PROJECT SYNDICATE – 28 LUGLIO 2025

Currency Dominance in the Digital Age

di Hélène Rey

As digital technologies become the rails upon which money moves, the resilience and credibility of currency networks increasingly hinge on the integrity of technological infrastructure. This fundamentally changes the logic of monetary competition, with far-reaching implications for financial and geopolitical stability.

PARIS – For more than 80 years, the US dollar has enjoyed unrivaled supremacy in world trade and finance, thanks to America's unique combination of economic scale, credible institutions, deep and liquid financial markets, and geopolitical might, as well as, crucially, network effects. But a new variable is poised to reshape the global monetary order: data integrity.

As digital technologies increasingly act as the rails upon which money moves – through stablecoins, tokenized assets, and central bank digital currencies – the resilience and credibility of currency networks increasingly hinge not only on macroeconomic fundamentals, but also on the technological strength and security of the relevant infrastructure. Of course, macroeconomic fundamentals still matter, and digital currencies raise some conventional macro challenges. In particular, by privatizing seigniorage and facilitating tax evasion, stablecoins could shrink countries' fiscal revenues.

Moreover, if a stablecoin breaks its peg – say, because its liquidity buffers prove insufficient – its credibility could collapse, triggering a run. If the stablecoin's interconnections with other assets is sufficiently dense, this may have systemic consequences. A disorderly run on US dollar stablecoins – privately issued digital tokens that are backed significantly by US Treasuries and can theoretically be exchanged one-for-one with dollars – could prove particularly disruptive. Opacity in

reporting and auditing, and insufficient regulations in some jurisdictions, compound the risks.

But such "classic" credibility issues are just the beginning. The world could also face a new kind of "cyber" run, triggered by weaknesses in the technological infrastructure underpinning digital assets. Mitigating this risk will not be easy: as the National Institute of Standards and Technology of the US Department of Commerce warned in 2016, quantum computers may soon be able to break many of the public-key cryptosystems currently in use. In other words, infrastructure that appears robust today may turn out to be flimsy tomorrow.

The implications for the global monetary order are far-reaching. As the issuer of the dominant international currency, the United States has long enjoyed an "exorbitant privilege," which includes the ability to borrow at low interest rates even in times of economic stress and run persistently large trade deficits. President Donald Trump's administration seems to be betting that the US will be able to retain this privilege, as the dollar's existing global status translates into demand for US dollar stablecoins and, in turn, US Treasuries, thereby lowering the US Treasury's financing costs.

Ultimately, America's exorbitant privilege is based on trust in its institutions, legal frameworks, and fiscal capacity. In a world where money circulates on programmable platforms, however, the credibility and integrity of the code, the quality of cryptographic standards, and the resistance of systems to hacking are as important as any of these factors. This fundamentally changes the logic of monetary competition: if the technological gap is large enough, the currency that is best protected from cyber threats – not necessarily the one backed by the most powerful economy or the most credible central bank – becomes the most attractive.

As stablecoins are being used for a growing share of cross-border payments, and as an on- and off-ramp for speculative crypto investments, much about their security and governance remains unknown. Regulators and citizens should thus be asking questions. Who is responsible for governing the ledger? To what extent is the system protected from malicious actors? What happens if a currency's cryptographic backbone is compromised by developments in quantum computing?

Answering these questions satisfactorily is a matter of national and international monetary stability. If policymakers fail to act accordingly, we might find ourselves

with the kind of volatile and fragmented monetary system that characterized the nineteenth century, when the unfettered issuance of private money opened the way for panics, runs, manipulation, and collapse.

In any case, we may be headed toward a multipolar monetary system, in which some currencies – and their associated digital ecosystems – command an "integrity premium," based on their ability to minimize their "attack surface" and maximize data verifiability. The most successful currencies will offer a very robust financial architecture, which covers every step, from the validation of transactions to the protection of user identities and transaction histories. So, a currency backed by a government with weak cyber defenses or opaque technological standards could lose ground, and a technologically sophisticated currency zone with high integrity standards could punch above its weight.

This new technological landscape could have significant geopolitical consequences. Just as naval supremacy once translated into trade dominance, control over payments infrastructure could increasingly determine economic sovereignty. The strategic value of payments data – not only for monetary policy, but also for surveillance, enforcement, and sanctions – means that digital currencies are not neutral technologies; they are contested spaces of power. The currencies that dominate tomorrow's international system will be those whose digital ecosystems inspire the deepest trust – both in their institutions and in their code.

Preserving international monetary stability in such a landscape will require more than technological innovation. Global coordination on standards for tokenization, cryptographic interoperability, data privacy, and post-quantum resilience will be essential. The alternative – the proliferation of balkanized networks governed by conflicting rules and exposed to systemic shocks – is a recipe for instability.