Evolving Mobile Networks, Artificial Intelligence and Low Orbit Satellite Systems as Enablers of Intelligent CBDC Ecosystems

Giori S.A.

Purpose of the Study

The coming together of five technologies including 5G/6G, Artificial Intelligence (AI), Low-Earth Orbit satellite constellations, and Central Bank Digital Currencies (CBDCs) creates a new paradigm in how we exercise money, identity, connectivity and sovereignty in the 21st century.

Each of the individual technologies will be transformative on their own but taken they create a sovereign digital nervous system that can support resilient, inclusive, intelligent and geographically autonomous monetary systems.

This document describes how the four layers will integrate into a next generation CBDC architecture for emerging markets, regional monetary unions and future proof central banks to improve sovereign security, increase financial inclusion and support the development of interoperable CBDCS systems alongside existing legal tender physical cash.

Executive Summary

Central bank digital currencies are now moving beyond the testing phase toward a strategic choice about what the central bank's monetary system will look like. In other words, a retail central bank digital currency is not simply an additional way for people to make payments; it is the digital version of the government's money and when implemented at a large scale it will become an integral component of the country's monetary base. Therefore, it will need to meet more than the standards of being innovative and efficient: it will also need to provide access to all citizens; provide reliability in times of stress; be secure; be trustworthy; and support financial inclusion, maintain monetary sovereignty, protect consumers, and contribute to maintaining systemic stability.

The primary message of this research is quite straightforward: most designs of central bank digital currencies have placed far too great an emphasis on ledger technology, token design, and cryptographic techniques and have given far too little attention to the fundamental building blocks upon which any functional central bank digital currency requires for reliable connectivity and operational intelligence to work in practice.

A digital currency can never be "cash-like" if it does not operate reliably in the event of network congestion; does not operate in rural communities; relies on expensive equipment; or collapse in disaster and crisis situations. The central bank digital currency will need to perform well in the edge cases of its usage, not merely in the idealized environment of urban centers.

Key messages for policy makers and regulators

1. **CBDC is an essential piece of the country's infrastructure.**
   A retail CBDC should be governed similar to a national utility. It must be designed to be universally accessible, continuous and resilient; have a defined accountable body for oversight and contingency planning.
2. **Connectivity is integral to the monetary system.**
   The success of CBDC is dependent upon both the communication layer (satellite, mobile network, etc.) and the ledger layer. If the communications layer does not provide reliable access, then neither will the money.
3. **Intelligence is required to ensure security and scalable compliance.**
   To prevent the use of traditional rule-based controls and manual review at the large-scale CBDC, fraud and AML risks require an automated adaptive approach that protects both the privacy and proportionality of users.

4. **Trust is a product of the design process and not a PR issue.**
   A CBDC must demonstrate privacy safeguards for everyday transactions, strong security and predictable behavior during outages in order to create trust. Without creating trust, CBDC adoption will be limited by the technical capabilities of the system.
5. **Architectural decisions today will influence CBDC for decades to come.**
   CBDC will have to function across multiple types of networks (3G, 4G, 5G, 6G), multiple satellite options, multiple evolving threats, and eventually post quantum cryptography. The system must be designed to continue to evolve and improve over time without needing to be completely rebuilt.

Why connectivity and intelligence are now central to the future of monetary infrastructure

The technological environment has changed. For example, although 5G offers faster speeds than previous generations of wireless networks (3G, 4G) for a larger number of people, many individuals are still accessing mobile phone services using their "dumb" (feature) phones via USSD (Unstructured Supplementary Service Data). At the same time, satellite constellations of Low Earth Orbit (LEO) satellites offer a resilience layer, providing access to remote and disaster-prone areas where building cell towers may not be economically viable.

However, connecting CBDC systems to the internet and allowing them to communicate with each other is not sufficient to make them secure or manageable. Artificial Intelligence (AI) is becoming the operational intelligence layer of CBDC systems, capable of detecting fraudulent activity in real-time, reducing false positives, supporting Anti-Money Laundering (AML) pattern detection, and adapting to emerging threats. However, using AI to achieve these objectives does not necessarily mean that the government will need to collect all the data from every transaction. Techniques such as privacy-preserving analytics, on-device risk-scoring, and federated learning enable organizations to meet their security requirements while limiting the amount of sensitive data collected about individual users.

Therefore, there is a new infrastructure stack: GSM (Global System for Mobile Communications) for basic inclusion, 5G for high-quality service, LEO for global continuity and AI for adaptive security and management. Together, these technologies enable CBDC to begin approaching and cooperating with what is referred to as the 'cash standard': usable by everyone, resilient in times of crisis, and managed as a public good. Furthermore, CBDC is complementary to cash and preserves the characteristics of cash in digital form.

Summary of strategic implications

1. **CBDCs need to be designed to be hybrid in their delivery options**
   There is no single level of cellular network availability in any one country. Therefore, CBDC needs to work seamlessly using both feature phones and smartphones, regardless of the strength of the cell signal, including satellite backup when necessary.
2. **Central banks need to establish baseline standards of acceptable services (service level agreements) for accessing a CBDC.**
   These would include how well the system performs during times of heavy demand, what type of service guarantee(s) are provided for monetary transactions, how the system defaults, and what types of business continuity plans are in place
3. **Monetary logic should be separated from transportation logic in the CBDC architecture.**
   Regardless of the underlying transportation layer used (e.g., GSM, 5G, Satellite), the monetary security and settlement rules should always apply consistently. This is similar to the GSMT / Intelligent E-note concept of having a stable monetary instrument while allowing lower-level access methods to evolve.
4. **Regulators will need to develop new regulatory models to oversee the use of artificial intelligence in monetary systems.**
   They will need to ensure that there are governance mechanisms in place for the AI models, and provide mechanisms for auditing the models, assessing potential biases and errors in the models, identifying concentration risk (i.e., telco/cloud/satellite providers), and clearly defining the limits of the data that may be collected and used. The goal is to allow for the use of AI, but to do so in a manner that is accountable and proportionate.
5. **Planning for post-quantum cryptography should be part of the planning process for CBDCs.**
   CBDCs are long-term systems, and thus they require the ability to be able to upgrade their security features, perform version control, and enable migration paths, so that the overall ecosystem is not disrupted when upgrading to more secure versions of cryptographic algorithms.

Call to Action

In summary, for decision-makers, the practical implication of this report is that the adoption of a CBDC will be primarily dependent upon the credibility of the infrastructure, rather than the theoretical debate of how CBDC should be designed. For CBDCs to move past pilot projects and achieve long-term, nationwide adoption, central banks and regulators should recognize connectivity and intelligence as critical components of the monetary infrastructure, outline specific requirements for resiliency and trust, and create an evolutionary architecture that can operate effectively within the limitations of the real world.

A CBDC that only works when all the networks are perfectly connected and all the devices are current will never become a nation's currency. A CBDC designed on a converged stack with accessible connections (GSM), high-performance capabilities (5G/6G), continuous operations (LEO), and adaptable security (AI) can reasonably be expected to serve as the national digital monetary core that public institutions seek.

Main Takeaways

CBDCs are now developing into the new generation of the world's financial infrastructure. They are based on advanced communication technology; advanced AI-based capabilities and next generation technologies. As such they can provide the backbone for supporting the digital economies around the globe.

Seamless, ubiquitous connectivity will be fundamental to successful global implementation of CBDCs. Convergence of 6G Networks and Low Earth Orbit (LEO) Satellite Constellations is expected to produce near universal coverage and thus enable reliable access to areas currently unserved or under-served. This hybrid architecture will allow for real-time transaction processing in an environment that is both secure and ubiquitously accessible. Essentially it represents a transformation from "Offline" payment systems toward a continuous, always-available payment ecosystem.

Artificial Intelligence (AI) will play an important role as a facilitator/enabler within the CBDC Ecosystems. AI will facilitate enhanced fraud detection, enhance monetary policy effectiveness through additional adaptive and responsive tools and assist users through multi-language intelligent interfaces. Additionally, AI-enabled analytical capabilities will provide further insight into economic phenomena. Collectively, AI will increase operational efficiency, expand financial inclusion and foster greater levels of confidence; particularly in geographies where there exists limited financial literacy.

As quantum computing continues to evolve, current cryptographic frameworks will become increasingly vulnerable to exploitation by the computing power of tomorrow's

computers. To mitigate this vulnerability, CBDC systems will require the incorporation of post quantum cryptographic solutions to maintain long term security and protect the integrity of monetary sovereignty. Post quantum cryptography will protect transactions, digital identities and critical central banking infrastructures from future computational threats.

Contents

1. Introduction

Central Bank Digital Currency (CBDC) is the digital form of a country's fiat money. It is issued and backed by central bank, and it represents evolution of current physical cash. It is aimed to be the digital monetary core of a country by complementing physical cash and preserving its core properties in digital form.

Since it will be the digital monetary core, CBDC needs to meet requirements which go beyond efficiency or innovation. It must be accessible by all the population, resilient and stable under stress. Furthermore, it must be aligned with public policy objectives such as financial inclusion, monetary sovereignty, and systemic stability. That's why the infrastructure supporting CBDC has great importance.

When the first CBDC technologies emerged, device and connectivity technologies were not aligned with current communication standards, which created some gaps in expectations and the CDBC products. To apply CBDC on national level and in every country with different infrastructure is a demanding task and limited mobile coverage and legacy devices have always been a problem in trial deployments.

But the technology environment has changed significantly. GSM networks have more coverage with expanded 4G/5G networks and promise even more features with upcoming 6G. Low Orbit Satellite (LEO) networks add a new layer of connectivity to complement GSM networks. Artificial intelligence has matured from experimental technology and is now widely used to improve security, detect fraud and systems improvement. Together these technologies can reshape what is possible with CBDC.

The report has been written by Giori S.A. associates to examine how these new technologies help CBDC provide future proof and resilient infrastructure needed. The audience of this document are central banks, monetary authorities, and public institutions involved in CBDC design and policy. It is also relevant for domain experts interested in digital money technologies.

Key Takeaways

- CBDC is critical national infrastructure, not just a payment innovation.
- Connectivity and intelligence are now core to monetary systems.
- Hybrid architecture (GSM + 5G + LEO) is required for real-world resilience.
- AI is essential for scalable fraud and AML — but must be privacy-preserving.
- Adoption strategy (not just technology) determines success.

2. GSM Networks, AI and LEO: The New CBDC Infrastructure Stack

A lot of discussion about the architecture structure of CBDCs is centered on ledger technologies, cryptographic techniques and standards. All those things are important, but they miss a very basic fact; none of them matter if you can't provide necessary level of intelligent connectivity to support the required reliability.
For the digital currency infrastructure to be able to handle all the transactions, it needs to be able to deal with the extreme edge case situations such as in remote villages or disaster zones and during times of economic crisis when traditional systems may fail.

Over the past year or so the technological prerequisites for developing fully resilient digital currencies have become available. This is not about making incremental improvements, these are structural changes in how connectivity, computation and intelligence come together. 5G networks are being rolled out across many cities around the world and satellite constellations are now providing the necessary level of coverage in areas where traditional terrestrial-based networks could never affordably cover. AI is now being deployed at scale within production systems to perform real time fraud detection and adaptive security.

This chapter will describe each layer of the new infrastructure stack required for CBDC deployment and examine what the technology capabilities, operational realities and strategic implications mean for Central Banks attempting to design monetary systems which work for everyone, and not just for the digitally enabled. The analysis is based on actual deployment data from mobile money systems, insights from payment network providers and the lessons learned by the first generation of CBDC pilots.

The question we are seeking to answer is this: Can the infrastructure required to support digital currencies achieve the same universalism, resiliency and trustworthiness as physical cash and deliver the speed, programmability and security expected of modern economies? The answer is dependent upon getting the infrastructure layer correct; everything else (such as smart contract functionality, cross border interoperability and monetary policy functions) builds on this foundational layer.

2.1 GSM and Legacy Mobile Networks

Most mobile connections are still provided via 2G and 3G connections in some countries. As developed countries have largely transitioned beyond 2G and 3G, the backbone of financial inclusion is still the GSM network in much of Africa, South Asia and Latin America. GSM is a feature that will need to be taken into consideration in any serious CBDC strategy.

One of the key properties of GSM is its ability to work on very simple devices. A feature phone made in 2010 can send USSD commands, make voice calls, and complete SMS-based transactions. This is particularly important as device replacement cycles in lower income populations is longer compared to developed countries.

Understanding the economics of this is also important. A basic feature phone can cost anywhere from 15 to 30 USD. A smartphone with sufficient capacity to operate most modern mobile banking applications typically costs eighty to one hundred fifty dollars. Therefore, if a person earns three to five dollars per day, the choice between an affordable feature phone and a more expensive smartphone is clearly going to be based on affordability. Additionally, there is the continued expense of owning a smartphone. You need to charge smartphones frequently and electricity can be scarce in some countries. But a feature phone, however, can continue to operate for up to a week on a single charge.

Current Coverage and Infrastructure Gaps

Global coverage now stands at approximately 95%-96% of the world's population, based on GSMA's State of Mobile Internet Connectivity 2025 Report [1]. Not 100% because low-density areas do not provide enough revenue potential for private companies to build cell towers, therefore government incentives and alternative methods of technology deployment are required.

There is also a difference in what we would consider good quality cellular coverage. For example, a tower may be able to reach an area; however, if it is transmitting 50,000 subscribers using a 2G backhaul connection, the quality of service for those subscribers will likely be very poor. A payment system requires continuous, low latency access to a network, not the spotty access you receive when large number of subscribers are competing for bandwidth to a cell tower 15 kilometers away.

For example, in Kenya, where M-Pesa has had great success, mobile network congestion during peak hours (such as lunchtime or the end of the workday) can cause transaction failures. To avoid these errors, users have learned to perform their transactions outside of peak hours; however, this is unacceptable for the use of the national currency system. Therefore, there must be "headroom" in the infrastructure to support peak loads without degrading performance.

A final challenge to providing a nation-wide CBDC infrastructure is population density. Many developing nations such as Bangladesh and Nigeria have large, densely populated urban centers. These urban centers are typically surrounded by less dense suburban and rural communities and/or villages. Therefore, the CBDC infrastructure must support each of these areas, and must support multiple fallback methods and graceful degradation.

Feature Phones and Basic Wallet Functions

Although there are many different types of advanced devices in the payment device ecosystem of emerging economies (such as smartphones), there is also a large number of "feature" phones (phones with basic capabilities of running Java ME or KaiOS, limited memory, small screen size and no application ecosystem) which are inexpensive, sturdy and will last all week on a single charge which is more important than the amount of processing capability when the user has unreliable electricity.

CBDC wallet implementations on feature phones will likely utilize three forms of deployment models. One form of deployment is using USSD (which works but offers awful UX for anything other than simple transactions). The second form of deployment utilizes SIM Toolkit Applications (which offer slightly better interfaces but require the user to coordinate with the mobile carrier, replace their SIM card and possibly replace their phone). The third form of deployment is utilizing lightweight applications on KaiOS, which can be used for local transaction signing and basic cryptography, but will still require some type of offline mode for successful operation.

USSD

USSD (Unstructured Supplementary Service Data) should receive consideration due to being one of the financial infrastructure protocols available today. It was proven with M-Pesa in Kenya as early as 2007 that you do not need to have an Internet connection to transfer money. USSD provides session-based connections that do not rely on a data plan and can be accessed even if a customer does not have enough credit to make a call.

Technically the architecture is very simple, yet powerful. A user simply dials a short code *(*XXX#)* and will establish a direct session with the USSD gateway. The gateway then directs the command to the appropriate service and returns a text-based response that is displayed on the simplest of phone screens. As stated above, the entire session runs over the signaling channel of the GSM network. Thus, the session will run over voice and data traffic channels before they begin.

From an engineering point of view USSD sessions are very reliable. Unlike TCP/IP stacks, USSD sessions operate across multiple networks and seamlessly follow the mobile device from one cell tower to another. The big downside is there is very little session state where users will be interacting with a menu driven interface and thus limited for sending messages with limited character length.

In addition, typical USSD sessions will take anywhere from 2 to 5 seconds to complete for simple functions. The typical implementation allows for up to 182 characters per message. While this significantly limits the complexity of what can be displayed, it also demands

good User Experience (UX) design where every single character counts when screen space is so constrained.

SIM Toolkit

The second method for developing a wallet on legacy GSM network could be utilizing SIM Toolkit Applications (STK) which offer an intermediate solution between pure USSD and full-fledged applications. STK is a small application that resides on the SIM card which has a secure element capable of performing cryptographic functions. A STK based CBDC wallet can securely store cryptographic keys and perform the necessary transaction signatures without revealing the keys to the phone's operating system and will provide persistent transaction logs even after the user replaces their phone since the SIM remains the same.

However, the limitation of STK is scalability. The mobile carrier(s) must agree to deploy the STK based application on SIM cards which require commercial negotiations and technical integration which can be a barrier to entry, especially if the central bank needs to negotiate with multiple carriers to roll out the application across the entire country. Depending on the level of regulatory oversight the central bank may be able to mandate that all mobile carriers support the STK application however, this would add another layer of complexity and potentially create delays in the rollout of the CBDC application since the central bank would be waiting on the mobile carriers to deploy the application.

KaiOS

Another recent alternative that is beginning to gain popularity is KaiOS, a new light-weight web-based operating system designed to run on previously underutilized low-end hardware. The costs of the devices supporting KaiOS are from $20 to $40 and they include physical keyboards which improve the user’s usability to enter PIN numbers and transaction amounts. They can also and can run HTML5 applications with limited JavaScript. With respect to CBDC, a web application can be developed to run off-line, to store encrypted wallet state in the local storage and synchronize with online servers when network connectivity becomes available. Unfortunately, this would not be as robust as developing a native application for Android but could be better than relying solely on USSD.

Another major constraint for KaiOS method will be the ability to compute, once these devices do not possess the capability to execute complex cryptographic functions due to their 512 MB RAM and 1 GHz processors. A CBDC wallet implementation would need to account for the limitations of this type of computing environment.

GSM Transition Timelines and Operator Strategies

How long do GSM/3G networks really have left? This varies greatly depending on the country. In developed countries, mobile operators are rapidly phasing out 2G & 3G to free

up 5G spectrum; AT&T closed its 3G network in Feb. 2022; Most European operators plan to shut down 3G by 2025-2027.

In developing countries, mobile operators have repeatedly delayed shutting down their 2G/3G networks due to the large number of subscribers that rely on them for voice & basic services; But these countries are also trying to find ways to accelerate the timeline. Understanding the business drivers behind these timelines will provide insight into what factors are influencing the decisions made by mobile operators. For example, mobile operators generate most of their revenue through data services (i.e., mobile internet, video streaming), rather than voice or SMS. Refarming 2G & 3G spectrum to be used for 4G/5G will increase mobile operator's ability to provide high speed data services, resulting in increased revenue.

In those markets where mobile operators have very thin margins & intense competition, there is significant motivation to transition to higher margin services. However, many government regulations limit the ability of mobile operators to prematurely terminate older technologies. Governments in many countries have regulations requiring mobile operators to maintain basic voice service capabilities for emergency communications, which sets a floor on how quickly 2G can be terminated.

2.2 5G: The Terrestrial High-Performance Layer

GSM has served as the foundational layer for 5G. 5G can be defined as the performance layer which supports next generation applications. The technology advancements in 5G are not simply incremental changes, but rather fundamental architectural changes that enable a completely new class of use cases for digital currency infrastructure.

The 5G specifications define three categories of services each tailored to a particular use case [2]:

- eMBB (Enhanced Mobile Broadband), supporting applications requiring very high speeds for data transfer.
- URLCC (Ultra Reliable Low Latency Communication) for Mission Critical Applications.
- mMTC (Massive Machine Type Communications), enabling communications for massive numbers of IoT devices.

For Digital Currency Infrastructure URLLC and mMTC will be more applicable, but eMBB provides richer user experience in wallet apps.

Low Latency and Edge Computing

Ultra-low-latency reliable communication (URLLC) is the headline capability of 5G. It is intended to provide low-latency communications with high reliability for mission-critical use cases such as financial transactions, autonomous vehicles, remote surgery etc. For comparison, 4G LTE has typical end-to-end latency of 20 ms to 50 ms in best case scenarios and significantly higher in worst case scenarios due to increasing levels of congestion on the network [3]. This latency has a material impact upon the user experience in a number of areas including real-time payment authorization, particularly at the point-of-sales where customers expect the same level of convenience as they do from contactless payment cards (which typically complete a transaction in less than 100 ms).

The ability to support URLLC is due to the adoption of edge computing architecture in 5G networks. As opposed to using centralized data centers which may be hundreds of miles away from users, 5G places compute resources at the edge of the network typically at a cell site or regional aggregation point. Single-digit milliseconds may be achievable in optimized deployments. Therefore, in a CBDC environment it would be feasible to perform wallet authorization logic, fraud detection, and validate a transaction near the user by reducing the round-trip time by an order of magnitude.

The multi-access edge computing (MEC) framework provided by 5G is specifically designed to enable this type of architecture. MEC provides a mechanism for third parties (e.g., central banks or their technology partners) to deploy their own applications at the edge of the network (near the radio base stations). Applications deployed in MEC can obtain low-latency access to local users and utilize network application programming interfaces (APIs) to gather information about the user's context (approximate location, network characteristics, device capabilities) while protecting the user's privacy.

Network Slicing and Quality of Service

Network slicing is an entirely new 5G capability that can have a significant impact on the way CBDCs can be deployed in financial services. Essentially, it allows the creation of separate and distinct "virtual" segments of the physical network, each with their own unique performance attributes. For example, a financial services slice may be provisioned to guarantee 99.999% up-time as well as receive priority bandwidth allocation, whereas a video streaming slice receives no such guarantees i.e., best effort delivery.

As a result, for central banks, there are exciting options to negotiate dedicated network slices for CBDC infrastructure so that payment traffic will always receive priority over other forms of traffic, even when the network is congested. So, if a disaster strikes having a

communications channel that is guaranteed for monetary transactions provides a critical form of business continuity.

To implement network slicing technically, central banks utilize Software Defined Networking (SDN) and Network Function Virtualization (NFV) to divide a single physical network into logically isolated virtual networks. With SDN/NFV, each virtual network slice receives its own dedicated set of radio resources (frequency band, time slot), core network resources (routing, switching), and computing resources (to support additional value-added services). While physically a single radio tower supports all slices, logical separation is what enables Quality of Service (QoS) guarantees. This is achieved by implementing sophisticated traffic management mechanisms to enforce these guarantees.

CBDC Use Cases Enabled by 5G

Several new CBDC capabilities become feasible through the combination of low latency, edge computing, and network slicing compared to legacy infrastructure:

- **Instant retail payments nationwide:** Transaction confirmations in sub-seconds, even under high volume loads, to create an equivalent user experience to contactless cards (e.g., tap, beep, done) without requiring specialized hardware other than their existing smartphones.
- **Secure wallet-to-wallet communication:** Device-to-device peer-to-peer transfers using 5G side link-based D2D protocols, allowing for transaction records to be created offline regardless of whether there is mobile network connectivity available. This capability has significant value in crowded venues such as markets, concerts, and transit stations where mobile networks may be overwhelmed but devices can communicate directly over short range radio links.
- **Real time policy signaling:** Central bank ability to dynamically update spending limits, velocity controls and geographic restrictions based on real time risk assessments which are useful for fraud prevention and controlling capital flows. For example, if abnormal transaction patterns are identified within a specific geographic area, the central bank can temporarily limit spending or require additional verification before transactions can be authorized and settled without having to wait for the typical batch processing cycle.
- **Massive IoT payment integration:** IoT-enabled devices such as those found in transportation systems, energy meters, and municipal services can be integrated into CBDC settlement rails to enable automated micropayment transactions without requiring human interaction. An example would be an EV charging system where the vehicle's wallet negotiates pricing, authorizes charging and settles payment by the kilowatt hour without any interaction with either an app or payment

terminal. To explore further, the massive machine type communications (mMTC), part of the 5G standard, provides the potential to support up to 1 million connected devices per km^2 [2]. For smart city infrastructure, this means each of the millions of parking meters, bus validators, and electricity meters could process CBDC transactions without the need for batch processing.

This is essentially programmable money that can be executed automatically based on data from IoT sensors. A good example of how this technology can work in practice is public transportation. Right now, most public transportation systems use contactless cards that require users to preload balances and then remember to refill them. This can create unnecessary inconvenience (remembering to top off, managing multiple cards for different cities).

Using 5G enabled CBDC and IoT integration, it will be possible to implement true "pay-as-you-go" transit: get on a bus, your phone's wallet will detect the validator using NFC or Bluetooth; negotiate the fare with the validator based on the distance you have traveled; and automatically settle payment when you exit the bus. All of this can happen with no card, no app opening, and no interaction with the user.

Deployment Timeline and Coverage Expectations

There are vast differences in the 5G rollout timeline by region. South Korea and China have largely covered all their large urban areas. Many countries in the U.S. and Western Europe are now actively deploying 5G and are covering many of their larger cities, however, much of their rural areas are far behind. Emerging market countries are just now conducting the first 5G auction and launching initial pilot deployments.

For CBDC planners, the realistic expectation for 5G is that it will be primarily an urban based network until at least 2027 – 2028. Coverage of rural areas will most likely take longer, probably well into 2030+, based on European Union's Digital Decade Strategy [4]. Therefore, any CBDC system must be capable of operating in a hybrid mode utilizing 5G features as available and fallback to 4G / 3G in areas lacking coverage or integration with satellite systems as explore in further chapters. This is not a flaw in architecture; rather, it is recognizing operational realities and creating systems that can operate along the entire coverage gradient.

The rate of rollout can also be influenced by the availability and allocation of radio spectrum. Countries that have completed the auction of 5G radio spectrum and assigned specific frequency bands to carriers tend to deploy 5G networks faster. On the other hand, countries where the 5G spectrum policy debate continues or where the auction of spectrum has been delayed for political or economic reasons tend to be further behind in terms of the deployment of 5G.

2.3 Looking Ahead: 6G and the Future of CBDC Connectivity

As we continue to roll out 5G deployments, 6G R&D is already looking towards the future of wireless infrastructure for the next decade. We expect the first 6G standards to appear around 2028-29 with commercial deployments to begin in the 2030-32 timeframe [5]. Since monetary systems that are being created today will likely be around 15-20 years, we believe that understanding 6G's capabilities is important for CBDC infrastructure planning.

6G is not simply 5G with better performance. It is a completely different approach to how wireless networks will be integrated with sensing, computing and AI. The target parameters for 6G include peak data rates of 1 Terabit per second (1000 times faster than 5G), latency less than 1 millisecond and the ability to support 10 million devices per km^2 [6]. However, the truly exciting aspects for CBDCs relate to the architectural changes in 6G and not simply the performance enhancements.

In contrast to 5G where AI is an application that runs on top of the network, 6G includes machine learning directly into Radio Resource Management, Beamforming and Spectrum Allocation. Therefore, the network itself can determine whether to prioritize payment traffic, predict congestion and optimize routing for payment transactions without manual configuration. Intelligence has been inserted into the network infrastructure rather than added to it after the fact.

Another defining aspect of 6G is the use of Terahertz frequency bands (100 GHz to 10 THz). Terahertz provides an enormous amount of bandwidth; however, they have a very limited range – tens of meters vs. kilometers. One possible application for CBDCs related to the use of Terahertz in 6G relates to ultra-high density transaction processing in specific locations. Imagine a stadium with 80000 fans making simultaneous payments for concessions, merchandise and transit. Today 4G/5G infrastructure would likely struggle to process these types of transactions; however, 6G terahertz cells could enable very high-density transaction environments.

One additional feature of 6G is Integrated Sensing and Communication (ISAC), which combines network infrastructure with sensor networks. In other words, 6G base station will transmit data while also sensing its environment, determining the location and movement of objects, detecting material properties etc. One example for CBDCs using ISAC relates to context aware payments; your wallet can detect that you are at a transit gate, detect the fare zone via network sensing and authorize the payment automatically without requiring you to scan anything or even pull your phone out of your pocket.

Additionally, the architecture of 6G assumes that satellite services will be available ubiquitously from the onset. This contrasts with 5G, where satellite service is treated as an

add-on. This is critical to ensure the resilience of CBDCs as the hand-off between ground-based networks and Low Earth Orbit (LEO) satellites will occur seamlessly and without any protocol changes or user interaction.

In addition to the above features, the architecture of 6G includes a completely revised approach to security. Post-quantum cryptography is included from the onset of 6G and not added afterwards. Additionally, physical layer security utilizes the inherent characteristics of the wireless channel (such as channel randomness and beamforming accuracy) to create secure communications that are extremely difficult to intercept. For CBDCs, this represents a further layer of security beyond the level of encryption that occurs within the applications themselves.

Based upon the timelines for both the rollout of 6G and the implementation of CBDCs, there are a few conclusions that can be immediately drawn regarding the development of CBDCs:

- CBDC systems rolled out in the 2025–2027-time frame will exist primarily in a 5G dominated world until the early 2030s when they begin to migrate to 6G.
- CBDCs will require infrastructure that can evolve as 6G is rolled out and does not require the wholesale replacement of existing systems.

Protocol design for CBDCs should be modular such that the core transactional logic remains unchanged and that the network access layers can be replaced as new technologies become available.

The last area being considered for development in 6G is energy efficiency. An energy efficiency target of 10 to 100 times better than 5G is expected for 6G. This will allow for longer battery life in mobile devices and lower operational costs for network operators. This will help especially in rural areas where electricity and charging might be a problem.

It is unlikely that CBDCs can wait until 6G is widely implemented before they start to use the new technology. CBDCs can, however, use 6G technology while designing with the technology in mind. To do this, the decision-makers creating the CBDCs need to create the CBDCs in a way that allows them to transition from 5G to 6G technology without needing to rebuild all their applications. Decision-makers must separate the concern of how users get network access from the concern of what applications the users want to run and create a clean interface between the two so that once 6G is available, they can easily add the new technology to their current system.

2.4 LEO Satellite: Monetary Continuity Beyond the Grid

Satellite constellations operating in Low Earth Orbit (500 - 1200 km) will be the largest advancements in connectivity infrastructure since the mobile revolution. Traditional Geostationary Satellites operate at an altitude of approximately 35,000 kilometers and therefore experience high latency and limited bandwidth [7]. In contrast, LEO satellites experience latencies similar to those of terrestrial networks and provide sufficient bandwidth to support real time applications.

In terms of CBDC infrastructure, the key issue LEO satellites resolve is geographic coverage by terrestrial networks. Terrestrial networks have economic limitations as it would never make commercial sense to build cellular towers in areas of low population density. On the other hand, once a LEO satellite constellation is operational in space, the marginal cost of providing coverage of an additional one square kilometer is virtually zero. Therefore, LEO satellites offer a good pathway to achieving universal connectivity, regardless of government subsidies or charitable deployments to cover such areas.

There are both positive and negative aspects to the physics of a LEO satellite orbit. Due to their relatively lower altitude, LEO satellites complete a single orbit around the earth in approximately 90 - 120 minutes. Consequently, LEO satellites are always in motion relative to any given ground station. To achieve constant coverage of any given area, a satellite constellation requires hundreds, if not thousands, of individual satellites. Starlink has already launched over 5,000 satellites and intends to launch an additional approximately 7000 satellites to achieve full operational capability.

One of the benefits of using LEO satellites is significantly reduced signal latency (approximately 30 - 50 ms vs. 600 ms for Geostationary Satellites), and improved signal strength allowing for smaller ground antenna sizes and lower transmission power requirements.

The Current LEO Landscape

There are three LEP constellations which are active today and they have different strategies and distinct technical features.

1. Starlink (SpaceX): It has launched more than 10000 satellites providing consumer internet service in more than 100 countries [8];bandwidth is impressive with download speeds of 100-200 Mbps and latency of 20-40 ms; however, the ground equipment used to communicate with the satellites currently require a fixed installation of a dish and consumes between 50-100 W of power, which is acceptable for rural broadband but impractical for individual mobile CBDC wallets. However, Starlink launched direct-to-cell capability with T-Mobile in 2025, first with messaging and increased support of voice

and data directly through satellites [9]. Starlink is aiming to expand this service, Spain in other regions soon [10].

2. OneWeb: It mostly focuses on enterprise and government connectivity, not mainly focusing on the consumer market. As such this may create opportunities for central banks to partner with OneWeb to obtain dedicated satellite bandwidth for CBDC communications that does not compete with consumer bandwidth. They have currently around 600 satellites active [11]. OneWeb's satellite operates in a higher orbit than those operated by StarLink (1,200 km vs. 550 km). This results in fewer satellites being required to achieve global coverage, but it also results in higher latency (50-80 ms vs. 30-50 ms).

3. Project Kuiper (Amazon): It has a lot of investment behind it, so it is expected to be a large-scale provider, but it is still in early stages. It is focused on consumer broadband like Starlink. Amazon's planned constellation will include satellites in multiple orbits optimized for different use cases (i.e., lower orbit satellites for low-latency applications and higher orbit satellites for wider area coverage).

In addition to the three main U.S.-based LEO constellations, several regional and national LEO constellations are emerging. For example, the European Union has plans for the IRIS^2 constellation as part of the EU's strategy for achieving strategic autonomy in satellite communications. The first launch of the IRIS^2 constellation is scheduled for 2027 [12]. China has announced plans for the GW (Guowang) constellation with the intention of launching 13,000 satellites to provide domestic coverage and coverage for other countries along the Belt and Road initiative [13]. In India, the Indian Space Research Organization (ISRO) is developing its own LEO system [14]. Central banks may see these regional and national initiatives as attractive alternatives to the U.S.-based LEO constellations, especially if they are concerned about geopolitical risks associated with relying on foreign providers for their CBDC systems.

Direct-to-Cell Capabilities

The most important feature for CBDC might be direct-to-cell satellite connectivity. This technology allows standard smartphones to communicate directly with LEO satellites without requiring special equipment.

The technical constraints are significant. It is a low bandwidth service like SMS and basic data, not video streaming. It provides 1-5 Mbps shared across potentially thousands of users within a satellite's coverage footprint. But for CBDC transactions, that's entirely adequate. 1-2KB of data should be enough for a wallet-to-wallet transfer. Even at degraded bandwidth, hundreds of transactions can be handled per second per satellite.

The technology behind this feature is impressive. Satellites traveling at 27,000 km/h need to track individual phones on the ground, establish radio links despite Doppler shift, and hand off connections as satellites move across the sky. The satellite essentially acts as a cell tower in space, using the same LTE/5G protocols that terrestrial networks use. From the phone's perspective, it's just another cell tower so no special firmware is required and there is no need for manual switching between terrestrial and satellite modes.

Obviously, the main feature is that it works anywhere, mountains, deserts, oceans, conflict zones. You get monetary infrastructure that operates independently of terrestrial networks, which provides resilience and sovereignty in case of natural disasters or any other unforeseen network shutdowns.

Coverage patterns also differ a lot from terrestrial networks. LEO satellites provide relatively uniform coverage regardless of terrain: for example, a valley surrounded by mountains gets the same signal quality as an open plain, unlike cellular which requires line-of-sight to towers. However, dense urban environments with tall buildings can block satellite signals, so LEO works best as complementary infrastructure rather than primary urban connectivity. The ideal architecture uses terrestrial networks where available and satellite as backup or for underserved areas.

Resilience and Disaster Recovery

Business continuity is also very important to consider in detail. The traditional way to do disaster recovery for electronic payment systems has been to create duplicate data centers at geographically redundant sites with failover procedures. The LEO satellite-based architecture presents a new paradigm: the network is distributed among hundreds of satellites by design.

If we examine a similar event to the 2011 Tohoku Earthquake (Tsunami) in Japan, which took down power and all forms of communication between a big population, even though the data centers were still functional; there was no way to connect to them to reach the affected populations. But the use of LEO satellites would allow for continued minimal payment function through the entire crisis period. It would enable those who require access to their money, and it would provide ability to make critical transactions without needing to rely on functioning ground-based infrastructure.

The engineering approach to accomplish this would include designing a hybrid system whereby normal operational activity utilizes terrestrial based networks due to both performance and cost considerations; however, once a user’s connection is lost, the associated wallet application automatically defaults to utilizing a satellite-based network. It would be somewhat degraded from a bandwidth perspective and increased latency-wise

compared to when using terrestrial networks; however, it represents the difference between being able to perform some level of operation versus a complete system failure.

Sovereignty and Strategic Considerations

A major concern from a central banking point of view for using private LEO satellite systems as part of the monetary infrastructure is the issue of sovereignty. There are three major LEO satellite system providers, which are U.S.-based companies; therefore, they are also subject to U.S. law and export regulations. If there was a conflict scenario or some sort of political dispute, access to the system could potentially be restricted, or communications could potentially be intercepted.

As a result, interests have developed in sovereign or regional satellite systems. The European Union is currently working on its IRIS^2 LEO satellite system as a means of obtaining "strategic autonomy." China is creating its GW LEO satellite system in order to have total independence from the western world's satellite systems. Neither of these will be fully operational by the late 2020s/early 2030s, but they represent a significant shift towards having multiple LEO satellite options available.

From a technical standpoint for architects designing CBDC systems, the practical approach is likely to be to achieve multi-provider redundancy, when possible, along with implementing security protocols and/or encryption methods that take into consideration the possibility of the network being compromised. If you properly design the system, then the satellite providers are simply dumb pipes, and cannot gain access to the transaction data or wallet credentials, much like you would not entrust your bank credentials to your telecommunications provider today.

In addition to the above-mentioned points, the encryption architecture must provide end-to-end protection. Transaction data should be encrypted at the wallet level prior to transmitting the data via any type of network, being terrestrial or via satellite. Even though a satellite provider may capture all the data transmitted through their system, they would only receive the encrypted payloads and therefore would have no knowledge of the amount of the transactions, the parties involved in the transactions nor the balance of the wallets involved. The cryptographic keys used for encrypting the transaction data will always remain on the user's device, specifically in secure element storage. Therefore, even if the network infrastructure were to be compromised, the integrity of the user's wallet remains intact.

From a geopolitical standpoint, there are several potential scenarios where satellite access could be denied. Such scenarios include, but are not limited to, sanctions against a particular country, the enforcement of export restrictions, or other types of geo-political conflict scenarios. As such, central banks will need to develop contingency plans. For

example, what would happen if one of the U.S.-based satellite providers were to be forced to terminate service to your country? The most logical response is to have multiple providers that operate within different geographic regions/jurisdictions. This way, the failure of one provider could rely on another one and have no catastrophic effects on the entire system. While this approach does increase costs, as it essentially pays for redundant capacity that hopefully will never be requested, it provides nevertheless the necessary degree of resilience required for critical infrastructure systems.

2.5 AI: The Intelligence Layer of Digital Money

Artificial Intelligence has now transformed from being a tool of experimental research into production systems. Regarding CBDC technology, AI is a critical enabler for developing a digital currency system that will continuously evolve to meet new threats as they occur.

AI capabilities have advanced significantly in terms of the capabilities of AI in the past ten years. Once we were limited to using rule-based systems that require continuous maintenance and manual tuning but now we are now utilizing machine learning models that adapt to changing patterns and trends on their own, identify edge cases that engineers could not anticipate or design for, and operate at scales that are unachievable with rule-based systems.

The potential economic benefits are tremendous; fraud detection powered by AI can enormously lower false positive rates compared to traditional methods of fraud detection.

From Rule-Based Systems to Adaptive Intelligence

The primary problem with traditional payment fraud detection is that these traditional methods rely on a set of pre-determined rules: "If a user's transaction total exceeds X, mark it as suspicious." "If a user completes Y transactions in an hour, block them." "If a user moves geographically more than Z miles in T minutes, ask for additional verification."

These types of rules work well enough, but they produce a very large number of false positives (i.e., legitimate transactions that are marked as suspicious). This produces two main problems: first, when a user has legitimate funds locked due to a false positive, it causes the user frustration. Second, when the security team spends a large portion of its time resolving false positives, the security team has less resources available to perform legitimate security functions.

Machine learning based approaches change this paradigm. Rather than defining a set of rules to detect suspicious activity, machine learning based systems are trained to identify anomalies i.e., those items that do not conform to some established pattern of normal behavior.

A typical technical stack used for training and inference includes Gradient Boosted Trees (e.g., XGBoost, LightGBM) or Deep Neural Networks using many different feature inputs such as the amount of the transaction, the category of the merchant, the time of day of the transaction, the location of the transaction, the fingerprint of the device used to complete the transaction, and over 100 other signals. However, given the nature of the use case where there is only little time to complete the scoring of the transaction, the best option is to deploy models to high-performance inference servers and optimize the inference process accordingly.

In addition, feature engineering also becomes increasingly important as the volume of data increases. As stated above, raw transactional data alone is not sufficient to identify behavioral patterns. Therefore, it needs to be created many new features that capture the essence of the user/merchant behavior. Examples include:

- How much is the amount of this transaction compared to the user's 7-day average?
- How much is the amount of this transaction compared to the user's 30-day average?
- How often does the user make transactions to this merchant category?
- Has the device used to complete this transaction moved to a significantly different geographic location in the last hour?
- Are there several high-dollar value transactions being made in close proximity to each other?

Creating these types of features is expensive and therefore, the companies will need to design very efficient data pipelines and caching mechanisms to be able to execute these queries quickly.

Finally, deployment of machine learning models requires ongoing evaluation and re-training of the models. Fraud schemes and attacks are continually evolving; that’s the reason what worked six months ago may not work today. So, production ML systems will need pipelines that monitor model performance and detect model drift (where the distribution of the data used to train the model has changed, resulting in lower model accuracy). Once a model drift event occurs, the pipeline should trigger a workflow to retrain the model.

Fraud Detection and AML Screening

Fraud detection is primarily concerned with detecting suspicious activity as transactions occur in “real-time”. In contrast, anti-money laundering (AML) is focused upon identifying behavioral patterns of individuals using financial products and services over extended periods of time. The most common ways individuals launder money include structuring

their deposits to remain under reporting thresholds, layering money through multiple bank accounts, and ultimately laundering money back into legitimate financial system.

Graph neural networks can provide solutions to these issues. Because graph neural networks can represent both transactional data and the relationship between transactions, they have become increasingly popular for anti-money laundering compliance. Graph neural networks model transactions as a graph, where each node represents an account and each edge represents a transaction. Once the graph has been created, the graph neural network is trained to recognize and flag suspicious subgraphs. Subgraphs are groups of connected nodes and edges within the larger graph. Because graph neural networks can look at the entire network of transactions rather than just a single transaction, they provide the capability to detect money laundering schemes that would not be possible to detect using a single transaction view. For example, a graph neural network can identify circular chains of transactions, unusual clustering of new accounts or money flows that follow money laundering typologies.

Of course, scaling becomes the main implementation challenge for implementing graph neural networks in an anti-money laundering system. A national central bank digital currency (CBDC) system may produce 10-50 million transactions per day. As a result, the size of the graph produced will be enormous, making continuous analysis difficult. To overcome this issue, organizations will need to implement distributed graph databases (e.g., Neo4j, TigerGraph), and/or streaming analytics platforms (e.g., Kafka, Flink).

Additionally, there will be the need to create sharding strategies to ensure efficient processing. Although this is technically feasible, the required engineering investments in infrastructure will be significant. Some examples of money laundering schemes that graph analysis can identify, yet rules-based systems cannot include:

- Smurfing: Breaking down a large transaction into several smaller transactions to remain below the reporting threshold.
- Round-Tripping: Moving funds from one account to another via multiple intermediate accounts before returning to the original account.
- Mule Account Network: Accounts that are compromised or complicit in attempting to hide the origin of funds.

The economic incentives surrounding anti-money laundering compliance are complex. In terms of the costs surrounding anti-money laundering compliance, banks incur significant annual costs related to compliance activities including manually reviewing all transactions for evidence of money laundering. Machine learning (ML) systems that can improve the accuracy of AML detection by reducing false positive rates can also significantly improve the overall economics of the compliance process.

For CBDC, where transaction volume could be 10-100 times larger than traditional banking systems, manual reviews of transactions will not be economically viable. As a result, automated machine learning screening of transactions will be very important for compliance with anti-money laundering regulations at scale.

Behavioral Risk Scoring Without Surveillance

There is a real tradeoff between how well a system can protect itself, and how much personal information about its users will be compromised during the process. A good system should be able to detect fraud, but it shouldn't allow for mass surveillance of users, and it certainly shouldn't allow for the creation of a database of users that would be available to an authoritarian regime. Technically, a middle ground can be found using differential privacy, federated learning, and on-device processing.

Differential Privacy allows for a limited amount of "noise" to be added to the training data and/or to the output of the model, so that no single user's transaction can be traced back to them using the model. However, the model can still identify general trends across all users, such as which merchant categories are at higher risk of fraud, or which hours of the day see the highest frequency of unusual transactions, etc.

Federated Learning builds upon the concept of differential privacy by training models on the user's device and then sending the model updates (gradients), encrypted, to the central server. The central server aggregates the model updates to update the global model, but it doesn't have access to any of the individual transaction data. Both Apple and Google are using some form of Federated Learning for their keyboard prediction features and other applications that need to learn from user behavior without compromising their privacy.

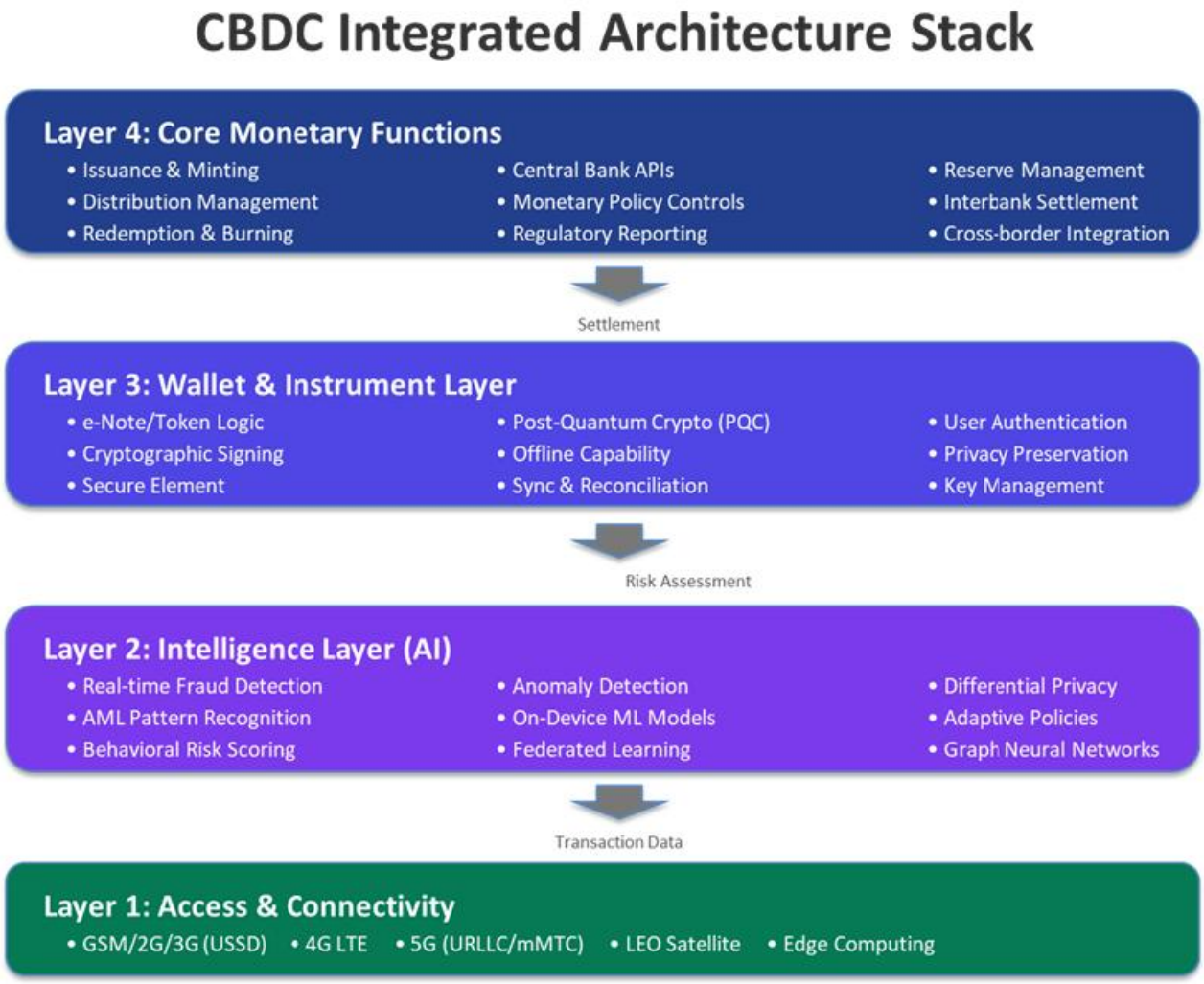
Similar architecture can be applied to Central Bank Digital Currency (CBDC) by having user's device to perform most of the fraud detection locally and only escalate any high confidence anomalies to the central system. This would reduce the amount of user data stored centrally within a government system but would also provide an adequate level of security. Implementing a system like this would require additional technical complexity compared to a more traditional centralized system, however, it would be the type of feature that would earn people's trust on CBDC.

Federated Learning requires a secure method of aggregating the updates received from each device to ensure that a central server cannot determine what individual device updates were used to generate the aggregated gradient. The two common methods to accomplish this are using threshold cryptography or secure multi-party computation. In both cases, only after a certain number of devices have submitted their gradients (for example, between 100-1000 devices) will the central server receive the aggregated gradient. Until then, the individual device contributions remain encrypted and therefore

unknown. Using Federated Learning provides protection against a curious server attempting to compromise individual user data while still providing for the ability to improve the global model.

2.6 The Integrated Architecture

The true strength of integrated architecture is the ability to create new features by combining existing ones, rather than relying on individual elements of architecture. By integrating a CBDC system using GSM for access, 5G for performance, LEO for continuous connectivity, and AI for security/adaptation capabilities, none of which could exist independently of each other, there are new capabilities being created.



Converged Architecture Model

The model described above is essentially a combined architecture with intelligent routing. The wallet application running on the consumer's device will monitor available connectivity options and determine the best option for the transaction and therefore select the most appropriate path.

This is not a new concept in terms of networking, mobile phones already perform similar functions based on whether they are connected to Wi-Fi, 4G, or 5G. However, the extension to financial infrastructure requires the architect to carefully consider how transactions will be finalized, how to reverse them, and how to ensure the integrity of security across all possible communication paths. Transactions that were started over 5G and completed over a satellite connection require the same level of security as those that remain on a single network throughout the entire transaction process.

The protocol should be transport independent. Regardless of whether the transaction is sent over 4G data, 5G with edge computing, or satellite link, everything should be identical like the cryptographic signing, validation logic, and settlement processes. Only the transport layer changes; depending upon the communications channel used, you may need to compress messages differently, send transactions differently, or use different encoding schemes to optimize bandwidth usage.

In addition to designing the protocols for transport independence, error handling also becomes an important consideration in heterogeneous networks. A transaction may begin over high-speed 5G but may complete over an intermittent satellite connection. In this case, the protocol must gracefully handle this situation. It needs to maintain the session state, retry failed operations using exponentially increasing timeouts, and provide users with feedback regarding their status.

Hybrid Connectivity and Intelligence

When it comes to an AI-based layer of intelligence, there are many different layers. There is fraud detection occurring on devices, fraud detection occurring at edge nodes within networks, fraud detection occurring in regional data centers, and fraud detection occurring in central systems. This division of labor will depend on how much time some control takes to complete, how sensitive the data is, and what computing power is available at each level.

For example, the device-side models could perform 80-90% of normal transactions with local approval and then flag those that are high-risk for further review by edge nodes. Those edge nodes would perform a secondary validation on the escalated transactions and have their own fraud pattern database. Then the regional data center would gather the cross-

account patterns from the various accounts and use them for Anti-Money Laundering (AML) detection purposes. The central systems would then be responsible for updating policies, training models, and making the necessary regulatory reports.

Communication between the levels will adapt based on available bandwidth. For example, on 5G you may be able to transmit a rich context (the "fingerprint" of your device, your history of locations, your patterns of behavior) for extensive analysis. However, if you fall back to using a GSM or Satellite connection you would likely need to compress that down to the most essential signals (for example the amount of the transaction, the Merchant ID, etc.). This option would probably require users to be willing to sacrifice some accuracy in the form of accepting a slightly higher false positive rate for the sake of maintaining service.

Alignment with Digital Cash Principles

Physical cash operates offline, so it can be used by anyone with little concern about their level of technological expertise. In addition, because it does not require surveillance for low value transactions, it also offers individuals anonymity for those small exchanges of money. As long as the overall system remains secure, there is no need for individual surveillance. This has been the primary problem of creating a digital version of cash.

The connectivity stack (GSM + 5G + LEO), will provide universal access to users and ensure an operational continuity of service similar to that which exists with cash; the intelligence layer (AI), will protect against fraud that cannot be prevented by cash while preserving privacy through the use of AI on device processing and differential privacy.

Although transactions occur immediately at the point of transactional exchange with cash, they do not settle until later. The CBDC technology stack will mirror this process where immediate exchanges occur locally, and eventually synchronization occurs remotely.

2.7 Offline Transactions (Continuity Through Multi-Path Connectivity)

A major issue for offline digital currency has typically been defined as a two-state model; either you're connected, or you're not. There could be good reasons for this definition in the past when mobile networks were the only means of connectivity and there were many gaps in those networks. However, with the emergence of GSM, 5G, and LEO satellite-based connectivity models, defining what "offline" means needs to evolve. The focus of the architecture of future CBDCs should therefore be on developing communications redundancy and graceful degradation of communications across multiple layers of connectivity.

Offline-First to Always-On with Failover

Historical requirements for robust offline capabilities within CBDC design originated from valid concerns regarding availability of networks. As cellular coverage reliability continued to decrease in certain geographic areas, offline transaction capabilities were viewed as being necessary to enable users to use digital currencies in the same ubiquitous manner as cash. These historical requirements, however, came at great technical cost to CBDC development causing many limitations on the amount of money that could be transacted per session, longer timeframes for reconciliation, increased exposure to fraudulent activity due to lack of real-time validation, and greater complexity associated with conflict resolution processes.

The converged connectivity model presented in section 2 fundamentally alters the equation for making decisions based upon network availability. With GSM serving as a base layer of connectivity, 5G serving as a high-performance connectivity layer in urban environments, and LEO satellites serving as gap-fillers for coverage, the likelihood of a complete loss of communication decreases to almost zero in most cases. Therefore, users will no longer choose between "on-line" and "off-line" operating modes. Rather, the system will automatically route the user through the best available connection, degrade gracefully rather than fail completely.

Consider the practical realities of operation; even in previously considered "off-line" territories, LEO satellite-based connectivity currently provides at least a low-bandwidth channel to authenticate transactions. What was once a day-long off-line period requiring local storage of transactions now represents a lower-bandwidth communication channel in which transactions still successfully reach the central systems, at a potentially longer delay. The system does not go "off-line," it merely goes into a lower-tier communication mode.

While this does not eliminate the need for local transaction processing on user devices, it significantly changes its purpose. Rather than supporting extended off-line operation in days or weeks, local transaction processing will serve as a continuity mechanism for temporary communication disruptions in seconds or minutes. The secure element on user devices continues to manage transaction state and address short-term communication failures but expects periodic synchronization opportunities via the multi-path connectivity infrastructure.

From Replicating Cash to Designing Resilient Digital Infrastructure

Cash functions as an off-line digital currency because it is a physical bearer instrument. Physical possession equals ownership, and physical exchange completes the atomic

transaction. Past designs of CBDCs have sought to replicate this feature digitally using various cryptographic guarantees (e.g., zero-knowledge proofs, blind signatures) or trusted hardware that prevents double-spending, even without network connectivity.

Although the technical aspects of these designs continue to be valid, their justification has changed in a multi-path connectivity environment. Rather than enabling days of disconnected operation, these features now provide resilience in the event of network transition and/or brief outage. The role of the secure element is evolving from autonomous transaction processing to managing state during network failure.

When a user initiates a transaction, the system does not ask "are we on-line or off-line?" Instead, it evaluates the options for available connectivity. The user experience remains unchanged in both scenarios; the transaction is completed. The variable factor in both cases is the path taken by the transaction and the potential delay in the completion of the transaction, whether or not the transaction is successful.

Traditional off-line models defined synchronization as an exceptional event to the point at which a disconnected device re-connected and synchronized its locally stored transaction history with the central systems. This posed significant technical challenges Merkle tree exchanges to determine which records were divergent, conflict resolution protocols, fraud detection on bulk transaction uploads.

The redundant connectivity model defines synchronization as a continuous, incremental process. Devices are always in near-continuous communication with central systems via some path, thus facilitating transaction-by-transaction validation instead of batch reconciliation. Individual transactions can be validated in real-time on LEO satellite connections with limited bandwidth, rather than queuing them for later processing. When a user experiences a network transition i.e., moves from 5G coverage to GSM-only, the system does not "go off-line" and create a backlog of reconciliation activities to perform. Instead, it merely transitions transport layers while continuing to utilize the same transaction validation workflow. The secure element's transaction buffer is designed to smooth out the microseconds or seconds required for a network hand-off, not to enable hours or days of autonomous operation.

Always Connected Architecture Fraud Risk Management

One of the primary arguments for traditional off-line capability was disaster scenarios e.g., earthquakes, hurricanes, conflicts, etc. in which terrestrial infrastructure would be destroyed. In such disaster scenarios, LEO satellite-based connectivity will be the key difference-maker. Even in the event of destruction of all cell towers in a given area, direct-to-cell satellite-based connectivity maintains a validation channel to central systems.

While LEO satellites have eliminated some need for offline capability, there still exist edge cases where satellite connectivity itself may fail (underground locations, extreme atmospheric interference). In such cases, some limited local transaction buffering will still be required. However, we are now designing for minutes of autonomous operation, not days and so the security and reconciliation needs will also change.

The Road Ahead: Achieving Resiliency Through Redundancy

We are not abandoning the reasons that motivated the development of offline capabilities universal access, resiliency in the face of catastrophes, independence from any individual piece of the underlying communication infrastructure. We are merely using a new method to achieve intelligent fail-over across multiple paths of connectivity, rather than independent local operation.

With GSM covering approximately 96% of the world's population, with 5G continuing to expand in urban centers, and with LEO satellite constellations capable of providing direct-to-cell connectivity, the technological foundations for always connected architectures are becoming increasingly viable. Therefore, CBDC systems will have the opportunity to move away from developing for offline capabilities and toward developing for redundant connectivity, thereby enhancing both user experience and security, while at the same time simplifying operational paradigms while maintaining the resiliency that offline capabilities were intended to provide.

No longer will the question be "for how long the system can operate in an offline mode?"; instead, the question will be "how many separate channels of connectivity will the system be able to use to continue to offer services?" This represents the maturation of telecommunication infrastructure, allowing for true universal connectivity, and not just universal offline capability as the basis for the digital currencies that are truly resilient.

2.8 Post-Quantum Proof CBDC

Quantum computers are expected to eventually be able to break nearly all public key encryption methods in the next 10-15 years, and then the industry will have time to migrate during this duration. Therefore, if it is important to build the infrastructure for CBDC today that could be easily migrated when this threat appears.

The Quantum Threat Landscape

Quantum Computers utilize quantum mechanics (superposition and entanglement) to perform certain computational tasks at an exponential rate over classical computers.

The specific threat related to cryptography is Shor's Algorithm that can be used to quickly factorize large numbers and compute discrete logarithms with sufficient qubits on a

quantum computer. As a result, Shor's Algorithm will compromise virtually all forms of public key encryption currently being used in digital applications, including RSA and ECC as well as Diffie-Hellman Key Exchanges.

However, symmetric encryption (AES) appears to be somewhat less susceptible to being broken by quantum computers. Grover's algorithm offers a quadratic speed-up for brute force attacks on symmetric encryption so if you double the length of your symmetric encryption keys then the time to crack the code will increase quadratically. For example, AES-256 is still secure against current quantum computers while AES-128 will be equivalent in security to AES-64 and therefore possibly vulnerable to attack. Therefore, increasing key sizes should be an acceptable solution to the problem of protecting symmetrically encrypted CBDCs.

It is difficult to estimate when large-scale practical quantum computers will appear. Some of the most optimistic estimates indicate that we should see practical quantum computers able to factor 2048-bit RSA by approximately 2030-35. More conservative estimates would place the availability of such devices at least into the mid-2040s [15]. However, one of the "harvest now, decrypt later" threats to CBDCs is that an adversary could obtain encrypted CBDC communications today and decrypt them once sufficient quantum computing power exists. As a result, this is likely to be a serious issue with respect to long-lived confidential information.

Currently, quantum computers contain approximately 100-1,000 stable qubits. It is estimated that a practical quantum computer (which can factor 2048-bit RSA) would require about 4,000 – 8,000 logical qubits [16]. Since each logical qubit will typically correspond from tens-of-thousands to hundreds-of-thousands of physical qubits due to the necessity of implementing error correction, we are far from achieving this level of capability. Nevertheless, the companies involved in developing these technologies (IBM, Google, IonQ) are making rapid progress toward developing larger and more reliable systems. While the engineering hurdles to develop such technology are considerable, there does not appear to be any significant physical barrier to eventually developing a quantum computer with the capabilities described above.

Post-Quantum Cryptography for CBDC

Post-quantum cryptography (PQC) relies on mathematical problems that will remain hard for quantum computers. In 2024, NIST completed the process of standardizing post-quantum cryptographic protocols by selecting a number of algorithms for various applications [17,18]:

- **CRYSTALS-Kyber** is a key encapsulation algorithm (for establishing a shared secret) based on the Module Learning with Errors problem.
- **CRYSTALS-Dilithium** is a digital signature algorithm, like Kyber it is based on the Module Learning with Errors problem but provides stronger security assurances.
- **FALCON** is an alternate signature algorithm which produces smaller signatures than Dilithium (it is based on NTRU lattices).
- **SPHINCS+** is a hash-based signature algorithm intended to serve as a conservative fallback (large signatures).

As far as CBDC is concerned, there are two primary concerns: signatures (validating transactions) and key establishment (protecting your channel of communication). Both Dilithium and FALCON can provide signature capabilities, but each has its own trade-off.

Dilithium's signature sizes are larger (2-4KB vs 700 bytes for FALCON), but Dilithium is capable of faster verification. The size of the signature does matter when dealing with large amounts of transactions and limited bandwidth (some users may be using GSM or LEO networks).

A main challenge of PQC is the increase in computation time from public key cryptography methods used today. The time to verify signatures for Dilithium will likely be approximately 0.5-1 ms whereas elliptic curve cryptographic signatures can be verified at a rate of about 0.1 ms [19]. Therefore, while signature verification via Dilithium is feasible for server-side validation, the potential delay could become problematic when validating large numbers of transactions per second on low resource mobile devices.

To ensure PQC will be viable on future feature phones, it will likely require dramatic reductions in execution time or use of some kind of hardware acceleration. Implementation libraries for PQC are being developed. liboqs (Open Quantum Safe) currently has C code implementations of the five NIST finalist PQC algorithms. PQClean is a project providing validated and constant time implementations of the algorithms to protect against side channel attacks.

Hybrid and Migration Strategies

Migration towards PQC needs to be implemented gradually and reversibly. A one-time direct switch on the deployment of new quantum resistant algorithms will result in all your existing devices and systems being incompatible. Hybrid Cryptography is the standard method used to implement both Classical and PQC algorithms in parallel to provide security as long as at least one of the two is still secure.

Hybrid schemes could also be implemented for CBDC signatures by concatenating an ECC signature with a Dilithium signature. To validate a transaction, both signatures must be

validated. The benefits of hybrid schemes are that they protect users against Quantum Computers (due to Dilithium's resistance to quantum attacks) but maintain backwards compatibility for systems that only understand ECC. The drawback is the overhead of the additional space required to store the concatenated signatures; roughly 2.5 KB instead of 64 bytes for pure ECC signatures.

Hybrid Key Exchange Schemes can also be implemented for key establishments Both parties would first perform a classical Diffie-Hellman and Kyber key exchange and then combine their resulting keys to establish a shared secret. As long as one of the key exchanges is performed securely, the other can still provide security if one of the algorithms is broken. The cost associated with hybrid key exchange schemes is performance; approximately 2-3 times slower than classical-only key exchange schemes. However, this is the only responsible way to design and deploy cryptographic infrastructure intended to operate for decades.

Cryptographic Agility and Protocol Versioning

One of the results of quantum computing roadmap is the necessity of developing agile cryptography. In other words, developing systems capable of changing one or more of their cryptographic components while maintaining minimal redesigns of the system itself. That’s the reason CBDC protocols should include a version identifier of the cryptographic algorithms currently in use to allow for the incremental transition to new algorithms as they become available, or older ones are removed from use.

This isn’t simply an issue of quantum-resistant cryptography. Cryptographic breaks occur unpredictably; MD5 was considered secure until it cracked. SHA-1 remained in use for many years after known weaknesses were identified. If the CBDC architecture has a rigidly defined cryptographic component e.g., using fixed, hard-coded versions of algorithms with no provision for upgrading, it will be very costly to emergency migrations when vulnerabilities in those algorithms are identified.

The general engineering approach to this problem is a form of protocol negotiation. In particular, the approach used by the Transport Layer Security (TLS) protocol for negotiating versions is instructive. As described in [TLS], wallet software and back-end servers indicate the set of cryptographic suites they support, and then select the strongest mutually supported suite. Older devices may only support classical cryptographic primitives; newer devices will support hybrid schemes (i.e., classical and quantum); and future devices will likely eventually cease to support classical cryptographic primitives altogether at some point after the danger of the quantum threat has been realized.

Doing version rollovers properly requires careful planning. When it is decided to remove old cryptographic algorithms from use, enough advanced warning needs to be provided with

users' time to update their devices. For example, "Classical-only signatures will no longer work in 24 months; hybrid support will be required in 18 months; pure PQC will be available in 12 months." This will give users time to migrate to compliant devices and will allow a smooth transition.

Testing and Validation

The extensive testing of PQC will be needed before it is used in production CBDC systems. These tests will include:

- correctness testing (will the algorithm generate a valid signature).
- performance testing to evaluate the speed of the algorithm under actual workload conditions.
- security evaluations to ensure that there is no vulnerability to side channel attacks introduced into the implementation of the algorithm.
- inter-operability testing to determine if all platforms and devices support the use of PQC.

Before deploying PQC in production of CBDC systems, central banks can create PQC test beds where pilot implementations of PQC could be tested and evaluated prior to their deployment into production. For example, central banks could issue test CBDC's using PQC algorithms to limit numbers of people and monitor the performance characteristics of the test implementations. After confidence in the implementation is established, the number of users can then be increased over time.

3. CBDC Infrastructure Outlook

3.1 Building the Next Generation Monetary Infrastructure

Central Bank Digital Currencies (CBDCs) cannot be developed as individual projects, but rather as a multi-generational transformation of the monetary infrastructure of the world. The key technical decisions made about the form of connectivity, intelligence, governance, and cryptography made in the development of CBDCs will have significant implications for how the global monetary system is structured by the 2030s and 2040s.

This report suggests that CBDCs must be co-designed with the communications and intelligence stack that supports them. In the longer term, the ultimate vision for CBDC is for it to become an evolved digital public infrastructure; to become a sovereign, resilient, interoperable, and evolvable digital public infrastructure that is supported by a converged network of intelligent operational layers.

The telecommunications roadmap over the next decade will directly determine the capacity of CBDCs to operate effectively:

- By the late 2020s, 5G will have expanded mostly to urban and peri-urban areas, providing ultra-reliable, low-latency communication, edge computing, and network slicing. These capabilities will provide increasing support to mission-critical payment applications and IoT based micropayment systems.
- The 6G research initiative has already identified native AI integration, post quantum security, and seamless terrestrial-satellite convergence as critical features for its development. This further reinforces the need for the design of modular CBDC protocols that can evolve without changing monetary logic.
- The LEO satellite constellation will reach maturity and diversification (regional, sovereign), eliminating the concept of "no coverage" for direct-to-cell connectivity and allowing for continued monetary activity in remote locations, disaster zones, and during times of conflict.

The strategic messaging for central banks is not to rely on single access technology for their CBDCs. Instead, central banks must architect their CBDCs to be transport independent and to route transactions across GSM, 4G/5G and satellite links with consistent security and settlement rules.

In the future, telecommunications companies will not only be vendors of connectivity services, but they will also be infrastructure partners providing guaranteed quality of service, priority slices for monetary transactions and reliable fallback channels. However,

they must be careful to remain only partners for connectivity and not create intermediaries for money creation or control. Monetary sovereignty must remain solely within the purview of the central bank.

3.2 Resilience, Autonomy, and Trust

There are reasons why physical cash has lasted so long and will likely continue to last for a considerable amount of time. First and foremost, it has been "resilient" and "predictable". To meet this same benchmark as digital sovereign money, the resilience of digital sovereign money will need to be measured by its ability to function over the next 20 years at an acceptable level, even if the digital sovereign money is operating at full capacity with no room for further growth (i.e. "peak congestion"), regardless of whether or not there is some type of systemic degradation; to have enough functionality to allow for the continued use of the digital sovereign money during times of infrastructure outages; to withstand cyber threats and the ever-evolving threats related to cryptography; and to provide a means to maintain continuity of use during times of geopolitical unrest..

The addition of terrestrial networks and Low Earth Orbit (LEO) satellites fundamentally changes the way we view resilience and creates a multi-layered, geographically diverse digital sovereign money system that can experience graceful degradation and therefore will never suffer from catastrophic failure.

Autonomy is also key to ensuring that digital sovereign money is viable and sustainable. With multiple satellite systems available (e.g. U.S., Europe, Asia, regional), central banks will need to develop multi-provider strategies to ensure the sustainability of their digital sovereign money systems; develop cryptographic protocols that provide end-to-end encryption; and develop contingency plans in the event of system failures. Sovereignty does not preclude the need for collaboration with other entities; however, sovereignty does require that central banks make specific design decisions to ensure that external infrastructure providers do not become a source of potential systemic risk. Trust is another critical component. A CBDC that provides users with adequate protection, while providing adequate protection of the system will create a basis for building durable public trust and credibility.

To achieve the above three components, digital sovereign money will need to provide:

- Proportionate privacy protections and technically enforce them.
- Evolve security measures to protect against future threats including quantum computing and AI enabled threats

- Provide adequate assurances regarding the predictable behavior of the system under stress
- Establish and communicate clearly defined governance boundaries

3.3 Systemic Monitoring and Stabilization Layer

As transactions increase, Artificial Intelligence (AI) is likely to become a key element of both fraud detection on an individual basis and the larger picture, or overall level, of fraud and anomaly detection. Long-term use of AI analytics can provide:

- Real-time monitoring of the flow of funds throughout the system
- Systemic fraud and network anomaly detection
- Early warning systems for potential financial distress
- Improved effectiveness of Anti-Money Laundering (AML) activities while also decreasing the regulatory burden

It is important that these AI-based capabilities are governed by strict and transparent policies to maintain their legitimacy as a tool for enhancing public and private sector policy insight and operational efficiencies, and not as an invasive tool for behaviorally monitoring individuals. To achieve this, privacy preserving technologies, model transparency, and some form of government or supervisory oversight will be required to preserve the legitimacy of AI based tools.

3.4 CBDC as National Digital Public Infrastructure

To be treated as national digital public infrastructure (DPI), CBDC would need to be viewed as more than just a payment solution; instead, it needs to be treated as an integral part of digital public infrastructure (DPI). DPI is composed of at least three layers, Digital Identity, Data Exchange Layers and Secure Communications Networks. As such, DPI has four primary objectives for its role in facilitating inclusive economic participation:

- To serve as a settlement anchor for private innovation,
- To provide a stable base for programmable services,
- To strengthen the domestic monetary policy transmission channel,
- To enable users to participate in the economy using their digital identity.

Therefore, the integrated GSM + 5G + LEO + AI stack described in this report aligns with this vision. In this model, the monetary core remains stable and sovereign and continues to provide a foundation upon which other evolving layers are built. Separation of the monetary

core from the connectivity and intelligence layers ensures that continuity of service can continue over the long term, regardless of technological changes.

Treating CBDC as DPI reframes public-private cooperation for infrastructure development. Telecom operators, cloud providers, fintech companies, and hardware developers support the development of the infrastructure while the central bank retains all rights as the issuer, governor, and policy authority. However, infrastructure partnerships cannot be allowed to result in the delegation of the monetary core.

Fragmented deployment of CBDC pilots could result in "parallel silos" being created if these pilots lack realistic connectivity and lack an approach to design for interoperability. Fragmented deployments also increase the cost of deploying CBDC and erode confidence in the system. There is a fundamental distinction between the concepts of "leapfrogging" and "fragmentation." Leapfrogging refers to developing new architecture for an entire sector or country based on current state-of-the-art technology. Fragmentation refers to creating many separate systems each designed for a specific use case. Countries that view CBDC as digital public infrastructure with well-defined modularity and standards will generate compounding benefits. Countries that develop short-term experimental approaches to implementing CBDC without developing a long-term roadmap for implementation will likely produce technical dead-ends.

3.5 Toward a Global, Interoperable, and Resilient Payment Fabric

Soon it's likely that central bank issued digital currencies (CBDCs) will be connected as part of a global network of interoperable sovereign systems. To achieve interoperability between these systems will require:

- Standardized Application Programming Interface (API) and messaging formats.
- Transaction protocol is independent of transport mechanism.
- Shared security standards, including transition to post-quantum encryption methods.
- Cross-border compliance frameworks that use risk-based approaches.

As terrestrial and satellite connectivity become more ubiquitous and interconnected, digital currencies can communicate and interact with each other more effectively. An ideal future payment infrastructure may enable seamless interoperability among sovereign CBDCs while still allowing for sovereignty and control of monetary policy by individual nations. This type of payment infrastructure will remove or decrease settlement costs, increase transparency, and improve overall financial stability at a regional level.

3.6 Alignment with Inclusion, Competition, and Innovation

A well-designed CBDC ecosystem should promote competition and innovation, not hinder it. A sovereign, neutral, settlement layer provides a trusted base for fintech companies to build upon, telecom providers to expand their reach without becoming financial gatekeepers, small institutions to compete on service offerings versus proprietary payment rail solutions and ultimately provide consumers with greater access to secure digital money. The inclusion of phones, smartphones, satellite backup, and adaptive security within one unified framework will increase inclusion. Increased competition through interoperability will prevent monopolistic lock-in. Stable and programmable monetary foundations will accelerate innovation.

.

4. Adoption Beyond CBDC Infrastructure

The purpose of this chapter is to propose an implementation strategy for the adoption of CBDC, which can complement the connection intelligence stack previously identified (i.e., GSM/5G/LEO + AI) and assist central banks in moving from pilot projects to the nationwide use of CBDC without disrupting the current structure of their payment systems.

4.1 Merchant Acceptance: Incentivizing and Phasing in Merchant Acceptance

Merchant acceptance represents the tipping point for the retail CBDC. Even though citizens can download wallets and store value within those wallets, they will not retain that stored value unless they have convenient ways to spend it. Therefore, a CBDC strategy must view merchant acceptance as a "distribution network" issue like the way that cash acceptance infrastructure is viewed, but instead as digital.

Incentive Toolkit for Merchants

Policymakers can encourage the early acceptance of CBDC among merchants without altering market conditions by providing temporary incentives and structural advantages. The most direct leverage for encouraging acceptance among merchants is through controlling the costs associated with accepting CBDC – capping or subsidizing CBDC acceptance fees for merchants during the rollout period, particularly for micro-merchants. Additionally, if CBDC is framed as a public infrastructure, there should be no additional cost to merchants for accepting CBDC compared to the lower cost digital rails already available to them today.

There are also other merchant-focused operational advantages that central banks can emphasize. Merchants benefit from faster settlement and immediate finality resulting in reduced working capital pressures and decreased credit risks. Merchants currently waiting for days for card payments to settle will see immediate, irrevocable CBDC settlement as an attractive option — an important enhancement in managing cash flow that will particularly benefit smaller merchants with very tight profit margins.

Tax and compliance simplification also presents an incentive vector. Policymakers can offer optional tools that reduce the administrative burdens associated with complying with regulations, such as automated receipts, and streamlined reporting dashboards that will help to encourage merchants to adopt CBDC while avoiding the creation of mandatory surveillance tools. The key will be to maintain clear governance boundaries, so that the convenience features do not evolve into all-encompassing transaction monitoring tools.

The physical equipment needed to achieve CBDC acceptance matters significantly to achieving rapid adoption. Lower-cost acceptance models that require less equipment will reduce friction, allowing merchants to accept CBDC through existing devices, including smartphones such as POS terminals, QR Codes, NFC, or even USSD on feature phones for informal merchants. The connectivity stack is also critical at this juncture, acceptance must operate reliably when experiencing network congestion and in low-connectivity zones, or merchants in areas where CBDC could provide the most value will not adopt it.

Sequencing: Build Density prior to Breadth

Another common mistake made by policymakers is attempting to go "national" prior to achieving significant density within a particular region. A preferable approach is a staged approach to scaling that places emphasis on building density rather than breadth. First, implement closed-loop controlled pilots in small geographic regions to test and validate system up-time, fraud control processes, and workflows supporting the use of CBDC. Next, focus on developing high-frequency merchant corridors (markets, transit, gas stations, grocery stores) where users transact daily. The high frequency of transactions in these locations enables users to develop habitual usage patterns.

Following the development of high frequency merchant corridors, add anchor merchant networks into the ecosystem (large retail chains and utility providers) that immediately increase spend utility across broad geographic regions. A relatively small number of large merchant nodes can provide widespread acceptance of CBDC, even prior to having a comprehensive level of coverage throughout a nation. Finally, expand into the long tail of SMEs and informal commerce. At this time, consumer demand will begin to create organic merchant adoption pressure.

By implementing this phased approach, a practical "spend surface" will develop rapidly, which is what develops habitual usage. Consumers need to understand that they can spend CBDC wherever they typically conduct transactions, not simply that acceptance of CBDC technically exists somewhere in the economy.

4.2 Public-Sector Use Cases: Fastest Adoption Accelerators

In many countries, the government is the single largest and most reliable source of transaction volume due to its large number of recurring payments. When used correctly, it can increase adoption rates while meeting the public policy objectives of CBDCs.

Government to Person High Impact Areas

Social welfare and support programs such as cash assistance, food aid, energy assistance, etc., offer ideal starting points. In addition to reducing leakage and accelerating the

distribution process, social welfare and support programs provide the perfect opportunity for delivering financial assistance to the underserved population that CBDCs aim to serve. When combined with the use of GSM and feature phones and resilient connectivity, CBDCs will be able to deliver government support more efficiently than current systems, providing access to people who do not have a bank account or a smartphone.

Using public payroll to fund certain types of employees provides predictable patterns of circulation, while also maintaining relatively stable levels of money in wallets. Emergency disaster-related distributions exemplify the unique capabilities of CBDCs. The LEO satellite and terrestrial network hybrid become the critical infrastructure when natural disasters damage traditional communication systems. As such, CBDCs act as a continuation channel of payment capabilities when the local communication system collapses.

Public procurement micropayments to small businesses to pay for goods and services paid for through CBDCs, reduces the cycle time of payment from weeks or months to hours or days. This will improve the liquidity of small businesses and encourage them to continue participating in the formal sector of commerce.

In addition to increasing the adoption rate of government-to-person payments, increased government acceptance drives the rate of adoption. Mandatory payments made to the government (taxes, permits, licenses) create the same level of utility and drive the creation of wallet adoption prior to merchants achieving the critical mass of transactions required to create the critical density of merchant coverage.

In addition to utilities, municipal services such as water, electricity, trash collection, etc., create routine usage of CBDCs. Similar to utilities, transit and transportation services should receive equal consideration since they offer both high transaction frequency and broad demographics. Commuters make numerous small transactions that increase the likelihood of creating habituated usage.

By combining government payments to citizens with their ability to spend CBDCs on essential items, citizens develop confidence and demonstrate the value proposition of CBDCs prior to achieving comprehensive merchant coverage.

4.3 Interoperability with Existing Rails: avoiding ecosystem locks

A large portion of the reason for potential fragility in the adoption of Central Bank Digital Currencies (CBDC) is because they are intended to replace, rather than supplement existing payment systems. Banks, Payment Service Providers (PSPs), merchants and many others have significant investments in the technology and operational structure of current payment systems. As a result, when attempting to supplant these ecosystems through the

introduction of a new system (the CBDC), there exists a natural barrier to entry for the new system, which may slow or even prevent its adoption, regardless of the merits of the technology itself. Therefore, CBDC should be implemented as an additional payment system, as a settlement layer, and one that works in conjunction with the current payment system architecture but does not replace it.

Principles of Interoperability

Coexist by default: CBDC is initially launched as a complementary alternative to cash and existing forms of digital payment. Thus, users will be able to maintain both CBDC and traditional bank deposits. Merchants will be able to continue to accept card, ACH/RT transactions, and cash while also accepting CBDC. The overall payment ecosystem will expand and become less fragmented.

Provide multiple access channels: Ensures competition and innovation will continue. Regulated entities such as banks, PSPs, Telcos, etc. will all be able to offer a wallet or user interface under a uniform regulatory framework. This will ensure that no single entity controls CBDC and ensures all access channels adhere to minimum standards of security and interoperability.

Standardized Integration provides technical foundation: Standardized messaging protocols and API layers are the technical basis upon which domestic interoperability will occur among various wallet providers and payment channels. In addition, cross-border interoperability can be built out incrementally as an expansion of domestic systems prior to developing international systems.

Interoperability can begin with simple features and grow over time: The initial phase of integration may include basic features such as cash-in/cash-out flows, bank transfer and merchant acquiring links. More complex features such as programmable payments can be added at a future date once the fundamental features of interoperability have been established. By enabling interoperability in a staged manner, the burden of integrating new systems will be reduced while providing opportunities for more advanced features to be incorporated into future versions.

4.4 CBDC Success Metrics: what central banks should measure

Historically, traditional payment systems were measured using transaction volume metrics. However, CBDC programs are intended to serve public policy purposes and therefore require broader and different metric-based frameworks. So, a CBDC program should establish an appropriate, balanced scorecard based on following key areas:

Availability and Resilience

Availability and resilience of a CBDC program should be established through Service Level Agreements (SLAs) targeting availability at cash-equivalent levels, overall availability of 99.9% or higher, with additional SLA targets for critical channels (e.g., core ledger, wallet services, offline continuity). The ability of a CBDC program to complete transactions during times of high demand (congestion) will indicate if the system can handle high volumes of activity. This includes lunch hours, end-of-day settlements, and mass transit rush-hour periods. Stress testing a CBDC system's architecture simulates disasters such as loss of internet access (disaster scenario) and tests if the multi-path connectivity architecture has enough redundancy to support continued operation of the system when all terrestrial networks fail.

The ability of a system to gracefully degrade will measure how well the system continues to operate at a minimum level of service when there is failure of a network. For example, when a 5G network fails, can the system automatically switch to 4G and/or GSM? If all terrestrial networks fail, will LEO satellite links continue to allow for some form of basic transaction capability? Each of these degradation paths requires specific performance targets.

Inclusion and Reach

Active usage of a CBDC program by demographic segments will help determine if a CBDC program has achieved its financial inclusion goals. The metrics tracking active use of a CBDC program by demographic segments should include regular use by the underserved (rural users, low-income groups, feature phone users), not just download statistics. Time and cost associated with onboarding will also determine the ease of entry into the system. Coverage of usable CBDC geographically will distinguish between network coverage and practical utility where transactions can be completed reliably is much more important than where transactions could potentially be completed.

Merchant Acceptance and Usability

Density of merchant acceptance in designated deployment zones will determine if merchant coverage is creating actual spending opportunities. Frequency of repeat usage per user and per merchant will indicate if habits are being formed. Time-to-pay at point of sale under various levels of connectivity will determine if the system provides reasonable user experience across the full range of network performance (i.e., transaction latency on GSM connections is much more important than ideal performance on 5G).

Integrity, Fraud and Compliance Efficiency

Loss rates due to fraud compared to other forms of payment (existing payment rails) will provide objective measures of the effectiveness of a system's security. False positive rates will strike a balance between security and usability (overly aggressive fraud controls that block legitimate transactions will frustrate the user). Workload per million transactions required to investigate false positives will demonstrate if AI-powered controls have reduced compliance costs or simply allow for greater surveillance capabilities.

Where AI is employed, Model Governance Key Performance Indicators (KPIs) become relevant. Time to detect model drift will measure how quickly degrading model performance is detected. Retraining frequency will determine if models remain current with changing fraud patterns. Audit pass rates will determine if model governance is maintaining adequate standards.

Financial Stability and Ecosystem Health

Indicators of disintermediation will monitor changes in commercial bank deposit behavior and funding pressures. By monitoring deposit flow, changes in deposit pricing and changes in bank funding costs, you can determine if usage caps and design features of a CBDC system have successfully prevented disintermediate related risks. Participation of intermediaries (regulated entities offering wallets and payment services) will measure the diversity and health of the CBDC service provider ecosystem. The number of regulated entities offering wallets and payment services will indicate if the system supports true competition.

CBDC will be viewed as trusted public money when it is useful every day, operates under extreme pressure and fits into the existing economic environment without disrupting it. The strategic implementation plan for a CBDC program must be developed with the same level of seriousness as the development of technical architecture. Creating merchant acceptance through targeted incentives and density-first rollouts will create spending utility. Utilizing government-to-person payments and public sector acceptance as initial circulation anchor points will create baseline transaction flows. Ensuring that a CBDC system is interoperable will protect the ecosystem and preserve competition.

Establishing clear, publicly-interest focused success metrics for measuring progress toward achieving policy objectives will ensure that focus remains on meeting the objectives of the policy (as opposed to the growth of the number of transactions). When combined with the integrated infrastructure described above (reach via GSM, performance via 5G, continuity via LEO satellites, and risk management via AI), this adoption framework presents a practical pathway from pilot capability to nationally accepted legitimacy.

5. Final Perspective: A Strategic Choice for Central Banks

The long-term CBDC vision is not to replace cash; it is not to compete with private payment service providers. Rather, the vision is to preserve the place of public money in an increasingly digital, networked, intelligent economy.

Whether or not public institutions take leadership in the evolving monetary system, the system is changing. Foreign infrastructures, non-sovereign digital assets, and private platforms are changing how people pay and where liquidity flows. In this environment, doing nothing is a choice. The question is no longer whether money will become digital—it already has. The real question is whether public money will remain structurally relevant in that transition.

This report shows that there are no longer significant technological barriers to implementing national scale CBDC. Ubiquitous mobile networks, emerging satellite capabilities, edge computing, adaptive AI, and advanced cryptographic standards have made most operational possibilities feasible.

But feasibility alone does not create legitimacy.

Now, central banks have a strategic obligation: to define the architectural framework, governance structures, resilience requirements and the public interest goals for digital money systems prior to when those systems become structurally reliant on external infrastructures outside of their control.

Connectivity has become a form of monetary infrastructure.
Intelligence has become a form of monetary security.
Resilience has become a form of monetary credibility.

If the components of the digital money ecosystem are allowed to exist as a collection of commercial interests and foreign dependencies then over time, monetary sovereignty will decline, not through crisis, but through gradual irrelevance.

Alternatively, if CBDC is seen as national digital public infrastructure (modular, interoperable, private conscious, and technologically adaptive), then it can:

- Reinforce financial stability rather than threaten it.
- Expand access while maintaining trust.
- Enable innovation without ceding control.
- Improve the transmission of monetary policy in a digital economy.

Therefore, the strategic decision facing policymakers is not "whether to try" an experiment. It is to determine the structural parameters of the next monetary era.

Short-term pilots can provide insights.
Long-term architecture determines outcomes.

Those central banks which take a structured, principle-based approach to defining the infrastructure necessary to support a new monetary order (one based upon resilience, interoperability, and adaptive security) will develop a monetary foundation that supports the ability of governments to engage in economic activity, maintain public confidence and maintain sovereign autonomy into the 2040's and beyond..

The opportunity and challenge are not technological.
They are institutional.

The time to develop that foundation is now.

References

[1] GSMA (2025). The State of Mobile Internet Connectivity 2025. GSM Association.

https://www.gsma.com/somic/wp-content/uploads/2025/09/The-State-of-Mobile-Internet-Connectivity-2025-Overview-Report.pdf

[2] ITU-R (2020). IMT-2020 (5G) Standards and Specifications. International Telecommunication Union.

Technical Specification Group Radio Access Network; Study on Scenarios and Requirements for Next Generation Access Technologies. 3GPP TR 38.913 v14.3.0. https://cdn.standards.iteh.ai/samples/53597/81b8dcb0334740bd8f229abc3b0eb3b1/ETSI-TR-138-913-V14-3-0-2017-10-.pdf

[3] 3GPP (2018). Technical Specification Group Radio Access Network; Study on Scenarios and Requirements for Next Generation Access Technologies. 3GPP TR 38.913 v14.3.0.

https://www.3gpp.org/specifications/releases

[4]European Commission – *Europe's 5G strategy towards the Digital Decade*
https://digital-strategy.ec.europa.eu/en/policies/5g-digital-decade

[5] **Ericsson blog on 6G specifications & commercialization timeline**
https://www.ericsson.com/en/blog/2025/6/blog-6g-standardization-technology-step-to-publish

Ericsson 6G timeline overview
https://www.ericsson.com/en/6g

[6] White Paper on Broadband Connectivity in 6G (6G Flagship / University of Oulu)

https://oulurepo.oulu.fi/bitstream/handle/10024/36799/isbn978-952-62-2679-8.pdf

[7] SpaceX Starlink Public Performance Data (2024); OneWeb Public Documentation (2024).

[8] Global Satellite Broadband Performance Report (https://www.benton.org/headlines/2025-global-satellite-broadband-performance-report)

[9] Communications Today Article: https://www.communicationstoday.co.in/att-users-show-interest-in-t-mobiles-starlink-satellite-service

[10] https://www.ultimahora.es/noticias/tecnologia-videojuegos/2026/01/13/2548615/starlink-confirma-servicio-cobertura-movil-satelital-direct-cell-estara-disponible-espana-proximamente.html

[11] https://www.eutelsat.com/satellite-network/oneweb-leo-constellation

[12] IRIS^2 EU satellite constellation (Wikipedia) https://en.wikipedia.org/wiki/IRIS%C2%B2

[13] Guowang Chinese megaconstellation plans (Wikipedia) https://en.wikipedia.org/wiki/Guowang

[14] India mulling LEO broadband constellation (Economic Times / PTI) https://telecom.economictimes.indiatimes.com/news/portal-in-portal/satcom/india-plans-own-low-earth-orbit-satellite-constellation-for-broadband-services/123464759

[15] NIST / PQC migration guidance https://www.nist.gov/publications/migration-post-quantum-cryptography

[16] ETSI Quantum Safe Whitepaper https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[17] NIST (2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. National Institute of Standards and Technology. Press Release, August 13, 2024.

https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[18] NIST (2024). Post-Quantum Cryptography Standardization. NIST Computer Security Resource Center.

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

[19] Masood, A. (2024). Federal Transition to Post-Quantum Cryptography https://medium.com/@abumasood/federal-transition-to-post-quantum-cryptography