Response to: https://www.bankofengland.co.uk/the-digital-pound/digital-pound-working-groups

Questions re Privacy and the Digital Pound (March 2024)

The Bank of England is currently running a series of smaller working groups relating to particular aspects of their CBDC proposals. They requested general feedback in relation to certain privacy queries, set out below. Bitcoin Policy UK has submitted a summary of this longer analysis to the Bank of England.

TLDR: while we remain opposed to the creation of a CBDC in its entirety, our view is that the 'least worst' option would be a form of anonymous Chaumian e-cash, which no third party can monitor, control or censor - namely, a digital bearer equivalent to physical cash. To quote Silkie Carlo, Director of Big Brother Watch, "Anonymous, private, low threshold e-cash could have a future - but Western Countries like Britain won't accept anything that looks like a 'spycoin'."

The Bank of England asks: "How could we ensure privacy for individual users of a digital pound while maximising its potential benefits and use cases?"

- Is there a range of levels and types of privacy that could be offered in a digital pound ecosystem that remains within the principles set out in the **Consultation Paper**?
- If so, what are the advantages and disadvantages of different options to the full range of actors in a digital pound ecosystem?
- How and where do existing legal and regulatory safeguards pose a challenge to different levels of privacy?
- How much and what kind of information should users have about how their data is used in a digital pound ecosystem, and what impact will this have on merchants and other participants processing payments?
- What are the main considerations for the introduction of tiered wallets, enabling consumers to choose different levels of privacy depending on access to services?

Bitcoin Policy UK response:

We remain opposed in principle to the creation of a digital pound or CBDC, and our policy position is unchanged - that it is a solution in search of a problem; one that will serve no useful purpose not already solved by existing forms of digital money. Nevertheless, we would argue that the 'least worst' implementation of a CBDC would be a form of Chaumian e-cash, that no centralised third party can monitor or censor in any way.

Different levels of privacy afforded by physical cash, CBDCs and other digital monies

The most private form of money that is in current circulation is of course physical cash. Any decline in the use of physical cash not only results in a decrease of user access to central bank money (rather than money which is the liability of a commercial bank) but also exposes the users of other forms of money to a loss of privacy, which in some cases is quite substantial. We note that the Bank of England (the "**Bank**") in its 2020 Discussion Paper did make reference to this decline in the use of cash: "***Physical cash has certain unique characteristics that would be lost if it were to fall out of general use. For example, cash offers a level of privacy in transactions that is not always available with existing electronic payment systems. Cash also has an important role in financial inclusion***." (BoE 2020 Discussion Paper, p.18).

It is important to note here that the proposed digital pound cannot be equivalent to cash for a number of reasons, not least of which because it it not proposed to be a digital bearer instrument and also because the extent of the private nature of transactions is likely to be extremely limited, with data on such transactions being shared not only with PIPS but also with the Bank itself (whether or not personal information relating to the end user is shared by the Bank). As such, it will have far worse protections for user privacy even than a public but pseudonymous system like Bitcoin - since it uses a public ledger, and pseudonymous addresses that can relatively simply be linked to named individuals, Bitcoin's privacy protections are actually surprisingly limited when transacting peer to peer on the base chain.

CBDC proposals are broadly similar to existing bank accounts - so what is the point?

Rather than detailing a new form of digital bearer cash, then, the proposals currently published by the Bank appear far more akin to a broad replication of modern bank accounts, where a certain minimum amount of KYC is required in order to open an account, and, in the case of the digital pound or CBDC, tiered access is granted upon provision of more and more personal data. **In short, the proposals come close to treating personal and transaction data as a form of currency themselves - the digital pound would become more useful the more personal data is surrendered by its users, who would pay for increased usability with the currency of their personal data.** It is therefore an exclusionary model of money resulting in perverse incentives, where those with legitimate privacy concerns - from students to lecturers, working parents, unemployed persons, doctors to barristers to MPs to Bank staff themselves - may be denied access to their national currency unless they surrender their data for harvesting.

We wish to go on record in stating that **this is a highly unusual and non-standard way to approach the issue, creation, and delineation of the properties of, any form of money. The concept that a money would have different levels of usability, or that its users would have different benefits from it depending on the amount of personal data with which they were comfortable to part, completely undermines the concept of fungibility** in relation to

that money and our organisation finds the proposal to do so extremely surprising, particularly coming from an institution that is ostensibly a central bank.

A tiered system of access would result in unintended consequences for the Bank where private money might have a greater real value on the free market than the 'less private' money in the form of the CBDC. The complexity that the Bank is considering is both shocking and akin to a technologically updated form of mediaeval alchemy, quite apart from the question whether the exceptional cost required to implement and maintain a domestic retail ledger is appropriate, possible or moral.

Pass through model analogous to existing bank accounts

However, the 'pass through' model proposed by the Bank will effectively treat the PIPs as user facing 'bank account providers' for the purposes of using the digital pound, with the Bank maintaining the private ledger. We assume that in this model and as indicated by the Consultation that the Bank would have access to transaction data, and the PIPs to both personal and transaction data, with some degree of sharing between PIPs and the Bank, the extent of which is still to be determined. It is not difficult to say that as described this model is no more private than existing customer bank accounts, and far less private than either physical cash or other existing forms of digital money such as Bitcoin. We note for the sake of accuracy that other forms of digital cash exist that are arguably even better at preserving user privacy than Bitcoin.

Regulation of a Great British stablecoin private market would be a far simpler, elegant and moral approach to digital currency in this country. Ensuring the stable coin market is backed 1:1 by short term GILTs would create a welcome buyer of government debt (not as deep a market as was once believed, as evidenced by the October 2022 sell off, continual fiscal deficits, and higher interest payments). Nullifying the stablecoin market with CBDCs would remove the fastest growing private sector government debt buyer, resulting in the Bank having to buy more itself. Therefore this is a conflict of interest for the Bank, being inherently political and potentially with questionable commercial ethics implications.

There is no sense in which we would currently advocate for an elimination of KYC and AML laws in relation to modern bank accounts offered by commercial banks. Our contention is instead that such bank accounts obviously do already exist in the UK alongside a system that has close-to-perfect privacy, namely the physical cash system that gives individuals access to central bank money. **There is therefore little to no sense in expending time, personnel, money and other resources in replicating a system that will be broadly identical to the modern system of commercial bank accounts, while having none of the advantages of the physical cash system,** which provides access to bearer money that affords its users a very high degree of privacy.

CBDCs are, if implemented at all, likely to have none of the advantages of physical cash, and no readily comprehensible advantages for the end user over existing bank accounts. Governments and central banks would be well advised to consider if it is worthwhile creating a system with zero apparent advantages that, as the data from other jurisdictions shows, will likely be soundly and rightly rejected by the people who are intended to use it.

Better privacy may be afforded by the implementation of Chaumian e-cash

Noting our unwavering opposition to the digital pound *ab initio*, we nevertheless believe that from a privacy perspective, the 'least worst' option would likely be a form of Chaumian e-cash. An e-cash of this nature most closely re-creates a digital equivalent of physical cash. It is private, can be used anonymously, and can be held directly by the user as a bearer instrument. It cannot be counterfeited, yet the issuing mint may be blind to the identity of the holder. Certain e-cash systems may even permit offline transactions. We refer by way of example to the Fedimint Protocol or to the Cashu Protocol, each of which may provide better privacy protections for users than the digital pound as currently proposed. We also refer to this response to the Bank's original consultation, which examines the characteristics and implementation of Chaumian e-cash systems in a level of detail beyond the scope of this short response.

We would highlight in summary several advantages of Chaumian e-cash over the permissioned token currently proposed by the Bank for the UK's CBDC:

1. **Double spending risk**: Online transactions with e-cash avoid double-spending because a trusted bank (namely the mint) verifies each payment. While the system can be enhanced to catch and penalise double-spenders even in offline situations, this feature is not always necessary. For most online purchases, just like most stores do not accept offline credit card payments, simply requiring the recipient to be online is ordinarily enough security.
2. **Privacy enhancement**: We note that the Bank (strangely) is opposed to a bearer instrument model for the CBDC (Consultation Paper, Box G). This is despite the fact that the Bank is responsible for the most widely used cash bearer instrument in circulation, namely physical cash. **It is concerning that the Bank does not want to afford users of its CBDC the same level of privacy that is enjoyed by users of its very own physical central bank money.** Nevertheless, the Bank has alleged that a bearer instrument approach, "where users never have to check back in with a central ledger, would lead to completely anonymous payments". It is a common misconception that anonymous transactions require avoiding ledgers altogether. However, both Bitcoin and even Monero (noted for its privacy features) and even most types of e-cash will all utilise ledgers to settle transactions while still enabling some level of anonymity. Anonymity

derives from how the ledger is designed, not from avoiding its use entirely. True anonymity might exist in a system with no ledger, but it is unlikely that such a system would be practical.

3. **Enabling remote transactions**: The Bank in its original consultation again appeared to perceive some difficulty in "conducting transactions between two individuals over distance as both hardware devices would need to be updated accurately." This is cited as another excuse for why a bearer instrument model is not supported by the Bank in designing its CBDC. However, e-cash once again offers a potential solution to this problem, since its transaction mechanics do not depend on user proximity, instead requiring, for example, that the receiver of e-cash is able to contact the mint to redeem the tokens received for newly issued tokens.

User control over their personal data

Users should ideally have as much control over the use and treatment of their personal data (including requests to be forgotten and access to data subject access requests) as is permitted both by the requirements of the Data Protection Act 2018 and existing and applicable AML legislation. We note that the Bank and the PIPs should ensure that, if a CBDC is implemented, they be ready to comply with data subject access requests from potentially every person who holds a CBDC account and whose personal data is or may be held by either the PIP or the Bank. We make the assumption that neither the Bank nor the entities likely to be appointed as PIPs currently have the resources to handle such a very large volume of requests, and note that considerable monetary and personnel resources will be required in order to implement these properly.

We should consider what the consequences of data breaches of the CBDC honeypot of user information might be for both PIPs and the Bank itself. If the Bank is intending effectively to enter the Retail Domestic Banking industry then we would highlight that the Prudential Regulation Authority should really have a role in regulating the Bank. Admittedly, the Bank has power to issue "Public Central Bank Money", but the CBDC proposals are suggesting the Bank effectively is to commence a new role in Transactional Domestic Retail Banking IT Infrastructure, which we would argue is outside the scope of "Public Money" - and, importantly, is totally *ultra vires* as regards the Bank's existing constitutional powers.

Discriminatory nature of tiered wallets

To the extent that the proposed digital pound is intended to emulate cash or bank notes, which are liabilities of the central bank, it is a contradiction in terms to postulate that a digital cash equivalent should require any form of identification or identity information at all in order to use it.

In fact, we would go further and point out that **if the provision of identity information is a gating item to this tiered access, it is a direct and egregious contradiction in terms of the Bank's stated aim of increasing access to finance and banking the unbanked**. The very same people who are excluded from the traditional financial system will also be excluded by these proposals for the digital pound. The freedom to transact, which a digital pound will arguable reduce or restrict, is central to theories of political economy developed by intellectual founders like Hume, Adam Smith, Frédéric Bastiat, Jean-Baptiste Say, John Stuart Mill, Ludwig von Mises, Friedrich Hayek, and others from across the European continent.

If KYC of any kind is required to use a UK CBDC, then it cannot by definition be as private, as usable, or as inclusive as physical cash. I quote from the Bank's own CBDC consultation paper, which sets out that: "***For the digital pound, tiered access would allow for different levels of user access and functionality based on the amount of identification (ID) a user is willing or able to provide. The stronger ID information a user provides, the more types and higher values of payments they would be able to undertake. For example, users might be able to open a basic digital pound wallet with limited ID***".

In other words, users will have to swap increasing amounts of personal data in exchange for increasing usability of the digital pound.

The very existence of tiered access, in fact, ensures that inequality between its users is intended to be built into the design of the digital pound from day one. This is far from the inclusive, user-agnostic way in which any form of cash should operate.

Such a CBDC cannot therefore be considered 'digital cash', or equivalent to cash, since the KYC provision requirement placed on prospective users before they can even access the digital pound will be a gating item, and those people who are currently unable to obtain a bank account are therefore also unlikely to be able to use it.

We believe very strongly that the Bank should continue ensuring access to central bank money in the form of physical cash, which is totally agnostic to the identity of its users and treats them all equally. The Bank has performed this function well throughout its long history and should continue to do so. We support any efforts to ensure access to bank branches and locations where people are able to obtain access to physical cash. While some claim that cash usage is declining, the latest data actually shows it has begun to rise again.

The consultations have stated that a digital pound would be created with 'privacy in mind'. We note the proposed 'Compliance Services' to which the consultations refer, which would gather both personal and transaction data from users. As a final point, we would flag the 'honey pot' risks that such a data-gathering service would pose, or to point out that money-laundering and sanctions-evasion appears to be carried out, today, with relative impunity through

highly-regulated banks and with apparent disregard for the AML and KYC requirements that these banks already have in place, and which would be likely to continue whether or not these restrictions are imposed on the users of a UK CBDC.

Conclusion

For the Bank's CBDC truly to replace physical cash, or to offer a genuine digital alternative to it, it needs to mirror the key features of physical cash. These include being a bearer instrument, offering strong anonymity for transactions and ownership, (the former two characteristics being of particular relevance to this privacy consultation) and must also allow direct claims against the central bank by the public.

Without these characteristics, the CBDC is unlikely to be attractive enough to compete with existing digital payment options, leading to public mistrust, low adoption, high running costs, and eventually the failure of the entire enterprise - which is not an outcome with which we as an organisation would be disappointed.

Furthermore, the Bank must consider the IT infrastructure cost associated with implementing and maintaining a tiered Transactional Retail Banking ledger. These significant costs will include the resource headcount costs for doing so, the operational hardware cost to maintain within the UK jurisdiction, the reputational cost for failure to implement or maintain successfully, and finally the regulatory costs for ensuring the PRA and Bank roles and responsibilities are appropriately segregated.