Central Bank Digital Currencies

Big opportunity or big challenge?

How much is a loaf of bread in Bitcoin? Well that depends on when and where you ask the question, and that's the problem with crypto currencies as they stand today. Let's say that in the UK the average price of a white sliced loaf is £1.07 (Office for National Statistics, 22nd April 2020), if I had bought that loaf with bitcoins at 11am on the 3rd May it would have cost me 0.000146534[1] bitcoins, by 7am the next day it would have cost me 0.000155982 , a change of nearly 7% in a day. To see that daily shift in pricing in pounds sterling I would have to go back to November 2016! Now I appreciate that you can't directly compare the volatility of a currency to the price of a loaf of bread, but that's my point, Bitcoin isn't a stable currency. For the vast majority of transactions it has to be converted into a more traditional central bank currency such as pounds or dollars, and that's where the volatility comes in. To attempt to address this issue a new class of crypto currency is on the rise, known as stablecoins. These new crypto currencies are backed by some form of reserve asset such as an existing traditional currency or a basket of multiple currencies and it's this move to combat excessive volatility that has really bought cryptocurrencies onto the agenda of the central banks.

Many central banks are now actively investigating digital currencies to assess the impact they might have on traditional forms of money as well as their impact on the role of central banks as financial controllers of the economy. In this article we will focus on digital currencies issued by central banks referred to as Central Bank Digital Currencies (CBDC) as well as the broader impacts of digital central bank money on the economy.

In this paper we seek to answer the following questions:

1. What are CBDCs and why do we need them?
   a) So why exactly do we need a Retail CBDC?
   b) Why is access to central bank money important?
2. What are the factors that will determine the success or failure of any CBDC?
3. Pros and Cons of differing approaches to CBDC implementations
   a) Tokenisation vs account based ledgers
   b) Distributed Ledger Technologies vs Centralised Ledger solutions
   c) Anonymity vs Traceability

1 Bitcoin value from CoinDesk, average volatility numbers from Bitpremier

1. What are CBDCs and why do we need them?

Central Bank Digital Currency is effectively an electronic version of central bank money. In the current system, wholesale central bank funds are accessed through reserve accounts at the central bank and retail central bank funds are cash issued by the central bank.

A CBDC would allow greater access to central bank money, particularly in the retail sector, as cash is difficult to use in many scenarios today. It could provide much greater functionality than cash as it could also, by its nature, be used in electronic transactions. Unlike cash a CBDC could also be interest bearing, but there is considerable debate about the pros and cons of this.

Importantly CBDC would have a different operational structure from other forms of central bank money, allowing it to perform different functions and serve a different purpose.

There are two main classes of CBDCs being investigated by central banks across the globe, Wholesale CBDC and Retail CBDC. Essentially the difference between the two is the user base, with wholesale CBDCs being primarily used by financial institutions and corporates to facilitate trade, and retail CBDCs being available to the general public. In this paper we will focus on Retail CBDC as the use cases for this are a little less obvious.

a. So why exactly do we need a Retail CBDC?

It really comes down to more direct access to central bank money - cash usage is reducing rapidly and currently cash is the only way that the average person has access to central bank money. Therefore to maintain relevance for everyday consumers and be able to continue to have tangible controls in place to maintain a stable economy CBDCs are likely to become an important component of future economic policy.

b. Why is access to central bank money important?

Central bank money is the safe haven for value if a commercial bank were to ever fail. While commercial bank deposits are guaranteed by the central bank, certainly in the UK and Europe, there are limits to such guarantees. All CBDC issued money would be an effective guarantee or promise to pay.

The growth of privately issued money, stablecoins, may mean that there is an increasing need for something to act as an alternative. The functioning of privately issued digital money will need to be matched by a CBDC to ensure that the central bank remains in control on monetary policy.

Access to cash and the relevance of CBDC is tied to usage of cash in society[2]. Central banks need to control the amount of central bank money in the economy in order to regulate interest rates to control inflation through monetary policy. There is however considerable debate on the effectiveness of Retail CBDC in transmitting monetary policy, with the general consensus being that the effectiveness of CBDC as an instrument of monetary policy is linked to the level of cash usage in the economy. In Sweden, for instance, where cash usage is extremely low throughout society[3], the impact of a CBDC on the transmission of monetary policy would be relatively low, whereas in an economy where cash is still heavily used the impact would be much greater.

Although consumers enjoy a range of digital payment solutions, these are still backed by central bank reserves and cash deposits held in physical vaults. Digital Currencies would become a more efficient and flexible means of storing value and be able to be divisible beyond the current physical limitation of cash.

Lastly, digital currencies are on the rise and some, such as basket currencies, claim to be as stable as central bank money. Private stable coins have the potential to reduce the efficacy of central bank monetary policy by reducing the share of money held as central bank funds. With greater adoption this could dilute or remove the monetary policy controls of the central banks to maintain stability in their economies.

2 IMF Working Paper - Cash Use Across Countries and the Demand for Central Bank Digital Currency, WP/19/46.
3 As of 2018 according to figures from the Swedish Central Bank, Riksbank

2) What are the factors that will determine the success or failure of any CBDC?

Availability – How the general public is able to access the new digital currency is critical. Will they need to access it through an intermediary (a bank account or 3rd party service provider) and how available will it be for the unbanked, including children, to use? What technology, such as smart phones, will be required and what about the parts of the population that do not have access to technology, how can technical barriers to access of the CBDC be reduced? Can it be used "offline" without introducing settlement finality problems for the Central Bank? Would it be easier to make CBDC more available, compared to physical cash, for certain groups of the population that have different kinds of special needs?

Resilience – This is a key area, simply because our society, whilst becoming increasingly digital, needs to have a well-functioning, super resilient, payment infrastructure. This suggests that even if one, two or even half of your national payments infrastructure components are down due to some kind of cyber-attack, wide spread power outage or business operational issues, the rest of the infrastructure should be operating as "normal". The resilience aspect is even more important in the retail use case, since there are a lot more actors to communicate with during an incident, and ultimately the degree of trust is the key factor here.

Scalability – In the context of the retail markets, digital currencies need to be able to keep up with demand for real-time transactions and be massively scalable where millions of transactions may happen concurrently. If you're in the wholesale side, although the value may be much higher, you typically only have a "few" actors that you need to consider (similar to the actors around an RTGS system).

Cyber Security – In the digital economy theft, fraud and cybercrimes (including state sponsored cyber warfare and terrorism) can happen many thousands of miles away at scale across large networks going undetected for months. To ensure institutional and consumer trust in a digital currency will require a continuous sophisticated and evolving Security counter measures to prevent abuse.

Usability & Security. This is not only how usable a solution is to carry out its basic functionality, but also how you at the same time cater for a very high degree of security AND the usability of this security mechanism. This is especially important when you considering for example technologies for distributed encryption key management, since securely managing your own keys is still difficult/complex from an end user perspective.

Societal buy-in. More nebulous perhaps, but the introduction of CBDC combined with the diminishing use of cash is likely to mean society's understanding of money, the way we educate our children as to what money is and what tools we use to understand and look after our own financial health will change significantly. Whether CBDC becomes a mysterious thing understood only by specialists or achieves a common understanding, acceptance and utility within wider society will be crucial for its success.

Integration. The impact on the amount of commercial bank money in circulation and the scale of commercial bank lending may be significantly altered by giving retail users access to CBDC. , the well-known disintermediation concerns. According to the Bank of International Settlement central banks expect there to be a balance between central bank and commercial bank money. Avoiding the two extreme situations, either "where the central bank acts as the sole issuer of money, or free banking, where commercial banks provide all the money required by the economy. Neither of these corner solutions has proven to be sufficiently stable or efficient to endure". In this case central banks must be careful in their creation of a CBDC to avoid the wholesale movement of deposits away from commercial banks to the relatively safe haven of central bank money.

Reliability – CBDC must be at least as reliable as cash or cash based payment accounts. There are two aspects of this reliability:

- The CBDC should be exchangeable for goods and services in the same stable way cash is. That is the assumed value of the CBDC should not be any more volatile than cash would be today. This would depend on the central bank and the particular economy in which the CBDC is issued.
- The CBDC should be extremely difficult to counterfeit. The opportunities to fraudulently claim ownership of units of the CBDC should be difficult, as should the ability to create new, counterfeit units. This means at least as hard to counterfeit as physical cash or crypto currencies. This should in theory be easier to control, if the generation and storage of the CBDC is managed by the central bank. In a distributed model this will be harder to manage, but elements of distributed ledger technology design should be used to mitigate this.

Of course all these points are moot if there are no benefits to the end user and the merchants they interact with. A retail CBDC provides some obvious benefits to the merchant, in that they don't have to pay cash handling fees, they don't have to worry about the physical security of cash deposits and they shouldn't (depending on how the CBDC is implemented) have to pay any interchange fees as they do currently on card transactions. Another significant benefit is the lower risk to the merchant of physical robbery and/or theft which often occurs through violent means. Merchants' will no-longer need to store large volumes of cash in their stores and therefore will be less of a target. The direct benefits for consumers are less clear, largely because digital payment services already exist utilising commercial bank accounts with card based and direct account payment services. If there is no additional incentive for the end user to use, or switch to, CBDCs then these merchant focused benefits will not occur unless cash based central bank money is phased out.

The Bank of England, for example has considered whether paying interest on CBDC, would give it an advantage over cash, but not over commercial bank deposits. Without this sort of interest bearing function it would not be possible to maintain parity between the value of the CBDC and other forms of central bank money.

The flight of deposits away from commercial banks into some form of CBDC is of particular concern in times of crisis. In the COVID-19 crisis there has been significant concern about what the economy will look like in the future and whether the current set of financial institutions will still exist in the medium to long term. Under these extreme circumstances it would not be unreasonable for people to move their deposits into CBDC as a relatively safe haven. The UK and Europe have deposit guarantee schemes that ensure that deposits are protected to the value of £85k or €100k respectively, but extreme circumstances could easily cause depositors to be concerned that these schemes may not be honoured, or certainly not immediately, thus encouraging them to move their deposits into CBDC ahead of failure of their commercial bank. This could have two effects, firstly it could hasten the demise of the bank by reducing its balance sheet and secondly it could significantly reduce the amount of money available for lending, thus further weakening the economy.

3) Pros and Cons of differing approaches to CBDC implementations

The combination of aspects that you would like to address in your CBDC solution will be based on the success factors discussed above. Central banks must also consider and decide upon a number of challenging questions in order to design a successful CBDC.

a. Tokenisation vs account based ledgers

Physical cash is a token of value. Each note or coin establishes its own unchangeable monetary value identified in its manufacture and issuance of the central bank. Secure anti-counterfeiting measures are incorporated into the manufacturing process to help the public identify and trust in the acceptance of cash for the purpose of trade. Inflation has the effect of devaluing the tokens (such that you may need more of them to buy goods or services) and interest is not payable on the tokens themselves.

Putting the technology solution aside for a moment, a digital currency issued as a token of value, perhaps stored in a digital wallet or card, has some distinct advantages over physical cash. Such digital stores could hold a balance, such that when interacting with other tokens or accounts, only the precise amount of the transaction is debited/credited and there is no need for a physical exchange. Carrying large token balances no-longer becomes impractical due to the physical challenges of needing to exchange for larger tokens or carry and secure large quantities of tokens, such as retailer's daily trips to deposit their cash takings each trading day. Retailers would also no-longer need to carry a variety of different denominations of currency solely for the purpose of issuing change. Since a transaction can be made with the precise amount, change itself may be a concept that is retired along with physical cash itself. Tokenisation of digital currency could in effect also reduce the need or desire for consumers storing value in accounts thus inviting greater innovation from banks to entice account based deposits (improved interest bearing options for example).

Actually, this is not an either or question. CBDC designed as both tokens and accounts have advantages and clear use cases, but in the end it is the decisions on the features and functionalities of the CBDC that matter. Until then discussion of Token vs Account based approaches are likely moot.

Digital Tokens then offer significant benefits over physical cash. The challenges in implementing them however pose significant security and trust issues. The monetary system and central bank money in particular relies on controlling the creation and issuance of new currency. Counterfeiting cash involves sophisticated printing machinery and access to complex materials and manufacturing processes. Even then, distribution is limited based on the need to 'move' the cash and introduce it discretely into circulation undetected. The challenge with Digital tokens is that any digital data record can be deconstructed to its relevant zeros and ones, such that exact replicas and copies of data can be reproduced at massive scale and speed – such as backing up your files or replication onto others computers or devices. This is where the need for ledgers come into play as they are required to record the finality of settlement and limit the creation of new currency to only the central banking authority. A third party source (be it a central bank or multiple trusted sources) then needs to be able to verify the authenticity of your digital currency token and thereby its value, otherwise what's to stop anyone from retrieving a backup of their digital wallet and spending the same money twice? Digital Ledgers can be Centralised or distributed, we discuss the benefits separately in this paper from a central bank perspective. Regardless, a real-time verification of value of your token and witness to settlement still needs to take place and therefore it makes it extremely difficult to transact if both parties are "offline". Offline transacting is becoming less of a concern in modern retail systems but is still a distinct disadvantage for physical cash usage. The advantage to token base ledgers is that anonymity matches more closely the use of cash today. It is the token value that is tracked and the holder doesn't necessarily need an "account" with the central bank or a financial institution. They need only to hold an encryption key for the value of the

token. Not too dissimilar to holding a cashbox key, except access to the contents is available real-time and on-demand. If you lose your key however, there may not be a replacement unless you have registered an account. Much in the same way as if you lose your wallet, that money is now lost. Except it is much less likely to return to circulation (as say if someone found the wallet and spent the cash) since its unlikely anyone could guess or recover your encryption key. It's therefore possible for digital money to be removed un-intentionally from circulation (through lost keys) and a means to re-patriate or re-circulate anonymous lost token value would need to be considered. Additionally if tokens are not implemented with a fixed value (but allowed to exchange value with other tokens) the transaction history required to establish the token's current value may over time become quite lengthy. A means to exchange tokens for a clean, reissued token would need to be considered, especially if a DLT based solution is used. In this scenario a variable token is not that much difference from a mini "account". It may just be a matter of whether they are anonymous or can be attributed to a specific individual or owning entity.

Anti-Money Laundering regulations will also play a part here, given the change in the size and movement of money through tokens, it is likely that guard rails will need to be established to govern the amount of value any token can hold, number of tokens held or to establish a chain of custody to individuals which may limit the level of anonymity.

b. Distributed Ledger Technologies vs Centralised Ledger solutions

There is a special circumstance regarding CBDC that is different to most other use cases found where you consider the pros and cons between a DLT based solution and a more traditional Centralised solution. This is the fact that in the CBDC scenario there is only one source / actor that needs to both originally issue and control all transactions at all times. This is due to the fact that ultimately the owner of a CBDC has a claim on the central bank, not to a commercial bank or any other actor. The consequence of this is that a DLT based solution is less attractive, since all transactions needs to be throttled through one single actor or node, which would make it more difficult to achieve a high throughput and also you have an inherent "hierarchical solution".

The availability aspect of a DLT/Blockchain based solution is typically achieved by distributing the nodes across many organizations and geographies (the most "extreme" example of this would be Bitcoin where every participant could run their own node in the system). The distribution aspect has some down sides though; you typically need to address how you perform the consensus algorithm in your network in order to achieve higher performance. The Centralised approach, i.e. using some kind of Centralised repository, could be just as resiliant as a DLT/Blockchain approach if using modern approaches, since you could distribute the underlying infrastructure and application to a very high degree (like many servers and many datacenters etc.).

Going back to the implications mentioned earlier regarding the " Centralised" aspect in combination with super high resiliency. As mentioned earlier, if a de Centralised approach is used to solve this problem, you would inevitably end up in a pseudo " Centralised approach" due to the implications that the resilience aspect would have, effectively forcing you to create a solution where all nodes have all transactions. But wait a minute, isn't that what Bitcoin does? Yes, that is true, but in contrast to Bitcoin where the transaction speed is very low (approx. 5-10 TPS), you would need a much higher transaction speed in a "retail CBDC" use case, hence you would then be back to this " Centralised approach". There are elements however of the resiliency and security of DLT solutions that could still be leveraged by distributing the central ledger over multiple nodes for consensus validation, while still being under the control of the central bank, making the solution much harder to penetrate, while still taking advantage of cloud based infrastructures.

Another concept central banks may wish to consider is the ability to 're-mint' or re-issue digital currencies. In the case of DLTs, where ever more sophisticated security threats or exploits are discovered, new protection codes or limits need to be able to be distributed by the central authority without creating "forks" in the chains. Lessons from Etherium DAO[4] can be learned here.

In summary we think a DLT/Blockchain approach would work fine for a "wholesale CBDC" use case but **right now we think the "retail CBDC" use case needs a Centralised approach** based on the need for scalability. This will of course change over time, due to the fact that exponential developments in the underlying technologies being used will increase the capabilities of participating nodes, even if these nodes are phones or smaller devices. The CBDC space is evolving and we will most likely see many different solutions for how to address the areas above.

c. Anonymity vs Traceability

Cash provides for simple anonymous transactions between individuals without a chain of custody. It requires trust between parties (that the cash received is not counterfeit for example), yet also provides some level of assurance that information related to the transaction cannot be collected, attributed or otherwise mined by third-parties independently. There is a legitimate need for law enforcement to prevent illegal trade and be able to trace and determine transaction history in very large transactions and movements of currency and yet, for smaller transactions, citizens may prefer not to be traced to such a degree. Do I really want my weekend movements, shopping habits and every purchase scrutinised or made available to marketers or even law enforcement? In its request for responses to a recent white paper, the Bank of England provocatively raised the question as to whether the bank has ever had an obligation to provide anonymity in the use of central bank money. Yet if we reverse the question one could also consider whether central banks have ever had the obligation to track and trace its citizen's use of central bank money? Central bank issued currency has after all only been a promissory note to pay the holder the equivalent value and not to establish a chain of custody or proof of ownership. Of course all bank notes carry serial numbers and, in the case of large scale bank theft, can be identified at the point of re-entry to the banking system. Therefore there is already a rudimentary tracking mechanism, but it is the currency token itself that is tracked, not the consumer or their activity with that cash before it is presented to the bank teller.

An argument could be made for leaving some cash usage in the economy to provide that level of anonymity, allowing transactions to continue to be made in cash when some level of anonymity is required. This would have the added effect of marginalising cash usage, potentially making it easier for law enforcement to trace criminal activity using cash. Alternatively, limits could be placed on the value of anonymous CBDC transactions to support the natural tendency of users to want some level of traceability and recovery should larger values of CBDC be lost or stolen in some way. This could work in much the same way as storing value on a travel card like Oyster, where unregistered cards cannot have their value retrieved if lost, but registered cards can, thus protecting the registered user from loss.

Answering this fundamental question of Anonymity vs Traceability we believe will have a material impact on consumer trust and therefore widespread adoption of CBDCs. **We think some appropriate level of anonymity will need to be offered even if it is not attractive to central authorities.** After all a highly tracked and traced solution will probably drive more people to anonymous private money solutions when physical cash becomes obsolete, especially in those economies where trust in the government is lower.

4 4 NY Times article: "Hacker may have removed more than 50 million from experimental cyber currency project"


SECURITY
CONFIRM
click here for more information

Conclusion

CBDCs are becoming a medium term reality. While many white papers have explored the benefits and/or advocated for particular technical solutions to enable CBDCs, this paper has also laid out a more cautionary set of questions related to the challenges for unbanked or digitally underserved members of the economy who still need access to central bank money.

We've also considered some societal challenges and opportunities that CBDCs bring - as the world around us continues to become more advanced, automated and digitally connected; the meaning, concept and comprehension of money and trade is becoming increasingly harder to understand. The implications for how to best teach our next generation about financial health in a digital currency world needs further thought and consideration;

On the key CBDC design questions:

- We think the debate between account vs token based CBDC capabilities are likely moot. We see there being a number of other questions and decisions that are more important to address first and depending on the outcome of these this specific debate will be settled
- We come down firmly on the side of centralization at least as far as retail CBDC is concerned
- We believe the ability to conduct anonymous transactions is essential, at least to a certain value and scale, to ensure successful adoption by the public.

If you would like more information or to discuss our white paper topics please contact our experts, russell.briggs@cgi.com or sean.devaney@cgi.com

The CGI team who contributed to this white paper:

Robert Book
Russell Briggs
Sean Devaney
Jerry Norton
Andy Schmidt
Malcolm Thomas

CGI

About CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. Operating in hundreds of locations across the globe, CGI delivers an end-to-end portfolio of capabilities, from strategic IT and business consulting to systems integration, managed IT and business process services and intellectual property solutions. CGI works with clients through a local relationship model complemented by a global delivery network to help clients achieve their goals, including becoming customer-centric digital enterprises.

Learn more at cgi-group.co.uk