



We appreciate the opportunity to contribute to this important consultation.

In our response, we refer to the paper “The digital pound: a new form of money for households and businesses?” dated February 2023, as presented to Parliament by the Economic Secretary to the Treasury (the “paper”).

We also refer to the paper “The digital pound: Technology Working Paper” (the “technology paper”).

Below, the term ‘The Bank’ or ‘BoE’ refers to the Bank of England, and the term ‘HMT’ refers to His Majesty’s Treasury.

PREAMBLE

The House of Lords economic affairs committee report on CBDCs is entitled: “Central Bank Digital Currencies – **a solution in search of a problem?**”¹. We agree with the House of Lords committee that there does not appear to be any good use case for a digital pound that is not currently served by existing forms of digital money. In terms of the production and use of physical cash, we agree with Lord Desai who observed in the debate on the subject that **“the most significant problem it will create is that it will deprive ordinary people of easy access to cash.”**

In our view, the Bank should continue to produce and provide access to physical cash - it has performed this function well during its long history and this is one of its key reasons for being. The production and administration of an untested digital currency, with far-reaching negative consequences, is not.

A paper prepared for the European Parliament notes that the **risks of rolling out a digital euro currently outweigh the benefits**, and a CBDC should not be introduced unless “new elements” emerge².

We also agree that the risks of rolling out this new technology are hard to quantify and such a step should not be taken lightly, if at all - and at the very least, not without Parliamentary debate and primary legislation. The extension of the powers of the Bank as suggested by the paper are unarguably *ultra vires* in the context of the Bank’s existing powers as granted by charter and statute.

Furthermore, we note that countries that have adopted CBDCs, at considerable cost and expense, have discovered their citizens simply do not want to use them³.

The House of Lords committee concluded that the introduction of a CBDC could have “far-reaching consequences” for households, businesses and the monetary system. The report said it could pose “significant risks”, which included state surveillance of people’s

¹ <https://committees.parliament.uk/publications/8443/documents/85604/default/>

² [https://www.finextra.com/finextra-downloads/newsdocs/ipol_ida\(2023\)741507_en.pdf](https://www.finextra.com/finextra-downloads/newsdocs/ipol_ida(2023)741507_en.pdf)

³ <https://www.coindesk.com/policy/2023/02/24/why-nigerians-arent-turning-to-the-enaira-despite-crippling-cash-shortages/>



spending choices, financial instability as people convert bank deposits to the CBDC during periods of economic stress, and an increase in central bank power without sufficient scrutiny. Additionally, it would involve the creation of a centralised point of failure that would be a target for hostile nation states or criminal actors. Lord King of Lothbury (himself a former Governor of the Bank) stated that **“in evidence to our committee, the Bank of England made it clear that it saw no need for a wholesale CBDC”**. He noted that the main conclusion of the House of Lords report was that **there were no problems to which a CBDC is the only, or even the most obvious, answer**.

The committee’s overall conclusion was that it was “yet to hear a convincing case” for why the UK needs a retail CBDC. The report stated that while a CBDC “may provide some advantages”, it could present “significant challenges” for financial stability and the protection of privacy. Lord Bridges stated in Parliament during the debate that the Governor of the Bank had himself told the inquiry **“we have to be very clear about what problem we are trying to solve before we get carried away with the technology and the idea. I am not convinced about some of the problems that we might be trying to solve.”** It is hard to square this prudent approach with the speed and enthusiasm with which the paper seems to anticipate that a CBDC will be created.

We refer also to the changing attitudes of the Bank of International Settlements over time. As recently as March 2019, Augustin Carstens (General Manager of the BIS) stated that central banks did not see the value of implementing CBDCs, and when considering the lack of demand plus the “operational consequences” of bringing them about, there was little urgency to the matter. **“There is no clear demand for CBDCs on the part of society. There are huge operational consequences for central banks in implementing monetary policy and implications for the stability of the financial system.”**⁴

However, something changed for Augustin Carsens in the intervening period. His more recent, and most famous quote on CBDCs is as follows: **“The key difference with the CBDC is the central bank will have absolute control on the rules and regulations that will determine the use of that expression of central bank liability, and also we will have the technology to enforce that.”**⁵ What has changed in the intervening period? What technological development can have led Carstens to fear central bank disintermediation, and to develop a taste for such totalitarian control over the spending decisions of law-abiding citizens?

We return to the *ultra vires* consideration as noted above. This is a debate of fundamental importance in our society - no one, anywhere in the world, and least of all in an ostensibly free society, has granted central banks a mandate to have “absolute control” over money and dictate the individual transactions of a nation’s citizens. It is not within their charter, and nor should it be. It should not even be within the remit of the government - criminal action should be punished only after the government has proven a person’s guilt beyond

⁴ <https://www.engage.hoganlovells.com/knowledgeservices/news/bis-central-banks-need-to-tread-cautiously-with-cbdc>

⁵ <https://www.youtube.com/watch?v=9FM4Fu2uiDE>



reasonable doubt in a court of law. Until this has been proven, then the law demands that the presumption of innocence prevails - and this presumption of innocence should apply equally to individuals and to the transactions into which they enter.

And yet, despite all of the above, HM Treasury and the Bank of England now appear determined to force the United Kingdom to adopt a CBDC. Why could this be?

We believe the reason is simple – an unjustified fear of Bitcoin.

Buried in the back of the paper is a revealing statement from the Bank: **“Widespread adoption of a non-sterling digital form of money in the UK is unlikely but its impact would be very significant and be beyond the tolerance of UK authorities... By reinforcing the use of sterling for UK payments and enabling new payments functionality, the digital pound could pre-emptively reduce the chance of widespread adoption of non-sterling digital money in the UK.”**

In the absence of any other remotely plausible use case for the digital pound, which is not already perfectly well served by existing forms of digital money, we believe that the statement above reveals the true reason for the drive to adopt a CBDC in the UK. We strongly advise the Bank and HMT to understand that if this is the case, then it is likely to fail, at great cost to the public purse, as Nigeria’s CBDC has failed⁶. We exhort both the Bank and HMT to look again at the permissionless, free and open source payment system that is already functioning, with 99.9% uptime over 14 years of operation, in the face of relentless attacks from governments and hackers alike (to all of which it has remained impervious), available to all, and upon which anyone is free to build, both for domestic and for international applications.

Our primary mission is to help the UK government understand that Bitcoin is a benefit, not a threat; and that adopting Bitcoin (whether as a Treasury reserve asset, or as a means of making faster, cheaper digital payments via the Lightning Network, or as an industry that can stabilise renewable grids via demand response and reduce methane emissions) can have manifest and far reaching benefits for economies that embrace it, rather than fruitlessly fighting it. This is particularly true if those economies are early adopters, rather than being late to the party.

The United Kingdom recently made much of ‘taking back control’. However we view the merits or otherwise of Brexit, it is undeniable that the desire not to be controlled sat behind much of the successful ‘Leave’ campaign. In the context of a CBDC, any appeal to the general population, once the loss of control over both their financial privacy and their ability to transact is widely understood, will be likely to strike a similar chord.

Augustin Carstens may eventually gain total control over the rules and regulations that determine the use of his CBDC. But he will never have even the smallest imaginable degree of control over Bitcoin. No person, no party, and no government can. Bitcoin is ‘rules without rulers’, and a level monetary playing field for all its users.

⁶ <https://cryptopotato.com/bitcoin-premium-tops-60-in-nigeria-amid-growing-demand/>



Any CBDC will also be subject to the same elastic monetary policy as are all liability monies, and exposed to the same risks of dilution and debasement over time. Bitcoin is not. Its monetary policy is set in code, is totally predictable, and cannot be changed. It is prudent to remember that in the fight between soft and hard money, hard money always wins in the end (even if we understand and sympathise with central banks being unwilling to give up seigniorage, and all the advantages that come with it).

Acknowledging this truth, we have a proposal. Instead of wasting time and money on fruitlessly forcing an unwanted CBDC onto a population that would likely reject it, instead study Bitcoin. Understand its protocol, its immutability, its censorship resistance, its inclusivity. Anyone in the world can participate in the Bitcoin network, and everyone is equal before the protocol. Countries that view Bitcoin as a friend, and not as an enemy, have an enormous opportunity to profit not only from the asset itself but also from the infrastructure, the tax revenue, the businesses, the tourism and the payment efficiencies that it brings with it. In considering these new protocols, it may be helpful for governments and banks to view the Bitcoin blockchain as the settlement layer (analogous to final settlement and clearing between banks via the central bank) and Lightning as an instantaneous payment layer (although transaction finality is instant, settlement only occurs when the Lightning channel is closed and the resulting transaction written to the base layer).

Other nation states are beginning to explore the Bitcoin ecosystem at a state level, whether El Salvador adopting Bitcoin as legal tender (with projected 2.4 percent GDP growth in 2023)⁷, or the United Arab Emirates mining Bitcoin in Abu Dhabi⁸, or Bhutan doing the same with its excess renewable resources⁹.

The United Kingdom, with its abundant wind energy, could do exactly the same. The country has an opportunity to be early to this party, and to retain the mined bitcoin as a Treasury reserve asset alongside our gold reserves - an asset that cannot be frozen or confiscated, that is at once absolutely ours and globally transmissible as easily as sending an email. Companies around the world are building on the network and exploring this functionality - whether Strike and its Send Globally API¹⁰, or CoinCorner with its Bolt Card¹¹, allowing merchants to avoid high interchange and other card scheme fees, in order to make direct peer to peer payments, using digital cash, that settle within seconds.

On the other side of the equation, we have the proposed digital pound. The questions we must ask ourselves, and which every citizen of the United Kingdom should ask, are as follows:

7

<https://www.imf.org/en/News/Articles/2023/02/10/el-salvador-staff-concluding-statement-of-the-2023-article-iv-mission#:~:text=Real%20GDP%20is%20projected%20to,of%20weaker%20global%20commodity%20prices>.

⁸ <https://cointelegraph.com/news/marathon-digital-announces-immersion-crypto-mining-operations-in-abu-dhabi>

⁹ <https://www.forbes.com/sites/iaimartin/2023/04/30/bhutan-bitcoin-mining-crypto/>

¹⁰ <https://fortune.com/crypto/2023/01/31/strike-expands-cross-border-payments-feature-philippines-remittances/>

¹¹ <https://www.coincorner.com/TheBoltCard>



“Do you want the central bank and the government to have absolute control over your money, over how much you are allowed to have, over what you spend it on, over when you spend it and how? Do you want the central bank and the government to be able to turn off your money at a keystroke, or include an expiry date on your money, or impose a negative interest rate on you, or prevent you from buying food, or transport, or shelter, if you say or do something with which they disagree? Do you believe that the central bank and the government should be able to spy on and control every single financial transaction that you undertake, no matter how lawful or innocent?”

If you responded ‘no’ to any of the questions above, then you must also join us in resisting the introduction of a CBDC, and in resisting its use if introduced. There is a real danger that with the current proposals under consideration, we will lose control over that most basic freedom, the freedom to transact, and never regain it.

We include below a copy of our formal responses to the Bank of England and HM Treasury, submitted in relation to the consultation on the digital pound.

Freddie New
Head of Policy
[Bitcoin Policy UK](https://www.bitcoinpolicyuk.com/)
71-75, Shelton Street, WC2H 9JQ



Questions in response to the BoE consultation: (see part B of the paper)

8. Do you have comments on how trends in payments may evolve and the opportunities and risks that they may entail?

Our view is that the current global focus on CBDCs - a largely untested, and, where trialled, unwelcome technology (1) has diverted attention from more promising technologies that already exist and are functioning in the market. We will cite examples in (i) international remittances, (ii) domestic payments and (iii) online micropayments. Each example below is currently functional, and operating today on a free & open source software (FOSS) permissionless network enabling the global transmission of value at a considerably lower price point than current rival technologies. Our illustrations suggest that the Bank and HMT, instead of being wary of existing FOSS systems, should consider whether these can be adopted and integrated into future sterling payment systems and processes. We note that FOSS systems are already extensively used by HM Government, for example in the use of Linux in NHS systems.

- (1) <https://www.coindesk.com/consensus-magazine/2023/03/06/nigerians-rejection-of-their-cbdc-is-a-cautionary-tale-for-other-countries/>

(i) International remittances:

Remittance Channel, following a cross-market survey, estimated the value of global remittances at USD 131.69 billion in 2022, USD 148.08 billion in 2023, and this is projected to grow at a CAGR of 12.58% to reach USD 339.87 billion by 2030. The World Bank has calculated that 6.3% on average is taken up with fees, and the IMF notes that fees can be much higher, in the order of 15-20%. Typically, the smaller a remittance and the less well off the sender, the higher will be the fees. Developing a system that is fairer and cheaper would be genuinely life-changing for those sending small amounts of money cross-border, for example to families back home. Remittances now form a crucial part of the economies of many countries - for example, remittances now account for over 50% of Lebanon's GDP.

Each of Strike (2) and CoinCorner (3) currently use a functioning product ("Send Globally") that enables individuals to send money cross-border using the Lightning network, at very low cost, virtually instantaneously and with final settlement in seconds. Each of these technologies uses the Lightning network and involves the use of this second layer Bitcoin protocol as a payment rail. Customers can choose to convert their fiat currency in real time to Bitcoin, transfer cross-border and convert into local currency, virtually instantaneously, and at a price point that is significantly cheaper than any other competing product on the market. Volatility risk is eliminated in two ways - firstly by the speed of transfer and settlement (which is virtually instant) and secondly by the parties agreeing to fix the price for the period of time that the transaction takes to settle. Send Globally with Strike is available in 11 nations that in 2022 received over \$109B in remittances, and the company has just announced that the service is expanding to 65 countries giving access to more than 3 billion people.

CoinCorner's deployment with Pouch in the Philippines, by way of example, does not require the recipient to use or hold a Bitcoin Lightning wallet at all - owing to the instantaneous transfer and settlement, funds sent over the Lightning network are immediately converted and deposited into the recipient's bank account in local currency. This is not currently possible with any other comparable technology and merits further study and support.

Jack Mallers, CEO of Strike, has recently presented to the IMF on his company's pioneering work in this space: <https://www.youtube.com/watch?v=jb-45m9f76l> .

- (2) (<https://www.businesswire.com/news/home/20230425005741/en/Strike-Expands-%E2%80%9CSEND-Globally%E2%80%9D-to-Guatemala-Bringing-Lightning-Fast-Money-Transfers-from-the-U.S.-to-Latin-America>)
- (3) <https://www.coincorner.com/SendGlobally#:~:text=Send%20Globally%20allows%20CoinCorner%20users.via%20the%20Bitcoin%20Lightning%20Network.&text=Your%20CoinCorner%20GBP%2FEUR%20balance.sent%20via%20the%20Lightning%20Net%20work>

(ii) Domestic payments: The Bank and HMT will be aware of the high fees charged by Visa, Mastercard and other card scheme rules. Again, solutions already exist in the market that allow for the virtual elimination of such fees, resulting in significant savings for merchants, and potentially also from consumers who buy from those merchants. Commercial solutions exist today (4), largely ignored by the Bank, that allow customers to pay in store at a point of sale using a traditional bank-style card, sending value over the Lightning Network, in some cases with an instantaneous currency conversion at each end (avoiding slippage and conversion risk) so that the merchant receives fiat currency, while at the same time without paying the high processing fees currently charged by payment rails such as Visa and Mastercard. In addition to its use case as a commodity savings technology, it is the payment innovation presented by Lightning that is in our view worthy of further investment and development in the UK. Companies such as CoinCorner are already pioneering use of this technology in the UK retail space, and have even enabled Oxford City football club to accept Bitcoin payments (5). CoinCorner has also recently partnered with the Seed Group in the UAE to build out Bitcoin payment capabilities in the UAE (6).

- (4) <https://www.coincorner.com/TheBoltCard>
- (5) <https://www.oxfordcityfc.co.uk/oxford-city-fc-enters-partnership-with-coincorner-to-deliver-bitcoin-matchday-payments>
- (6) <https://blog.coincorner.com/coincorner-partners-with-seed-group-to-facilitate-bitcoin-transactions-in-the-uae-9c2933474cf>

(iii) Micropayments: The Lightning network sits behind the 'zap' function on Nostr (7). Nostr is a totally decentralised alternative to Twitter, and many software clients that access the Nostr protocol have already included micro-tip functionality, similar to a 'like' button, where users can instantaneously and totally anonymously send value to each other simply by integrating their Lightning wallets and tapping a Lightning icon on a post. The potential

implications of this technology are far-reaching, whether as a means of paying for a single newspaper article (rather than purchasing a full subscription) or by purchasing any manner of goods and services online in the simplest possible way. It is unlikely that any UK CBDC would ever be able either to catch up with, or rival, the payment functionality that already exists on Nostr as of today, let alone in several years at the point when a CBDC may be eventually launched.

In the payments industry, Bitcoin and the Lightning network may in one sense be thought of in the same way as the SMTP protocol that moves mail across the internet, or TCP/IP upon which the Internet itself runs. Bitcoin and Lightning are open, permissionless protocols that any developer and any government in the world can use freely, and an enormous amount of innovation is taking place in this space (we add one further interesting instance in the form of Lightspark, where David Marcus (previously of Facebook) is now CEO (8)).

(7) <https://nostr.how/en/zaps>

(8) <https://www.theverge.com/23696466/bitcoin-crypto-lightning-network-lightspark-ceo-david-marcus>

9. Given our primary motivations, does our proposed design for the digital pound meet its objectives?

There appears to be absolutely no good use case for a digital pound that is not already served or superseded by the capabilities of the various forms of digital money that already exist.

Furthermore, it appears to come with a number of potentially dangerous and destabilising disadvantages, not least of which would be additional tools for central banks to manipulate monetary policy. Any such expansion of a central bank's powers should only be undertaken with great caution and, as we argue elsewhere, only following primary legislation. A CBDC would give the Bank access to "fully programmable base money, enabling them to determine interest rates, deposit limits, spending limits, and permitted transaction counterparties for every individual and every token for any period of time." (Dr. Natalie Smolenski, Texas Bitcoin Foundation & Bitcoin Policy Institute, Jan 2023). With these powers, and with ever increasing pressures from inflation and the burden of servicing an expanding national debt, it is almost certain that any increased arsenal of monetary policy powers would be used if available.

The paper states that "Our primary motivations for the digital pound are the availability of central bank money as an anchor for confidence and safety in money, and promoting innovation, choice, and efficiency in payments." The Bank can achieve its primary goal here very simply, by continuing to produce physical cash and ensuring that it remains available. BPUK fully supports, as a policy matter, the continued availability and accessibility of physical cash issued by the Bank. As to payments efficiency, it is not clear to us how the UK's existing RTGS, CHAPS, and Faster Payments Systems do not already achieve this



aim. Faster Payments has been operationally functional for more than a decade and many fintech companies and banks have used this system to advance payments domestically in the UK. It is implausible that a digital pound would add very much to payments efficiency, particularly given the enormous effort and cost required to build and run a system whose purported payment capabilities already appear to be replicated and functioning in existing systems.

Furthermore, there is no feasible way that a UK digital pound, centralised at the BoE and with PIPs as gatekeepers, could compete with the payment efficiencies offered by the Bitcoin and Lightning networks. It is already possible to send a billion dollars of Bitcoin across the world for a fee as low as USD 0.50 (9), and on the other side of the scale, it is possible, today, via the integration of the Lightning network with the Nostr protocol, to send a fraction of a penny to an unknown person via Nostr, simply by clicking a lightning icon on their profile (10). A digital pound as proposed by the Bank cannot, and will never, compete with a network of such power and versatility.

Payments sent using the Lightning network settle instantaneously and virtually for free, and the network currently has a theoretical limit of 1 million transactions per second - and potentially more (11). Innovation in terms of these payment mechanisms is happening now, but is at risk of being driven off shore and into more friendly locations such as Abu Dhabi (12), while the Bank and HMT are wasting time, money and resources on an effort to create a digital pound that is likely to be rejected by those citizens who are intended to use it. Already, other second layer protocols (such as Liquid) exist, upon which stablecoins may be issued as bearer assets and backed by government bonds. We suggest that a better use of time and resources in this context would be to develop clear regulatory guidelines on the use and format of stablecoins, allowing the Bank to concentrate on its primary mission of economic stability and maintaining access to cash rather than wasting time researching, implementing and running a financial technology network.

Our assumption is that the real intention and the primary objective behind the digital pound is to stifle and prevent the growth of Bitcoin as a means of payment and a store of value, and secondly to ensure that the Bank and HMT are able to monitor and control the way in which citizens lawfully choose to spend their money. We quote Augustin Carstens of the Bank of International Settlements: *"The central bank will have absolute control on the rules and regulations that will determine the use of that expression of central bank liability, and also we will have the technology to enforce that"*. This level of control over the lawful financial transactions of a nation's citizens is not only *ultra vires* as regards the Bank's statutory powers, but is absolutely unacceptable in a free society and should be resisted at every possible stage of its introduction.

Rather than wasting time, effort and resources on a CBDC, likely to be rejected by its end users and becoming a costly white elephant, we exhort the Bank and HMT to explore and understand the many innovations and opportunities presented by Bitcoin and Lightning as a new and open payment technology instead of attempting to dismiss or ignore them. Using

the Lightning network for payments will not automatically mean that the Bank is no longer able to issue sterling bank notes. It is simply a better payment technology for online transactions than any other which has been invented to date.

Regarding the general availability of central bank liability money, as a matter of policy we in fact wholeheartedly support the Bank's intention to maintain access to physical cash as an absolutely crucial element in maintaining the privacy and financial autonomy of British citizens.

- (9) <https://cointelegraph.com/news/how-to-transfer-1-billion-for-basically-free-bitcoin-whale-watching>
- (10) <https://nostr.how/en/zaps>
- (11) <https://cointelegraph.com/news/bitcoin-lightning-network-vs-visa-and-mastercard-how-do-they-stack-up>
- (12) <https://cryptoslate.com/marathon-zero-two-to-launch-sustainable-mining-operation-in-abu-dhabi/>

10. Do you have comments on our proposition for the roles and responsibilities of private sector digital wallets as set out in the platform model? Do you agree that private sector digital wallet providers should not hold end users' funds directly on their balance sheets?

If we concede that a UK CBDC exists, and that it exists as a liability of the central bank, then any such liabilities should as a matter of law exist as a bilateral relationship between the end user and the central bank. However, this illustrates the absurdity of the proposal. The digital pound is not intended to be a bearer asset, like Bitcoin - which is digital cash - but will be a permissioned token that requires at least one and potentially multiple trusted third parties in order to be usable. The Bank, on the other hand, is simply not equipped (even via the intermediation of the PIPs) to run digital pound accounts for seventy million UK residents.

The proposed platform model will render the CBDC essentially unspendable without the active involvement of trusted third parties such as the PIPs, and while the CBDC should not at law be included in the PIPs balance sheets (as it would be neither their liability nor owed to them) it is absurd that it should require their involvement at all to be held or spent - if it represents a liability of the central bank.

It is possible to create a valid Bitcoin wallet simply by rolling dice or by flipping a coin, and instantaneously to use that new wallet to transact with anyone, anywhere in the world, virtually for free, and without any counterparty risk - and without asking permission from anyone. There is no sense in which a permissioned CBDC, that requires the involvement of PIPs as gatekeepers, and the central bank to manage and control the ledger, could possibly rival the functionality already presented by Bitcoin.



In terms of the safety and security of the proposed digital pound, the Bank should note that the attack surface which it will expose to hostile actors is significant. The digital pound ledger will be a honey pot both for state and non-state attackers, and it is questionable even in the period before AI is being widely used to assist in such attacks, whether it is possible for a complex web of PIP wallets and the Bank's centralised ledger adequately to defend themselves from exploitation.

11. Do you agree that the Bank should not have access to users' personal data, but instead see anonymised transaction data and aggregated system-wide data for the running of the core ledger?

This question demonstrates the challenge in bridging the gap between a digital bearer asset, like Bitcoin, and a permissioned digital token, such as a digital pound. Cash as it exists today obviates the need for any personal data collection and is typically understood as being a valid instrument to discharge all debts, public and private. No personal data collection is required to transact with cash - this is in many ways the entire 'point' of cash. A seller does not need to 'know' their customer at all in order to transact with them if the customer is paying in person, with cash. Title to the bearer asset is simply transferred and perfected upon delivery to the recipient.

If we concede that a digital pound will exist, it is manifestly clear from the paper that it will not (and cannot) be a form of digital cash as it fails the most basic tests for the same *ab initio*. If it is not digital cash, then the logic of the entire enterprise is suspect and the only sensible conclusion is that the Bank should save time, cost and effort, and acknowledge that individuals should simply continue to transact with e-money, their existing bank accounts, or the other forms of digital money that already exist and are already functioning.

Our view is that a digital cash system should not in any way collect personal data of the user at all. If the Bank and law enforcement wish to collect personal data, they are free to monitor users' bank accounts and their transactions with the other forms of digital money that already exist. Any further expansion of the Bank's powers here is arguably not merely *ultra vires* (above and beyond the powers granted to the Bank by its charters and related legislation), but also a potential breach of the Human Rights Act 1998 and the underlying European Convention on Human Rights - quite apart from the relevant data protection legislation. We address each of these briefly below:

(i) **Bank of England - potential ultra vires actions:** The gathering of the transaction data of every single citizen whether in the UK or worldwide, whosoever uses the digital pound, is such an egregious overreach of the powers granted to the Bank by statute (13) that is is incomprehensible it has ever been suggested. Absolutely no steps should be taken in this direction without detailed debate in Parliament followed by primary legislation, and even then such actions should be strongly resisted not merely by human rights and civil liberties groups but also by the general citizenry of the United Kingdom as well. The freedom to transact is absolutely fundamental to the existence of a free society and underpins many other

freedoms. The existence of a potentially programmable money that could in theory be modified to include limits on holdings, or restrictions regarding where and how it can be spent, or even expiry dates such as the digital yuan includes, is nothing short of an extraordinary and astonishing expansion of the Bank's powers deep into the realm of social control and engineering. This is not, and never should be, in the Bank's mandate.

(ii) **Human Rights - potential violations:** The European Convention on Human Rights (ECHR), incorporated into domestic law via the Human Rights Act 1998 (HRA) provides at Article 8 that "everyone has the right to respect for his private and family life, his home and his correspondence... There shall be no interference by a public authority [*read: The Bank*] with the exercise of this right except such as is in accordance with the law **and [our emphasis]** is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." It is arguable that the gathering of transaction data by a public authority (the Bank, in conjunction with the PIPs who will gather personal information) who is not authorised by statute to gather or hold that information, and in particular where such information gathering does not appear 'necessary', will violate the human rights of every single person who uses the digital pound and will leave the entire enterprise rightly open to challenge.

Secondly, Article 10 of the ECHR provides that "everyone has the right to freedom of expression... This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." The transmission of a digital currency transaction is, in definitional terms, the transfer of information. By way of example, no asset physically changes hands in a Bitcoin transaction - **the protocol at its simplest is an unstoppable messaging protocol and a Bitcoin transaction may be understood as a message sent to the entire network with instructions regarding the changes of balances.** In the same way, a transaction where a person sends a digital pound may be understood as a transmission of information, and it is arguable that the Bank's proposed gathering and monitoring of transactions, in conjunction with the PIP's gathering of personal data, violates this right and will also be subject to challenge.

We do not propose to discuss in detail the impact of the UK's data protection legislation on the proposed digital pound, but are of the view that it will also pose significant challenges for the Bank and the PIPs and potentially will require new primary legislation.

(13) <https://www.bankofengland.co.uk/-/media/boe/files/about/legislation/1998-act.pdf>

12. What views do you have on a privacy-enhancing digital pound?

Based on the paper and the accompanying technology paper, it appears impossible for the digital pound to be privacy-enhancing - this is a complete contradiction in terms.

The gold standard here should be the creation of a peer to peer digital cash, on a network that has solved the Byzantine General's problem, and which operates as a digital bearer asset. The only open, permissionless and censorship resistant solution to this problem is the Bitcoin proof of work algorithm, that removes the need for a trusted third party to maintain the ledger of transactions, and at the same time ensures that anyone may join or leave the network, and may freely transact while using that network, without any information on the user being gathered by a centralised party as they transact - namely, exactly as physical cash operates today.

If the digital pound is not a digital bearer asset that can be freely exchanged between transacting parties without the need to share any personal data at all as part of the transaction, then those parties should simply use their existing bank accounts. There is zero purpose and zero use case for a much worse form of digital token and a slightly worse system of sending digital money.

A potentially viable alternative is e-cash, of which several variations exist in the market. The EU has for some time been exploring e-cash with its inventor, David Chaum. Although this effort has not yet delivered results, several teams of Bitcoin developers currently have working e-cash models (Fedi and Cashu by way of example), which could serve as good sources of study for the Bank.

13. What are your views on the provision and utility of tiered access to the digital pound that is linked to user identity information?

We refer to our other responses regarding privacy and the nature of this proposed digital instrument. To the extent that the proposed digital pound is intended to emulate cash or bank notes, being a liability 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 continent¹².

14. What views do you have on the embedding of privacy-enhancing techniques to give users more control of the level of privacy that they can ascribe to their personal transactions data?

¹² <https://www.btcpolicy.org/articles/why-the-u-s-should-reject-central-bank-digital-currencies>



Please see our previous responses. The only acceptable form of a digital money in this context is a digital bearer instrument analogous to cash, for which no KYC or identification is required. Anything short of this will perpetuate and entrench pre-existing inequities and ensure that those who are currently excluded from the financial system remain excluded.

Privacy is the ability to reveal oneself selectively to the world; any system that requires identification as a gating item is no different from the existing payments system and the current financial regime. If there are no differences between the existing regime and the putative regime of CBDCs, then our strong recommendation is that the Bank and HMT do not waste time, money and resources in creating a new system that will be broadly identical to the existing system, with a number of additional downsides in terms of privacy and the control and monitoring of users' transactions - each of which will be strongly resisted by any citizens in a free society. As noted by Florida's Chief Financial Officer Jimmy Patronis in March of this year, a "Central Bank Digital Currency is the cornerstone of a federal government that could track each and every transaction that happens in the world. There would be no privacy, and if there is no privacy, there are no rights."

Significantly, we note that the paper states, "All payments should be able to be made using the digital pound so long as they are lawful, observe any restrictions (for example, maximum user holdings...) and comply with regulatory obligations laid down by authorities. Subject to a payment being lawful, the Bank would be neutral in processing it, and does not envisage applying any limitations on payments on ethical grounds." We do not need to point out that 'not envisaging' an action is very far from ensuring that it cannot happen. The digital pound will be technically capable of including these limitations and including programmability, and there is no indication that those with the power to control it will not at some stage in the future decide to implement these capabilities.

We note that there will be 'restrictions' on the use of one's own money in CBDC form. This is in stark contrast to Bitcoin, where the network imposes no restrictions on the end user in relation to the use of their money, and where the user has complete freedom and autonomy provided they comply with the rules of the protocol.

Secondly, we note that payments would be processed 'subject to being lawful'. We merely ask: "How will the Bank know which payments are lawful or not? What data is being transmitted to the Bank to enable them to make this decision?" The paper is silent on this point, but we can only assume that there is a proposed degree of information sharing likely between PIPs and the Bank that will ensure that additional transaction data is available upon demand in order to ensure a level of financial surveillance that should be unacceptable in a free society.

We need not point out to the Bank and to HMT that what is lawful or otherwise is continually in flux and arguably subjective over time. Governments around the world have repeatedly used the 'law' to oppress their critics, and it is by no means safe to assume that the United Kingdom would remain always immune to such repression. Increasingly, financial repression

is being used as an efficient method of stifling dissent, as the non-exclusive examples below demonstrate:

- When protests in Lagos occurred in 2020 against police violence, within days the government had frozen the bank accounts of protesters
- Amnesty determined to halt work in India after its bank account was 'frozen' in 2020
- The European Court of Human Rights in 2021 ruled against the state of Azerbaijan for freezing of bank accounts intended to paralyse an NGO's human rights work in the country
- As noted in a letter to the US Congress from 21 Human Rights Leaders in June 2022 "When crackdowns on civil liberties befell Nigeria, Belarus, and Hong Kong, Bitcoin helped keep the fight against authoritarianism afloat."¹³

The issue is not that the sitting government or any of the current political parties within the UK would seek to replicate the actions of more authoritarian countries around the world. It is that we should always be wary of assuming that democracy and the associated institutions that support it are robust enough to endure without diligent and focused support. Providing the technical functionality to enable authoritarian actions to be undertaken should always, therefore, be a point of contention.

We quote: "The assumption that leaders we empower with technology will always work in the public interest and for the public good is one of the myths dispelled by the political theorists of the Enlightenment. The principle that power corrupts gave rise to the separation of powers and to the highly federated form of government that has characterized the United States since its foundation. As Professor Andrew Ferguson at the American University Washington College of Law has succinctly stated, "Assume the tyrant."¹⁴

15. Do you have comments on our proposal that in-store, online and person-to-person payments should be highest priority payments in scope? Are any other payments in scope which need further work?

It has been suggested that the only plausible potential use case for a CBDC, which is not currently presented by existing forms of digital money, is in that of a wholesale settlement mechanism between commercial banks. While we do not propose to comment on the benefits or otherwise of a wholesale CBDC, a retail CBDC appears an authoritarian and *ultra vires* attempt to control, surveil and censor every law-abiding citizen who is unfortunate enough to have to use it.

16. What do you consider to be the appropriate level of limits on individual's holdings in transition? Do you agree with our proposed limits within the £10,000-£20,000 range? Do you have views on the benefits and risks of a lower limit, such as £5,000?

¹³ <https://www.nasdaq.com/articles/human-rights-leaders-pen-letter-to-us-congress-for-responsible-bitcoin-legislation>

¹⁴ <https://www.btcpolicy.org/articles/why-the-u-s-should-reject-central-bank-digital-currencies>



We regard any restriction on the ability of a person to hold any amount of currency as a restriction on their civil liberties and a potential breach of their rights pursuant to the Human Rights Act and/or the ECHR. Having said this, we very much hope that no UK citizen will ever hold or use any digital pound tokens at all.

17. Considering our proposal for limits on individual holdings, what views do you have on how corporates' use of digital pounds should be managed in transition? Should all corporates be able to hold digital pounds, or should some corporates be restricted?

We do not see that holding or being able to hold digital pounds will be an advantage in any respect to any corporation. Treasury functions at corporations are already complex, and digital pounds (as stated earlier in our submission) are not digital cash or digital bearer instruments and so will be unable to replace the cash treasury or 'kitty'. The digital pound as proposed is a permissioned token, administered at the back end by the Bank, and at the front end by PIPs. It is challenging to see how such a token will have any feasible use case for any corporation that is not already adequately served by existing forms of digital money. The potential restrictions on holding amounts effectively put an end to the digital pound's potential utility for corporations, as it is inconceivable that any company would find an asset useful in any respect if it is subject to an upper holding limit. Such a proposal will increase, not decrease, treasury function complexity and would be unlikely to be adopted.

18. Which design choices should we consider in order to support financial inclusion?

If the Bank and HM Treasury genuinely wish to support financial inclusion, then they should eliminate any and all forms of KYC or identification requirements before using the digital pound. ID verification, including but not limited to the provision of a permanent address, are among the factors ensuring that, for example, people without a home address are excluded from the banking system. Private sector innovation is taking place across Africa, for example, to support financial inclusion without the need for centralisation and/or privacy trade-offs, also reducing customer friction and access costs. We suggest the Bank review innovative solutions such as Machankura and BitText that enable people to broadcast Bitcoin transactions via the Lightning Network using feature phone and mobile phone networks - sending value without even a smartphone using no more than an SMS. Quite apart from these new technologies, various forms of cash, acting as completely accessible bearer instruments, have of course been used by humans for thousands of years. Cash has no barrier to entry, and the suggestion that a person should be required to show their ID in order to use it is nothing short of absurd.

Bitcoin, by contrast, excludes no one. Any person is able to create a Bitcoin wallet (either using free and open source software, or by techniques as we describe earlier). As soon as the wallet is created, that person is then able to transact with any other person, anywhere on the globe, who also has a Bitcoin wallet. There is no feasible way that a permissioned token



like the digital pound can possibly offer a similar level of financial inclusion that could compete with the level of inclusivity offered already by Bitcoin.

We note that the Annex of the paper highlights what we believe is the genuine reason behind these proposals for a CBDC. "Widespread adoption of a non-sterling digital form of money in the UK is unlikely but its impact would be very significant and be beyond the tolerance of UK authorities....It is possible, however, that non-sterling digital money would offer attractive new functionality in the future. Non-sterling digital money could become widely adopted if it tapped into existing digital networks to offer new propositions. That is judged unlikely but, if it materialised, the impact would be very significant and so this scenario is beyond UK authorities' risk tolerance.

By reinforcing the use of sterling for UK payments and enabling new payments functionality, the digital pound could pre-emptively reduce the chance of widespread adoption of non-sterling digital money in the UK." [Our emphasis].

It is important for the Bank to understand that non-sterling digital money is already here, and it already offers attractive new functionality today, without any further development being necessary. Besides this functionality, it has a capped supply, it cannot be manipulated or debased by any central bank, and its monetary policy is already predetermined in its code and is viewable by any of its users. It does not require any KYC or any fixed address to be used and in every respect (other than widespread adoption) it is simply a better form of money and a better payment technology.

However, our policy position is that this represents an opportunity for the UK, and not a threat - and that countries which understand and adopt this new technology first will have an advantage. Central banks may continue to perform their core functions; while businesses and individuals remain free to use and adopt a payment technology that is able to move money instantaneously on a neutral settlement layer that is freely available to all.

The Bank and HMT have assumed that people like Bitcoin because it is 'digital', and that it can be forced into irrelevance by creating a new form of bank token that is also digital. This is a fundamental misunderstanding of the power and potential of Bitcoin. People do not like it simply because it is 'digital'. It merely 'happens' to be digital. People like it because it cannot be controlled, debased or confiscated by any government or central bank. They like it because the transactions they make with it cannot be censored, and because it enables them truly to own their own property in a form that no government can dilute or remove from them.

No permissioned bank token, subject and exposed to identical risks of debasement, dilution, confiscation and control, can ever compete on the same footing as the non-sterling money that is already here in the UK, and being held and used by millions around the world.



19. The Bank and HM Treasury will have due regard to the Public Sector Equality Duty, including considering the impact of proposals for the design of the digital pound on those who share protected characteristics, as provided by the Equality Act 2010.

Please indicate if you believe any of the proposals in this Consultation Paper are likely to impact persons who share such protected characteristics and, if so, please explain which groups of persons, what the impact on such groups might be and if you have any views on how impact could be mitigated.

While we do not have a particular view regarding persons with protected characteristics, we do reiterate the general point that the ostensible aims of the digital pound inasmuch as it is purported to increase financial inclusion are completely undermined by the requirements to identify users to PIPs. This will instantaneously exclude the very people that require access to the financial system the most.