CENTRAL BANKERS' NEW CYBERSECURITY CHALLENGE

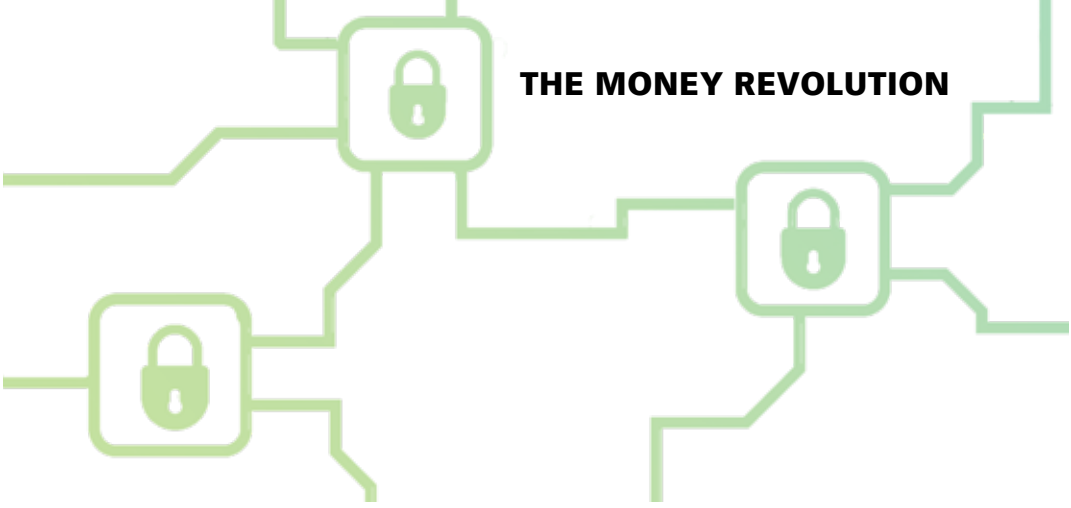
Central bank digital currencies may pose security risks, but responsible design can turn them into opportunities

Giulia Fanti, Josh Lipsky, and Ole Moehr

In the typically cautious world of central banking, the idea of a central bank digital currency (CBDC) is moving at lightning speed. Atlantic Council GeoEconomics Center research shows that 105 countries and currency unions are currently exploring the possibility of launching a CBDC, either retail—issued to the general public—or wholesale, used primarily for interbank transactions. That's up from an estimated 35 as recently as 2020. It is not just smaller economies that are interested, either; 19 Group of Twenty (G20) countries are considering issuing CBDCs, and the majority have already progressed beyond the research stage.

But as more countries launch CBDC pilot projects, concerns about cybersecurity and privacy loom large. Federal Reserve Chair Jerome Powell recently listed "cyber risk" as his number one worry relating to financial stability, and a recent UK House of Lords report specifically described cybersecurity and privacy risks as potential reasons not to develop a CBDC.

These concerns are not unfounded. CBDC vulnerabilities could be exploited to compromise a nation's financial system. CBDCs would be able to accumulate sensitive payment and user data at an unprecedented scale. In the wrong hands, this data could be used to spy on citizens' private transactions,



Technology enables central banks to ensure that both cybersecurity and privacy protection are embedded in any CBDC design.

obtain security-sensitive details about individuals and organizations, and even steal money. If implemented without proper security protocols, a CBDC could substantially amplify the scope and scale of many of the security and privacy threats that already exist in today's financial system.

Until recently, little work had been done publicly in the cybersecurity and central banking world to actually understand the specific cybersecurity and privacy risks associated with CBDCs. Few have considered whether CBDC designs could mitigate risks or perhaps even improve the cybersecurity of a financial system.

Our new research, published in the Atlantic Council's recent report, titled "Missing Key–The Challenge of Cybersecurity and CBDCs," analyzes the novel cybersecurity risks CBDCs may present for financial systems and makes the case that policymakers have ample options to safely introduce CBDCs. There are many design variants for CBDCs, ranging from centralized databases to distributed ledgers to token-based systems. Each design needs to be considered before reaching conclusions about cybersecurity and privacy risks. These designs also need to be compared with the current financial system—the one that keeps Powell up at night—to determine if new technology could deliver safer options.

So what are some of the main new cybersecurity risks that could arise in a CBDC? And more important, what can be done to mitigate these risks?

Centralized data collection

Many of the proposed design variants for CBDCs (particularly retail CBDCs) involve the centralized collection of transaction data, posing major privacy and security risks. From a privacy standpoint, such data could be used to surveil citizens' payment activity. Accumulating so much sensitive data in one place also increases security risk by making the payoff for would-be intruders much greater.

However, the risks associated with centralized data collection can be mitigated either by not collecting it at all or by choosing a validation architecture in which each component sees only the amount of information needed for functionality. The latter approach can be aided by cryptographic tools, such as zero-knowledge proofs, which authenticate private information without revealing it and allowing it to be compromised, or cryptographic hashing techniques. For example, Project Hamilton (a joint effort by the Boston Federal Reserve and the Massachusetts Institute of Technology to explore a US CBDC) has designed a system that separates transaction validation into phases, and each phase requires access to different parts of the transaction data.

These cryptographic techniques can be extended even further to build systems that verify transaction validity with only encrypted access to transaction details like sender, receiver, or amount. While these tools sound too good to be true, they have been tested extensively in privacy-preserving cryptocurrencies such as Zcash and are based on significant advances in the cryptography community. The bottom line is that technology enables central banks to ensure that both cybersecurity and privacy protection are embedded in any CBDC design.

Transparency vs privacy

A common concern with privacy-preserving designs (including those that use specialized cryptographic techniques) is reduced transparency for regulators. Regulators generally require enough insight to identify suspicious transactions, enabling them to detect money laundering, terrorism financing, and other illicit activities.

But even this is not an either/or decision. Cryptographic techniques can be used to design

PHOTO: FUNTAP VIA GETTY IMAGES

International standard-setting and more knowledge sharing between banks is critical at this moment of rapid development and adoption.

CBDCs that provide cash-like privacy up to a specific threshold (for example, $10,000) while allowing government authorities to exercise sufficient regulatory oversight. This kind of threshold is not so different from the current system in the United States, which allows reduced reporting for transactions under $10,000. The reality is that in many ways, a new CBDC system would not need to reinvent security protocols but could instead improve on them.

Several countries have committed to or even deployed retail CBDCs whose underlying infrastructure is based on distributed ledger technology. Nigeria's eNaira, launched in October 2021, is a good example. Such designs require the involvement of third parties as validators of transactions. This introduces a new role for third parties (for example, financial and nonfinancial institutions) in central bank money operations. Critically, the security guarantees of the ledger would depend on the integrity and availability of third-party validators, over which the central bank may not have direct control. (Although it is possible to implement distributed ledger technology with all validators controlled by the central bank, doing so largely defeats the purpose of using the technology.) The associated risks can potentially be mitigated through regulatory mechanisms such as auditing requirements and stringent breach disclosure requirements. However, there is not a clear blueprint for devising these regulations in a system as time-sensitive and closely interconnected as a distributed-ledger-based CBDC. This is why the need for international standard-setting and more knowledge sharing between banks is critical at this moment of rapid development and adoption.

Threat or opportunity?

Over the past 18 months some central banks have prematurely decided that a CBDC poses too many cybersecurity and privacy risks. We wanted to determine what is truly a threat and what is actually an opportunity. We concluded that governments have many CBDC design options to choose from, including new variants that have not yet been fully tested in current central bank pilots. These variants present different trade-offs in terms of performance, security, and privacy. Governments should choose a design option based on a country's needs and policy priorities. Based on our evaluation of these trade-offs, CBDCs are not inherently more or less secure than existing systems. While responsible designs must take cybersecurity into account, that should not prevent consideration of whether to design and test a CBDC in the first place.

One thing is abundantly clear in our research. Fragmented international efforts to build CBDCs are likely to result in interoperability challenges and cross-border cybersecurity risks. Countries are understandably focused on domestic use, with too little thought for cross-border regulation, interoperability, and standard-setting. Regardless of whether the United States decides to deploy a CBDC, as issuers of a major world reserve currency, the Federal Reserve should help lead the charge toward development of global CBDC regulations in standard-setting bodies. International financial forums, including the Bank for International Settlements, IMF, and G20 have a similarly critical role to play.

CBDCs' cybersecurity and privacy risks are real. But solutions to these challenges are within the grasp of technologists and policymakers. It would be unfortunate to preemptively decide the risks are too high before developing solutions that could actually help deliver a more modern and stable global financial system. FD

GIULIA FANTI is a senior fellow at the Atlantic Council GeoEconomics Center and an assistant professor of electrical and computer engineering at Carnegie Mellon University.
JOSH LIPSKY is the senior director of the Atlantic Council GeoEconomics Center and a former IMF staff member.
OLE MOEHR is a fellow at the Atlantic Council GeoEconomics Center.