Visa
Economic
Empowerment
Institute

Imagining an Open
Future for Payments

Finding a secure solution for offline use of central bank digital currencies (CBDCs)

ERIN ENGLISH / MARCH 2021

Insights

- Many central banks that are exploring the creation of a central bank digital currency believe the ability to conduct a secure offline transaction is a requirement.
- Offline transactions are not a given, and without finding a secure solution, CBDCs could open themselves up to digital counterfeiting.
- Visa's research and product teams have proposed the creation of a secure payment system protocol that can allow a user to make a digital payment in CBDC while both the sender and receiver are temporarily offline.

When the Bank of International Settlements (BIS) published its annual central bank digital currency (CBDC) survey in January, it was probably not a surprise to most observers that the percentage of central banks exploring a CBDC had made a year-on-year jump from 80 percent to 86 percent (Boar and Wehrli, 2021). However, as the thinking along the exploratory scale moves from the conceptual to the pilot stage, so do concerns that such an undertaking cannot be done securely and have the proper consumer protections. For instance, one of the challenges identified by many central banks is how to ensure that the digital currencies that central banks issue can still be accessed offline, and be resilient and secure enough to protect against cyber-threats and the risk of a potential new type of financial crime: counterfeiting CBDCs. Central banks that are exploring or progressing toward a CBDC need tools to combat a 21st-century version of a millennia-old problem. With these problems in mind, on December 14, 2020, Visa Research and Visa Product teams released a white paper that addresses some of the security problems of offline payments. In the three months since publishing that paper, there has been a strong interest in the report's findings, and it is worth reacquainting our readers with this excellent analysis. At a basic level, the authors propose a solution to the technically challenging problem of a potential future everyday occurrence: how to use a digital currency when neither the payer nor the payee is connected to a payment network.

The paper's objective is to educate central banks on how using an online payment system protocol, or a set of rules or procedures for transmitting data between electronic devices, can allow a user to make a digital payment in CBDC while both users are

temporarily offline. This offline payment system, or OPS, can be used to instantly complete a transaction involving any form of digital currency over a point-to-point channel without communicating with any payment intermediary. These are not abstract concerns for regulators and policymakers. Last year, the Bank of England warned that a CBDC without offline capability "would limit the usability and usefulness of CBDC" by exposing the buyer, the seller, or the central bank itself to the risk that a payment might not be settled (Bank of England, 2020).

Even though these are innovative technologies, there is still a risk that criminals will try to exploit these new forms of money and platforms. Not surprisingly, many central banks have pointed out that offline payments, or CBDCs in general, must be secure against digital counterfeiting, fraud, and other types of cybersecurity risk and criminal exploitation. In October 2020, the Bank of Japan expressed concern that offline CBDC usage, without proper security protocols, could deteriorate CBDC security and make it more prone to counterfeiting (Bank of Japan, 2020). We know that people will not use technology they don't trust, which is why the Visa team grounded this technology in tried-and-true security architecture.

As a first step, the foundation for security in this offline system builds upon the principles of public-key cryptography. Today, most mobile devices, for example smartphones and tablets, are equipped with secure hardware to store keys and other sensitive material that can be accessed only through strong user authentication measures, such as biometrics. It has been shown that compromising these hardware-protected mobile devices without help from their manufacturers is very difficult. This secure environment can potentially make mobile devices a viable option for storing a user's CBDC funds and sending offline payments using hardware-protected credentials provisioned by the central bank or one of its delegates. The security of the device hardware is critically important, but provided it has not been tampered with, the process detailed by the Visa team in this paper significantly mitigates the risk of double-spending attacks, or the attempt by an individual—usually in a coordinated fashion with other actors—to spend his or her digital currency more than once.

For the many central banks that are exploring CBDCs, the opportunity to make a secure and reliable digital version of cash for their citizens, regardless whether that person is connected to the internet, is critically important. If central banks want to develop a CBDC, it must be made widely available, and in a manner that connects every citizen to the rapid innovations in financial services. Digital transformation holds great promise for society and the broader economy, but only if the technology is accessible to everyone, everywhere.

Sources

Boar, C., and Wehrli, A. (2021). "Ready, steady, go? Results of the third BIS survey on central bank digital currency." Bank of International Settlements. https://www.bis.org/publ/bppdf/bispap114.pdf

Bank of England (2020). "Discussion Paper: Central Bank Digital Currency Opportunities, Challenges, and Design." https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

Bank of Japan (2020). "The Bank of Japan's Approach to Central Bank Digital Currency." https://www.boj.or.jp/en/announcements/release_2020/data/rel201009e1.pdf

---

About the Visa Economic Empowerment Institute

The VEEI is a non-partisan center of excellence for research and public-private dialogue established by Visa.

The VEEI's overarching mission is to promote public policies that empower individuals, small businesses, and economies. It produces research and insights that inform long-term policy within the global payments ecosystem. Visa established the VEEI as the next step in its ongoing work to remove barriers to economic empowerment and to create more inclusive, equitable economic opportunities for everyone, everywhere.

Visit: visaeconomicempowermentinstitute.org

©2021 Visa. All rights reserved.