectively fulfil AML regulations, as criminals could circumvent the existing rules. Such an approach could also be difficult to understand from a consumer perspective. A privacy-by-design approach — where transactions contents are technically obscured but the user's identity can be revealed in cases of suspicious activities, according to predetermined and transparent rules — might be an approach that provides a high level of privacy while ensuring basic regulatory compliance. This would require further analysis and possibly the introduction of additional safeguards, such as limits.[24] Limitations could decrease user demand while high privacy might increase CBDC acceptance and use.

USER PREFERENCES FOR PRIVACY

One deciding factor for the success of CBDC is acceptance on the user side of payments, which may depend on the level of privacy the CBDC offers to its users. There is strong evidence that users generally prefer a high level of privacy when choosing between payment methods. In the Bundesbank's 2020 study on payment behaviour, 94 per cent of respondents cited privacy as a very important feature of payment instruments, with 59 per cent of respondents rating protection of privacy as absolutely crucial for choosing a payment instrument.[25]

The rise of so-called cyptocurrencies (we prefer the term crypto tokens) has highlighted that there is some demand for privacy-preserving electronic systems. For example, Bitcoin allows users to transact pseudo-anonymously, meaning transactions are traceable, but the user's identity is not revealed within the network. However, Bitcoin has evolved more into a speculative investment and is used only for payments — the original intended use case — in a niche market thus far.

It is not just individuals who might want to send or receive illicit payments or protect their data from the government who are demanding privacy — the wider general public, too, are interested in keeping their data protected from other parties in the network. This may be the case for payments for medication, where disclosure could be followed by deeper repercussions from third parties (eg employers, insurance companies) or just mere annoyance, such as becoming a target for spam mails.[26] There is a legitimate case for protecting one's personal data from exploitation for unintended purposes, which is why data protection legislation like the EU General Data Protection Regulation exists. The desire to keep data private unless consumers agree otherwise should not be stigmatised.

It may therefore be beneficial to provide a payment instrument that fulfils users' demand for privacy in an environment where cash cannot be used. However, different user groups may prefer different degrees of privacy. There may be privacy fundamentalists who will not use an online payment instrument unless it offers full privacy and anonymity. Other users may be satisfied simply to know that their payment data are in safe hands. Public providers like independent central banks may have a potential competitive advantage here, because they lack the incentive to share payment data or personal information. As long as the data are not disclosed to third

parties, a wide range of users may have a preference for CBDC in such a setting.

INDEPENDENT CENTRAL BANKS — A TRUSTWORTHY PROVIDER OF PRIVACY

At the end of the day, a decentralised structure does not necessarily ensure privacy or anonymity. As soon as a wallet is linked to a bank account, a user's identity will become visible, for example. What matters are governance structures and trust that data are not being mishandled and misused.

Standards are needed that ensure the responsible treatment of data, and there must be clear rules guaranteeing that access is restricted to public authorities fulfilling their mandates. Independent central banks are ideally positioned to serve as an honest broker in protecting user privacy in a CBDC system. The other side of the (electronic) coin is that privacy is a hot topic that bears high reputational risks for central banks. Data breaches in the system and even in the surrounding ecosystem could undermine trust in the payment system and consequently also in central banks as the operators or overseers of that system. Central banks may also face political pressure which could threaten their independence.[27]

Cash is the best-known product of central banks. A digital form of money would constitute another product associated with them. Gaining and maintaining public trust and acceptance will be a challenge. Carefully designing a well-functioning system to maintain trust will be even more challenging if CBDC is implemented.

However, central banks can rise to the challenge. After all, providing means of payment that protect users' privacy is nothing new to them. Central banks are well experienced in operating wholesale payment systems used by banks, so why not offer a retail infrastructure for the digital world and thrive in the role of privacy provider?

ACKNOWLEDGMENTS

The authors thank Martin Diehl, Jochen Metzger, Matthias Schmudde, Dirk Schrade and Heike Winter, as well as the two anonymous referees for highly useful comments and feedback. The views expressed in the paper are solely those of the authors and do not necessarily represent the views of the Deutsche Bundesbank or the Eurosystem.

REFERENCES

(1) Auer, R., Cornelli, G. and Frost, J. (2020) 'COVID-19, cash, and the future of payments', *BIS Bulletin*, No. 3, Bank for International Settlements, available at: https://www.bis.org/publ/bisbull03.pdf (accessed 8th July, 2021).

(2) Garratt, R. and M. van Oordt (2021) 'Privacy as a public good: a case for electronic cash', *Journal of Political Economy*, Vol. 129, No. 7, pp. 2157–2180.

(3) See, for example, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

(4) European Central Bank (2021) 'Eurosystem Report on the Public Consultation on a Digital Euro', available at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf#page=4 (accessed 8th July, 2021).

(5) Gritzalis, S. (2004) 'Enhancing web privacy and anonymity in the digital era', *Information Management & Computer Security*, Vol. 12, No. 3, pp. 255–287.

(6) Camenisch, J., Piveteau, J.-M. and Stadler, M. (1994) 'An efficient electronic payment system protecting privacy', in in Gollmann D. (ed.) 'ESOCRIS 94: Proceedings of the Third European Symposium on Research in Computer Security, Brighton, 7th–9th November', Springer, pp. 207–215.

(7) Chaum, D. (1983) 'Blind signatures for untraceable payments', in Chaum D., Rivest, R. L. and Sherman, A.T. (eds) 'Advances in Cryptology', Springer, Boston, MA, pp. 199–203.

(8) Armelius, H., Claussen, C. A. and Hull, I. (2021) 'On the possibility of a cash-like CBDC', Sveriges Riksbank Staff memo, available at: https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf (accessed 8th July, 2021).

(9) Bank of England (2020) 'Central bank digital currency: opportunities, challenges and design', discussion paper, available at: https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf (accessed 8th July, 2021).
(10) Griffoli, T., Peria, M., Agur, I., Ari, A., Kiff, J., Popescu, A. and Rochon C. (2018) 'Casting light on central bank digital currencies', IMF Staff Discussion Notes, No. 18/08, available at: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233 (accessed 8th July, 2021).
(11) Orcutt, M. (2020) 'No, coronavirus is not a good argument for quitting cash', *MIT Technology Review*, 12th March, available at: https://www.technologyreview.com/2020/03/12/905341/coronavirus-contaminated-cash-quarantine/ (accessed 8th July, 2021).
(12) Selyukh, A. (2020) 'Cities and states are saying no to cashless shops', NPR, 6th February, available at: https://www.npr.org/2020/02/06/803003343/some-businesses-are-going-cashless-but-cities-are-pushing-back?t=1625741156054 (accessed 8th July, 2021).
(13) Sveriges Riksbank (2020) 'Second special issue on the e-krona', *Economic Review*, Vol. 2020, No. 2, available at: https://www.riksbank.se/globalassets/media/rapporter/pov/engelska/2020/economic-review-2-2020.pdf (accessed 8th July, 2021).
(14) Bagnall, J., D, Bounie, K, Huynh, A, Kosse, T. Schmidt and S. Schuh (2016) 'Consumer cash usage: a cross-country comparison with payment diary survey data', *International Journal of Central Banking*, Vol. 12, No. 4, pp. 1–61.
(15) Darbha, S. and R. Arora (2020) 'Privacy in CBDC technology', Bank of Canada Staff Analytical Notes, 2020-9, available at: https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/#:~:text=Privacy%20in%20a%20CBDC%20goes,requires%20consultation%20with%20external%20parties (accessed 8th July, 2021).
(16) Financial Stability Board (2020) 'Enhancing Cross-border Payments — Stage 1 report to the G20: Technical background report', available at: https://www.fsb.org/wp-content/uploads/P090420-1.pdf (accessed 8th July, 2021).
(17) Financial Stability Board (2020) 'Enhancing Cross-border Payments, Stage 3 roadmap', available at: https://www.fsb.org/wp-content/uploads/P131020-1.pdf (accessed 8th July, 2021).
(18) Chaum, D., Grothoff, C. and Moser, T. (2021) 'How to issue a central bank digital currency', Swiss National Bank Working Paper 2021-03, available at: https://www.snb.ch/n/mmr/reference/working_paper_2021_03/source/working_paper_2021_03.n.pdf (accessed 8th July, 2021).
(19) *Ibid*.
(20) Garratt, R., Lee, M., Malone, B. and Martin, A. (2020) 'Token or account-based? A digital currency can be both', Federal Reserve Bank of New York, Liberty Street Economics, available at: https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both.html (accessed 8th July, 2021).
(21) Armantier, O., Doerr, S., Frost, J., Fuster, A. and Shue, K. (2021) 'Whom do consumers trust with their data? US survey evidence', *BIS Bulletin*, No. 42, Bank for International Settlements, available at: https://www.bis.org/publ/bisbull42.pdf (accessed 8th July, 2021).
(22) Organisation for Economic Co-operation and Development (n.d.) 'Trust in Government', available at: http://www.oecd.org/gov/trust-in-government.htm (accessed 8th July, 2021).
(23) Deutsche Bundesbank (2020) 'Money in programmable applications — cross-sector perspectives from the German economy', Working Group on Programmable Money, available at: https://www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf (accessed 8th July, 2021).
(24) Chaum *et al*., ref. 18 above.
(25) Deutsche Bundesbank (2021) 'Payment behaviour in Germany', available at: https://www.bundesbank.de/en/publications/reports/studies/payment-behaviour-in-germany-738024 (accessed 8th July, 2021).
(26) Kahn, C. (2018) 'Payment systems and privacy', *Federal Reserve Bank of St. Louis Review*, Vol. 100, No. 4, pp. 337–344.
(27) Chaum *et al*., ref. 18 above.