nChain

Central Bank Digital Currencies

Everything you need to know

Contents

About this Playbook

The purpose of the First Edition of this Playbook is to encourage the public and private sectors, particularly central banks, governments, and citizens, to reflect on the drivers for Central Bank Digital Currency (CBDC) as well as their benefits and trade-offs.

This Playbook aims to walk readers through how such programmes can be designed and implemented, and some of the key questions that need to be addressed to help ensure a successful CBDC implementation. We believe it will be particularly relevant to government officials, central bankers, financial service providers, corporate executives and journalists, as well as to readers interested in innovation.

For further reading, links to other resources are provided at the end. The landscape of this emerging topic is fluid, and we welcome any contributions or questions that can help advance the industry.

Who we are

nChain is a global blockchain technology company offering software, IP licensing and consulting services. We have developed solutions for both retail and wholesale CBDCs, as well as remittances, cross-border payments and stablecoins – all built on public ledger technology.

nChain has also prepared and shared our views on CBDCs in response to various discussions papers on digital currencies, including those by the Bank of England, The Federal Reserve and the European Central Bank. We are working with the Tuvalu Government, specifically the Ministry of Finance, to explore the use of a stablecoin to support the National Bank to improve financial inclusion across the islands.

Foreword

Society is changing. The way we communicate is changing. More importantly, the way we make payments is changing. The role of cash is and will continue to change. But we also know that financial inclusion is still increasingly important, and with the way the world is changing, so is digital and societal inclusion. The need for an inclusive yet relevant and effective form of central bank money grows with each passing week. Yet there are still many unknowns when identifying the drivers behind the need for a CBDC and what central banks must do to identify the right approach for their CBDC programmes that delivers the maximum benefits for citizens and the private sectors.

nChain is a pioneer in the use of public ledger technology to build secure and scalable solutions for our clients across the world. We seek to raise awareness across the public and private sectors of the risks and opportunities of different CBDC implementations arising from the most important and overlooked design consideration: the choice of ledger technology.

But this is just one design choice to be made. As an organisation, we have spent the past three years speaking to central banks from across the world, asking questions and listening so we could understand what is driving the need for a CBDC and what role it could play in the future. From retail and wholesale CBDCs to offline payments, cross-border payments and financial inclusion, there are several different requirements for delivering an effective CBDC. Each of these requirements help to further define the approach that needs to be taken to delivering a CBDC solution.

It is the culmination of the work we have done over the last few years that has influenced our decision to publish this CBDC Playbook. We believe sharing our experiences, expertise, and thoughts to support central banks to work through this initial discovery and research phase can be hugely beneficial in identifying an optimal design for CBDC.

CBDC represents an important modernisation of public payments infrastructure informed by a long history of tensions between public and private interests. We therefore welcome any comments, contributions or questions that can help advance this industry.

We hope you find this Playbook insightful and informative, and we look forward to supporting you on this exciting journey.

Leandro Nunes
Chief Commercial Officer
nChain

Key takeaways

- CBDCs are an innovative, electronic form of national money issued by a central bank that people can use to make payments.
- The only central bank-issued digital money currently are reserves, which are unavailable to the public.
- Apart from physical cash, citizens hold commercial bank deposits which raises questions over control of the money supply.
- Financial inclusion, economic stability and direct monetary policy are some of the major benefits of CBDCs.
- Challenges can include transition risks (loss of data), the risk of centralisation and the possibility of banking disintermediation.
- Changing or declining physical cash usage, and well-developed digital infrastructure, are major drivers for CBDCs.
- Over 100 governments are investigating CBDCs, with nearly 40 that have an active proof of concept or currency.
- Two key types are retail CBDCs, which are intended for business or household payments, and wholesale CBDCs, which are suitable for interbank settlements.
- It needs a central 'ledger' to record the status of all central bank liabilities, and an interface to enable users to exchange currency.
- Blockchain, often mistaken with cryptocurrency or stablecoins, offers the most secure, scalable, and efficient CBDC solution.

What is a Central Bank Digital Currency?

A Central Bank Digital Currency is an innovative, digital form of national money issued by a central bank that individuals and businesses can use to trade and make payments.

It is different from a reserve, a bank deposit, and physical cash.

Historically, central banks have provided notes and coins to the public to act as a medium of exchange, a unit of account and a store of value – as part of a government's policy objectives. Payments are an essential public service, protected by legal tender laws.

But as cash use has been shown to be declining[1], households or businesses may no longer have access to direct central bank money. Today, many choose the convenience of paying with credit/debit cards, phones, or online banking. Each time we do this, we create data, share valuable personal information, and become more dependent on private payments systems or commercial banks, raising questions over the control of the supply of money. The only central bank-issued digital money are reserves, unavailable to the public.

As European Central Bank President Christine Lagarde stated, "We have a responsibility to ensure that our citizens have choice and cannot be excluded from the payments ecosystem due to the actions of others."[2]

CBDCs are a new form of central bank-issued, universally accessible electronic currency. They can provide increased payment system security, financial stability and regulation, trade efficiencies, and financial inclusion for underserved citizens.

They come in various forms, including retail or wholesale, and account-based or token-based, and feature a digital ledger that can use technology like a blockchain. CBDCs require the building of new infrastructure: databases, networks, apps, wallets, and so on. While novel, a well implemented CBDC can streamline financial plumbing and maintain the usability of modern payment infrastructure.

1 www.axios.com/2021/07/16/legal-cash-economy-decline-pandemic
2 Payments in a digital world Speech by Christine Lagarde, ECB President, at the Deutsche Bundesbank online conference on banking and payments in the digital world Frankfurt am Main, 10 September 2020, www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200910~31e6ae9835.en.html

Understand the terms[3]

Cash

Physical paper notes and metal coins that are typically minted by the central bank or treasury, and available to all users in the economy.
Can be exchanged with bank deposit money.

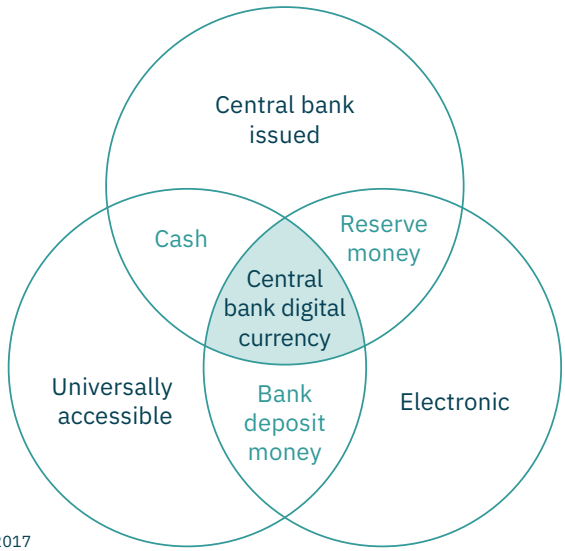
Bank deposit money

Electronically recorded deposit account liabilities on the ledgers of commercial, private banks.
Accessible to anyone with a bank account.
Can be supplied by crediting the accounts of depositors, typically with revenue generated from providing loans to borrowers.

Central bank reserve money

Electronically recorded current account liabilities on the ledgers of central banks. This money is only accessible to money users that hold an account with the central bank: usually commercial banks. Supplied by being credited to commercial banks' current accounts as part of the purchase of governments bonds or certain other financial securities.

How CBDC relates to the existing monetary system



Berg 2017

Myth busters

To clarify some common misunderstandings, CBDCs:

- Aren't based on unstable digital assets, commonly but inaccurately referred to as 'cryptocurrencies'
- Are governed centrally rather than by autonomous individuals
- Are different from stablecoins, pegged to the national currency
- Can support offline, instantaneous peer-to-peer payments
- Integrate seamlessly with existing systems, including physical cash

3 papers.ssrn.com/sol3/papers.cfm?abstract_id=2985381

A short history of CBDCs

CBDCs are a rapidly emerging area of interest for businesses and governments. Consumer behaviour around the use of cash has changed[4], and people are more familiar with paying for goods using their smartphones. In emerging markets especially, mobile money is a popular alternative to decreasing cash dependency. Covid has caused a rapid digitisation globally of different economic sectors, and recent technological milestones, notably the Bitcoin white paper in 2008, have made the concept of CBDCs more feasible than ever.

The last two years have seen a flurry of papers, reports, and roadmaps on CBDCs from the Bank of England, the European Central Bank, the G7, and more. Over 100 governments have investigated CBDCs – or are currently doing so – with nearly 40 that have an active proof of concept or currency.

Timeline

- **650 b.c.** First coins minted by Kingdom of Lydia
- **1700s** Shift from commodity money (coins) to bank-issued fiduciary money
- **1904** Riksbank given monopoly on issuing cash in Sweden
- **1913** Federal Reserve System established in the U.S.
- **1990s** Finland launches anonymous e-money card Avant
- **2008** Publication of the Bitcoin white paper

Sparks rapid increase in activity

- **2014** China begins research on e-CNY
- **2019** Bahamas tests digital Sand Dollar
  Facebook attempts to launch Libra digital currency
- **2020** Bank of International Settlements issues first major CBDC report
  Bank of England issues CBDC discussion paper
  Financial Stability Board shares G20's roadmap on cross-border payments
- **2021** European Central Bank launches digital euro project
  G7 issues report on guiding principles for developing CBDCs
- **2022** 105 countries, representing over 95% of global GDP, exploring CBDCs. 10 countries have fully launched a digital currency[5]

4 www.imf.org/en/Publications/WP/Issues/2022/02/04/Falling-Use-of-Cash-and-Demand-for-Retail-Central-Bank-Digital-Currency-512766
5 www.atlanticcouncil.org/cbdctracker/

CBDC principles

The Bank of International Settlements gives three foundational principles[6] for central banks considering whether to issue CBDC, that flow from their common mandates for monetary and financial stability.

Do no harm

CBDC should continue to fulfil public policy objectives and not interfere with or impede a central bank's ability to carry out its mandate for monetary or financial stability.

Coexistence

CBDC should coexist with cash and robust private money.

Innovation and efficiency

CBDC should drive innovation and efficiency in a jurisdiction's payment system (which includes public and private participants).

To enable these foundational principles of CBDC to be realised in practice, nChain has three additional considerations that build on top of the above:

Data integrity

The history of CBDC transactions should be immutable; not able to be changed by any party for any reason. Corrective transactions should only occur as new entries to the ledger.

Programmability

Users should exchange and interface with CBDC using a flexible scripting language that can automatically execute operations, such as enforcing terms and conditions and enabling smart contracts.

Privacy

User privacy should be protected. Users should have the opportunity to own and control their data and see who also has read access to their fields and metadata.

Ask yourself

Does the current banking system uphold these principles?

Can you think of any other principles that are important to you when issuing a CBDC?

6 Page 10, BIS, Central bank digital currencies: foundational principles and core features, 9 October 2020 www.bis.org/publ/othp33.htm

Benefits and the opportunity

There are multiple reasons why a central bank would adopt a CBDC. Not least because they allow functionality not possible with physical cash, such as real-time monitoring, auditability, automatic taxation and the ability to immediately transmit interest rates through returns[7]. Creating a centralised, digital currency can provide many benefits that impact citizens, companies, and governments alike. Some of the most important will likely be:

Economic stability

Better payments

Financial inclusion

We estimate implementing a well-designed CBDC takes at least 3-5 years, including the discovery, research, and pilot phases, but the sooner a government begins the scoping process, the sooner they can get in front of an inevitable global economic, social, and technological shift.

7 www.ukfinance.org.uk/system/files/CBDC-report-FINAL.pdf

Economic stability

CBDCs support a central bank's ongoing role in issuing currency and maintaining economic stability. They can improve the competitiveness of a local currency as a means of payment in dollarised economies such as Venezuela or Lebanon. Central banks should consider CBDCs as a more direct and efficient means of executing policy.

More secure, less costly peer-to-peer and interbank payments may promote stability. As will the fact that central banks can monitor economic data in real time and gain greater visibility on the flow of money, building resilience against shocks such as inflation, recession, or the impact of events like a global pandemic.

Today, citizens and consumers primarily hold money in banks, as the most convenient way of making payments is by using debit/credit cards. With the adoption of a CBDC it is conceivable that citizens may start to hold more cash in their wallets and use digital cash as their primary payment method. This may reduce current account balances at commercial banks, forcing banks to review their exposure to risky investments and instilling market discipline.

Public trust is also critical for stability. Governments that commit to protecting citizens' privacy, reducing crime, and ensuring transparency in the banking system will more easily gain such confidence.

Policy benefits

CBDCs allow for tighter control over monetary and fiscal policy. Interest rate changes, or distributing financial aid by way of fiscal payments like during Covid, can be instant. Currently, policy decisions can take time to come into effect and impact citizens.

A more direct control over policy can lead to fraud reduction, opportunities for innovation, improved public interest in policy decisions, and cost reductions in policy implementation and execution. And if cash is not readily available, CBDCs can also provide a delivery mechanism for negative interest rates. Digital currencies can address the zero-lower bound on conventional monetary policy, using cashback payments on expenditures paid in CBDC.

A CBDC would also allow governments to receive instant feedback on the impact of policy changes across agencies in real-time and make adjustments accordingly.

Financial inclusion

CBDCs extend the benefits of physical cash to modern digital payments. They do so by offering an inclusive and scalable gateway for the unbanked and underbanked to access electronic payments as well as a wide variety of products and services[8].

Cash is more financially inclusive than a digital bank account, which not everyone has the financial literacy, means, nor the accepted proofs of identity and address, to open[9].

Commercial bank branches may be far away, and services can have limited working hours, whereas retail CBDCs offer 24/7 payments anytime, anywhere, including via mobile devices, smart cards, and apps. This is especially transformative in emerging economies for remote, marginalised communities.

In many countries the costs exceed the value of a small transaction and digital cash can facilitate casual micropayments which can benefit poorer citizens. Instant transactions and check depositing can also be a benefit for those who cannot afford delays when being paid.

8 www.bis.org/fsi/publ/insights41.pdf
9 www.paysafe.com/en/blog/the-role-of-cash-in-tackling-financial-inclusion

Better payments

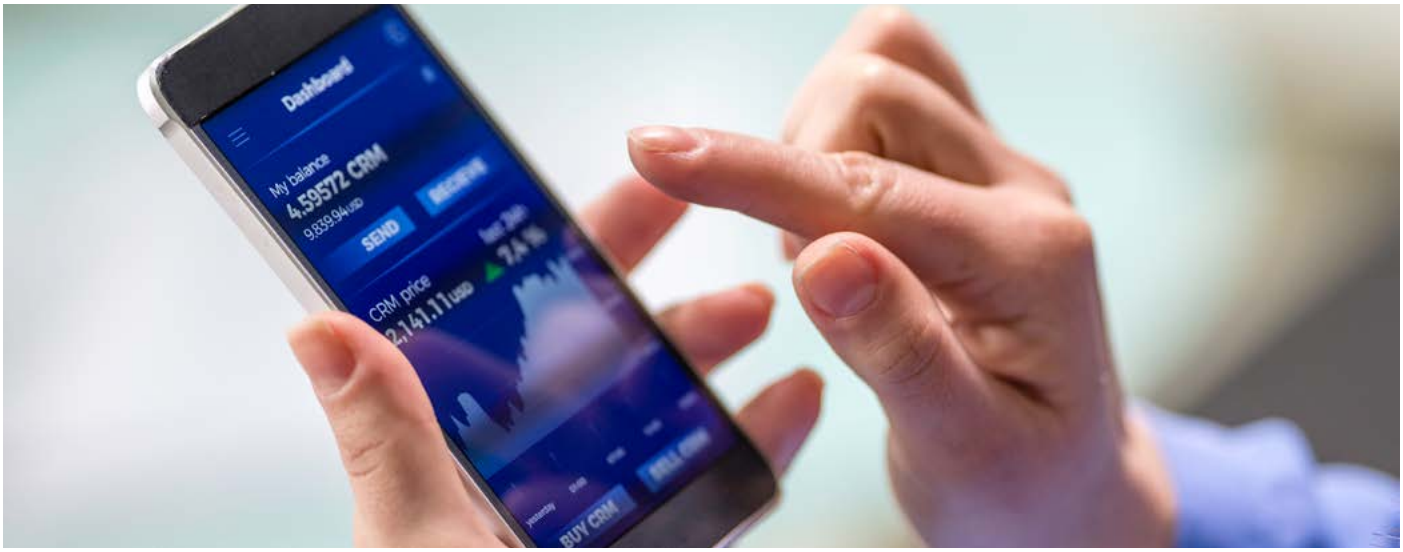
Settlement with digital currencies can be significantly cheaper and faster than today's legacy payment systems. This applies to wholesale CBDCs, that offer faster interbank settlements, as well as to retail CBDCs, for peer-to-peer payments between citizens or merchants at the point of sale. A digital peer-to-peer cash system can also facilitate payments between connected devices, such as IoT.

Leading ledger technology demonstrates the ability to handle over 50,000 transactions per second, for stable fees as low as a fraction of a cent. This compares to VISA's average of around 5,000 transactions[10] per second. CBDCs are cheaper than using credit card payment providers such as VISA or Mastercard, while also reducing the likelihood – and therefore the financial burden – of errors, crime, and reconciliation due to the tamper-proof transaction record. Operating on a single immutable and distributed ledger is more efficient than across multiple, mutable ledgers.

An open transaction processing market model can also unlock competition, encouraging even lower prices and innovation.

CBDCs can offer instantaneous peer-to-peer local and global payments, reducing network hops and cutting cross-border payments down from days, as with legacy systems, to mere milliseconds. Network hops may also introduce additional KYC protocols at every cross-border exchange, which CBDCs can simplify by embedding identity management.

Public blockchain technology can validate and settle transactions even offline or where the user has an unreliable connection, a functionality that is not currently possible with legacy systems. Offline payments should be a key requirement for central banks to ensure digital cash remains as inclusive and accessible as physical cash is today and provide resilience to the wider payment landscape.

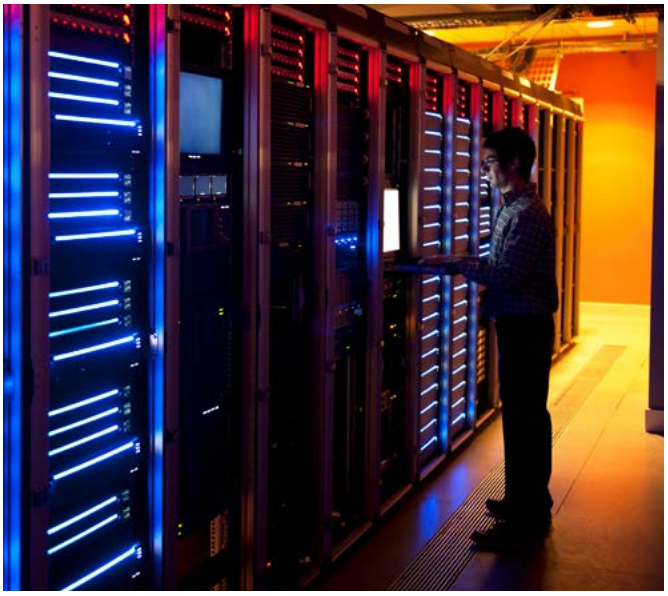


10 This is based on VISA's publicly disclosed report on transaction volumes

Security

CBDCs are more secure than legacy systems, both in the system design and in the technology. One of the critical benefits is that CBDCs enable digital payments with less fraud risk, and less systemic and counterparty risks. Nothing is perfectly secure, though levels of economic security can be achieved by making the costs of an attack exceed any potential benefits.

This is just not a matter of adding tools like cryptography but also in the design, authentication method, rules, and regulations that the network can enforce, as well as the reliance on third parties. Resilience and security are achieved using an economic model that incentivises good behaviour. Digital currencies that are based on a public distributed ledger provide critical security improvements because they eliminate central points of failure. Even if the majority of nodes on a blockchain network fail or attempt to cheat, the system will continue to operate.



Making tax easier

CBDCs can make taxation simpler, safer, and more reliable for governments. Key features include real-time taxation at source (via multi-party payments), real-time tax rebates, automatic auditing, and automated contract (commonly called smart contract) integrations with immutable public and private registries.

Such benefits can together improve tax collection, thereby increasing government revenues, while also decreasing the tax compliance burden and associated cost of fraud or tax evasion.

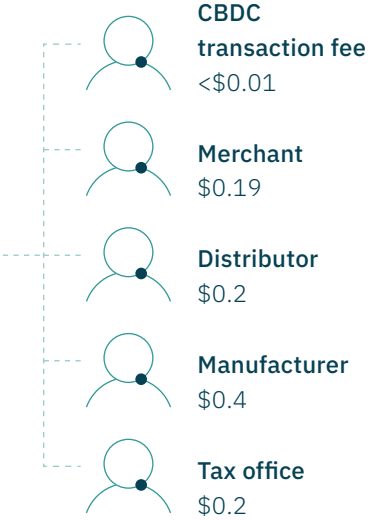
Instead of placing significant accounting burdens on individuals and companies to track, report, and pay value added tax, governments can receive VAT automatically and in real-time by using multi-party payments at source.

In practice

How can tax be collected using a digital currency?

Automatic taxation

A $1 equivalent purchase with a CBDC would allow the ability to instantly transmit currency to every stakeholder in the supply chain. It could reduce costly overheads and the tax burden, while also providing real-time sales data across the product life cycle.



Transparent government

CBDCs can increase transparency and public accountability.

They allow openness, innovation, and competition. Legacy infrastructure is often fragmented, with interoperable but closed-loop systems that citizens rarely see or understand the links between; taxation, public services, payments, bank deposits etc. CBDCs can help resolve this. From a technology standpoint, an immutable record or one that is public encourages even more transparency. This can help build people's confidence in a central bank or government, and provides a mechanism to instil market discipline across the sector. The protection of personal data is also a vital part of public trust.

A transparent and traceable CBDC may help external investors have a greater sense of trust in the movement of money across a country, encouraging greater investment.

Preventing crime

CBDCs can be a powerful anti-money laundering (AML) solution, providing tools and mechanisms that reduce the risk of financial crime and lower the barrier to justice. This is heavily dependent on programme design, but at a minimum, having a permanent, immutable payments record disincentivises dishonest behaviour, fraud, or theft. Pseudonymous privacy can mean appropriate authorities, like law enforcement or tax offices, can be given tiered access to certain identifiable information with the digital ledger where authorised.

Connected to appropriate identity, registry, and other services, CBDCs can even prevent financial risks in real-time via automatic monitoring, automatic audit, and event-driven taxation. These services can also improve economic stability. Public networks that feature advanced digital signatures to authorise transactions can easily incorporate existing standards around AML and customer due diligence.

For wholesale CBDCs, incorporating digital identity solutions with AML/KYC data alongside the transaction provides flexibility in the way service providers can adhere to upcoming regulations, such as the Travel Rule.

Safeguarding citizens

CBDCs offer a similar level of privacy to cash, while remaining discoverable within the constraints of the legal framework. A fully anonymous CBDC is not recommended, but pseudonymity is important to maintain the financial privacy of citizens when using CBDCs. Users should also be able to see who has read access to their fields and metadata. Token-based CBDCs, based on a public network, can further ensure privacy by allowing personal data to be stored at the edges of the network (rather than on the ledger itself). By allowing only relevant parties to have access, data from pseudonymous users remain private.

Privacy is a key issue, as evidenced by legislation such as the EU's GDPR and China's PIPL.

Currently, citizens rarely know who holds what data in a payments system – and often personally identifiable information is stored by third parties in databases that are at risk from hackers.

Instead of people filling out detailed forms (sharing personal information) with every merchant or business, CBDCs can offer a system where merchants simply validate that a customer's encrypted data has been verified by a trusted know your customer (KYC) authority. In other words, it removes the need to share unnecessary personal data.

In practice:
How can CBDC payments protect user privacy?

Traditional card payments

Amount	$ 7.50
Merchant ID	999 999 999 999
Name	Joe Blogs
Date of birth	3 Jan 1985
Card network	Visa
Bank	ABC Bank
Number	5212 5255 2253 2583

Lost privacy
Private sector captures data flows.

CBDC

Amount	$ 7.50
Merchant ID	999 999 999 999

Improved privacy
No leakage of unnecessary data fields. Central bank access to certain fields for public interest.

Cross-border remittances

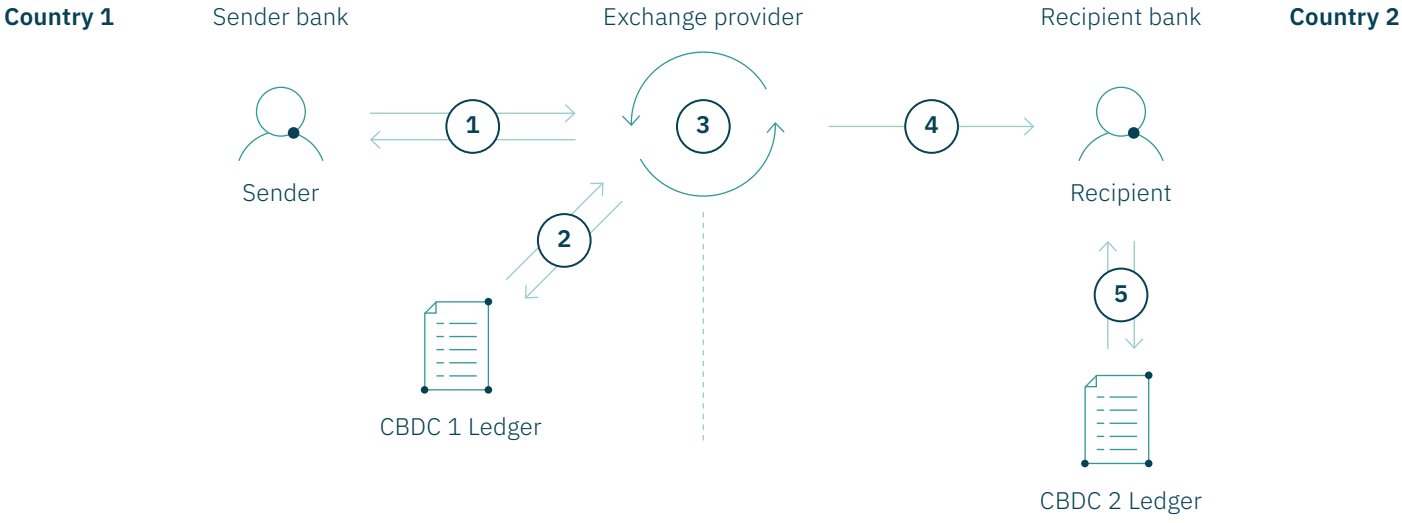
CBDCs can remove friction with cross-border payments that may bridge different regulatory frameworks, market dynamics, data practices, and infrastructures – in accordance with the FSB's stage 3 roadmap. This will depend on interoperability, or the ability for national CBDCs to be easily connected; a benefit that commercial banks using a wholesale CBDC will appreciate. The central banks of China and the United Arab Emirates are already exploring such a concept with the Multiple CBDC (m-CBDC) bridge project. Project Dunbar, between the central banks of Singapore, Australia, Malaysia and South Africa, is another such prototype. For citizens, instant micropayments provided by certain ledger technologies can improve the way remittances are sent and received, reducing the reliance on transfer services such as Western Union or OMT.

In practice

How would a typical cross-border transfer work?

1. Sender notifies exchange provider that they wish to transfer to their family member abroad. The exchange provider confirms the rate and prepares a purchase order and billing.
2. Exchange provider submits transaction to be settled on the CBDC 1 ledger in the sender's country.
3. Exchange provider, who holds both CBDC 1 and CBDC 2 currency, makes an internal conversion.
4. Exchange notifies recipient bank of the transaction in CBDC 2 currency.
5. Recipient bank submits transaction to be settled on CBDC 2 ledger.

Hypothetical cross-border transfer



Ask yourself

Which of these benefits would be most transformative in your country?

Will CBDCs cause inflation?

It is important to consider the impact of CBDCs on inflation given that 2021 and 2022 have seen rising inflation globally, at least partly due to Covid, a manufacturing and supply chain slowdown, and geopolitical factors[11].

While individual central banks have their specific mandates, all of them have a role to play in targeting price stability. One obvious way central banks ensure stability is through the target interest rate, which directly impacts capital markets and flows through to the real economy.

CBDCs will not cause inflation, but can give a central bank more direct tools to execute monetary and fiscal policy that they do not currently have. Monetary transmission can be instant; there is no need to wait for rate changes to be executed by commercial banks before having an impact on citizens. A central bank is also able to impose negative interest rates on a CBDC, overcoming the zero-lower bound if they so choose.

Moreover, a full implementation of a CBDC provides an indisputable proof of the official money supply. Current research suggests that central banks are managing policy based on a best estimate, not concrete fact. A digital money supply does not need to rely on approximation; the volume of cash and/or money is provable.

Targeting a long-term inflation rate relies on having strong macroeconomic data. CBDCs can give more granular data in real-time; the source of which is trusted—on an immutable ledger, for example. Gathering such data, in a well-designed CBDC, can be achieved without citizens giving up privacy or reducing their rights to conduct business.

This allows authorities to track changes in terms of the pricing and velocity of money instantly, meaning price stability does not need to rely on lagging indicators which report on volatility after the trend. CBDCs can therefore give a central bank better visibility on the impact of policy on the economy.

11 www.imf.org/en/Publications/WEO/Issues/2022/04/19/world-economic-outlook-april-2022

Challenges and risks

There are challenges associated with implementing a CBDC. Digital currencies remain in an early phase, and more research and experimentation are required to provide the necessary understanding of their possible economic and social impact. Nonetheless, our analysis finds the case for central bank-issued digital currencies to be compelling, especially given the many flaws with current legacy payment systems.

Many of the challenges outlined below are risks associated with implementing a poorly designed, insecure CBDC. The cost of inaction and rising systemic risk from stablecoins must also be considered. Some of the most important risks to mitigate against will likely be:

Transition risks

Loss of privacy

Theft, loss, and cyber attacks

Transition risks

CBDCs are an innovative concept, allowing citizens to make digital payments using central bank money for the first time[12]. Because of this, they will require the migrating of both data and value to new infrastructure and systems. This is no small task, and presents risks including system downtime, data loss, and insecurities. Transitioning to digital currencies also poses a risk in terms of technology lock-in effects. These can have a substantial negative economic impact if not properly mitigated against and planned for. Moreover, citizens – who will be the largest user group of a CBDC – may be confused about the technology or even the purpose of a new digital currency.

Thorough testing at all levels, clear strategies and migration assessments, robust training, and a public campaign are essential requirements of a CBDC program.

Banking disintermediation

Commercial banks may fear a loss of bank deposits and associated profits from clients withdrawing assets to use CBDCs, resulting in a shift in power over digital payments towards the citizen and the state. But the introduction of a CBDC also provides opportunities to commercial banks and other financial institutions, including cost optimisation and a more efficient back-office operation. A retail CBDC will be like cash is today, non-interest bearing and credit-free, therefore commercial banks will still have a vital role in providing banking services, including lending and credit, to citizens. The introduction of retail CBDC does not remove the need for deposit money or forms of private money, such as stablecoins, so commercial banks will continue to be a key part of the payment landscape. Furthermore, depending on the design of the CBDC itself, commercial banks could provide the interfaces into a retail CBDC.

Additional strategies to mitigate any risks of disintermediation, that require further research, exploration and testing could include:

- Modifying capital requirements
- Modifying CBDC designs and incentives
- Providing and paying bank guarantees and deposit insurance in CBDC
- Restricting on-demand conversion of digital cash to deposit money

12 www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

Loss of privacy

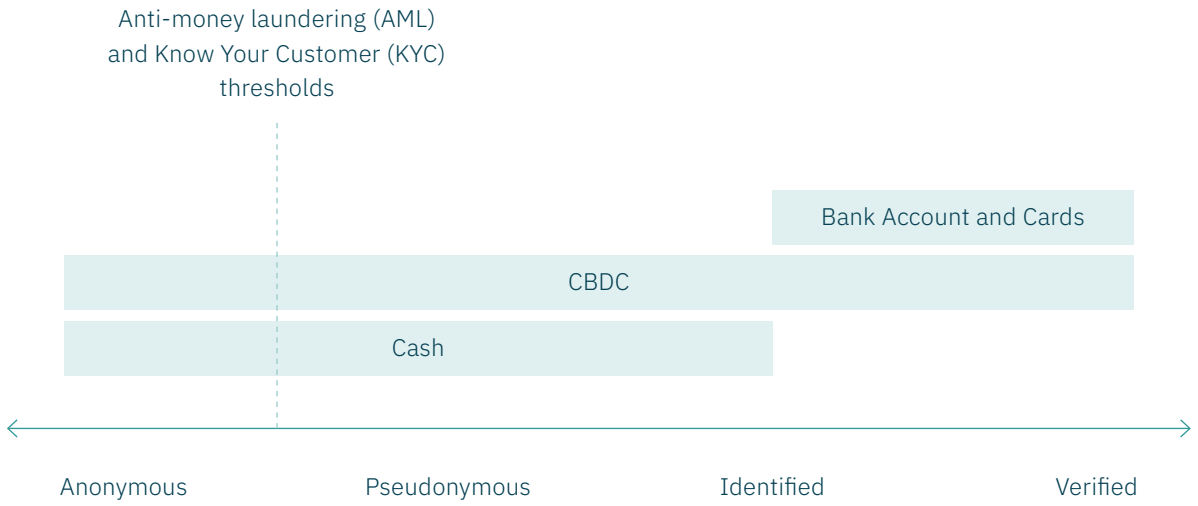
Physical cash presents fewer privacy risks for citizens than current digital payment systems where data and sensitive information is shared with private banks, payment providers, and even large tech companies – and can be unknowingly monitored. CBDCs raise a question over state surveillance and government access to personal data. While CBDCs can shift privacy back to the individual, giving access to the central bank and various providers only on a 'per need' or 'as negotiated' basis, designs can easily fail to replicate the privacy benefits of physical cash. A one-system solution like a CBDC, while less fragmented, does mean data is stored only in a single place: the core ledger. This could present a privacy concern for citizens who may be unwilling to share account or transaction data, with the risk of creating a 'pay-with-privacy' model that incentivises the disclosing of information. A public, immutable ledger can expose users to new risks that do not exist with fragmented legacy systems. Privacy protections are a core principle of any CBDC and must be built into the design.

In practice

Anonymous: A person's identity is unknown, and their actions are not trackable.

Pseudonymous: It is possible to assign actions to the same person, but their identity is unknown.

Payment privacy spectrum



Centralisation risk

CBDCs can undermine integrity and accountability because they introduce a conflict of interest between ledger management and monetary governance. This is particularly the case in centralised, private systems, where power is concentrated in one entity that has both operational control and executional responsibility. This raises the risk that bad actors could abuse their power in a way that undermines honest governance, and ultimately, citizen's rights. The power to write transactions must be separate from managing and processing transactions.

Law enforcement, government agencies and a central bank should have tiered access to a CBDC to ensure regulatory compliance, especially with AML or anti-crime initiatives. Because any actions are recorded on an immutable ledger, this process can be more robust than legacy systems.

These can be addressed with security and governance controls, but these can be costly. A programmable CBDC running on a public distributed blockchain ledger can improve governmental integrity and system stability by allowing the law and rules to be programmed into the currency itself. Central banks can retain more or less total control over all aspects of their CBDC, while it would allow for the ability to correct mistakes through appended transactions. Bad actors, however, are unable to tamper with the ledger and alter history.

Theft, loss, and cyber attacks

The technology underpinning most digital currency designs, although not new, is less established than current payment systems. This can introduce the risk of myriad types of cyber-attack by bad actors wishing to gain control of the system or assets stored on transacted with the ledger. CBDCs are also less fragmented than current payment systems, but this centralisation can also present a single point of failure for attacks with the added potential added potential to destabilise the economy.

In a token-based (retail) CBDC merchants and citizens may use credentials in the form of a private key to make a transaction. This creates a risk that keys could be lost or stolen, through phishing or other attacks, and assets and data compromised. Threshold signature or multi-sig technology, in a public blockchain, could mitigate some of this risk. Transactions can be secured by allowing only authorised users to spend their CBDC tokens and a key if one is lost, such as if a user's mobile phone that contains their digital wallet is stolen. Tools also now exist to freeze or recover digital assets in such cases. Nonetheless, the more advanced systems become, the more barriers to adoption there may be. Technology must not sacrifice usability.

Ask yourself
Have you thought about these risks?
Who will be responsible for managing them in your country?

Launching a CBDC

Launching a CBDC must follow a clear process, involve multiple stakeholders, and consider the wider social, political, economic, and structural context. The roadmap for implementing a CBDC given here will not be universally applicable, but is a helpful illustration of how implementation can work.

Drivers

The Bank for International Settlements outlines the following factors[13], based mainly on data from the World Bank:

- Digital infrastructure, such as mobile phone and internet use, is developed
- Capacity for innovation (R&D) across business, government and education is advanced
- Government institutions are effective (having a digital minister would be ideal)
- There is a large informal (shadow) economy
- GDP per capita, and financial development, are high
- Fewer citizens have access to transaction accounts
- There is public interest in CBDCs
- Cross-border demand for payments and remittance flows are high

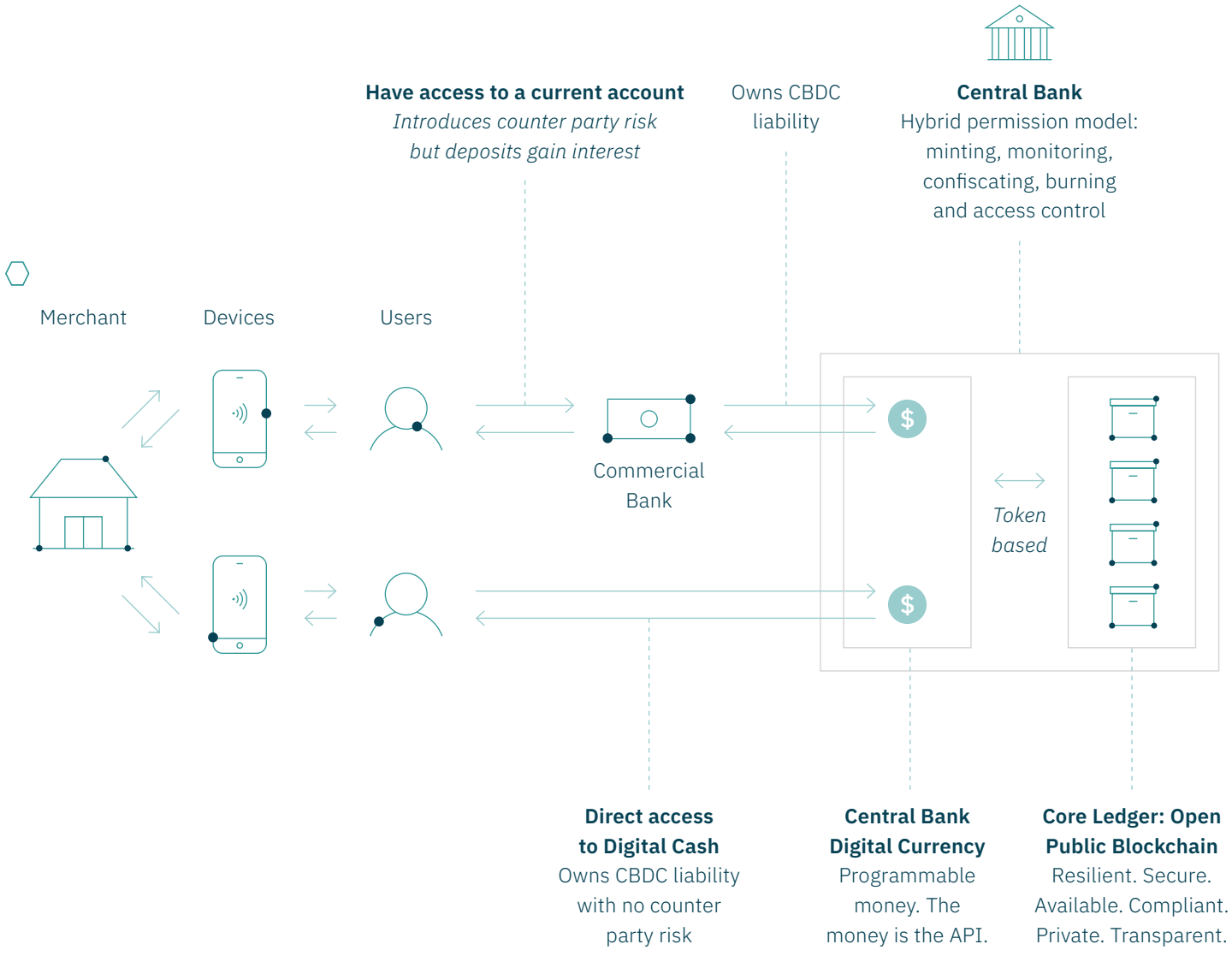
We believe that changing consumer behaviour around physical cash and mobile payments and its knock-on effects for financial inclusivity is also a significant driving factor.

13 www.bis.org/publ/work880.htm

What it looks like

Every digital currency must have a similar structure, including an issuer, a service provider, users and a ledger. Differences occur depending on whether a two-tiered (involving a commercial bank) or direct approach is chosen.

Here is a typical example of what both could look like:



Stakeholders

A country-wide digital currency system will inevitably involve every kind of actor, from an individual citizen to a central bank governor. Some of the key stakeholders and their responsibilities are:

Central Bank

A central bank is responsible for issuing the CBDC. The central bank will also be responsible for removing CBDC from circulation. These actions can be referred to as minting and melting/burning. Central banks will define the Terms of Service that are inherited automatically by any and all participants interacting with their issued CBDC. The CBDC itself is the API.

Central banks manage the digital currency in accordance with the Terms of Service. This may include (where appropriate, with other government agencies and partners) various actions associated with cash such as new issuances, freezing criminal funds, thawing CBDC funds, responding to court orders, managing various CBDC policies and complying with court orders.

A central bank could choose to outsource several services to a CBDC service provider. These allow central banks to retain complete control over their CBDC, while also allowing private enterprises to support the central bank in providing key services to the users. Services could include:

1. Onboarding of users
2. Distribution of CBDC to users
3. User support

Payment interface providers

One possible design for a retail CBDC is a two-tiered model. In a two-tiered model, central banks could choose to work with payment interface providers to enable overlay services in addition to the services mentioned above. Payment interface providers will be regulated entities who provide services, such as:

1. Providing support for programmable money and automation (commonly referred to as smart contracts);
2. Account management, including management of user keys for managing funds, encryption, and decryption;
3. Provision of Know Your Customer or AML services;
4. Auditing and enforcement of CBDC terms & conditions; and
5. Analytics, reporting and dashboards.

Users who interact with the CBDC via the payment service providers will continue to comply with the Terms & Conditions set by the issuing central bank. Payment service providers are not necessary to facilitate peer-to-peer payments between users.

Users

Users may either be citizens, merchants (e.g. a shop selling goods), or connected devices. Users hold digital currency themselves, exchanging transactions peer-to-peer. They can access additional services provided by Payment Interface Providers.

As an electronic bearer instrument, similar to cash, those who choose to hold CBDC themselves are responsible for securing and safeguarding their claim to central bank money. Any loss or compromise is the responsibility of the individual. But unlike physical cash:

- In the case of lost keys, central banks may elect to allow (by itself or via Payment Interface Providers) services for recovering 'lost' funds; and
- Direct CBDC holdings may or may not be subject to remuneration (interest), depending upon the issuing central bank's policy.

Transaction processors

Transaction processors, in a blockchain-based CBDC, compete publicly to write CBDC transactions to blocks and append those blocks to the core ledger, risking significant capital investment to do so. As network nodes, their role is to record, index, and confirm transactions, while users transact in a peer-to-peer manner. This model prevents the double-spending of any coins, a service currently provided by centralised payment systems.

Central Banks may operate (or tender for the provision of) additional Transaction Processors to provide further CBDC resilience for their jurisdiction beyond the network baseline.

Timeline

Below is a generic implementation schedule for rolling out CBDCs. Any CBDC deployment can be interoperable with existing digital asset services, such as R3 Corda exchange platforms.

Given that it took four years to launch the Sand Dollar, and at least several years to launch the e-Naira, we estimate that a timeframe of 3-5 years seems appropriate for emerging economies. It will likely take much longer for a CBDC to be introduced in markets such as the Eurozone, US or UK. This timeline may be reduced significantly if off-the-shelf products that need little customisation (e.g. digital cash, digital money, digital ID, wallet), as well as the underlying infrastructure, are available.

During each phase it will be vital to both advance knowledge among key stakeholders on CBDCs, while also minimising the risk of triggering a banking crisis. We recommend conducting simulation and market research on economic design choices affecting CBDCs, including factors such as holding limits, reimbursement (interest and non-interest bearing), and guarantee mechanisms.

It will also be important to test and analyse what mix of efficiency, convenience, privacy, and other features maximises the public interest, and test base assumptions about conditions that can affect public acceptance and adoption of digital currencies.

CBDC timeline

Regulatory approval

1	2	3	4	5
6–12 months	6–12 months	6–12 months	12–24 months	6–12 months
Phase 1: Scoping and assessment Analysing the context, choosing a service provider, identifying goals and requirements, briefing stakeholders, economic modelling, risk assessment, evaluating benefits/ risks, and scoping alternative options.	**Phase 2: Design** Choosing CBDC structure and technology, defining operating model and establishing rules.	**Phase 3: Proof of concept** Developing a prototype to test in an internal environment, get feedback, and refine.	**Phase 4: Full implementation** Implementing governance processes, integrating technology, migrating data and onboarding stakeholders (banks, payment providers).	**Phase 5: Launch** Educating citizens, running a campaign and deploying the CBDC.

Continued on next page

Resources required

CBDCs require new infrastructure, entities, and regulation to be set up. It is a fundamental change for a country's payments system. Governments need to allocate significant financial and human resources for such a program, and have a robust change management plan. Although no figures on how much was spent to establish active CBDCs such as the Bahamian Sand Dollar or Nigeria's e-Naira are available, it is estimated that a single implementation could cost upwards of tens of millions of US dollars. This can be offset by the economic benefits and cost savings of a CBDC.

Ask yourself
How ready is your country for a CBDC, based on the drivers listed? Can you think of any other stakeholders who would be involved?

Design choices

There is no one-size-fits-all CBDC, and each will inevitably reflect the unique economic, structural, and technical needs of the country in which they are implemented.

Governments wishing to implement digital currency solutions will have to make a number of considerations, not least of all the extent to which a CBDC replaces cash.

At minimum, CBDC must record transactions, which represent central bank liabilities, on a ledger. More sophisticated functionality will depend on the issuing country's needs but may include CBDC wallets, custody and exchange systems, national identity systems, monetary policy tools to affect CBDC interest and limits, product and service registers for managing real-time taxation at source, and much more.

Some key design choices are:

- Instrument
- Authentication method
- Openness
- Technology

We give a more detailed overview below, but our analysis finds that a government-issued and controlled private permissioned CBDC running on a public network – the blockchain – is by far the most secure, scalable, and efficient model for both retail and wholesale applications.

Instrument

CBDCs are designed to be used by every kind of stakeholder in an economy, as with cash. But we can broadly categorise the types of payments that would typically be made with a CBDC into:

- Retail (households and businesses)
- Wholesale (banks, financial institutions, payment providers)

Retail CBDCs have a wider use, intended to fulfil the everyday payment needs of people and companies in a country. This is where central banks issue a digital form of a banknote to complement the existing notes and coins they provide. The size of payments in a retail CBDC would typically be smaller than a wholesale CBDC. A general-purpose CBDC like this supports a more efficient, resilient, and diverse domestic payments system. An example of a retail CBDC would be the US Fedcoin, the Bahamian Sand Dollar, or the Nigerian eNaira.

Wholesale CBDCs, on the other hand, would only be used by specific financial institutions as a settlement asset in the interbank market, and involve larger sums, as a kind of accounting system. Central banks can issue such currencies to make the clearing and settlement of trades between banks (including tokenised assets and commodities) more efficient and secure; even cross-border. They can also address issues of counterparty credit risk and liquidity. An example of a wholesale CBDC would be the Canadian CADcoin.

Both types of CBDC can be catered for by standalone solutions. One does not rely on the other; although it is important to choose a design and technology approach that ensures interoperability and convertibility between a retail and wholesale CBDC where a central bank is looking to deploy both.

In the future, it is entirely possible that we will see hybrid solutions that attempt to deliver token-based forms of money, using a more traditional account-based solution. Some implementations of stablecoins follow this approach, and others, like Apple Pay, are slowly moving away from traditional account-based forms of money to something more similar to a token-based, digital cash CBDC in the form of peer-to-peer payments between Apple devices.

Authentication method

The difference between an account-based or token-based approach of CBDC may be technical, but it has significant implications for identity and access management, cost, and design. Put simply, the former means the system is made up of accounts that each have a recorded balance, whereas the latter means the system consists of individual assets, or tokens, which have key holders.

An account-based approach typically involves the use of a trusted third party to verify a user's identity as the account holder, and check their account balance, before they are allowed to make a payment. The accounts are then debited and credited accordingly. This may introduce unnecessary overheads, while the need for extra verification steps can repeat similar flaws with today's legacy systems. The need for a third party can also affect the governance of the network. As a result, an account-based approach seems more suitable for a wholesale CBDC (interbank settlements), where the trade-off between accessibility and proof of identity seems more straightforward.

Token-based verification meanwhile uses blockchain technology to overcome the need to check a customer's balance before allowing a transaction – as long as they can show that they are the token holder by signing the transaction, such as by using a private key, and meeting identity requirements at the appropriate level. While a risk is often associated with the loss of a private key, solutions exist to maintain the control of ownership in such events. These systems can provide a more direct, cash-like approach, without the need for an account. Account-based and multi-factor authentication features are still able to run on top.

Both methods are used to prevent double-spending, in which the same funds can be spent more than once, or simultaneously spent and returned to the user; a problem that physical cash, and blockchain technology, do not have.



Openness

The CBDC ledger may be on either a private or a public network. Digital currencies can use either, or a combination of the two. More detail is provided in the 'Technology behind CBDCs' section.

Private networks, where data is only accessible by a controlled audience, are often associated with more anonymity, privacy, and control over personal data. But as recent news reports on the handling of private customer data have shown, and as modern systems must increasingly interoperate with the structures of the internet, privacy has steadily been eroded. Examples of closed networks include cloud computing and private servers.

Public networks involve the wide distribution or public announcement of transactions and data, such that any entry of data, intended or not, is recorded on an open ledger and can no longer be deleted in any feasible manner. A common misunderstanding is that public networks are inherently risky because they broadcast data openly, but the opposite is true. Eliminating the ability to easily remove critical data, including transaction data, is precisely what makes it secure and immutable. Public networks include blockchain. While transactions are publicly broadcast, privacy can be protected by only allowing authorised parties to access sensitive information.

Ask yourself
What do you think is a bigger priority: a retail CBDC (digital cash) or a wholesale CBDC (interbank settlement)?

Future research areas

The study of CBDCs is ongoing but there are specific areas we believe could benefit from future research by academia, government, or industry. A non-exhaustive list includes:

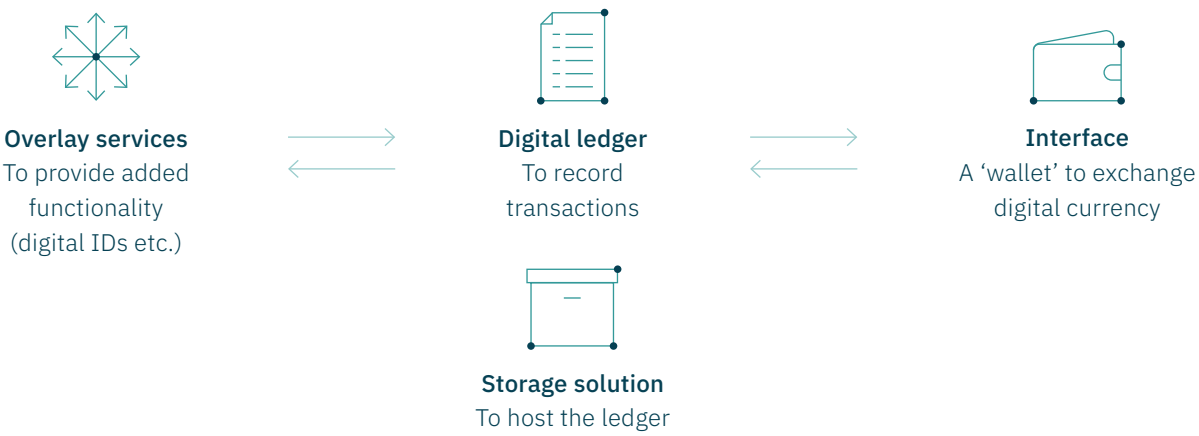
- An anthropological look at how digital currencies could change social norms and behaviour
- The macro- and micro-economic impact of CBDCs, especially for cashback after shocks like Covid
- Links between CBDCs, foreign policy and the global balance of power
- What political architecture needs to be in place to effectively govern a CBDC
- Assessing the optimal way to ensure technical interoperability between different CBDC systems
- How CBDCs will affect the distribution of humanitarian aid and international assistance

We welcome insight into these areas and would be happy to collaborate on any research paper.

The technology behind CBDCs

A CBDC, at minimum, consists of a record of transactions (a ledger) and an interface to enable users to exchange currency. This core ledger, which should be stored in a secure environment, forms the basis of a CBDC and allows assets to be issued by a central bank. On top of this, other products, including for identity management and payment gateways will likely be necessary depending on the purpose of the CBDC.

The basics of CBDC technology



Digital Ledger

The ledger's role is to record central bank liabilities and enable the minting of digital currencies. It should be highly secure, available, resilient, fast, efficient, immutable, and interoperable for recording transactions at the cost of micropayments[14]. This record represents the status of all issued central bank money.

Three common types:

- Traditional database
- WORM database
- Distributed ledger

14 www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

Traditional database

A CBDC could use a traditional database for the ledger of liabilities. Such a record can easily be manipulated. However, such and previous entries amended or deleted by malicious actors. This is therefore ill-equipped for widespread adoption by households and businesses, and not a suitable choice for a CBDC.

Worm database

Write once read many (WORM) systems, including, for example, Oracle-based databases, allow users to store data but not delete entries. CD-Rs share this quality.

Immutability is critical for a CBDC, and in a WORM database, any updates to data entries are instead appended. This is similar to blockchain technology and inherently more secure than traditional databases. WORM databases form the backbone of modern accounting software, often deployed across large-scale industries. Such systems solve the problem of mutability and malicious data manipulation, but since there is only a single copy of a WORM database, data loss is an inherent risk.

Distributed ledger

A distributed ledger is most often associated with CBDC implementations. Examples include Bitcoin^{SV}, Ethereum and Hyperledger.

Distributed ledgers may be either private or public. As the name suggests, the record of transactions is shared across multiple instances, rather than stored in a single place. Data is replicated and synchronised between several entities without the need for a central administrator, making the record more secure against potential attackers. Blockchains, for instance, time-stamp entries of transactions that can be conducted peer-to-peer. This allows transactions to be sent directly from one party to another and then settled on-chain, without going through a financial institution.

Like paper-based double-entry bookkeeping ledgers if any records must be updated or errors corrected, values can be added. The difference is that on the blockchain, values, including errors, cannot be deleted and remain in the record even after corrections. This is to ensure the integrity of data, particularly when being updated and amended.

Token systems overlaid on top of the blockchain can give central banks control of the number and allocation of tokens for government-backed money like a CBDC.

Three important components are used in distributed ledgers like blockchains:

1. Digital signatures
   Private-public key pairs present a way to perform transactions between two parties. For high-value transactions, each participant can use such keys pairs to produce a secure digital identity reference, using certificate authorities and public key infrastructure. The issue of identity forms one of the most important aspects of blockchain technology.

2. Peer-to-peer communication
   Users or clients of the network can engage peer-to-peer, handing transactions directly to one another, before being settled on-chain. All transactions are pseudonymous, maintaining privacy, yet traceable.
3. Public distribution
   When a transaction is authorised, transactions are publicly announced and broadcast across the entire network, making double-spending infeasible. Users can easily query the status of their own transactions and ensure integrity in the order of transactions.

In a blockchain network, node operators publicly announce authorised transactions and update the blockchain – forming the ledger of central bank liabilities – through the creation of blocks.

The miner who wins the right to confirm a transaction and add it to the blockchain must confirm the integrity and validity of the requested transaction, including that the digital cash to be spent has not already been spent, and abide by other rules of the protocol.

Storage Solution

The digital ledger must be stored. This can be done using a private or closed network, or a public network.

Three common types:

- Private server
- Cloud storage
- Blockchain network

Private server

The most basic storage solution is to store the CBDC ledger on a closed network, for which access is restricted. This means it would use an on-site, privately-owned server – not the cloud – that is controlled by a central bank. Private servers can be costly to set up and maintain, and are vulnerable to both attack and system outages.

Using this method to save the database of transactions is not recommended, since it is far less secure. Actors can exert direct control over the protocol of, and data stored using, the underlying network. Any compromise of such entities presents a potential compromise of the system and the data stored therein. Crucially, transaction data can be deleted without leaving a record of the change, allowing malicious actors to cover their tracks, and limiting the ability to hold parties accountable.

Such inherent characteristics make it easier for malicious actors to retain their anonymity and make it more difficult to comply with anti-money laundering (AML) directives and know your customer (KYC) guidelines.

Cloud storage

Storing the CBDC ledger in the cloud, using a service such as Microsoft Azure, Amazon AWS, or Google Cloud, would allow a central bank to reduce fixed costs of running a private server, while also providing the flexibility to scale where necessary. Installing and maintaining server infrastructures can be expensive and requires specific expertise. Amazon claim some key benefits of a cloud architecture setup would be disaster resiliency, security, and throughput[15]. Central banks may employ the services of multiple cloud providers as an insurance against the risk that one fails.

While efficiencies by and large have improved, cloud infrastructure remains expensive for small casual transactions, or any exchange of small sensitive data – and can be prone to data security issues. An exposed vulnerability in Microsoft Azure's flagship Cosmos DB database in August 2021 meant that potential malicious actors could have obtained keys that controlled access to databases held by thousands of companies.

This has raised concerns over consumer privacy – critical for a CBDC – as well as over the fact that large systems would lie in the hands of private cloud providers and corporations. Cloud infrastructure seems therefore less suitable as critical infrastructure for a widespread payment network.

Blockchain network

The ledger can also be stored on a blockchain network. Blockchain technology therefore refers to both the record of transactions (distributed ledger) as well as the storage solution (the public network).

In this design, transactions are announced publicly to the network and are therefore visible, though pseudonymous, by everybody. Each node has an exact copy of the ledger. This makes blockchain uniquely transparent and immutable.

It is important to clarify that many distributed ledger software operate on private networks, including Hyperledger, Ripple, Quorum, and Corda. Although these share a similar design to a blockchain, since both consist of multiple nodes that hold a copy of the record, access to the nodes is restricted since they are hosted in closed networks on the cloud or on private servers. This negates much of the benefit offered by blockchain technology, and such a setup also lacks any inherent ongoing incentive for improvement and innovation beyond the initial investment, by discouraging competition.

A public network such as a blockchain is ideally suited to host the ledger of transactions or central bank liabilities.

15 aws.amazon.com/blogs/publicsector/future-money-digital-how-cloud-deliver-solutions-central-bank-digital-currencies

Comparing the tech

		Storage solution		
		Private server	**Cloud hosted**	**Blockchain network**
Ledger design	Traditional database	Easy to edit or delete stored data without trace. Vulnerable to attack and costly to setup and maintain.	Reduces storage costs and downtime, and is more scalable. Data can still be edited or deleted without trace and it is vulnerable to attack.	Since data can be edited or deleted, records may become desynced. Less cost to setup, but it goes against the very nature of blockchain technology.
	WORM database	Cannot edit or delete stored data without trace, but vulnerable to attack and costly to setup and maintain.	Cannot edit or delete stored data without trace and reduces costs. Database may be vulnerable to attack.	Data is immutable and cannot be changed. The public network is secure against attack and is transparent.
	Distributed ledger	Costly to setup and maintain. Data can be edited or deleted without trace.	Less cost to setup and maintain and less vulnerable to attack. Data can be edited or deleted without trace.	

Interface

A digital wallet, accessed usually using a mobile phone or internet browser, is the most obvious point of connection for users wanting to exchange currency in a retail CBDC. This allows true peer-to-peer exchange between individuals, or even merchants and businesses.

Wallets can simplify and mirror the current digital payment infrastructure where citizens might have their bank card or PayPal saved on a smartphone. The difference is that in a CBDC, peer-to-peer transactions can be settled instantly, and do not require recipients to be online.

Where the penetration of smart phones is low, it is possible to provide an interface to the CBDC via industry standard protocols such as Unstructured Supplementary Service Data (USSD) that can be supported by older GMS based devices.

To drive financial inclusion, it is also worth considering the role of smart cards where data connectivity is unavailable and there is a lack of access to mobile devices.

Apps

We define apps as any overlay software or gateways that interact with a CBDC ledger. Some of these, including identification management, will almost certainly form a necessary part of any CBDC design.

Digital certificates/ID

Identity and payments are closely linked. A digital ID or e-Certificate, such as a digital passport, is likely essential for any CBDC if it is to provide benefits such as KYC and preventing illicit activities, including AML. Permissioned CBDCs with tiered authorisation to access different data fields require robust identity management to ensure users – for example law enforcement – are who they say they are.

Such a product allows tokenising, sharing, and managing identifiable data through certification and audibility.

The benefit of a blockchain, token-based CBDC is that an ID can incorporate any amount of sensitive information including health data, biometric data, or financial data; but do so in a way that protects user privacy by granting businesses and authorities viewing rights only of the essential information needed to, for example, process a transaction.

Payment APIs

APIs to create interoperable digital payment systems that connect citizens, merchants, banks, and other financial providers to services such as VISA, Mastercard or foreign exchange.

Other overlay software

A programmable CBDC would allow for other overlay software to be built on top.

Ask yourself
Which ledger and storage combination makes most sense for you?
How much do you know about blockchain technology?

Conclusion

It is an exciting time for CBDCs. The critical mass of research and pilot projects globally suggest we are not far from a seismic shift in the global payments and banking sectors. This momentum will only increase with every successful CBDC launch, and as in-market large scale products and solutions show the technology is reliable.

Governments and businesses would still be well-advised to take steps to understand the impact such digital currencies will have, how to mitigate against critical risks, and what role they could play in a CBDC system.

This guide has given a comprehensive look at the state and design of digital currencies, but more research, particularly on the areas outlined earlier, would be welcome.

Institutional uncertainty around CBDCs we believe is more closely linked to wrong design choices, rather than inherent to the concept itself. Our view is that CBDCs that use permissioned public blockchain technology can be an immensely effective tool for economic stability, policy execution and financial inclusion, and that this approach presents the most secure and scalable model possible.

More to come

In the meantime, visit our website to stay up to date.

We welcome collaboration, additional insight, and we also offer further expertise. Please get in touch at contact@nchain.com.