MIT DCI response to Bank of England CBDC discussion paper

Digital Currency Initiative (DCI)

1. The DCI is a research group based at the Massachusetts Institute of Technology (MIT) within the Media Lab. The DCI employs researchers from a diverse set of backgrounds including technology and public policy experts.

2. This paper is the DCI response to the Bank of England discussion paper published on March 12, 2020.[1] Our response is structured to address the seven ways in which CBDC could support the Bank's objectives set out in chapter 2 of the discussion paper.

Supporting a resilient payments landscape

3. Adding CBDC to the existing payments landscape improves resilience in two ways. The first is by creating redundancy in retail payments generally. Presently there is high concentration in retail payments such that a high volume of retail payments in an economy are reliant on one or two major card networks.[2] If one of these systems fails CBDC would provide an alternative method of moving money from households to businesses (the CBDC model contemplated in the paper being a retail system), especially as cash declines. The second way is through architecture. For this to be a positive factor the architecture of the CBDC system has to be sufficiently different from existing payment systems that it will not suffer similar failures. In addition, the creation of CBDC provides the opportunity to use an architecture that is inherently more resilient than what has gone before it.

4. The concept of resilience also has different aspects, it includes both resilience to failure (unintentional) and resilience to attack (intentional). Increasing resilience of a system means both reducing the probability of failure and susceptibility to attack in addition to mitigating the effects. The design of a CBDC affects all of these issues.

Access

5. Existing payment systems – retail and wholesale – make the system difficult to attack by limiting access. There are different types of access to the system, for example retail payment systems have members, merchants and end users and all of these types of access are limited in different ways. Becoming a member of a payment system is a laborious process and in turn those members limit who they allow to use the system. Once admitted there are rules in place to ensure that there are negative consequences for members and users attacking the system and mechanisms in place to expel them if

[1] https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

[2] See for example the DNB's concern over the Netherlands reliance on Mastercard (p11 of Occasional Study CBDC, De Nederlandsche Bank, April 2020)

they try. This does not prevent attacks on payment systems but resilience is achieved by restricting access – in essence various obstacles are put in the way of anyone who wants access to the system, impeding would be attackers.

6. Cryptocurrencies achieve resilience in a different way. For example, access to the Bitcoin system is not limited at all. Anyone can maintain a copy of the ledger, submit transactions, create transactions and accounts as well as validate transactions. There are no obstacles to participation, instead relying on the system of incentives and technical measures to deter attacks.

7. For example, Bitcoin uses digital signatures to validate transactions. Signatures are secured using public key cryptography meaning that if a user can keep their secret key secure then it is computationally infeasible to forge their signature. It is possible for an attacker to submit a transaction with a false signature but such a transaction would be rejected by the nodes in the Bitcoin network and the transaction would likely never make it into a block. The reason for this is that any block containing an invalid transaction would ultimately be rejected by the network once it had been mined so there is a strong incentive for miners not to include invalid transactions.

8. Another method of adding resilience to the system is to restructure it in a way that eliminates the need for the information needed to make the payment (e.g. card details) to be shared. The use of public key cryptography is an example of this method. Bitcoin does not require the information needed to make the payment (the secret key) to be shared with the recipient of the payment. This improves resilience of the system by eliminating the need to transmit and store information which is required to make a payment. This is a structural improvement over existing payment models such as credit cards which requires the information needed to make the payment (card details) to be transmitted securely to the vendor and, in some cases, stored for future purchases. The structural weakness of the credit card system is that this information has to be transmitted, stored and policed when it could simply be eliminated using a different technique.

9. None of this is to say that a CBDC can wholesale adopt the techniques of a cryptocurrency to have a completely open system. However central banks can learn useful lessons on CBDC design from cryptocurrencies such as Bitcoin which has operated successfully in a hostile environment for over a decade. This type of resilience is an impressive feat and should be studied carefully for lessons which could be applied to CBDC.

Simplicity

10. At present there are two generations of cryptocurrency systems. The first generation started with Bitcoin and its clones. This generation uses Bitcoin script to add programmability to the system. The Bitcoin script is a relatively simple language, it is not

Turing complete and uses an interpreter alone to run scripts. One consequence is that Bitcoin is limited in terms of its programmability but this is a deliberate choice to reduce the attack surface.

11. The second generation of cryptocurrencies, most notably Ethereum launched in 2015, differed from Bitcoin by adding extra functionality in their scripting languages. Ethereum Virtual Machine (EVM) code is Turing complete and most developers use a compiler on top of an interpreter. This makes Solidity more expressive and considerably more complex than Bitcoin script.

12. As with most technological design decisions this choice represents a tradeoff. Bitcoin has opted for a simpler system in which less can go wrong and offers a smaller attack surface. This means Bitcoin users cannot do as much with their scripts but they gain a simpler and more secure system – because it can do less, less can go wrong.

13. Ethereum can do more but that added functionality comes at the cost of greater risk of failure and an increased attack surface. Ease of programming is another factor, it's harder to write Bitcoin script which discourages creating complexity. Solidity, the most popular language for creating smart contracts in Ethereum, is easier to use which means it is easier to add complexity to the contracts people create.

14. The question for CBDC architecture is where it should be located along this spectrum - from no programmability to an Ethereum like system. Some degree of programmability is desirable to meet the other CBDC goals outlined in the Bank's discussion paper such as improving the usability of central bank money, supporting innovation and interoperating with other systems. Therefore, a CBDC should have sufficient functionality to be able to support these functions. More than a decade of experience with Bitcoin script has shown that a relatively limited set of functions – a smaller set than Bitcoin has – are required to implement a layer 2 network or cross chain swaps, for example.

15. As a starting point therefore, CBDC experiments should start with the minimum programmability required to implement the desired features. The CBDC can be architected in a way that allows it to be upgraded over time so that design decisions made at the start do not permanently limit the possibilities of the system.

Redundancy

16. Hardware fails all the time for a variety of reasons so any system has to be engineered to withstand failure in part of the system. Bitcoin achieves this by having a network of nodes and miners that maintain and update the ledger, creating redundancy in the system. Any one of the miners or nodes can fail and the network can continue to function.

17. One of the questions which crops up repeatedly is whether CBDC should use a distributed ledger. In practice, as the discussion paper acknowledges in section 6.3, any CBDC system is likely to be distributed to some degree in the sense that there will be multiple copies of the ledger that need to be synchronized. The question is how many copies of the ledger would there be and who operates them.

18. One option is for a central bank to maintain all the copies of the CBDC ledger itself. This solution would be fully centralized from an institutional perspective but decentralized from an architectural perspective. Alternatives considered in the paper include private participants in the system and other central banks maintaining copies of the ledger.

19. The discussion paper notes the tradeoff between redundancy and performance. The more copies of the ledger there are in the system the longer it will take to synchronize the data across all the ledgers. One method is to optimize the performance of the databases and keep the total number of ledgers to a minimum. This approach can work up to a point – maximum throughput of existing retail payment systems is significant, for example in 2017 the Visa network claimed a maximum capacity of 65,000 transactions per second.[3]

20. Any system with a significantly decentralized architecture will probably not be able to match this performance in the core ledger. By comparison, Bitcoin can manage about 7 transactions per second on the core ledger. While there may be certain optimizations which could increase this number, a decentralized system like Bitcoin will never approach the core ledger performance of a much more centralized system.

21. An alternative to increasing the throughput of the core ledger is to investigate whether all transactions in the system need to be put through it. Layer 2 solutions such as the Lightning Network[4] have emerged in Bitcoin which allow users to make many more payments much more quickly with only a couple of transactions anchoring them to the core ledger. Layer 2 solutions such as the Lightning Network in Bitcoin are an elegant solution to the problem of scaling and decentralization and any CBDC project should explore how such innovations could be adapted to the CBDC use case. This is another example of how CBDC architecture can learn from experiments first tried in cryptocurrencies.

Avoiding the risks of new money creation

22. Stablecoins pose risks to monetary and financial stability as well as democratic accountability.

[3] https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf
[4] https://lightning.network/lightning-network-paper.pdf

23. A stablecoin is a representation of a unit of national currency which is backed by some kind of asset which gives the coin value. There are obvious financial stability risks from managing the credit and market risks of the backing asset whatever it may be. The only way of solving the problem of risk in the backing asset is for the central bank to require stablecoin issuers to back their currencies 1:1 with central bank reserves. Such a system would be similar to the Bank's own requirements for Scottish and Northern Irish banknotes.[5] In a scenario where a central bank has decided to make CBDC available to the public it is simpler to require wallet providers to join the CBDC system rather than creating the complexity of a parallel system of stablecoins which would need a separate regulatory architecture to manage the unique risks they pose.

24. From a monetary policy perspective multicurrency stablecoins like Libra pose the risk of substitution by stealth. The composition of the backing asset is decided by a private entity with no reference to the democratic accountability mechanisms under which central banks operate. At the start the currency could be predominantly backed by the local currency but in response to a shock or other financial crisis this could rapidly change leaving the local population with what is, in effect, a foreign currency and severely diminishing the central bank's ability to influence the economy.

25. In the case of Libra, its governing Libra Association recognized this concern and updated its proposal with the following:

> "*To limit concerns about the Association updating the ≈LBR weights unilaterally, the Association would welcome the oversight and control over the basket composition (both currencies included and their respective weights) by a group of regulators and central banks or an international organization (e.g., IMF) under the guidance of the Association's main supervisory authority, the Swiss Financial Market Supervisory Authority (FINMA).*"[6]

26. This statement underlines rather than mitigates the problem. First of all, it is questionable whether any central bank would regard as satisfactory the control afforded by membership of a group 'under the guidance' of the IMF or Swiss authorities. Nor is it clear the IMF or FINMA would welcome being in this position relative to their peer organizations. Secondly, the fact that the Libra Association regards itself as having the authority to put sovereign governments in the position of petitioner to a private entity suggests that this setup is not desirable. Ultimately central banks are democratically accountable whereas stablecoin providers are not, anything that weakens this link should be avoided.

[5] https://www.bankofengland.co.uk/banknotes/scottish-and-northern-ireland-banknotes
[6] https://libra.org/en-US/white-paper/#the-economic-and-the-libra-reserve

Supporting competition, efficiency and innovation in payments

27. One of the potential benefits of CBDC is the prospect of more competitive intermediation for payments and it would be desirable for a CBDC to be architected to facilitate this.

28. In existing card-based retail systems, for a user to make a payment to a merchant both need to be members of the same network. All of the payments are then routed through this network in exchange for a fee which is charged to the merchant. Ultimately these costs fall back on the users in the form of higher prices but the fee is largely invisible to the customer. Switching costs are high for both user and merchant so once a network is established there is relatively little competition. Over the years these problems have been recognized by antitrust and competition authorities in the US[7] and EU.[8]

29. A CBDC could be architected in a variety of different ways some of which could mitigate this problem and provide greater competition. The Bitcoin Lightning Network (LN) referred to above in the context of scaling could also have competition benefits. Nodes in the LN are able to charge fees for routing payments. The key difference between the fees in existing card systems and LN fees is that payments do not have to use any particular node so that if a node starts to overcharge for routing payments it can be easily routed around. This system structure makes switching costs extremely low and as a consequence increases competition.

30. Establishing a layer 2 network like LN in a CBDC would require a certain amount of programmability in the core ledger. Investigating the minimum functionality required to unlock the competition and scaling benefits of a CBDC layer 2 is a potentially desirable feature but this is a tradeoff worth testing as the extra functionality in this case adds both potential scaling and competition benefits if an active layer 2 network can be established for a CBDC.

Meeting future payments needs in a digital economy

31. There are two ways of approaching designing a CBDC to make it future proof. One way is to add a high degree of programmability to the core CBDC system. The benefit of this approach is that it allows developers to create a much broader range of CBDC applications. The risks of this approach are that a highly expressive language built into the base CBDC layer means that more can go wrong accidentally and there is a larger attack surface. This demonstrates one of the tradeoffs when designing a CBDC system, increased functionality comes at the expense of security and resilience.

32. The alternative is to start with a simple CBDC design with limited programmability. Even taking this approach, the same tradeoff arises between functionality and security. If we

[7] https://www.justice.gov/opa/pr/justice-department-sues-american-express-mastercard-and-visa-eliminate-rules-restricting
[8] https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39398

accept that some degree of programmability is desirable to allow the CBDC to interact with other parts of the financial system and enable innovation elsewhere the question is what is the minimum programmability needed to achieve this.

33. Earlier in this paper we discussed the potential benefits of a layer 2 system in relation to scalability. Building sufficient programmability into the core CBDC system to enable a layer 2 to be built on top would open up these benefits as well as others relating to privacy, discussed below. We have learnt from Bitcoin that relatively little of its original programmability is used day to day and even a significantly reduced instruction set opens up considerable potential for applications in the layers built on top of a CBDC.

34. Another consideration is to make the CBDC extensible. Cryptocurrencies have a process through which users can propose changes which are then considered and discarded and implemented. This allows them to evolve over time. Central banks could learn from this process and create pathways for CBDC users to submit desirable changes to the system. Using open source software for the CBDC system would also benefit this approach as it would allow third parties outside the central bank to experiment safely with the core software and come up with improvements. The central bank could then benefit from the input of a much wider range of software developers than those it engaged directly itself.

Improving the availability and usability of central bank money

35. There are four basic functions a CBDC needs to facilitate: payments, layer 2/payment channels, payment versus payment and delivery versus payment.

36. The Bank's discussion paper describes a retail CBDC which may obviate the need for delivery versus payment as a use case. Dvp is worth retaining as a use case because retail investors do buy shares and bonds and the functionality required to implement it is broadly the same as payment versus payment.

37. The other use cases are relatively straightforward, payments are the core function, layer 2/payment channels help with scalability and privacy, and payment versus payment is needed to make cross border payments function. This relatively limited set of uses fits with the platform model set out in chapter 4 of the discussion paper. Overall it fits with the idea of CBDC as a secure and resilient core with sufficient functionality to enable innovation at other levels in the system.

38. Section 5.4 addresses the economic design of CBDC, in particular whether CBDC should be remunerated or not. From a design perspective the simplest option is to have the CBDC unremunerated. All of the elements described in the paper around structure and tiering of remuneration could be implemented in a CBDC but doing so adds complexity to the system and would come with tradeoffs in terms of performance and security. The same goes for implementing limits. Different options could be implemented

and tested as a central bank develops a CBDC while recognizing the overall benefit of making the CBDC system simple and robust.

Addressing the consequences of a decline in cash

39. In addition to broad availability, one of the main benefits of cash is that it provides users with privacy. Its existence also demonstrates that a private payment mechanism issued by the central bank can coexist with AML and KYC laws.

40. In relation to CBDC there are different public policy considerations which need to be reconciled. CBDC users have a right to privacy and require a system which shields them from both state and corporate surveillance. The focus tends to be on the former but many privacy incursions now come from companies rather than the government.

41. From the perspective of the central bank, its role is to operate the core infrastructure and the discussion paper proposes a structure in which all interaction with the end users is handled by the private sector. This setup suggests that the core ledger should be fully private such that the central bank cannot infer anything about who the users are or what they are doing by virtue of operating the core ledger. Setting up a CBDC in this way protects the users from state surveillance and the central bank from the charge of surveilling citizens.

42. There is a performance tradeoff with implementing shielded transactions[9] and the central bank would have to decide how to implement them in its system. For example would it be optional for users to shield their transactions from the central bank or would it be required for all transactions? The performance implications would also have implications for the design of the rest of the system. If the shielded transactions reduced throughput on the main ledger then layer 2 could take more of the traffic in the system to reach the performance necessary for a retail system.

43. Channels themselves also offer potential privacy benefits. As the transactions are lifted away from the main ledger then only the parties privy to the payment would be able to know who they were going to and what they were for. It is important to note that recent work on privacy in payment channels has cast doubt on how reliable privacy in payment channels actually is.[10]

44. This setup would require additional consideration to how wallets and payment channels functioned to ensure that as users were onboarded to the system the necessary KYC and AML regulations could be applied. This requirement should also come with

[9] Shielded transactions allow for anonymous transactions on the core ledger, in contrast to Bitcoin which only offers pseudonymity.
[10] Privacy-Utility Tradeoffs in Routing Cryptocurrency over Payment Channel Networks, Tang et al, June 2020.

safeguards to ensure Payment Interface Providers themselves did not use these capabilities to erode user privacy. This suggests a role for a strong privacy regulator in any CBDC system to represent the privacy rights of CBDC users.

45. Section 4.7 of the discussion paper states:

> *"In most cases, the payer should be able to pay without revealing their identity to the payee. In this sense, they could have anonymity with regards to other users, without having anonymity with regards to law enforcement."*

46. The CBDC system should be set up such that by default users have privacy with regards to all other participants in the system, including law enforcement. Law enforcement authorities themselves are subject to laws and should not enjoy a blanket right to surveil CBDC users. Any request for private data from law enforcement should be subject to the proper legal process and private data should only be revealed in these limited circumstances. It is possible for these checks and balances in the system to be supported by the architecture of the CBDC system and these are some of the most important questions when designing a CBDC.

<u>Building block for better cross-border payments</u>

47. Several central banks around the world are now working on CBDCs. As these projects progress it would be useful for them to share information with each other on how they intend to handle payment versus payment with the goal of developing common standards on how the different systems should interact with each other.

48. This does not mean that every central bank has to architect its CBDC system in exactly the same way. One beneficial approach could be for different central banks to contribute to an open source CBDC codebase which each could then tailor to its own specific circumstances. This would allow all central banks to benefit from insights and research conducted by others while retaining control over exactly how they implement the software.

49. The overall goal should be to create an open source, common core CBDC platform which can be adapted to the specific needs of a particular country. Many governments use open source software in mission critical infrastructure and the adoption of this approach for CBDC has the potential to bring considerable benefits. Using open source software means that central banks will be able to draw on the expertise of a much broader range of software developers and avoid being locked in to vendors.

Robleh Ali
Research Scientist | MIT Digital Currency Initiative
June 12, 2020

Appendix: Selected Q&A

Q2 How could CBDC be designed in a way that improves the efficiency and speed of payments, while also facilitating competition and innovation?

A2 By implementing a CBDC architecture which enables the development of layer 2 services which both takes the load off the core CBDC ledger allowing it to scale and also has potential privacy benefits.

Q6 What factors would determine the level of adoption of CBDC as a means of payment in the UK?

A6 Two big drivers would be (a) how good the developer tools around CBDC are to make it easy to offer payments online and within mobile apps, and (b) the costs to merchants of providing CBDC payments – if CBDC were much cheaper than card transactions due to the competition benefits then retailers would be swift to adopt CBDC payments and this would drive end user adoption.

Q11 Could the potential benefits of CBDC be alternatively achieved by enabling new innovative private sector arrangements (eg stablecoins) to develop?

A11 CBDC functionality could be replicated with stable coins but the risks would be higher as discussed above.

Q12 What opportunities could CBDC provide to enhance monetary or financial stability?

A12 Creating a payment system with no credit or liquidity risk, providing an alternative to existing payment systems which would add resilience, and creating a much more direct transmission mechanism for monetary policy.

Q20 Are there viable business models that would incentivise firms to offer CBDC-related payment services in this approach?

A20 The lower barriers to entry for intermediating payments and collecting payment fees would incentivize more firms to enter the payments market.

Q21 What are the respective advantages or disadvantages of (a) the pooled accounts model described in Chapter 4.2, and (b) the alternative approach described in Box 3 in Chapter 4?

A21 The pooled account model would make it more difficult to port accounts when a Payment Interface Provider failed as there would be a secondary ledger that would have to be retrieved and sorted through. The alternative approach is essentially a reserve account backed stablecoins which are also discussed above.

Q22 What kind of overlay services would be most useful? What functionality would a CBDC core ledger need to provide to enable these?

A22 Payment channels/layer 2 network, payment versus payment and delivery versus payment would be most useful. The core CBDC ledger would have to provide some kind of timelock or equivalent functionality to make these functions work.

Q25 - What is the appropriate privacy model for CBDC? Is it necessary, or feasible, to replicate any of the privacy aspects of cash?

A25 Private at the core ledger so central bank has no access to end users' information. PIPs do KYC/AML but with strong privacy regulations to prevent abuses.

Q28 What are the main trade-offs that arise in deciding on a technology approach? What should we be prioritizing in these trade-offs?

A28 The tradeoffs are privacy vs performance, complexity vs security and decentralization vs performance. Central banks should prioritize simplicity and security and opt for the minimum functionality necessary to do useful things rather than building in too much complexity at the start.

Q29 The core ledger for this model of CBDC could be centralized, or operated through a consensus-driven distributed approach. Which is the optimum approach, and why?

A29 Any CBDC system is likely to be decentralized to a certain degree. The main question is how the tradeoff between decentralization and performance is managed. Implementing a layer 2 network which can take the strain off the core ledger is one option for getting the resilience benefits of decentralization without sacrificing performance.

Q30 What are the merits, or challenges, of either 'token-based' or 'account-based' approaches to a CBDC ledger? Are there particular use cases that are better supported by either approach? Are there alternative approaches?

A30 It is not clear at the moment, central banks should be experimenting with both and seeing which model performed better. There is evidence that UTXO based systems can take advantage of scaling innovations such as utreexo[11] better than account based systems.

Q31 What are the key use-cases for programmable money?

A31 Payment channels/layer2, payment versus payment, delivery versus payment.

Q32 What architecture choices would best support programmable money functionality in a CBDC? Would it be preferable to build this functionality into the core ledger, via a separate module, or to enable the functionality to be provided by third parties? Are there alternative approaches?

A32 Minimum functionality in the core ledger to enable layer 2 etc. other functionality can be added later or built outside the core CBDC layer.

Q35 What other future technology and digital economy innovations should we be factoring into the potential design of CBDC? How might these impact the future demands placed on CBDC, and potential approaches to designing a CBDC?

A35 The rest of the financial system is likely to undergo technology driven change as CBDC is designed and implemented. It would be useful for central banks to consider how CBDC could interact with other types of tokenized assets as they conduct their CBDC work. Having a view of how other parts of the future financial system such as securities, commodities, derivatives, lending etc. will look in the future would be a very helpful approach.

[11] https://dci.mit.edu/utreexo