DMI OMFIF Digital Monetary Institute

aws

THE FUTURE OF MONEY

CBDC cyber resilience and the payments revolution

Wed 17 May 2023 14:00 - 15:15
Virtual roundtable

Participants at roundtable

Michael Greenwald
Senior Executive and Global Lead of Digital Assets and Financial Innovation, Amazon Web Services

Aristides Andrade Cavalcante Neto
Chief, Cybersecurity and Technical Innovation Office, Banco Central do Brasil

Peter Faykiss
Director, Digitalisation Directorate, Magyar Nemzeti Bank

AWS, together with OMFIF, convened a roundtable to discuss concerns over central bank digital currency cyber resilience. A panel of cybersecurity and digitalisation experts from Banco Central do Brasil, Magyar Nemzeti Bank and AWS explored the metrics for resilient CBDC design, cyber resilience approaches that could apply to wholesale and retail CBDCs and cyber threat identification and mitigation strategies for central banks.

With the idea of how CBDC payment rails can maximise secure interoperability for transactions and other digital assets, a key point was made about how the architecture of CBDC can be guided – not only by privacy and efficiency concerns – but by monetary policy goals as well. These concerns were explored in a poll of the audience at the event. The most common answer, with 38% of respondents choosing it, was low adoption, followed by cybersecurity with 31% (Figure 1).

If CBDC systems lack resilience, this could result in personal data breaches for both institutions and individuals as well as reputational harm to the central bank. This was identified as the greatest vulnerability in deploying a CBDC by audience members at the event (Figure 2).

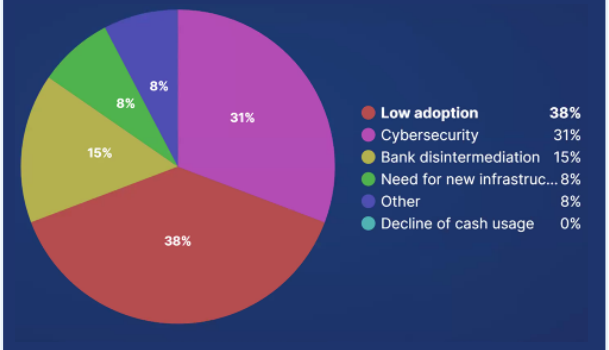
Counterparty risk and liquidity risk are also a concern as many CBDC projects are being designed to potentially work across jurisdictional borders, as well as offer foreign exchange settlement capabilities. If a cyber threat was able to compromise these operations, then a lack of trust in cross-border payments could hamper trade.

Moreover, supporting new financial services in decentralised finance will attract more cyber threats as the protocol used to interface between two platforms (for example, hashed timelock contracts) can be the point most vulnerable to cyber risk.

With this in mind, new network entrants and payments service providers should be informed of the liquidity and cyber controls expected by the central bank. Joint cyber testing can accelerate the development of sound cyber resilience strategies and regulation should be proportional to the level of risk in the financial activity being carried out.

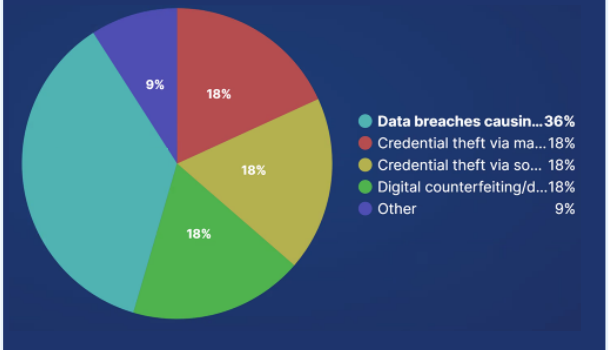
Some distributed ledger technology architecture

Figure 1. Low adoption is the greatest concern in CBDC deployment



Source: OMFIF audience poll

Figure 2. Data breaches identified as main vulnerability

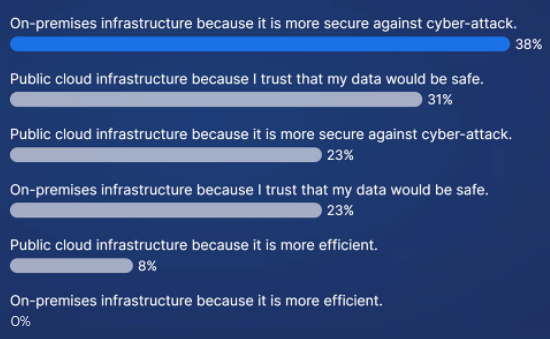


Source: OMFIF audience poll

can leave user data exposed to the validators of the consensus algorithm. Another point of vulnerability is smart contracts codes, which are more exposed than they would be in centralised systems and could be exploited to steal large amounts of cryptocurrency. To address this, clear governance structures and monitoring of access privileges is essential, as is control over what oracles can be used.

Zero-knowledge proofs and confidential computing could potentially resolve these concerns. The panel suggested that a wholesale CBDC system transaction

Figure 3. On-premises architecture still preferred to cloud services for CBDC



Source: OMFIF audience poll

in supply chain arrangements using smart contracts may be best achieved with blockchain-backed architecture. For a retail CBDC – where the focus may be on high transaction speeds – centralised architecture may support this aim.

Core banking and money processing systems are also a potential solution. Some banks have one system for customers' personal data and a separate system for storing transaction data. This modular approach enables system agnosticism regarding the question of centralised architecture or DLT.

Points of failure can arise from external factors outside the network, with data breaches causing loss of personally identifiable information. End users may be targets of fraud through social engineering, malware or other means. However, this can be helped through improved financial and digital literacy, fraud detection methods to identify unusual activity and periodical social media reviews. To mitigate the impact of digital wallets being hacked, fund limits can be set on the account balance.

Upskilling staff and operators of CBDC platforms and systems should incorporate knowledge from the private sector's working practices in technology, cybersecurity strategy and user experience design. Central banks can refer to international standards for password structure (such as numbers, letter case variation and special characters) and implement suggestions from user feedback.

Technological developments in AI and machine learning should also be included in cyber resilience strategy development. At present, physical cash coexists with commercial bank money. CBDCs will need to be designed with the potential for interoperability with stablecoins and other DeFi instruments.

Central banks will implement high standards of cybersecurity for CBDCs and similar standards would need to be applied to stablecoins and digital assets if they are to be used in the CBDC payments network. Central banks should form their own risk management strategies and make use of the best digital architecture for their projects.

Some central banks have highlighted that hybrid cloud or multi-cloud strategies could be useful tools in delivering CBDC scalability, cybersecurity and resilience. These approaches have highly developed, robust disruption recovery strategies.

Through cloud, smaller fintech firms can catalyse their cyber resilience practices by using technology that already meets international standards for data management and operational resilience. In some cases, cloud service providers can support financial institutions to manage their process flows more effectively than using on-premises architecture exclusively.

Although there are clear benefits to using cloud services – scalability, cybersecurity and flexibility – there are other factors that central banks must consider. Data sovereignty is a key issue for central banks looking at cloud technology. Storing data on premises can ensure greater security and is still preferred by most central banks but it deprives institutions of the benefits of the cloud (Figure 3). Cloud technology providers working to deliver data privacy, sovereignty and regulatory changes in this area are a key point of interest for central banks.

'Some central banks have highlighted that hybrid cloud or multi-cloud strategies could be useful tools in delivering CBDC scalability, cybersecurity and resilience. These approaches have highly developed, robust disruption recovery strategies. '

Aligned approaches to operational and cyber resilience can form the foundations of regulatory frameworks that central banks can apply to payment service providers seeking to operate within the CBDC ecosystem. CBDC design should be led by use cases observed through dialogue between the public and private sector and the types of transactions central banks foresee these new payment rails being used for in their jurisdiction.

While several digital architecture options may be accessible and useful, it is also necessary to comply with regional legislation pertaining to privacy (particularly with the personal data of children), and other requirements for payments information and processing. •

omfif.org/dmi