The Bretton Woods Committee

OCTOBER 2026

WORKING GROUP MEMBERS

Axel Weber
President,
Center for Financial Studies

Frannie Léautier
Chief Executive Officer,
SouthBridge Investments

Harold James
Professor of History and International Affairs, Princeton University

Joaquim Levy, Co-Chair
Director for Economic Strategy and Market Relations, Banco Safra SA

Keiko Honda
Professor,
WASEDA Business School

Luis Alberto Moreno
Former President, Inter-American Development Bank

Min Zhu
Vice Chairman, China Center for International Economic Exchanges

Minouche Shafik
Former Chief Economic Advisor to the UK Prime Minister

Ngaire Woods
Founding Dean, Blavatnik School of Government; Professor of Global Economic Governance, Oxford University

Robert Kopech
Adjunct Professor, Columbia University School of International and Public Affairs

Siddharth Tiwari, Co-Chair and Lead Author
Associate Fellow, Chatham House, London

Sopnendu Mohanty
Group Chief Executive Officer, Global Finance & Technology Network

Stefan Ingves
Chair,
Toronto Centre

Vera Songwe
Chair and Founder, The Liquidity and Sustainability Facility

Governing Digital Infrastructure: Gaps and a Framework for Growth

A Publication from the Bretton Woods Committee's Multilateral Reform Working Group

Executive Summary

Digital infrastructure is now an instrument of sovereign power. Internally, countries that build it govern better and deliver benefits to citizens faster. Externally, they shape who participates in the digital economy and on what terms. Countries that don't build it cede that power to others.

This paper builds on the premise that building digital infrastructure is not a technical upgrade but rather a policy choice about who controls the rules, and whose rules other countries end up living under. Departing from the traditional multilateral playbook where trends move from advanced economies to developing countries, the paper draws upon a few powerful examples of digital infrastructure innovations from emerging market countries that have been proven at scale.[1]

In a world of stretched public finances and impatient populations, digital infrastructure has repeatedly proven transformative and nearly free, letting countries leapfrog decades of development at a fraction of the cost and time of traditional infrastructure. It has also helped early movers, especially emerging markets, accrue first-mover advantages. For example, India compressed 47 years of progress on financial inclusion into 8 years.

Yet most countries remain stuck building expensive, custom, one-off systems. Years and tens of millions of dollars are spent before a pilot even begins. Much as software as a service transformed how companies deploy software, digital infrastructure as a service (DaaS) is transforming how countries deploy infrastructure: as pre-packaged, cloud-based building blocks that can resolve the financial and capacity constraints that currently lock out 100 smaller countries (disproportionately in Africa).

1. Previous parts of this work have benefited from presentations at the Bank for International Settlements (BIS), International Monetary Fund (IMF), and Chatham House. In addition to the working group members, comments from Agustin Carstens, Alexis Crow, C.V. Madhukar, Kalpana Kochhar, Paul Samson, Pavle Avramovic, Pramod Varma, Rahul Matthan, Todd Fox, the World Bank, and the IMF are gratefully acknowledged.

To address the pressing challenge of building a global infrastructure rather than many incompatible systems, this paper identifies three critical gaps: a governance gap, an adoption gap, and an accountability gap.

For a country to benefit though, each foundational digital rail—a platform or protocol that moves data and credentials at near zero marginal cost such as the internet, GPS, India's Aadhaar and the Unified Payments Interface (UPI), Brazil's Pix, and Estonia's X-Road—must connect to another within the country as well as across its borders. Otherwise, the global economy ends up with 100 cheap, fast, incompatible national systems instead of one genuinely open interoperable infrastructure. The fragmentation of these digital infrastructures may also pose significant risks to global financial stability.

At the country level, the paper proposes a "public-anchor, private-engine" model wherein the government sets the vision and owns the standards but does not necessarily build the infrastructure itself. In other words, industry-owned vehicles design and deliver it, competing and innovating on top, while regulators ensure that underlying protocols and standards are open and interoperable. This is "marketcraft," not traditional statecraft. The state's job is to design the market, not run or control it. Too much government control produces the expensive, proprietary systems most countries are stuck with today, and too little produces monopoly risk. Yet financing for these in-country projects—from the IMF, World Bank, regional development banks, and official development assistance alike—remains a fraction of what is needed: development institutions have directed less than 1 percent of their infrastructure portfolios toward it when the needs and returns are significantly higher.

But the deployment technology of DaaS is not a governance architecture. To address the pressing challenge of building a global infrastructure rather than many incompatible systems, this paper identifies three critical gaps. These are the three faces of the same underlying failure—nobody owns the responsibility for making these systems work, for everyone, together.

- Governance gap: No global forum exists to help countries agree on standards, so each designs critical infrastructure in silos with no shared blueprint.
- Adoption gap: More than 100 countries lack the technical capacity to build this infrastructure at all, with no institution to help prevent creating dependence on a single vendor.
- Accountability gap: When systems fail, there is no mechanism to investigate or coordinate a response.

The paper also lays out a framework based on eight principles grounded in the successful examples of UPI, Pix, X-Road, and the UK's payments architecture. The same public-anchor, private-engine principles can also be applied across borders, although that requires institutional coordination, not merely robust domestic policy.

To bridge the governance, adoption, and accountability gaps, the paper argues against the need for any new institution. Existing entities—the Group of Twenty (G20) in its two tracks, the Organisation for Economic Co-operation and Development (OECD), Bank for International Settlements (BIS),

IMF, World Bank, and regional development banks—must adapt their operations to fill these gaps.

- The G20 (with the support of global and regional institutions) should lead through its two tracks—the sherpa track setting the political agenda and best practices and the finance track directing their implementation—providing global coordination for digital infrastructure akin to what it already does for other domains. But this approach will only work if, unlike previous instances, best practices reflect the experience of emerging markets, which are leading in the digital space.
- The OECD should harmonize best practices across its membership.
- The IMF should extend best practices to every economy through its surveillance function and lending where appropriate.
- The World Bank should extend best practices through its lending—financing conditioned on openness and interoperability, delivered through private-sector execution where capacity exists.
- The regional development banks are the critical last mile: they offer regional legitimacy, deeper government relationships, and a structured channel for non-G20 countries to feed implementation experience back into how best practices are set.
- Finally, Africa needs its own node in BIS's existing Innovation Hub network.

Ultimately, the same cohesive action that builds digital infrastructure to power growth contains the risks of leaving it ungoverned. Choosing now, with the institutions that already exist, is how a country ends up governing its future instead of inheriting whatever fragmentation and monopoly emerges in its absence.

The rest of this paper is organized as follows. Sections I–VI develop the three-gap diagnosis. Section VII proposes a framework for closing them. Section VIII concludes.

Table of Contents

Glossary of Terms 5

Section I. The Technology Inflection Point 10

Section II. Digital Infrastructures 12

Section III. The Evidence: Leapfrogging Through Digital Infrastructures 14

Section IV. Design of Digital Infrastructures 16

Section V. Development Finance Needs New Rails, Not Just New Roads 18

Section VI. Three Gaps Limiting the Scaling of Digital Infrastructure 20

Section VII. A Framework for Bridging the Identified Gaps 22

Section VIII. Conclusion: Digital Infrastructure of the Next Economy 31

Annex: Official Sector Activity 32

Glossary of Terms

Aadhaar. India's national digital identity system, covering nearly the whole population; cited for generating large fiscal savings and financial-inclusion benefits relative to its cost.

Accountability gap. The absence of any international mechanism to verify that digital infrastructures meet security, privacy, interoperability, or resilience standards, or to investigate and respond when they fail (e.g., cyberattacks, data breaches).

Adoption gap. The widening divide between the roughly 100 countries with the technical capacity to build and sustain sophisticated digital infrastructures and the roughly 100 that lack it, with no international institution providing technical support to close the gap.

BankID. Sweden's digital identity system, used by 8.6 million people but operating only nationally; its 2025 cyberattack illustrates the accountability gap, since no international body could investigate or coordinate a response.

Basel Committee (on Banking Supervision). Sets international standards for bank regulation ("Basel" standards); used throughout as the model for the technical standards digital infrastructures currently lack.

BIS (Bank for International Settlements). An international organization for central banks, which has researched and published on digital infrastructure, including the India Stack study cited in Box 2.

CPMI (Committee on Payments and Market Infrastructures). A BIS-hosted body that sets standards for payment and settlement systems, directly relevant to cross-border digital payment rails.

Custom-built/full-stack development. The traditional approach to building digital infrastructure: designing and building every component from scratch for a single country, typically taking one to three years and $50–200 million before a pilot launches.

DaaS (Digital Infrastructure as a Service). A model, proposed by Carnegie India, in which countries deploy pre-packaged, cloud-ready, open-source digital infrastructure components rather than building from scratch, cutting deployment time from years to months. DaaS solves the deployment problem but not the governance problem.

Data sovereignty. A country's ability to control where its citizens' data is stored, processed, and governed, even when using cloud-based or externally supplied digital infrastructure.

Digital Chapter. The first stage of the paper's proposed reporting pathway: a section on digital infrastructure embedded into existing IMF/World Bank country instruments, such as Poverty Reduction Strategy Papers, for the first three years.

Digital Framework Report. The third stage of the reporting pathway (from year four): a standalone, country-owned report produced through multi-stakeholder consultation on a three- to five-year cycle, consolidating the country's digital infrastructure strategy.

Digital Public Infrastructure (DPI). This term is used by the G20, the World Bank, and others, and is roughly interchangeable with digital infrastructures: open, interoperable digital systems—typically for identity, payments, and data exchange—that function as public goods which are broadly accessible and in the public interest.

Digital ROSC. The second stage of the reporting pathway (from around year three): an assessment of a country's digital infrastructure progress against its accumulated track record, modeled on the IMF/World Bank's existing Reports on the Observance of Standards and Codes (ROSCs).

Digital infrastructures. Digital platforms and protocols (sometimes forming a "stack") that move data at near-zero marginal cost, providing the infrastructure for finance, commerce, health, education, and government services—analogous to railways in the 19th century or electricity grids in the 20th. Examples include the internet, GPS, Unified Payments Interface, Pix, and X-Road. Digital infrastructures generally do not include the physical infrastructure they run on (cables, satellites, data centers), though that infrastructure is a precondition for them to function. Their role is developmental, analogous to railways in the 19th century or electricity grids in the 20th. A system that provides one particular activity, e.g., identification or payments, is often called "a rail"; many applications require more than one rail to function.

FSB (Financial Stability Board). Coordinates international financial regulation and monitors global financial stability.

G20 Finance track. The G20 process led by finance ministers and central bank governors and their regulatory bodies; in this paper's framework, it provides the technical standards and accountability mechanisms that close the governance and accountability gaps.

G20 Sherpa track. The G20 process led by leaders' personal representatives ("sherpas"), covering the full political agenda; in this paper's framework, it provides political commitment to interoperability principles, closing the governance gap.

Governance gap. The absence of any global institution or forum where countries can develop shared standards and best practices for digital infrastructures, leaving each country to design critical infrastructure without common blueprints.

Governance vacuum. Shorthand for the fact that, unlike telecommunications, finance, or aviation, digital infrastructures have no international institution, standards body, or certification authority—the root cause of all three gaps.

GovTech. A World Bank/IMF initiative area focused on digitalizing government operations and public financial management.

ICAO (International Civil Aviation Organization). The UN body that sets global aviation safety and operational standards; used as a comparator institution for digital infrastructures.

IDA21. The 21st replenishment of the International Development Association (the World Bank's fund for low-income countries), which elevated digital transformation as a priority in its $100 billion December 2024 package.

Horizontality. In systems design, a component is horizontal when it cuts sideways across many domains and provides a capability that none of them owns exclusively. Horizontal layers, such as digital infrastructures, are those that everything else sits on—think of the power grid, or the IP layer of the internet. digital infrastructures are not tied to any single problem, in the same way that the power socket doesn't know whether it's running a fridge or a laptop; IP doesn't know whether it's carrying email or video. Vertical components, by contrast, go deep on a single problem and own the whole path from user to outcome: a passport-renewal service, a food-delivery app, one bank's loan product.

India Stack. The broader set of interoperable digital identity, payments, and data-sharing systems built by India, including Unified Payments Interface and Aadhaar, credited with compressing decades of financial-inclusion progress into about eight years. India Stack components are called a "stack" because applications often use more than one rail together, e.g., a bank accesses both the payments and identification components, and UPI itself uses Aadhaar to identify the payer and, eventually, the receiver of a transfer.

Interoperability. The ability of different digital systems—built by different countries, companies, or agencies—to connect and exchange data using shared standards, so that, for example, a payment made in one country's system can be received in another's. Interoperability can be classified as a global public good, and involves technical aspects, governance aspects, and accountability aspects that help facilitate cross-border coordination. It also lets an e-government service or notary platform access an identity rail directly, and lets a payment made in one country's system be received in another's using inter-recognizable "money push" rails.

IOSCO (International Organization of Securities Commissions). Sets international standards for securities regulation, relevant to tokenized assets riding on digital infrastructures.

ITU (International Telecommunication Union). The UN body that sets global technical standards for telecommunications; used throughout as the model of an institution digital infrastructures currently lack.

Network effects. The phenomenon where a system becomes more valuable to each user as more people use it (e.g., a payments system is more useful the more merchants and banks accept it). Digital infrastructures depend on network effects, which is why fragmentation across countries is so costly.

OECD (Organisation for Economic Co-operation and Development). Has published policy frameworks and best practices on digital government and digital public infrastructure, and produces the Digital Government Index cited in Section IV.

"Once-Only" Principle. When databases can query each other automatically, preventing citizens and businesses from having to submit the same information, e.g., for authentication, to multiple government agencies or private institutions to obtain consent, consult personal data, or obtain health care.

PagoPA. Italy's digital payments platform, financed by the European Investment Bank; cited as an example of development finance successfully, if modestly, supporting digital infrastructures.

Pix. Brazil's instant payments system, launched without replacing existing banking infrastructure, cited as an example of leapfrogging via interoperable rails. In Brazil, consumers continue to be able to make payments using debit or credit cards, or through interbank wires, despite the wide use of Pix.

Primitive actions. A digital rail typically provides one or more "primitive" actions that applications would otherwise have to build themselves: verifying an individual's identity, exchanging data between government or commercial databases, transferring money between accounts, or obtaining consent to access personal information. A vertical application, a commercial service or a government e-service, calls these primitives through the rail's API (Application Programming Interface) rather than replicating them.

Public anchor, private engine. The organizing principle of the paper's domestic framework: government sets the vision and standards (the "anchor") while industry-owned vehicles design and deliver the infrastructure (the "engine").

SaaS (Software as a Service). The commercial software model DaaS is loosely based on, where customers use shared, cloud-hosted software rather than building their own. The analogy also highlights that the gains of scale achieved by a provider of DaaS to several countries may translate into great market power if not adequately regulated. Also, if many providers implement non-standardized services in one or different jurisdictions, the risk of fragmentation will arise. Any of these scenarios would increase the cost of developing end-user APIs and the fruition of the benefits that digitalization, AI and tokenization can bring.

SLA (Service Level Agreement). A formal, negotiated contract between a service provider and a client. It outlines the exact scope of work, expected quality standards, and performance metrics (like uptime or response times), while detailing penalties if those commitments are missed.

We stand at a comparable inflection point today. Digital infrastructures of the 21st century are the railways of the 19th.

Tokenization. Representing assets such as currency, securities, or property as digital tokens on a programmable platform, enabling automated, multi-party transactions. Paired with digital infrastructures and AI, this is described as the next frontier of digital infrastructure.

UPI (Unified Payments Interface). India's instant payments system, a core example of an open, interoperable digital infrastructure built on a public anchor, private engine model.

Vendor lock-in. A situation wherein a country becomes dependent on a single supplier's proprietary system, making it costly or impossible to switch providers or interoperate with other countries' systems. Open standards are intended to prevent this.

X-Road. X-Road is often cited as a model for the domestic governance framework. X-Road is decentralized, open-source software that serves as Estonia's secure digital backbone. It allows hundreds of disparate public and private databases to communicate and exchange data in real time without merging into a single, hackable central system. Data is encrypted, timestamped, and signed as it moves through secure servers. It captures the "Once-Only" principle, since databases can query each other automatically. It already incorporates some international interoperability, making cross-border e-services, such as automated tax declarations or prescription sharing, possible within the Baltic region. Estonia's data-exchange layer connecting government and private-sector databases, underpinning its digital government services; cited as a model for the domestic governance framework.

I. The Technology Inflection Point

Technological revolutions throughout the last two centuries have determined which economies prosper, and how fast: the digital revolution is the latest such wave (Figure 1). In 2022, digital sectors accounted for 10 percent of US GDP[2] but generated more than a third of its growth over the past decade;[3] globally, the digital economy reached $16 trillion in 2024, 15 percent of world GDP.[4] Mobile telephony allowed African countries to bypass fixed-line infrastructure entirely, and by 2020, sub-Saharan Africa had higher mobile penetration than landline penetration ever reached.[5]

Figure 1: Digitalization is Increasing at a Dizzying Pace

	Front and Back End Security	Access	Compute Power	Date Streams	Hardware	Analytics
2000	Password and Token	200Kb/s 3g APIs, Netflix reaches 1 million subscribers 3.5 years after its launch	Intel Pentium III microprocessor: 1.4 gigaflops (1.4 billion)	Transaction data (E-commerce)		
2002	Advanced Encryption Standard					Cloud Computing DLT (Blockchain)
2004	Elliptic-curve cryptography (ECC)	Windows Mobile			Nvidia CUDA GPU	Machine Learning
2006		iPhone 3G 3Mb/s, Spotify launches, reaches 1 mil subscribers in 5 months	iPhone 1: 1.6 gigaflops (1.6 billion)	Mobility data (Google Map Mobile)	Commercial Solid State Disk	AI Technology
2008			NVIDIA GTX GPU; 1.3 teraflops (1.3 trillion)(at peak)		Parallel Processing	Quantum Computing Data lakes
2010		iPad, 4G Android 1.0, 1 billion smartphone users	IBM Watson: 80 teraflops (80 trillion)	Lifestyle data (mobile payments/ SNS)	Superconductors	
2012	Biometrics on smartphones	E-wallet		Social Media (sentiments)		Large Language Models
2014	Smart contracts	Apple Pay	iPhone 6: 172 gigaflops (172 billion)	Internet of Things (machine generated data)		
2016	Facial Payments	2 Billion Smart phone users			Cloud Servers	
2018		3 billion smartphone users, 5G 10Gb/s			Data Centers	
2020		Chat GPT launches, reaches 1 mil users in 5 days	MacBook air (m1 chip): 2.6 teraflops (2.6 trillion)		HBM3	
2022	Password-less security	4 billion smart phone users, threads launches, reaches 1 mil users in 1.5 hours	Frontier Supercomputer: 1.2 exaflops (1.2 quintillion)	AI Prompts and Conversations AI-created training data	Liquid Cooling	
2024						
2025	Zero Trust Architecture Passkeys	Cloud 6PU Doubling of FIDO2 Cloud Computing AI Analytics	NVIDIA rack-scale: 15 exaflops	Processing of data at scale Apache Kafka	Rack-scale 72-6PU	

We stand at a comparable inflection point today. Digital infrastructures of the 21st century are the railways of the 19th. They will determine which countries achieve sustained growth over coming decades. This moment differs from that of previous infrastructure transitions in that the institutional architecture to govern it is being built—or not built—at exactly the timepoint that the technology is moving the fastest. Major powers are diverging, standard-setting is fragmenting, and the window for establishing frameworks that allow scaling is narrowing.

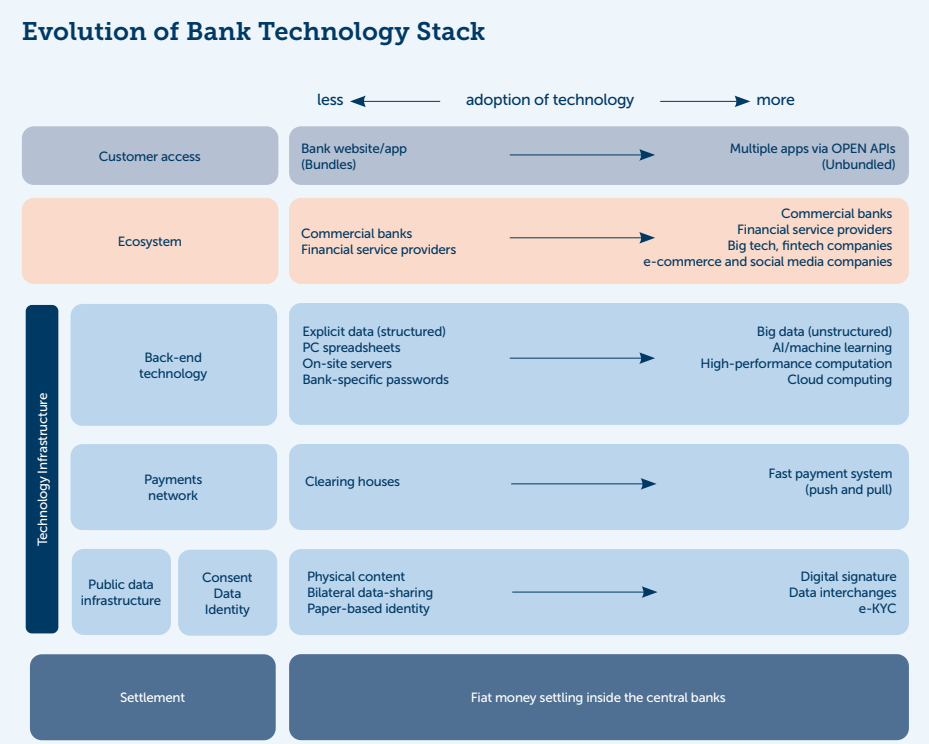
2. U.S. Bureau of Economic Analysis, "U.S. Digital Economy: New and Revised Estimates, 2017-2022," Survey of Current Business, December 6, 2023. https://www.bea.gov/data/special-topics/digital-economy
3. https://www.bea.gov/data/special-topics/digital-economy Robert D. Atkinson, "Six Tech Industries Accounted for More Than One-Third of GDP Growth in the Last Decade," Information Technology and Innovation Foundation, May 30, 2023.
4. https://itif.org/publications/2023/05/30/six-tech-industries-accounted-for-more-than-one-third-of-gdp-growth-in-the-last-decade/ International Data Center Authority, Global Digital Economy Report (IDCA, 2025). https://www.idc-a.org/insights/qUi9XgvyrzSkyDUy9Tqr
5. Pew Research Center. "Cell Phones in Africa: Communication Lifeline" (2015). https://www.pewresearch.org/global/2015/04/15/cell-phones-in-africa-communication-lifeline/

The acceleration is visible on both sides of the market. On the demand side, Netflix achieved 1 million users in 3.5 years, Spotify reached the same number in 5 months, ChatGPT in 5 days, and Threads in 1 hour. These metrics reflect more than consumer enthusiasm. They signal the maturing of the technologies that enable instant global reach at negligible marginal cost.

On the supply side, computing power now operates at scales unimaginable five years ago. A single large artificial intelligence (AI) model today commands more computing power than all personal computers on Earth combined. What once required billions in capital and years of deployment can now be accessed on-demand through cloud infrastructure, creating leapfrogging opportunities for countries that lack legacy systems.

For illustrative purposes on how technological revolutions impact systems, see the evolution of banking operations in Figure 2.

Figure 2: Evolution of Bank Technology Stack



II. Digital Infrastructures

Digital infrastructures are digital platforms protocols, and governance rules that function as a utility (Box 1). Rather than every application building its own identity verification, data exchange, or payment transfer from scratch, it plugs into the rail via an API (Application Programming Interface) to execute these basic actions at lightning speed and near-zero marginal cost, allowing countries to bypass the expensive, decades-long infrastructure buildouts that constrained previous generations.

Box 1. What are Digital Infrastructures?

Digital infrastructures are—platforms or protocols—that allow many different organizations and people to exchange credentials, data, or value quickly, cheaply, and on equal terms. Two examples offer a helpful analogy: many different shippers move goods along the same railway track; or, many appliances draw power from the same electrical grid. Digital infrastructures do the same for data and digital transactions.

Individuals already use digital infrastructures every day, often without realizing it:

- **Global Positioning System (GPS).** Built and operated by the US government, GPS is the "rail" that every ride-hailing app, delivery service, and farming tool runs on top of.
- **Galileo.** The EU's satellite navigation system, built by the EU and European Space Agency, offers the same free positioning service as that of GPS but under European governance.
- **The internet.** The original digital infrastructure—a shared set of protocols that allow any computer, anywhere, to exchange data with any other, without a custom connection to each one.
- **India Stack.** Components include: (i) **Aadhaar:** a biometric-based national digital identity system giving every resident a unique 12-digit ID number for verifying identity across government and financial services; (ii) **Unified Payments Interface (UPI):** a shared payments "rail" that allows any registered institution (bank, fintech, BigTech, individual, or merchant) to send and receive instant payments in the same way email allows any provider's users to message users of any other provider; and (iii) **eSign:** the backbone for paperless workflows across financial and government services (2 billion signatures to date).
- **Estonia's X-Road.** A data-exchange layer that allows government agencies and private companies to securely share information about a citizen, with consent, without each building its own connection to every other database.
- **Brazil's Pix.** An instant-payments system connecting every bank and fintech in Brazil to every other, launched without dismantling the existing banking system.

Digital infrastructures underpin digital services in every sector, including financial services, e-commerce, farming, healthcare, and education. Countries with effective digital infrastructures can deliver emergency fiscal transfers to hundreds of millions, coordinate vaccine distribution, provide scalable education platforms, and enable digital commerce through integrated payment systems.

What matters is the architecture and its governance. If the underlying protocols/standards (both technology and governance/regulation) are open and managed by public/regulatory authorities, the infrastructure platforms themselves can be built, owned, and operated by governments, private firms, or public-private partnerships. The key is open and interoperable architecture[6]: anyone meeting the technical standard can connect and use it, the same way any phone on one network can call any phone on another network. Most applications need to access several digital rails to execute a complex task and deliver a service to an end-user as shown in Figure 2. Such architecture creates network effects that sustain innovation through open, contestable markets. A farmer using digital payments can access crop insurance from different providers. A student with digital identity can receive targeted scholarships. An entrepreneur can incorporate a business, open a bank account, and begin trading—all digitally, often in hours rather than months.

Why this matters for policy: A single country can build its own digital identity system, payments network, or health data platform in isolation. But its value—and its ability to support trade, finance, and emergency response—depends on whether it can connect to the systems other countries build.

Beyond current applications, AI and tokenized assets riding on digital infrastructures represent the next frontier. Digital infrastructures provide the secure infrastructure, standardized protocols, and scale. While AI systems add real-time analysis, fraud detection, personalization, and automation, they differ in kind. They emerge from data, and their capabilities are shaped by what they are trained on in ways that are not fully predictable or controllable in advance.[7] The next generation of digital infrastructure is being designed with AI embedded from the start, not added on top, which fundamentally changes the governance questions. Tokenization enables multi-asset, multi-function, and multi-party transactions on a programmable platform. Together, these create systems that were not possible with either technology alone: credit scoring for the unbanked, real-time economic policy adjustment, self-executing contracts, personalized education, and preventive healthcare. This paper focuses on the governance of digital infrastructures, not on the challenges posed by AI.

Countries will experience a time-sensitive opportunity to leapfrog. Network effects and first-mover advantages are accruing to early movers. The question is no longer whether digital infrastructures drive growth. That evidence is clear. It is whether countries will build them with open standards that enable continued innovation, or closed systems that lock in today's technology and tomorrow's digital divides.

6. Connectivity infrastructure—whether mobile networks, fixed broadband, or satellite systems such as Starlink—is the prerequisite layer on which all digital infrastructures depend. The governance principles this paper proposes apply here as well: without open standards and interoperability mandates at the connectivity layer, the most sophisticated payment rail or identity system remains unreachable for the populations it is designed to serve.
7. This is unlike railways, electricity grids, and telecommunications networks which are designed, built, and operate predictably within defined parameters—they do what their engineers intended.

III. The Evidence: Leapfrogging Through Digital Infrastructures

Digital infrastructures dramatically accelerate the learning and adoption curves that historically required decades to traverse. This acceleration is particularly significant for marginalized populations—women, the less educated, the unemployed, residents of remote areas—that have traditionally been excluded from formal economic and social systems.

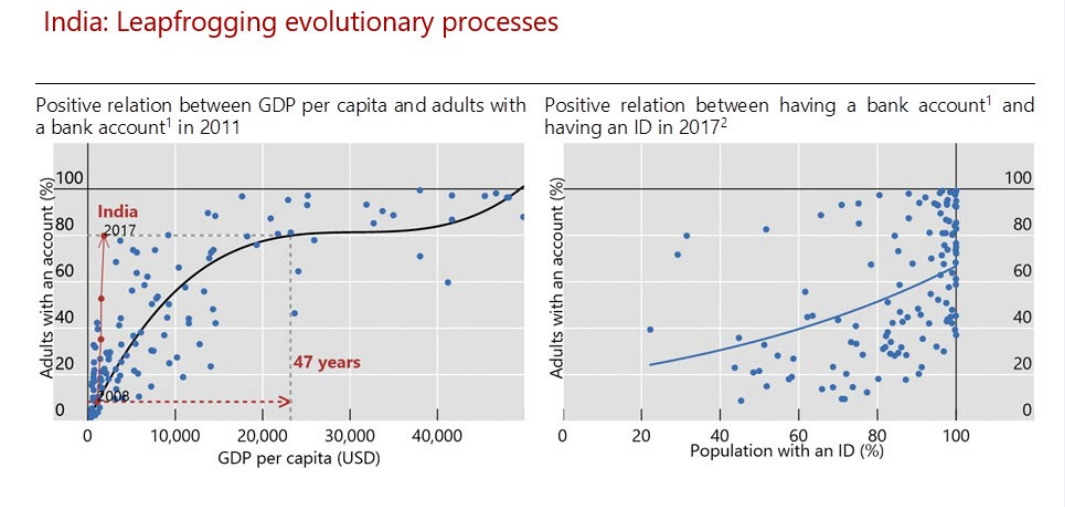
Digital infrastructures lower barriers to entry: They reduce transaction costs, eliminate geographic constraints, enable access without physical presence or extensive documentation, and provide 24/7 availability. The result is not merely inclusion, but also pathways for economic participation and upward mobility that can break generational cycles of poverty.

Box 2. Leapfrogging Evolutionary Processes

Work conducted at the Bank for International Settlements has shown that through the India Stack, India achieved financial sector outcomes in 8 years when a traditional evolutionary development process would have taken 47 years, thereby accelerating financial inclusion and productivity gains.

Between 2011 and 2017, the share of the population with bank accounts soared to 80 percent—the largest increase (45 percentage points) recorded for any of 121 countries in the sample during this period. The gender gap diminished from 17 percent to 6 percent. The inclusion difference between those in and out of the labor force fell from 18 percent to 9 percent; between those with and without secondary education from 29 percent to 10 percent; and between rich and poor from 14 percent to 5 percent.

Figure 3: India: Leapfrogging Evolutionary Processes



Source: Tiwari, S et al., "The Design of Digital Financial Infrastructure: Lessons from India," BIS Papers, no. 106 (Bank for International Settlements, 2019). https://www.bis.org/publ/bppdf/bispap106.htm

Work conducted at the Bank for International Settlements (BIS) has shown that through the India Stack, India achieved financial sector outcomes in 8 years; a traditional evolutionary process would have required 47 years (Box 2). India's DIKSHA platform offers 19,698 courses with 182.3 million enrollments supporting 36 languages.[8] At the same time, China's WeBank serves 270 million consumers at $10 per customer,[9] 93 percent below traditional acquisition costs.[10]

Adoption isn't automatic, even for the government that builds the rail. India's own e-rupee illustrates the limit: retail circulation fell roughly 24 percent over the past year,[11] and daily transactions dropped from a 2023 peak of 1 million to about 100,000, because UPI had already provided Indians with a frictionless alternative they trusted.[12] The lesson isn't that central bank digital currencies fail—it's that a well-governed rail is attractive and an early-mover advantage is real.

Advanced economies demonstrate parallel acceleration. Korea tops the 2023 OECD Digital Government Index, leading in firm AI adoption.[13] Denmark ranks second, with 92 percent of internet users accessing digital public services via shared identity and consent APIs.[14] Estonia's X-Road connects more than 900 organizations,[15] delivers 99 percent of public services online,[16] and saves 2 percentage points of GDP in bureaucratic costs annually.[17]

Among Organisation for Economic Co-operation and Development (OECD) countries surveyed, 85 percent have data sharing systems and single digital gateways, while 73 percent have implemented digital identity systems.[18] Digital infrastructures can increase GDP of low- and middle-income countries by 1 to 1.4 percentage points by 2030.[19] Yet success requires complementary investments: two-thirds of the population in high-income countries possesses basic digital skills, compared to only 21 percent in lower-middle-income countries and less than 5 percent in low-income countries, a preview of the adoption gap examined in Section VII.[20]

---

8. UNESCO, DIKSHA Platform Statistics and Digital Learning in India. (UNESCO Institute for Statistics, 2025). https://www.unesco.org/en/dtc-financing-tool-kit/diksha
9. Sally Chen, et al., "Virtual Banking and Beyond," BIS Papers, no. 120 (Bank for International Settlements, 2022), 14, Box A, https://www.bis.org/publ/bppdf/bispap120.pdf.
10. Sally Chen, et al., "Virtual Banking and Beyond," BIS Papers, no. 120 (Bank for International Settlements, 2022), 14, Box A, https://www.bis.org/publ/bppdf/bispap120.pdf.
11. Ashwin Manikandan, "India's RBI Plans Expansion of Digital Rupee Through Welfare Schemes, Cross-Border Payments," Reuters, May 29, 2026. https://www.reuters.com/world/india/indias-rbi-plans-expansion-digital-rupee-through-welfare-schemes-cross-border-2026-05-29/
12. Jaspreet Kalra, "India Digital Currency Transactions Slump After Reaching Initial Central-Bank Target," Reuters, June 25, 2024. https://www.reuters.com/technology/india-digital-currency-transactions-slump-after-reaching-initial-cbank-target-2024-06-25/
13. OECD, 2023 OECD Digital Government Index: Results and Key Findings. OECD Public Governance Policy Papers, No. 44 (OECD Publishing, 2023). https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html
14. Jon Kvist, ESPN Thematic Report on Access to Essential Services for Low-Income People—Denmark, European Social Policy Network (Brussels: European Commission, 2020), https://ec.europa.eu/social/BlobServlet?docId=22817&langId=en.
15. OECD/SIGMA, Implementation of Laws on General Administrative Procedure in the Western Balkans, SIGMA Papers no. 62 (Paris: OECD Publishing, 2021). https://one.oecd.org/document/GOV/SIGMA%282021%292/en/pdf
16. OECD, "Case Study: The Estonian Education Information System (EHIS)," in Strengthening the Governance of Skills Systems: Lessons from Six OECD Countries, OECD Skills Studies (Paris: OECD Publishing, 2020). https://www.oecd.org/en/publications/strengthening-the-governance-of-skills-systems_3a4bb6ea-en/full-report/component-6.html
17. e-Estonia Briefing Centre and OECD, Digital Public Infrastructure for Digital Governments. Policy Papers, No. 68 (OECD Publishing, 2024). https://www.oecd.org/en/publications/digital-public-infrastructure-for-digital-governments_ff525dc8-en.html
18. OECD, Digital Public Infrastructure for Digital Governments, OECD Public Governance Policy Papers, no. 68 (Paris: OECD Publishing, 2024) 13, fig. 3. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf
19. United Nations Development Program, The Human and Economic Impact of Digital Public Infrastructure (UNDP, 2023). https://www.undp.org/publications/human-and-economic-impact-digital-public-infrastructure
20. World Bank. Digital Progress and Trends Report 2025: Strengthening AI Foundations (World Bank, 2025). https://www.worldbank.org/en/publication/dptr2025-ai-foundations

Effective digital infrastructures combine open, modular, reusable, and interoperable architecture with appropriate governance.

IV. Design of Digital Infrastructures

a. Emerging Best Practices

Effective digital infrastructures combine open, modular, reusable, and interoperable architecture with appropriate governance. Open systems enable the private sector—from startups to enterprises—to connect and innovate on equal footing. Modularity allows new functionalities to be introduced without redesigning entire platforms. Interoperability through shared protocols ensures systems can scale as populations and technologies evolve.

Best-in-class implementations feature end-to-end digital workflows with federated data management,[21] **privacy protections built into the architecture,** and technical standards enabling automated compliance, reducing transaction costs while maintaining security and regulatory oversight. A rural user handing cash to a banking agent who completes the transaction on the underlying rail is fully included. The rail is digital even where the last mile isn't, and multi-modal access of this kind is a permanent design feature for reaching the marginalized, not a stopgap on the way to eliminating human intermediaries.

b. The Limits of Custom-Built Approaches

If digital infrastructures deliver such dramatic results, why haven't more countries adopted them? The answer lies in how most countries have approached development.

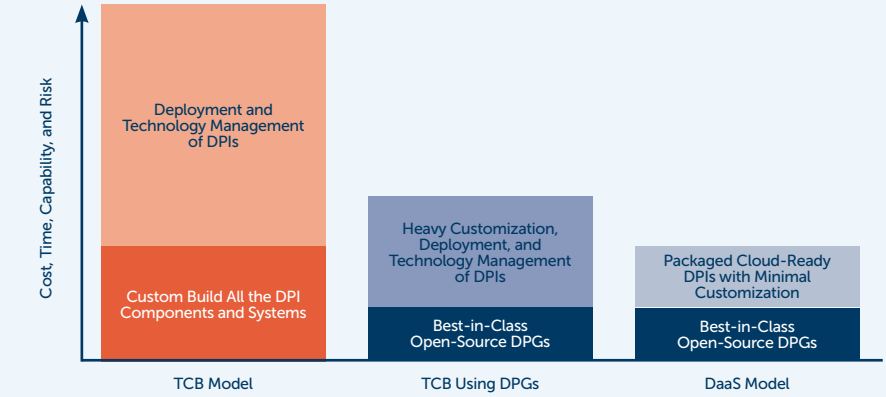
Traditionally, countries have built digital infrastructures through custom, full-stack solutions, digitalizing one business process at a time, building all components from scratch. Custom solutions reduce reusability, interoperability, and adaptability while incurring significant costs. The procurement cycle typically takes one to three years and requires substantial upfront investment before even beginning a pilot.

Another problem sits upstream: many countries never reach the point of choosing between custom-built and shared infrastructure at all. Ministries procure a health system, a finance system, a registry—each as a standalone point solution, with no infrastructure-first framing in the decision. This is not a governance failure so much as an advocacy and consensus failure.[22] Governance architecture answers what happens once a country decides to build infrastructure—it does not by itself create that decision.

Even where there is the intent to build digital infrastructures that could provide an efficient and reliable infrastructure for public and private applications, countries may not have the ability to do so. More than 100 countries lack the technical capacity to build and maintain population-scale bespoke digital infrastructures. This is the adoption gap in concrete terms: without a different delivery model, these countries are effectively locked out.

21. In implementations such as Estonia's X-Road, data continues to sit in its original institutions rather than being consolidated into one place, reducing the risk of a single, high-value target for attackers.
22. The case for thinking "shared, reusable building blocks" before "solve this one problem" has not been made and accepted widely enough, across sectors, to change how spending decisions are framed in the first place.

Figure 4: Comparing the Different Digital Infrastructure Rollout Models



Source: Adapted from "DaaS in a Nutshell," Centre for Digital Public Infrastrucutre, February 2024, https://docs.cdpi.dev/additional-info/dpi-as-a-packaged-solution-daas/daas-in-a-nutshell

c. Packaged Solutions, Missing Governance

The international community is increasingly recognizing the importance of modular, open-source frameworks that enable countries to deploy digital infrastructures by adopting proven components rather than starting from scratch. Varma et al propose a digital infrastructure as a service (DaaS) approach: pre-packaged, cloud-ready systems deployed in six months instead of years.[23] Where the traditional model requires $50–200 million in upfront costs, three to five years of gestation and hundreds of engineers, DaaS offers cloud deployment, open-source foundations, no vendor lock-in, and data sovereignty—transforming prospects for 100-plus countries lacking capacity to custom-build (Figure 4).

But the software as a service (SaaS) analogy ends here. When commercial software fails, companies lose productivity. When digital infrastructures fail, citizens cannot access government services, open bank accounts, or cross borders. And unlike SaaS—wherein companies benefit independently—DaaS's payoff compounds with coordination and starts at home and then extends cross-border. Twenty countries deploying incompatible versions create fragmentation, not infrastructure. Network effects require networks, and networks require governance.

The governance vacuum is acute. Unlike telecommunications (International Telecommunication Union–ITU), finance (Basel Committee on Banking Supervision–BCBS), or aviation (International Civil Aviation Organization–ICAO), digital infrastructures have no international institution, no standards body, and no certification authority. The result is that even DaaS built on common open-source foundations spawns incompatible national

23. Pramod Varma et al., The Future of Digital Public Infrastructure: A Thesis for Rapid Global Adoption, Carnegie India, February 13, 2024. https://carnegieendowment.org/india/research/2024/02/the-future-of-digital-public-infrastructure-a-thesis-for-rapid-global-adoption

systems if countries customize differently. Sweden's BankID serves 8.6 million users but remains national. Its 2025 cyberattack was a major disruption. Imagine the scale of that fragmentation in a global event. This is the governance gap and the accountability gap together: no existing body sets the standards that would prevent such fragmentation, and no standards body would have investigated the failure had it cascaded across borders.

A distinction that the policy debate frequently blurs—and about which this paper is explicit—is the difference between digital infrastructure's front-end and the back-end. The front end is the user-facing application layer: the apps, interfaces, and services that consumers and businesses interact with directly. This layer can and should be competitive, diverse, and market-driven—the 500-plus fintech ecosystem built on India's UPI is a front-end, not a back-end achievement. That front-end includes Big Tech alongside domestic challengers: Google Pay and PhonePe (recently acquired by Walmart) dominating the market alongside WhatsApp Pay and Paytm, proof that an open back-end allows every platform in as a competitor. The back-end is the infrastructure layer: the settlement systems, identity rails, data exchange protocols, and regulatory reporting architecture that the front-end runs on. This layer requires standardization, government oversight, and cross-border coordination precisely because it cannot be left to market competition without producing fragmentation or monopoly.

The public-anchor, private-engine principle applies differently at each layer: government sets and owns the back-end standards; industry competes and innovates on the front-end. Conflating the two produces either over-regulation of innovation or under-regulation of infrastructure—both of which are evidence from failed digital infrastructure deployments.

DaaS offers a genuine breakthrough in deployment, but deployment technology is not governance architecture. The choice is not whether to adopt DaaS-style deployment, which is clearly advantageous for many small or less-developed countries. It is whether to build the governance architecture that prevents DaaS from becoming 75 national solutions instead of a global infrastructure.

V. Development Finance Needs New Rails, Not Just New Roads

Development finance institutions face a strategic misallocation. Their portfolios remain weighted toward traditional infrastructure—roads, power plants, water systems—while digital infrastructures demonstrate superior returns and advance multiple development objectives simultaneously. Yet development banks allocate less than 1 percent of infrastructure portfolios to digital infrastructures,[24] despite the fact that most countries already possess the first layer for digital services—reasonably functioning telecommunications, internet, and electricity networks (see Annex).

24. "Asian Infrastructure Investment Bank, "AIIB Investing to Address the Digital Divide in Asia," January 17, 2020. https://www.aiib.org/en/news-events/news/2020/AIIB-Investing-to-Address-the-Digital-Divide-in-Asia.html

This misallocation, which reduces the potential return on existing physical infrastructure, is the adoption gap viewed from the supply side of finance: the countries that are most in need of help building digital infrastructures are those least likely to find it on offer.

The economics are compelling.[25] Digital infrastructure reaches a marginal cost of zero at scale while traditional infrastructure scales linearly—each kilometer of road costs proportionally. Network effects compound value as each user makes the system more valuable to others. India's Aadhaar cost $2.1 billion over 15 years and generated $42 billion in direct savings through improved subsidy targeting, plus significant additional indirect benefits from financial inclusion—a 28:1 return, against roads at 3-4:1 and power at 2-3:1.[26,27]

Another possibility is that a low allocation may reflect rational caution, not simply institutional failure. Digital infrastructures often need a public-interest launch phase—priced low or free to drive adoption—before the rail can sustain itself. India's UPI illustrates the pattern: it launched near-free, funded by government incentives before fees are introduced.[28] This is not a special failure of digital infrastructures. Roads follow the same logic; fuel taxes and tolls fund the maintenance that free initial access could not. Appraisal frameworks built for one-time capital projects rarely price for that lifecycle.

Digital infrastructures also advance competing development priorities simultaneously—a rare attribute in infrastructure wherein trade-offs typically dominate. The same infrastructure reduces subsidy leakage, enables fintechs, generates AI training data, and builds digital literacy through daily use. The United Nations Development Programme estimates that digital infrastructure could add $200–280 billion to GDP across 70 countries by 2030.[29]

Private capital builds digital services wherein returns are clear. Digital infrastructures, however, which are similar to a utility that supports many users/developers, exhibit classic development finance characteristics. Social returns vastly exceed private returns, and digital infrastructures require interoperability while private firms prefer proprietary lock-in that fully captures the benefits in each vertical. Left to markets, countries end up with fragmented systems. Development finance can condition funding on open standards and unlock the unique opportunity to leapfrog. India built modern payment infrastructure without dismantling banks. Estonia created digital government without reforming bureaucracy first. Brazil launched instant payments without replacing existing networks, or the vast web of credit and debit cards, or bank wire services.

25. India's digital identity system delivers a 28:1 return on investment. Estonia saves 2 percent of GDP annually through digital government infrastructure.
26. Unique Identification Authority of India, "Finance and Budgets," annual expenditure data through FY 2023–24. https://uidai.gov.in/hi/budget
27. Government of India, Ministry of Finance, "India's DBT: Boosting Welfare Efficiency," April 21, 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2123192
28. A 2026 parliamentary review found covered only 11 percent of industry costs. India is now reintroducing fees for large, profit-making merchants while keeping the rail free for individuals and small businesses.
29. United Nations Development Programme and Digital Public Goods Alliance, Bold Investments for Digital Public Infrastructure: Quantifying the Human & Economic Impact—Executive Summary, with Dalberg Advisors, (New York: UNDP, 2022), 1–2. https://www.digitalpublicgoods.net/Bold-Investments-Executive-Summary.pdf

Development institutions already finance digital services successfully—just nowhere near the scale that the evidence warrants. The European Investment Bank (EIB)'s financing of Italy's PagoPA platform and its investment in digital payment infrastructure across 20 African countries prove development banks can finance digital rails effectively. Yet even the EIB's investments represent small fractions of its €100 billion annual target.

Three roadblocks must be addressed. First, development institutions lack digital infrastructure expertise—project teams most often understand roads, power and water, not platforms and protocols. Second, current project appraisal frameworks struggle with network effects and platform economics; new frameworks must capture direct returns, enabling effects, option value, and crucially, fiscal space created for other priorities. Third, digital infrastructures require interoperability, but development institutions operate independently. A coordinated digital infrastructure network across the World Bank, IMF, European Bank for Reconstruction and Development (EBRD), EIB, regional banks, bilateral agencies, and standard-setters could share lessons, develop standards, and pool technical assistance.

Development finance needs new rails because new rails generate resources for roads and electrification. Digital infrastructures meet all three criteria that define development finance's mandate: (1) social returns exceed private returns, (2) coordination failures require intervention, and (3) patient capital enables leapfrogging. The question is whether development finance will scale a workable solution.

VI. Three Gaps Limiting the Scaling of Digital Infrastructure

Although impressive, the scale of institutional activity is proceeding without coordinating architecture. Multilateral banks mobilize billions, UN agencies develop safeguard frameworks, bilateral donors fund pilots, and foundations catalyze innovation. Yet no institution sets mandatory technical standards. No body certifies compliance. No mechanism ensures systems built in neighboring countries can communicate. The contrast is stark: telecommunications have the ITU, finance has Basel, and aviation has ICAO. Digital infrastructure has financing and technical assistance, but not the advocacy and consensus needed to make infrastructure-first thinking the default—nor the governance framework that follows once it is.

The gaps cited throughout this paper are not isolated frictions. The self-reinforcing divide between countries with mature and immature digital infrastructures (Section I), the choice between custom-built and DaaS deployment without governance to match (Section IV), and the misallocation of development finance toward roads rather than rails (Section V) are three components of the same underlying problem: the absence of an institutional architecture for digital statecraft. This section names that problem directly.

Departing from the traditional multilateral playbook where trends move from advanced economies to developing countries, the paper draws upon a few powerful examples of digital infrastructure innovations from emerging market countries that have been proven at scale.

The result is predictable: fragmented national systems, duplicated effort, incompatible implementations, and growing risk that the global digital economy splinters along technical fault lines that will prove extraordinarily costly to bridge once systems harden.

The following three critical gaps define the challenge:

Governance Gap. No global institution exists wherein countries can share experiences and agree on best practices for digital infrastructure governance (i.e., guidance that would support both domestic design choices and cross-border frameworks). Countries are designing critical infrastructure without blueprints, risking incompatibilities that will be nearly impossible to reverse once systems harden. This is a statecraft failure: ceding standard-setting power to whoever moves first, rather than shaping the rules through deliberate sovereign strategy. The G20's 2023 commitment to a Global Digital Public Infrastructure Repository remains unfulfilled.

Adoption Gap. A digital divide is emerging between countries that can build and maintain sophisticated systems and those that cannot. More than 100 countries lack the technical capacity for custom digital infrastructure development. No global institution provides technical adoption support, conducts periodic assessments against best practices, or helps countries navigate vendor selection without lock-in. The gap between digital leaders and laggards will widen irreversibly as first-mover advantages and network effects compound. Section VII proposes a concrete answer: a technical secretariat staffed partly by multilateral secondees (Principle 6), backed by IMF surveillance and World Bank financing conditionality, with regional development banks as the implementation last mile. But institutions cannot substitute for domestic ownership: governments that treat capacity-building as a priority, not an afterthought, close this gap fastest—with regional banks, the multilaterals, and philanthropic funders (Section VII) supporting that effort, not replacing it.

Accountability Gap. No global institution verifies that digital infrastructures meet international standards for security, privacy, interoperability, or resilience. The absence of any body equivalent to Basel for banking or ICAO for aviation has left digital infrastructures without a mechanism to certify compliance or coordinate responses when infrastructure fails.

Trust in digital infrastructures is not siloed by design—it's siloed only once tested. A crisis in one system, whether a digital outage or a stablecoin de-peg, tends to spill into doubt about others. Users don't distinguish between architectures, only between confidence and its absence.[30] The accountability gap this paper names is precisely what digital infrastructures currently lack: the anchor that makes one failure look contained rather than systemic.[31] As digital infrastructures become as essential as electricity grids,

30. This mirrors bank runs, which spread until depositors learn the system is anchored—by deposit insurance, a lender of last resort, credible supervision—and contagion becomes the exception rather than the rule.
31. This cuts both ways: fragmentation that blocks interoperability also blocks contagion. A system that never connected to its neighbors cannot import their failures, only its own. The case for connection is not that it eliminates this trade-off, but that a well-anchored, interoperable system contains failures better than either an isolated one or a poorly anchored connected one.

the absence of accountability frameworks creates vulnerability at both national and global levels.

The consequences compound. Without governance, countries build incompatible systems. Without adoption support, only well-resourced nations succeed, widening digital divides. Without accountability, systemic risks accumulate unchecked until failures cascade.

VII. A Framework for Bridging the Identified Gaps

The recommendations that follow are grounded in evidence and in what has demonstrably worked in India, Brazil, Estonia, Kenya, and elsewhere. They cover both principles to build domestic governance and the potential use of existing international institutions to promote global governance in the absence of a dedicated organization. They are offered as a starting framework. Digital infrastructure governance does not yield to a single design applied uniformly across 190 economies with different political systems, institutional capacities, and development trajectories. Implementation will require flexibility as country contexts vary, patience as institutional cultures adapt, and sustained political will must be channeled through architecture. The distance between a well-designed framework and its realization in practice is real. What the evidence does show is that the direction is right, the tools exist, and the cost of not acting—measured in widening digital divides, fragmented systems, and compounding vulnerabilities—is far higher than the cost of beginning.

a. Frameworks Within Countries

Governance begins at home. The three aforementioned gaps all have national dimensions: how should countries organize themselves to design, build, and sustain digital infrastructure in a way that unleashes private innovation rather than constraining it?

More government is not the answer. Most countries have instinctually treated digital infrastructure development as a government IT project—housed in a federal agency/ministry, procured through public tender, staffed by civil servants, and accountable to a minister. This model has produced some notable successes in countries with exceptional state capacity. But it has also produced the expensive, proprietary, and poorly interoperable systems that now litter the digital landscape of middle- and low-income countries. The evidence from successful deployments points in a different direction: the countries that have built the best infrastructure most quickly separated public authority over purpose from private responsibility for execution.

Framework Recommendations: Eight Principles

Eight principles define this better model, grounded in India's UPI, Brazil's Pix, Estonia's X-Road, and the UK's next-generation retail payments

architecture. They apply across all digital infrastructure domains—finance, data exchange, health, education, agriculture—without requiring a separate governance regime for each sector. These principles are relevant also in countries that chose to adopt DaaS.

Principle 1: Public anchor, private engine. The public anchor retains what matters: sets the vision, owns the standards, safeguards the public interest, and enforces open interoperable architecture. What it does not do is build (Box 3). Infrastructure design and delivery are led by industry-owned vehicles. India's UPI is designed and operated by the National Payments Corporation of India, an industry-owned entity within a framework set by the Reserve Bank of India. Brazil's Pix was architected by the central bank but built on mandatory private sector participation. The United Kingdom hands design and delivery to an industry-owned and funded company, with the Bank of England setting strategic direction. In each case, private ownership of the engine drove the speed, innovation, and commercial sustainability that government-led models struggle to match.

Box 3. What Do "Standards" Mean for Digital Infrastructure?

"Public anchor, private engine" (Principle 1) says government owns the standards. In practice, that means six distinct categories, not one:

- **Interoperability standards.** The technical specification that allows any compliant system to connect, the way ISO 20022 allows banks worldwide to exchange payment messages in a common format.
- **Open standards.** A specification for the digital system/infrastructure that is publicly available, developed through an open process, free of vendor lock-in, and interoperable by design.
- **Security standards.** Authentication and fraud prevention requirements every participant must meet, such as FIDO2 (Fast Identity Online 2) for passwordless authentication or PCI-DSS (Payment Card Industry Data Security Standard) for card-data handling.
- **Identity assurance standards.** How confidently a system verifies who someone is, graded by frameworks such as National Institute of Standards and Technology 800-63 or the EU's eIDAS (electronic Identification, Authentication and Trust Services).
- **Data governance standards.** Consent, portability, and revocability rules for personal data, such as India's Data Empowerment and Protection Architecture/ORGANS principles or the EU's General Data Protection Regulation, without which interoperability cannot exist.
- **Consumer protection standards.** Liability and reimbursement rules when things go wrong, such as the UK's mandatory reimbursement framework for authorized push payment fraud.

Principle 2: Representation follows the ecosystem, not the organizational chart. The governance framework must reflect the value chain—incumbents, telecoms, platforms, merchants, civil society, and end users. Telecommunications companies deserve particular mention: their absence from governance boards has been a persistent and costly blind spot.

Representation should be secured through open nomination rather than ministerial appointment and should evolve as the ecosystem evolves.

Principle 3: Strategy, design, and delivery are separated by design. Vision-setting requires public legitimacy. Technical design requires ecosystem expertise. Delivery requires capital and execution accountability. Conflating these functions produces delays, cost overruns, and proprietary lock-in. The UK model provides the clearest template: the Payments Vision Delivery Committee sets outcomes; the Retail Payments Infrastructure Board translates strategy into design; an industry-owned delivery company builds the rails, while applications compete on top. The same three-layer logic applies across sectors. A Digital Identity Board or Agricultural Data Board would follow identical structures with sector-specific compositions.

Principle 4: The regulator observes, it does not chair. Regulatory oversight is essential but must be structurally separated from design and delivery governance. The regulator participates—flagging public interest concerns and monitoring systemic risk—but it does not direct technical choices.[32] In the UK model, the Financial Conduct Authority and Payment Systems Regulator sit as observers on the infrastructure board. For countries wherein the central bank anchors, regulates, and operates systems, clearer internal separation of these functions is the practical equivalent. The principle holds regardless.[33, 34] In contrast, identity, health, and data infrastructure typically split oversight across multiple regulators with overlapping mandates—a data protection authority, a telecommunications regulator, a sector ministry—where "the regulator" is not one body but several.

Principle 5: Interoperability built on open standards is a condition of participation, not a negotiating position. Open standards must be embedded in the mandate of the governing board and delivery vehicle from inception. In practice, this means that vendors proposing proprietary systems are ineligible; interoperability certification is a pass-fail procurement criterion; and the public anchor retains explicit legal rights to enforce open architecture so that a change of commercial ownership cannot convert public infrastructure into a proprietary platform.

Principle 6: Capacity scales with ambition. Most countries building digital infrastructures lack the deep domestic expertise. Treating capacity as a precondition is a counsel of indefinite delay. The more productive approach is to build capacity through governance: constitute the board, provide external technical support, and develop domestic expertise through designing real infrastructure. A technical secretariat staffed partly by domestic officials and partly by secondees from multilateral partners provides the expertise boards need without creating permanent dependency. AI can accelerate this further.[35]

32. This extends to DaaS providers: the regulator does not select them, but does set the qualification criteria they must meet.
33. Pix is a partial exception. The Central Bank of Brazil designed it, mandated participation, and regulates the private rails it now competes with, i.e., the conflict this principle warns against. Pix's success shows the cost of skipping it.
34. Pix's design has also drawn international trade friction: the US imposed Section 301 tariffs on Brazil, citing Pix's fee-free structure; Brazil disputes the characterization since such governance choices can carry consequences beyond the country that makes them.
35. The World Bank GovTech AI program trains government teams in low- and middle-income countries to deploy practical AI tools for public administration, the same capacity-through-doing model this principle proposes, applies to digital infrastructure governance.

Principle 7: Private sector innovation is the purpose, not a byproduct. The entire governance architecture exists to create conditions for private innovation. Open rails with clear and stable standards are the signal private actors need. India's 500-plus fintech ecosystem built on UPI, Brazil's fintechs leveraging access to Pix, and Estonia's 900-organisation data exchange ecosystem on X-Road are not government achievements—they are private sector achievements made possible by governance quality. The same logic lies behind Singapore's regulatory sandbox, which lets firms test live financial products under temporarily relaxed rules rather than waiting years for full licensing. Governance success is measured not by the quality of board deliberations but by the volume and diversity of private innovation and consumer protection the framework enables. The largest private actors and telecoms have a direct financial interest in governance quality. Capturing their co-investment in governance architecture is one of the framework's most neglected opportunities.[36]

Principle 8: Consumer protection is a design requirement, not an afterthought. The speed and frictionlessness that define effective digital infrastructures create consumer vulnerability as well as value. Fraud prevention, scam detection, and liability frameworks must be embedded in the governance architecture from inception. This means clear allocation of liability between platform operators and government; mandatory reimbursement frameworks for fraud; and cross-border coordination mechanisms for scam prevention. The public anchor's responsibility extends beyond interoperability standards to ensuring the rails it mandates are safe for the people who depend on them.

Domestically, "public anchor, private engine" is increasingly well understood. Internationally, the same recognition has not yet taken hold: governments that readily separate anchor from engine at home rarely extend that logic to cross-border coordination.

b. Frameworks across borders

Sound domestic governance is the foundation of all national frameworks. But a world of well-governed national digital infrastructure systems that cannot talk to each other has solved half the problem. The farmer in Kenya still pays extortionate fees to receive remittances from London. The entrepreneur in Brazil faces analogue friction the moment she trades internationally.

The within-country model does not simply scale. Domestically, a sovereign sets rules; a regulator enforces them; the private sector complies or exits. Across borders, no sovereign has authority over the whole system. Best practices must be agreed on, not mandated. Compliance must be coordinated across many regulators, not enforced by one. Structural issues compound this challenge: cross-border compliance costs vary by jurisdiction, and data

36. The World Bank GovTech AI program trains government teams in low- and middle-income countries to deploy practical AI tools for public administration, the same capacity-through-doing model this principle proposes, applies to digital infrastructure governance.

No institution today has the authority to set standards that countries will actually adopt. The response is not to create one. Rather, it is to use the forum where sovereigns already make commitments.

ownership remains legally unsettled in most countries. None of these issues should delay the governance of digital infrastructures—it should shape how governments, the private sector, and civil society build it together.

The cross-border architecture comprises of three layers, each closing one or more of the three gaps.

Political commitment closes the governance gap. No institution today has the authority to set standards that countries will actually adopt. The response is not to create one. Rather, it is to use the forum where sovereigns already make commitments. The G20 Sherpa track is that forum. Sovereigns should commit through the Sherpa track to binding interoperability principles—openness, portability, privacy by design, and the capacity to connect—with private sector input embedded from the start. Industry knows which standards are technically feasible, and which will be quietly ignored. Political commitments made without that knowledge tend to be aspirational rather than operational.

Institutions are needed to implement visions and tackle the accountability gap. The G20's record on follow-through is uneven. The unfulfilled commitment to a Global Digital Public Infrastructure Repository cited in this paper is evidence of the governance gap and is itself a G20 failure. The G20 works best when it generates political momentum that existing institutions then operationalize. The Sherpa track is asked to do only what the G20 does reliably (i.e., secure heads-of-government level political commitment to a set of principles). Implementation is deliberately routed through institutions: the Finance track's regulatory bodies, IMF, World Bank, and regional development banks.

Regulatory convergence closes the governance and accountability gaps. The G20 Finance track is where technical substance is decided. It already houses the institutions that made cross-border financial regulation and tax effective: the Financial Stability Board, Committee on Payments and Market Infrastructures (CPMI), BCBS, and OECD. The CPMI is the natural home for payment rail and technical specifications, with the OECD providing the broader policy framework.

This framework addresses the accountability gap. The absence of any body equivalent to Basel for banking has left digital infrastructures without a mechanism to certify compliance or coordinate responses when infrastructure fails. The Finance track provides that mechanism and private sector representation in the Finance track is a design requirement. The firms bear the cost of compliance and the risk of systemic failure. Standards shaped without their accountability will not hold.

Private sector co-authorship of standards requires more than a seat at the table. The Basel process offers the template: clear separation between standard-setting and compliance, and regulatory bodies retaining explicit override authority so that standard-setting cannot be captured by incumbents protecting proprietary systems. This is precisely the architecture

that has made Basel durable across decades. What digital infrastructures currently lack is the application of its architecture at the international level. This should not be a new invention, but rather an extension of a proven model to a domain that has so far escaped it but with a governance structure that both currently lack. This structure needs to place emerging markets at the table from inception.

Universalization closes the adoption gap. The G20 has 20 economies with only indirect representation of many others. The countries most in need of digital infrastructures have no seat of their own at the G20.

Three institutions are in a position to bridge that gap.

(1) The IMF's 190-member surveillance function extends agreed standards to every economy, recognizing adoption and supporting those that have not yet achieved it.

(2) The World Bank translates standards into implementation—financing conditioned on interoperability alignment creates both the incentive and the support to adopt.

(3) The regional development banks are the critical last mile: regional legitimacy, deeper government relationships, and a structured channel for non-G20 countries to feed implementation experience back into standard-setting.

In the near term, regional development banks have the operational latitude to move ahead of the larger institutions. Regional trade agreements are one such channel: the EU-Mercosur accord shows plurilateral groups building shared digital-trade rules ahead of global consensus. But these are useful only as inputs to common best practices, not substitutes for them—a regional standard that never scales beyond its bloc reproduces the fragmentation.

Assigning roles to the IMF, World Bank, and regional development banks raises an obvious objection: these are not institutions known for speed, agility, or digital expertise. Their procurement cycles are long, and their staff expertise has been built around roads, power, and water rather than platforms and protocols. These are real constraints, and a framework that ignores them will not survive contact with reality. The World Bank's shift toward policy loans is a structural fit for financing digital infrastructure specifically.

Three mitigations apply here.

- First, the regional development banks have demonstrated more operational flexibility and should move first. This does not mean regional implementation proceeds outside of G20 oversight: regional development banks and country-level experts already participate in G20 working groups as invited contributors, feeding implementation experience back into Sherpa-level review as it develops.

- Second, conditionality frameworks—financing conditioned on interoperability alignment—create institutional incentives to develop digital expertise.
- Third, the Digital Chapter embedded in existing instruments is a reporting and assessment function. The international financial institutions are not asked to become something they are not. They are asked to do what they already do—country assessment, standard-setting, and financing—for a domain they have so far underweighted.

Cross-border interoperability is the frontier at which the hardest implementation challenges remain unsolved, a claim this paper does not dispute. Pricing is the most persistent: the G20 has maintained a roadmap to reduce cross-border payment costs with limited progress, not because the technical infrastructure is lacking but because incumbent pricing structures create powerful incentives against change that governance frameworks alone cannot dissolve. Part of the resistance comes from compliance and Know Your Customer requirements, not pricing power alone. Different levels of system maturity create a second layer of friction: connecting a sophisticated, decade-old payments infrastructure to a nascent system creates both arbitrage opportunities and security vulnerabilities.

Last-mile access remains broken in many contexts even when core infrastructure functions—digital literacy gaps and trust deficits sit between a technically functioning digital infrastructure, the development of effective end-user applications, and their actual adoption by the people it is designed to serve. And downstream adoption friction—use cases mismatched to real needs—means that technical interoperability does not automatically produce economic inclusion. The governance architecture is a necessary condition for addressing these challenges, but not a sufficient one. Closing the governance gap creates the institutional home in which pricing reform and adoption friction can be systematically worked through. Without it, these problems are addressed piecemeal. With it, they become a defined agenda rather than an open frontier.

Between domestic governance and global interoperability lies a tier the paper's framework explicitly recognizes: regional coordination. Even technically sophisticated countries have concluded that maintaining independent back-end payment infrastructure is too costly and too fragile. The Nordic central banks determined that running their own payment systems independently was neither efficient nor sustainable and moved toward consolidation around European Central Bank infrastructure. The case for regional coordination in Africa, Southeast Asia, and Latin America is decisive. Africa's Pan-African Payment and Settlement System represents exactly this logic—shared back-end infrastructure at the regional level. The framework proposed here should explicitly encourage and support regional coordination as the near-term path. Global standards set the destination; regional coordination is the road most countries will actually travel.

The sequencing matters as much as the architecture. The instinct to begin with global consensus has a poor track record. Global initiatives stall because reaching agreement across 190 economies takes longer than the technology will wait for consensus. The more realistic path runs in the opposite direction: regional coordination first, global standards second. The Single Euro Payments Area demonstrated that a region can build shared payment infrastructure without waiting for global consensus. Africa's Pan-African Payment and Settlement System is demonstrating the same today—regional initiatives that are building the evidence base from which credible global standards can eventually be derived rather than imposed. The G20's role in this framework is not to design the global system but to create the political conditions under which regional systems can interoperate.

There is an urgent need to start a BIS Innovation Hub Center in Africa. One gap in the current institutional landscape demands a specific response: Africa has no BIS Innovation Hub, and no equivalent source of the technical assistance, and implementation support that the Hub provides elsewhere. Africa is where the adoption gap is most acute where the absence of vendor-neutral technical guidance leaves countries most exposed to proprietary lock-in and fragmented systems.[37]

Together, the domestic and cross-border frameworks express a single logic: a public anchor sets standards, private actors deliver, and accountability measures outcomes. Domestically, the anchor is a sovereign and its regulators. Across borders, it is a coalition of sovereigns acting through the G20 and the international institutions. The private sector's role expands as borders are crossed—from engine of domestic delivery to co-author of the global standards. The fundamental architecture does not change: separate authority from execution, embed interoperability from the start, and hold the system accountable to the people it serves.

c. From Digital Chapter to Digital Framework Report: Building Country Ownership

Digital infrastructures generate data at scale—every payment transaction, every identity verification, every health record, every agricultural exchange that passes through digital infrastructure creates a data trace. That data is the raw material from which AI systems are trained. The design choices embedded in digital infrastructures—who sets the standards and who audits the infrastructure—determine the conditions under which that data is used. Countries that govern their digital infrastructures well are shaping the environment in which their AI future develops. Digital infrastructure governance is urgent: the infrastructure being designed today will determine what AI systems learn from them.[38, 39]

37. The BIS Innovation Hub Center in Singapore is the natural conduit to extend that mandate to Africa Hub as it is already running Project Nexus and Singapore has the technical expertise and emerging market relationships. Site selection normally favors a BIS member country with financial-hub capacity—a combination only South Africa currently offers in sub-Saharan Africa.
38. For a framework governing data at the national level, including the ORGANS principles (Open, Revocable, Granular, Auditable, Notice, Secure) for consent-based data sharing and evidence from India's Data Empowerment Protection Architecture as a working model, see S. Tiwari et al., "The Design of a Data Governance System," BIS Papers, no. 124 (Bank for International Settlements, 2022). The authors note that cross-border data governance interoperability remains unaddressed—precisely the gap that digital governance frameworks must fill.
39. The eight principles are built for digital infrastructure governance specifically; extending them to directly govern how digital infrastructure-generated data is used to train AI systems is a related but separate task this paper does not undertake.

The most durable governance frameworks are those built on domestic ownership rather than external compliance. The lessons from poverty reduction programs make clear that the quality of multi-stakeholder consultation matters. Countries that genuinely consulted stakeholders produced better outcomes than those that treated poverty reduction strategies as a donor compliance exercise.

A parallel instrument for digital infrastructure governance should draw on this lesson while avoiding the poverty reduction exercises' well-documented pitfalls—its tendency to become a formulaic document rather than a genuine national strategy. The framework proposed here builds domestic ownership progressively.

In the first three years: a Digital Chapter embedded in existing instruments. For low-income countries, a structured digital infrastructure section added to the Poverty Reduction Strategy Paper. For middle-income countries, a Digital Annex integrated into the Article IV consultation. The Digital Chapter follows a standard template—covering digital infrastructure development strategy and compliance with the eight principles. Digital Chapters also generate the repository of governance practices and implementation lessons that the G20 committed to create in 2023. They can also be valuable communication pieces to the private sector.

Around year three: a Digital ROSC. After three years of Digital Chapters, a country has a track record of gaps identified. The Digital ROSC evaluates progress against a known baseline, and provides the external validation that anchors the transition to standalone reporting.

From year four: a standalone Digital Framework Report. It is country-owned, multi-stakeholder report grounded in accumulated experience rather than assembled from scratch. The Digital Framework Report consolidates what the Digital Chapters established and produces a national digital infrastructure strategy anchoring IMF lending and World Bank financing. It is not a government document. It is a national document—produced through a multi-stakeholder process that includes the private sector, civil society, the telecoms, and the technology platforms. A Digital Framework Report produced without genuine private sector and civil society input is a compliance document.

The architecture of governance, like the architecture of digital infrastructure, is best built in layers. Starting with a chapter embedded in existing processes sidesteps the political resistance that conditionality invites. By the time the standalone Digital Framework Report is introduced, countries have three years of experience and the instrument feels like natural evolution rather than imposition. Digital infrastructure systems are being deployed today. The governance choices are being made this year and next.

Data sovereignty without compute sovereignty is incomplete. The AI systems that grow on digital infrastructure-generated data require chips and energy to run them—resources that are concentrated in a small number

Digital infrastructure systems are being built now, and the standards, ownership structures, and habits of cooperation set during this period will be difficult to unwind later.

of countries and companies. This paper does not develop a framework for compute and energy governance. A country which governs its data infrastructure while remaining entirely dependent on foreign compute will find its sovereignty constrained. The governance agenda this paper addresses is necessary but not sufficient: it is the foundation, and the foundation must be built first.

VIII. Conclusion: Digital Infrastructure of the Next Economy

Statecraft and marketcraft are not two projects here, but one. The same design choice that lets digital infrastructure power growth is what keeps it governed. The tools to do this already exist—inside the G20, the IMF, the World Bank, and the regional development banks—and none of them need a new mandate. What has been missing is not capacity but the decision to point it at this problem, the way the world once did for banking, aviation, and telecommunications.

That decision cannot wait for the hard problems—pricing, system maturity, last-mile access, the widening gap between countries with strong digital foundations and those without—to resolve themselves first. They won't. What a governance architecture changes is not the difficulty of these problems, but whether countries face them together, year after year, or alone.

The window for that choice is this year and next. Digital infrastructure systems are being built now, and the standards, ownership structures, and habits of cooperation set during this period will be difficult to unwind later. The data these systems generate will also train the AI systems built on top of them. Thus, the governance choices made now will shape not only how money and identity move, but what the next generation of AI learns from that movement. That stake did not exist the last time payments infrastructure was redesigned at this scale. It exists now, and it raises the cost of waiting.

Nothing here asks a government or institution to become something it is not. It asks each to do, in this domain, what it already knows how to do elsewhere. The tools are not the constraint. The will to use them, in time, is.

Annex
Official Sector Activity

The global development community has mobilized significant resources around digital infrastructures since the COVID-19 pandemic revealed digital capabilities as essential. India's 2023 G20 presidency catalyzed unprecedented consensus, with the G20 members agreeing on a digital infrastructure framework encompassing digital identity, payments, and data exchange.[40] The momentum has generated substantial activity across multilateral organizations and philanthropy demonstrating both the urgency of the agenda and the fragmentation of current efforts.

a. Multilateral Agencies

The World Bank and IMF have begun integrating digital infrastructure but through different mechanisms. The World Bank's IDA21 replenishment ($100 billion, December 2024) elevated Digital Transformation to one of five core focus areas.[41] The Bank's ID4D initiative has catalyzed $2.3 billion for digital identity systems benefiting 550 million people across 60 countries, while G2Px supports 35 countries digitalizing government-to-person payments affecting 120 million recipients. The World Bank's approach articulates principles related to interoperability, modularity, and security that align with the G20 framework.[42]

The IMF has integrated its work on digital infrastructure primarily through research and capacity development rather than lending operations. The IMF Fiscal Affairs Department established a GovTech initiative focusing on digitalization of public financial management, tax administration, and treasury operations as well as bringing country practitioners and experts to share implementation lessons. IMF research reinforced the benefits of embracing digital infrastructure. However, the October 2024 Poverty Reduction and Growth Trust Review, despite comprehensively addressing financial sustainability, debt management, and access policies, made no mention of the central role of digital infrastructures.[43]

The Organisation for Economic Co-operation and Development (OECD) has been actively advancing work on digital public infrastructure by promoting policy frameworks, best practices, and international cooperation to enhance digital transformation, data governance, and inclusive access to technology across its member countries.

Together, these institutions demonstrate progress and persistent gaps. The World Bank has operationalized support through dedicated initiatives but focuses on broadband connectivity and government digitalization rather

40. G20 Digital Economy Ministers, G20 Digital Economy Ministers Meeting: Outcome Document and Chair's Summary, Bengaluru, August 19, 2023, paras. 6–8 and Annexure 1, para. 7. https://g7g20-documents.org/database/document/2023-g20-india-sherpa-track-digital-economy-ministers-ministers-language-g20-digital-economy-ministers-meeting-outcome-document-and-chair-summary
41. World Bank, "A Record Funding Round Replenishes the Best Deal in Global Development," December 16, 2024. https://www.worldbank.org/en/news/feature/2024/12/16/a-record-funding-round-replenishes-the-best-deal-in-global-development; International Development Association, IDA21 Policy Package: The Focus Areas Paper, World Bank, June 2024.
42. World Bank Group, Digital Public Infrastructure and Development: A World Bank Group Approach (World Bank, 2025). https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099031025172027713
43. IMF, 2024 Review of the Poverty Reduction and Growth Trust Facilities and Financing—Reform Proposals, IMF Policy Paper No. 2024/047, October 2024. https://www.imf.org/-/media/files/publications/pp/2024/english/ppea2024047.pdf

than comprehensive digital infrastructures with mandated interoperability. The IMF has the analytical capacity to translate understanding into program design or financing mechanisms. Neither has established frameworks ensuring digital infrastructure meets international standards for interoperability, security, and privacy. Regional development banks have launched initiatives, but digital infrastructure has not achieved comparable coordinated mobilization.[44] In fact, no institutional capacity to establish dedicated financing envelopes and conditionality frameworks for cross-cutting development priorities exists for digital infrastructures, leaving it confined to technical assistance rather than integrated into the structural reform programs that shape country policy frameworks.

b. United Nations and Standard-Setting Bodies

The Financial Stability Board and Bank for International Settlements (BIS) examine digital payments and central bank digital currencies and focus on public infrastructure design in the payments space. The International Telecommunication Union (ITU), responsible for telecommunications standards since 1865, has begun extending its mandate toward digital infrastructure but faces jurisdictional ambiguity. The ITU sets technical standards for connectivity and cybersecurity but lacks authority over the application layer where digital infrastructures operate. No equivalent to the ITU exists for digital infrastructure.

The United Nations has positioned digital public infrastructure as critical for achieving Sustainable Development Goals by 2030. The United Nations Development Programme (UNDP) established specialized teams focused on the implementation of digital infrastructure, developing a universal safeguards framework through multi-stakeholder consultations culminating at the September 2024 Summit of the Future. This framework addresses principles, methods, and practices for responsible deployment of digital infrastructure, with pilots in five countries. UNICEF advances digital identity for children and digital learning platforms, while UN Women integrates gender considerations into digital infrastructure design to prevent exclusion and bias.

The G20's 2023 framework represented breakthrough consensus but created no implementing institution. The commitment to establish a "Global Digital Public Infrastructure Repository" remains unfulfilled. Countries agreed on principles—interoperability, inclusivity, security, privacy—but established no mechanism to enforce them, no certification process to verify compliance, no technical assistance structure to support implementation. Individual countries are left to interpret principles independently, risking incompatible national systems despite common rhetorical commitments.

44. For example, the African Development Bank's Mission 300 commits to electrify 300 million Africans by 2030.

c. Bilateral Donors and Philanthropic Initiatives

Bilateral development agencies have launched targeted digital infrastructure programs. Before its closure, U.S. Agency for International Development's Digital Strategy emphasized digital identity and payments infrastructure across priority countries. The UK's Foreign, Commonwealth & Development Office supports digital public goods through partnerships with organizations such as MOSIP (Modular Open Source Identity Platform), which provides open-source digital identity solutions deployed in the Philippines, Morocco, and Ethiopia. Germany's GIZ implements digital governance programs emphasizing data protection and privacy frameworks.

The Gates Foundation has positioned digital infrastructures as central to its development strategy, co-convening the 2024 Global Digital Public Infrastructure Summit and providing substantial funding for digital identity and payment infrastructure projects. The Omidyar Network supports open-source digital infrastructure development and advocates for governance frameworks protecting individual rights. The Rockefeller Foundation has defined digital infrastructures as fundamental infrastructure for the digital age[45] and championed digital public infrastructure as a catalyst for equitable development.

Carnegie India's work focuses on (i) shaping outcomes on Digital Public Infrastructure (DPI) principles; (ii) providing practical roadmaps for alternative ways to build DPI rapidly; (iii) DPI at the center of inter-state dialogues; and (iv) working with DPI builders, architects, and implementers. The Brookings Institution has explored digital public infrastructure through research and analysis, focusing on its potential to drive inclusive economic growth, improve governance, and enhance public service delivery, while addressing challenges such as data privacy and equitable access. The Digital Impact Alliance is providing research, tools, policy through country engagement on DPI.

These philanthropic efforts generate innovation and pilot programs but lack the scale and coordination to establish global standards or ensure interoperability across national implementations.

45. Observer Research Foundation, Digital Public Infrastructure: Defining a New Framework for Economic and Social Prosperity (ORF, 2021). https://www.orfonline.org/