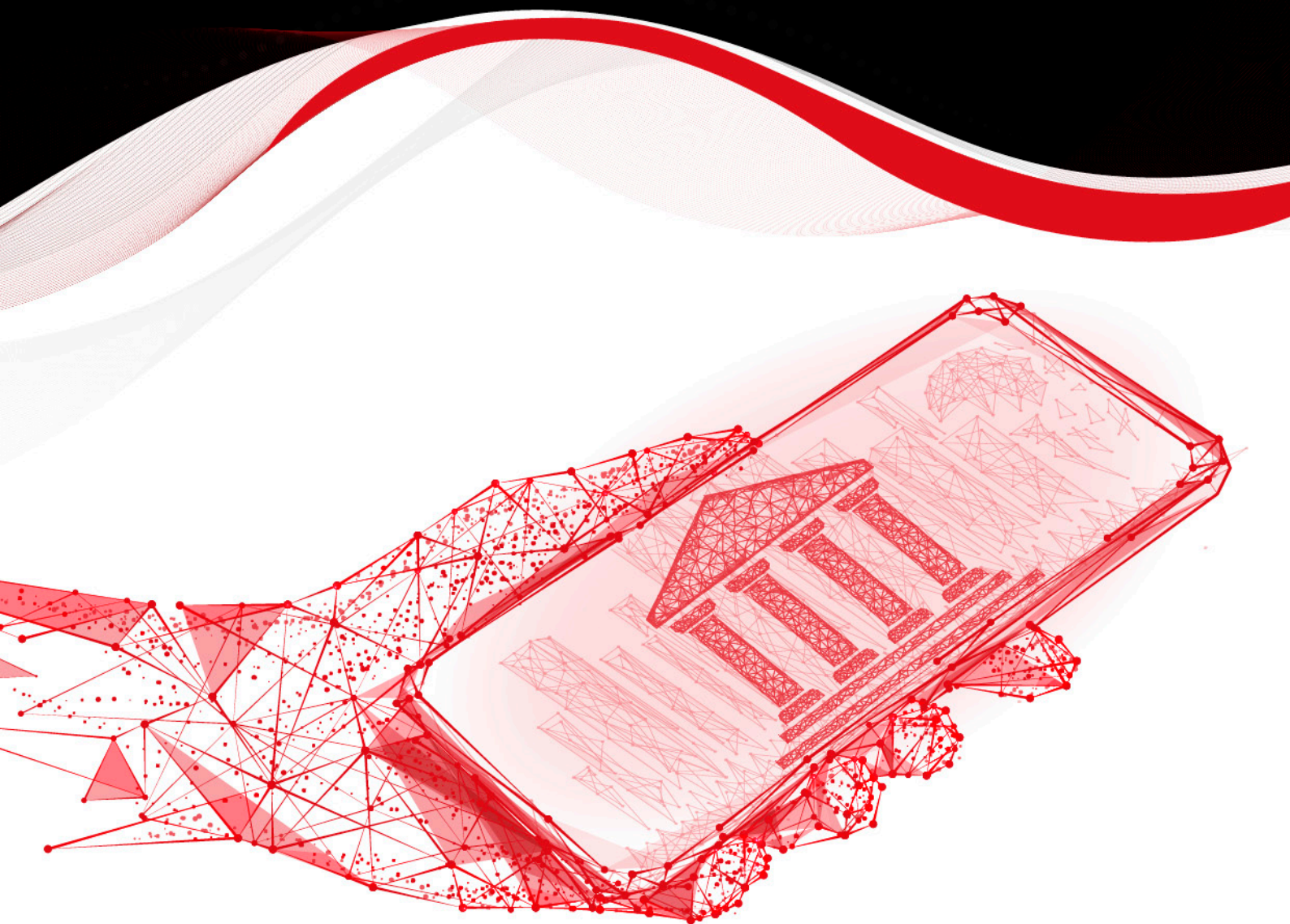


CENTRAL BANK DIGITAL CURRENCIES

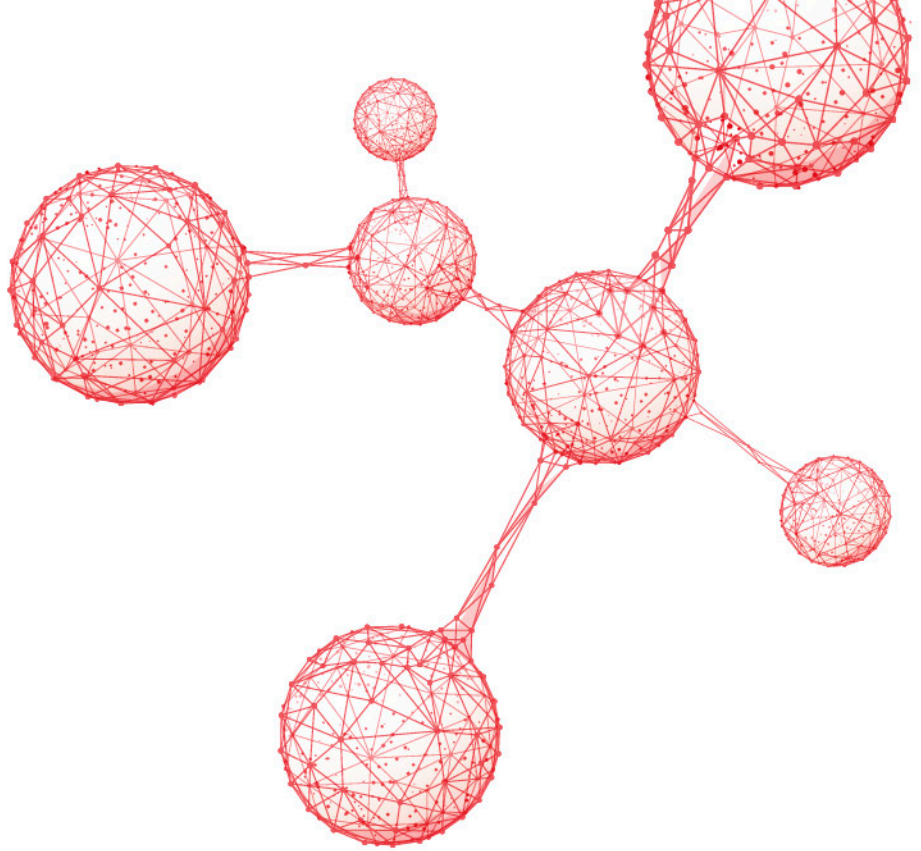
The quest for public digital payment infrastructures



INSTITUT
POLYTECHNIQUE
DE PARIS



BLOCKCHAIN
@POLYTECHNIQUE



Prepared by Xavier Lavayssière.

The author would like to thank Camilla Carabini, Gabriel Soderberg, Noémie Dié, Paul Desprairies, Sonja Davidovic, John Kiff, Kateryna Zhabska, Sebastien Choukroun, Louis Bertucci and Mathias Ros for their inputs and careful reviews, as well as Julien Prat and Daniel Augot for their trust.

The views expressed by the experts are personal opinions and do not necessarily represent their respective organisations.

TABLE OF CONTENTS

| | |
|---|-----------|
| INTRODUCTION | 5 |
| WHAT ARE CENTRAL BANK DIGITAL CURRENCIES?..... | 6 |
| Money and payment | 6 |
| A new public form of money | 7 |
| WHY CENTRAL BANK DIGITAL CURRENCIES?..... | 8 |
| Shifting payment context | 8 |
| Sovereign means of payment | 9 |
| Inclusive and connected infrastructure | 10 |
| Digital monetary policy | 10 |
| The Bahamas - Sand Dollar | 11 |
| HOW TO DESIGN A CBDC? | 12 |
| Design an ecosystem | 12 |
| China - Digital Renminbi | 13 |
| Plan for adoption | 14 |
| Protect financial stability and actors | 15 |
| Legal and political decisions | 16 |
| European Union - Digital Euro | 17 |
| Facilitate interoperability | 18 |
| HOW TO BUILD A CBDC TECHNOLOGICALLY?..... | 20 |
| Core technological arsenal | 20 |
| Pure tokens | 21 |
| User experience | 22 |
| Resilience and security | 23 |
| WHERE ARE WE NOW? | 24 |
| Research and skills | 24 |
| International competition | 25 |
| Competing initiatives | 26 |
| A quest for balance and innovation | 27 |
| GLOSSARY | 28 |
| REFERENCES | 29 |



Blockchain@X is the academic chair on blockchains of École Polytechnique. It was created in 2017 with the support of Capgemini, Nomadic Labs and Caisse des Dépôts. As a multidisciplinary research center, Blockchain@X combines academic excellence with business and technology leadership to accelerate blockchain applied innovation.

Founded by Daniel Augot et Julien Prat, the center brings together researchers in computer science and economics whose research focuses on blockchains and associated technologies. The center has three specific mandates : academic research, teaching and thought-leadership.



"Capgemini, as a world leading IT services & consulting company, must be at the core of the transformation induced by blockchain & distributed ledger technologies.

By partnering with the Blockchain@X Research Center, we express our trust to deepen the overall understanding of these technologies and their current & future impacts on economies, particularly on areas like CBDCs, digital assets, tokenization, Defi"



"At Nomadic Labs, we are working on the core development, evolution and adoption of the Tezos protocol in France, Luxembourg and Belgium.

As one of the largest research and development centers within the Tezos ecosystem, it is important for us to support research in our field. We also help companies and institutions to use the Tezos Blockchain for their business needs, providing technical support."



"Always supporting the common interest, Caisse des Dépôts is both a key player and a supporter in the French Blockchain ecosystem in which the research and development sector is fundamental.

Thanks to the Blockchain@X research center, some technological obstacles could be lifted and this accelerate the emergence of industrial projects in France and Europe."

INTRODUCTION



With these pieces of paper, made of the bark of the Mulberry Tree, The Emperor causes all payments on his own account to be made; and he makes them to pass current universally over all his kingdoms and provinces and territories, and whithersoever his power and sovereignty extends. And nobody, however important he may think himself, dares to refuse them on pain of death. And indeed everybody takes them readily, for wheresoever a person may go throughout the Great Kaan's dominions he shall find these pieces of paper current, and shall be able to transact all sales and purchases of goods by means of them just as well as if they were coins of pure gold. And all the while they are so light that ten bezants' worth does not weigh one golden bezant.

Book of the Marvels of the World - Marco Polo



As economies become increasingly interconnected and digital, the role of central banks in payments and money is challenged. Retail payments have slowly shifted from cash to cards and even mobile applications, accompanied by a shift in actors from public institutions and regulated banks to large tech companies and startups.

Moreover, the 2008 financial crisis and high inflation have eroded the public's trust in financial institutions and regulators. New categories of assets have emerged culturally and technically. In a shifting economic order, crypto assets and projects of global stablecoins question the status of sovereign currencies.

Over the recent years, a new field of options has appeared to propose new public digital infrastructures. Central Bank Digital Currencies (CBDC) are a collection of projects offering a new form of digital money. While inspired initially by crypto assets, CBDCs vary in their objectives and some design elements.

Three characteristics are consistent across CBDC projects. First, CBDCs are a purely digital form of money. This approach, leveraging various techniques and technologies, differs from existing systems that have often been the digital transcription of paper-based processes. Second, CBDCs are a liability of the central bank. In practical terms, this signifies the guarantee of convertibility to other forms of money by the Central Bank. Finally, CBDCs are denominated in a national or regional currency. As such, they are recognised by the national or regional laws, with international consequences.

Central Bank Digital Currencies are a global research and development effort that involves central banks, universities, international organisations, and private companies. They investigate mature and cutting-edge technologies with various designs. A few pioneer projects have been issued already.

However, the research and technical discussions should not hide the most critical underlying political questions that must be investigated. What are the policy goals that require such infrastructure? What should be the respective role of central banks and private actors regarding money creation and payments? What efforts, costs and impact can be anticipated? What design would best fit the needs of the population? How to balance privacy, security and the fight against fraud and financial crimes? What will be the impact of this new form of money on the international monetary order? Are there synergies with other policies, such as social disbursements? And in the end, are CBDCs the most relevant solution to tackle identified problems?

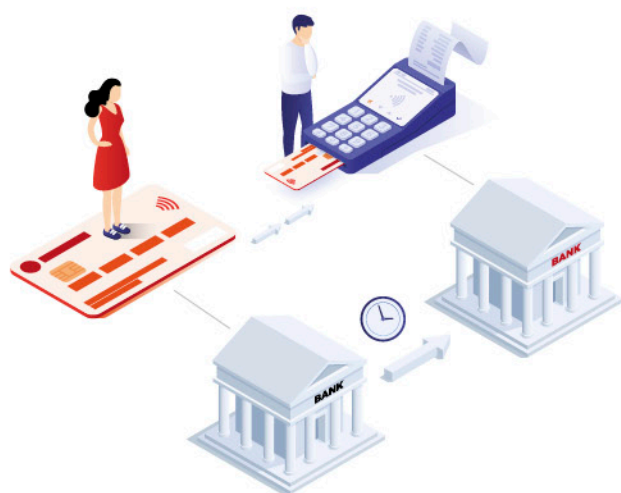
WHAT ARE CENTRAL BANK DIGITAL CURRENCIES?

MONEY AND PAYMENT

To understand CBDCs, we must take a step back to look at **current forms of money**. When effectuating a payment in a shop, for instance, three means of payment could be used. Cash, in the form of banknotes or coins, credit and debit cards, or a payment app such as Lydia, WeChat or Paypal. The three payment methods give access to different forms of money.

Cash is a payment instrument provided as a public-private infrastructure. **Banknotes and coins are issued by the central bank**, distributed by banks and usable by anyone. Transactions are concluded instantly by handing over the physical object. It is guaranteed to be accepted over the territory as legal tender and counterfeiting is illegal. Banknotes and coins usually represent national symbols and figures.

When cash is deposited in a bank account, the bank takes possession of the cash and credits the corresponding amount as a “deposit” in the account. It is a bank’s liability of the bank toward its customers. The bank mainly creates this form of money when asking for a loan. This “bank money” **only exists in the bank’s books**.

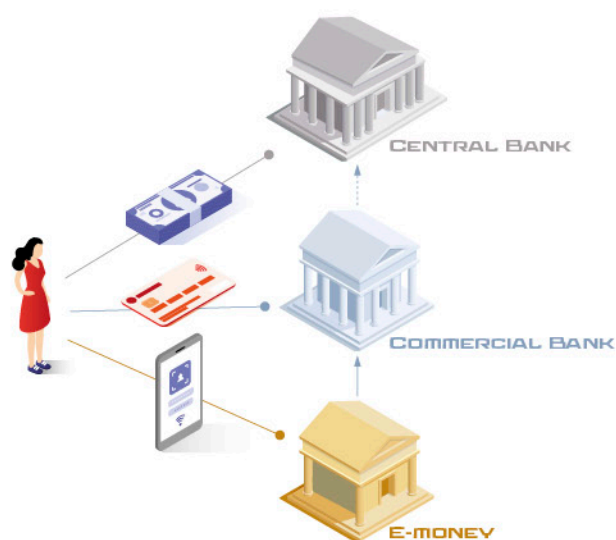


In this example, Alice uses a credit card to sign a transaction to pay Bob. The transaction is settled later.

Because of this, most payments using cards, bank transfers, or cheques are operated in two phases. The first phase is an order to transfer the funds. A payer signs a message to authorise the transfer. This transaction is validated by the payer’s bank and sent to the payee. But the funds

are usually not available instantly. The second phase is the settlement, by which the money is effectively transferred between the banks. Funds are debited by the payer’s bank and credited in the bank’s books of the payee. This process can take a few days.

E-money and Mobile money are convenient digital payment methods provided by private actors. They have grown significantly over the past two decades to offer suitable payments for a wide range of the population. When creating an account, money is added from another source and kept in a reserve. This one-for-one reserve in a commercial bank’s account guarantees the value of the digital instrument. Meanwhile, payments can use various technologies such as phone applications or dedicated cards to pay friends and merchants. As long as the money stays within the same ecosystem there is no need for a settlement between financial institutions. If two users of the same application pay each other, the money never moves from the reserve account.



Main retail payment methods and corresponding liabilities

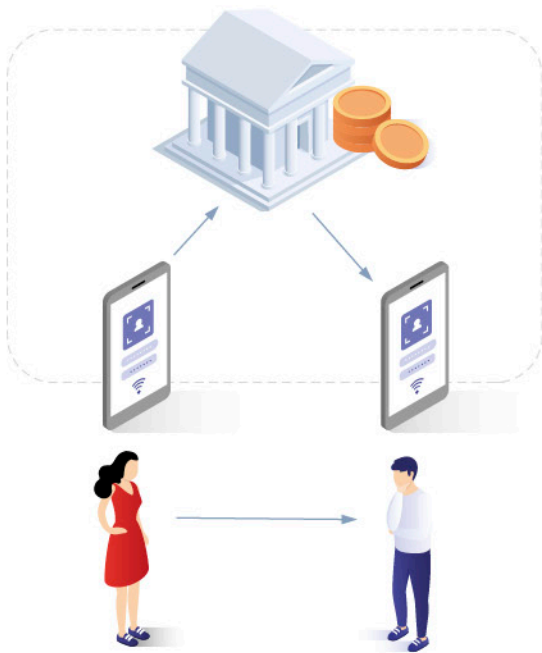
Finally, a form of money exists in the central bank’s books. This digital central bank money is operated like a bank account but guaranteed to the full extent of the central bank’s credibility. **This form of money is available via digital systems that allow banks to settle high-value transactions and obtain liquid money in exchange for financial instruments.** Those systems are generally not available directly to the public.

WHAT ARE CENTRAL BANK DIGITAL CURRENCIES?

A NEW PUBLIC FORM OF MONEY

What value does a CBDC add to these existing options? CBDC is the **public implementation of digital money**. It aims to combine the convenience of cash, some of the technologies of e-money and the central bank's guarantee.

As a digital instrument, it is a **public digital platform** upon which different actors and software applications could be connected. The most important feature of this ecosystem is to allow individuals, businesses or financial institutions to realise **digital payments** between users, companies and banks. It requires a digital infrastructure to keep track of the value and processes and interfaces to allow payments. More advanced functionalities can be added.



To more formally define a CBDC, we can identify three criteria:

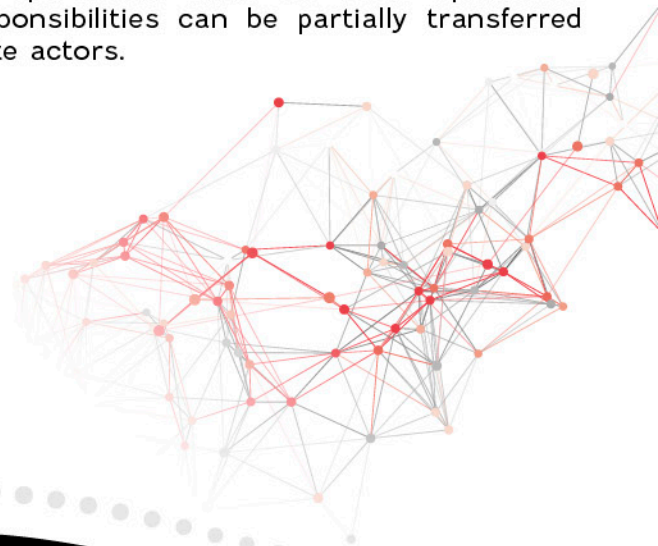
- First, CBDCs are a purely **digital** representation of value. Most banking and payments rely on concepts and processes established in the Italian renaissance. CBDCs leverage the capabilities of the digital world. For instance, payments can be instantaneous, reducing part of the parties' risks.

- Second, CBDCs are a liability **to the central bank**. This secures transactions and funds by alleviating counterparty risks. If a commercial bank goes bankrupt, its customers should still be able to use or retrieve their money in other forms via the central bank. This feature has limited benefit when there is a deposit guarantee for retail users, but it is essential for large financial transactions.

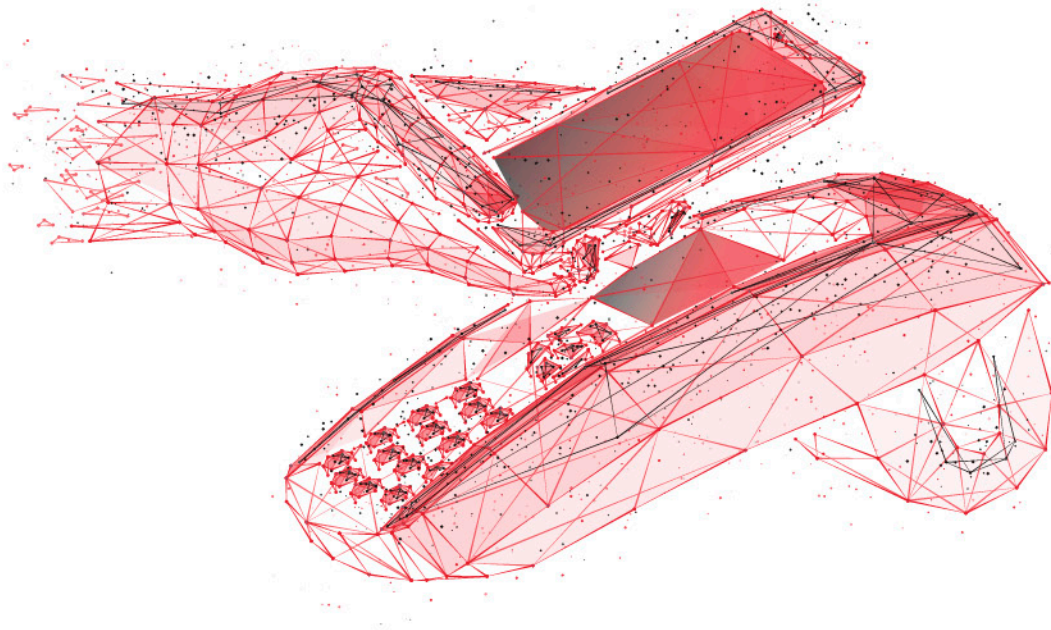
- Finally, **CBDCs are denominated in a national or regional unit of account**. It gives a stable value in the monetary area and legal status. Ultimately, policies, stability and economic strength are determinant to the quality of a CBDC.

An important distinction in CBDCs is whether they are used for daily retail payments or only between financial institutions. The former, a **retail CBDC**, allows payment to be made to a merchant in a physical store or online, between peers, or even to pay taxes. The latter, a **wholesale CBDC** is used between financial organisations to facilitate high-value payments and financial transactions. Wholesale CBDCs functionalities are closer to existing settlement systems between banks.

Currently, retail CBDCs attract most of the attention, but the work on **wholesale CBDCs** might have a **profound infrastructural impact**. A wholesale CBDC could fulfil some of the functionalities of current central banks' infrastructures operations, facilitate financial market infrastructures operations and allow the emergence of new cross-border payments platforms. Moreover, a well designed retail CBDC requires the adequate design of the wholesale level of operations, while the retail operations and responsibilities can be partially transferred to private actors.



WHY CENTRAL BANK DIGITAL CURRENCIES?



SHIFTING PAYMENT CONTEXT

A set of potential benefits have been identified for CBDCs, with various levels of relevance. Ultimately, priorities depend on the particular context of each country.

Looking at retail payments first. **Cash is still the most used method for paying in a store or between individuals.** In the Euro Area, they represent 73% in those cases and even 92% for transactions below 5€². While cash usage has fallen below 10% in Nordic countries in a few years, its decline is gradual in most of the world. Moreover, cash is also used for storing value within a country and abroad for global currencies. Therefore, demand for cash is generally increasing. Cash is likely to be maintained in the foreseeable future, even with the advent of a CBDC.

Digital payments are provided by a large industry with numerous actors. Economically and technically, solutions are fragmented. Payment apps, for instance, often come with their own ecosystems, with limited interoperability between them. Underlying technologies spread in complex architectures from legacy to APIs across various types of acquirers and issuers.

In particular, the main forms of digital payment in developed countries, credit and debit cards, are **dominated by a few large companies.** While card schemes such as Visa and Mastercard are the most visible, a handful of companies control various aspects of card payments behind the scenes, such as point-of-sale terminals, payment gateways, and routers. As a result, each payment incurs a substantial fee paid by the merchant. Moreover, monopolistic tech companies like Apple or Google have entered the space, providing mobile interfaces for contactless card payments and other services. This concentration is an increasing policy concern.

Finally, elephants entered the room. Bitcoin has proven the possibility of providing a global asset and payment system relying mostly on technology. As an asset, it maintains a fluctuating but sustained interest. With additional innovations such as *smart contracts* or *layer two* networks, **crypto assets have developed payment methods with advanced functionalities.** They have allowed the creation of a vivid ecosystem of monetary and financial instruments.

WHY CENTRAL BANK DIGITAL CURRENCIES?

SOVEREIGN MEANS OF PAYMENT

Among crypto assets, stablecoins combine relative stability and new technologies. Using different mechanisms, such as on-chain or traditional reserves, they offer the advantages of crypto assets with a value determined in a fiat currency. While they have been mostly used for market arbitrage, their global and interoperable infrastructure offer potential as a new generation of electronic money. This possibility became particularly obvious when a prominent tech company challenged existing currencies with a **potential new global payment system**³. The vitality of stablecoins is not without raising consumer protection and financial stability questions that have led to the development of dedicated regulations.

Beyond technology, the international monetary system has been challenged over the past decades. The slow erosion of trust or political decisions in some countries has led to adopting foreign currencies, a phenomenon known as currency substitution. Intense financial crises have also led to some national currencies' sudden loss of value. Conversely, the growth of the Chinese economy and its importance in international trade have contributed to promoting the Renminbi as an international currency. Moreover, geopolitical factors such as the increased use of financial sanctions by the United States encourage the usage of other currencies and the development of alternative cross-border platforms.

Therefore, among the first motivations is the **sovereignty of the payment system**. CBDCs are seen as a way to gain leverage in the situation of oligopolies on payment and over potential foreign influence. They can provide an alternative payment system with a different risk profile than existing platforms. If there is a hack or a geopolitical conflict, states could not be as dependent on solutions provided by foreign private actors. As economies are increasingly digital, this becomes a critical question. Moreover, convenience, availability, and robustness reinforce sovereignty over money and monetary policy. If users can pay reliably with a currency, they might be more likely to use it. The technological quality reinforces the role of the currency over the territory and internationally.



The challenge is that big tech or decentralised systems are viable alternatives that will bleed off people from the banking system if there is not a government option to respond to it.

David Yermack

INCLUSIVE AND CONNECTED INFRASTRUCTURE

A key motivation for CBDCs is to provide a common and low-cost payment infrastructure. Private actors could more easily participate in the payment industry, and new use cases could emerge. Instead of replicating a costly infrastructure, new startups could leverage systems provided by the public sector to offer additional services for the users or other market actors. However, this requires network effects and designing appropriate business models for those actors. CBDC payments are generally intended to be free. From the operator of the system, internal costs must remain low.

A policy goal often presented as a result is **financial inclusion**: to provide digital payment solutions for those that do not have access to bank accounts. In some countries, banks do not have the capacity or financial interest to reach all customer segments⁴. While a CBDC will not be a full bank account, it will offer some practical benefits. For instance, it can preempt the need for vulnerable populations to store or transport cash over distances, which can be dangerous and time-consuming⁵. Moreover, this might be

the first step to accessing other services, such as microloans based on payment history or transaction data. As we will see below, there are challenges to achieving this goal with a CBDC.

A CBDC could also provide a **guaranteed settlement asset** and advanced functionalities. A CBDC, conceived as a public digital platform, can facilitate settlements between banks for retail payments. This is particularly relevant for countries which do not yet have that infrastructure. It could also facilitate the development of cross-border payments, particularly relevant in economies that rely on remittances.

Finally, it could allow the development of **more efficient financial market infrastructures**. As financial instruments are represented in new digital forms⁶, the availability of central bank money would facilitate the settlement of financial transactions. The delivery of financial instruments against a CBDC payment has been experimented by, for instance, the Bank de France⁷. As Decentralised Finance shows, composability could offer promising outcomes.



The key to digital finance is digital cash. To move forward with digital assets, we need a wholesale CBDC

Philippe Laurensy

DIGITAL MONETARY POLICY

A general idea for CBDCs is to use it to refine the monetary policy. Get better data and level for action. Payments from the government to people (G2P), for instance, have shown relevance during the pandemic. However, it can be difficult and costly to identify who would benefit from financial help and how to deliver it effectively. A CBDC could provide a solution to **send financial help** in different manners. For instance, in the case of a natural catastrophe, a CBDC could be delivered to inhabitants of a specific region via online accounts or on offline mediums such as physical cards. Those capabilities would facilitate targeted social disbursements⁸.

By providing a convenient digital means of payment, a CBDC might accelerate the shift from

cash. A shift could **reduce the informal economy** and facilitate compliance. Once transactions are digital, hiding them from fiscal authorities might be more difficult. Other law enforcement operations might be facilitated too. However, those objectives must be balanced with inclusiveness and privacy considerations. Requiring identification or limited privacy guarantees may deter categories of users from using it.

Another motivation for the central bank is the ability to **monitor flows in the economy**. Monitoring money flows provides insight into the dynamics of certain sectors or the speed of money circulation. This might allow policymakers to react in real-time, improve nowcasts and forecasts and design better monetary responses⁹.



The ability to pay is a public good. There is a need for a public alternative to commercial payments

Andreas Park

4- Chiu et al. 2019 / 5- WEF 2021 / 6- HCJP 2022
7- Banque de France 2021 / 8- Prat et al. 2020
9- Glannone et al. 2008



THE BAHAMAS SAND DOLLAR

The Sand Dollar is an interesting example of a project designed to answer specific local needs. Among the main objectives of the central bank of The Bahamas there was resiliency, reduction of the cost of services, financial inclusion strengthening national defences against money laundering¹⁰.

In the context of a country made of small islands, a central bank digital currency is a great way to reduce costs associated with transporting cash. Moreover, the country is subject to hurricanes, such as Dorian in 2019, which significantly disrupted business operations. It might be easier to bring back online a digital platform and even mobile networks than reopening bank branches and provisioning ATMs with cash.

The CBDC project was particularly fast from its initial research in 2017 to its launch in 2020. New financial infrastructures could be built with little legacy technological and institutional constraints. The approach selected is to provide a comprehensive retail CBDC solution and the infrastructure for wholesale operations. The central bank endorses a multi-purpose role, including currency issuance and monitoring. However, most developments were conducted by a third-party technology provider. They handle the data on the CBDC accounts, provide a primary wallet and offer a programmatic interface (API). This interface allows third-party providers, including banks, to integrate the CBDC into their own applications.

More importantly, user adoption appears central after its limited initial success. The central bank of the Bahamas noticed the importance of partnership with private actors, education and engagement with the population. As it was launched during the pandemic, reaching physically those that would need it the most was difficult.



*Digital Bahamian Sand Dollar Wallet -
© 2022 Sand Dollar.*

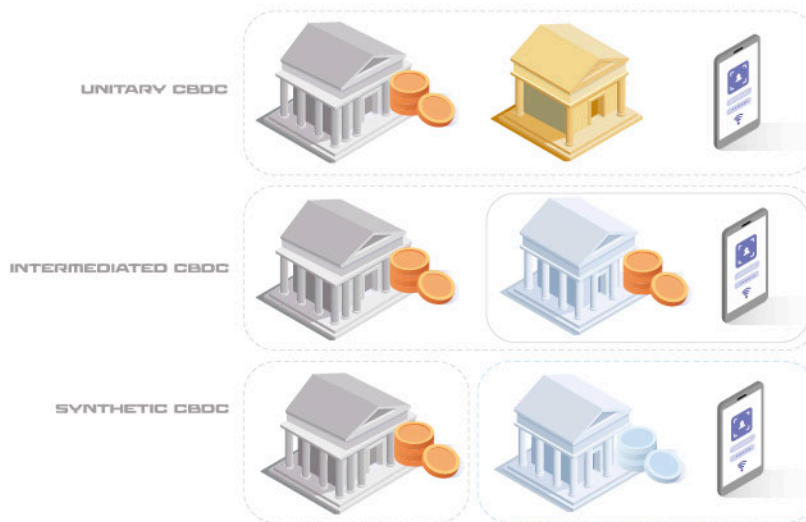
10- Central Bank of The Bahamas 2019

HOW TO DESIGN A CBDC?

DESIGN AN ECOSYSTEM

New technological trends inspired some early ideas of CBDCs. As research has grown over the years, those models must be adapted to fit a particular country or region's economic, cultural, technical and legal needs and structures. Many projects have shifted toward a more conventional approach, relying partially on existing financial institutions. The level of intermediation of financial institutions in the operations and additional services of the CBDC establish theoretical categories of CBDCs.

In a **unitary CBDC**¹¹, the central bank fully provides the service. The central bank offers wallets, establishes compliance procedures, and manages users' balances. Operators can provide some or all of those services under a contract with the central bank. In a strict sense, this model is rather theoretical.



Three levels of intermediation of a CBDC

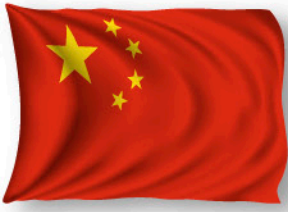
In an **intermediated CBDC**, financial institutions are responsible for onboarding users and managing their balances. The central bank controls the issuance and is the guarantor of the system. The base infrastructure is provided by the central bank or its service providers. Some reconciliation mechanisms must be designed to ensure coherence between the actions of financial institutions.

In a **synthetic CBDC**, private actors issue a digital means of payment that the central bank supervises and fully guarantees. This model would be operationally similar to e-money or a stablecoin backed by a central bank account or a wholesale CBDC. The distinction, still subject to a semantic debate, depends on the initiative and responsibilities of the central bank. Private-led initiatives are considered e-money or stablecoins, while a CBDC is developed under the central bank's initiative.

In practice, all CBDC projects are public-private partnerships. The distinction between the three depends on the nature of the contractual relationship between the central bank and private actors. In a unitary CBDC, most responsibilities are kept by the central bank. Operators are selected via a call for tender. In an intermediated CBDC, where substantial parts of the operations are conducted by private actors, laws and regulations establish the requirements to join the project. In a synthetic CBDC, there is a functional disconnection between the central bank's systems and private actors' operations.

Public-private partnerships demand to combine policy objectives and find suitable business models for private actors. As CBDCs are generally intended to be free for users, new economic models should be devised. Among the options, there is the possibility of direct remuneration by the central bank and the opportunities for complementary business models.

¹¹- Unitary CBDCs are also referred to as direct or unilateral CBDCs



CHINA DIGITAL RENMINBI

The Digital Renminbi (e-CNY) is a substantial undertaking at the crossroads of various policy questions.

The Chinese population has already widely adopted digital payment solutions. WeChat and Alipay are massive national successes with hundreds of millions of users. They fit everyday habits as well as traditions, such as the ability to send monetary gifts in “red envelopes” (Hongbao). They have developed lucrative business models relying on their ecosystems and user data. An example of such innovation is the ability to provide loans to SMEs based on their up-to-date payment data.

This private duopoly on payments challenged existing banks and the role of the public sector. Over the past years, they have been subject to antitrust action to force them to open their ecosystem. Moreover, a portion of the Chinese population still lacks access to essential financial services, particularly in rural areas, despite the People’s Bank of China (PBOC) efforts over the past two decades.

To conduct its CBDC project, the PBOC has worked with the private sector while developing its own capacity. The central bank launched an initial study group in 2014. Then, the PBOC has hired people internally, conducted small-scale experiments and large-scale pilots, including during the 2022 Olympics games. The People’s Bank of China grew its technological expertise and assessed the project’s fitness to China’s society and economy. The digital infrastructure leverages the experience of Chinese tech companies in terms of robustness and transaction handling. With a simple design, the main wallet application is meant to be easy to use. It seems to have been downloaded by one-fifth of the population, with positive feedback¹².

The application can be connected to various financial service providers, including bank accounts to replenish the account and the digital “super apps” to proceed with digital payments¹³. E-CNY is a payment solution that acts as a point of entry to a wide digital ecosystem.



12- Official numbers and survey conducted on 1000 Chinese respondents Survey conducted by <https://morningconsult.com/2022/06/13/e-cny-adoption-in-china-is-coming/>

13- PBOC 2021

HOW TO DESIGN A CBDC?

PLAN FOR ADOPTION

Adoption is one of the most challenging aspects of designing a CBDC. Most CBDC launches and pilots have received a mixed response from the public. While current CBDC projects have different adoption targets depending on the country, reaching those targets is a balancing exercise.

The first factor is **user-centric design**. Payments are cultural, and they must fit the local needs. Depending on the country or region, people may prefer to use an app, a specific device, or cash. They might transact in different currencies and choose to receive payments in a form that they can easily use to pay themselves. Particular conditions such as a shortage in the network need to be addressed too. As an example of diversified adoption, mobile money was a success in sub-Saharan Africa, while it didn't catch on in Europe.



Designing and building a CBDC with the user in mind is essential in facilitating user adoption.

Sonja Davidovic

Moreover, different profiles of users have other requirements. For instance, accepting a new form of payment requires investment in devices, training, and accounting procedures from merchants. **New opportunities or lower fees must balance new costs.** For instance, Merchants have been instrumental in the success of mobile money, partly as they saw the opportunity to provide a new service that would attract customers.

Adoption is particularly critical to reaching financial inclusion goals. The initial situation is vastly contrasted between countries. According to the World Bank, more than 99% per cent of residents in Germany and Nordic countries have a bank account or a mobile money service provider. It falls below 50% in Argentina or Colombia and below 10% in central Africa. **Root causes of financial exclusion such as digital**

and financial illiteracy are not easily addressed by issuing a CBDC. Populations struggling with existing payment solutions might find it even more challenging to adopt new payment methods. Existing discrepancies between men and women or populations in urban and rural areas on access to bank accounts and relevant literacy could be reinforced without targeted policies.

CBDCs could provide additional financial incentives. The principal opportunity is reducing merchants' debit and credit card interchange fees and worker's remittance fees. Some projects consider paying an interest rate to the amounts held in CBDC or lower taxation on transactions conducted via the CBDC. These incentives will require a delicate balancing act with broader economic concerns.



HOW TO DESIGN A CBDC?

PROTECT FINANCIAL STABILITY AND ACTORS



And the Kaan causes every year to be made such a vast quantity of this money, which costs him nothing, that it must equal in amount all the treasure in the world.

Book of the Marvels of the World - Marco Polo

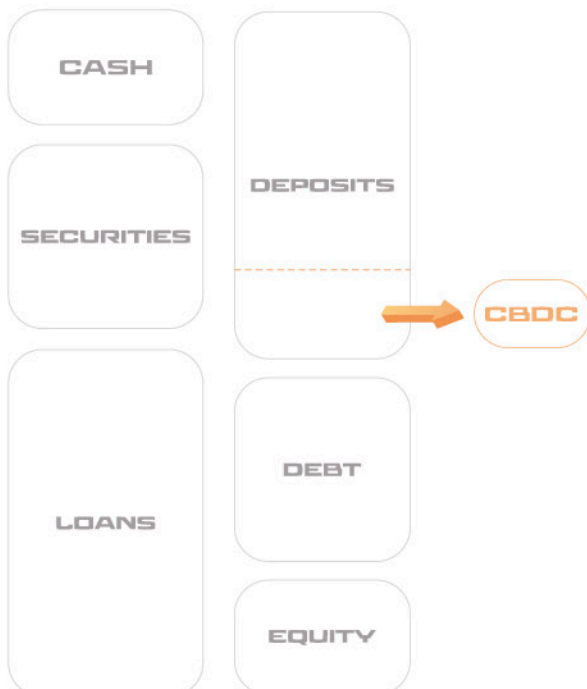
CBDCs challenge the role of banks in money creation and competition in the payment market. Currently, banks create money by issuing loans and are required to maintain ratios between those loans, their capital and clients' deposits for financial stability reasons. With a CBDC, they might lose part of those deposits. They would become a liability to the central bank. The central bank would become a more prominent financial actor, increasing the size of its balance sheet. Meanwhile, financial resilience and loan issuance capabilities could be reduced¹⁴.

One idea to solve this is to **limit the CBDC supply**. This can be achieved with a limit on the amount held in a wallet, a "cap". For instance, the Nigerian central bank has set daily transaction and balance limits on e-Naira. Another possibility would be to have negative or low-interest rates compared to the rest of the economy. However, such measures might not be practical or acceptable for users.

More generally, there are **competition** concerns¹⁵. As a CBDC becomes a major payment instrument, how to incentivise payment companies to compete and innovate in this market? The current primary approach is to make the financial sector, including startups, stakeholders of the CBDC ecosystem.

A CBDC could also reinforce **currency substitution**. In some countries, foreign currencies are used for exchanges and as a reserve. It can result from the population and business choices due to a lack of trust in the national currency or a political decision. A foreign CBDC, convenient to use and denominated in a trusted currency, might be preferred to the local currency.

Finally, the value of the CBDC could fluctuate compared to other forms of money. This **asset parity** requires legal and operational guarantees to always allow the conversion at par between the various forms of money.



Effect of a CBDC on the balance sheet of a bank

HOW TO DESIGN A CBDC?

LEGAL AND POLITICAL DECISIONS

To change the form of money involves a series of legal and political decisions. As money touches different points of society and institutions, a CBDC project relates to multiple bodies of law. Some legal questions are formal, but others will be subject to significant political debates.

The first question is whether the central bank is allowed to issue this new form of money¹⁶. The **role and abilities of the central bank are constrained**. A legal document defines them, such as the constitution, a law or a treaty. Most of them have not been drafted in the digital age, so they have to be adapted, which might require a lengthy institutional and political process.

The second question is the **status of the currency**. For instance, will every merchant have to accept it? This obligation is generally referred to as “*Legal Tender*”. Such a measure presumes that the instrument is available conveniently to every merchant. Otherwise, it would be ineffective. Exceptions could be carved out legally or by allowing it contractually. Moreover, other elements of monetary laws, such as the prohibition of counterfeiting, will have to be adapted.

The most practical impact will stem from **compliance**. As this instrument is handed to millions of users, financial institutions, as well as the central bank, will have to apply existing frameworks and devise strategies to tackle illicit activities such as payment fraud, theft, money laundering, and sanction evasion.

Ex-ante procedures such as the identification of customers will be applied. A common idea is to offer **tiers of identification**. Below a threshold, transactions might be partially anonymous. Above the threshold, a digital copy of a governmental identity document (ID) could be required. For the Bahamian Sand dollar, the first tier without governmental ID limits holdings to \$500 and monthly transactions to \$1,500. With a government-issued identification document, those limits are \$8,000 in holdings and \$10,000, and the account can be linked to a bank account¹⁷.

However, current implementations might not fully address privacy and financial inclusion concerns. Data on low-level transactions is still available, protected to the extent of the law and the security measures of the central bank and operators. The lack of identification means is already a key factor of financial exclusion. Portions of the population do not have such documents as recent immigrants. Therefore, the effects of the thresholds will have to be measured.

During operations, ex-post procedures will **analyse and monitor payments**. Regulated financial institutions have dedicated compliance teams and software analysing transaction data. Suspicious transactions can be reported to public authorities or even blocked directly. However, the efficiency of this model is debated. Rules and implementation vary, compliance is costly, and public authorities do not always have the means to investigate reports. In the end, large volumes of illegal transactions still circulate via the financial system. A CBDC could be an opportunity to revise those strategies.

This raises the question of the **responsibilities** of the various actors of the payment chain, with a more prominent role of the central bank. Various payment regulations will have to be implemented, such as the possibility to cancel fraudulent payments¹⁸ or procedures to deal with failures.

It is important to note that **public opinion has not been fully formed yet on these matters**. Interactions between central banks and the broader public have been limited to surveys¹⁹ and public consultations. As a CBDC is a complex undertaking, large debates and different designs will likely be adopted depending on the values of each country.



Registration requirements per stored amount

16- Bossu & al 2020

17- <https://www.sanddollar.bs/individual>
18- In the EU, fraudulent payments can be cancelled up to 13 months

19- For instance see a survey of EU citizens at ECB-Kantar Public 2022



EUROPEAN UNION DIGITAL EURO

In the European Union (EU), several strategic motivations exist for issuing a digital euro. European citizens increasingly use digital payments, and the European Central Bank (ECB) or the European private sector does not provide complete solutions. A digital euro might also help to reinforce European Economic and Financial integration and support EU competitiveness, providing a solution for local and foreign businesses, travellers and investors.

Part of the EU's difficulty is navigating governance with multiple layers. The digital euro investigations are conducted by the Eurosystem comprising the ECB and the member states that have adopted the Euro. Moreover, such an undertaking would likely require cooperation with the other EU institutions and potentially a modification of the EU treaties.

The Eurosystem already shares a few common infrastructures. The backbone is the real-time gross settlement system (RTGS) called TARGET²⁰. Its second version, launched in 2008, handles billions of euros and hundreds of thousands of transactions daily, settled in less than a minute. TARGET 2 Securities, one of its secondary systems, can settle transactions with financial instruments. Finally, TARGET Instant Payment Settlement (TIPS) was launched in 2018 to allow account-to-account transfers. Two banks participating in TARGET can offer direct and instantaneous transfers between individual accounts. However, this system is restricted to some financial institutions and has limited usage.

The investigation on the digital euro started in late 2019, informally first. In parallel, national central banks were conducting experiments. Central banks strongly involved in the operations of Target 2 have been particularly active: Banque de France, Deutsche Bundesbank, Banco de España and Banca d'Italia. In October 2020 the first report was published²¹. It devises high-level requirements for a digital euro and design options.

The core principles for a digital euro established in this report are that every euro should have the same value. Cash, money in a bank account and digital euros must be equivalent. This requires that conversion can be operated at any time between them. The digital euro, as central bank money, is a liability of the Eurosystem. It must be widely accessible in all euro area countries through supervised service providers and it should not crowd out private solutions. This is probably one of the most difficult points to balance. Finally, a digital euro should be trusted by end-users.

In July 2021, the decision to formally launch a 24-month investigation was announced. The ECB and national central banks are conducting technical experiments and surveys and collaborating with stakeholders. A final decision on whether a digital euro will be launched is expected in fall 2023.

While it is plausible that a digital euro will be launched, it will have different impacts depending on design decisions. Among the technical options discussed, there is the possibility to develop the capabilities of TIPS, develop a hybrid solution combining TIPS and DLT technologies, or investigate a fully new platform²².

20- For a complete presentation of EU systems see Banque de France 2021

21- See ECB 2020

22- See ECB digital euro report and experimentations' reports published by national banks.

HOW TO DESIGN A CBDC?

FACILITATE INTEROPERABILITY

To be used in retail or wholesale payments, a CBDC should be connected to other systems. This includes other national payment systems, service providers and international systems. The difficulty is that the payment industry is fragmented nationally and internationally. For instance, to exchange a CBDC for bank money,

the systems of the bank must be connected to the CBDC platform. Multiplied by the various participants in the CBDC project, this might represent an important undertaking. Moreover, legacy systems might not provide convenient programmatic interfaces (APIs) or even network connections.



The provision of wholesale CBDC prevents market fragmentation, thanks to giving access to a common and safe settlement asset usable by market stakeholders while it could help make cross-border payments faster and cheaper by creating interoperable multi-CBDC arrangements across jurisdictions.

François Villeroy de Galhau

There is already a standardisation effort in the payment industry. An element of this standardisation stems from regulatory requirements. For instance, open banking laws have pushed banks to offer APIs. This effort aimed at facilitating the emergence of new fintechs is still incomplete. It has been recently redoubled with the notion of open finance to expand it beyond banks. Another element has been universal technology standards. The internet technology stack (TCP/IP) has replaced proprietary networks. Web standards such as REST have been adopted by financial APIs. More industry-specific standards, such as ISO 20022, build on those web standards to define the format of financial messages.

The recent efforts to create common national payment infrastructures might facilitate interoperability. CBDCs share similar objectives. They could reuse some concepts or share technical components. They might even be redundant. The strategic question is to decide the pivot infrastructure that will facilitate conversion from one form of money to another. Pix, a Fast Payment System in Brazil and Unified Payments Interface (UPI) in India are good examples of such successfully common infrastructure.

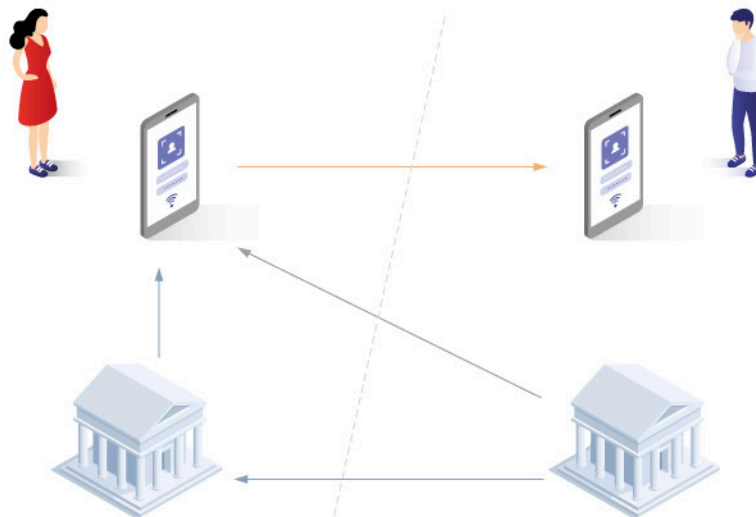
HOW TO DESIGN A CBDC?



The Pix system was mandatory for large banks. Then, small banks wanted to jump on it. In the end, it is the best way for them to offer a payment system and stay competitive with large banks

Darell Duffie

Cross border payments are presented as an opportunity for CBDCs. Correspondent banking is complex and costly. However, two levels of interconnections raise challenges. At the first level, there are practical questions on **how a foreign individual or business can access the CBDC**. Can foreign apps integrate the CBDC? Can foreign financial institutions hold the CBDC? Otherwise, can foreigners easily create an account upon arriving in the country?



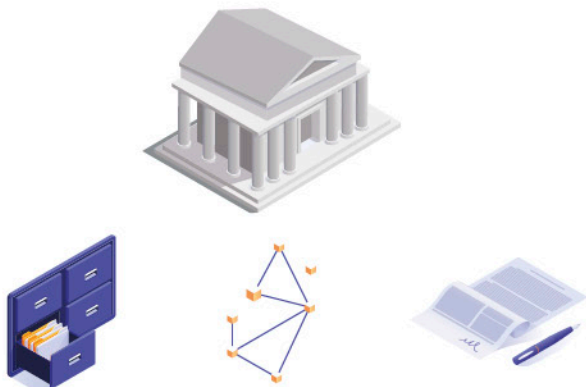
Alice could access a foreign CBDC via her bank or by creating a local account.

The second level is the processing of international payments. International CBDC payments, starting from its acquisition by a foreign entity, will require a **change operation and the connection of digital systems**, raising economic, technical and regulatory challenges. Those connections could be built via common standards, cooperation, or building settlement platforms. Several such platforms are currently being experimented such as Dunbar, m-CBDC and Jura. It will likely be a domain of fierce competition with potentially new forms of fragmentation.

HOW TO BUILD A CBDC TECHNOLOGICALLY?

CORE TECHNOLOGICAL ARSENAL

The core technological challenge of a CBDC is to provide a **nationwide solution for payments**. It must be resilient, offer reasonable privacy guarantees, handle a large number of transactions, minimise fraud and offer guarantees against counterfeiting. All of which are more challenging in a digital environment than with physical cash. Simply put, the perfect solution does not exist.



Three main levels of operations could be distinguished. A **core infrastructure** operated directly by the central bank. An **intermediary layer** whose role depends on the model opted for the CBDC²³. And **access for end-users** for retail CBDCs. A wholesale CBDC or synthetic CBDC will require a robust core infrastructure with a limited number of transactions and programmatic interfaces. Unitary and intermediated CBDCs, on the other hand, may require high throughput of transactions and a more complete design.

Across those layers, various categories of technologies could be used: **Highly efficient distributed databases**, provided by the central bank or partially shared with intermediaries, **Distributed Ledger Technologies (DLT)** to provide a secure wholesale operation level, and **digital bearer instruments**.

In any case, a CBDC will be a **distributed system**²⁴. Most modern computing relies on coordinating several processors, computers, and software. When operations are intensive, they are run in parallel. This is the case when rendering 3D animation, handling millions of players, or processing hundreds of thousands of transactions per second during commercial events. A combination of techniques, relying on a

network of computers, ensures that the system is always responsive to the user while absorbing the load of transactions and maintaining data consistency.

In line with those examples, various CBDCs are delivering systems centred on highly efficient **distributed databases**. The industry already offers on-the-shelf and mature database solutions. One of the workstreams of the ECB is focused on ensuring high availability and throughput of transactions leveraging the existing system, TIPS²⁵. The more experimental Open CBDC project²⁶ combines some data models of Bitcoin with such an approach. Those models generally require connectivity and offer limited privacy.

The Bitcoin blockchain has been an inspiration to conceive CBDCs²⁷. Subsequent projects, such as Diem, reusing some blockchain concepts within a permissioned system have led to using the ambiguous term Distributed Ledger Technologies (DLT) to accommodate various technologies. In those decentralised models, **transactions are replicated and potentially validated among participants**. It generally limits throughput to the capabilities of the weakest node. There are also other tradeoffs. Software updates, for instance, must be coordinated among participants to obtain a resilient system.

In practice, DLT are relevant as a core infrastructure for wholesale CBDC scenarios if similar technologies are adopted by financial market infrastructures or by adding a second layer of operations. Intermediaries could handle high throughput with other technologies, either more conventional or using “Layer 2” solutions developed in the blockchain ecosystem. Some CBDC projects have even considered the possibility of using public blockchains as infrastructure.

Several **intermediary models** are considered. Part of the throughput and data could be managed independently by financial intermediaries and consolidated at the central bank level. In those cases, technology and ecosystem design are strongly related. Such intermediation can offer more flexibility and room for innovation, but guaranteeing the integrity of data scattered among various actors is a technical challenge.

23- See section “Design an ecosystem” above.

24- Tannenbaum 2017

25- See box above “European Union-Digital Euro”

26- Lovejoy 2022

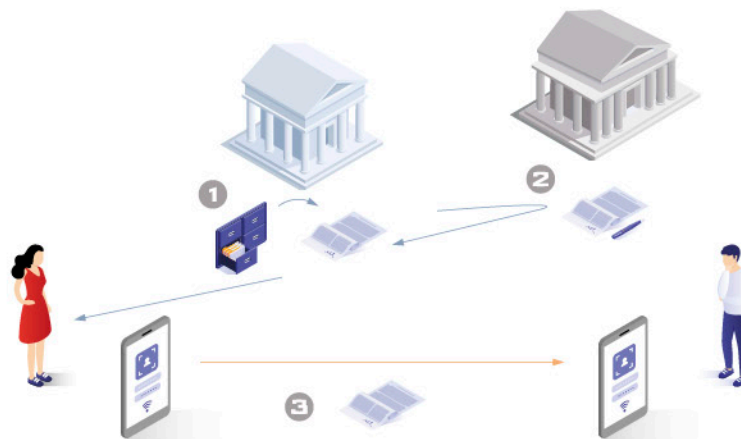
27- Koning 2014

HOW TO BUILD A CBDC TECHNOLOGICALLY?

PURE TOKENS

A radically different category of approaches relies on a pure bearer instrument secured by cryptography. The general idea is that the money in a regular bank account or a CBDC online account is converted to a **digital banknote signed by the central bank**²⁸. This digital banknote can be held

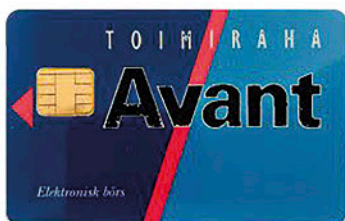
by the end-user on a phone. The loss of the phone would generally result in a loss of funds. Using blind signatures, such a system can guarantee privacy and integrity. This approach can be used in conjunction with a more conventional CBDC.



The digital banknote instrument is (1) attributed to a user by converting bank money, (2) signed by the central bank, and (3) transferred in a peer-to-peer manner.

A variant of this model can be guaranteed by **secure hardware**. Similarly, as above, the first step consists in withdrawing the funds from an account. The funds are stored using a dedicated secure element. This secure element can be in a dedicated payment card or in a smartphone. The secure element will guarantee the digital banknote origin and update the balance with each payment. Several consecutive offline payments can be processed this way. This model was used in the “Avant card” in the 1990s, in what can be considered the first CBDC²⁹.

A recurring question is whether the digital representation is only a representation of a contractual relationship between the user and a financial institution or if it is a digital bearer instrument. It leads to a confusing conversation as it might designate different properties depending on whether we look at it from a technical, legal, or economic point of view. For instance, a private key works as a bearer instrument for public blockchains but still relies on being connected to the blockchain network. If a CBDC uses a permissioned DLT, the relationship will likely be operated as an account by the actor giving access to it. A CBDC could use the same technology as bearer instruments to handle payments while maintaining the identity and contractual relationship with users.



Token and account cover various meanings depending on the context. We should rather discuss the different underlying properties

Neha Narula

28- See Chaum 2021
29- Grym 2020

HOW TO BUILD A CBDC TECHNOLOGICALLY?

USER EXPERIENCE

From a user experience point of view, the main criteria is the ease of use. This might mean approaching the **user experience of existing payment solutions**. To be adopted, CBDCs might also have to integrate technologies favoured by most users, such as card networks, requiring extensive partnerships that might constrain the technological development of the CBDC. The infrastructure must accommodate various legacy models as users use different interfaces. User experience might also be crucial to minimise fraud. As a new form of payment emerges and is not fully mastered by populations initially, there is a high risk of various fraudulent schemes targeting users.

Developing countries might require further adaptation to limited connectivity and **inexpensive technologies**. Substantial efforts have been deployed to leverage “feature phones” without advanced smartphone capabilities. USSD, for instance, is an interface and communication available in any phone that allows users to interact with various services. In India, the Central bank launched a service for payment available by typing *99#. Offline payments have also leveraged sim card capabilities.



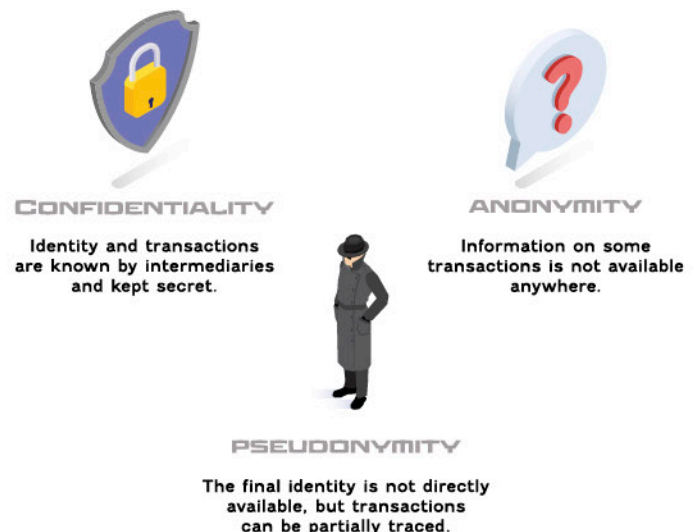
Data and privacy will also be part of the infrastructure and user experience discussion. Data can offer opportunities for tailored financial services and help monitor fraud and crimes. However, privacy is valued by some users and a condition for civil liberties. Any digital payment will require the exchange of identifying data to all parties for regulatory and technical reasons. Therefore, protecting privacy is a challenge. To rely on compliance with existing privacy regulatory frameworks is insufficient for a large scale CBDC. Finding the right privacy balance is a long-term discussion between citizens, the central bank, financial institutions and law enforcement.



Information sharing between the user and operators can improve loss recovery, but there are privacy tradeoffs

Marteen van Oordt

Three high-level approaches could be distinguished. The first one used in the current payment systems is **confidentiality**. Identifying data exists, but each actor is required to protect this data. It can be revealed to third parties, including law enforcement, in legally defined conditions. The second is to have intermediary identifiers that are not directly linked with identity during the payment. This is **pseudonymity**. This model is used in blockchains with full transaction traceability. Therefore any reconciliation of identity provides a full view of the transaction history. The third one is full **anonymity**. Pure digital bearer instruments can achieve this. Advanced cryptographic techniques such as Zero-Knowledge Proofs (ZKP) or secure elements could provide full anonymity while retaining some control.



HOW TO BUILD A CBDC TECHNOLOGICALLY?

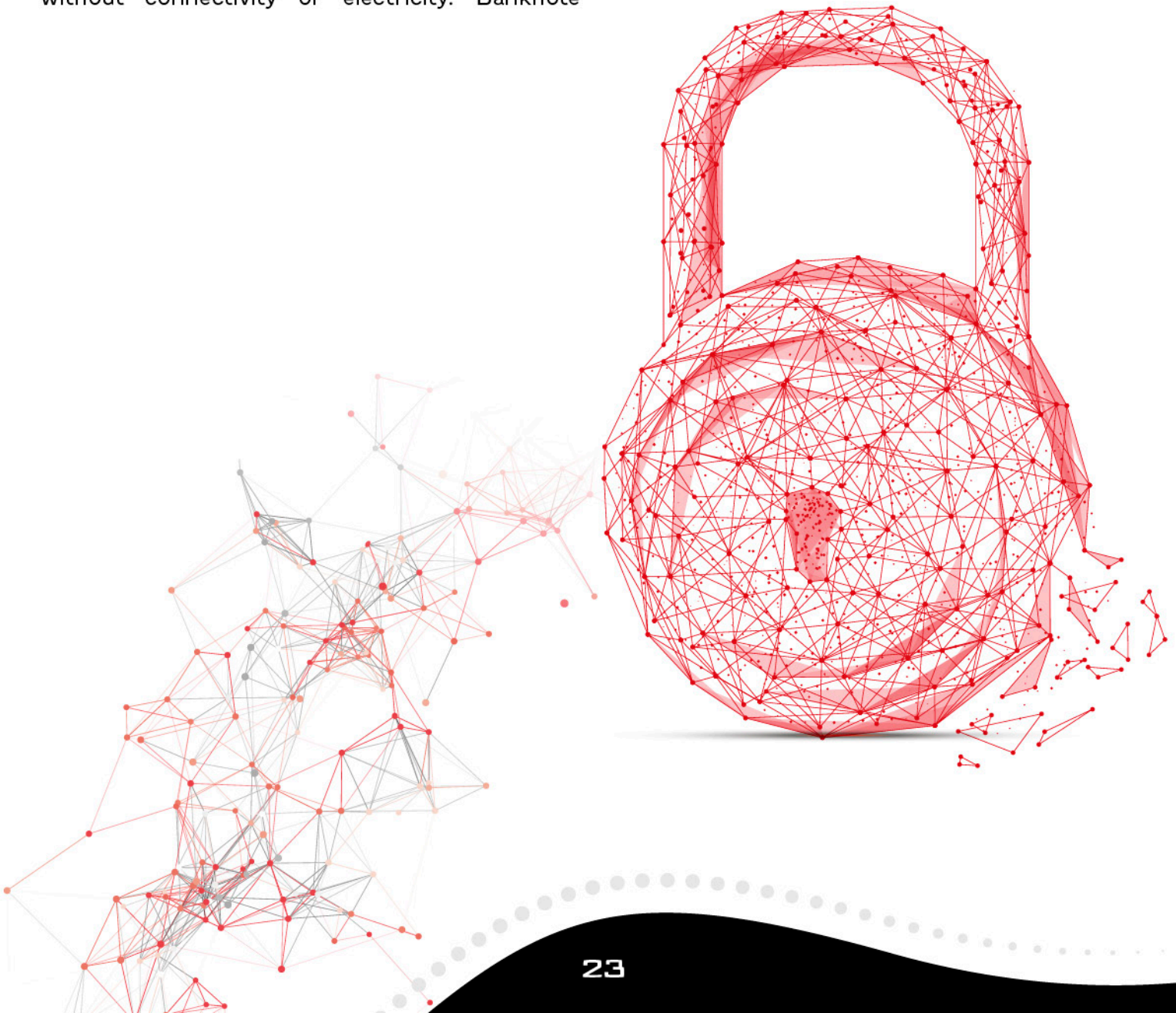
RESILIENCE AND SECURITY

A CBDC will be a **critical national infrastructure**. It must mitigate any natural or malicious attack, yet it offers a large attack surface. There could be consensus failures, denial of service attacks by sending too many requests, undue access, network failure, counterfeiting, cryptographic failures using cryptographic backdoors, quantum computing... Any programmability feature could encounter bugs and hacks. At the user level, messages could be intercepted, bearer instruments could be stolen, and various frauds could misguide users.

The question becomes more acute if CBDCs are considered even partially to replace cash. CBDCs must offer similar resiliency properties than cash for national security and inclusiveness. Cash payments can be processed in any condition, without connectivity or electricity. Banknote

technologies and law enforcement strategies have brought counterfeiting to historically low levels.

In CBDCs, an additional difficulty is the **number of partners involved** at the national level. Central Banks are likely to use external service providers. Outsourcing can distance the control and expertise of the central bank from the operations of the CBDC. Similarly, as many central banks consider a tiered architecture, financial intermediaries might have keys to critical elements of the infrastructure. Their internal security procedures and capacity to respond to an incident will come into play.



RESEARCH AND SKILLS



The interesting research questions of CBDC are at the confluence of money as a social bond and the technologies of crypto.

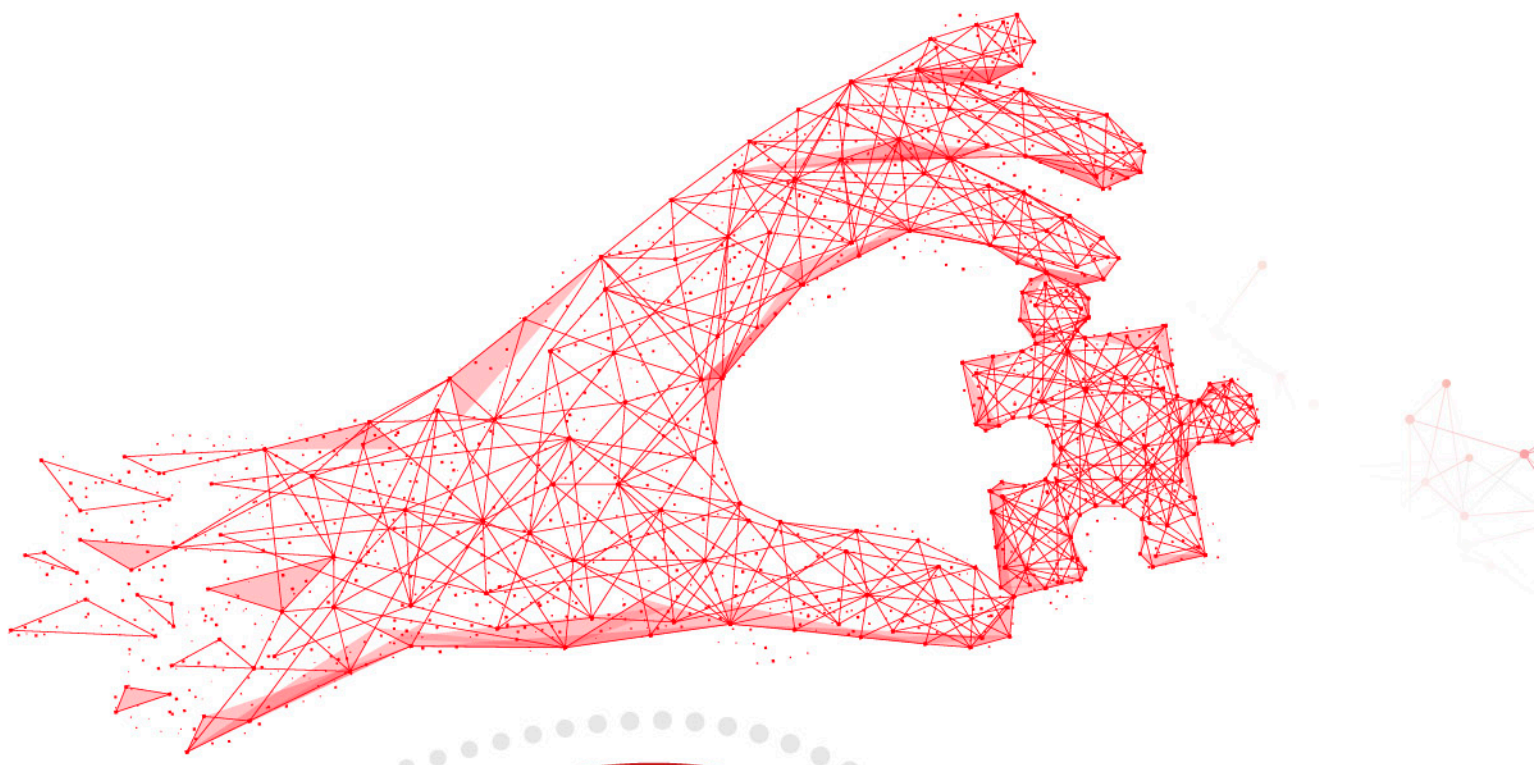
Noémie Dié

Currently, we see important research and development efforts involving central banks, academics, international organisations, and private companies. Central Banks are at the forefront of the topic. They have a deep understanding of their national economic challenges, and can assess the need to upgrade the payment system. It is also the opportunity to develop expertise in digital matters. International financial institutions are studying the topic, generally focused on interoperability questions that might be relevant for their roles. Private actors have been proposing solutions, relying on innovative or proven technologies.

There is no established playbook or “*on-the-shelf solution*”. CBDC requires conducting **research and development**, requiring national and international cooperation. Fundamental cryptography and distributed systems research is necessary to

develop appropriate solutions and ensure their robustness. Quantum computing, for instance, might challenge most digital payments in the coming decade as the underlying cryptography used in most systems could be weakened by it. More practical industrial and engineering questions such as the financial and environmental cost assessment and hardware supply chains are not thoroughly evaluated yet.

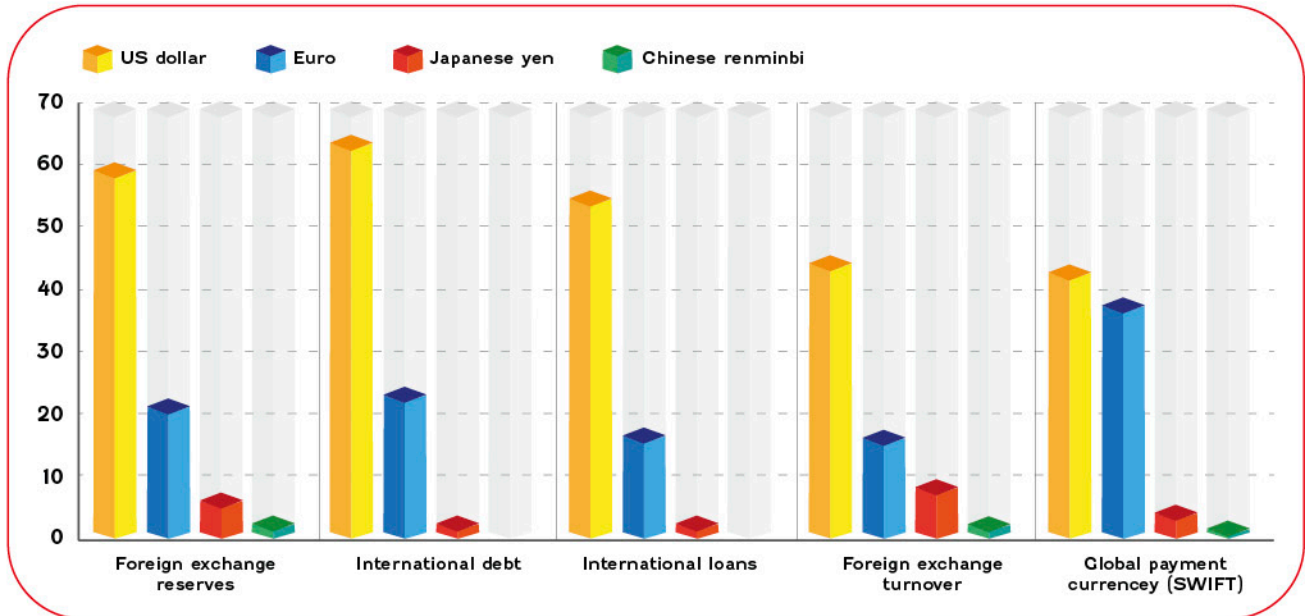
While economic research has been prolific on the topic, other fields of social sciences are relevant to assessing adoption factors such as trust and social interactions as well as long-term impact. The **expertise available** in the market to accompany CBDC projects is still limited. Overall, current research efforts help to finance and grow this expertise.



INTERNATIONAL COOPETITION

This cooperative research effort is ambivalent. While the primary objective of central banks is to provide an adequate solution for national needs, a secondary motivation can be to showcase digital

capabilities internationally. As we have seen above, a CBDC might also be an element of sovereignty by reinforcing the status of a currency along with traditional factors³⁰.



The current respective international role of various currencies - ECB

This ambivalence is particularly obvious in the field of cross-border payments. As recent wars and tensions have shown, cross-border payments can be a geopolitical matter. Several regions have already developed solutions for cross-border

payments, such as the South African development community (SADC-RTGS) or the Arab world (Buna). The introduction of CBDCs increases possibilities for new platforms.



The decision on CBDC implementation is a delicate balance of policy goals, central banks' mandate and technology choices.

Kateryna Zhabska

30- Such as the size of the issuing economy in terms of global trade and finance, the soundness of economic policies, financial market depth and liquidity, and inertia in international currency use

WHERE ARE WE NOW?

COMPETING INITIATIVES

In parallel to international pressures, privately led initiatives have increased the pressure, providing inspiration as well as competition for CBDCs. Those solutions will likely cohabit in the coming years, with different features and positioning.

In the private sector, **mobile money**, for instance, has proven to be an efficient financial inclusion tool in several regions, with an impressive increase in Government to People (G2P) or international payments over the past years.

Bitcoin is used for payments by various private actors. Some countries, such as El Salvador or the Central African Republic, have developed a national strategy to facilitate its usage. While stability concerns and implementation errors have been raised, it contributes to building the case as a global reference infrastructure and asset.

While **stablecoin** usage is currently limited to crypto-asset markets, large technology companies are considering leveraging them to provide global payment methods. Moreover, private financial market infrastructures are also considering issuing wholesale stablecoins.

Moreover, other public infrastructure initiatives can deliver similar functionalities. **Fast payments systems** for instance provide instant settlement and can have various options on privacy and API integrations. Such efforts have shown remarkable developments in large countries such as India and Brazil.

| | Cash | CBDC | Mobile money | FPS | Bank account | Crypto |
|-------------------|-----------|----------------|-----------------|-----------------|-----------------|---------------|
| Form | Physical | Digital | Digital | Digital | Digital | Digital |
| Counterparty risk | CB | CB | Bank | CB | Bank | None |
| Denomination | National | National | National | National | National | New |
| Privacy | Anonymity | ? | Confidentiality | Confidentiality | Confidentiality | Pseudonymous |
| Compliance | Limited | High? | Risk-based | Risk-based | Risk-based | Limited |
| Finality | Instant | Instant? | Indirect | Instant | Days | Probabilistic |
| Maturity | High | In development | In production | In production | High | In production |

Simplified comparison of the properties of various forms of money



There has not been programmable money until now. Open banking is not enough. We see the difference in new ideas and projects of a programmable bearer instrument.

Jeremy Allaire

A QUEST FOR BALANCE AND INNOVATION

Ultimately, CBDCs are in the process of finding their positioning regarding alternative solutions. Questions remain as to whether CBDCs make sense as new solutions and, if so, to which extent they should integrate recent solutions, technologies and designs. Ultimately, in a fast-paced domain, it is less about finding perfect current adequation and more about enabling future evolution and innovation.

Existing initiatives demonstrate the potential of a technology-first and open-source approach. Distributed systems and advanced cryptography such as zero-knowledge proofs and multi-party computation pave the way for secure, scalable and confidential systems. Decentralised Finance has proven that even a spontaneous ecosystem can reach critical mass via composability. However, the particular designs adopted by the crypto ecosystem need to be adapted for national projects while keeping their strengths.

What should be the roles of the public and private sector to enable the next generation of payments? Should the central bank focus on limited core infrastructure and standards or provide a full solution? Could a CBDC be transacting on open blockchains or private DLT networks? By the time a CBDC is developed and eventually adopted, how relevant will it be? Should a central bank focus on usage and areas that might not be fully covered yet, such as machine-to-machine payments, microtransactions and programmability? What synergies with other public policies?

While important questions remain open, ongoing efforts to bring public money to the digital era will be defining for the payment industry, economic development and sovereignty.



GLOSSARY

APPLICATION PROGRAMMING INTERFACE (API):

Digital access used by visual interfaces or external actors to connect to resources on a server. Programs that interact with the API can retrieve data, store it or order operations.

CENTRAL BANK DIGITAL CURRENCY (CBDC):

A digital form of a currency that is a direct liability of the central bank.

COMPLIANCE:

Set internal procedures by private actors to ensure that relevant laws and regulations are observed. In the financial industry, they mainly aim at tackling illicit financial flows such as money laundering, terrorism financing, and international sanctions.

DISTRIBUTED LEDGER TECHNOLOGIES (DLT):

Distributed system allowing the joint update of one or several ledgers according to the procedures defined in its consensus protocol. Blockchains are the most common category of DLT, using chained blocks of transactions as updates and a financially incentivised consensus.

E-MONEY:

Electronic form of money privately issued for payments against the deposit of funds in a bank account. For instance, it can be issued on a prepaid payment card or a smartphone. The term could broadly cover most electronic payments such as mobile money or stablecoins. In the EU, a specific regulation defines the conditions to issue e-money.

FAST PAYMENT SYSTEM (FPS):

Public digital infrastructure allowing instantaneous payments between accounts of users. Compared to regular bank transfers, funds are available to the payee in near-real-time.

REAL-TIME GROSS SETTLEMENT (RTGS):

Digital infrastructure provided by the central bank that allows the settlement of large transactions between financial institutions.

RETAIL CBDC:

CBDC used by customers for payments at a store, online or peer-to-peer to another user.

SETTLEMENT:

Completion of a transaction with the effective transfer of funds. It is the last payment step that settles the parties' legal obligations.

SYNTHETIC CBDC:

Privately issued digital form of a CBDC. In this arrangement, while units are fully guaranteed liabilities of the central bank, private actors are in charge of most operational aspects.

WALLET:

In the context of a CBDC, the wallet is a digital application that allows the user to consult its balance and send and receive payments.

WHOLESALE CBDC:

CBDC used by the Central Bank and Financial Institutions to settle transactions.

ZERO-KNOWLEDGE PROOF (ZKP):

Cryptographic technique by which a prover demonstrates the validity of a statement without revealing the underlying data. In a CBDC, ZKP could be used to prove that payment is valid, including additional constraints, while maintaining privacy.

REFERENCES

- Banque de France (2021) Payments and market infrastructures in the digital era https://publications.banque-france.fr/sites/default/files/media/2021/01/07/payments_market.pdf
- Banque de France (2021) Wholesale Central Bank Digital Currency Experiments https://www.banque-france.fr/sites/default/files/media/2021/11/09/rapport_mnbc_0.pdf
- Bech, M. and Garratt, R., Central Bank Cryptocurrencies (2017). BIS Quarterly Review September 2017, <https://ssrn.com/abstract=3041906>
- Benigno, P., Schilling, L. M., & Uhlig, H. (2022). Cryptocurrencies, currency competition, and the impossible trinity. *Journal of International Economics*, 136, 103601. <https://doi.org/10.1016/j.jinteco.2022.103601>
- Bijlsma, M., van der Crujisen, C., Jonker, N., & Reijerink, J. (2021). What triggers consumer adoption of CBDC?.
- Bindseil, U. (2020). Tiered CBDC and the financial system. <https://doi.org/10.2139/ssrn.3513422>
- Bjerg, O. (2017), Designing New Money - The Policy Trilemma of Central Bank Digital Currency. CBS Working Paper, June 2017, <http://dx.doi.org/10.2139/ssrn.2985381>
- Bossu, W., Itatani, M., Margulis C., Rossi, A., Weenink, H, Yoshinaga, A., (2020) Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations
- Bounie, D., Buthion, J. P., & François, A. (2010). Une analyse des facteurs de l'acceptation et de l'usage des instruments de paiement par les commerces en France. *Revue d'économie financière*, 187-213.
- Central Bank of The Bahamas (2019) Project Sand Dollar: A Bahamas Payments System Modernisation Initiative
- Chaum, D; Grothoff, C.; Moser, T. (2021) How to issue a central bank digital currency
- Chen, Tongjie 陈同杰; Huang, Xiaofeng 黄晓锋 (2017) Fight Peak Data Traffic On 11.11: The Secrets of Alibaba Stream Computing <https://102.alibaba.com/detail?id=35> (Accessed May 22, 2022)
- Chiu J., Davoodalhosseini M., Hua Jiang J., Zhu, Y. 2019. «Bank Market Power and Central Bank Digital Currency: Theory and Quantitative Assessment.» Staff Working Papers 19-20, Bank of Canada. <https://doi.org/10.2139/ssrn.3331135>
- Davoodalhosseini, M., Rivadeneyra, F., & Zhu, Y. (2020). CBDC and monetary policy (No. 2020-4). Bank of Canada.
- Del Giudice, L.; Duclos, R.; Ajdenbaum, J. (2022) Mind the Gap between the Ledger and the online wallet
- ECB (2020a) Report on a digital euro https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf
- ECB (2020b) Study on the payment attitudes of consumers in the euro area (SPACE) https://www.ecb.europa.eu/pub/pdf/other/ecb_spacereport202012~bb2038bbb6.en.pdf
- ECB (2021) The international role of the euro https://www.ecb.europa.eu/pub/ire/html/ecb_ire202106~a058f84c61.en.html
- ECB, Kantar Public, (2022) Study on New Digital Payment Methods
- ECB (2022) Central bank digital currency and bank intermediation
- Fernández-Villaverde, J., Sanches, D., Schilling, L., & Uhlig, H. (2021). Central bank digital currency: Central banking for all?. *Review of Economic Dynamics*, 41, 225-242.

- Fungáčová, Z., Kerola, E. & Weill, L. Does Experience of Banking Crises Affect Trust in Banks?. *J Financ Serv Res* (2021). <https://doi.org/10.1007/s10693-021-00365-w>
- Giannone, D., Reichlin, L., & Small, D. (2008). Nowcasting: The real-time informational content of macroeconomic data. *Journal of monetary economics*, 55(4), 665-676.
- Grym, A.; Heikkinen, P.; Kauko, K.; Takala, K. (2017). «Central bank digital currency». *BoF Economics Review*.
- Grym, A. (2020) Lessons learned from the world's first CBDC
- GSM Association (2022) State of the Industry Report on Mobile Money
- Guerraoui, R. (2018) « Algorithmes : à la recherche de l'universalité perdue » leçon inaugurale au collège de France
- HCJP (2020) Rapport sur les titres financiers numériques («Security tokens») https://www.banque-france.fr/sites/default/files/rapport_39_f.pdf
- Koning, J. (2014) Fedcoin <http://jpkoning.blogspot.com/2014/10/fedcoin.html>
- Kumhof, M., & Noone, C. (2018). Central bank digital currencies-design principles and implications.
- Lampert, L. (1998). «The Part-Time Parliament». *ACM Transactions on Computer Systems*. 16 (2): 133-169. doi:10.1145/279227.279229.
- Lavayssière, X. (2014) La crypto monnaie bitcoin pourrait participer à la sécurisation des transactions financières *Les Bulletins Electroniques des Ambassades de France* <https://xalava.github.io/publications/Bitcoin-transactions-financieres.pdf>
- Lee, M. and Garratt, R., Monetizing Privacy with Central Bank Digital Currencies (2021). FRB of New York Staff Report No. 958, Available at <http://dx.doi.org/10.2139/ssrn.3767028>
- Lovejoy, J., Fields, C., Virza, M., Frederick, T., Urness, D., Karwaski, K., & Narula, N. (2022). A High Performance Payment Processing System Designed for Central Bank Digital Currencies. Cryptology ePrint Archive.
- People's Bank of China (2021) Progress of Research and Development of E-CNY in China
- Prat, J., Dié, N., & Michau, J. B. (2020) Helicopter Money and CBDCs: Are DLT the perfect infrastructure for monetary policies in time of crisis?
- Raskin M. and Yermack, D, Digital Currencies, (2021) Decentralized Ledgers, and the Future of Central Banking *NBER Working Paper No. 22238*
- Soderberg, G., Bechara, M., Bossu, W., Che, N., Davidovic, S, Kiff, J, Lukonga, I, Mancini-Griffoli, T, Sun, T and Yoshinaga A (2022) Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons
- Tanenbaum, A.S., van Steen, M. (2017) *Distributed Systems*, 3rd ed., distributed-systems.net.
- Verdier, M. (2020). Digital Currencies and Bank Competition. Available at SSRN 3673958.
- WEF - Digital Currency Governance Consortium (2021) What is the Value Proposition of Stablecoins for Financial Inclusion?
- Zamora-Pérez, A. (2021) The paradox of banknotes: understanding the demand for cash beyond transactional use *ECB Economic Bulletin, Issue 2/2021*



ABSTRACT

Central Banks provide foundational public infrastructures for payments such as cash and gross settlement systems. In an evolving context, Central Bank Digital Currencies (CBDC) are efforts to leverage new patterns and technologies to provide infrastructures relevant to the digital age. Various research endeavors intend to anticipate their adoption vectors and potential consequences. However, CBDC projects are confronted with contradictory motivations and a large panel of design options. On the technological level, state-of-the-art cryptography and distributed systems are being considered, as well as more mature technologies. While some initial projects have limited relevance, they raise fundamental questions about the functions of Central Banks, the respective roles of the public and private sectors, technological design and international monetary competition that will be defining for the payment industry, economic development and sovereignty.



ABOUT THE AUTHOR

Xavier Lavyssière is an independent researcher on digital finance. Graduated in Public Law of the Economy and Computer Science, Xavier focuses on the intersection of technical architectures, policy objectives and regulations of new digital finance infrastructures. Mr Lavyssière has participated in developing foundational technical projects, education programs and research publications. He is a lecturer at University Paris Panthéon-Sorbonne.

Director of publication: Julien Prat • Author: Xavier Lavyssière • With the kind participation of: Camilla Carabini, Gabriel Soderberg, Noémie Dié, Paul Desprairies, Sonja Davidovic, John Kiff, and Kateryna Zhabska

And the proofreading assistance of: Sebastien Choukroun, Louis Bertucci and Matthias Ros • Editorial assistance: Fatou Dione
Graphic design : Graphissime - September 2022 • Outlook publication of the Blockchain@X - Ecole Polytechnique

Supported by Capgemini, Nomadic Labs & Caisse des Dépôts



**BLOCKCHAIN
@POLYTECHNIQUE**



**INSTITUT
POLYTECHNIQUE
DE PARIS**



SUPPORTED BY :



nomadic labs

