QUANT

WHITEPAPER

Implementing a CBDC

The challenges and a solution

November 2021

WHITEPAPER

Implementing a CBDC

The challenges and a solution

November 2021

Today, CBDCs are close to becoming a reality in many countries. Yet a number of significant challenges remain before effective implementation is possible. Here, we look at these challenges and describe a solution that is being piloted in Latin America and the Caribbean.

Martin Hargreaves
Chief Product Officer, Quant

The concept of a CBDC is not new.

In fact, there have been multiple attempts at introducing a CBDC system (previously termed e-money), dating back to the Bank of Finland's Avant smart card system in the early 1990s. None of these attempts, however, proved practical, or gained mass user acceptance, and it is only with the relatively recent emergence of Distributed Ledger Technology (DLT) that the CBDC, a term first used by the Bank of England in 2015, became a realistic prospect. Today, it is generally recognised that CBDCs offer a wide range of benefits, from faster, less costly transactions to enhanced financial inclusion. As a result, many governments are now seriously considering the use of a CBDC and, as recently as March 2021, China became the first country to announce that it would be launching a pilot system. According to the BIS Papers No 114[1] "Ready, steady, go? – Results of the third BIS survey on central bank digital currency" published in January 2021. A vast majority of central banks surveyed, 85% are now exploring the benefits and drawbacks of CBDCs. Central banks are moving into more advanced stages of CBDC engagement. 60% (up from 42% in 2019) are conducting experiments and proofs-of-concepts and 14% are moving forward to development and pilot arrangements.

2021 has built upon the progress in 2020. From a previous BIS Report No 880[2]" Rise of the central bank digital currencies: drivers, approaches and technologies", "As of mid-July 2020, at least 36 central banks have published retail or wholesale CBDC work, At least three countries (Ecuador, Ukraine and Uruguay) have completed a retail CBDC pilot. At least three countries (Ecuador, Ukraine and Uruguay) have completed a retail CBDC pilot. Six retail CBDC pilots are ongoing: in the Bahamas, Cambodia (Bomakara (2019)), China, the Eastern Caribbean Currency Union, Korea (Bank of Korea (2020)) and Sweden). Meanwhile, 18 central banks have published research on retail CBDCs (eg Harahap et al (2017), Burgos and Batavia (2018), Kiselev (2019) and Bank of Japan (2020)), and another 13 have announced research or development work on a wholesale CBDC."

However, this paper is not concerned with the reasons behind the explosive growth of interest in CBCDs, or arguments in favour of, or against, their implementation. It is taken as given that their use is seen as desirable by many central banks. Instead, we are addressing the practical issue of CBDC implementation. We will examine the challenges that face any central bank looking to issue a CBDC, and describe a solution to these challenges. We will conclude with an important and illustrative example of how this solution is already being deployed.

[1]Ready, steady, go? – results of the third BIS survey on central bank digital currency' BIS working paper, No 114, January 2021

[2]Rise of the central bank digital currencies: drivers, approaches and technologies', BIS working paper, No 880, August 2020.

The challenges

Central banks looking to deploy CBDCs face many challenges. And few, if any, of them can be more critical, in terms of gaining public acceptance, than that of ensuring privacy and security. Yet this is also one of the areas of greatest opportunity. While data protection and criminal activity have historically been a point of concern with all financial systems, our accelerating progression into the digital era offers us a chance to develop new systems that exceed the security of existing systems, and allow us to address the cybersecurity challenges we inherited with legacy systems. This is because the new digital technologies such as digital assets and distributed ledgers enable the development and implementation of simpler and more secure models than those used by today's systems, which often force the entire industry to rely on the security and capabilities of a central system or provider operating in silos, and focused within their own institutions.

Despite this, however, overcoming the security hurdle will not be easy. Indeed, it will be of particular difficulty, because of the fundamental paradox that lies at the heart of financial system protection. This is the paradox of anonymity: i.e. that the anonymity enjoyed by cash in the offline world, and that permissionless DLTs strive for, is the very same anonymity that fuels criminal activity. While a move towards permissionless systems may help to deliver the privacy demanded by individuals and institutions, it also works against the requirement that public DLTs must comply with regulatory frameworks such as GDPR, by exposing all transaction data to the world. Somehow, a balance must be struck.

But privacy and security are just two of several significant challenges which must be overcome. Another is disintermediation. This is not so much a technical challenge as an economic and political one. The elimination of intermediaries in financial transactions is one of the key aims benefits of distributed technology, yet doing so carries real dangers if effected at a systemic level. Deploying a CBDC could undermine the existing retail financial arrangement and, as well as potentially causing economic damage, could put central banks in a customer-facing role. This has been a finding by the Bank of England in the March 2020 discussion paper titled "Central Bank Digital Currency Opportunities, challenges and design[3]". This is unlikely to be tolerable to any central bank.

Of course, any decision by a central bank to implement a CBDC will be contingent on the benefits it can deliver and their place and function in the money supply. To justify its deployment, any new system must necessarily deliver improved benefits in terms of functionality over existing systems. While CBDCs offer a range of inherent functional advantages over existing fiat systems, there are two areas in which they offer particularly significant advantages. One of these areas is programmable money or smart money. The use of tokenised cash, controlled by smart contracts, offers a massive opportunity to transform the transactional world, and could revolutionise everything from cross-border payments to direct debits. The other major area of CBDC advantage is the provision of a single source of truth for compliance teams and for regulators who can access real-time compliance of any institution. This can lead to faster and much more efficient payment systems, offering many benefits such as lower reconciliation costs and easier dispute resolution processes. But, while both of these benefits are both desirable, neither will be easy to achieve.

[3]Bank of England Discussion Paper "Central Bank Digital Currency Opportunities, challenges and design" March 2020

The challenges described above are considerable. To further compound the issue, they are challenges that must be addressed while maintaining compatibility with existing systems. In particular, the implementation of a CBDC should retain compliance with the ISO20022 payments messaging standard, and Open Banking / Payment Services (Directive 2) wherever possible, as financial systems drive towards global standardisation. Delivering such compliance is a non-trivial issue.

Implementation requirements

Before describing a way forward for all these issues, we will review the fundamental requirements of any CBDC system. These are the conditions which the system must meet before it can provide the flexibility to support a wide range of use cases reliably, securely, and at the scale necessary for national and international implementation. These requirements include:

Two-tier model

As with cash, central banks will manage wholesale (inter-bank) payments, and intermediaries such as banks will manage payments between consumers and businesses. This helps to mitigate the risk of (a) structural disintermediation of banks and centralisation of the credit allocation process within the central bank, and (b) the risk of facilitating systemic runs on banks in crisis situations.

Compatibility and process change

To maximise buy-in and engagement from commercial banks, it is important that they are not forced to adopt a new technology platform in order to operate with a CBDC. Instead, the new system must allow the use of existing banking technology and systems, and leverage recent IT investments. A CBDC system must compliment the existing banking environments, core backends and business workflows, requiring minimal changes to current bank treasury processes, such as collateralisation and settlement.

Usability

A CBDC system must support a wide range of use cases, including push and pull payments across P2P (Person to Person), P2M (person to merchant), B2C (business to consumer), G2C (government to citizen), B2B (business to business) and M2M (machine to machine)

Rich data

Rich data is critical to many current and emerging transactional processes, such as cross-border, real-time payments. The international standard for capturing rich data is ISO 20022, which provides a common vocabulary for interbank and business-to-bank payments and reporting messages. A CBDC will therefore need to be compliant with ISO 20022 and its successors.

Platform for Innovation

A CBDC must allow banks to innovate – for example, to issue their own programmable/ purposeful money, and add their own rules and logic around how the retail bank stablecoins can be used. The retail CBDC should be meaningfully more useful than stablecoins issued by a bank that are pegged to the wholesale CBDC – primarily with ubiquity and acceptance across all the banks, and a higher level of consumer trust.

Openness

It is necessary that a CBDC system should be usable by a range of institutions, including banks. However, it should also allow implementation by regulated institutions, such as EMIs (Electronic Money Institutions), PIs (Payments Institutions) and VASPs (Virtual Account Service Providers).

High performance and scale

A CBDC must scale In line with PSD2 and projected payment volumes, and offer continuous availability without single points of failure.

Privacy and security

The need to meet strict privacy and security standards, such as GDPR compliance, is one of the most important aspects of any central currency system. The implementation of a CBDC offers the opportunity to not only meet, but improve, the security and accountability standards of existing systems. This can be done in a number of ways. In many current systems, for example, senders authenticate payments to central infrastructures, and these infrastructures authenticate payments to receivers. Receivers never get authentication from the actual sender. The disintermediation potential of a CBDC means that this issue can be addressed.

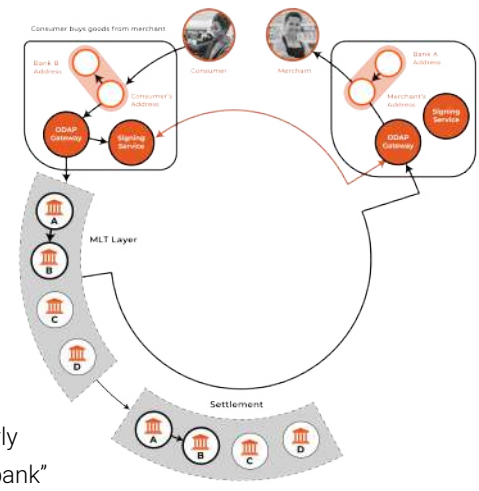
Implementing a CBDC – a way forward

Quant's Blockchain Payments offering called Multi-Ledger Token Solution (MLTS) provides a proven mechanism for meeting all the requirements of a CBDC described above. It is a solution which implements the IMF's "semi-decentralised" model, and enables simple and flexible implementation of synthetic CBDC. It can also be used by banks as a more flexible type of stablecoin.

In this section, we will look in detail at how the Quant MLTS works. In brief, however, funds or collateral are held in escrow with a financial institution, such as a central bank or large regional bank, and tokens to the same value are issued ("minted") on a private DLT. These funds can then be used on any DLT, or mixture of DLTs, public or private, and Quant-patented Multi-Ledger Token (MLT) technology is applied. This ensures that wherever the tokens are used, changes of ownership are recorded on the original DLT, and a clear, auditable record is maintained. The nature of MLT means that the tokens are "open" and can be used on new and different DLTs as they emerge, or as use cases grow. This opens up the walled gardens of many eMoney solutions.

The Quant MLTS model

Figure 1 shows the basic structure of the Quant MLTS model.



At the core of the MLTS system is a ledger of interbank retail and wholesale payments. This receives transaction feeds in real time from financial institution DLTs via an API, as well as individual transactions or roll ups (TBD). The ledger can be operated by a central bank or other PSO (Payment Systems Operator), and multiple ledgers can be deployed if, for example, a central bank needs to separate retail and wholesale payments. The system also allows institutions to handle accounts in multiple currencies. A settlement Interface is also provided, to ensure that escrow funding levels properly reflect tokenised payments. While we use the term "bank" in this paper, the Quant MLTS can be operated by any bank or other regulated institution.

The key elements of the Quant MLTS are:

Bank DLT Infrastructure
This mirrors the bank's balance in MLTS, and holds a variety of accounts. These include customer accounts, as well as the bank's internal holding accounts, such as those used for card settlement (where CBDC accounts have card front ends). The DLT infrastructure also holds counterparty accounts. Although banks do not know the counterparty balance of these accounts, they can apply credits and debits to those accounts on a bilateral basis, giving them a real time settlement position. Debits from counterparty accounts to customer accounts (inbound payments) require a DLT level signature from the sending institution, via the Authorisation Service, described below. Interbank payment messages are via the MLTS system, with authorisations occurring directly between banks, in a similar manner to Open Banking / PSD2 authorisations. The DLT infrastructure can be maintained by each individual bank (or other institution), though this could also be provided as a service by a national or regional DLN, such as LACChain.

Bank Authorisation Service
Each bank runs an authorisation service to confirm payments upon request from counterparties. In order for another bank to process a payment from a sending bank in its own ledger, it must obtain a DLT level signature from the Authorisation Service of the sending bank. This signature can also be enriched with ISO20022 compliant data, or other data, to allow sharing of data between banks. This can be important for purposes such as addressing anti-fraud, including the reduction of authorised push fraud by reaching out to affected customers prior to payment authorisation. Other criminal activities which would be impacted include AML (Anti-Money Laundering) and CTF (Counter Terrorist Funding). It also allows customers to share data without it being seen or processed by MLTS or the central bank. Only authorised data controllers have sight of GDPR-sensitive PII, under conditions of customer consent for specific purposes.

Purpose-specific CBDC scheme support
Although, as described above, a general purpose CBDC will deliver high standards of security, it can also be helpful to mint enhanced or restricted types of tokenised money to ensure funds are used for their intended purpose, thus reducing the possibility of fraud or other misuse. The Quant MLTS provides this capability, facilitating a wide range of specific use cases that have significant social or commercial impact. Examples include:

- **Housing benefit.** Use of a CBDC can ensure that payments are paid only to registered landlords. This would reduce the number of vulnerable people facing eviction for defaulting on rent payments.

- **Emergency payments to vulnerable people.** A CBDC could ensure that payments are used only for essentials, and not for recreational purposes.

- **Luncheon vouchers/cheques.** These could be replaced with a CBDC that can only be used with caterers registered with that scheme.

- **Internet of Things/Machine to Machine.** Automated charging of electric vehicles, smart meters and other PAYG applications can be in a CBDC that can only be redeemed by authorised providers, reducing any incentive for fraud

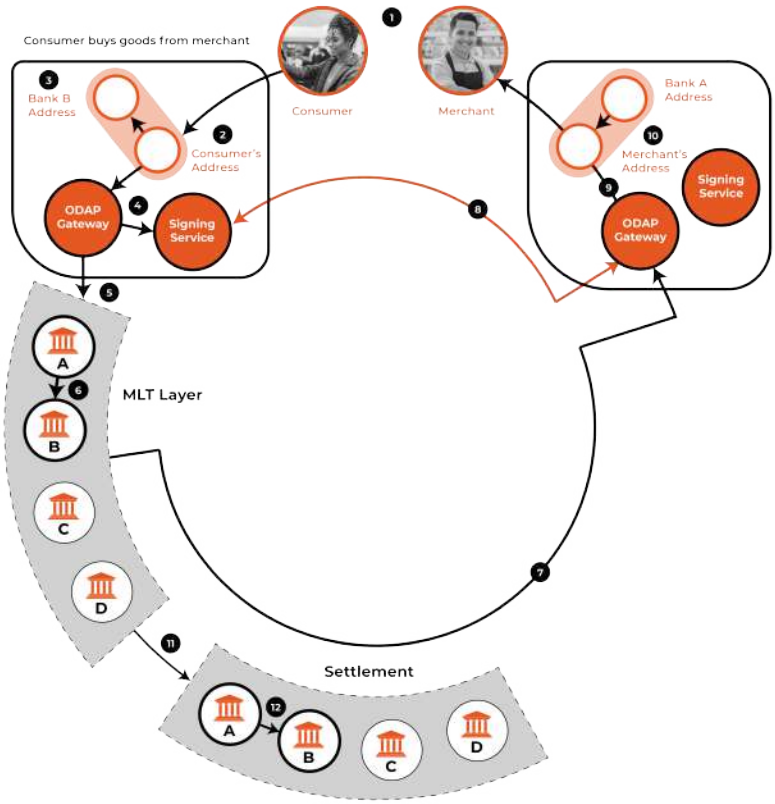
The key elements of the Quant MLTS are:

However, the examples above are just a few of the possibilities. As a platform for commercial and governmental innovation, a CBDC can deliver a wide range of benefits and address many social and technical issues

Multi-jurisdiction / Multi-currency / Multi-region scheme support
The Quant MLTS allows the operation of accounts in multiple currencies, as well as accounts for FX liquidity providers. FX transactions can be accomplished within MLTS using intra-DLT atomic swaps, and multiple central bank/settlement interfaces can be created to settle currencies natively. While this requires a certain amount of political consensus, it is certainly a realistic possibility. Indeed, it is one of the key objectives of the LACChain project, described below (Section 5).

Non-CBDC Use Cases
While this paper is focused on the implementation of CBDCs, it is worth noting that the Quant MLTS can play an enabling role in a wide variety of other use cases, including regional bank consortia, agency banking, loyalty schemes and cross border payment schemes.

An end-to-end payment journey with MLTS
Figure 3 and Figure 4 show a CBDC payment journey, using Quant MLTS, in a peer-to-peer and a card context.



The LACChain Project

While the implementation of a CBDC is not necessarily based on Distributed Ledger Technology, this is by far the most likely progression route. This is because DLTs can also support a wide range of use cases with high social impact, beyond CBDCs and other financial applications. It is for this reason that many national governments have developed, or have begun to develop, managed DLT infrastructures, known as DLNs. But, while national DLNs have huge potential, regional (multinational) DLNs have even more. This is because they deliver even more value than national infrastructures, by providing the ability to deal with cross-jurisdictional issues and to support cross border trade. In fact, the benefits of regional DLNs are so significant that some are already live, or in an advanced state of development. In the EU, for example, the EBSI DLN is coming online, while China's BSN infrastructure is now rolling out globally. Probably, however, the most advanced example of a regional DLN is currently LACChain, an alliance led by the Inter-American Development Bank. Operating across the Latin American and Caribbean region, LACChain is already having demonstrable positive social impact, and the consortium has developed a roadmap which will ultimately lead to the interconnection of regional DLT ecosystems.

Fundamental to the success of this aim is the integration of LACChain (which combines Consensys, Ethereum/BESU and EOS technologies), and Quant's unique Overledger technology. This will facilitate the creation of a new, fast cross-border payments systems for the region, using tokenised money. By flexibly tokenising money, using Quant's (patent-pending) multi-DLT token technology (MLTS), the LACChain DLN will power a variety of new solutions, ranging from transferring money between private individuals, to government and corporate payments, as well as many other future LACChain use cases. The project will also implement solutions from Adhara (Settlement, bank interfaces) and involve close working partnerships with the regional banks. One immediate benefit of this breakthrough will be a revolution in remittances and financial inclusion. For example, where, currently, cross-border banking services for people such as migrant workers or farmers, are hard to access and unreliable, the LACChain solution, supported by Overledger, will allow foreign and/or local currency to be transferred in a simple but secure manner, with affordable transaction costs. The system has the potential to be expanded to the large-volume market of the unbanked, or others currently excluded from the financial system. In short, the LACChain/Quant partnership will open the door to a host of faster, more efficient and more inclusive financial processes and applications in the LAC region, ranging from cross-border and interbank settlement, to the deployment of digital wallets and smart contracts. The pilot phase of the LACChain project is already well advanced, and full commercial development and scaling is expected to begin in 2022. The coming twelve months will be a landmark year for DLTs and CBDCs.

ABOUT THE AUTHORS

Martin Hargreaves
Chief Product Officer, Quant

Martin Hargreaves is Chief Product Officer at Quant, with 25 years industry experience. With a technical background, he has been leading product teams for eight years building nationally critical B2B SaaS and payment products, joining Quant in the first half of 2020. His passion is building world class products and product teams, and delivering the critical systems that will improve our lives in the future.

martin.hargreaves@quant.network

Thomas Hardjono
MIT Connection science & engineering

Dr Thomas Hardjono is currently the CTO of Connection Science and Technical Director of the MIT Trust-Data Consortium, located at MIT in Cambridge, MA. Previously he was the Executive Director of the MIT Kerberos Consortium. He has held various industry technical leadership roles and is active at the forefront of several industry initiatives around digital identity, data privacy, trusted computing, financial cryptography, and cybersecurity.

hardjono@mit.edu

Gilbert Verdian
CEO, Quant

Quant is leading the connectivity revolution. We've already developed Overledger DLT gateway –the world's first DLT gateway for enterprise that delivers interoperability across different systems, networks, and DLTs. Now, we're building on this platform to help enterprises, governments, and individuals, across the globe benefit from the true potential of an incredibly powerful technology.

QUANT

Contact us to learn more about and pilot our tokenised money solutions, for CBDC and commercial applications.

WWW.QUANT.NETWORK

Registered Offices

United Kingdom
20-22 Wenlock Road
London
N1 7GU

www.quant.network