The challenges with designing a CBDC, explained

ABSTRACT

There is growing interest by central banks on the launch of digital currencies accessible to everyone. The main goal is to produce a more resilient, efficient and inclusive payment system. This column argues that central bank digital currency alone will not achieve those goals unless central banks are willing to engage in all the steps of the payment system or complement their digital currency with a broad set of regulatory changes to ensure competition and interoperability of payments.

The Blockchain Forum

Design of CBDC: It's all in the details

When it comes to the design of CBDC there are three main possibilities being considered (Auer and Böhme 2020):

1. **Direct CBDC**. Accounts are opened directly at the central bank. The central bank controls the ledger and is involved in the execution of retail payments. The central bank acts like a regular bank.
2. **Hybrid or intermediated CBDC**. The accounts also represent a liability on the central bank balance sheet, but private intermediaries handle retail payments (and possibly account opening). The difference between the hybrid and intermediated model is in whether or not the central bank keeps a central ledger of all transactions.
3. **Synthetic CBDC**. Accounts are not on the balance sheet of central banks and, for this reason, many argue that this is not true CBDC. Intermediaries hold the liability but are required to deposit 100% of the customers' accounts at the central bank.

1. What are the challenges of designing a central bank digital currency?

Central banks face a trilemma as they try to create a practical CBDC.
Identity, programmability and privacy all matter when it comes to a digital currency that's designed for use by the masses — but focusing on one can be at the expense of another.

Inevitably, many countries pursuing CBDCs have legal compliance at the forefront of their minds. As a result, the identities of those who use these digital currencies need to be verifiable to ensure funds aren't used for money laundering or other forms of illicit activity.

This is easier said than done. Any identity-based system ends up threatening a user's privacy, and instantly makes the digital currency in question less anonymous than cash.

Programmable money is another big draw that CBDCs provide — ensuring that funds can be used for specific purposes. Although the token-based systems that blockchains provide make this possible, user-specific features can't be introduced without personal data… again risking user privacy.

Because of all this, central banks are walking a tightrope as they attempt to build a CBDC that scores equally well on identity, programmability and privacy.

2.Are there issues with the design choices currently being made?

Many payment-based CBDC solutions are sacrificing privacy in order to achieve identity and programmability.
Right now, we're seeing a lot of blockchain and cryptocurrency-based CBDCs sacrifice the protection of user identities to achieve privacy and programmability.

To an extent, this is understandable. A CBDC with a weak identity system — or none at all — can have some rather unpleasant consequences for the end user.

Without such a system, a consumer who forgets or misplaces their private keys can end up losing access to all of their assets — replicating the issue seen with other cryptocurrencies.

3.What happens if a CBDC has a good identity mechanism?

This ends up opening a whole new can of worms.
CBDCs can be based on traditional payment gateways — delivering an account-based solution with a good identity mechanism.

Not only is this approach 100% compatible with conventional banking systems and legally compliant, but it also offers some recourse to users in the event that their private keys go missing. Now, such a situation can be treated like forgetting the password to a bank account — the information can easily be recovered.

The fact that personal information is readily available resultantly means that programmable money features can easily be introduced. A good example can be the introduction of automatic taxation, where funds are immediately deducted based on their income.

Although all of this could deliver some much-needed streamlining, such a centralized system does have its downsides. It creates that dreaded single point of failure that cryptocurrencies were designed to avoid, and there could be a risk of devastating data leaks.

4. How are CBDCs being built in practice?

It's fair to say that central banks are keenly aware about this design trilemma.
Among them is the European Central Bank, which has long said that digitization "represents a major challenge for the payments ecosystem, requiring that a balance be struck between allowing a certain degree of privacy in electronic payments and ensuring compliance with regulations aimed at tackling money laundering and the financing of terrorism."

The Bank of England, which is exploring a potential CBDC for the U.K., doesn't necessarily believe that such a currency needs to be built using distributed ledger technology — adding "there is no inherent reason it could not be built using more conventional centralized technology." It says distribution and decentralization could end up making the CBDC more resilient and available, but this could compromise performance, privacy and security.

One country that's streets ahead of the competition when it comes to rolling out a central bank digital currency is China. Mu Changchun, who is heading up research on the CBDC at the People's Bank of China, says a completely anonymous approach wouldn't work… but this doesn't have to be at the expense of user privacy. Instead, Beijing's stance champions "controllable anonymity" — meaning small transactions can be held in private, payment information can be encrypted, and telecoms operators are stopped from disclosing personal data and phone numbers with the central bank.

Some critics have taken a dim view about what "controllable anonymity" might mean — expressing concerns that this could result in transaction history being surveilled.

5. How can this CBDC design trilemma be overcome?

An identity-based, meta-blockchain can achieve all three design goals of identity, privacy and programmability.
While blockchain systems can be structurally decentralized, the operation itself can be very much centralized and sequential.

The problem lies in how transactions cannot be processed in parallel — and multiple smart contracts cannot be operated simultaneously.

A meta-blockchain that can operate smart contracts in parallel could be the answer here, as it can ensure that a user's information is kept secret at all times.

In summary, achieving the stated CBDC goals requires a lot more than creating an asset at the central bank balance sheet. Issues around acceptance of CBDC as a means of payment, regulation and interoperability of payment systems seem to be much more important. There is no doubt that CBDC could be part of a comprehensive strategy to improve the digital infrastructure of payments, but it cannot be seen as the ultimate solution.