Renato Dias De Brito Gomes: Emerging technologies, lessons from Pix and Drex, and future perspectives

Speech by Mr Renato Dias De Brito Gomes, Deputy Governor of the Central Bank of Brazil, at the Digital Money Summit 2025, London, 20 May 2025.

* * *

Good morning, ladies and gentlemen,

It is a great honor to address this distinguished audience.

I would like to thank OMFIF for the opportunity to be here and share with you the Central Bank of Brazil's journey with emerging financial technologies.

Today, I would like to take stock of some valuable lessons learned from our digital initiatives - specifically Pix, our instant payments system, and Drex, our Central Bank Digital Currency (CBDC) pilot project[1].

Pix

Pix, launched in November 2020, is perhaps our most visible success in financial technology.

Designed as a public, open instant payments platform, Pix quickly transformed Brazil's payments landscape.

Its key benefits-instant transfers available 24/7, broad range of use cases, low transaction costs, ease of use, and high security-have driven widespread adoption among both consumers and businesses, aside from the government. Currently, Pix handles billions of transactions monthly, significantly reducing the reliance on cash and reaching previously underserved populations.

Beyond these achievements, looking ahead, the Central Bank of Brazil believes that Pix may serve as a foundational infrastructure that could facilitate more complex financial arrangements, including settling transactions involving tokenized assets.

This is indeed a possibility we are envisioning for the near future and that I will explore later in this talk.

The success of Pix highlights the merit of digital public infrastructures, which, with an open architecture and inclusive design, level the playing field across industry participants.

We took to heart this observation in deciding to initiate Drex.

Drex

Recognizing the transformative potential of CBDCs, we initiated a pilot to test Drex, our digital currency initiative.

In its original design, Drex was conceived as a multi-asset programmable DLT platform.

The platform consisted of various layers. At the wholesale level, financial institutions would settle transactions exchanging Central Bank money, to which we refer as wholesale Drex.

At the retail level, agents would hold tokenized bank deposits issued by financial institutions, which we call retail Drex.

Transfers at the wholesale level would reflect the execution of smart contracts at the retail level.

This multi-layered architecture aimed at reconciling the benefits of financial intermediation with the efficiency gains promised by the programmability of settlement transactions.

To implement this vision, we initiated a pilot program with two phases. The central focus of the first phase of the pilot was addressing privacy, a must-have component for public trust and acceptance of digital currency.

We were interested in observing the performance of smart contracts and their composability, as well as the suitability of privacy tools to the Brazilian legal framework.

Specifically, we simulated transactions between participants and their users involving three different assets (central bank money, tokenized bank deposits, and treasury bonds).

We considered one single business case that corresponds to the life cycle of a Treasury bond that includes:

a) Emission of Treasury bond in a tokenized format
b) public offering to participant financial institutions and their users
c) secondary market transactions
d) transference of bonds among wallets
e) bond amortization against tokenized CB money and bank deposits

This phase 1 of Drex involved intensive testing of advanced privacy technologies, including zero-knowledge proof, network segregation, confidential computing, and various data obfuscation techniques.

For instance, one technology we considered is Anonymous Zether, a zero-knowledge proof technique that creates private versions of tokens.

This technology was able to guarantee the privacy and anonymity of transactions for participants not involved in the transaction itself, but did not guarantee full disclosure to regulators and other authorities.

Another technology we considered is Rayls, developed by Parfin. This solution creates segregated ledgers based on EVM, which are interoperable through a common underlying communication layer. In this way, the tokens required to execute a contract on the segregated ledger are transferred and deposited within the ledger itself, ensuring that only the ledger owner has visibility into the operations performed.

This solution was again successful in ensuring the anonymity of transactions. However, it presented serious scalability challenges.

Just to give some idea on the platform speed, our RTGS can process 300 transactions /second, Drex with no privacy solution can process 150 transactions/second, and Drex with this privacy solution can process less than 10 transactions/second.

We also considered other privacy solutions, such as Starlight, developed by Ernst & Young (EY).

Overall, our extensive evaluations showed significant promise in protecting privacy; however, in all cases, the system's response time became longer, user experience got worse, and programmability was impaired.

Our experience confirms what is often referred to as the "privacy trilemma," a challenge in simultaneously achieving privacy, scalability, and programmability within distributed ledger technology (DLT).

Despite technological advancements, tough trade-offs persist.

Phase 2: Exploring Business Models and Programmability

With these insights in mind, we moved forward into Phase 2, shifting our attention toward deepening our understanding of how financial markets could benefit from a DLT-enabled built-in programmability.

In Brazil, high borrowing costs and collateral constraints disproportionately affect small and medium-sized enterprises (SMEs).

A case in point is that of bank-issued time deposits (CDBs).

Currently, roughly a third of the total funding by Brazilian financial institutions takes the form of CDBs.

Yet, there is no secondary market for these assets, which are typically not redeemable before maturity.

As a result, if an investor wants to sell her CDB, she must negotiate a rate with the issuer, who then exerts monopsonistic power over the investor.

Current technical restrictions on the trading and collateralization of bank-issued time deposits (CDBs) could be significantly eased through tokenization, which greatly facilitates the integration with front-end applications.

This phase of the pilot – still being carried out – evaluates various use cases that enlarge the set of collateralizable assets, including CDBs, public debt, credit card receivables, and debentures.

Early results already confirm the transformative potential of DvP with atomic settlement and programmability in streamlining complex financial transactions, lowering costs, reducing settlement risks, and increasing market efficiency.

Combining the lessons learned from phases 1 and 2, we devised a strategy with a short-term and a long-term dimension.

In the short term, we remain technology-agnostic, prioritizing solutions that effectively address current market frictions using existing infrastructure.

Rather than committing to widespread DLT adoption or full-scale CBDC implementation, our current approach seeks incremental improvements that leverage established financial market infrastructures.

The idea is to provide a bridge between current Central Bank settlement systems and specific token arrangements.

Related examples that come to mind include the Banca d'Italia hash-time-locked-contracts model and the trigger solution by the Deutsche Bundesbank.

Looking further ahead, we envision a scenario where tokenized asset arrangements increasingly become commonplace, including those arrangements that settle with fully backed stablecoins [and, thus, indirectly using central bank money].

Within such an ecosystem, central banks will play essential role, for instance, acting as custodians of reserve backing of stable coins, managing omnibus accounts, or creating interoperability through bridges to RTGS systems.

If the current shortcomings of DLT and other emerging technologies are effectively addressed, central bank money itself could potentially be tokenized and integrated into distributed ledger environments.

This possibility would entail even more significant efficiencies, programmability, and market democratization.

As time goes by, the challenge is to identify assets which privacy requirements are compatible with available technology.

As the technology frontier expands, it will become possible to privately trade more and more assets in a programmable ledger.

In the meantime, we need flexibility to be able to pivot to a DLT-based unified ledger when the time comes.

For this future to become true, I believe that collaborative efforts by regulated entities and Central Banks are crucial.

In Brazil, we will insist on the same collaborative market-driven approach that made Pix a success.

Collaboration across jurisdictions is also essential to share best practices and highlight common challenges.

These interactions reinforce our belief that cooperation and continuous dialogue are vital for successful innovation.

Conclusion

Our journey with Pix and Drex has taught us critical lessons about managing innovation strategically and pragmatically.

By balancing visionary goals with careful risk management and continuous market collaboration, we remain committed to exploring technology's full potential to strengthen financial systems and benefit society at large.

Thank you for your attention, and I look forward to continuing this important dialogue throughout the summit.

---

[1] The Brazilian Approach to Financial Innovation
At the Central Bank of Brazil, we believe that innovation must serve clear objectives: efficiency,
inclusivity, security, and financial stability. Our approach is to be proactive yet pragmatic, fostering
innovation through rigorous experimentation and close collaboration with market participants,
international regulators, and academia.