Wits Institute for Social and Economic Research
Kim Dancey
23 January 2022

Privacy is core to the development of Central Bank Digital Currencies

Introduction

"If you make customers unhappy in the physical world, they might each tell 6 friends. If you make customers unhappy in the [digital world], they can each tell 6,000 friends." – Jeff Bezos, founder Amazon

Over 97% of the money in circulation today is from funds deposited online and converted into a string of digital code by a commercial bank. A vast number of previously cash based transactions have now been digitised. Furthermore, there is documented evidence that the adoption of digital payments has increased significantly during the era of the COVID-19 pandemic.

By large this digitisation has not impacted traditional models of banking. The type of digitisation seen to date has not disrupted the commercial banks, which have, broadly speaking, adapted well to these digitisation models. The Chinese financial sector has, however, seen more disruption, as illustrated by the emergence of Alibaba's Ant Financial and Tencent's WeBank, which have benefited from looser data privacy protection and smart data analytics to dominate consumer payments. This is about to change as more central banks are looking into the possibility of issuing central bank digital currencies (CBDC). As governments grapple with the challenge of regulating the explosion of cryptocurrencies such as Bitcoin, government-backed CBDC's present a potential alternative to these cryptocurrencies and to physical cash. CBDC's will provide faster and more secure payments domestic payments, at a hopefully lower cost. Despite the number of central banks investigating CBDC's, there is currently no consensus on how a CBDC system should be designed and what features it should have. This is the subject of much current debate and intensive research, both in industry and in the public sector.

To reduce the country's dependence on Alipay and WeChat, and reduce the threat from cryptocurrencies, both of which potentially threaten a governments' ability to manage its economy, China has been running an experiment with CBDC's. The Chinese CBDC pilot started with the distribution of 100 million digital Yuan through lotteries. At end September 2021, the digital currency pilot had recorded around 500 million transactions with 140 million users. The idea of CBDC's is catching on; Sweden, Singapore, and South Korea are among 13 other countries testing pilots. The US Fed has a project underway, in collaboration with MIT, to design a dollar based CBDC prototype. As CBDC's must identify users and track their payments, the view expressed by the Federal Reserve Chairman, Jerome Powell in April 2021, is significant: "*it is far more important to get it right than [...] to do it fast*". He went on to say that "*The currency that is being used in China is not one that would work here [in the US]. It is one that [...] allows the government to see every payment for which is it used, in real time*." This comment raises the privacy conundrum – balancing a better, faster, cheaper payments system with the requirements of privacy, security and transparency.

Central Bank Digital Currencies and Privacy

A brief introduction: in a CBDC world, the digital code for each currency unit is issued by the central bank on a 1:1 basis to the existing government mandated currency[1]. The CBDC is held by the user in a digital wallet, to be transferred seamlessly by the wallet-holder to another person's digital wallet. At this level, the understanding of a CBDC framework operates much like mobile money wallets. Each CBDC unit will have a unique, unchanging digital identity. It is not meant to replace cash, but coexists with cash as an additional form of a payment method. It is a new form of money, which exists only in digital form and is a direct liability on the central bank, just as current physical currency is. This is a key differentiation from the "digital funds" that exist today in a bank account, which is a liability of the issuing bank only.

As more central banks begin experimenting with the idea of issuing CBDC's, there is a concern about the impact that this programmable digital money will have on privacy concerns. The European Central Bank (ECB), in consulting with stakeholders on the possibility of a Euro-denominated CBDC, found overwhelmingly that the question of privacy was key to CBDC acceptance. Unlike Bitcoin or other cryptocurrencies, which are decentralised and used globally, CBDC's share similar characteristics to the common understanding of "money". However, transactions made using digital payment rails enable the capture of much more data than cash transactions. Therefore, for CBDC's to be successful, a comparison to physical cash is a good benchmark as cash seemingly provides a high degree of privacy and anonymity to its users. The privacy feature is therefore inherent to the use of cash. Privacy is not binary though; privacy rights in the financial services sector need to be balanced with the combatting of money laundering and other financial crime fears. Although the concept of privacy differs from jurisdiction to jurisdiction, consumers are increasingly becoming aware of to whom they entrust their data and how it is used. In response, regulators are increasingly issuing data protection regulation. It is estimated that by 2024, more than 80% of organisations globally will have to comply with privacy and data protection regulations[2]. Thus, a primary priority for any government looking to successfully issue CBDC's is to provide a "trust" framework. To achieve this, the matter of privacy must be thoroughly understood and the CBDC framework must be deliberately designed with privacy enhancing techniques.

A useful reference to use as a benchmark is the World Economic Forum's Principles on Privacy: [3]

1. Prioritise the best interests of citizens, especially vulnerable populations, when collecting data
2. Limit the collection to necessary identifiable information
3. Use the data for the purposes for which is was provided

What this translates to, in a CBDC world, is:

1. Users should be able to use CBDC's without being subject to undue tracking or surveillance by government or corporates
2. Users should be able to opt in or out of not vital information sharing

[1] Commonly referred to as "fiat currency"

[2] Moore, S: "A proactive approach to privacy and data protections helps organisations increase trust"., Gartner 20 January 2020

[3] World Economic Forum, Global Blockchain Council, Presidio Principles: Foundational Values for a Decentralised Future

3. Law enforcement access to the data should be controlled by due legal process

At a foundational level, CBDC systems verify the uniqueness, security and settlement of a transfer of a CBDC by answering the following questions:

a) "Is this money genuine?"
b) "Has the user spent this money before?"
c) "Did a transfer of money occur successfully?"

The operators of the system (the central bank and/or its designated regulated entities) may not necessarily need to have visibility into account balances, identity information or other transaction-related information. The choice to have visibility into that information is a policy choice and can be limited, threshold-based and audited.[4] It is vital to build a system that provides users with safeguards that their transactional data will not be used for surveillance and control. Failure to ensure this, combined with the failure to communicate these safeguards effectively to users, leaves a threat of privacy intrusion that will likely get significant push back, at least in more liberal geographies.

Privacy By Design

The key to the issue of privacy protection in a CBDC framework is the architecture. As previously mentioned, there is currently no consensus on how a CBDC should be designed and what features it should have. The most widely used architecture, currently, is based on a two tiered model developed by the Bank of England where traditional commercial banks are at the system's front-end and the CBDC is on the back end, ensuring that the central bank is not a direct participant in the retail operations. In this scenario, users would not even be aware of the mechanics of the CBDC platform. This preserves the current model where people would still have to use a traditional financial institution to access a domestic banking platform.[5] Nevertheless, this model and any other potential model must address the privacy aspect in the interests of full disclosure and trust.

The Swedish model is worth mentioning, where privacy-by-design is taken into account. The Swedish Riksbank e-Krona pilot is a CBDC with a direct claim on the Riksbank and is a need-to-know model, where there is a degree of physical separation between transactors and the central bank. The network architecture is designed to only share to the central bank and other financial regulatory authorities what these entitles *need-to-know* and allows for a level of privacy that is akin to the two-tiered model used by central banks today.

Advancements in cryptography, powered by the technological progress in mathematical computing are enabling ever newer methods which can be applied to achieve privacy and confidentiality in applications that are being developed. Although many of these methods are at the frontier, they

[4] World Economic Forum, Privacy and Confidentiality Options for Central Bank Digital Currency, White Paper November 2021

[5] This model is not favoured by financial inclusion advocates due to a lack of trust in banks and the perceived costs. The financial inclusion benefit of dealing directly with the central bank and not through a commercial bank intermediary, is that bank charges are presumed to then be minimal or zero, ultimately democratising banking for those who can't afford a bank account. Further discussion on the financial inclusion aspect of CBDC's is beyond the scope of this paper.

require further development to be used at scale without impacting system performance, but they could be developed to increase the privacy features of a CBDC system.

It is imperative to note that one of the most important aspects to consider when moving to a privacy-preserving system is to additionally preserve, in parallel, its integrity requirements. Privacy and integrity must be complimentary. In a transparent system, the operators of the system ("validators") usually verify the integrity requirements by looking at the transaction data and accepting transactions that follow the established rules, for example to ensure that there is no double spend. Thus, when building a privacy preserving system, it is important to consider that the validator needs a way to accept the correct transactions without necessarily seeing the transaction data. This is where the power of cryptography reveals its potential.[6] Three examples of these models include: *zero-knowledge-proofs* which enables the sharing of computing outputs with a party, without sharing the inputs to the computation; *symmetric-key cryptography* which requires a single key to perform the algorithms, one is a commit algorithm and the other a reveal algorithm and *hash functions* are where two computations have the same hash and no other message will give that same result. There are a number of additional cryptographic examples under consideration[7], the three set out here aim to illustrate that there is significant potential to mathematically ensure a high level of privacy and confidentiality where this requirement is deliberately taken into account.

Conclusion

There will be significant learning and evolution in CBDC's over the next few years. In order to assess which cryptography methods may be useful, central banks must first make decisions about the level of privacy they would like to create and enforce within their financial system. The central bank must ensure that the CBDC privacy scheme takes into account related local policies, laws and regulations as well as public and private sector stakeholder preferences. Keeping pace with the variety of architectural models to support the privacy objectives of a domestic CBDC system is critical. Several frontier technology developments already reveal that privacy in CBDC's will require a collaborative approach to technical design and choices. The success of a CBDC system's adoption and its responsible deployment, is critically dependent on well thought-out "privacy by design" principles.

[6] The cryptographic concepts that could be used to enhance privacy mentioned here are by name as the level of detail required is beyond the scope of this document.

[7] World Economic Forum, Privacy and Confidentiality Options for Central Bank Digital Currency, White Paper November 2021