

# CBDC

**a privacy-eroding  
pound?**



**Lessons from international  
central bank digital currency  
pilots for the UK**

# About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

## Contact

Silkie Carlo

Director

Email: [silkie.carlo@bigbrotherwatch.org.uk](mailto:silkie.carlo@bigbrotherwatch.org.uk)

Jake Hurfurt

Head of Research and Investigations

Email: [jake.hurfurt@bigbrotherwatch.org.uk](mailto:jake.hurfurt@bigbrotherwatch.org.uk)

Susannah Copson

Legal and Policy Officer

Email: [susannah.copson@bigbrotherwatch.org.uk](mailto:susannah.copson@bigbrotherwatch.org.uk)

**CBDC - a privacy-eroding pound? Lessons from international central bank digital currency pilots for the UK**

Published: November 29 2023

# Contents

|  |    |
|--|----|
| <b>Introduction</b> .....                        | 1  |
| <b>Glossary</b> .....                            | 4  |
| <b>e-Peso</b> .....                              | 7  |
| <i>Aims of the Pilot</i> .....                   | 9  |
| <i>Transfers and Traceability</i> .....          | 9  |
| <i>Anonymity and Security</i> .....              | 10 |
| <i>Pilot Findings</i> .....                      | 11 |
| <b>E-krona</b> .....                             | 13 |
| <i>Design</i> .....                              | 13 |
| <i>Motivations</i> .....                         | 16 |
| <i>Privacy, Anonymity and Traceability</i> ..... | 17 |
| <i>Programmability</i> .....                     | 18 |
| <b>Digital Shekel</b> .....                      | 21 |
| <i>Model</i> .....                               | 21 |
| <i>Justifications</i> .....                      | 22 |
| <i>Privacy</i> .....                             | 23 |
| <i>Programmability</i> .....                     | 25 |
| <i>CBDC Risks</i> .....                          | 25 |
| <b>eNaira</b> .....                              | 27 |
| <i>Motivations</i> .....                         | 27 |
| <i>Model</i> .....                               | 28 |
| <i>Privacy</i> .....                             | 30 |
| <i>Success</i> .....                             | 32 |
| <b>Digital Euro</b> .....                        | 34 |
| <i>Objectives and Motivations</i> .....          | 34 |
| <i>Model</i> .....                               | 36 |
| <i>Privacy</i> .....                             | 38 |
| <i>Risks from a Digital Euro</i> .....           | 41 |
| <i>Programmability</i> .....                     | 41 |
| <b>Jam-Dex</b> .....                             | 43 |
| <i>Motivations</i> .....                         | 44 |
| <i>Model</i> .....                               | 44 |
| <i>Usage</i> .....                               | 45 |

|  |    |
|--|----|
| <b>e-CNY</b> .....   | 46 |
| <i>Model</i> .....   | 47 |
| <i>Privacy</i> .....   | 47 |
| <i>Programmability</i> .....                                     | 49 |
| <br>   |    |
| <b>Digital Pound</b> .....                                       | 51 |
| <i>Model</i> .....   | 51 |
| <i>Privacy</i> .....   | 52 |
| <i>Programmability</i> .....                                     | 54 |
| <br>   |    |
| <b>Policy Analysis</b> .....                                     | 56 |
| <i>Privacy</i> .....   | 56 |
| <i>CBDCs and surveillance</i> .....                              | 56 |
| <i>Privacy by design</i> .....                                   | 61 |
| <i>Data rights</i> .....   | 63 |
| <i>Programmable money</i> .....                                  | 64 |
| <i>Inclusion or exclusion?</i> .....                             | 65 |
| <i>Digital identity</i> .....                                    | 68 |
| <i>Legal developments and democratic involvement</i> .....       | 70 |
| <i>CBDCs in action: what's gone wrong?</i> .....                 | 72 |
| <i>Conclusion</i> .....  | 74 |
| <br>   |    |
| <b>Appendix - summary of major cbdc's around the world</b> ..... | 78 |
| <i>Full launch</i> .....   | 78 |
| <i>Pilot</i> .....   | 79 |
| <i>Proof of concept, research &amp; cancelled</i> .....          | 83 |

# Introduction

More than 130 central banks around the world are currently researching, piloting or have introduced a form of Central Bank Digital Currency [CBDC].<sup>1</sup> These range from small countries with limited economic output, to nations with heavily cash-based economies and some of the world's biggest economic actors. Authoritarian and democratic states alike are examining the possibility of introducing a digital currency – many claim to be motivated by the declining use of cash, the instability of cryptocurrencies and other digital assets, and the growth potential that new technologies could unleash.

Among the countries looking at developing a CBDC is the UK, where the proposal is dubbed "Britcoin". In mid-2023, the Bank of England and His Majesty's Treasury launched a consultation about a potential future digital pound – although details about how this might look are currently limited.

Big Brother Watch is concerned that a UK CBDC as outlined in the consultation would be detrimental to people's privacy, their freedom to spend money anonymously and the potential for the data collected to be used for surveillance.

A digital pound would be subject to many of the same invasive surveillance rules as bank accounts including anti-money laundering regulations, laws to prevent the financing of terrorism, fraud checks and investigatory powers laws – only, with a CBDC, our private information would be one step closer to the state. Against this existing legal backdrop, digital currency would be much less private than physical cash as the authorities are practically legally obliged to conduct mass surveillance of transaction data where they can.

The dangers of programmable money, even if remote, could have further serious impacts on human rights and civil liberties – a CBDC could be designed to limit how, when or where money is spent which could give those holding the purse strings the ability to influence people's behaviour like never before.

In addition to the risk of intrusion from the state, CBDCs could also exacerbate intrusion by private actors. Depending on the design of a British CBDC, there is the risk that the vast quantities of data generated would be attractive to private businesses to power ever more intrusive and personalised marketing. It is not only companies that will have an interest in our financial information – the collation of all this data would also make a UK CBDC a honeypot for criminals who would see the information as a treasure trove for illicit use. Given that CBDCs are highly likely to be linked to our digital identities, the risk of theft,

<sup>1</sup> Central Bank Digital Currency Tracker, Atlantic Council, accessed 2nd October 2023, <https://www.atlanticcouncil.org/cbdctracker/#:~:text=130%20countries%2C%20representing%2098%20per-cent,advanced%20stage%20of%20CBDC%20development>.

misuse and unauthorised access is particularly severe.

With countries all over the world developing CBDCs it is reasonable to expect that the Bank of England will learn from other central banks as it moves through its own process of developing one. Different governments and banks have published a huge amount of information about their projects, offering significant insights into the potential harms of various aspects of digital currencies and serving as a warning about what would happen if the Bank of England were to pursue certain design options.

Taking a sample of six CBDCs, at various developmental stages, this report examines how other countries are seeking to implement digital currency programs, analysing their models and assessing their privacy harms with a view to scoping the risks of a potential UK CBDC. We present in depth examinations of Jamaica's Jam-Dex, the EU's digital euro, Uruguay's e-Peso pilot, Sweden's e-krona, the Israeli digital shekel and Nigeria's enaira.

Each CBDC program highlights different areas of concerns as to how CBDCs might develop and how they could have a detrimental impact on the general public. Nigeria and Jamaica are tying their digital currencies to digital identity schemes, Israel is using the digital shekel to pursue a goal of pushing cash out of the economy and to deprioritise privacy and Uruguay's pilot offered the authorities the ability to trace transactions with participants relying on weak pseudonymisation. In Sweden and the EU, where significant attention is paid to privacy, the findings of both countries' central banks illustrate how a CBDC will never be truly private or anonymous, with the best case scenario seeking pocket change-level transactions protected while bigger purchases are subject to anti-money laundering and counter terror financing (AML/CTF) transparency rules in a way cash is not.

This report focuses on a certain type of digital currencies termed "retail CBDCs", which are designed for use by the general public. There is another significant form of CBDCs that are intended for use solely by financial institutions known as "wholesale CBDCs", and at present a significant number of the countries researching digital currencies are focused on this use case.

A retail CBDC is a version of a central bank-issued digital currency that is intended to fulfil a similar role to cash in the economy, being part of transactions between individuals and businesses.<sup>2</sup> This is the form of CBDC which would touch on the daily lives of ordinary people, and potentially poses significant privacy risks. The effects that retail CBDCs have on the general public are both the motivation and focus of this report.

Wholesale CBDCs, although also digital currency issued by a central bank, would play a vastly different role in the economy. They would exist purely to be used in transactions

<sup>2</sup> What Will A Retail Central Bank Digital Currency Mean? UK Finance, accessed 19th October 2023, <https://www.ukfinance.org.uk/news-and-insight/blogs/what-will-retail-central-bank-digital-currency-mean>

between central banks, commercial banks and other financial institutions.<sup>3</sup>

Large quantities of money often move between these financial institutions in transactions referred to as "interbank payments", with funds most commonly being held in accounts run by central banks. Interbank payments are often of high value and can include end-of-day settling up of transactions between two institutions' retail customers at the bank level, foreign exchange transactions and more.<sup>45</sup> Cross-border payments are processed in a similar fashion but often have added hurdles stemming from less-than-seamless integration between different national banking systems.

Digital forms of money are already used to settle interbank payments. Central banks do not move pallets of banknotes between vaults, but rather balances are recorded on digital systems with financial institutions trusting that balances are convertible to cash in theory. This means that digital central bank money is already available to financial institutions.<sup>6</sup> A wholesale CBDC would differ from this system as it would be a separate kind of central bank liability, based on a distributed ledger or similar platform, and would likely be a tokenised form of central bank money that could be exchanged between financial institutions.

As wholesale CBDCs, would not be a part of the wider public's day-to-day transactions and would play a fundamentally different role in the economy, this report centres on retail CBDCs alone.

Big Brother Watch highlighted our concerns about the UK Government's CBDC proposals in our April 2023 consultation response<sup>7</sup> – and this research paper analysing different approaches to CBDCs around the world concludes that, the world over, the costs of CBDCs far outweigh any claim to benefits.

<sup>3</sup> Wholesale Central Bank Digital Currency, Banque de France, 3rd October 2023, <https://www.banque-france.fr/en/governors-interventions/unveiling-potential-wholesale-cbdc-what-in-sights-and-prospects>

<sup>4</sup> Examining CBDC and Wholesale Payments, Economic Research, FEDS Notes, 8th September 2023, <https://www.federalreserve.gov/econres/notes/feds-notes/examining-cbdc-and-wholesale-payments-20230908.html>

<sup>5</sup> Interbank Payments: Payments Between Financial Institutions, Danmarks Nationalbank, accessed 19th October 2023, <https://www.nationalbanken.dk/en/what-we-do/safe-and-efficient-payments/in-terbank-payments#:~:text=Like%20citizens%20and%20businesses%2C%20banks,which%20also%20cover%20customer%20payments.>

<sup>6</sup> Speech: Demystifying Wholesale Central Bank Digital Currency, Fabio Panetta, European Central Bank Executive Board, 26th September 2022, <https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220926~5f9b85685a.en.html>

<sup>7</sup> Big Brother Watch's submission to the HMT and Bank of England consultation on a digital pound, April 2023: <https://bigbrotherwatch.org.uk/campaigns/no-spycoin/#BRIEFINGS>

## Glossary

**Monetary anchor** - The "safest" form of money in an economy, usually central bank money that is guaranteed by the state, which all other forms of money are convertible to.

**KYC** - Know Your Customer verification, where banks and other financial institutions are required to check the identity of new clients and assess them for potential risk.

**AML** - Anti money laundering regulations.

**CTF** - Counter terror finance regulations.

**Private money** - A form of money issued or maintained by a non-state actor, such as a commercial bank. An example of this is bank deposits as banks will honour your account balance, but do not hold specific hard currency corresponding to your account balance in a vault.

**Public money** - Money issued by a central bank that is widely accepted and used by everyone, and regulated by the state.

**Distributed ledger** - A shared digital record or database that is simultaneously synchronised across multiple devices and accessible by multiple people across a large peer-to-peer network, without a central administrator. Changes [such as recording transactions] are effectively vouched for by peers in the network, through consensus tools, such as proof-of-work or proof-of-state, and then communicated across the network.

**Blockchain** - A form of distributed ledger technology [DLT] where changes are linked to the end of the existing ledger as a "block" to make a chain, with blocks being signed by encrypted signatures [hashes] which can be used to validate their legitimacy.

**Public blockchain** - The most commonly used form of blockchain which underpins many cryptocurrencies, such as Bitcoin, where anybody can become a peer in the network to add transactions and act as a validator.

**Private blockchain** - A blockchain where a central administrator grants access to the network, and grants permissions to trusted parties to add and validate transactions.

**Electronic money** - An electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer.

**Intermediary** - An entity acting between a central bank and end users.

**Conditional payments** - A payment set up to process automatically when certain, pre-set conditions are met.

**Smart contracts** - A digital contract programmed to automatically execute pre-determined actions when certain, pre-set conditions are met. A conditional payment is a specific example of a smart contract.

**Programmable money** - Money with built-in rules that restrict its use. This could range from where/when money is spent, or on what, positive or negative interest rates or even expiry dates.

## Augustín Carstens

General Manager of the Bank for International Settlements

“We don’t know, for example, who’s using a \$100 bill today and we don’t know who’s using a 1,000 peso bill today. 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.”

## e-Peso Uruguay

Stage: Pilot

### Summary

- Pilot saw **low uptake of the e-Peso**, particularly among women and older people
- All remaining e-Pesos **were destroyed** following Uruguayan pilot
- Mobile phone numbers were used as **unique identifiers** for e-Peso wallets
- Transaction and wallet data was pseudonymised, and **was traceable** if deemed necessary
- Privacy protection with the e-Peso was poor, as **transactions were highly traceable**

Uruguay piloted its CBDC, the e-Peso, for six months from November 2017 to April 2018, one of the first large-scale pilots of digital central bank money in the world.<sup>8</sup> The trial was limited to 10,000 people and a total circulation of 20 million Uruguayan pesos [c. £521,600 at the time]. Individual users were limited to \$U30,000 [c. £780 at the time], while businesses could hold up to \$U200,000 [c. £5,200] worth of e-Pesos.<sup>9</sup>

The pilot utilised wallets held on mobile phones. The Bank of Uruguay worked with the country’s state-owned telecoms firm ANTEL [one of three mobile networks in the country], whose customers provided the user base for the trial. E-Pesos could be used to pay for goods and services or to conduct peer-to-peer transfers between account holders.<sup>10</sup>

Monetary security firm The Roberto Giori Company [RCG] worked with the central bank to develop the CBDC trial and the core technology underpinning the e-Peso trial. RedPagos, a Uruguayan payment network which provides a host of services from bill payments to pension collection and cash withdrawals, similar to PayPoint in the UK, provided the interface between e-Peso wallets and other forms of money. This allowed physical currency or digital money [such as bank account balances] to be exchanged for the CBDC or vice versa.<sup>11</sup>

Other infrastructure for the trial was provided by tech giant IBM which was responsible for data storage and call centre management. The digital wallets used by pilot participants were developed and managed by local fintech firm InSwitch Solutions.

8 Seven Lessons From The E-Peso Pilot Plan, Banco Central del Uruguay, March 2022, <https://www.bcu.gub.uy/Sistema-de-Pagos/Documents/Vigilancia/Libros/CBDC%20march2022.pdf>

9 Uruguayan E-Peso On The Context Of Financial Inclusion, Gerardo Lincandro, Banco Central del Uruguay, 16th November 2018, [https://www.bis.org/events/eopix\\_1810/licandro\\_pres.pdf](https://www.bis.org/events/eopix_1810/licandro_pres.pdf)

10 Ibid

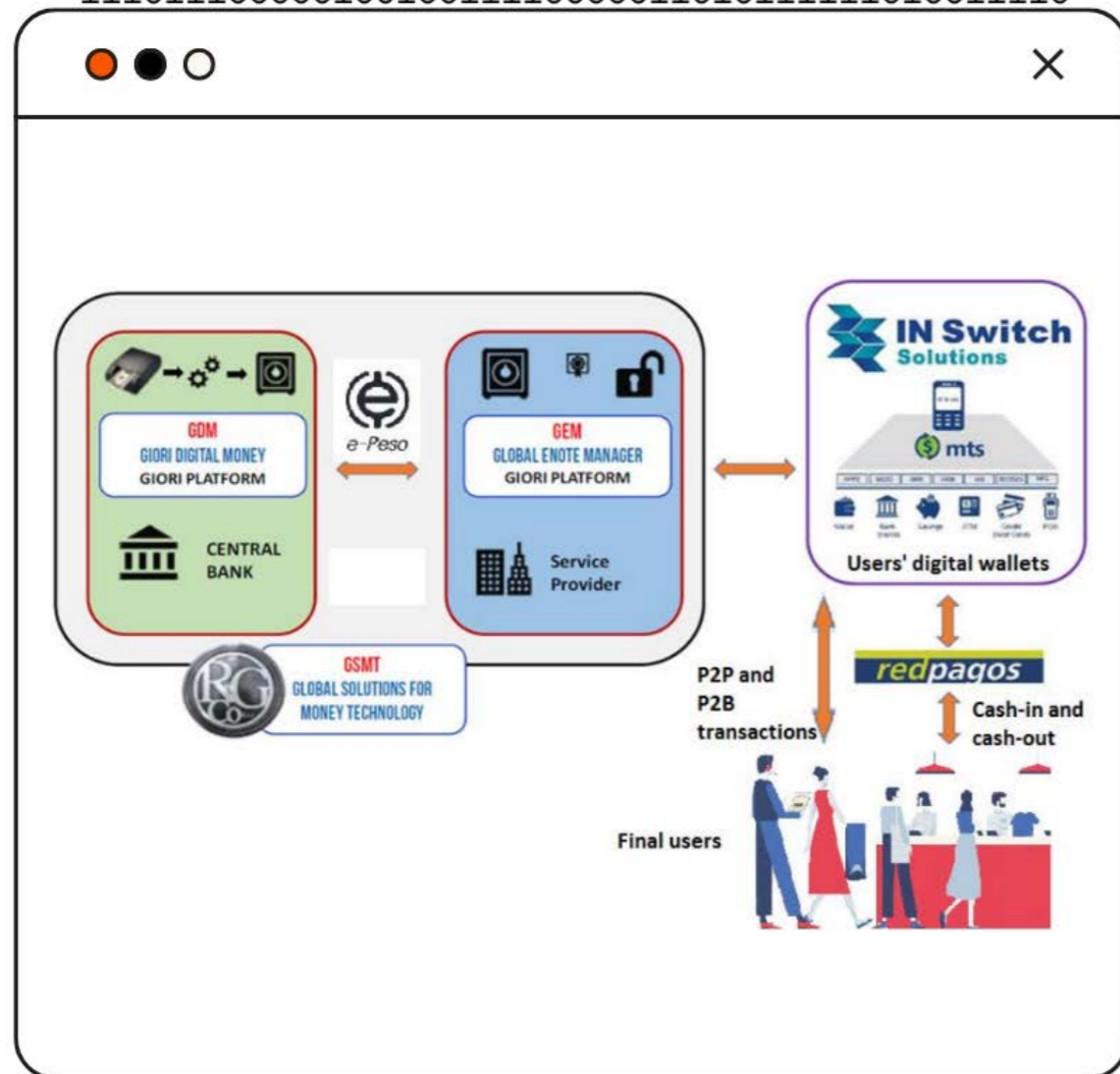
11 Ibid



```

10011110010111100011110001011011000111101100001
00110001111100100100011101101110011110010001100
10111001111000001111001110011110001111001001100
01111100000111100000000111111010011110001111101
11101110000010010011110000011010111111010011110

```



```

010001100110000001100000000011101111111110000
000011100111100110111001110100000110010011
11111000011001101110000110100111001111110110010
00110011110011011010011001001110100110001001001
00111011100011100010100110011100011000011000011

```

Following the conclusion of the trial in April 2018, Uruguay’s central bank destroyed all e-Pesos with participants converting the CBDC back to cash or private digital money.

Financial incentives were offered to encourage participation in the scheme. The first 1,000 people signing up received 500 e-Pesos and five monthly lotteries took place which were open to active individual users [10 monthly transactions or more] and active business users [3 invoices collected in e-Pesos per month].<sup>12</sup>

<sup>12</sup> Uruguayan E-Peso On The Context Of Financial Inclusion, Gerardo Lincandro, Banco Central del Uruguay, 16th November 2018, [https://www.bis.org/events/eopix\\_1810/licandro\\_pres.pdf](https://www.bis.org/events/eopix_1810/licandro_pres.pdf)

### Aims of the Pilot

Uruguay has a law mandating the government to promote financial inclusion, which has been in place since 2014. It contains targets for universal access to the financial system, as well as measures to formalise the country’s labour market and improve digital payment system efficiencies to widen accessibility while lowering costs.<sup>13</sup> Inclusion has been cited as a major motivator for the BCU to examine the utility of an e-Peso - as a way of competing with privately owned digital payment systems.

Elderly people generally prefer cash over private digital money, and there are others in society who the BCU state see added value in the use of cash for “cultural reasons”.<sup>14</sup> It was suggested that a central-bank-backed digital cash system could present a solution suitable for those who prefer cash and would support those with cultural attachments to cash towards using digital payment methods.

The so-called cost of cash appears to be a further motivator for the Central Bank of Uruguay (BCU) to investigate the e-Peso. It regularly cited both direct costs of cash transactions and costs to the wider economy from them as a justification for a digital currency. BCU papers on the country’s cash economy argued that the aggregation of cash handling fees, insurance for holding cash and other implicit costs from physical money cost up to 0.58% of Uruguay’s GDP.<sup>15</sup> There was also a discussion of Uruguay’s informal economy and the role a CBDC might play in taxation in BCU presentations on the digital currency.

### Transfers and Traceability

The e-Peso trial took a token-based approach to CBDCs, effectively storing digital banknotes in users’ wallets. This means users will have “held” e-Peso tokens of various values totalling up to the value held in their wallet. These tokens [digital bills and coins] each had unique reference numbers that made them traceable.<sup>16</sup> Early plans for the e-Peso would have allowed users to see specific digital bills in their wallets, but this was scrapped.

Wallets were designed to work with just a basic mobile phone signal and without an internet connection. If there was no internet connection transactions could be validated by using a technology similar to text messages which only required a GSM [pre-3G] mobile

<sup>13</sup> Seven Lessons From The E-Peso Pilot Plan, Banco Central del Uruguay, March 2022, <https://www.bcu.gub.uy/Sistema-de-Pagos/Documents/Vigilancia/Libros/CBDC%20march2022.pdf>

<sup>14</sup> Ibid

<sup>15</sup> The Cost Of Using Cash and Checks In Uruguay, Marcelo Álvez, Rodrigo Lluberías & Jorge Ponce, Journal of Central Banking Theory and Practice, 2020(2), <https://sciendo.com/pdf/10.2478/jcbtp-2020-0016>

<sup>16</sup> Seven Lessons From The E-Peso Pilot Plan, Banco Central del Uruguay, March 2022, <https://www.bcu.gub.uy/Sistema-de-Pagos/Documents/Vigilancia/Libros/CBDC%20march2022.pdf>

connection.<sup>17</sup> Transactions were settled instantaneously when made online and offline, although some later validation may have been needed for offline payments.

The unique identifiers assigned to each token were a check against “double spending”. It appears that the digital wallets worked as a virtual replica of a real wallet with e-Peso tokens moving between devices and being stored on the mobile phone-based wallet, as notes would be stored in a physical wallet.

### *Anonymity and Security*

Jorge Ponce, Head of Economic Research for the BCU, wrote in a 2019 paper presented to the Spanish Central Bank that reconciling the anonymity of cash with a CBDC would be hard and may put users off.<sup>18</sup>

Unlike many CBDCs in development, the e-Peso was not based on distributed ledger technology. It instead used proprietary technology developed by RCG for the CBDC pilot, which came in two parts. Giori Digital Money [GDM] issued e-Pesos on behalf of the Uruguayan Central Bank while the Global E-Note Manager [GEM] acted both as a “virtual vault” and a digital wallet for the storage of e-Pesos.<sup>19 20</sup>

Users effectively had two wallets: the identifiable public wallet on their phone created by InSwitch Solutions and a pseudonymised, encrypted wallet, or vault, at the system level powered by GEM. These two wallets were connected on a one-to-one basis, with the mobile phone wallets linked to a specific mobile number as an identifier.

E-Pesos were not transferred directly between mobile-phone-based wallets. Tokens were moved from the mobile wallet to the user’s linked pseudonymised, encrypted vault to be validated before being transferred to the recipient’s mobile wallet via their encrypted vault.

At the GEM level, with the encrypted vault, pseudonymised transaction data is visible to the central bank. This meant that the BCU could see how e-Pesos moved between the encrypted wallets, but by default could not see any identifying information or the mobile phone wallet they are linked to. The design allowed the veil of anonymity to be

17 Ibid  
18 Digitalization, Retail Payments and Central Bank Digital Currency, Jorge Ponce, Revista De Estabilidad Financiera (39), Banco de España, Autumn 2020,  
19 Digitalization, Retail Payments and Central Bank Digital Currency, Jorge Ponce, Revista De Estabilidad Financiera (39), Banco de España, Autumn 2020, <https://www.bde.es/f/webbde/GAP/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanciera/20/Digitalization.pdf>  
20 Central Bank Digital Currency: the Uruguayan e-Peso Case Mario Bergara & Jorge Ponce; Do We Need Central Bank Digital Currency? Economics, Technology and Institutions, ed. Ernest Gnan and Donato Masciandaro, 2018, [https://www.suerf.org/docx/s\\_cf0d02ec99e61a64137b8a2c3b03e030\\_7025\\_suerf.pdf](https://www.suerf.org/docx/s_cf0d02ec99e61a64137b8a2c3b03e030_7025_suerf.pdf)

lifted in some circumstances, such as following a court order or request from a competent authority, linking the encrypted wallet to the identifiable wallet.<sup>21</sup>

Using the encrypted vaults as intermediaries in transactions also allowed each side of an e-Peso to remain pseudonymised to one another in any transaction records held on the mobile phone wallets.

In presentations outlining the pilot’s findings, the BCU admitted that there were concerns about the role of “big brother” in digital currency and the potential control over people’s spending.<sup>22</sup> However, bar a brief claim that the e-Peso “satisfied all preferences for privacy” due to pseudonymisation, there did not appear to be a substantial discussion about the potential privacy risks of a digital currency.

### *Pilot Findings*

Participants in the pilot were significantly younger than Uruguay’s general population, with those aged 30 to 44 the most likely to take part. People aged 18 to 29 participated at a similar rate to their population share, while those aged 45-64 participated slightly less. Those aged 65 and over were much less likely to take part in the CBDC trial.<sup>23</sup> The gender split of participants saw men make up 75 per cent of those taking part.

Transaction data from the pilot found that the vast majority of participants only used their CBDC wallets a handful of times, while the mean value of the transactions made stayed roughly flat until the final month of the trial [after which all e-Pesos were turned back to other forms of money]. Most transactions were for small amounts and peer-to-peer transfers were common.

The BCU found that the e-Peso was a “valid instrument” for small payments. It also outlined warnings from banks and other financial institutions about the potential for a CBDC to compete with bank accounts for digital stores of cash, which would have a significant impact on the retail banking industry.<sup>24</sup> This is a fear that has also been reflected by the European Central Bank, as if people swapped bank deposits and debit cards for a CBDC, banks would have much less liquidity to lend which could seriously undermine investment in the economy.

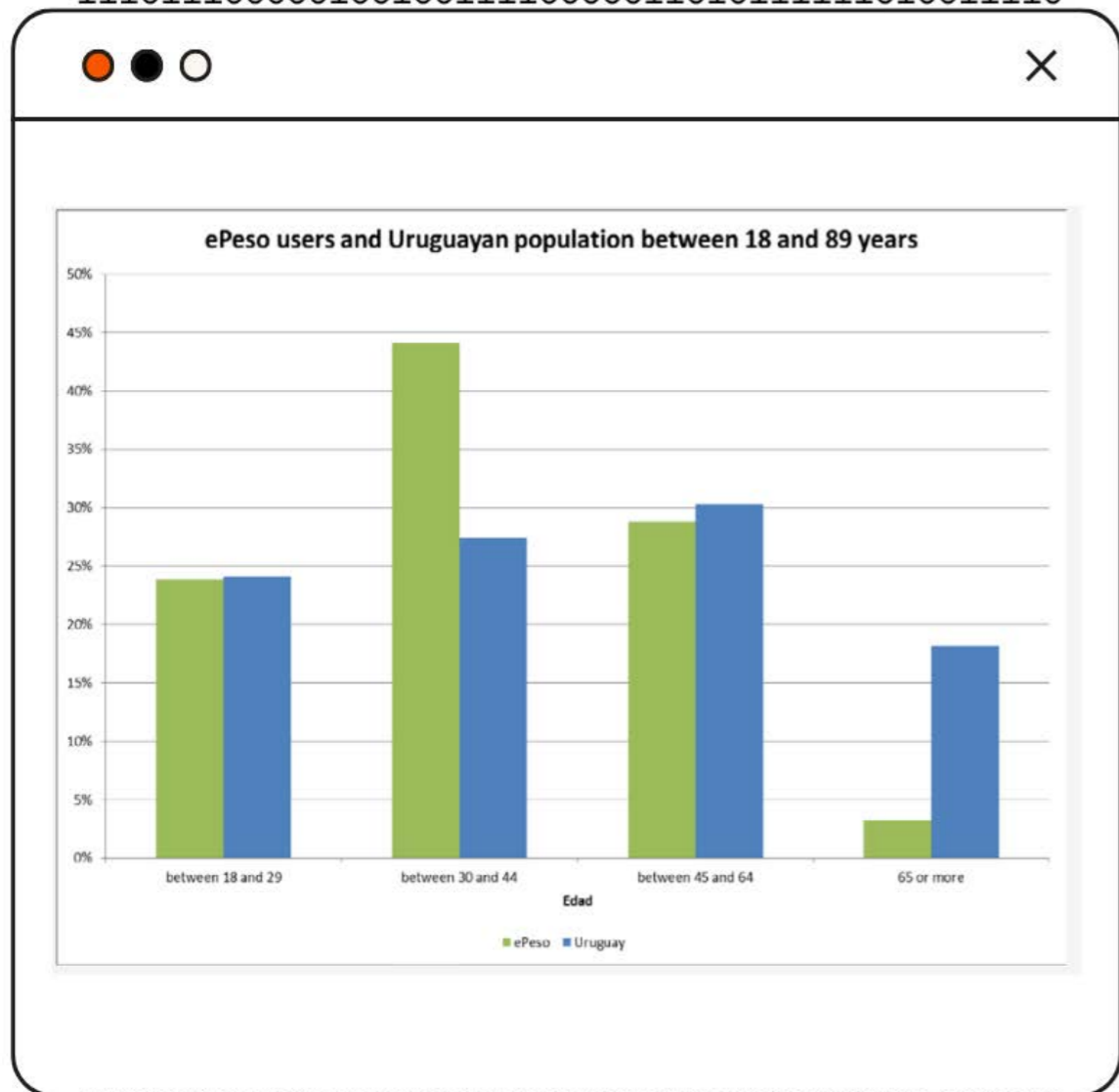
Uruguay’s central bank does not view the e-Peso as competing with banks for larger

21 Ibid  
22 Seven Lessons From The E-Peso Pilot Plan, Banco Central del Uruguay, March 2022, <https://www.bcu.gub.uy/Sistema-de-Pagos/Documents/Vigilancia/Libros/CBDC%20march2022.pdf>  
23 Uruguayan E-Peso On The Context Of Financial Inclusion, Gerardo Lincandro, Banco Central del Uruguay, 16th November 2018, [https://www.bis.org/events/eopix\\_1810/licandro\\_pres.pdf](https://www.bis.org/events/eopix_1810/licandro_pres.pdf)  
24 Seven Lessons From The E-Peso Pilot Plan, Banco Central del Uruguay, March 2022, <https://www.bcu.gub.uy/Sistema-de-Pagos/Documents/Vigilancia/Libros/CBDC%20march2022.pdf>



transactions. Instead, it argues that the ePeso would be complementary to existing methods for larger transactions, functioning in the same market space as physical cash does today.<sup>25</sup> This is further reflected in the limits the BCU states would be placed on CBDC holdings, underlining that the e-Peso is not envisaged to remove the need for private digital money.

```
10011110010111100011110001011011000111101100001
00110001111100100100011101101110011110010001100
10111001111000001111001110011110001111001001100
0111110000011110000000011111010011110001111101
11101110000010010011110000011010111111010011110
```



```
010001100110000001100000000011101111111110000
00001110011110011011100111001110100000110010011
11111000011001101110000110100111001111110110010
00110011110011011010011001001110100110001001001
00111011100011100010100110011100011000011000011
```

25 Seven Lessons From The E-Peso Pilot Plan, Banco Central del Uruguay, March 2022, <https://www.bcu.gub.uy/Sistema-de-Pagos/Documents/Vigilancia/Libros/CBDC%20march2022.pdf>

## E-krona Sweden

Stage: Pilot

### Summary

- A central username database **linked to alphanumeric wallet IDs**
- Privacy protections in law would be on a par with retail banks, and **offer less privacy** than cash
- Token transactions would be **traceable** on the ledger
- Riksbank is examining the possibility of using the e-krona to facilitate **“conditional payments”**

The Riksbank, the central bank of Sweden, has been piloting a CBDC called the e-krona since 2020. In 2023, the central bank is focused on testing the technical side of the e-krona platform before a conducting wider pilot. It is also investigating the potential impacts on the economy, end users and businesses.<sup>26</sup> How any future and final e-krona may look is subject to change - this analysis is based on publications from the Riksbank that outline the central bank’s current thinking.

### Design

During the pilot, the e-krona has been based on the Corda distributed ledger system [similar to a blockchain]. Corda is an open-source blockchain technology, which differs from other DLTs in that it settles transactions instantly, rather than waiting for other transactions to complete a “block” which is then signed with a hash – as happens with Bitcoin. Unlike many other DLTs, access to information stored on the ledger is permissioned rather than being available to anyone viewing it. Data is shared on a “need to know” basis, for example, between parties in a transaction. Although it is not as open as the Bitcoin ledger, the Riksbank and Swedish authorities could access information from the e-krona DLT if required.<sup>27</sup>

As distributed ledgers generally use complex alphanumeric strings as identifiers for particular wallets, Riksbank has developed a username-based system [“aliases”] to allow users to easily identify one another. For example, Winston Smith could choose the unique alias “Wsmith84” that others could use to find him on the CBDC platform, rather than sharing a long alphanumeric string. A transaction will then see the platform search for an

26 E-Krona, Riksbank, accessed 8th August 2023, <https://www.riksbank.se/en-gb/payments--cash/e-krona/>

27 E-Krona Pilot Phase 2, Riksbank, April 2022, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2022/e-krona-pilot-phase-2.pdf>

alias, which will in turn identify the correct unique wallet ID [alphanumeric string] to send the money to. A lookup table where usernames are matched to wallet IDs is stored in a central database.<sup>28</sup>

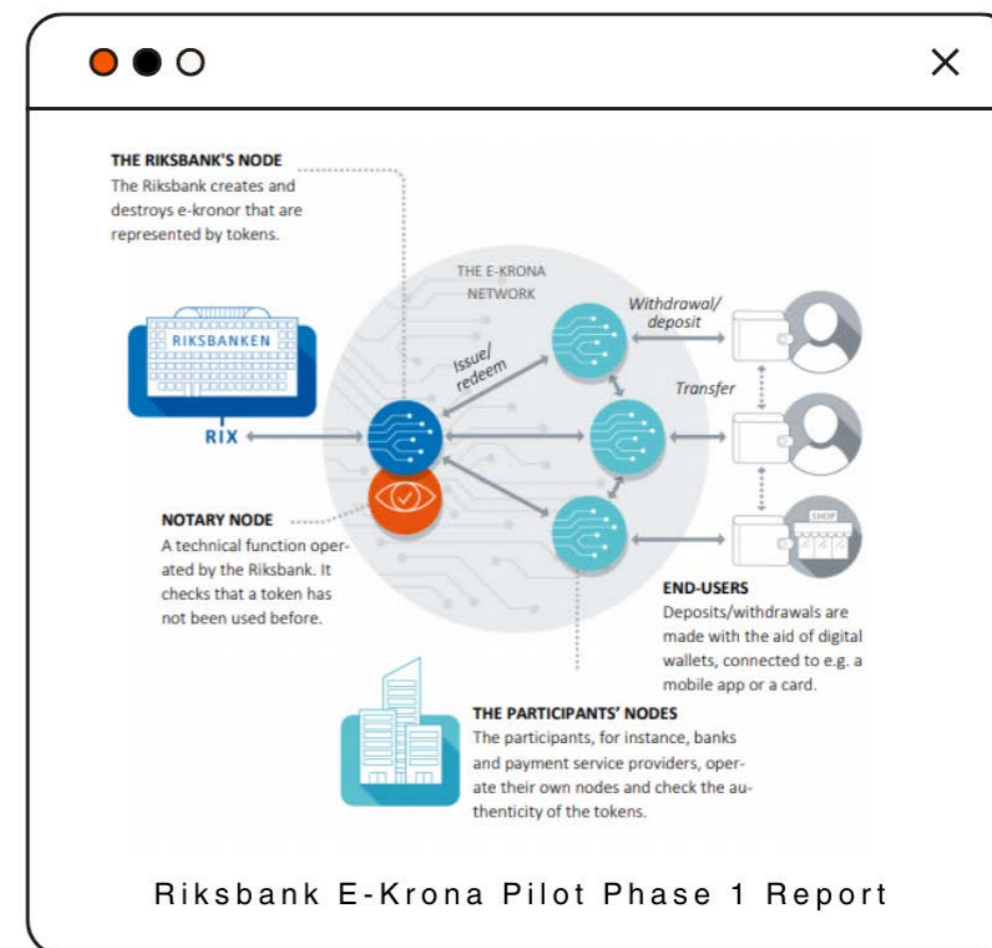
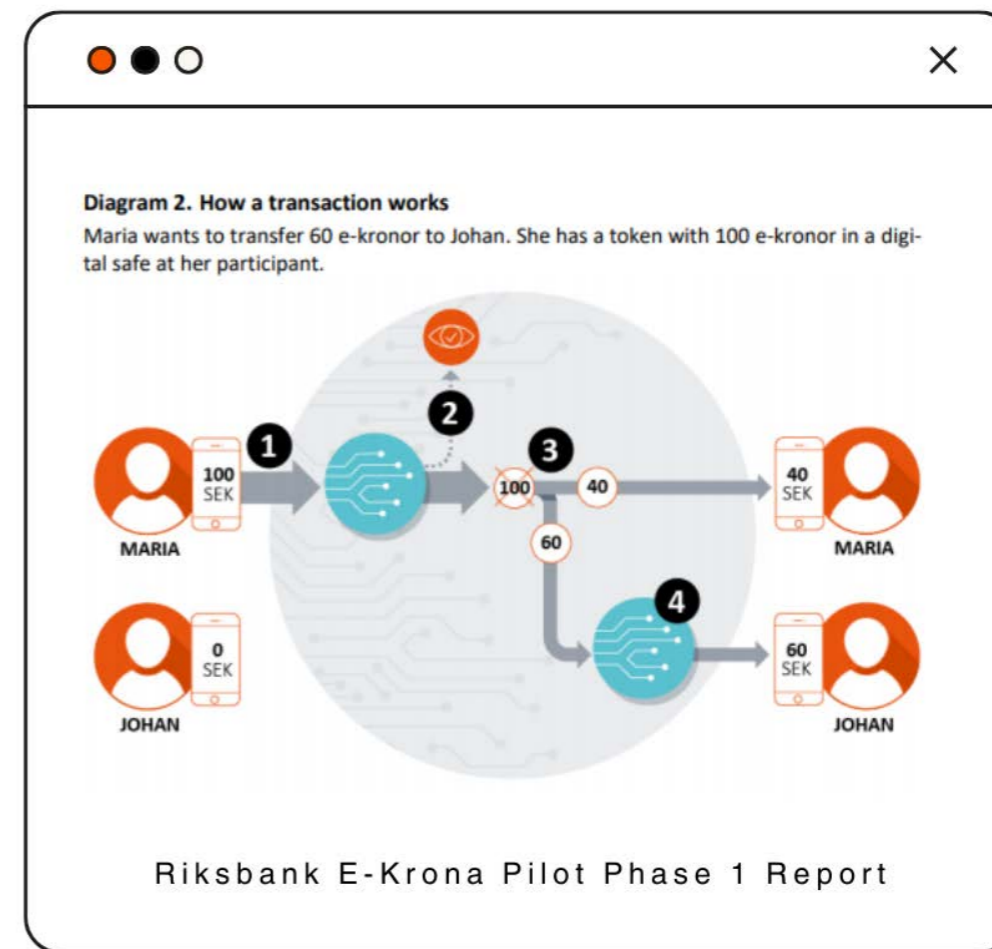
Sweden’s pilot CBDC is token-based, meaning each e-krona is seen as a digital unit of value akin to a note or a coin, although users see their holdings as a balance similar to a bank account balance rather than a pile of virtual coins or notes, and the tokens are not limited to pre-determined denominations.<sup>29</sup>

The e-krona tokens are single-use and are destroyed in the process of a transaction taking place. In a given transaction a token or tokens of equal or superior value to the relevant amount are sent to a validation “node” in the network, which authenticates that the token has not been previously used. Simultaneously the original token is destroyed and a new token of the relevant value is generated for the recipient, and if required a second new one for any change to be returned to the payer.<sup>30</sup>

Riksbank has trialed several wallet models for the e-krona, looking at local storage, which would allow for some offline functionality and network storage for the CBDC tokens. The central bank outlined offline payments as being treated as effectively pending, although balances would update, until the mobile phone is linked to the relevant wallets connected to the internet to communicate with the validation nodes in the network and settle the transaction. There is also the potential for the technology to allow offline transactions to be chained, effectively allowing A to pay B offline, and for B to then pay C.

However, Riksbank expressed concern about the greater risk of fraud in offline transactions and suggested limits on transaction size and the number of offline payments to mitigate this. The e-krona is also designed to integrate with point of sale [card payment] terminals, either to allow the Riksbank to introduce e-krona cards or for NFC communication between a mobile phone and the terminal to effect a transaction.<sup>31</sup>

28 E-Krona Pilot Phase 2, Riksbank, April 2022, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2022/e-krona-pilot-phase-2.pdf>  
 29 E-Krona Pilot Phase 3, Riksbank, April 2023, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2023/e-krona-pilot-phase-3.pdf>  
 30 E-Krona Pilot Phase 1, Riksbank, April 2021 <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2021/e-krona-pilot-phase-1.pdf>  
 31 E-Krona Pilot Phase 1, Riksbank, April 2021 <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2021/e-krona-pilot-phase-1.pdf>



Transactions are processed through a series of nodes which ultimately communicate with the distributed ledger to record them. End users's wallets, or nodes, communicate with "participant" nodes which authenticate the legitimacy of e-krona tokens. The participant nodes are run by private institutions, such as banks, who provide the wallets – these in turn communicate with the central bank-run notary nodes which verify that a token has not been used before, legitimising the transaction.<sup>3233</sup>

### Motivations

The Riksbank offers several different reasons for its decision to pilot the e-krona.<sup>34</sup>

The first is to "preserve several functions of cash" when physical money is only used infrequently and ceases to be a useful monetary anchor. Cash acts as a guarantee that every krona deposited in the bank is worth the same no matter where it is stored, as banks promise to always convert bank deposits [a form of private money] into cash, which is universally accepted. If cash becomes less used it could fail to be useful as a monetary anchor and the Riksbank claims that it sees a CBDC as a tool to maintain the monetary system.

Cash is losing popularity in Sweden, making up around only ten per cent of all payments, and the Riksbank acknowledges Sweden is a unique example internationally with the low levels of cash use in the country's payment mix. Riksbank argues that if cash, as the only form of legal tender, were to disappear from use the central bank would be expected to act – but the manner is left open to question.<sup>35</sup>

The initial concept of the e-krona, first developed in 2017, envisaged the CBDC primarily being a tool for smaller payments and not replacing existing methods for larger financial transfers. Like cash, it explicitly will not accrue interest, unlike bank deposits.<sup>36</sup>

A central bank-backed digital money system could also act as an alternative to private digital payment networks and strengthen resilience in this field. Riksbank argues that it is necessary to have several forms of digital payment in case of technical disruptions, while a CBDC infrastructure could allow for innovation in digital payments.<sup>37</sup>

32 E-Krona Pilot Phase 1, Riksbank, April 2021 <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2021/e-krona-pilot-phase-1.pdf>

33 E-Krona Pilot Phase 2, Riksbank, April 2022, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2022/e-krona-pilot-phase-2.pdf>

34 E-Krona Project Report 2, Riksbank, October 2018. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>

35 E-Krona Pilot Phase 2, Riksbank, April 2022, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2022/e-krona-pilot-phase-2.pdf>

36 E-Krona Project Report 1, Riksbank, September 2017. [https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport\\_ekrona\\_uppdaterad\\_170920\\_eng.pdf](https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf)

37 E-Krona Pilot Phase 2, Riksbank, April 2022, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2022/e-krona-pilot-phase-2.pdf>

### Privacy, Anonymity and Traceability

Riksbank acknowledges that the e-krona would have to meet the standards for banking privacy under Sweden's Payment Services Act, which applies to all other forms of electronic payments. However, this privacy requirement is not as effective as the potential anonymity granted by paying in cash and the discussion of ensuring financial confidentiality must be understood in this context. These requirements operate in tandem with general Swedish data protection regulations.<sup>38</sup>

How financial privacy laws would interact with the novel technology of a CBDC in Sweden is "unclear" according to the Riksbank. It does acknowledge that transactions and related data would likely be covered by the regulations, but suggests that new laws would be required to clarify the situation if the e-krona were rolled out fully.

Riksbank contrasts the data collection preferences of a state-run digital currency with that of a private digital payments network, with the central bank arguing that private providers would seek to collect data for marketing purposes whereas it would not.<sup>39</sup>

As e-krona only transacts via unique, identifiable tokens that move through nodes in the network, the Swedish CBDC is ultimately traceable, with the bank admitting that "all electronic payments leave traces".<sup>40</sup> Riksbank raises the question of how traceability, particularly in the context of DLT where even anonymous transactions are traceable [see Bitcoin], can be reconciled with financial confidentiality requirements.

Anonymous payments will only be permitted to a limited extent and will be bound by Swedish money-laundering regulations, presumably in a similar way to other transactions. It is unclear whether accounts will be anonymous at all, as know-your-customer regulations may apply, regardless of whether transactions below a certain limit will be anonymous or not.<sup>41</sup>

It was suggested that anonymous accounts could work similarly to pre-paid debit cards with customers "buying" an e-krona account at a retailer. However, it would likely come with limits on incomings and outgoings, which would necessarily limit the utility of any anonymous e-krona accounts that were offered.<sup>42</sup>

38 E-Krona Pilot Phase 2, Riksbank, April 2022, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2022/e-krona-pilot-phase-2.pdf>

39 E-Krona Design Models: Pros, Cons and Trade-Offs, Economic Review 2 2020, Riksbank, 18th June 2020, <https://www.riksbank.se/globalassets/media/rapporter/pov/engelska/2020/economic-re-view-2-2020.pdf>

40 E-krona design models: pros, cons and trade-offs. Economic Review 2 2020, Riksbank, 18th June 2020, <https://www.riksbank.se/globalassets/media/rapporter/pov/engelska/2020/economic-re-view-2-2020.pdf>

41 E-Krona Pilot Phase 1, Riksbank, April 2021 <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2021/e-krona-pilot-phase-1.pdf>

42 E-Krona Pilot Phase 2, Riksbank, April 2022, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2022/e-krona-pilot-phase-2.pdf>



## Programmability

The Riksbank is examining how the e-krona could be programmable and used in smart contracts. However, the central bank claims that it is interested in conditional payments [similar to escrow] rather than conditional money [only programming the e-krona for use in certain circumstances]. Riksbank acknowledges that is a necessary property of money as an asset class to be useable for payment no matter the context.<sup>43</sup>

It argues that it does not intend to control or limit the use of a potential e-krona as it would undermine the CBDC's function as a form of money, and is a threat to individual privacy.

Instead, it outlines potential programmability as a way of allowing people to set up conditional payments, where transactions are executed in certain circumstances. An example given by the bank involves the purchase of a car:<sup>44</sup>

1. A buyer and a seller agree on a deal, in this case for a car at a certain price. They look for a "technical solution" for them to complete the deal if the other side holds up the bargain.
  - a) In this example, it is the transfer of funds when the car is registered in the buyer's name. Today, escrow may be used for this but requires third-party involvement.
2. Using the e-krona platform a smart contract can be created, allocating specific tokens to the transaction and holding them until the condition [transfer of car ownership] is met.
  - a) The platform is supposed to give confidence to the buyer that funds will only be sent when the car is theirs, while the seller is sure they will receive the money once the car is transferred.
3. As the condition of the car ownership transfer is an external condition, there must be a way to validate this being met on the DLT platform.
  - a) Riksbank proposes including an "Oracle" node operated by a trusted third party which verifies the condition is met.
4. Once conditions have been certified, i.e. the car is verified to have been registered in the buyer's name, the money is unlocked and sent to the car dealer.
  - a) If any time limit expires for the conditions to be met the funds are re-released to the buyer.

<sup>43</sup> E-Krona Pilot Phase 3, Riksbank, April 2023, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2023/e-krona-pilot-phase-3.pdf>

<sup>44</sup> E-Krona Pilot Phase 3, Riksbank, April 2023, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2023/e-krona-pilot-phase-3.pdf>

```
10011110010111100011110001011011000111101100001
00110001111100100100011101101110011110010001100
10111001111000001111001110011110001111001001100
01111100000111100000000111111010011110001111101
11101110000010010011110000011010111111010011110
```



```
0100011001100000011000000000111011111111110000
00001110011110011011100111001110100000110010011
11111000011001101110000110100111001111110110010
00110011110011011010011001001110100110001001001
00111011100011100010100110011100011000011000011
```

It would require significant data far beyond the payer, payee and amount to be processed and potentially recorded by the distributed ledger to make these more complex or conditional transactions possible. External data sources would have to feed into the CBDC platform to provide information about other smart contracts, which in turn would make transaction records much more detailed than even a credit card statement.



### Problems identified by the Riksbank

Swedish central bankers acknowledge that many people who prefer physical cash would prefer to do so over a CBDC if cash remained available. The digital nature of a CBDC also makes it less likely to address the problems some groups may face as cash use declines.<sup>45</sup>In particular the bank sees the digital infrastructure as being a barrier to some elderly people, and disabled people who already experience problems using non-cash, digital payment methods. As Sweden already has a significant age divide in its payment mix, with older people relying on cash, there are questions as to whether a CBDC would address the digital divide.

Riksbank states that the more complicated potential use cases for the e-krona should be developed separately from the core use case of a digital currency.<sup>46</sup> It views any future CBDC as primarily as access to digital cash rather than the additional use cases and suggests that the private sector rather than the bank could develop the advanced tools.<sup>47</sup> However, this comes with the risk of private sector control over aspects of digital money - the very issue a CBDC is allegedly designed to avoid.

45 E-Krona Pilot Phase 2, Riksbank, April 2022, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2022/e-krona-pilot-phase-2.pdf>

46 E-Krona Pilot Phase 3, Riksbank, April 2023, <https://www.riksbank.se/globalassets/media/rapport-er/e-krona/2023/e-krona-pilot-phase-3.pdf>

47 Ibid

## Digital Shekel Israel

Stage: Proof of Concept

### Summary

- Smart contracts and **programmable payments** could be added to the CBDC design at a later date
- The digital shekel aspires to facilitate the state's **tax collection**
- It supports laws already in place to **cap cash purchases and transactions** between individuals
- Privacy is explicitly **not a priority**

Israel's central bank has been looking at the role a digital currency could play in the nation's economy since 2017. A November 2018 report recommended against the introduction of an Israeli digital currency but advised the Bank of Israel to maintain a watching brief on the issue. Shifting payment patterns, exacerbated by the Covid-19 pandemic, have renewed Israeli interest in a CBDC – the digital shekel.<sup>48</sup>

The Bank of Israel [BOI] has conducted public consultations and is undertaking work to develop a potential future digital shekel but has laid out certain conditions which will influence a decision as to whether an Israeli CBDC is introduced:<sup>49</sup>

- Other countries issuing a CBDC, particularly in Europe or the US
- A faster-than-expected reduction in the legitimate acceptance and use of cash in Israel, undermining the role of cash as public money-laundering
- Stablecoins or other private payment methods becoming widely adopted in Israel
- A lack of competition in the domestic payment system
- Technology changes that make a CBDC more justifiable

### Model

In the proof of concept documents, the BOI assumes any CBDC would be a two-tier model, with the central bank issuing and regulating the digital currency while regulated private sector organisations [e.g. banks, finance companies] provide the public interface and operating wallets.<sup>50</sup>

48 Report Of The Team To Examine The Issue Of Central Bank Digital Currencies, Bank of Israel, November 2018, <https://www.boi.org.il/media/vqtkntna/digital-currency.pdf>

49 Potential Scenarios for Deciding to Issue a Digital Shekel, Bank of Israel, April 2023, <https://www.boi.org.il/media/j40nvorg/april-2023-potential-scenarios-for-deciding-to-issue-a-digital-shekel.pdf>

50 A Bank of Israel Digital Shekel: Potential Benefits, Draft Model, and Issues to Examine, Bank of Israel,

The general public [individuals and businesses] would interact with the digital shekel system through these third parties. These organisations would be responsible for KYC checks and compliance with AML/CTF rules. The providers would not be exposed financially, like they are when lending out deposits, with the digital shekels directly held by customers rather than being treated akin to a deposit which could be a source of lending liquidity.

How identity checks would be conducted, and the levels of verification required, has not yet been laid out. The proof of concept only used BOI employees and sought to establish the technical infrastructure, so used internal systems to identify users. The bank did not lay out how checks or identification may impact a future wider digital currency rollout.

It is unclear whether the CBDC would be token or account based. In experiments the BOI has used tokens to represent the digital shekel, which gives some insight into its thinking, but the bank has not decided on the final structure of any future digital currency.<sup>51</sup> The bank appears to be leaning towards a blockchain/DLT basis for the future digital shekel – a platform it trialled as a proof of concept in 2022. It also suggests that advanced options such as smart contracts, programmable payments and micropayments will be developed by the private providers at a future date, with the bank focussing on the core CBDC product.<sup>52</sup> These advanced features appear to be viewed by the BOI as add-ons rather than necessary features.<sup>53</sup>

Offline payments will be developed; however, they will be limited to protect against double-spending or counterfeiting. Facilitating digital payments without an internet connection is seen as one of the key technological challenges for any digital currency and the BOI recognises offline payments as a necessary feature.

### *Justifications*

There are several reasons the BOI says it might choose to introduce a digital shekel. They include maintaining access to public money in a digitised economy, creating infrastructure for efficient cross-border payments, and providing secondary payment infrastructure to support any issues with private payment networks. Some of the reasons given underline the privacy and civil liberties dangers a CBDC may pose:<sup>54</sup>

51 May 2021, <https://www.boi.org.il/media/pscnnurd/2021-5-a-bank-of-israel-digital-shekel.pdf>

52 Experiment on a Distributed Platform, Bank of Israel, June 2022, <https://www.boi.org.il/media/10kj4j2c/experiment-on-a-distributed-platform.pdf>

53 Experiment on a Distributed Platform, Bank of Israel, June 2022, <https://www.boi.org.il/media/10kj4j2c/experiment-on-a-distributed-platform.pdf>

54 A Bank of Israel Digital Shekel: Potential Benefits, Draft Model, and Issues to Examine, Bank of Israel, May 2021, <https://www.boi.org.il/media/pscnnurd/2021-5-a-bank-of-israel-digital-shekel.pdf>

55 Experiment on a Distributed Platform, Bank of Israel, June 2022, <https://www.boi.org.il/media/10kj4j2c/experiment-on-a-distributed-platform.pdf>

- “Maintaining the public’s ability to use digital means of payment while ensuring a certain level of privacy” – the BoI acknowledges that AML, CTF and tax reporting rules applied to other digital payment schemes would apply to the digital shekel. It would only maintain some of the characteristics of cash, and privacy would be balanced rather than default.
- “Creating an innovative technology that will ensure the adaptation of the payment system to the needs of the future digital economy” – this includes programmable or conditional payments, which may be limited to escrow-style services but come with greater risk of state control over how people spend their money.
- “Support of government policy to reduce the use of cash in the struggle against the “shadow economy”” – cash is key to illicit parts of the economy and many governments seek to regulate cash use to undermine the black market. However, the use of a digital currency explicitly as a means of controlling the economy highlights the CBDC’s potential for increasing state surveillance, control and thus power.

Declining cash use in Israel is cited as a key reason for the CBDC to be considered, with card payments on a sharp upward trend, rising from 55 per cent of private consumption in 2016 to 68 per cent in 2020. The BOI argues that this decline means that it should monitor the use and acceptance of cash over a period of time, in order to assess how it might act in a situation when physical money appears to be falling out of use.<sup>55</sup>

The BOI views a CBDC as a potential way to address the issues faced by the unbanked as a digital shekel would be available to those without internet access or a bank account. However, these people would face a lower level of privacy than they presently enjoy with cash payments. There are also digital illiteracy issues which the bank has not addressed. Financial inclusion appears to only be a secondary goal for the bank – and Israel already has laws in place giving every citizen the right to a basic bank account, unlike other countries. This means that a digital shekel may not further increase accessibility to banking, if it required bank-level identity checks.<sup>56</sup>

### *Privacy*

Any Israeli CBDC will be “designed in concert with money laundering and terrorism financing prohibition [AML-CTF] rules” says the central bank. It will also be designed to facilitate tax collection and the BOI admits “absolute privacy will not be possible”, but a degree of privacy will remain in relation to private companies involved in the digital

55 Ibid.

56 A Bank of Israel Digital Shekel: Potential Benefits, Draft Model, and Issues to Examine, Bank of Israel, May 2021, <https://www.boi.org.il/media/pscnnurd/2021-5-a-bank-of-israel-digital-shekel.pdf>

shekel network.<sup>57</sup> The bank acknowledges that privacy is a virtue of cash payments for some people. However, it places significant emphasis on any privacy protections for a future CBDC being limited to small transactions and stresses the applicability of AML/CTF controls.<sup>58</sup>

The BOI does not give special value to privacy, instead stating it is only a single consideration alongside the wider good of the economy and the bank's general goals. It is explicit in stating that "it will not be possible to enable the absolute privacy of the payer or receiver" unlike with cash payments.<sup>59</sup> This is strong evidence that an Israeli CBDC would be damaging to privacy when compared with cash, and that the BOI would not seek to create a privacy-first digital currency.<sup>60</sup>

Israel already has strict laws that limit how cash can be used, namely the "Reduction of Use of Cash Law". Payments to businesses in cash are capped at 6000 Israeli new shekels [NIS] [c.£1,260]. Private citizens can exchange up to 15,000 [c.£3,160] NIS in cash between them.<sup>61</sup> Above these limits, transactions must be made using alternative methods, such as debit/credit card or online transfers. The country's tax authority is explicit in its goal to reduce the public's use of cash. It claims that it will undermine organised crime – but there remain more than a million Israelis without a bank account.<sup>62</sup>

Privacy protections will be customisable, with the BOI envisaging payment providers being able to offer customers additional services in exchange for access to their transaction information – raising the spectre of privacy being a tradable asset, which is concerning. Power imbalances between major institutions and customers could be exacerbated and lead to unnecessary data transfers – with alleged consents hidden in lengthy privacy documentation.<sup>63</sup>

There is also the reality that "bans" on high-value cash transactions will not impact organised criminals who by definition exist to break the law. A group that engages in drug trafficking will have little problem in using cash above the legal limit and the bank acknowledges that, unless cash ceases to exist, criminal groups will continue to use it, lawfully or not.

In its 2022 proof of concept, the BOI developed the idea of ordinary and private digital

57 A Bank of Israel Digital Shekel: Potential Benefits, Draft Model, and Issues to Examine, Bank of Israel, May 2021, <https://www.boi.org.il/media/pscnnurd/2021-5-a-bank-of-israel-digital-shekel.pdf>

58 A Bank of Israel Digital Shekel: Potential Benefits, Draft Model, and Issues to Examine, Bank of Israel, May 2021, <https://www.boi.org.il/media/pscnnurd/2021-5-a-bank-of-israel-digital-shekel.pdf>

59 Ibid

60 Ibid

61 Israel Bans Use Of Cash For Purchases Larger Than NIS 6,000, The Jerusalem Post, 28th July 2022, <https://www.jpost.com/business-and-innovation/banking-and-finance/article-713354>

62 A Bank of Israel Digital Shekel: Potential Benefits, Draft Model, and Issues to Examine, Bank of Israel, May 2021, <https://www.boi.org.il/media/pscnnurd/2021-5-a-bank-of-israel-digital-shekel.pdf>

63 A Bank of Israel Digital Shekel: Potential Benefits, Draft Model, and Issues to Examine, Bank of Israel, May 2021, <https://www.boi.org.il/media/pscnnurd/2021-5-a-bank-of-israel-digital-shekel.pdf>

shekels, with the latter not recorded openly on the blockchain. Policymakers can then set a "budget" for given periods where people can make private payments that are not recorded. The BOI suggested a 1,000 private shekel [£210] limit before transactions are recorded on the distributed ledger.<sup>64</sup>

A zero-knowledge proof was tested to maintain the privacy of the private digital shekels in the proof of concept, which if executed correctly would offer significant reassurance about the level of privacy with the private digital currency. However, the availability of these private tokens to users would still be in the gift of the central bank or the Israeli authorities. As an example of conditional privacy as a feature, rather than by design, it is plausible that the private digital shekels could have certain requirements or be at the whim of the authorities in a way that privacy-by-design would not.

### *Programmability*

The proof of concept imagined smart contract-style programmability acting like escrow payments. This is very similar to the approach outlined by the Riksbank [see page 13]. There is little other mention of programmability in the BOI's documents, which may be in part due to the bank's intention for third parties to develop advanced features rather than the central bank.<sup>65</sup>

Smart contracts themselves come with some risks, the BOI admits, as poor drafting in terms or code could undermine transactions or the system as a whole. It therefore sees the ability to draft smart contracts as being restricted to trusted providers, and even then under strict supervision.

### *CBDC Risks*

The BOI admits there are several risks posed by a potential CBDC, from privacy and civil liberties to economics.

As with other central banks, the potential of a CBDC to draw down bank deposits and thus liquidity in the private banking system is outlined as a serious danger. The ability of quick transfers from bank accounts to a digital shekel, much faster than a traditional bank withdrawal, makes the danger posed by any bank run much more serious and could lead to accelerating economic crises.<sup>66</sup>

64 Experiment on a Distributed Platform, Bank of Israel, June 2022, <https://www.boi.org.il/media/10kj4j2c/experiment-on-a-distributed-platform.pdf>

65 Experiment on a Distributed Platform, Bank of Israel, June 2022, <https://www.boi.org.il/media/10kj4j2c/experiment-on-a-distributed-platform.pdf>

66 Report Of The Team To Examine The Issue Of Central Bank Digital Currencies, Bank of Israel, November 2018, <https://www.boi.org.il/media/vqtkntna/digital-currency.pdf>

These risks are a major reason for the BOI considering limitations on holdings or use levels of the digital shekel. Different account types could have different limits and the bank claims that it will primarily aim to maintain private banking sector liquidity through these limits – by ensuring that money is not held in the CBDC system to the detriment of bank balance sheets. Restrictions on transfer amounts and frequency were tested in the 2022 proof of concept as a way of ensuring that a CBDC would not result in capital flight from retail banks.<sup>67</sup>

There are also questions over a digital shekel's necessity. The existence of faster digital payments systems already in operation in Israel led the BOI to question whether a CBDC is necessary as the two systems would operate in similar spaces.

67 Experiment on a Distributed Platform, Bank of Israel, June 2022, <https://www.boi.org.il/media/10kj4j2c/experiment-on-a-distributed-platform.pdf>

## eNaira Nigeria

Stage: Full rollout

### Summary

- Tiered holding and transaction limits on wallets according to ID status, ranging from a phone number to biometrically verified national insurance number
- central bank access to identity and transaction data
- Inadequate explicit privacy protections with experts doubting the enforcement of data rights laws
- There are plans to require tuition fee payments to be made in eNaira, and to pay government officials in the CBDC
- 6 per cent of the population has an eNaira wallet, but 98 per cent of wallets have never been used

Nigeria is one of the biggest countries to have rolled out its CBDC, the eNaira, for general use. The African country went live with its digital currency in September 2022 following a pilot in late 2021 and early 2022.<sup>68</sup> However, the full rollout of the eNaira is widely viewed as a failure with low uptake among Nigerians.<sup>69</sup>

### Motivations

The Central Bank of Nigeria (CBN) sees facilitating an increase in the use of digital payment methods at the expense of cash use as a positive goal it is working toward, mostly as a means to address its wider economic objectives.<sup>70</sup> Since January 2012, the CBN has had a “cash-less” policy with the aims of “modernising Nigeria’s payment systems”, providing “more efficient payment options”, and making monetary policy a more effective tool in impacting inflation and the economy generally.<sup>71</sup> The main aim for this policy was described as cutting the number of notes and coins handled by businesses without completely phasing cash out.<sup>72</sup> Daily limits on cash deposits for individuals and businesses, withdrawal fees for cash and campaigns to promote alternative payment

68 Overview, eNaira, Central Bank of Nigeria, accessed 8th August 2023, <https://enaira.gov.ng/about/overview>

69 Nigeria’s eNaira CBDC: What Went Wrong, Pratham Rawat, Cornell SC Johnson College of Business, 28th April 2023, <https://business.cornell.edu/hub/2023/04/28/nigerias-enaira-cbdc-what-went-wrong/>

70 Cash-less Nigeria, Central Bank of Nigeria, accessed 8th August 2023, <https://www.cbn.gov.ng/cashless/>

71 Design Paper For The eNaira, Central Bank of Nigeria, 1st October 2021, [https://enaira.gov.ng/assets/download/eNaira\\_Design\\_Paper.pdf](https://enaira.gov.ng/assets/download/eNaira_Design_Paper.pdf)

72 Cash-less FAQs, Central Bank of Nigeria, accessed 2nd October 2023, <https://www.cbn.gov.ng/cashless/Cash-Less%20FAQs.pdf>



methods are three of the main poles of the cash-less policy.

It cites a number of alleged harms due to the large role cash plays in the Nigerian economy as justification for policies to reduce cash use. These include the high cost of cash handling and the risks of cash handling. There are also claims that a high cash share of the payment mix facilitates corruption, fraud and money laundering, and buttresses the informal economy which the CBN struggles to influence with monetary policy.<sup>73</sup> As part of the “cash-less” policy the CBN has introduced limits on cash transactions through Nigerian bank accounts, and charges to discourage the use of physical cash over other payment means.

The CBN also has a complementary aim of its CBDC rollout of enabling 95 per cent of Nigerians to access financial and banking services by 2024, up from 36 per cent in 2010 – encouraging new financial firms to enter the market at the same time. The CBN also introduced unique Bank Verification Numbers for customers [BVNs] in 2014 to standardise identification processes and KYC in the country’s financial sector. BVNs are now the main way KYC checks are performed in the Nigerian financial system.<sup>74</sup>

The eNaira is viewed by the CBN as a key part of Nigeria’s future digital payments system, which can facilitate greater financial inclusion and offer several opportunities:<sup>75</sup>

- Enabling direct welfare and support payments to individuals, and perhaps businesses
  - The CBN suggests that a CBDC would make it easier for the government to make direct transfers which reach the correct people quickly.
- Facilitate remittances from the Nigerian diaspora and make cross-border transactions quicker and cheaper
  - Remittances are an important source of foreign currency for Nigeria and a CBDC may make paying them easier, while it may also reduce the cost and friction involved in cross-border payments.

#### Model

The eNaira is based on blockchain/distributed ledger technology maintained by the CBN. As with other DLT-based CBDCs, the ledger is private, meaning that only central-bank-approved nodes can add transactions to the blockchain and validate them.<sup>76</sup> Initial design

<sup>73</sup> Cash-less Nigeria, Central Bank of Nigeria, accessed 8th August 2023, <https://www.cbn.gov.ng/cashless/>

<sup>74</sup> Design Paper For The eNaira, Central Bank of Nigeria, 1st October 2021, [https://enaira.gov.ng/assets/download/eNaira\\_Design\\_Paper.pdf](https://enaira.gov.ng/assets/download/eNaira_Design_Paper.pdf)

<sup>75</sup> Ibid

<sup>76</sup> Design Paper For The eNaira, Central Bank of Nigeria, 1st October 2021, [https://enaira.gov.ng/assets/download/eNaira\\_Design\\_Paper.pdf](https://enaira.gov.ng/assets/download/eNaira_Design_Paper.pdf)

proposals for the currency suggested that private institutions would have a significant role in offering wallets to retail customers; however, at the time of writing, the CBN-developed Speed Wallet appears to be the only major digital wallet on offer.<sup>77</sup>

Private institutions, such as banks and mobile payment providers, have a role in converting the eNaira to private digital money or cash, as they process transactions “topping-up” accounts as intermediaries [akin to buying Bitcoin with a bank card] or moving the digital currency to other forms of money.

It is an account-based CBDC, meaning that ‘balances’ will be displayed in wallets but they will not be represented by discrete tokens within the eNaira network. The accounts are tied to identities, which are based on identifiers including telephone numbers, bank identification numbers or Nigeria’s national identity number. The CBN views the tying of wallets to identities as key to a “robust KYC framework”.<sup>78</sup>

Depending on the level of verification associated with each account, individual customers’s wallets have different limits on daily transactions and total balances. Having a telephone number is necessary both to verify a bank account and obtain a national identity number [NIN]. Corporate accounts will have no limit.<sup>79</sup>

| Tier | Category                 | Requirement   | Daily Transaction Limit [NGN] | Daily Cumulative Balance [NGN] |
|------|--------------------------|---|-------------------------------|--------------------------------|
| 0    | Non-bank account holders | Telephone number, National Identity Number [NIN] not verified   | 20,000 [c.£20]                | 120,000 [c.£120]               |
| 1    | Non-bank account holders | Telephone number, NIN verified  | 50,000 [c.£50]                | 300,000 [c.£300]               |
| 2    | Bank account holders     | Bank Verification Number, some personal details verified against official databases.                                | 200,000 [c.£200]              | 500,000 [c.£500]               |
| 3    | Bank account holders     | Bank Verification Number, full identity information verified to comply with AML/CTF rules, risk based verification. | 500,000 [c.£500]              | 5,000,000 [c.£5,000]           |

Access to eNaira accounts that are able to spend or hold significant amounts of currency are limited to those who provide significant amounts of personal information and verify it. The consequence of this policy will be to limit those without bank accounts to a low level of financial transactions, which risks undermining the aim of an eNaira to promote

<sup>77</sup> Speed Wallet, Central Bank of Nigeria, accessed 8th August 2023, <https://enaira.gov.ng/about/new-features>

<sup>78</sup> Design Paper For The eNaira, Central Bank of Nigeria, 1st October 2021, [https://enaira.gov.ng/assets/download/eNaira\\_Design\\_Paper.pdf](https://enaira.gov.ng/assets/download/eNaira_Design_Paper.pdf)

<sup>79</sup> Nigeria’s eNaira, One Year After, WP/23/104, Jookyung Ree, International Monetary Fund, May 2022

financial inclusion. That a CBDC could lead to further financial exclusion is a risk the CBN acknowledges, particularly with the internet and digital focus of the eNaira, but the bank claims that it will factor in inclusiveness as a design principle without offering much detail.

### Privacy

Users on the eNaira platform are identifiable through their NIN and BVNs. The CBN partially justifies this as a way to have the eNaira comply with counter-terror financing and anti-money laundering regulations.<sup>80</sup> However, it is not only the central bank which will be able to identify customers – private financial institutions offering additional services on the eNaira network will still conduct their own KYC checks to comply with financial regulations.

The eNaira design paper claims data protection and privacy are fundamental to the CBDC architecture. It does not lay out in any detail what protections are offered to consumers. It dedicates only two paragraphs to the issue of data protection, which indicates that it was not one of the more pressing issues addressed by the CBN in its push to introduce a digital currency.

Account-based CBDCs like the eNaira are unable to offer the same level of privacy that is technically available with a token-based architecture, even if central banks do not take advantage of this confidentiality.<sup>81</sup> This is because account-based models necessarily keep records of how specified accounts transact with each other in a way that anonymised tokens could potentially avoid. There are concerns that the CBN and intermediaries will be able to easily see identity, transaction and other related data.

KYC requirements pose a further risk to privacy, with even Tier 0 unverified accounts requiring a photo, name, date of birth and an address as part of the setup, meaning that wholly anonymous eNaira accounts are impossible. Accounts with greater limits are subject to high levels of verification.

Bank verification numbers [BVNs] are unique identifiers issued to Nigerians which act as an ID number throughout the financial system.<sup>82</sup> The BVN is a biometric identification system and the numbers are linked to fingerprints or facial biometrics of the user, effectively meaning that those wanting to access more capable eNaira wallets are required to submit to biometric data processing in order to do so.

80 Design Paper For The eNaira, Central Bank of Nigeria, 1st October 2021, [https://enaira.gov.ng/assets/download/eNaira\\_Design\\_Paper.pdf](https://enaira.gov.ng/assets/download/eNaira_Design_Paper.pdf)

81 Nigeria's Central Bank Digital Currency Is 'Same Naira, More Possibilities' – If You Count Government Snooping, Dr Kemi Omotubora and Dr Subhajit Basu, The Register, 22nd November 2021, [https://www.theregister.com/2021/11/22/e\\_naira\\_legal\\_privacy/](https://www.theregister.com/2021/11/22/e_naira_legal_privacy/)

82 Bank Verification Number (BVN), Guaranty Trust Bank, accessed 8th August 2023, <https://www.gtbank.com/bvn>

Nigeria's National Identity Number [NIN] is a compulsory biometric identity scheme, requiring fingerprints alongside a photo and a large amount of personal information.<sup>83</sup> Anything but the most basic wallet tier with the eNaira requires Nigerians to link their identity clearly and explicitly to the wallet, making it simple for the authorities to link spending to a specific individual.

Even Tier 0 of eNaira wallets effectively requires biometric data to be used as the law in Nigeria requires a NIN to register a new SIM card, and by extension mobile number.<sup>84</sup> Although the additional links in the chain make the basic wallet tier less easily identifiable than the rest, the linking of wallets to mobile numbers which are effectively linked to the country's national identity scheme makes the distinction little more than academic.

For those who have so far avoided Nigeria's identity schemes, if a CBDC became more prevalent they may be forced into registering with the state just to access financial services or buy basic goods that should be open to all. The IMF working paper claims that the privacy of the eNaira, as an account based, identity-linked CBDC, will be on a par with bank accounts and legal requests will be required to access customer data.<sup>85</sup> However, critics of the eNaira argue that the Nigerian state has a poor record when it comes to data protection, raising questions about how robust these protections may be.<sup>86</sup>

The eNaira's privacy policy states that the CBN collects and "may use" a huge amount of information derived from the wallet, including account information [personal details, ID number, source of funds, IP address], information of contacts from a user's mobile phone and transaction details.<sup>87</sup> User data may be disclosed to the CBN's service partners, as well as in response to legal requests or when it "becomes necessary in order to protect the rights, property and safety of the Bank, our users and the public". No guarantees are made about banking confidentiality in the privacy policy.

The combination of the eNaira's linking of wallets to state-backed identity schemes, limited privacy policy and minimal discussion of privacy in official documentation is a recipe for disaster.

83 About NIN, Nigerian Identity Management Commission, accessed 11th August 2023, <https://nimc.gov.ng/about-nin/>

84 New SIM Card Registrations With Biometric ID Number Resume In Nigeria, Biometric Update, 19th April 2021, <https://www.biometricupdate.com/202104/new-sim-card-registrations-with-biometric-id-number-resume-in-nigeria>

85 Nigeria's eNaira, One Year After, WP/23/104, Jookyung Ree, International Monetary Fund, May 2022, <https://www.imf.org/en/Publications/WP/Issues/2023/05/16/Nigerias-eNaira-One-Year-After-533487>

86 Nigeria's Central Bank Digital Currency Is 'Same Naira, More Possibilities' – If You Count Government Snooping, Dr Kemi Omotubora and Dr Subhajit Basu, The Register, 22nd November 2021,

87 E-Naira Terms Of Service, Central Bank of Nigeria, accessed 8th August 2023, <https://enaira.gov.ng/about/terms-of-service>

## Success

Nigeria's CBDC was rolled out relatively quickly with third party trackers estimating that it took less than two years to bring to the fore.<sup>88</sup> The CBN claims that it had been working on a digital currency since 2017 but it had not published a proof of concept or any useful amount of trial data before mass use, critics argue.<sup>89</sup>

The eNaira launch in Nigeria is not viewed as a success, with low uptake among Nigerians. The International Monetary Fund, in a report assessing the eNaira's first year of operation, said that there had been few technical issues and no major breaches – but uptake had been limited notwithstanding this. Only around 0.8 per cent of people with bank accounts [c.860,000 people] and 10 per cent of merchants with digital payment setups had downloaded the wallet, as of November 2021 according to the IMF.<sup>90</sup>

Spring 2023 has seen an uptick in the number of wallets and the use of the CBDC but this has coincided with a major currency crisis, where the amount of physical cash in circulation had dropped by around two-thirds.

Godwin Emefiele, the governor of the CBN, announced in late March 2023 that eNaira transactions for the year to date were valued at around 22 billion Naira [c.£39.5 million at the time], up 63 per cent.<sup>91</sup> 13 million people had opened eNaira wallets in total, he added. In an attempt to increase uptake the CBN has announced plans to pay the salaries of government workers in eNaira, as well as pushing for tuition fees at public universities in the country to be paid via CBDC.<sup>92,93</sup>

In early 2023, Nigeria's currency crisis was a major international news story with Africa's largest economy seeing banks limit cash withdrawals. This arose after the CBN sought to reissue Naira notes, swapping old for new, but many businesses stopped accepting older notes. This led to a sharp contraction in the amount of cash in circulation, in a largely cash-based economy.

Despite the major currency crisis, it is estimated that the number of wallets still only makes up around 6 per cent of the Nigerian population [around 13 million], as of May 2023. However estimates from the IMF published in May 2023 further found that 98 per cent of wallets had never been used – meaning that only a tiny fraction of the population had used

88 Enaira, CBDC Tracker, accessed 8th August 2023, <https://cbdctracker.org/currency/nigeria-e-naira>

89 Nigeria's Central Bank Digital Currency Is 'Same Naira, More Possibilities' – If You Count Government Snooping, Dr Kemi Omotubora and Dr Subhajt Basu, The Register, 22nd November 2021,

90 Nigeria's eNaira, One Year After, WP/23/104, Jookyung Ree, International Monetary Fund, May 2022, <https://www.imf.org/en/Publications/WP/Issues/2023/05/16/Nigerias-eNaira-One-Year-After-533487>

91 The value of the Naira in relation to the pound plummeted in late June 2023 the value of this in GBP is now much lower.

92 Salaries And School Fees To Be Paid With Enaira As CBN Scrambles For Adoption, TechPoint Africa, 25th May 2023, <https://techpoint.africa/2023/05/25/salaries-and-school-fees-to-be-paid-with-enaira/>

93 CBN Wants School Fees Paid Through E-Naira, Vanguard, 22nd May 2022, <https://www.vanguardngr.com/2023/05/cbn-wants-school-fees-paid-through-e-naira/>

the CBDC, even if they had set up a wallet.<sup>94</sup> This suggests that even though the number of wallets increased significantly between November 2021 and May 2023, the eNaira was not widely used as a payment alternative by Nigerians, despite cash circulation falling sharply.

Despite a major government push and a crisis with hard currency it appears that the eNaira has not enjoyed significant success, making it difficult to evaluate its real world harms, although from published documents, the Nigerian CBDC comes with significant risks.

94 Nigeria's eNaira, One Year After, WP/23/104, Jookyung Ree, International Monetary Fund, May 2022, <https://www.imf.org/en/Publications/WP/Issues/2023/05/16/Nigerias-eNaira-One-Year-After-533487>

# Digital Euro

## European Central Bank

Stage: Research

### Summary

- Transaction data would be **monitored by European Central Bank**, which says complete anonymity is “not a viable option”
- Acceptance of digital euro **likely to be made mandatory** for shops and businesses
- Europeans surveyed about a future CBDC **placed strong priority on privacy**
- Potential digital euro infrastructure **could allow for conditional payments** and smart contracts, but programmability has been rejected

A Eurozone CBDC, if introduced, would instantly become one of the most prominent examples of digital currency in the world. There are 20 countries in the Eurozone, including some of the most advanced economies on Earth, covering around 350 million people and 12 per cent of the global economy. Six more states, mostly smaller ones, also use the Euro without being part of the Eurozone.<sup>95 96</sup>

The European Central Bank, the Eurozone’s central bank, is in the research phase for the digital euro. As a major global central bank the if, when and specifics of how the ECB decides to pursue a retail CBDC will have significant influence on other digital currencies worldwide – with the Bank of Israel explicitly labelling a digital euro rollout as a sufficient condition for it to introduce an e-shekel.<sup>97</sup>

In June 2023 the European Commission put forward a legislative proposal that sought to set out the framework of a potential future digital euro, as issued by the ECB. The bank has been in an ‘investigation’ or research phase since October 2021, running to October 2023.<sup>98</sup>

### Objectives and Motivations

The ECB published a July 2022 paper outlining the potential motivations for a digital euro and considerations which should be taken into account for its design. The objectives, in

95 What Is The Euro Area?, European Commission, accessed 10th August 2023, [https://economy-finance.ec.europa.eu/euro/what-euro-area\\_en](https://economy-finance.ec.europa.eu/euro/what-euro-area_en)

96 The Euro Outside Of The Euro Area, European Commission, accessed 10th August 2023, [https://economy-finance.ec.europa.eu/euro/use-euro/euro-outside-euro-area\\_en](https://economy-finance.ec.europa.eu/euro/use-euro/euro-outside-euro-area_en)

97 Potential Scenarios For Deciding To Issue a Digital Shekel, Bank of Israel, April 2023,

98 Digital Euro Package, European Commission, accessed 10th August 2023, <https://www.boi.org.il/media/j40nvorg/april-2023-potential-scenarios-for-deciding-to-issue-a-digital-shekel.pdf> [https://finance.ec.europa.eu/publications/digital-euro-package\\_en](https://finance.ec.europa.eu/publications/digital-euro-package_en)

the view of the central bank, are:<sup>99 100</sup>

1. **To preserve the role of public money as the “monetary anchor” in the Eurozone payment system and an alternative in the face of declining cash use**
  - a) Central bank money [e.g. cash] is seen as underpinning all other payment methods, such as bank cards, as all other methods are ultimately convertible to central bank money which is backed by the authority of the state, ‘anchoring’ the system. There are fears that declining cash use could undermine this trust, while a privately maintained payments system could see abuse of market position by operator companies, many of which are based outside of the EU. A digital euro is seen as a way of having a regional digital payment network not subject to private or foreign interests.
2. **Alternatives in an era of digital change and innovation**
  - a) The ECB expresses concern about the potential rise of stablecoins or cryptocurrencies made by non-EU states or private tech companies and suggests a CBDC could be a platform for digital innovation with the benefits it claims a central bank offers [e.g. efficiency, liquidity and stability].

How a digital euro is designed is key to making it successful, argues the ECB. It must add “value” or benefit to users, compared to existing payment methods, such as cash or bank cards. Privacy must also be of the “highest standard” but in compliance with the law, which raises the spectre of a digital euro being subject to checks and verification on par with banks and not offering the anonymity of cash. A CBDC should also promote financial inclusion and widen access to payment services.<sup>101</sup>

In a public-facing factsheet published in June 2023 the European Commission [EC] claimed that a digital euro would be easier to use than other digital payment methods, would offer consumers more choice and would even offer privacy on a par with cash.<sup>102</sup> Online payments would only share the same amount of data as paying online with a bank card, claims the EC, whereas offline payments would only reveal the same amount of data as an ATM withdrawal does on an individual’s bank statement. Prototype testing of the architecture of a future digital euro saw online and offline transactions operate with different technical solutions, albeit they would remain interoperable so online and

99 The Case For A Digital Euro: Key Objectives and Design Considerations, European Central Bank, July 2022, [https://www.ecb.europa.eu/pub/pdf/other/key\\_objectives\\_digital\\_euro~f11592d6fb.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/key_objectives_digital_euro~f11592d6fb.en.pdf)

100 Digital Euro – Our Future Money Presentation, Evelien Witlox, Program Director, Digital Euro Project, European Central Bank, 11th October 2022, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs221017\\_ecbatsibos.en.pdf?447523fb3a77c4c58413c7f-3870340da](https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs221017_ecbatsibos.en.pdf?447523fb3a77c4c58413c7f-3870340da)

101 The Case For A Digital Euro: Key Objectives and Design Considerations, European Central Bank, July 2022, [https://www.ecb.europa.eu/pub/pdf/other/key\\_objectives\\_digital\\_euro~f11592d6fb.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/key_objectives_digital_euro~f11592d6fb.en.pdf)

102 Digital Euro Factsheet, European Commission, June 2023, archived 23rd July 2023, [https://web.archive.org/web/20230703014605/https://finance.ec.europa.eu/system/files/2023-06/230628-digital-euro-factsheet\\_en\\_0.pdf](https://web.archive.org/web/20230703014605/https://finance.ec.europa.eu/system/files/2023-06/230628-digital-euro-factsheet_en_0.pdf)



offline wallets could interact.<sup>103</sup> The implication of this is that it is likely privacy features of offline transactions would be integral and not allow third parties to view transaction data. However, there is no detail given about the traceability of transactions if the state acquired access to the offline transaction wallet itself, perhaps through a court order.

The Commission claims that a digital euro would also help “preserve” the financial inclusion of groups who currently make greater use of cash, such as older people, or those who cannot currently access the banking system, such as refugees.<sup>104</sup>

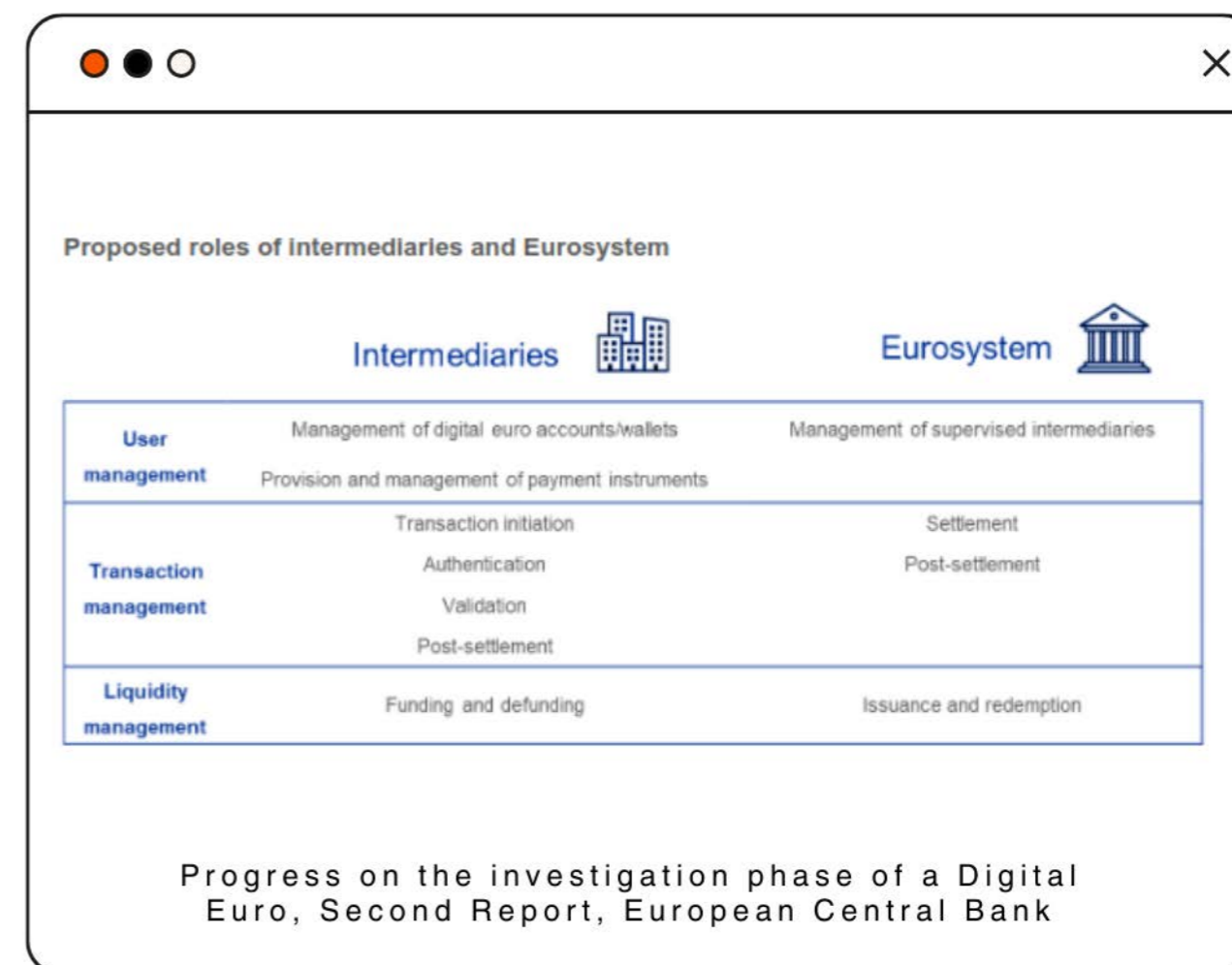
### Model

Although the European Commission has already begun to lay down legislation that would underpin a future digital euro, both the EC and European Central Bank are still working to examine what the technological basis for the CBDC would be. This includes examining whether the digital currency would be based on a distributed ledger solution, or whether an alternative architecture would be more suitable.<sup>105</sup>

The European authorities have indicated that they will look to use a two-tier intermediary-style model, as with other CBDCs including those proposed in Israel, Uruguay and Sweden. In broad brush statements, the EC states that digital euro interfaces would be provided by banks, who would be compelled to offer CBDC services as part of their role as commercial banks.<sup>106</sup> This would include basic accounts. Additionally, some public bodies would be empowered to “distribute the digital euro”, such as post offices or local government, to people who do not wish to or are not able to set up an account with a bank. Compulsory acceptance appears to be a likely feature of a digital euro, with all Eurozone merchants except the very smallest being required to accept the digital currency if it is introduced.<sup>107</sup>

Bodies “distributing” the digital euro to the public, effectively acting as their gateway to the CBDC, would be the ones responsible for conducting customer checks as part of the onboarding process, to comply with money laundering and other local/EU regulations.<sup>108,109</sup>

103 Digital Euro – Prototype Summary and Lessons Learned, European Central Bank, 26th May 2023, [https://www.ecb.europa.eu/pub/pdf/other/ecb\\_prototype\\_summary20230526~71d0b26d55.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb_prototype_summary20230526~71d0b26d55.en.pdf)  
 104 Questions On The Single Currency Package, European Commission, 28th June 2023, [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_3502](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3502)  
 105 FAQ on a Digital Euro, accessed 10th August 2023, [https://www.ecb.europa.eu/paym/digital\\_euro/faqs/html/ecb\\_faq\\_digital\\_euro.en.html](https://www.ecb.europa.eu/paym/digital_euro/faqs/html/ecb_faq_digital_euro.en.html)  
 106 Single Currency Package: New Proposals To Support The Use Of Cash And To Propose A Framework For A Digital Euro, European Commission, 28th June 2023, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_3501](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3501)  
 107 FAQ On A Digital Euro, European Central Bank, accessed 2nd October 2023, [https://www.ecb.europa.eu/paym/digital\\_euro/faqs/html/ecb\\_faq\\_digital\\_euro.en.html](https://www.ecb.europa.eu/paym/digital_euro/faqs/html/ecb_faq_digital_euro.en.html)  
 108 Digital Euro – Our Future Money Presentation, Evelien Witlox, Program Director, Digital Euro Project, European Central Bank, 11th October 2022, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/profuse/shared/files/dedocs/ecb\\_dedocs221017\\_ecbatsibos.en.pdf?447523fb3a77c4c58413c7f-3870340da](https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb_dedocs221017_ecbatsibos.en.pdf?447523fb3a77c4c58413c7f-3870340da)  
 109 Progress On The Investigation Phase Of A Digital Euro, Second Report, European Central Bank, 21st December 2021, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/)



The digital euro will be impacted by European AML and CTF regulations, with online transactions being fully subject to the rules. Offline transactions will be subject to holdings and transaction limits, determined by risk assessments, as a way of mitigating supposed AML/CTF risks.

Online and offline payments are being built into the digital euro with differing levels of privacy, with the ECB being clear that it plans to allow the digital currency to be used across the Eurozone regardless of internet connectivity. The ECB implies that offline transfers will use secure hardware features to facilitate the use of the currency without an internet connection, with these transactions later effectively settled through the digital euro system when an internet connection is available.<sup>110</sup> Although these are not explicitly defined, it is implied that offline transactions could use NFC or similar technology to interact to execute the transfer.

110 Progress On The Investigation Phase Of A Digital Euro, Fourth Report, European Central Bank, 13th July 2023, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb\\_degov230713-fourth-progress-report-digital-euro-investigation-phase.en.pdf?704b0eee4c20eee4dbe-4970f5091a96a](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb_degov230713-fourth-progress-report-digital-euro-investigation-phase.en.pdf?704b0eee4c20eee4dbe-4970f5091a96a)

Each device would then verify the transaction and its value – with the EC claiming that nobody, not even the ECB, would be able to see details of offline transactions bar that €X had left the wallet. However, the EC also states that it expects offline transactions to be mainly used for small payments, though it does not mention specific limits.<sup>111</sup>

Online transactions would make more data available to intermediaries and potentially the central bank and authorities. The EC says it is on par with the data shared when making a card payment online. The Commission claims that the ECB will only be able to see encrypted data that is necessary to settle transactions and process payments.<sup>112</sup> An internet connection will be necessary to deposit or withdraw digital euros, or to transfer them to devices which are then used to make offline payments.

The settling of online transactions would be done by the ECB, as the digital euro [like cash] is a central bank liability and its movement would need to be recorded by the bank, regardless of what privacy measures are enacted on top of this.<sup>113</sup> Offline transactions would be verified and settled in the hardware of devices, whilst topping up an offline digital euro wallet or withdrawing currency from it to a bank account or cash would require online access. This may be by using an ATM-style machine to add or take Euros off it, by bank card payment or by “transferring” from an online digital euro account – in this case, documents imply that the ECB would only see a block of digital euros settled offline [akin to a bank statement seeing €X withdrawn from an ATM].<sup>114 115</sup>

## Privacy

Concerns around the privacy of a European CBDC have been rife, with high-level figures inside the European Commission reportedly attempting to delay the legislative proposals for a digital euro, laid in summer 2023, in order to address privacy worries.<sup>116</sup> Proponents of the CBDC, including the EU Finance Commissioner Mairead McGuinness claim that it is “not a Big Brother project”, but the concerns were serious enough that Ursula von der Leyen, the Commission President, attempted to push back the proposals to strengthen

111 Digital Euro Factsheet, European Commission, June 2023, archived 23rd July 2023, [https://web.archive.org/web/20230703014605/https://finance.ec.europa.eu/system/files/2023-06/230628-digital-euro-factsheet\\_en\\_0.pdf](https://web.archive.org/web/20230703014605/https://finance.ec.europa.eu/system/files/2023-06/230628-digital-euro-factsheet_en_0.pdf)

112 The Euro: Single Currency Package, European Commission, 28th June 2023, [https://finance.ec.europa.eu/system/files/2023-06/230628-digital-euro-factsheet\\_en\\_0.pdf](https://finance.ec.europa.eu/system/files/2023-06/230628-digital-euro-factsheet_en_0.pdf)

113 Progress On The Investigation Phase Of A Digital Euro, Second Report, European Central Bank, 21st December 2021, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb.degov221221\\_Progress.en.pdf?f91e0b8ff8cbd6654d7e6b071a8f7071](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov221221_Progress.en.pdf?f91e0b8ff8cbd6654d7e6b071a8f7071)

114 Progress On The Investigation Phase Of A Digital Euro, Second Report, European Central Bank, 21st December 2021, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb.degov221221\\_Progress.en.pdf?f91e0b8ff8cbd6654d7e6b071a8f7071](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov221221_Progress.en.pdf?f91e0b8ff8cbd6654d7e6b071a8f7071)

115 Digital Euro Factsheet, European Commission, June 2023, archived 23rd July 2023, [https://web.archive.org/web/20230703014605/https://finance.ec.europa.eu/system/files/2023-06/230628-digital-euro-factsheet\\_en\\_0.pdf](https://web.archive.org/web/20230703014605/https://finance.ec.europa.eu/system/files/2023-06/230628-digital-euro-factsheet_en_0.pdf)

116 Privacy Fears Dominate Launch of Digital Euro Plan, Politico, 28th June 2023, <https://www.politico.eu/article/privacy-dominate-launch-digital-euro-plan/>

the language on privacy in the plans. Responses to the digital euro consultation placed privacy as the most important aspect of the CBDC, with 43% of people putting it first.<sup>117</sup>

In October 2022 the European Data Protection Board raised several privacy concerns about the digital euro. The EU’s GDPR watchdog demanded the introduction of offline, anonymous peer-to-peer payments be a priority, anonymity for transactions below a certain threshold and specific legislation to be introduced to ensure balancing of privacy against AML/CTF rules rather than relying on existing regimes.<sup>118</sup>

Presentations by the ECB suggest that the level of privacy in a future digital euro is fundamentally a political choice, that may end up being balanced against other policy objectives.<sup>119</sup> Although the EU is bound by the General Data Protection Regulations, which is a relatively strong data protection regime when compared internationally, these protections are not absolute and other goals such as countering fraud or national security can outweigh them – leaving the door open to weaken the CBDC’s privacy if it is deemed necessary.

The baseline scenario for a digital euro will be equivalent to private digital payment networks [e.g. PayPal] with user and transaction data visible to intermediaries providing the wallets at least for AML/CTF purposes. Full anonymity is “not considered a viable option from a public policy perspective” says the ECB.<sup>120</sup> However, the European Commission claims that neither the ECB nor respective national central banks will be able to link transaction or usage data to individuals – with transparency limited to intermediary operators.<sup>121</sup> Effectively, online payments with a digital euro will be treated in a similar manner to online private payment methods [such as bank cards] for data transparency concerning money laundering and counter terror financing rules. The European Data Protection Board has raised concerns about the transparency of data to intermediaries and suggested that the validation of all online transactions [as opposed to just those based on risk] may breach proportionality and necessity principles.<sup>122</sup>

Little detail has been provided so far about what form AML/CTF checks would take, partly

117 Progress On The Investigation Phase Of A Digital Euro, European Central Bank, 29th September 2022, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf)

118 Adopted Statement 04/2022 On The Design Choices For A Digital Euro From The Privacy And Data Protection Perspective, European Data Protection Board, 10th October 2022, [https://edpb.europa.eu/system/files/2022-10/edpb\\_statement\\_20221010\\_digital\\_euro\\_en.pdf](https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf)

119 Digital Euro Privacy Options, Eurogroup – European Central Bank, 4th April 2022, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb.degov220404\\_privacy.en.pdf](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220404_privacy.en.pdf)

120 Progress On The Investigation Phase Of A Digital Euro, European Central Bank, 29th September 2022, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf)

121 Proposal For A Regulation Of The European Parliament And Of The Council On The Establishment Of The Digital Euro, COM(2023) 369, European Commission, 28th June 2023, [https://eur-lex.europa.eu/resource.html?uri=cellar:6f2f669f-1686-11ee-806b-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:6f2f669f-1686-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF)

122 Adopted Statement 04/2022 On The Design Choices For A Digital Euro From The Privacy And Data Protection Perspective, European Data Protection Board, 10th October 2022, [https://edpb.europa.eu/system/files/2022-10/edpb\\_statement\\_20221010\\_digital\\_euro\\_en.pdf](https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf)

because these will be left to intermediaries such as banks who currently have a legal duty to enforce these regulations. The implication is that these will be similar to the checks currently run on bank accounts and other private digital financial systems.<sup>123</sup> These bodies will also perform the KYC checks, which it is also implied may be similar to those run when opening a bank account. As these rules are in part regulated by national governments, it would be complicated to analyse them all here but identity checks are likely to be a part of this.

Offline digital euro payments are envisaged as having much more privacy. Executed using on-device hardware to validate transactions rather than a third-party [such as a centralised database or DLT node] would be close to cash in terms of functionality, with the ECB investigating peer-to-peer transactions that operate without the need for central validation.<sup>124</sup> The bank is also examining so-called “selective privacy” for low value transactions, which could take a variety of forms, some of which could offer better privacy – however, this depends on whether the “selective privacy” can be undone or is conditional.<sup>125</sup>

The EU currently has limits on cash transactions that can be conducted without ID or other KYC checks. Laws approved by the European Parliament in March 2023 limit cash transactions to €7,000 – a cap above which the customer must be identified for the payment to go forward.<sup>126</sup> Several EU member states, including some in the Eurozone, have lower limits and cash restrictions that go beyond requiring ID.<sup>127</sup> These limits on cash payments raise questions about the role AML and CTF checks should play in all transactions, and the impact either verification requirements and absolute caps for high-value cash payments have on privacy. Similar question exist about the limits on wholly private CBDC transactions, and these become more serious if the proposed limit on anonymous CBDC payments turns out to be much lower than the cash limit – as inferences may be drawn about secondary purposes of digital currency beyond technical innovation.

123 Speech: A Digital Euro That Serves The Needs Of The Public: Striking The Right Balance, Fabio Panetta, Member of the Executive Board of the ECB, 30th March 2022, [https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220330\\_1~f9fa9a6137.en.html](https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220330_1~f9fa9a6137.en.html)

124 Digital Euro – Our Future Money Presentation, Evelien Witlox, Program Director, Digital Euro Project, European Central Bank, 11th October 2022, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs221017\\_ecbatsibos.en.pdf?447523fb3a77c4c58413c7f-3870340da](https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs221017_ecbatsibos.en.pdf?447523fb3a77c4c58413c7f-3870340da)

125 Progress On The Investigation Phase Of A Digital Euro, European Central Bank, 29th September 2022, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf)

126 New EU Measures Against Money Laundering And Terrorist Financing, European Parliament, 28th March 2023, <https://www.europarl.europa.eu/news/en/press-room/20230327IPR78511/new-eu-measures-against-money-laundering-and-terrorist-financing>

127 Cash Payment Limitations, European Consumer Centre France, 29th September 2022, <https://www.europe-consommateurs.eu/en/shopping-internet/cash-payment-limitations.html>

## Risks from a Digital Euro

The ECB sees a major risk to monetary stability if the digital euro displaces retail bank deposits, with people holding the CBDC rather than money in traditional bank accounts. This is because deposits provide liquidity for bank lending as mass-flight from retail bank accounts to CBDC accounts would significantly hamper bank lending and thus economic investment.<sup>128</sup>

Limitations on holdings and the velocity of money moving from retail accounts to CBDC accounts are suggested as measures that would help reduce liquidity flight, but would have the consequence of restricting how people can use their money if they look to make use of a digital euro. One tool suggested is a “waterfall” setting, where excess digital euros above a holding limit are automatically sent to a retail bank account – but this may act as an effective ceiling for the utility of the CBDC for the unbanked.<sup>129130</sup>

The EC views fraud in digital payments as something which could put people off the digital euro and seeks to place anti-fraud measures at the heart of the design. Monitoring and risk scoring of transactions, as well as data gathering, are proposed as ways to battle this – however, the mass-monitoring of transactions would have a detrimental impact on privacy.<sup>131</sup> Details on what data would be collected and analysed are scant, but proposals to risk score transactions could have significant effects.

## Programmability

The ECB claims that digital euros will not be programmable in the sense of restricting transactions and that neither the ECB nor national authorities will be able to set limits on where, how or when they are spent. The Commission does say that the digital currency could be programmable by users to set up recurrent payments akin to direct debits. Conditional payments, or smart contracts, where a transaction is executed when certain conditions are met are outlined as a potential use case for the digital euro.<sup>132</sup>

Officials from the ECB and documents from the EC have consistently rejected the

128 Progress On The Investigation Phase Of A Digital Euro, European Central Bank, 29th September 2022, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf)

129 Ibid

130 The Case For A Digital Euro: Key Objectives And Design Considerations, European Central Bank, July 2022, [https://www.ecb.europa.eu/pub/pdf/other/key\\_objectives\\_digital\\_euro~f11592d6fb.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/key_objectives_digital_euro~f11592d6fb.en.pdf)

131 Progress On The Investigation Phase Of A Digital Euro, Fourth Report, European Central Bank, 13th July 2023, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb.degov230713-fourth-progress-report-digital-euro-investigation-phase.en.pdf?704b0eee4c20eee4dbe-4970f5091a96a](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov230713-fourth-progress-report-digital-euro-investigation-phase.en.pdf?704b0eee4c20eee4dbe-4970f5091a96a)

132 Progress On The Investigation Phase Of A Digital Euro, Third Report, European Central Bank, 23th April 2023, [https://www.ecb.europa.eu/paym/digital\\_euro/investigation/governance/shared/files/ecb.degov230424\\_progress.en.pdf](https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov230424_progress.en.pdf)

possibility of the digital euro becoming programmable money insofar as controlling how or where the CBDC is spent. They argue that it would not be in line with the principles of the currency and would undermine its functionality as central bank money treated as on par with physical cash, as programmed money could not be convertible to physical currency easily.

## Jam-Dex Jamaica

Stage: Full rollout

### Summary

- linked to **photo ID** and **tax registration** – and plans to integrate with national ID
- plans to issue **welfare payments** via Jam-Dex
- low uptake of **only 6.8 per cent** of the population

Jamaica's Central Bank Digital Currency, Jam-Dex, was fully rolled out in the Caribbean country in the summer of 2022. The Bank of Jamaica recognises Jam-Dex, short for the Jamaica Digital Exchange, as legal tender on par with the Jamaican Dollar.<sup>133</sup> Jam-Dex began a pilot phase in August 2021 with a ceremonial "first minting" of the digital token. It began with the Bank of Jamaica minting 230,000,000 Jamaican Dollars worth [c.£1.1million at the time] of Jam-Dex. Less than a year later the central bank decided on a full rollout of the CBDC. At the time of writing the Bank of Jamaica does not appear to have published any substantial findings from the pilot, bar a blog post celebrating the pilot's success.<sup>134135</sup>

Legislation to underpin Jam-Dex was passed in May 2022, with the backing of senior ministers in the Jamaican government. Ministers claimed that a CBDC would increase financial inclusion in the country, reduce cash handling fees and make transactions more efficient.<sup>136</sup>

Unlike many other central banks, the Bank of Jamaica has not published extensive documents or white papers about its CBDC, with the bank rapidly moving from pilot to full rollout. Generally, central banks seeking to introduce a digital currency have laid out their motivations, provided information on the technical architecture of the product and drafted policies around how the CBDC will be used. With the BOJ failing to make this information available, despite Jam-Dex being fully operational, the bank makes it much harder to evaluate its CBDC, and more difficult for the public to make an informed decision about whether to use it.

133 Jamaica Launches "Jam-Dex", Becomes First Nation To Legalise Digital Currency, Outlook India, 10th June 2022 <https://www.outlookindia.com/business/jamaica-launches-jam-dex-becomes-first-nation-to-legalise-digital-currency-news-201592>

134 Ceremonial First Minting Of BOJ CBDC, Bank of Jamaica, accessed 2nd August 2023 <https://boj.org.jm/core-functions/currency/cbdc/ceremonial-first-minting-of-boj-cbdc/>

135 BOJ's CBDC Pilot Project A Success, Bank of Jamaica, 31st December 2021, <https://boj.org.jm/bojs-cbdc-pilot-project-a-success/>

136 Senate Approves Central Bank Digital Currency, Jamaica Information Service, 4th June 2022, <https://jis.gov.jm/senate-approves-central-bank-digital-currency/>



## Motivations

The Bank of Jamaica claims that Jam-Dex will offer a host of benefits for individuals, the private sector and the central bank. In addition to greater financial inclusion, the bank argues that the digital currency will increase efficiency in the payment system, modernise it and allow for a greater range of related services to be on offer. The central bank itself will also save on the costs of acquiring physical currency.<sup>137</sup>

## Model

Private sector third parties, such as banks or building societies, operate retail CBDC wallets in Jamaica. Setting up a wallet requires someone to provide their name, address, government-approved photo ID and their taxpayer registration number – clearly linking the CBDC wallet to a specified individual.<sup>138</sup>

Jam-Dex is not blockchain based and is instead based on a custom real time payment settlement system, with the central bank stating that it chose the model in order to integrate the CBDC with existing payment infrastructure.<sup>139</sup>

“Frequently Asked Questions” published by the Bank of Jamaica state that wallet information is not shared by default when a transaction is performed – with the centralised system only recording the value of the transaction. Wallet providers can see and link transactions to specific individuals, and the Bank of Jamaica claims that this would only be shared with authorities in the event of an official request – such as one concerning terrorism or money laundering regulations.

There are also plans to integrate Jam-Dex with Jamaica’s new National Identification System [NIDS], which was announced in 2022. NIDS is described as “a reliable database of all Jamaican citizens” where identities will be tied to a unique number. This will link digital currency accounts to a centralised identity database.<sup>140</sup> The system will also integrate with some online government services, giving it a flavour of a digital identity card.

Regardless of how frequently requests for identifying information are made, or indeed granted, Jam-Dex is clearly not fully anonymous. A degree of privacy is a design feature, where identities are masked by default, but this can easily be lifted and linked to an official ID. There is an important distinction between irreversible anonymity and a pseudonym

137 A Primer On BOJ’s CBDC, Bank of Jamaica, 31st March 2020, <https://boj.org.jm/a-primer-on-bojs-central-bank-digital-currency/>

138 CBDC FAQs, Bank of Jamaica, accessed 2nd August 2023, <https://boj.org.jm/core-functions/currency/cbdc/cbdc-faqs/>

139 A Primer On BOJ’s CBDC, Bank of Jamaica, 31st March 2020, <https://boj.org.jm/a-primer-on-bojs-central-bank-digital-currency/>

140 Senate Approves Central Bank Digital Currency, Jamaica Information Service, 4th June 2022, <https://jis.gov.jm/senate-approves-central-bank-digital-currency/>

which can disappear at the click of a button.

## Usage

As of 19th June 2023, at least 2,350 merchants in Jamaica accept Jam-Dex as a means of payment. Data from February 2023 found that 190,000 people had signed up to Jam-Dex out of a population of 2.8 million, around 6.8 per cent of all Jamaicans.<sup>141</sup> In 2021, the Jamaican government said it was seeing to make welfare payments digital in the future by paying them via Jam-Dex wallets, rather than via financial institutions, a decision which would place pressure on some vulnerable people to adopt the CBDC if the government followed through on it.<sup>142</sup>

The uptake of Jam-Dex in Jamaica has been slow, and the central bank has offered significant financial incentives to merchants and individuals to encourage growth. From April 2023, the first 10,000 merchants to sign up have been offered a J\$25,000 [c.£1,250] bonus while individuals were all offered two per cent cash-back up to J\$5,000 [c.£250] a month on all purchases. Businesses were required to share their registration, bank details and a certificate of tax compliance to set up a commercial Jam-Dex wallet and receive the bonuses.

141 Gov’t Provides Incentives to Boost JAM-DEX Use, Jamaica Information Service, 9th March 2023, <https://jis.gov.jm/govt-provides-incentives-to-boost-jam-dex-use/>

142 Jamaica To Digitise Welfare Payments Through CBDC, Our Today, 29th May 2021, <https://our.today/jamaica-to-digitise-welfare-payments-through-cbdc/>

# e-CNY

## China

Stage: Pilot

### Summary

- Limited English language information on the e-CNY despite it being the **biggest CBDC pilot on Earth**
- Account based model means **privacy is necessarily limited**
- Low-level wallets require a phone number, which in turn **needs ID**, higher level wallets need direct ID verification
- Trials are already using the CBDC to **nudge behaviour**, from sign up bonuses to “cashback” for using public transport over private cars

China’s pilot of its CBDC, the e-CNY [informally the digital yuan], is one of the largest in the world by transaction volume. In July 2023 Dr Yi Gang, the governor of the country’s central bank, claimed that ¥1.8 trillion [c.£200 billion] worth of transactions had been made using the digital yuan, across 950 million total transactions with more than 120 million wallets being open.<sup>143</sup> This is a marked rise of 18 times over the volume of ¥100 billion reported at the end of August 2022.<sup>144</sup> The figures quoted by Dr Yi Gang suggest that the average transaction is worth around £210, at exchange rates at the time of publication.

However, these numbers also appear to contradict earlier figures published by the Chinese government in 2022, which said 261 million people had set up e-CNY wallets, suggesting that some figures, even when published by the People’s Bank of China [PBOC], could be unreliable.<sup>145</sup>

Even though the transaction volumes for e-CNY are large, it is still only in the pilot stage, which has been operating since August 2020. The pilot covers more than 25 cities and hundreds of millions of people across the country, but no date for a full national roll-out has been set.<sup>146</sup> The purposes of the digital currency, according to the director general of the PBOC’s Digital Currency Institute, are to improve financial inclusion, increase efficiency in the central bank payment systems and provide a backup option to private retail payment systems such as Alipay.<sup>147</sup> The bank also plans to use the e-CNY to facilitate easier cross-

143 China Open To Exploring Real-Time Settlements With Singapore: Central Bank Governor, Channel NewsAsia, 19th July 2023, [https://www.youtube.com/watch?v=TooIUeG\\_wCk](https://www.youtube.com/watch?v=TooIUeG_wCk)

144 China’s Digital Yuan Transactions Seeing Strong Momentum, Says Cbank Gov Yi, Reuters, 19th July 2023, <https://www.reuters.com/markets/asia/chinas-digital-yuan-transactions-seeing-strong-momentum-says-cbank-gov-yi-2023-07-19/>

145 China Will Expand CBDC Trials To Most Populous Province, CoinTelegraph, 20th September 2022, <https://cointelegraph.com/news/china-will-expand-cbdc-trials-to-most-populous-province-report>

146 What’s Next For China’s Digital Currency, 3rd August 2023, MIT Technology Review, <https://www.technologyreview.com/2023/08/03/1077181/whats-next-for-chinas-digital-currency/>

147 Ibid

border payments, although the focus is primarily on domestic use.

### Model

Despite the scale of the Chinese CBDC pilot, there is little published information outlining the details of the e-CNY’s model or architecture. A single 16-page document and occasional statements from senior PBOC officials make up the bulk of the primary sources available in the English language about the e-CNY’s design and these do not offer a comprehensive picture. It is therefore difficult to write with the same detail about the technical aspects of the e-CNY as is possible with other CBDCs, including on any privacy protections in place. This is despite the claims of millions of e-CNY users and the advanced stage of the project. As such, drawing definitive lessons from the pilot is not simple.

The e-CNY is an account-based CBDC, meaning that wallets function more like bank accounts instead of storing digital tokens that represent the currency as many other CBDCs do.<sup>148</sup> It operates on a two-tier model with the central bank issuing the currency and backing it, while private sector operators such as commercial banks create the wallets and public-facing infrastructure. These companies are responsible for complying with AML and CTF rules, and other financial regulations, rather than the central bank. At present the e-CNY is not DLT based and instead, the PBOC runs a centralised ledger for transactions. However, it is seeking to facilitate the private wallet operators building technology on top of the basic platform to diversify their offerings in the future.

Wallets are being designed either as software-based, such as on mobile phones, or as hard wallets – which are linked to a physical device such as a SIM card.<sup>149</sup> The latter type is still a developing technology but seeks to provide a way of making payments without an internet connection. The PBOC argues that the different wallet formats will help address issues of financial inclusion.<sup>150</sup>

### Privacy

The PBOC describes privacy in China’s CBDC as built on the principle of “managed anonymity” described as “anonymity for small value and traceable for high value”.<sup>151</sup> The

148 Progress of Research & Development of E-CNY in China, Working Group On E-CNY Research & Development, People’s Bank of China, July 2021, <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>

149 China Digital Currency: Beijing Forum Promotes SIM-Based ‘E-CNY Hard Wallet’ As An Alternative For Mobile Payments, South China Morning Post, 13th October 2023,

150 Progress of Research & Development of E-CNY in China, Working Group On E-CNY Research & Development, People’s Bank of China, July 2021, <https://finance.yahoo.com/news/china-digital-currency-beijing-forum-093000739.html> <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>

151 Progress of Research & Development of E-CNY in China, Working Group On E-CNY Research & Development, People’s Bank of China, July 2021, <https://finance.yahoo.com/news/china-digital-curren->

PBOC claims that it places significant value on protecting privacy, but the design still seeks to enforce AML and CTF rules and to “guard against the misuse of e-CNY in illegal and criminal activities”<sup>152</sup> from tax evasion to online gambling [which is illegal in China]. This suggests a significant degree of digital surveillance. It also states that there is an internal firewall within PBOC systems to segregate the information generated by the e-CNY and that protocols exist to regulate third party or other government agency requests to access to the data, according to relevant laws and regulations.

However, with the limited information available about the e-CNY there is no published detail about the technical design of any privacy protections for the digital currency, nor detail about the policies that are supposed to protect user confidentiality. Therefore, it is difficult to assess what managed anonymity would mean for an e-CNY customer. The account-based design of the CBDC also limits the degree anonymity can be applied, as all transactions are ultimately linked to a specific account.

Wallets in the e-CNY system are tiered and users get access to higher transaction and balance limits as they offer greater amounts of identification. As of summer 2022, the lowest level of account, which only requires a phone number, has a balance limit of ¥10,000 [c.£1,100], and transaction limits of ¥2,000 [c.£220] a time and ¥5,000 [c.£550] a day.<sup>153</sup> The linking of the lowest wallet tier to a phone number demonstrates that the CBDC is not truly anonymous, as ID has been required to register a new phone number in China since 2010.<sup>154</sup> A wallet verified with a Chinese ID card has limits of ¥50,000 [c.£5,500] per single payment, ¥100,000 [c.£11,000] in daily payments and a balance cap of ¥500,000 [c.£55,000].<sup>155</sup>

Chinese officials point to the country’s recent data protection rules, the Personal Information Protection Law, as evidence of the e-CNY’s privacy credentials. Mu Changchu, the Director of the Digital Currency Research Institute at the PBOC published a paper in October 2022 arguing that the e-CNY attaches importance to privacy.<sup>156</sup> He stated that transaction data is held by wallet providers, while the central bank sees de-identified information to record transactions, and that only when a competent authority makes a legal request can the data be made identifiable. However, the scope for such legal requests is likely to be very broad.

[cy-beijing-forum-093000739.html http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf](http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf)

152 Ibid.

153 A Report Card on China’s Central Bank Digital Currency: the e-CNY, Atlantic Council, 1st March 2022, <https://www.atlanticcouncil.org/blogs/econographics/a-report-card-on-chinas-central-bank-digital-currency-the-e-cny/>

154 China Demands ID From All Buyers Of Mobile Phone Numbers, The Guardian, 1st September 2010, <https://www.theguardian.com/world/2010/sep/01/china-mobile-phone-number-identity>

155 China Reveals e-CNY Wallet Specifications, Forkast, 14th June 2021, <https://forkast.news/china-reveals-e-cny-wallet-specifications/>

156 E-CNY: Balancing Privacy and Security, Mu Changchu, Director, Digital Currency Research Institute, People’s Bank of China, 14th October 2022

Despite the claims by officials in the country that the e-CNY will seek to protect privacy and that protections will be in place, the authoritarian and opaque nature of the Chinese government has raised fears about how much protection is really on offer to CBDC users.<sup>157</sup> The rule of law is also a significant issue when applying privacy protections, and in a country where the government enjoys few checks and balances, the misapplication or bending of rules also necessarily means that even if technical protections are good they are at permanent risk of circumvention.

China’s payment system is currently dominated by private companies who tie in mobile payments to other services, such as gaming or social networks, so privacy in competing digital money systems is already limited meaning the e-CNY only has a low bar to clear to offer greater privacy to users. However, suggestions that China will soon seek to use AI and big data to tackle “suspicious” and illicit activities imply that data from the e-CNY will undergo massive, and potentially intrusive, processing in the name of safety.<sup>158</sup>

### *Programmability*

Smart contracts, as automatic conditional payments, are being built into the design of the e-CNY with the stated aim of facilitating business innovation according to the PBOC progress report.<sup>159</sup> As with other aspects of the e-CNY, there is little concrete detail on how this works in practice, and there are fears that programmability could be used for more nefarious purposes.

In October 2023, a senior official at China’s foreign currency exchange regulator went further and suggested that programmability could be used to modify the effectiveness of monetary policy, for example by changing interest rates on CBDC holdings, which could impact whether people and businesses want to hold more or less of the digital currency in their wallets.<sup>160</sup>

There is already evidence that at the local or regional level, the CBDC is being used to influence behaviour. Financial incentives of up to ¥250,000 [c.£28,000] were offered in a lottery to new sign-ups in the city of Suzhou, while 50,000 randomly picked residents of Shenzhen were given mobile cash envelopes containing e-CNY with the aim of boosting

157 China’s Digital Yuan Works Just Like Cash – With Added Surveillance, WIRED, 8th November 2022, <https://www.wired.com/story/chinas-digital-yuan-ecny-works-just-like-cash-surveillance/>

158 A Report Card on China’s Central Bank Digital Currency: the e-CNY, Atlantic Council, 1st March 2022, <https://www.atlanticcouncil.org/blogs/econographics/a-report-card-on-chinas-central-bank-digital-currency-the-e-cny/>

159 Progress of Research & Development of E-CNY in China, Working Group On E-CNY Research & Development, People’s Bank of China, July 2021, <https://forkast.news/china-reveals-e-cny-wallet-specifications/> <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>

160 China FX Regulator Says CBDC Features Could Improve Monetary Policy, Reuters, 13th October 2023, <https://www.reuters.com/markets/currencies/china-fx-regulator-says-cbdc-features-could-improve-monetary-policy-2023-10-13/>

uptake.<sup>161162</sup> In Shanghai, users of public transport are offered e-CNY for using low-carbon options such as the metro or a bus. The willingness of officials to use the e-CNY to encourage sign-up, or nudge towards different transport options suggests that CBDC could be used to influence behaviour more widely – and programmability would be a powerful tool to do so.

161 China's Ambitious e-CNY Plan Faces A Giant Hurdle: Winning Over 1 Billion Consumers At Home, South China Morning Post, 4th March 2023, <https://www.scmp.com/tech/policy/article/3212245/chinas-ambitious-e-cny-plan-faces-one-giant-hurdle-winning-over-1-billion-consumers-home>

162 Practice Makes Perfect: What China Wants From Its Digital Currency In 2023, Atlantic Council, 24th April 2023, <https://www.atlanticcouncil.org/blogs/econographics/practice-makes-perfect-what-china-wants-from-its-digital-currency-in-2023/>

## Digital Pound United Kingdom

Stage: Research and consultation

### Summary

- pseudonymised **transactions**
- tiered wallets depending on **identification level**
- prospect of **third-party data sharing** to gain commercial 'benefits' for individual users
- Bank of England **exploring programmability** options

The Bank of England [BoE] and the Treasury launched a consultation on a potential British CBDC, the digital pound, in February 2023. The response period ran until the end of June 2023 and at the time of writing the outcomes and findings have not yet been published.<sup>163</sup> As the UK is in the early phases of its work on the digital pound there is limited concrete detail on the form the CBDC would take, but some early suggestions and overarching principles nevertheless provide some useful insight.

### Model

The BoE envisages the digital pound as being a two-tier public-private partnership, with the currency issued by the central bank but wallets and other public-facing infrastructure being operated by private sector organisations.<sup>164</sup> As the public interface of the CBDC system, these private organisations would be responsible for performing KYC, AML and CTF checks on account holders.

Although operating the wallet interfaces, the private organisations would never hold customers's digital pounds as banks directly hold funds. Instead, they would provide the interface to the underlying digital currency ledger. When executing transactions the private institution would issue pseudonymous instructions to the central BoE ledger to move funds between wallets on it, with the bank claiming it would not know the involved parties' identities.<sup>165</sup> However, this veil could be lifted with a court order or similar legal authority, meaning it is pseudonymous rather than anonymous.

It is not yet clear whether a digital pound would operate on DLT, or a more traditional centralised database, with the BoE still exploring technical options for the CBDC.<sup>166</sup>

163 The Digital Pound, The Bank of England, accessed 5th October 2023, <https://www.bankofengland.co.uk/the-digital-pound>

164 Section D1, The Digital Pound Consultation Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>

165 Ibid

166 Technology Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/technology-working-paper>



The private sector organisations operating CBDC wallets would not be limited to traditional financial institutions such as banks, as the BoE does not think the interface providers will need to be subject to the same controls as banks because they will not hold funds as banks do.<sup>167</sup> Plans for a wider range of organisations to offer wallets would also facilitate innovation in the products on offer, claims the BoE, as would the design of the underlying infrastructure. Potential external providers may also provide additional non-wallet services in the CBDC ecosystem, with the BoE suggesting these could include business analytics, budgeting and fraud monitoring tools, taking advantage of read-only access to the ledger.

Wallets could be used to make payments online or in person, using mobile devices or a card, and would effectively function in a similar way to card payments today.<sup>168</sup>

Limits would be placed on digital pound holdings, in part to protect retail banks whose business models rely on cash holdings. The BoE expects the limit to be between £10,000 and £20,000 at least initially.<sup>169</sup> It is claimed that this limit would allow the majority of people in the UK to hold their salary in digital pounds while restricting outflows from retail banks that would endanger liquidity ratios.

In the consultation document, the BoE makes references to the harms of financial exclusion, which impacts certain groups disproportionately.<sup>170</sup> The BoE argues that a CBDC could facilitate greater inclusion for some groups, who do not want to or cannot engage with the retail banking industry, as the digital pound provides another option. However, the BoE does concede that digital exclusion-linked financial exclusion may not be addressed by adopting a digital currency. Resultantly, the BoE is seeking to make the CBDC simple to use, but there are significant barriers to overcome with digital exclusion that will be a challenge to wider adoption.

### Privacy

Pseudonymised data could be used commercially by private wallet providers, according to the BoE. This would give private organisations greater insight than ever before into British

[co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf](https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf)  
167 Section D1, The Digital Pound Consultation Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>  
168 Section D3, The Digital Pound Consultation Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>  
169 Section D1, The Digital Pound Consultation Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>  
170 Section D1, The Digital Pound Consultation Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>

people's spending habits, both with businesses and inter-personal transfers.<sup>171</sup> Mass data collection on this scale, even if stripped of identifiers, would be an advertising goldmine and facilitate a new era of targeted advertising based on granular spending data for a country at large.

Fraud features heavily in the BoE's consultation document and it is clear that anti-fraud controls would be a key part of the digital pound infrastructure, at least on a par with controls that exist with private digital money, which will necessarily incur intrusion on the privacy of the CBDC.

The bank claims that the digital pound would be subject to "rigorous standards of privacy and data protection", in line with the UK's data protection rules.<sup>172</sup> It seeks to put CBDC transactions on a par with bank and credit card payments, which leave a trail of transaction and personal data that is retained by financial institutions for AML and CTF reasons, among others. This data is available to law enforcement, and other competent authorities such as the bank or government agencies, for law enforcement purposes. It is also monitored by banks themselves to meet anti-money laundering obligations. A CBDC would similarly allow bank, government and police access.

Data flows from digital transactions mean that these are much less private than cash transactions, even if they are retained under secure conditions for certain purposes.<sup>173</sup> This is because cash transactions do not generate data at all, making any data trail, even one that is well protected, inherently less private than cash transactions. By extension, treating CBDC transactions as on a par with private digital money, rather than physical cash, the digital pound would also be inherently less private than cash.

Digital pound wallets would be tied to some form of identifier, with greater levels of identity verification providing wallets with greater capabilities – however, the forms of identification and capability variance are still being discussed.<sup>174</sup> These identifiers would not be shared with the bank when transactions are recorded on the ledger, and the bank claims this will amount to anonymisation – however, as wallet providers will be able to reverse this, it will merely be pseudonymisation. Creating tiered levels of access to money in exchange for increasing amounts of identification would amount to a discriminatory identity paywall that would most affect migrants, ethnic minorities, older people, and poorer people, who are least likely to hold advanced forms of ID.

The consultation document also raised the prospect of digital pound customers being

171 Section D1, The Digital Pound Consultation Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>  
172 Section D2, The Digital Pound Consultation Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>  
173 Ibid  
174 Ibid

able to effectively pass on greater amounts of personal data to wallet providers, or other third parties, in exchange for access to greater benefits or additional services. This would create the danger of higher levels of privacy effectively becoming a luxury for those who can afford it.

The BoE claims that it is open to exploring ways for a limited number of small-value transactions to have enhanced privacy protection but it appears to veer away from suggesting total anonymisation even for these transactions, suggesting that a CBDC will always be less private than cash.<sup>175</sup>

#### *Programmability*

The BoE is considering how programmability could be used in the digital pound ecosystem. It has outlined how wallet providers could allow users to execute smart contracts, i.e. to make payments when certain conditions are met.<sup>176</sup> More disconcertingly, the BoE also mentioned the potential for programmable money, whereby users could limit spending on certain products. The example given is blocking spending on gambling, which may be a virtuous goal, but the introduction of wider capabilities on how digital currency is spent creates a risk of financial control either where third parties have access to someone's finances, or if the state looks to introduce controls on CBDC spending.

In the Technology Working Paper on the digital pound the BoE suggested that third parties, such as wallet providers, would be the driving force behind any programmability with the British CBDC.<sup>177</sup> It may even be that programmable functions are separate from the core CBDC ledger, depending on the architecture of the system.

At present, the BoE states that it will not develop or implement functions where the central bank can program the digital currency.<sup>178</sup> Instead, the bank appears to be looking at how a CBDC could enable smart contracts or user-enabled programmability, such as automated savings. While this statement is welcome it will be important to assess how any programmable capabilities in a future digital pound, developed by the bank or third parties, could be abused by state or private actors with malevolent intent, to ensure that capabilities with well-intentioned ends cannot be repurposed.

<sup>175</sup> Section D2, The Digital Pound Consultation Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>

<sup>176</sup> Section B, The Digital Pound Consultation Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf>

<sup>177</sup> Technology Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf>

<sup>178</sup> Technology Working Paper, The Bank of England, 7th February 2023, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf>

Sir John Cunliffe

Bank of England CBDC Taskforce Co-Chair

“You could think of smart contracts in which **the money would be programmed** to be released only if something happened.

“You could think of giving your children pocket money, but **programming the money** so that it couldn't be used for sweets. There is a whole range of things that money could do, **programmable money**, which we cannot do with the current technology.”

# Policy Analysis

CBDCs are a venture fraught with significant risks. The introduction of a centralised digital currency stands to dramatically reshape the entire financial landscape, posing a threat to various human rights and fundamental freedoms, all while incurring substantial costs. A particular cause for concern lies in the potential for widespread population surveillance and intrusions on privacy, as well as exacerbating existing inequalities. Given the magnitude and gravity of these risks, the burden of proof for CBDCs to demonstrate substantial benefits over the current financial system is considerable. However, central banks have yet to present a compelling case for CBDCs as a viable solution to any existing problem. Even the alleged benefits suggested in various design papers and consultations have failed to convincingly outweigh the plethora of potential harms that CBDCs could entail.

Government responses to the question of CBDC benefits have often cited the declining use of cash and financial inclusion as justifications for CBDCs but have not substantiated why CBDCs are the most suitable means to achieve these objectives. The lack of a clear vision or rationale behind current proposals raises questions about the motivations of central banks in pursuing their own digital currencies. Many proposals justify their endeavours by referring to international interest in digital currencies. In the absence of a clear benefit that CBDCs will bring to the public, it seems that they are being used as part of the global innovation race.

As central banks continue their exploration of CBDCs, multiple independent inquiries have failed to identify any urgent need for a national CBDC. Our analysis agrees with the findings of the UK's Economic Affairs Committee, which deemed a UK CBDC a "solution in search of a problem".<sup>179</sup> In the absence of a compelling benefit, CBDCs appear to be a misguided venture that would expand surveillance while offering little – if any – value to the general public. Policymakers must seize the advantage of the early stages of these plans to push back against the introduction of a UK CBDC, as the disproportionate harms it could bring have yet to be justified by any discernible benefit.

## Privacy

### *CBDCs and surveillance*

Central bank digital currencies present a series of unique privacy challenges. Even if they do not completely replace physical cash, their widespread adoption will generate large volumes of data from everyday, seemingly innocuous, transactions. As of yet, no

<sup>179</sup> Central bank digital currencies: a solution in search of a problem?, Economic Affairs Committee, 13 January 2022: <https://publications.parliament.uk/pa/ld5802/ldselect/ldeconaf/131/131.pdf>

governments have proposed a totally anonymous CBDC. This has been done on the basis that identification and surveillance of digital transactions are proportionate measures to address risks of money laundering, drug trafficking and terror financing. However, creating the centralised infrastructure in which identity-related information is connected with financial activities could empower governments to create detailed profiles of the public, escalating the likelihood of population surveillance. As the old adage goes, knowledge is power. Even within democratic systems, the sheer volume of data being generated risks creating an environment in which the state has intimate knowledge of an individual's identity, income, and financial transactions. To illustrate – if someone buys a large quantity of chocolate in cash, no one would know the nature of their purchase. However, if the same individual uses a CBDC for the transaction, their identity could be linked with the purchase and these details shared with a health insurer.<sup>180</sup> This would be an irreversible intrusion on individuals' privacy and disproportionate to the policy aims underpinning the development of this new form of currency. Any system based on centralised oversight of individuals' private lives runs the risk of expanding surveillance. It is imperative that CBDCs do not become a mass surveillance tool; a "digital Leviathan".<sup>181</sup> Any utilisation of CBDCs for surveillance would engage privacy rights and principles, challenge the core political culture of democratic states, and redefine the relationship between government and the public.

CBDCs inherently lend themselves to surveillance by generating individuals' financial data that would otherwise not exist in a centralised format, increasing opportunities for state oversight in the process. While electronic payments made between commercial banks can already be monitored, governments generally need to request this information from banks. In the UK, for instance, authorities must issue banks with a "third-party notice" for data access, a process involving lengthy procedures and potential court involvement.<sup>182</sup> A CBDC would likely remove such barriers that impede routine transaction monitoring. Even if states claim they will not be able to view transactions, this often refers to future privacy policy decisions rather than a privacy-by-design design decision that would make it technically impossible to view transactions (i.e. system infrastructure would not allow access). In the case of the former, such claims require scrutiny, particularly given the existing legal environment of extensive surveillance powers and financial regulations. Good intentions offer little protection in a world in which mass surveillance is increasingly normalised. Even democratic states have chilling track records of engaging in expansive surveillance. For instance, the UK was found to have led decades-long mass surveillance programs to capture citizens' private communications, unlawfully and without even parliament's knowledge.<sup>183</sup>

<sup>180</sup> Ibid

<sup>181</sup> Ibid

<sup>182</sup> Central bank digital currencies risk becoming a digital Leviathan, Andrea Baronchelli, Hanna Halaburda and Alexander Yetyelboym, *Nature and Human Behaviour* 6(7), 2022: <https://ora.ox.ac.uk/objects/uuid:23234634-dd99-4460-8b06-6570b9c66dc0>

<sup>183</sup> UK mass surveillance found unlawful by Europe's highest human rights court, Big Brother Watch, 25th May 2021: <https://bigbrotherwatch.org.uk/2021/05/uk-mass-surveillance-found-unlawful-by-eu-ropes-highest-human-rights-court/>



The UK has a particularly pernicious history of engaging in financial surveillance, and there is a complex net of legal frameworks conferring various powers to authorities to collect information in relation to the prevention and detection of welfare and tax fraud.

The Department of Work and Pensions (DWP) has been criticised for spying on people in the welfare system through excessive surveillance techniques, including calling upon private companies to hand over individuals' transaction data.<sup>184</sup> The Regulation of Investigatory Powers Act (RIPA) 2000 enables the DWP and local authorities to authorise covert, directed surveillance where it is deemed necessary and proportionate for the purposes of preventing or detecting crime. Under the Social Security Administration Act 1992 (SSAA), DWP-authorized officers have powers to request information for the purpose of investigating offences connected with all social security payments (including tax credits). It also gives local authority officers powers to request information for the purpose of investigating offences connected with Housing Benefit, Council Tax Benefit, Income Support, Jobseekers Allowance, Incapacity Benefit, State Pension Credit and Employment Support Allowance.<sup>185</sup> The subsequent Social Security Fraud Act 2001 further amended the powers for the DWP and local authorities to obtain information, including bank statements, from specified persons and organisations about their customers to help detect benefit fraud.<sup>186</sup> Section 68 of the Serious Crimes Act 2007 enables public authorities to share data with third parties in relation to fraud.<sup>187</sup> The Welfare Reform Act 2012 authorises HMRC officers to exercise information seeking powers under the SSAA. A refusal to comply with a request for information under these provisions is a criminal offence under the SSAA.

Further, the Investigatory Powers Act 2016 consolidates powers available to authorities to covertly obtain communications data, conduct interception, and to gather 'bulk personal datasets' (BPDs) of information, with various criminality thresholds required to access the data. BPDs are defined as "a set of information that includes personal information relating to a number of individuals where the nature of the set is such that it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service."<sup>188</sup>

Other examples of existing financial surveillance include the Home Office's use of state-issued smart (debit) cards ('Aspen' cards) to monitor the day-to-day spending and movements of asylum seekers, data from which was used against individuals to contest

184 DWP uses excessive surveillance on suspected fraudsters, report finds, The Guardian, 14 February 2021: <https://www.theguardian.com/society/2021/feb/14/dwp-excessive-surveillance-on-suspected-fraudsters-privacy-international>

185 Prosecuting welfare and health fraud cases – CPS, September 2019: <https://www.cps.gov.uk/legal-guidance/prosecuting-welfare-and-health-fraud-cases>

186 Code of practice on obtaining information: Social Security Fraud Act 2001 – DWP, 8 November 2016: <https://www.gov.uk/government/publications/social-security-fraud-code-of-practice-on-obtaining-information/code-of-practice-on-obtaining-information-social-security-fraud-act-2001>

187 Serious Crime Act 2007, s.68: <https://www.legislation.gov.uk/ukpga/2007/27/section/68>

188 Investigatory Powers Act 2016, s(7)(1)(b): <https://www.legislation.gov.uk/ukpga/2016/25/part/7/enacted?view=plain>

their asylum claims, destitution status, and to make people ineligible for financial support and shelter.<sup>189</sup>

In 2022, the DWP announced that the government will seek to further expand legal powers to investigate potential fraud, including by investigating crypto assets.<sup>190</sup> A centralised currency system would make it much easier for public authorities to directly access and passively monitor this kind of data, particularly in combination with the expansive powers that law enforcement, anti-fraud, and intelligence agencies already possess. If there were significant public uptake of CBDCs, there is a high risk that the centralised financial data generated could be harnessed for bulk surveillance purposes, impacting millions of people who are not suspected of any crime and broadly without their knowledge.

A UK CBDC would not just tempt surveillance – it could legally require it. The Bank of England has said that a CBDC would need to comply with anti-money laundering (AML) and counter-terror (CT) regulations, and that privacy features would be subject to meeting compliance requirements and government objectives in relation to financial crime.<sup>191</sup> In order to be compliant with AML/CT law, commercial banks are required to conduct identity checks and routine financial surveillance. The main AML laws in the UK are the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Money Laundering Regulations 2017), in addition to the Financial Service and Markets Act 2000, Terrorism Act 2000, Anti-Terrorism, Crime and Security Act 2001, Counter-Terrorism Act 2008, Proceeds of Crime Act 2002, and the Financial Conduct Authority (FCA) Handbook for FCA regulated firms. Under the Proceeds of Crime Act, financial institutions must monitor transactions in the instance of 'reasonable grounds for suspicion of criminal activity' and report any suspicious activity.<sup>192</sup> The Money Laundering Regulations (2017) require banks to perform Know Your Customer (KYC) checks, which refer to the process of identifying and verifying a customer's identity. The AML Regulations inform the primary objectives of KYC and Customer Due Diligence (CDD) checks, which require a company engaging in a new business relationship with a customer to:<sup>193</sup>

189 Big Brother says 'No': Surveillance and income management of asylum seekers through the ASPEN Card, Privacy International, 16 October 2019: <https://privacyinternational.org/long-read/3259/big-brother-says-no-surveillance-and-income-management-asylum-seekers-though-aspen>

190 Fighting fraud in the welfare systems – DWP, May 2022: <https://www.gov.uk/government/publications/fighting-fraud-in-the-welfare-system/fighting-fraud-in-the-welfare-system--2>

191 The digital pound: a new form of money for households and businesses?, Bank of England and HM Treasury, February 2023: <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultationworking-paper.pdf?la=en&hash=5CC053D3820DCE2F40656E772D-9105FA10C654EC> 53.

192 'Know your customer' guidance, Department for Levelling Up, Housing & Communities, 4 October 2016: <https://www.gov.uk/government/publications/know-your-customer-guidance/know-your-customer-guidance-accessible-version>

193 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (s28): [https://www.legislation.gov.uk/uksi/2017/692/pdfs/uksi\\_20170692\\_en.pdf](https://www.legislation.gov.uk/uksi/2017/692/pdfs/uksi_20170692_en.pdf)



- a) Identify the customer
- b) Verify the customer's identity
- c) Understand the customer's activities and source of funding
- d) Regularly monitor the customer's activities

These objectives simultaneously require individuals to provide personal information to banks, and for providers to engage in financial surveillance in which they are obliged to inform fraud prevention, debt recovery and law enforcement agencies of suspicious activities.<sup>194</sup> The FCA also provides guidance that firms must "have in place policies and procedures in relation to customer due diligence **and monitoring**" (emphasis added).<sup>195</sup> There is no prescribed method for CDD procedures or monitoring, which leaves a relatively broad scope for interpretation. Banks must perform KYC checks when an account is first opened and are required to regularly re-verify their KYC information at least annually for high-risk customers and every two to four years for medium and lower risk customers. Part of this review can include transaction monitoring. In a CBDC system this means that transactions must be traceable to some degree so that KYC checks can be performed on account holder records.

It is mandatory for banks and businesses to conduct KYC/CDD tests on customers in accordance with spending amounts in certain contexts. Identification and verification is required if a person spends over £2,000 on gambling, for instance.<sup>196</sup> If CBDCs are to be treated as analogous to cash, it would follow that these rules would apply to a digital pound. It remains to be seen whether enhanced KYC checks would be extended beyond current contexts into other industries or for certain items, and if they would be required for purchases over a certain sum.

We have yet to see how law enforcement and other public authorities would interact with a CBDC, or how existing laws and exceptional circumstances could be leveraged to exploit a new system for surveillance purposes. However, we know that there is currently an established and expansive system that engages the public's privacy rights in the name of tackling financial crime. While the current intention may not be tracking and surveillance, existing law would require it to a great degree, and there is no way to know how future governments, bad actors, or exceptional circumstances will impact how these systems are used. This is not to suggest that such events are guaranteed to happen. However, the malleable nature of CBDC systems coupled with the historical evidence of state surveillance practice indicates that such circumstances are entirely possible, if not

<sup>194</sup> "Know your customer" guidance, Department for Levelling Up, Housing & Communities, 4 October 2016: <https://www.gov.uk/government/publications/know-your-customer-guidance/know-your-customer-guidance-accessible-version>

<sup>195</sup> Money laundering and terrorist financing, Financial Conduct Authority, 21 February 2023: <https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing>

<sup>196</sup> The prevention of money laundering in combating the financing of terrorism, Gambling Commission, 30 May 2023: <https://www.gamblingcommission.gov.uk/guidance/the-prevention-of-money-laundering-and-combating-the-financing-of-terrorism/prevention-of-ml-and-combating-the-financing-of-terrorism-part-6-8-threshold-approach>

probable.

### *Privacy by design*

The global drive to develop CBDCs raises a series of concerns around the appropriate degree of privacy that should be integrated into CBDC systems. International privacy law requires states to consider a certain set of binding standards, which should be considered when developing and determining national CBDC policies.<sup>197</sup> Unfortunately, these global privacy minimum standards have not been well reflected in many of the plans to develop a new central digital currency.

Privacy by design and default should be a central element for developing new technologies. However, the majority of CBDC projects have made user privacy a relatively low priority, often only paying lip service to the concept. Aside from complying with privacy laws and ensuring public acceptance of a new digital currency, central bank remits mean they generally lack an incentive to issue a CBDC with a strong focus on privacy. Pilots including Jamaica's Jam-Dex, Uruguay's e-Peso and Nigeria's eNaira would not be anonymous and would allow, under certain requirements and to different extents, for this data to be accessible in a de-anonymised format.

The design paper for the Nigerian eNaira claimed to prioritise privacy but failed to provide specific details of any protective measures. The promises of privacy are largely undermined by the eNaira's architecture - as an account-based CBDC it cannot offer the same level of privacy as a token-based system. Critics have also raised concerns about Nigeria's adherence to its own data protection laws, which raises a series of legal questions about how the minimal data protections will be complied with.

The Bank of Israel states that it will not allow "absolute" privacy despite acknowledging the array of risks associated with CBDCs. Instead, it offers various levels of privacy and suggests that privacy levels in relation to intermediaries will be customisable, with private companies being able to offer access to auxiliary services based on the level of data a user provides. This raises concerns about privacy being treated as a commodity that is tradeable for increased economic access or extra privileges, depending on the limitations set. Indeed, the Bank of Israel only affords substantial privacy protections to an extremely limited amount of small transactions, referred to as "private shekels". Although there is limited information on this in the consultation, it is clear that policymakers would set the budget of this less-traceable token. It's possible that policy could dictate which users are afforded anonymity, which risks politicising or weaponising privacy in the process.

<sup>197</sup> See for example International Covenant on Civil and Political Rights, 16th December 1966, art. 17: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>; Universal Declaration of Human Rights, 10th December 1948, art. 12: [https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A\\_RES\\_217\(III\).pdf](https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_217(III).pdf); General Data Protection Regulation, 2018: <https://gdpr-info.eu/>.

The architecture of centralised digital currency rings alarm bells for privacy and data rights. The two main systems – account-based and token-based – offer differing levels of privacy, yet both allow central banks some degree of access to the public’s financial data and sensitive information. Account-based CBDCs pose the more severe threat to privacy as they require the central clearing party (the bank) to verify each transaction. This process would normalise the mass surveillance of all bank transfers within the system. In contrast to the current system where multiple private banks collect customer information in a segmented way, this infrastructure would centralise a substantial amount of sensitive data. This would significantly increase opportunities for governments to access and interfere with sensitive financial data.<sup>198</sup> In the event of a state retiring its physical currency – something we must consider in the creep towards cashless societies – an account-based CBDC could grant public authorities unrestricted access to all transactions, raising serious concerns about privacy and surveillance.

Token-based systems, while recognised as more privacy-friendly, can still be exploited for surveillance purposes. The main difference between token-based and account-based system lies in the verification process. Account-based CBDCs rely on intermediaries to verify user-identities, whereas token-based CBDCs use tokens that are verified by the receiver. However, it’s important to note that data generated through identifying tokens and reference numbers, in projects like Uruguay’s e-Peso and Sweden’s e-Krona, could allow a CBDC to be traced. Sweden verifies CBDC tokens via validation nodes which naturally increases traceability, as it authenticates that a token has not already been used. Traceable tokens could support states in monitoring financial activities or tracking spending behaviour. In addition to the problems this raises for surveillance, it would be difficult to reconcile traceability functions with the obligations of financial institutions to keep sensitive customer information confidential, such as personal identification, financial records, and transaction history.

An important design decision in CBDC architecture is the choice between a traditional centralised ledger and distributed ledger technology (DLT), which distributes specific functions to other providers. DLT platforms come in two formats: open, where anyone can participate in validating transactions, and permissioned, where participation is restricted to approved parties. Opting for a DLT-based platform means that the central bank does not have to hold any private data. However, decentralising this power means that ledger access is outsourced to third parties, and central banks make decisions regarding who can access the ledger and the associated user data.<sup>199</sup> Relying on DLT requires a central bank to trust external parties with ledger access and management, potentially introducing vulnerabilities and dependencies. Although DLTs are the preferred platform for privacy concerns, it is essential to acknowledge that they are not without their challenges.

198 The Privacy Cost of Currency, Karin Thrash, Michigan Journal of International Law 42(2), 2021:

<https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2111&context=mjil>

199 Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs), G7, 2021: [https://www.mof.go.jp/english/policy/international\\_policy/convention/g7/g7\\_20211013\\_2.pdf](https://www.mof.go.jp/english/policy/international_policy/convention/g7/g7_20211013_2.pdf)

## Data rights

The development of new technologies for public sector use must be done in accordance with existing data protection rules. Approaches to privacy with a CBDC will naturally vary with national laws and regulations. These legal frameworks vary in comprehensiveness, the level of protection they afford, and the extent to which they are enforced. Citizens in regions where data protection frameworks are less stringent may find the data generated through their daily activities subject to lower levels of protection, especially in a cashless society where such data becomes unavoidable.

It is crucial to remember that legal frameworks are subject to change. The UK is currently overhauling its data protection regime<sup>200</sup> with legislative reforms that will increase its information sharing powers, weaken data rights and facilitate the flow and use of personal data for law enforcement and national security purposes. This would increase the extent of data processing permissible in a variety of ways that would impact a CBDC system.

The UK’s CBDC proposal claims that the government would not be able to access the public’s CBDC data. Indeed, processing personal data in the UK is currently only lawful if it is performed for at least one lawful process, which is then subject to a balancing test that weighs the purpose for processing against the interests or fundamental rights of the data subject. However, the Data Protection and Digital Information (No.2) Bill (DPDI Bill) introduces the concept of ‘recognised legitimate interests’, which will allow for data to be processed without a legitimate interests balancing test. The examples of recognised legitimate interests provided are incredibly broad, including national security, public security and defence, emergencies, crime, and even direct marketing. Given the far-reaching nature of these categories, it would be entirely possible for the data generated by CBDCs to be processed beyond its original purpose without the account holder’s knowledge or consent. In the instance that existing recognised legitimate interests are not vague enough to justify data processing, the Bill empowers the Secretary of State to add further recognised legitimate interests via secondary legislation. These could be added to this list at any time and for any reason with minimal parliamentary scrutiny, facilitating the flow and use of personal data for limitless purposes and in a way that is subject to shifting political will. This power could easily be used to leverage data to surveil the public and in a way that would disproportionately impact marginalised groups who already suffer from disproportionate data collection and processing practices, such as migrants and people in the welfare system. If the Bill is passed in this form, the change in data protection rules would allow larger quantities of data to be legally processed than current frameworks allow, which could risk a grave intrusion upon user privacy in the context of CBDCs.

200 Briefing on the Data Protection and Digital Information 2.0 Bill for House of Commons Committee Stage, Big Brother Watch, May 2023: <https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Big-Brother-Watch-Briefing-on-the-Data-Protection-and-Digital-Information-2.0-Bill-for-House-of-Com-mons-Committee-Stage.pdf>

The combination of granular population data and a lack of clear data protection principles creates a perfect environment for the wholesale collection and linking of data to user profiles by public authorities, private companies, or even malicious actors. Beyond revealing transaction information, CBDCs could be harnessed to track spending and saving patterns, reveal identity details, and track location data. This could facilitate the development of comprehensive CBDC user profiles. Any system generating such vast quantities of sensitive information runs the risk of potential abuses or function creep, where data is repurposed beyond its original intent. Even if governments do not use the data themselves, the granular user records would be highly valuable to private companies or skilled hackers.

Offering personal data to private companies without consent is not unprecedented. The UK in particular has a track record of marketing data which includes the National Health Service sharing patient records without proper consent;<sup>201</sup> HMRC initiatives designed to sell off taxpayers' data to private companies;<sup>202</sup> and data relating to school pupils being made available for use by private companies.<sup>203</sup> CBDCs would offer vast amounts of data that could be similarly leveraged without the public's consent. Depending on data flows and the roles various entities play in CBDC systems, privacy breaches and flaws could manifest within various design options. Given these risks, it was bizarre that the UK consultation considered what would be done with CBDC data as a matter to be decided "in due course".<sup>204</sup> It does not outline exactly what data will be collected, how third party organisations will integrate and provide security, who collects, stores, and analyses user metadata, whether the data will allow for targeted marketing or ads, etc. Answers to these questions are key to determine the degree of privacy a CBDC user would have. It is disappointing and concerning not to see this explicitly addressed in the UK's current CBDC plans, particularly given the changing landscape of data rights.

### *Programmable money*

Programmable money consists of a CBDC with predefined rules governing its use, potentially granting governments not only insight into public transactions but also the power to influence and shape individuals' spending habits. In the worst case scenario, programmability features could enable complete government control over how money is spent. CBDCs could be programmed to include spending directives or expiration dates,

201 DeepMind faces legal action over NHS data use, BBC, 1st October 2021: <https://www.bbc.co.uk/news/technology-58761324>

202 HMRC wants to share taxpayer data with private companies, Wired, 19th April 2014: <https://www.wired.co.uk/article/hmrc-selling-off-data>

203 Government offers school pupil data to private companies, Wired, 25th April 2014: <https://www.wired.co.uk/article/national-pupil-database>

204 Bank of England and HM Treasury, 'The digital pound: a new form of money for households and businesses?' (February 2023): <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultationworking-paper.pdf?la=en&hash=5CC053D3820DCE2F40656E772D-9105FA10C654EC> 53

equipping governments with the ability to shape people's financial behaviour in line with policy objectives or law enforcement purposes. These features raise fundamental questions about the extent of influence and control governments wield over individuals' lives.

The process could begin innocuously. The head of the UK's CBDC taskforce himself suggested that parents could have the power to allocate pocket money with restrictions on specific purchases like sweets.<sup>205</sup> However, this functionality could open the door for a world in which governments dictate how CBDCs are spent – in extreme circumstances, for example, welfare recipients could be limited to buying essential food and healthcare items, or people with asthma could be unable to purchase cigarettes. US SNAP cards offer an example of how spending can be shaped. SNAP cards are state-issued pre-paid cards for welfare recipients to spend on essential food items with restrictions on what types of food the holder can purchase.<sup>206</sup> In severe scenarios where the spender is limited in what they can purchase, the scope of restrictions could extend to various facets of life from unhealthy food to travel. At their worst, CBDCs could be used as a tool of digital authoritarianism, a way to exert total control over the public's transactions. This could result in financial censorship without due process or avenues for recourse, which would be likely to disproportionately impact marginalised groups. These risks are not explicitly posed by any proposal thus far, but demonstrate what could happen in a worst case scenario.

Even in cases where programmability is introduced with seemingly reasonable intentions, such as conditional payments, it still generates substantial volumes of data. This creates significant operational risks. Designs that allow programmability functions could cause serious security issues. For example, some experts say that smart contracts used in architectures for processing programmable money would make it possible for hackers to exploit their security vulnerabilities. This could render national CBDC systems vulnerable to attacks that could disrupt the economy and threaten national security.<sup>207</sup> Given the severity of such potential risks, there is a pressing need to clarify the legality of programmability and the scope in which it should be introduced in CBDCs to prevent ambiguities, misuse, or abuse of its functions.

### *Inclusion or exclusion?*

Financial exclusion refers to the inability, difficulty or reluctance to access mainstream financial services which, if left unaddressed, can exacerbate social exclusion, poverty

205 'Bitcoin': Bank of England seeks views on economic impact – Ian King, Sky News, 7 July 2021: <https://news.sky.com/story/britcoin-bank-of-england-seeks-views-on-economic-impact-12327110>

206 Supplemental Nutrition Assistance Program (SNAP), U.S. Department of Agriculture, 17th November 2017: <https://www.fns.usda.gov/snap/eligible-food-items>

207 CBDC - How Dangerous is Programmability?, Patrick McConnell, The FinReg Blog, 21st September 2021: <https://sites.duke.edu/thefinregblog/2021/09/21/cbdc-how-dangerous-is-programmability/>



and inequality. Many CBDC programs, including the UK's proposal, cite the promotion of financial inclusion as a key motivation for developing a central digital currency. While this is an important goal, it is neither clear nor convincing how CBDCs would be the most appropriate means to achieve it. The UK's situation is different from many developing countries pushing for a CBDC, where larger parts of populations may be unbanked and rely heavily on cash. The Financial Conduct Authority estimates that 2.1 per cent of UK adults are unbanked compared to, for example, the estimated 55.2 per cent in Nigeria.<sup>208</sup> More broadly, the 2023 Global Financial Inclusion Index ranked the UK as 7th for its financial inclusion score.<sup>209</sup> This is not to say that the UK does not have issues of financial exclusion that need addressing, but rather to demonstrate that the scale of the problem suggests that introducing a CBDC and its corollary harms is a very different equation in the UK compared to some less economically developed countries. Further, there are more straightforward and efficient ways to support access to financial services without completely overhauling the entire financial landscape at the expense of the public's privacy. Such measures may include ensuring continued access to cash, upholding the integrity of cash infrastructure, improving financial and digital literacy, and supporting local and community-based methods of access to cash.

Proponents consider CBDCs to be inclusive as they offer a banking option that is supposedly widely available. However, the new digital currency will predominantly be operated via smartphones. This raises clear issues for accessibility and inclusion for people who cannot afford a smartphone; elderly people without a smartphone or with low levels of digital literacy; people who choose not to use a smartphone; or people with physical disabilities that impair smartphone use. Other access issues will arise for countries with more rural communities, increased poverty, or gender gaps in smartphone ownership. Some CBDC proposals, such as the digital euro, have attempted to address accessibility issues by vowing to facilitate transactions without an internet connection. However, it is likely that there would be payment caps and limitations on this function, which would continue to disadvantage already digitally marginalised groups. It is also important to consider that if a CBDC is being targeted towards groups that typically face financial exclusion, this will create a system which processes their data excessively. If such data were then to be misused or abused by state or non-state actors, it would disproportionately harm marginalised individuals and groups.

The UK's proposal states that CBDCs are designed to sit alongside cash rather than replace it. However, it must be recognised that cash is declining in availability, use, and its infrastructure.<sup>210</sup> It has been established that CBDCs are a less private alternative to

208 Financial Lives 2022: Key findings from the FCA's Financial Lives May 2022 survey, 26 July 2023: <https://www.fca.org.uk/publication/financial-lives/financial-lives-survey-2022-key-findings.pdf>; Nigeria's Financial Inclusion: The Way Forward, Joshua Okoduwa and Nene Odiboh, KPMG, August 2021: <https://assets.kpmg.com/content/dam/kpmg/ng/pdf/nigerias-financial-inclusion-the-way-forward.pdf>  
 209 Global Financial Inclusion Index 2023: [https://secure02.principal.com/publicsupply/Get-File?fm=WW1074&ty=VOP&EXT=.VOP&\\_gl=1\\*1rj3sq\\*\\_ga\\*MTAwNTc1MDc3Ni4xNjk2NDlwMjI4\\*\\_ga\\_GP3ZP21MGH\\*MTY5NjQyMDIyOC4xLjAuMTY5NjQyMDIyOC4wLjAuMA..](https://secure02.principal.com/publicsupply/Get-File?fm=WW1074&ty=VOP&EXT=.VOP&_gl=1*1rj3sq*_ga*MTAwNTc1MDc3Ni4xNjk2NDlwMjI4*_ga_GP3ZP21MGH*MTY5NjQyMDIyOC4xLjAuMTY5NjQyMDIyOC4wLjAuMA..)  
 210 Statistics on access to cash, bank branches, and ATMs, Lorna Booth, House of Commons Library, 1

physical cash but it could become the primary method of payment as society moves closer towards being cashless. In light of this, it is important to consider the equalities impacts that a less privacy-preserving payment method would have. Financial control is a key feature of abuse and gender-based violence in relationships. For survivors of domestic abuse, most of whom are women, cash is a lifeline.<sup>211</sup> It allows individuals at risk to make anonymous and untraceable payments to prevent their abusers from tracking them. In the absence of a cash option that allows this level of privacy, individuals could be put at increased risk in already very dangerous situations. Indeed, monitoring phone usage and access is another method of coercive control.<sup>212</sup> If an individual could not access their smartphone and cash were not readily available, it would be very difficult for them to leave a controlling relationship or exercise financial freedom. These examples are just two of many possibilities to highlight the kinds of potential consequences that new technologies can have. If the case were made for a UK CBDC (which we have yet to see), it is vital that it would be developed with equality, ethical, and human rights impact assessments to properly explore and seek to mitigate the consequences of a CBDC throughout its lifecycle.

It is crucial to consider how CBDCs would, or would not, address the systemic issues that underlie financial exclusion. Many states still have a significant number of unbanked individuals and households, as illustrated by the case of Israel, where over one million Israelis lack a bank account. There are various reasons as to why people remain unbanked. Some prefer the cash economy and the benefits it provides, such as increased privacy. Some may not have a local or easily accessible bank, especially as banks continue to close local branches.<sup>213</sup> Others may distrust banks.<sup>214</sup> In a time of generally low trust in governments, people may be even more hesitant to trust central banks.<sup>215</sup> Indeed, a survey found that the British public's attitude towards a UK CBDC was one more of suspicion than excitement.<sup>216</sup> Other barriers to financial inclusion include a lack of appropriate identification documentation or secure immigration status, which both prevent someone from opening a bank account. Each of these issues stem from privacy concerns, limitations in cash infrastructure, public trust crises, and issues with identification - none of which a CBDC would resolve. Instead of addressing these concerns, a new CBDC is likely to exacerbate them.

Many CBDC proposals and pilots claim to be inclusive by providing different levels

September 2023: <https://commonslibrary.parliament.uk/research-briefings/cbp-8570/>  
 211 Domestic abuse charity urges government to stop cash machine closures to protect victims, The Independent, 5 May 2022: <https://www.independent.co.uk/news/uk/politics/cash-machine-closures-economic-abuse-domestic-refuge-b2072403.html>  
 212 <https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/coercive-control/>  
 213 Almost half of the UK's bank branches are gone – it's now or never to halt the cash crisis, Josh Wilson, Which?, 26 April 2022: <https://www.which.co.uk/news/article/almost-half-of-the-uks-bank-branches-are-gone-its-now-or-never-to-halt-the-cash-crisis-ag6B83o1AWKd>  
 214 Edelman Trust Barometer 2022: Trust in Financial Services Sector, Edelman: [https://www.edelman.com/sites/g/files/aatuss191/files/2022-03/2022%20Edelman%20Trust%20Barometer\\_Trust%20in%20Financial%20Services.pdf](https://www.edelman.com/sites/g/files/aatuss191/files/2022-03/2022%20Edelman%20Trust%20Barometer_Trust%20in%20Financial%20Services.pdf)  
 215 Edelman Trust Barometer: Navigating a Polarized World - Social fabric weakens amid deepening divides, Edelman: <https://www.edelman.com/trust/2023/trust-barometer>  
 216 <https://www.politico.eu/article/cryptocurrency-survey-uk-central-bank-digital-currency-fintech/>



of banking access based on the amount of identification a customer can provide. For instance, users with less identification have lower limits on their CBDC holdings and daily transaction allowances, as seen in the eNaira and the UK proposal. While this is presented as inclusive, it is quite the opposite. Different limits will result in citizens having tiered access to money based on the amount of personal data they are willing to share. This could effectively press-gang individuals into exchanging their data for economic participation, often without a clear understanding of who will use it or for what purposes. Instead of respecting user privacy rights, this approach creates a barrier for individuals with limited identification, particularly impacting those who are financially excluded or unbanked as they already face challenges in providing proof of identity. This could further hinder people's ability to save, spend, and improve their financial wellbeing, potentially leading to social exclusion and difficulties in securing employment; especially if employers are able to opt to pay solely into CBDC accounts. In this way, CBDCs could extend financial exclusion rather than improve it.

### *Digital identity*

CBDCs are inherently incompatible with privacy. Research suggests that issuing such currencies without a comprehensive national identity system would be difficult, if not "nigh on impossible".<sup>217</sup> Transition to ID-based money raises critical considerations regarding user data, function creep, and the broader implications for personal freedoms and civil liberties.

Tying CBDCs to national digital identity systems raises a number of privacy and surveillance concerns. It is wholly possible that payments or access to services could be made conditional based upon identity. One can envisage a situation where programmability impacts the way in which money is spent. A serious example could be using CBDCs to geofence an individual by programming a person's funds to not work outside of a certain town or area, which could impact anyone from a person on house arrest, an asylum seeker, or even the entire public in the case of national travel lockdown in a pandemic. Even if not the current intention, models such as Nigeria's and Jamaica's that integrate a comprehensive digital ID system lay the groundwork for potential future exploitation by government; current or future. This level of government control is clearly incompatible with fundamental freedoms, but would be made much easier with a centralised link between finance and identity information.

As discussed, banks are obligated to adhere to identity checks for customer and transaction monitoring to meet KYC, AML, and CTF requirements. It would not be impossible in some CBDC designs for transaction histories to be linked to digital IDs and possibly other personal information, such as credit histories. If identity and transaction data were fused it would generate a wealth of highly sensitive information, effectively creating a national

217 Why CBDCs will likely be ID-based, Financial Times, 5th May 2021: <https://www.ft.com/content/88f47c48-97fe-4df3-854e-0d404a3a5f9a>

database of population behaviour. Such is the case in the eNaira pilot, which is linked to a user's personal data including their telephone number, banking number or national ID number, effectively creating a national biometric ID database. Although this may not be the intention of current administrations, this store of information would be ripe for exploitation and function creep - third party companies could access and exploit data for extensive profiling and marketing purposes, identity attributes could be leveraged by governments or third parties to make funds conditional, or successful hackers could exploit identity and financial data through a single point of failure. Combining digital identity with CBDCs would increase surveillance opportunities from both public and private actors, as well as introduce security vulnerabilities.

Beyond concerns of surveillance and security, implementing CBDCs with a digital ID system would redefine individuals' ability to access the economy, making it dependent on having both a digital identity and a CBDC. Individuals without such credentials or who do not want a digital ID could be left on the wayside, an exclusionary approach that would disproportionately affect digitally and financially marginalised individuals. Many people who primarily use cash may do so because they cannot provide the identification information to satisfy KYC requirements. For example, the eNaira requires a Bank Verification Number and National Identity Number for registration. Poorer people are less likely to have the documentation to support this and obtaining it can be a costly process in both time and money.<sup>218</sup> As this system is currently only accessible to people who already have bank accounts, it fails to support promote financial inclusion.

It is possible that CBDCs could introduce new digital ID capabilities such as biometric checking (e.g. fingerprint, voiceprint, facial recognition technology) for identity verification,<sup>219</sup> potentially leading to the disproportionate biometric data collection from marginalised groups who are unable to provide other forms of ID. Again, the Nigerian CBDC presents a worrying case study here. The eNaira offers a "Tier Zero" account for customers without an existing bank account and verified national insurance number. However, researchers who tried to open a Tier Zero account were asked to provide bank account details and biometric details; making the supposedly more accessible option more intrusive than a standard bank account.<sup>220</sup> Caveating economic access with the provision of digital identity information is ever more concerning when viewed within the broader context of the increasing digitisation of society, decline in cash use, and consequent shift towards a cashless society. With either no or low levels of physical cash, people may

218 Identity Documents, Welfare Enhancement, and Group Empowerment in the Global South, Wendy Hunter, *The Journal of Development Studies* 55(3): <https://www.tandfonline.com/doi/full/10.1080/00220388.2018.1451637>; Financial Services for the Poor: Lack of Personal Identification Documents Impedes Access, Nicola Jentzsch, *German Institute for Economic Research* 5(17): [https://www.econstor.eu/bitstream/10419/151056/1/diw\\_wr\\_2009-17.pdf](https://www.econstor.eu/bitstream/10419/151056/1/diw_wr_2009-17.pdf)

219 World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit*, January 2020: [https://www3.weforum.org/docs/WEF\\_CBDC\\_Policymaker\\_Toolkit.pdf](https://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf)

220 Central bank digital currencies risk becoming a digital Leviathan, Andrea Baronchelli, Hanna Halaburda and Alexander Yetyelboym, *Nature and Human Behaviour* 6(7), 2022: <https://ora.ox.ac.uk/objects/uuid:23234634-dd99-4460-8b06-6570b9c66dc0>

be compelled into using financial systems that require more data and offer lower levels of privacy protection than current systems. This undermines the core principle of financial inclusion that many CBDCs claim to uphold.

Given these risks, we would expect to see more discussion about how digital identities may or may not fold in to the development of a UK CBDC. Disappointingly, the consultation lacked much of this important information. Private sector companies would be responsible for “recording the identity of digital pound users”<sup>221</sup>, but there was no information regarding what would be done with this information or the safeguards surrounding such collection. Third party companies often seek to maximise public data collection, with sometimes disastrous consequences for privacy rights and public trust. The Facebook and Cambridge Analytica scandal, for instance, saw a political consulting firm build profiles on hundreds of millions of Facebook users without their knowledge.<sup>222</sup> These profiles were then exploited for persuasion purposes. A CBDC could grant third party companies with a similar avenue to develop extensive profiles on the population, which would be a highly valuable asset for interested parties. Any further work on a UK CBDC proposal must clarify the safeguards around the use of digital identities in order to rule out the risks that such a combination could pose.

#### *Legal developments and democratic involvement*

CBDCs are more than just a technological innovation. They raise fundamental questions about the concentration of state power and the potential expansion of digital surveillance, and will have profound political, economic, and social consequences. Given the extensive potential risks, it is vital that a strong case is made for CBDCs and that the benefits are demonstrated to be important enough to outweigh the costs, before proposals are developed any further. Should the case be made, any development must follow democratic processes including engagement, consultation, a democratic mandate, political scrutiny, and primary legislation. The risks of CBDCs and their ancillary functions, such as programmability, are too severe for mere promises to be an appropriate protection. Without being firmly grounded in legislation, and with no effective enforcement mechanisms or penalties in place, such commitments are easily reneged on and individuals would have nothing to hold governments accountable to. This would ensure that claims made in design papers – such as the UK’s claim that the Bank of England would not have programmability functions, or Nigeria’s pledge to treat privacy as paramount – are kept. If not, the assurances will remain just that: assurances.

221 The digital pound: a new form of money for households and businesses?, Bank of England and HM Treasury, February 2023: <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf?la=en&hash=5CC053D3820DCE2F40656E772D-9105FA10C654EC> 53.

222 Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, 17 March 2018, The Guardian: <https://www.theguardian.com/news/2018/mar/17/cambridgeanalytica-face-book-influence-us-election>

Should countries proceed with issuing a CBDC, it must be firmly grounded in a robust legal framework that protects the public’s right to privacy, equality, freedom of expression and property. Central banks should have a clear legal basis for issuing and distributing a central digital currency, which should be developed through public engagement and political scrutiny. Authorities must also establish a legal foundation for implementing a regulatory framework to ensure its safe roll out and use. However, mandates authorising CBDCs are not widely held at the time of writing. According to an IMF study, 61% of central bank laws limit the ability of currency issuance to banknotes and coins and only 23% of central bank laws allow for the direct issuance of a digital currency. In 16% of central bank laws, it is unclear whether creating a digital form of central bank currency is permitted.<sup>223</sup> This legal lacuna raises significant concerns about the legitimacy and accountability of many ongoing CBDC initiatives.

Any justification for an interference with privacy rights must be defined in law and in accordance with international human rights standards. While some policy objectives underpinning CBDCs may be considered lawful and legitimate, the extensive intrusion into and interference with privacy in payments strongly suggests a disproportionate outcome. The absence of a legal framework means that determining who should be held accountable in the event of CBDC system abuse (e.g. mass surveillance, data leaks or breaches, illegal sale of data, or theft by hackers) becomes a complex and uncertain matter. Consider the issue of which entity has liability for data rights in two-tier models. Users should have a clear understanding of what processes to follow should a claim need to be brought, but two-tier systems could fragment responsibility between the central bank and third party provider. This is a clear example of where greater clarity is needed, and such clarity should be enshrined in law.

The lack of a legal basis or appropriate framework may give rise to a multitude of issues with a democratic deficit, accountability, and the protection of individual rights at the forefront. Another area where legislation will be crucial is data protection, as many jurisdictions already have laws governing personal information processing. As a CBDC drastically increases the scope of citizens’s personal data processing by the public sector, it raises new policy considerations and legal questions around its safeguarding and use. Finally, it is also important that CBDCs are issued in states with a strong rule of law and robust institutions and regulators. As the IMF highlights, this is necessary “to ensure effective protection of rights and mitigate risks of corruption and fraud related to CBDC issuance and conversion”.<sup>224</sup>

223 Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations, Wouter Bossu, Masaru Itatani, Catalina Margulis, Arthur Rossie, Hans Weenink and Akihiro Yogshinaga, International Money Fund, 20th November 2020: <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827>

224 How Should Central Banks Explore Central Bank Digital Currency? A Dynamic Decision-Making Framework, Gabriel Soderberg et al, International Monetary Fund, September 2023: <https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/How-Should-Central-Banks-Explore-Central-Bank-Digital-Currency-538504#>

There have been some legal developments relating to CBDC development. The European Commission's regulatory proposal establishes the legal framework for a digital euro by introducing a draft law, and claims to incorporate privacy and data protection by design and default.<sup>225</sup> User data would be predominantly accessed and processed by the relevant Payment Service Providers, and the proposal claims that central banks would not be able to identify individual users or their financial activities and that they would only have limited access to encrypted data for specific functions and services. The regulatory proposal requires privacy preserving measures "to ensure that the European Central Bank and the national central banks cannot directly identify individual digital euro users".<sup>226</sup> This seems one of the more preferable approaches to privacy; however, still allows supervising banks and payment providers to identify individual users. This would make the system pseudonymous rather than anonymous, which means it would be technically possible to trace user activity using either technology, legal powers, or both. The ability to uphold privacy protections is only as good as the legislation that underpins them. Adopting this approach would still legally allow for users to be identified by other key parties, which may appear to be a relatively subtle distinction but retains the potential for user identification and data access.

The stealth introduction of a mass financial surveillance system would set a worrying precedent authoritarian regimes may follow, and CBDCs could become an instrument of state surveillance in democratic and non-democratic settings alike. In addition to direct harms from the growing digital panopticon and increased government monitoring, the threat of digital surveillance could undermine the stated purpose of a CBDC by harming its acceptance and uptake by the public.

#### *CBDCs in action: what's gone wrong?*

None of the CBDC programmes examined in this report has launched successfully. Several countries that have fully launched have reaped the consequences of launching a CBDC without a clear reason, resulting in low levels of public uptake. Any CBDC system is doomed to fail if there is not sufficient buy-in from the public. The UK proposal has yet to make a convincing case as to how a CBDC would directly benefit members of the public. When coupled with the array of privacy and surveillance risks, it seems unlikely that the public would voluntarily engage with a new digital currency in significant numbers, whether from lack of interest or lack of trust.

Jamaica, for example, has struggled securing widespread public uptake of Jam-Dex. Despite being fully launched, there is limited information available about the new currency. It is unclear whether this lack of transparency surrounding Jam-Dex, the speed

225 Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs), G7, 2021: [https://www.mof.go.jp/english/policy/international\\_policy/convention/g7/g7\\_20211013\\_2.pdf](https://www.mof.go.jp/english/policy/international_policy/convention/g7/g7_20211013_2.pdf)

226 Digital euro draft law: banks mandated to provide free services, Ledger Insights, 28th June 2023: <https://www.ledgerinsights.com/digital-euro-draft-law/>

at which it was released, or the public's attachment to physical cash caused a slow and reticent adoption. In response, the government offered both merchants and individuals financial incentives in exchange for using the CBDC.<sup>227</sup> Reliance on financial incentives to encourage broader adoption of systems that generates a vast amount of data raises questions about free consent. Where transaction information is tied to user identity, and in a country where data privacy and protection is "relatively understated", the questions grow louder.<sup>228</sup> Given the limited amount of publicly available system information, it is unclear whether users truly understand the details of what they are agreeing to upon signing up for Jam-Dex. This leads to consideration of the extent to which the government's financial incentives for CBDC participation could be deemed coercive. It is highly questionable that the public sees any inherent benefit to a CBDC when the only reason they use it is due to manufactured financial incentives.

Less than 0.5 per cent of Nigerians used the eNaira a year after its launch,<sup>229</sup> a rate deemed "disappointingly low" by the IMF.<sup>230</sup> Such low adoption rates may reflect a spectrum of public feeling toward the new currency, ranging from indifference to distrust. The eNaira's underwhelming rollout has led the Central Bank of Nigeria to enlist tech firms to develop a new national CBDC system only two years after its initial release.<sup>231</sup> While adoption rates have increased, this occurred during a national cash shortage crisis.<sup>232</sup> It would be inappropriate to consider this increase as a success or even fully consensual, as the cash crisis left many Nigerians with no other way to access their money. Instead, the eNaira experience paints a cautionary tale of CBDCs in cashless or low-cash societies, where people may be compelled to use such intrusive systems simply due to a lack of other options.

Some countries have found that there is no sufficiently convincing case to justify the greatly complex and costly process of developing a CBDC. During its development of the e-Krona, the Riksbank acknowledged that the new currency would not be able to meet financial inclusion objectives for two key reasons. Firstly, the digital nature of a CBDC would not be able to address the difficulties that many groups face as cash use declines. Secondly, CBDCs would not be able to attract the majority of people who prefer physical

227 Jamaica, we have a CBDC, Financial Times, 20th July 2023: <https://www.ft.com/content/91ac9f03-1ff8-47c9-bd0f-64449e2159d8>

228 Jamaica's new information commissioner talks meeting DPA mandate from the ground up, IAPP, 22nd March 2022: <https://iapp.org/news/a/jamaicas-new-information-commissioner-talks-meeting-dpa-mandate-from-the-ground-up/>

229 Digital-Currency Plan Falter as Nigerians Defiant on Crypto, Bloomberg, 25th October 22: <https://www.bloomberg.com/news/articles/2022-10-25/shunned-digital-currency-looks-for-street-credibility-in-nigeria?sref=3REHEaVI&leadSource=verify%20wall>

230 Nigeria's eNaira, One Year After, Jookyung Ree, International Monetary Fund, 16th May 2023: <https://www.imf.org/en/Publications/WP/Issues/2023/05/16/Nigerias-eNaira-One-Year-After-533487>

231 Nigeria Seeks Partners for Tech Revamp of Its eNaira Digital Currency, Bloomberg, 21st February 2023: [https://www.bloomberg.com/news/articles/2023-02-21/nigeria-seeks-new-tech-partners-to-revamp-enaira-central-bank-digital-currency?utm\\_source=google&utm\\_medium=bd&cmpid=google](https://www.bloomberg.com/news/articles/2023-02-21/nigeria-seeks-new-tech-partners-to-revamp-enaira-central-bank-digital-currency?utm_source=google&utm_medium=bd&cmpid=google)

232 Nigeria Digital Currency Transactions Jump 63% on Cash Shortages, Bloomberg, 21st March 2023: <https://www.bnnbloomberg.ca/nigeria-digital-currency-transactions-jump-63-on-cash-shortages-1.1898692>



cash. Given these and other factors, a government-appointed investigation concluded that Sweden does not yet need a central digital currency.<sup>233</sup> Other investigations have come to similar conclusions, such as the UK's Economic Affairs Committee report which found CBDCs to be a "solution in search of a problem".<sup>234</sup>

### Conclusion

Global explorations of Central Bank Digital Currencies have varied with their approaches to privacy. Each design has its own unique issues, and none is perfect. Indeed, none has managed to successfully navigate the privacy issues raised by CBDCs, nor has any made a case powerful enough to demonstrate that any perceived benefit would outweigh the litany of risks it would bring. The thematic issues raised by the chosen case studies provoke important questions over how a UK CBDC could be developed. No decision has yet been made whether to proceed with the plans for a digital pound. The infancy of the plans puts us in a unique position as, like other CBDCs examined, the UK has failed to make conclusive arguments that would justify introducing such a harmful piece of technology. Should the government proceed with its plans, it seems unlikely that it is possible to design a CBDC in a sufficiently privacy-preserving way. Addressing these concerns is vital in ensuring that any exploration of a CBDC in the UK does not compromise privacy, freedom, or financial inclusion in the international race for innovation.

There are many conversations that must be had and questions to be answered in the consideration of whether the UK should pursue a digital pound. One of the key takeaways is that public uptake of CBDCs has been poor so far, whether due to reasons of distrust and privacy concerns, or little interest in a payment that has no tangible benefit to the user. The pilots examined in this report offer a number of valuable lessons. This analysis has addressed the ways in which CBDCs can – or cannot – address financial exclusion. There are multiple examples of systems that encourage account holders to trade identity information for economic access and offer lesser services to those unable or unwilling to share this, such as in Israel's digital shekel or Nigeria's tiered wallet. The UK would do well not to follow in these footsteps that will exacerbate financial exclusion, rather than reduce it.

Much uncertainty still exists around a UK CBDC. At the heart of the issue is that no case has yet been made that provides a compelling benefit or justifies the threats that a digital pound could bring. Beyond this, proper consideration has not been given to their legal governance, or to how existing systems (such as AML/CTF obligations) would apply to a CBDC system. Other issues include data protection concerns, particularly in light of the

<sup>233</sup> Sweden does not yet need CBDC, inquiry finds, Central Banking, 31st March 2023: <https://www.centralbanking.com/fintech/cbdc/7957236/sweden-does-not-yet-need-cbdc-inquiry-finds>

<sup>234</sup> Central bank digital currencies: a solution in search of a problem?, House of Lords Economic Affairs Committee, 13rd January 2022: <https://publications.parliament.uk/pa/ld5802/ldselect/ldecon-af/131/131.pdf>

UK's weakening data protection regime.

Should the decision be made to progress plans for a digital pound, the evidence we have examined supports the following recommendations:

- **Any exploration of a CBDC should maximise user privacy.** Architectural design decisions should be token-based rather than account-based, and use distributed ledger technology (DLT) rather than centralised. However, measures must be taken to safeguard against the traceability functions of a token-based system.
- **Any CBDC system must ensure privacy by design and that the central bank collects only the minimum data necessary for functionality.** Technical infrastructures should be prioritise privacy-by-design rather than surveillance and the automation of regulatory burdens, as such systems are unlikely to build trust with the public and will be rejected in favour of cash and private cryptocurrencies. Neither the central bank, government, or public authorities should be able to directly access individuals' private financial data absent a clear judicial process and warrant, and the roles of CBDC system participants must be clearly defined.
- **User data must be safeguarded.** Individuals must be able to choose whether or not to use a CBDC, be able to exert control over their personal data if they do, and be informed about what data is shared, with whom, and for what purpose. A retail CBDC must be supported by appropriate privacy legislation to protect users and support trust in its governance and use. The UK is on track towards drastically diluting data rights via the Data Protection and Digital Information (No. 2) Bill – the Bill should be paused and HMT should publish an assessment of how the Bill would impact privacy and data rights in the context of a UK CBDC.
- **User data must not be shared without meaningful, informed and freely given consent.** Payment Service Providers and other third parties that collect or utilise payment data must not monetise or use this data for profiling purposes without proper informed consent from the account holder. No financial incentives should be offered in exchange for data sharing, as this compromises the consent process.
- **Decisions over whether to proceed with a new central bank digital currency must meaningfully engage the public and lawmakers,** and not remain within the remit of the central bank. National conversations must be had to assess concerns, the input of which should inform decisions on whether to proceed.



- **Inclusion must be meaningful.** Any introduction of a CBDC must not be done in detriment to the cash economy, which should be protected. Further, issues that limit people's ability to engage in a digital economy must be addressed e.g. lack of infrastructure, smartphone availability, or digital literacy.
- **Programmability functions must be prohibited by law.** Programmability is a major public concern given the risks that it could pose in a CBDC system, such as money being programmed to have spending restrictions or an expiration date. In order to guard against these concerns, it must not be technically or legally possible to institute functions that could impede upon civil liberties and freedoms into a UK CBDC system. We suggest that, if a CBDC is pursued, such a legal protection should be codified within a wider Digital Bill of Rights.

## House of Lords Economic Affairs Committee

“(...) the introduction of a UK CBDC would have **far-reaching consequences** for households, businesses, and the monetary system for decades to come and may pose significant risks depending on how it is designed. These risks include state surveillance of people's spending choices, financial instability as people convert bank deposits to CBDC during periods of economic stress, an increase in central bank power without sufficient scrutiny, and the creation of a centralised point of failure that would be a target for hostile nation state or criminal actors.”

“There is **no convincing case** for why the UK needs a central bank digital currency.”

“We concluded that the idea was a **solution in search of a problem.**”

# Appendix – Summary of major cbdcs around the world

## Full launch

| Country | CBDC Name | Comments   | ID Requirement                                       | Account/Token | Programmability |
|---------|-----------|--|--|---------------|-----------------|
| Jamaica | Jam-Dex   | World's first full rollout CBDC. Adoption has been slow, with the central bank adopting incentives to encourage uptake. Welfare payments may soon be paid via Jam-Dex. Accounts are linked to tax registration and government ID, and there are plans to integrate it with the national ID system. Despite full rollout Jamaica has not published much information about the CBDC, | Linked to government ID and tax registration number. | Token         | No              |

## Pilot

| Country              | CBDC Name | Comments  | ID Requirement  | Account/Token | Programmability  |
|----------------------|-----------|---|---|---------------|--|
| China <sup>235</sup> | eYuan     | Biggest CBDC pilot on the planet with around 260 operational million wallets across 250 cities in China, competing with private-company run eWallets. ECNY is account-based with pseudonymity for small transactions and greater traceability for high-value ones. Government regulations govern access to transaction details, and China has made noises that AI and data analysis will be used to monitor potential illicit activities. Comments have been made about the potential for the eCNY to be used as a tool of state control, but as it stands these are predictions and speculation rather than being based on specific evidence. The design appears to be similar to other CBDCs and concerns stem from the people with power, rather than the specifics of the technology compared to other countries. | Variable, from a phone number for the lowest tier wallet to bank account & ID for the top tier. | Account       | Smart contracts in development   |
| Ghana <sup>236</sup> | eCedi     | Full launch was targeted in 2023 but it was delayed due to economic issues in Ghana. Wallets are run by private institutions such as banks or mobile money operators. KYC verification is risk-based and tiered, with greater checks leading to fewer wallet restrictions. Fraud monitoring occurs and transactions can be reported to the Bank of Ghana, with the design paper stating a desire to strike the right balance between privacy and transparency needs.  | Tiered ID requirements linked to wallet capabilities.   | Token         | Programmable payments may be supported, including potentially welfare payments – although what this means is not detailed. |

235 China Digital Currency: Beijing To Expand E-CNY Trials To Four Entire Provinces Including Guangdong, South China Morning Post, 20th September 2022, <https://www.scmp.com/tech/article/3193125/china-digital-currency-beijing-expand-e-cny-trials-four-entire-provinces>

236 Design Paper Of The eCedi, Bank of Ghana, accessed 20th September 2023, <https://www.bog.gov.gh/news/design-paper-of-the-digital-cedi-ecedi/>

|                          |               |  |   |       |   |
|--------------------------|---------------|--|---|-------|---|
| India <sup>237</sup>     | Digital Rupee | Pilot limited to a handful of city and a set number of accounts, operated by select banks. India is testing both a retail and wholesale version - the CBDC-R for general use and CBDC-W for wholesale use. The eRupee is token-based although the tokens do not appear to be as linked to physical denominations as with Uruguay. CDBC accounts are linked to bank accounts in the trial, but transactions below a certain threshold are not automatically recorded into the central database. | Pilot accounts linked to phone numbers and bank accounts, via financial institutions.     | Token | Smart contracts being investigated  |
| Russia <sup>238</sup>    | Digital Ruble | Trial with 13 banks taking part. Consumer-focused pilot covers 30 outlets in 11 cities, with an emphasis on testing peer-to-peer transfers, automatic payments, retail purchases and QR-code infrastructure.   | Financial institution-linked accounts, who will verify customer IDs, including signatures | Token | Smart contracts under development, including the limitation of digital ruble spending to certain goods/ services. |
| Australia <sup>239</sup> | eAUS          | Pilot launched in May 2023. Public-private partnership with financial institutions performing KYC checks and being the public gateway to the CBDC. Transactions and balances are visible to the central bank, but KYC data will not be – pilot accounts are pseudonymous.  | Third parties conduct KYC checks which verify user identities.                            | Token | Conditional payments under consideration.   |

|                      |             |  |  |       |  |
|----------------------|-------------|--|--|-------|--|
| Korea <sup>240</sup> | Digital Won | Korea has conducted experiments and devised a PoC for a potential digital won, with a second phase test completing in November 2022. Several of the key reports by the BoK are only available in Korean, but it has been reported that they are currently building a pilot platform for a CBDC. The PoC was standard two-tier system in construction with private entities running the end user experience. BoK has trailed a zero-proof anonymity protecting method of CBDC transactions but it appeared to be very slow, otherwise privacy appears to be akin to private digital money transactions. BoK has expressed skepticism about the necessity of a CBDC in terms of monetary policy. | Unclear. DLT-based model implies pseudonymity, with third parties running wallets for the general public.  | Token | Smart contracts being developed by the BoK.                          |
| Japan <sup>241</sup> | Digital Yen | Japan began the pilot phase of its CBDC in Feb 2023, having published two fairly detailed proof of concept documents in the preceding 18 months. Japan's pilot does not seem to be akin to a functional pilot, rather it is still exploring the options for how a finalised digital Yen will look. AML, KYC and terrorism transparency obligations are being considered alongside privacy obligations but BoJ is still experimenting and determining which options to use.   | Unclear, but suggestion is intermediaries will operate wallets with some responsibility for holding user data. Work on what identity verification will be needed is ongoing. | Token | Programmable payments are being investigated as part of the process. |

237 What Is Digital Rupee?, Forbes, 14th June 2023, <https://www.forbes.com/advisor/in/investing/digital-rupee/>

238 Russia Is Ramping Up Its Cbdc. Will Putin's 'Robot Ruble' Work?, Atlantic Council. 29th August 2023, <https://www.atlanticcouncil.org/blogs/new-atlanticist/russia-is-ramping-up-its-cbdc-will-putins-robot-ruble-work/>

239 Central Bank Digital Currency, Reserve Bank Of Australia, accessed 20th September 2023, <https://www.rba.gov.au/payments-and-infrastructure/central-bank-digital-currency/>

240 Payment And Settlement Systems Report 2022, Bank of Korea, 19th July 2023, <https://www.bok.or.kr/eng/bbs/B0000179/view.do?nttId=10078478&menuNo=400063>

241 Central Bank Digital Currency, Bank of Japan, accessed 20th September 2023, <https://www.boj.or.jp/en/paym/digital/index.htm>

|   |              |   |   |       |  |
|---|--------------|---|---|-------|--|
| Thailand                                      | Digital Baht | The Bank of Thailand ran a limited pilot of a retail CBDC with three payment providers in Summer 2023. Staff of the payment providers took part in the pilot which aimed to cover up to 100,000 people and 100 outlets. The pilot has been billed as a learning process, rather than a commitment to launch and the bank maintains it has not made a decision about a wider introduction, | Accounts linked to bank accounts or phone numbers, with KYC mirroring those needed for bank accounts.             | Token | Programmable payments are being assessed for future development. |
| Eastern Caribbean Central Bank <sup>242</sup> | D-Cash       | Cross-country CBDC project across the ECCB. Limits apply to accounts based on KYC, AML and terrorism verification and checks. Financial institutions operate wallets and run checks on account holders, and can provide records to the authorities via legal requests.  | Signing up needs a government ID, or a verification code from a bank account [which will have needed ID to open]. | Token | Unclear  |

### Proof of concept, research & cancelled

| Country                    | CBDC Name        | Stage                        | Comments   |
|----------------------------|------------------|------------------------------|--|
| USA <sup>243</sup>         | Research         | Digital Dollar               | The Federal Reserve is researching a potential future US CBDC. The White House has laid out broad policy objectives for a "digital dollar", suggesting that a digital currency will be introduced at some point in the future. However, there is limited public work so far on any technical details or particulars, and there has been no public announcement of a functioning prototype.   |
| Canada <sup>244</sup>      | Research         | EDollar                      | Canada's central bank is researching a retail CBDC and conducted a public consultation in Spring 2023, which saw more than 85,000 responses. The results are yet to be published. The proposal states that the central bank does not see the need for a CBDC now, but that may change. Canada also has a previously cancelled CBDC project, Project Jasper, which was wholesale only.  |
| Brazil <sup>245</sup>      | Proof of Concept | DREX [formerly Digital Real] | Brazil has launched a pilot of the digital real in mid 2023, using a private-wallet central-bank issuance model, with no offline payments at present. Brazil already has an advanced instant digital payment system that works well for private digital money, Pix, which is central bank regulated. The Digital Real is focused on wholesale, but with retail access via tokenised deposits. Privacy is regulated under Brazil's data protection laws and banking privacy laws, with the implication it is on a similar level to private digital money. |
| Denmark <sup>246</sup>     | Cancelled        | E-kroner                     | In a 2017 speech the then governor of National Bank said that it was not clear that a CBDC would serve the role of an anchor in the monetary system, particularly with Denmark's high level of digital money use, but the country has not published much more information so may not be enough to work with. This stance was reconfirmed in a 2023 statement by the present governor Signe Krogstrup.  |
| New Zealand <sup>247</sup> | Research         | Unknown                      | The Reserve Bank of New Zealand is exploring design options for a potential future CBDC in the country. Currently the central bank states that it has not decided whether a digital currency will be necessary or not, and is at Stage 2 of a four stage process towards potential implementation. Stage 2 includes establishing policy teams as well as seeking technical feedback, ahead of Stage 3 which would be a multi-year process of experimentation and widespread consultation.  |

243 Central Bank Digital Currency, Federal Reserve, accessed 20th September 2023, <https://www.federalreserve.gov/cbdc-faqs.htm>

244 Digital Canadian Dollar, Bank of Canada, accessed 20th September 2023, <https://www.bankofcanada.ca/digitaldollar/ba>

245 DREX, Banco Central De Brasil, accessed 20th September 2023, [https://www.bcb.gov.br/en/financialstability/drex\\_en](https://www.bcb.gov.br/en/financialstability/drex_en)

246 Governor Signe Krogstrup's Speech At Danmarks Nationalbank's Conference New Types Of Digital Money, Danmarks Nationalbank, 9th March 2023, <https://www.nationalbanken.dk/en/news-and-knowledge/publications-and-speeches/archive-speeches/2023/governor-signe-krogstrups-speech-at-danmarks-nationalbanks-conference-new-types-of-digital-money>

247 Central Bank Digital Currency, Reserve Bank of New Zealand, 21st July 2023, <https://www.rbnz.govt.nz/money-and-cash/future-of-money/cbdc>

242 D-Cash, Eastern Caribbean Central Bank, accessed 20th September 2023, <https://www.eccb-centralbank.org/d-cash>



# **BIG BROTHER WATCH**

[@BigBrotherWatch](#)