The Evolution of CBDCs: From Domestic Experiments to Interoperable Networks

October 4, 2024   8 min read
Author: Anthony Butler

Anthony Butler is a Chainlink advisor, and former CTO of IBM Services, Middle East and Africa.

Central Bank Digital Currencies (CBDCs) continue to be the subject of extensive research, experimentation, and analysis globally as central banks consider what the future of money may look like and whether tokenised central bank money should play a role in that future. This journey didn't begin, of course, in 2024 but goes back many years: with the CBDC concept evolving substantially from the earliest domestic experimentations through to cross-border experimentation and now, the emergent concept of a "finternet" that seeks to weave together the worlds of tokenised and non-tokenised assets into a common fabric.

History of CBDCs

The first CBDC experiments appear to go back to 2014 when the Central Bank of Uruguay and China experimented with the e-Peso and e-CNY respectively. This was followed by various experiments such as Canada's Project Jasper, South Africa's Khoka, Monetary Authority of Singapore's Ubin, and others. Some of these projects sought to replicate a form of digital cash (i.e. retail CBDC) and others sought to replicate the features and functions of the RTGS (i.e. wholesale CBDC).

Much of this early phase of experimentation was focused on understanding this new technology called "blockchain" and whether there was a potential to create something in a regulated context that resembled the innovations

that were happening across the crypto ecosystem with Bitcoin, Ethereum, and so forth.

These domestic experiments were quickly followed by multi-jurisdictional experiments where the aperture was broadened to consider how CBDC could be used as instruments of cross-border settlement. For example, Hong Kong and Thailand's Project Lionrock, Saudi Central Bank and UAE Central Bank's Project Aber, Canada and Singapore's integration of Jasper and Ubin (known as Jasper-Ubin), and Project Dunbar in which the BIS brought together the central banks of Australia, Malaysia, Singapore and South Africa to test multiple CBDCs on a single shared platform. This latter project demonstrated the efficacy of CBDCs for international settlement and led to Project mBridge.

The drivers for cross-border experimentation were different, with the primary goal of these initiatives being to address inefficiencies in international payments and remittances, which are often slow, costly, and opaque. For example, cross-border payments frequently take 3-5 days to clear and banks "continue to be the costliest channel for sending remittances," with an average cost of 12.1% according to the World Bank.

Current CBDC landscape

Today, there are still experiments being conducted domestically and cross-border and there are a small number of countries that have, having seen projects provide significant efficiency, programmability, and composability advantages, made a decision to move forward with CBDCs. At the same time, there are now many examples of private money being tokenised too, such as the tokenised deposits that are issued as tokenised claims against commercial bank balance sheets. As with wCBDC, many of these are exploring cross-border scenarios too.

As we look at the evolution of this space and the efforts underway globally, it is clear that it is highly improbable that the world will converge on a single blockchain platform that will span the globe and be the "universal ledger" onto which all assets and forms of money will be tokenised.

Key reasons why a singular "universal ledger" will not be realised:

1. Not all countries will move towards tokenisation at the same time or same pace, so there will be a need for coexistence between the legacy and new systems for an extended amount of time.

2. The choice of protocol or technology to tokenize an asset, such as permissioned or zero-knowledge based chains for privacy, fast-finality solutions for payments, and public blockchains for decentralized security, will be informed by the local jurisdictional requirements, the type of asset being tokenised, the types of markets that the asset will need to be listed in, and a myriad of other functional and non-functional requirements that will lead towards a particular technology. It is probable, for example, that different commercial banks may choose to use different technologies for tokenised deposits, central banks may use other technologies for their CBDCs, assets will be tokenised on a number of other heterogenous networks based on where there is demand and liquidity, and each system will need to interconnect with a myriad of other systems outside their jurisdiction such as the various DLT and non-DLT based messaging and cross-border payments systems.

3. The technology is evolving quickly with scalability solutions that can support mass adoption and the barriers to entry are being lowered such that it is conceivable that, at some point in the future, instantiating a blockchain network will be analogous to the instantiation of a relational database today; a situation that will further lead to proliferation of networks.

4. There are already emerging regional and other blocs in which different jurisdictions are coming together to build their own cross-border networks focused on a particular set of corridors or a particular region.

The end result is fragmentation, silos, and islands that, without bridges, will not be able to deliver on the original promise of blockchain.

Digital Islands
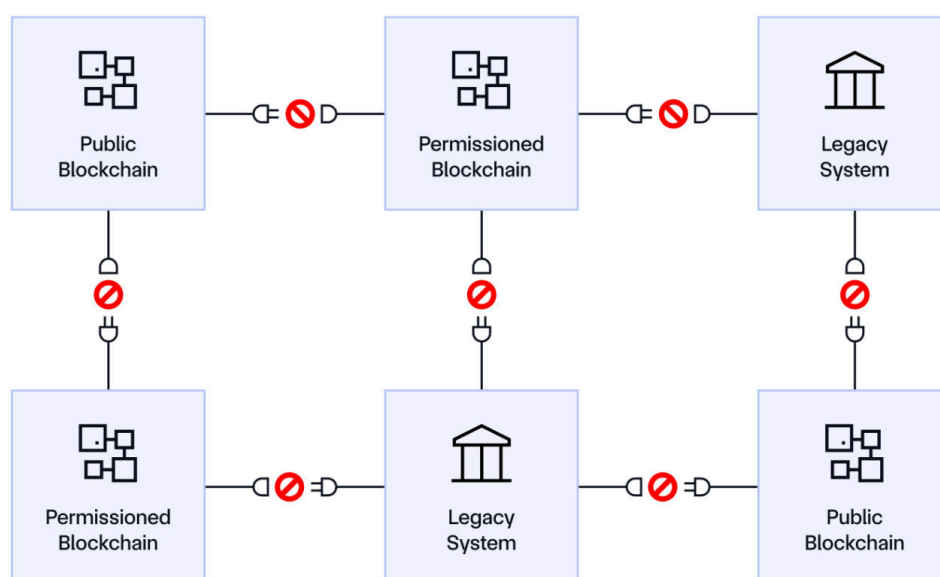
Without blockchain interoperability, a fragmented ecosystem would emerge.

We can find synergies in the origins of the Internet. In the early days of the Internet, there were distinct networks that emerged to service different communities. There was ARPANET, CSNET, and NSFNET, for example, and a number of other networks that emerged in other parts of the world. They did not have any way to communicate with each other and were, like the various DLT networks of today, islands. On January 1st, 1983, this would change when they would adopt a common "language" known as Transfer Control Protocol/Internetwork Protocol or TCP/IP as it is commonly known today. It was the adoption of this universal language that led to the birth of the Internet.

As we see the various DLT-based financial networks following a similar trajectory with islands emerging, the question that must be asked is how will we solve the interoperability challenge? What, one might ask, is the TCP/IP of the blockchain era that will allow the TradFi and DeFi worlds to interoperate but also, within each, allow the various tokenised assets, deposits, and CBDC platforms to talk to each other? As with the Internet, it is only through the seamless integration of these networks that the true value can be realised.

What would a TCP/IP of the blockchain world need to offer?
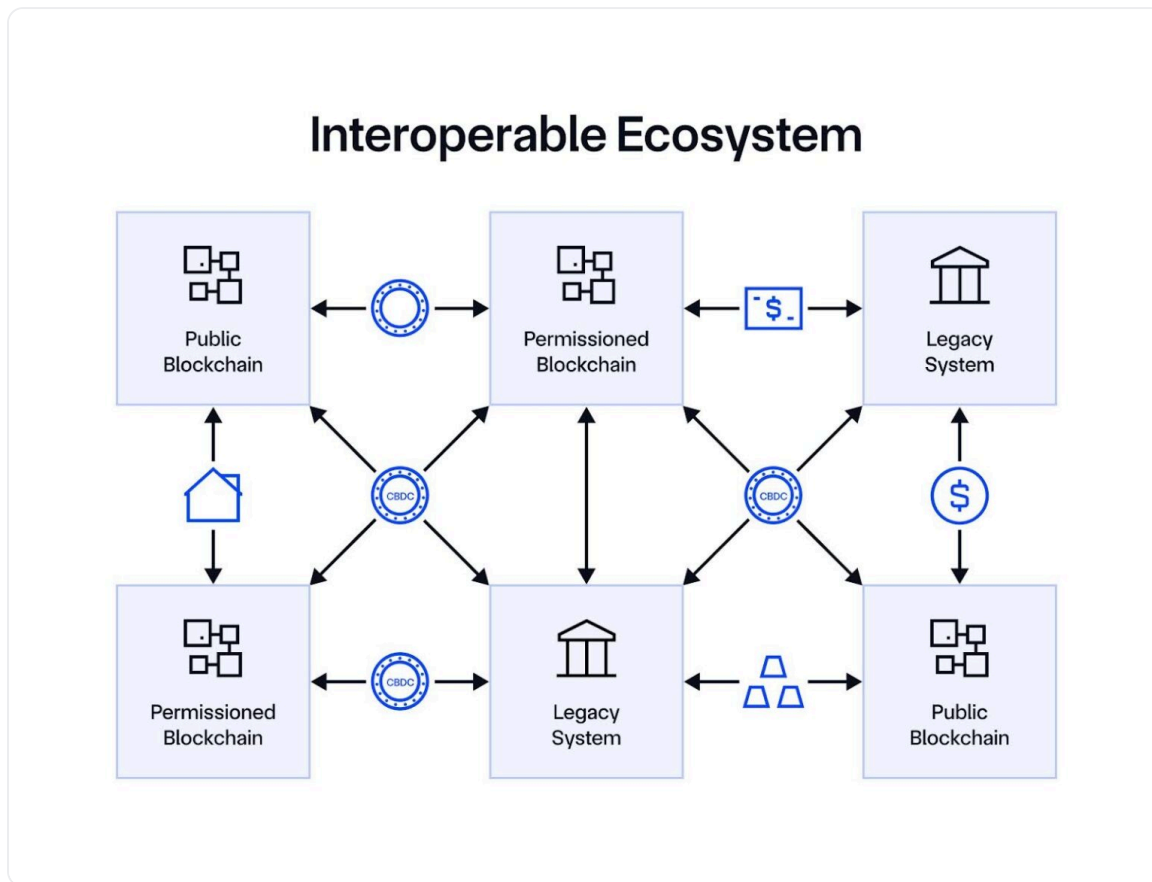
A TCP/IP of the blockchain world enables an interoperable ecosystem.

Firstly, this protocol should enable tokens—the "packets" of blockchain-based finance (onchain finance) containing value and data—to move securely between networks, even heterogenous protocols, such as public and permissioned. It should do so in a way that ensures security and the integrity of the system. For example, it would obviously be problematic if some tokenised money was moved from one network to another yet it continued to persist in the original network since this would enable "doubling spending" and would undermine the integrity of the entire system.

Second, smart contracts should be able to govern and orchestrate the movement of these tokens such that sophisticated settlement use cases can be executed, such as the transfer of a CBDC from one network to another occurs only contingent on the transfer of a tokenised security from one network to another; or various payment versus payment scenarios such as exchanging CBDC on one network in one currency for CBDC on another

network and in another currency. In order to support complex operations cross-chain, the interoperability solution must be programmable, embedding both tokens and instructions on what to do with those tokens in a single cross-chain transaction.

Thirdly, these tokens may be created as representations of some physical or "real-world assets", such as a security or real estate. At the time of being created, this link will be established and, as the token moves between networks or cross-border, this link should not be broken but should continue to ensure that the token-holder has visibility and can have confidence in the linkage between the digital and physical worlds through real-time proof of reserve verifications. Further, as attributes of the physical asset change over time, the token should also be updated with offchain data being injected into the token's smart contract to reflect these changing values.

Fourth, whilst TCP/IP was based on the movement of packets without consideration for what information was embedded in them, a TCP/IP of the blockchain world needs to take into account that much of what is being moved is of real financial value and is subject to a range of complex regulatory and other considerations. There needs to be an appropriate oracle-based privacy and permissions mechanism that ensures the security of the system while also supporting compliance with various regulations, enabling institutions to apply predefined controls and limits across transactional activity, including policies around identity, AML/KYC, legal requirements, organizational restrictions, and more.

Fifth, there needs to be a recognition that so-called legacy systems will need to co-exist and synchronize with the new systems and therefore the protocol should enable the seamless movement of value and data between these legacy worlds and the tokenised world—and vice versa.

Finally, as CBDCs or other tokenized assets move across chains through their lifecycle, they must be continually updated with key price, reserves ownership, compliance, and other data, regardless of which environment they're transferred to. This would enable the creation of a unified golden record—a single source of truth that all stakeholders can read from.