Finternet: technology vision and architecture

A user-centric, unified, and universal approach for our financial future

Nandan Nilekani (@NandanNilekani)
Pramod Varma (pramod@becknprotocol.io, @pramodkvarma)
Siddharth Shetty (siddharth@siddharthshetty.com, @imsiddshetty)

We would like to express our gratitude to Anusree Jayakrishnan for her contributions to the digital public infrastructure section of this paper. We also acknowledge the assistance provided by GPT-4, which was instrumental in editing, framing, and summarizing the content presented herein.

This paper builds upon and extends the ideas presented by Carstens and Nilekani (2024) in their work, "Finternet: the financial system for the future."

Abstract

The Finternet is a framework for interconnecting multiple financial ecosystems inspired by the structural principles of the Internet. Its primary aim is to empower individuals, businesses, and numerous other organizations by placing them at the center of their financial lives. It will facilitate seamless integration across various financial services, enhancing accessibility and efficiency.

The proposed architecture emphasizes user-centricity, unification (across asset categories, sectors, and geographies), and universality with a focus on ensuring that the financial services ecosystem is adaptable to the needs of a diverse international user base of individuals and organizations, retail and wholesale. Key to this architecture is its interoperability across systems and scalability, which enables a wide range of financial transactions across different platforms and legal frameworks. The initiative prioritizes inclusion and innovation while balancing security, privacy, and compliance with regulatory standards to build trust and reliability in financial transactions.

The Finternet model advocates for collaborative efforts between public and private sectors to establish a universal digital infrastructure that promotes financial inclusivity, and empowerment, and enables a new set of exponential innovations as seen during the Internet era. This paper presents the Finternet as a concept aimed at creating a more equitable financial environment, highlighting its potential to facilitate economic engagement and growth on an international scale.

Table of Contents

1. State of the current economic system

The digital finance landscape, while brimming with potential for innovation and improved service delivery, contains many challenges that impede its progress. These challenges span across various domains, including institutional structures, governance mechanisms, technological infrastructure, and the roles played by private sector innovation. Central to these issues are the high transaction costs, often exacerbated by vendor lock-in and a dependency on isolated, non-interoperable technologies. This situation not only elevates operational expenses but also complicates the financial ecosystem, making services less accessible and increasing complexity for both users and providers.

Governance issues manifest in the difficulty of coordinating between different regulatory bodies and implementing systems that span multiple sectors and service providers. Regulatory frameworks, such as Know Your Customer (KYC) protocols, are essential for maintaining security and compliance but often result in tedious and slow processes. The fine line between ensuring stringent regulation to maintain system integrity and fostering an environment conducive to technological innovation is hard to tread. Too strict regulations may hinder technological evolution, while too lenient ones could compromise the system's stability, safety, and the trust of its users.

The consumer experience in traditional financial setups, characterized by limited choice and reliance on paper-based systems, leads to slow, costly, and fraud-prone operations, which further deters digital adoption. Despite the emergence of neobanks and digital banking solutions, these alternatives struggle to scale and integrate within the broader financial ecosystem, primarily due to outdated infrastructures and limited collaboration.

This fragmented financial landscape, marked by discrepancies in technology access and financial literacy, creates a high-friction, high-cost, low-innovation environment prone to fraud and complexity. The resultant digital divide not only limits the reach of financial services but also highlights the necessity for an inclusive approach to digital finance reform, prioritizing both technological advancements and regulatory frameworks that support growth, security, and accessibility.

The current intermediation processes, characterized by extensive bilateral contractual requirements, manifest a high-friction, costly environment that hinders widespread adoption and fails to generate significant network effects. Solutions to these challenges must therefore be cost-effective to implement and capable of

generating new revenue streams for participants, fostering a more inclusive financial ecosystem. Addressing these issues necessitates an overarching strategy that not only improves access, reach, and digital literacy but also enhances customer choice and streamlines service delivery through automation, effectively minimizing the dependence on manual processes and intermediaries.

The financial sector is on the brink of significant evolution, with emerging trends and technological advancements paving the way for a new era in financial services. This period of change is reminiscent of historical shifts, where technology convergence catalyzed societal and economic transformations. The digital era has increased economic aspirations, pushing the demand for financial services that are accessible, customized, and efficient. This demand is coupled with a regulatory momentum aimed at fostering financial innovation responsibly.

The notion of universal access, bolstered by widespread internet and smartphone usage, is essential for bringing financial services to the broader population, including those in remote or underprivileged areas. Technological strides in cryptography and artificial intelligence (AI) are set to redefine the financial landscape, enhancing security and user experience while ensuring that financial systems are adaptable and inclusive. These advancements support the vision of the Finternet, a concept aiming to integrate and revolutionize financial interactions internationally. By bridging technological potential with regulatory clarity, the Finternet aspires to create a financial environment that is not only inclusive but also conducive to the collective economic advancement of society.

As we move forward, understanding these dynamics is crucial for designing ecosystems that are not only scalable but also robust and adaptable, as detailed in a later section on design principles. It's also prudent to examine previous attempts at population-scale transformations, identifying common principles of success, as further explored in the following section.

2. Experiences from building at a societal scale

Technology is a key enabler in driving large-scale societal transformations. It's also a great leveler, bringing transparency, and providing equitable access regardless of geographical or socioeconomic boundaries. Leapfrogging developmental outcomes involves creating new models of governance, adopting new technology, and restructuring systems to accommodate it. The Digital Public Infrastructure model shows the impact of technology on solving societal problems. The DPI movement is inspired by the open standards & specifications that created the Internet (TCP-IP,

HTTP, HTML, SMTP, etc) and mobile networks (GSM, SMS, LTE, etc) - which operated as the original digital infrastructure of the late 20th century, catalyzing a wave of public and private innovation that drove inclusion.

The core of a DPI is a framework for sustainable innovation via creating reusable, shared infrastructure that combines 1) the right technology architecture; supplemented by 2) governance frameworks that are transparent, accountable, and participatory; and 3) robust public and private market innovation.[1]

Policymakers, governments, and the private sector are pivotal in navigating societal transformations toward an uncertain future, often with a constrained perspective on emerging solutions. Digital Public Infrastructure (DPI) plays a crucial role in this context, not as a complete solution but as foundational infrastructure facilitating diverse innovations. DPI enables cross-sectoral inclusion and sparks innovation across essential services such as financial, healthcare, education, e-commerce, and energy sectors, setting the stage for extensive societal benefits and improved access to critical resources.

India has effectively utilized and scaled up DPIs to catapult its digital economy forward, bypassing decades of traditional progress. DPI has been instrumental in mass formalization, enabling access to services and facilitating seamless transactions across sectors. India's ID infrastructure (Aadhaar), the verifiable identity system (issued to over 1.39 Bn users), provides ultra-low-cost authentication and eKYC services. The country could leapfrog years of progress by enabling its citizens to access formal financial services and affordable mobile connectivity. Unified Payments Interface has revolutionized the payment landscape of India, making digital payments ubiquitous and affordable to the public. The payments sector witnessed a substantial leap; 1.5 Mn PoS terminals to 50 Mn merchant acceptance points, 50 Mn users to 500 Mn+ users of digital payments totaling over $2 Tn annually. Verifiable Credentials (VCs) issued on DigiLocker are a powerful means of personal data sharing—user-controlled, inclusive, multimodal (online/offline), and asynchronous. Their scale-up has been across various use cases, ranging from identity documents, vaccination credentials, and income certificates to grade cards, as evidenced by the 6.2+ Bn credentials already issued to over 249+ Mn users. The financial data sharing framework, also known as Account Aggregator[2], has empowered individuals and organizations with their financial data as digital capital, enabling them to control and share data for accessing various

[1] Definition of DPI from the Centre for Digital Public Infrastructure wiki - https://docs.cdpi.dev/
[2] https://sahamati.org.in/what-is-account-aggregator/

socio-economic opportunities. 2.2 Bn financial accounts are live on this infrastructure today.

Finally, open transaction networks (OTNs) for the discovery and fulfillment of goods and services across sectors (digital commerce, energy, healthcare, agriculture, mobility, education & employment) have helped people transact outside of closed platforms, ushering in a new era of innovation and equitable access. Open Network for Digital Commerce (ONDC)[3], a beckn[4] protocol powered open network has scaled to 530 cities and 28.3 Mn orders within just a year of its launch. Namma Yatri[5] is a peer-to-peer decentralized ride-hailing network using the beckn protocol, and it offers taxi drivers in India hail rides on their terms without the need for a central intermediary. Beckn protocol based Unified Energy Interface (UEI) is also now live in India enabling interoperable EV charging and energy exchange micro-transactions over a decentralized network.

DPIs have been architected with certain guiding characteristics that helped them reach the entire population. These have been outlined below:

a. **Reusability:** DPI can be thought of as shared building blocks that can be used by 3rd party ecosystem players to build solutions by combining with other blocks. This shared, building block nature of DPI powers many diverse, independent solutions and use cases to address diversity and continuous innovation. For example, a trade license issued as a verifiable credential can help SMEs get access to loans, direct government subsidies to the eligible accounts (using Government to Person payments infra), or digitally onboard them to various transaction systems.

b. **Enable Private Innovation:** The core of the DPI approach is how to design infrastructure that private players can leverage to give citizens access to affordable, inclusive access to products and services. Many private and public players (like financial institutions, and telcos) have leveraged the ID infrastructure to verify users to open over 500 million bank accounts and low-cost SIM registrations. Fintechs have used India's Unified Payment Interface (UPI) rails to create new categories of products like autopay, merchant soundbox[6], systematic investment plans, etc.

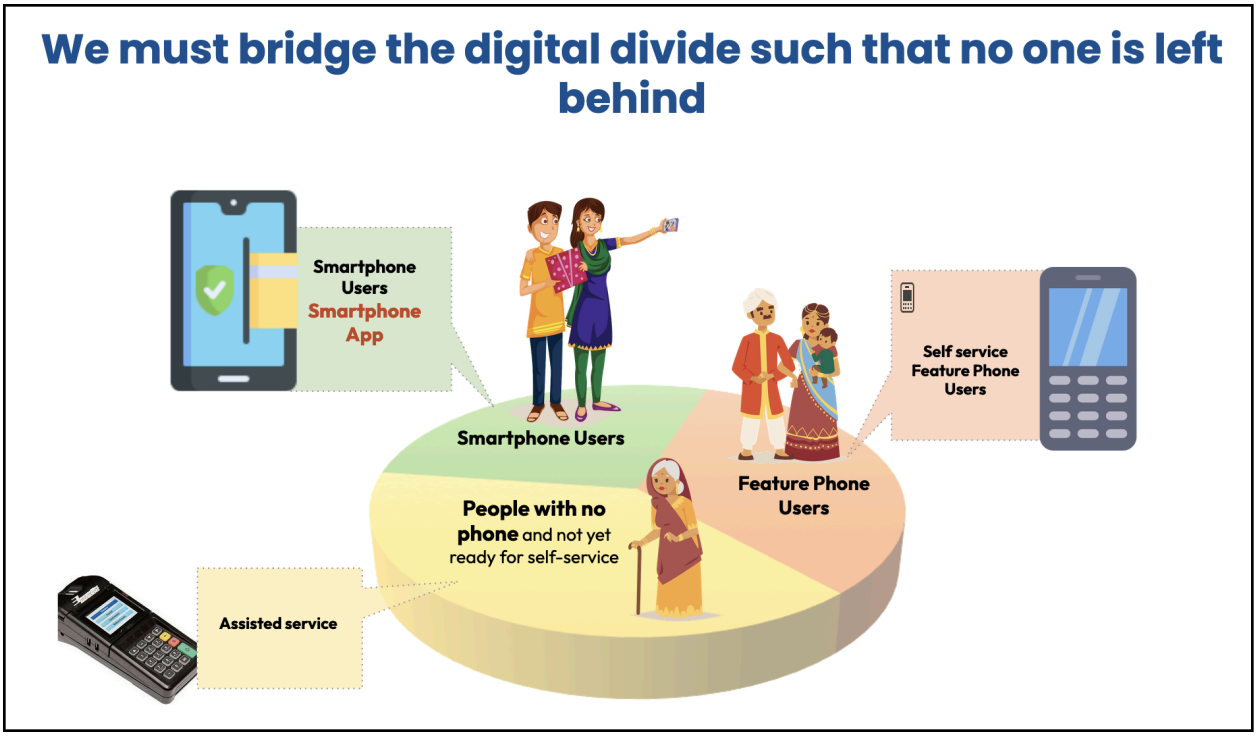
[3] https://ondc.org/
[4] https://becknprotocol.io/
[5] https://nammayatri.in/open?cr=usd&tl=at
[6] A low cost substitute for POS machines - https://business.paytm.com/soundbox

c. **Ecosystem adoption:** The end benefits of digital rails were carried to the users by an ecosystem of private and public players who created a business model using the said rails. Today, 500+ financial institutions are on India's Unified Payment Interface and 35+ third-party apps provide various financial services to 500 Mn+ users. India's financial data sharing infrastructure (Account Aggregator) has been implemented by over 600+ market players across public and private sectors, expanding the overall market for personal financial management, lending, banking, investments, and insurance.

d. **Unified Infrastructure, Diverse Experiences:** A unified approach can harmonize a wide array of stakeholders under a shared digital infrastructure while maintaining their operational autonomy. This architecture assigns specific roles to each participant, enabling each of them to leverage their strengths. For example, in systems like India's Unified Payment Interface, central bank-regulated entities manage the core financial transactions, while fintechs enhance the customer interface, ensuring diverse and enriched user experiences across the ecosystem. Voice and Indic language user experiences are expected to be launched this year to expand the diverse options.

e. Significant cost reduction: The creation of the DPI blocks that performed a few fundamental functions (like identity verification, digital payments, and data sharing) drastically brought down the cost of service delivery with the infrastructure itself being a low-cost intervention. With India's ID infrastructure and verifiable credentials, the cost dropped (from $6 to 0.4 cents) with verification becoming tamperproof and digital from manual and paper-based.

f. Inclusion at scale: Although the infrastructure backbone was digital, the system was designed to be used with a wide variety of interfaces to bridge the digital divide. For example, India's Unified Payment Interface (UPI) payment rails were designed to work for users across the economic and literacy spectrum. People with smartphones could use any of the apps on UPI, while people with feature phones could make payments via IVR or USSD. For the lowest income groups, UPI was also leveraged for assisted payments using biometric authentication.



g. **Minimalism** - India's digital infrastructure layers were designed to be minimal and generalized so that it can be combined easily into various application contexts. This approach, in addition to addressing reusability, also helped in accounting for the diversity. Many of these are inspired by the design of the Internet protocols and standards, GPS, etc.

h. **Asynchronous adoption:** It was necessary to design these assuming that various entities adopt these at different points in time. This allows different use cases, different actors, different sectors, etc to all adopt the infrastructure asynchronously. Ecosystem participants could come on board when they were ready to and saw the value in adopting the system. It relieved the pressure of convening all the stakeholders together.

There's a rising international focus on building digital infrastructure with many countries adopting this model to drive their digital transformation. Brazil has implemented an interoperable payments infrastructure called Pix, which has scaled to 42 billion transactions annually, leveraging the fintech ecosystem. Similarly, the Open Belem Mission[7], is the first city-wide open transaction network using beckn protocol in Brazil. The ambition is to position Bélem as a digital hub in the Amazon basin to link producers to local and international markets with climate resilience

[7] https://belemaberta.com.br/

and sustainability as the overarching guiding principles of the open network mission. Nigeria has a verifiable digital identity (NIN) that has enrolled over 100 million people and is now used at scale for low-cost SIM card registration, bank account opening, travel authorization, and more. Thailand's fast payments scheme, Promptpay has deployed an interoperable QR code infrastructure and has scaled to 3.7 million merchants as opposed to 140,000 merchants accepting debit/credit cards. Singapore is implementing a digital ID and credentials infrastructure named Singpass, which drives efficiency using digital ID. Many more nations[8] like Indonesia, Uganda, France, the USA, Bangladesh, Malawi, and Argentina have been moving towards building their digital infrastructure.

In addition to the digital infrastructure efforts across the world, there have been multiple efforts within the cryptographic world that have been making similar attempts to solve the problems outlined in this paper. Some of these efforts have been detailed below.

[8] Non-exhaustive list

Current crypto efforts across the world

Web3 refers to the vision of an open, decentralized web, where users have more control over their data and interactions online. It incorporates various decentralized technologies, including blockchain, decentralized storage, and identity solutions, to enable more forms of value creation and exchange. The core tenets of web3 are decentralization, openness, and transparency.

DeFi: DeFi encompasses a broad range of financial applications built on blockchain networks, aiming to decentralize traditional financial services such as lending, borrowing, trading, and asset management. Projects like Compound, Aave, and Uniswap are notable examples within the DeFi space.

Bitcoin: Introduced decentralized digital currency, revolutionizing the concept of money and store of value. As of March 2024, Bitcoin has a market capitalization exceeding $1200 billion, with over 460 million Bitcoin wallet users worldwide.

Ethereum: Pioneered smart contracts, enabling the creation of decentralized applications and tokens, fostering innovation in DeFi and beyond. Ethereum-based projects have raised over $40 billion through Initial Coin Offerings (ICOs) and token sales since its inception, powering a vibrant ecosystem of DApps and protocols.

Hyperledger: Hyperledger is an umbrella project of open-source blockchains that hosts over 300 member organizations, including leading companies like IBM, Intel, and Oracle, driving collaborative efforts to advance blockchain technology.

Corda: Corda is a blockchain platform designed for businesses to create interoperable, permissioned networks. Corda's ecosystem comprises over 300 technology and service providers, with deployments spanning industries such as finance, healthcare, and supply chain management.

These are just a few examples of pioneering technology that places the user at the heart of digital evolution. They collectively represent a movement towards user-centricity, ushering in a future where individuals have absolute control over their online presence and financial transactions.

Finternet stands as the natural evolution, combining the learnings and design principles of multiple schools of thought to create an inclusive, robust technology infrastructure with multiple levels of governance.

The establishment of common protocols, specifications, standards, and shared infrastructure services are critical pillars in the development of digital ecosystems. By defining a uniform protocol or set of guidelines—much like how the simplicity and universality of URLs have streamlined access to web content across the globe—common standards ensure interoperability and compatibility across different systems and platforms. Similarly, the concept that "a website is a website" regardless of its backend technology or hosting environment, showcases the power of standardized web technologies that empower developers and creators alike. This universal approach not only facilitates seamless integration and communication between disparate technological entities but also significantly lowers barriers to entry for innovators. When innovators are not constrained by compatibility issues, they can focus on building new functionalities and improving user experiences. Consequently, common standards and services unleash ecosystem innovation by providing a stable and consistent foundation upon which dynamic solutions can be developed and deployed across various sectors and industries. This not only accelerates technological advancement but also enhances the overall utility and scalability of digital solutions.

As we navigate through the complexities and challenges of the current digital finance landscape, it becomes evident that a shift in design principles is imperative to address these myriad issues effectively. The next section of this paper will delve into the specific design principles that can facilitate this transformation.

Going beyond platforms to open networks

Transitioning from a closed-loop, platform-centric digital world to an open-loop network-centric model significantly alters the dynamics of the digital landscape. This shift, characterized by interoperability and decentralization, counters the decline in competitiveness and the restriction of choices and autonomy previously seen. By encouraging the unbundling of services and promoting specialization, this approach mitigates reliance on any single platform. It fosters a more equitable and efficient ecosystem that supports innovation and collaboration across various sectors. This model enables barrier-free participation in the digital economy, ensuring that all entities—regardless of size, location, or demographic—have equal access. Such a paradigm amplifies opportunities and fosters a more inclusive, accessible digital environment, thereby enhancing the vitality and inclusiveness of the digital economy.

Open networks, unlike platforms, inherently possess the capability to scale through the interconnectedness and decentralized nature of their structure. Networks thrive on the principle of multiple nodes—be they individuals, organizations, or technology systems—interacting in an open and dynamic environment where each node can act independently and yet contribute to the growth and resilience of the entire system. This distributed model enables networks to expand exponentially as new nodes join and integrate, leveraging the collective capacity and diversity of the network without centralized bottlenecks or the scalability constraints often seen in platform-based models. Platforms, in contrast, typically operate under a centralized model that can limit scalability due to bottlenecks in capacity, control, and innovation. While platforms can efficiently manage and streamline processes under a unified system, they often struggle to adapt rapidly to change or scale beyond a certain point without significant restructuring or investment.

In essence, the scalability of networks is derived from their ability to organically grow and adapt through the contributions and interactions of an ever-expanding number of participants, making them superior in scaling compared to the more rigid and controlled environments of platforms. Therefore, we must envision the Finternet as a network of networks, where each network is self-contained with all the functionality for it to operate independently yet interoperable with others.

This will encourage diversity and flexibility, allowing each network to function independently while benefiting from a larger, interconnected ecosystem.

2.1 Addressing governance and consumer protection

Building successful digital infrastructure at a societal scale requires the incorporation of governance and consumer protection norms. This necessitates a multifaceted approach that includes establishing robust institutions, clear laws, and strong regulatory frameworks. Effective governance must encompass norms and regulations that ensure dispute resolution mechanisms are accessible and fair, enhancing consumer protection. It's also critical to promote digital inclusion and bridge digital divides to ensure equitable access to technology. Moreover, there must be accountability measures in place to address any harm that arises, maintaining trust and integrity within the system.

2.2 Going beyond digitization

Tokenization represents a significant evolutionary step beyond digitization in the way we interact with financial and real assets. Here's how it builds on these concepts:

1. Digitization refers to the process of converting physical information or processes into digital formats, primarily for internal use. For instance, turning paper records into electronic documents serves as a foundational step, focusing on creating digital replicas of existing physical entities. This process is essential for streamlining internal operations and enhancing accessibility within organizations. However, transactability across different enterprises often presents challenges.
2. Dematerialization takes digitization a step further by eliminating the need for the physical form. This is often seen in the financial sector where physical stocks or bond certificates are replaced with electronic records. This means that the asset doesn't need a physical counterpart to exist; its existence and ownership are recognized purely through digital records. Dematerialization also grants legal sanctity to the digital record.
3. Tokenization builds on these concepts by making digital representations of assets not only exact but also programmatically rich and operationally flexible, thus making them transactable, accessible, and affordable to all.

Unlike mere digital copies, tokenized assets become embedded with enhanced capabilities for transactions and management. This approach scales transactions exponentially, thanks to the inherent reach and efficiency of the internet. Each tokenized asset can contain embedded transaction capabilities, making each unit independently operable within an open, digital-first system. This integration allows for direct control and manipulation of assets' features and behaviors through programmed instructions, without relying on external systems or platforms. By making assets programmable, tokenization unlocks a new layer of functionality, enabling a wide range of transactions and interactions that are secure, immediate, and highly efficient. This not only increases the liquidity of assets but also broadens access to them, potentially transforming various sectors by enabling new models of ownership and exchange.

Building on the advanced capabilities enabled by tokenization, we can envision transitioning into a world characterized by low cost, high trust, high velocity, and richly innovative environments. This transformation paves the way for creating what could be described as "innovation playgrounds," where new ideas and business models can flourish without the traditional barriers associated with cost, complexity, and trust. The inherent efficiencies and capabilities of tokenized assets allow for rapid transactions and interactions, fostering a dynamic and responsive ecosystem. This setting not only supports but actively encourages innovation by reducing the friction typically associated with financial and asset management operations. Consequently, stakeholders can engage more freely, securely, and effectively, driving forward a new era of economic and technological advancement. This scenario presents a promising future, leveraging the full potential of digital transformation to create a more inclusive and prosperous world for all.

3. The three U's: User-centric, Unified, and Universal

The framework is designed to be:

- **user-centric**, serving the needs of individuals and organizations in both retail and wholesale sectors;
- **unified**, by integrating diverse asset types, across sectors, and across geographies over time; and
- **universal**, making it accessible to everyone—users, organizations, application builders, etc.

This section details each of the three concepts in detail.

3.1 User-centric: designing with users at the center

Adopting a user-centric approach means creating technology tools and policy frameworks that truly put the user in the center, empowering them to navigate and utilize these systems effectively. This empowerment is about providing solutions that are accessible and adaptable to the specific needs and challenges of individuals and organizations. It ensures that the technology and policies are not one-size-fits-all but are designed to enhance the agency and capability of each user. By prioritizing the needs of the user, these systems become enablers of success, helping individuals and organizations to thrive in a digital and interconnected environment. This shift towards user-centric design and policy-making fosters an ecosystem where technology and regulations actively contribute to unlocking potential, driving innovation, and ensuring that every user has the tools and opportunities to succeed in their endeavors. Delivering universal access to high-quality financial services is central to our vision. Such access is only possible when we place users – be they individuals or organizations – at the core of financial interactions.

The key attributes of such a user-centric system, summarized in Table 1, provide a blueprint for a digital economy that is truly by and for the user. This has been incorporated from the Finternet: the financial system for the future (2024) by Carstens and Nilekani[9].

Table 1: Key Characteristics of a user-centric Finternet		
#	**As a user, I …**	**Examples**
1	Could be any natural person or legal person	Individuals and legal persons (eg corporations, governments, non-profits, trusts, and partnerships)
2	Could use my electronically verifiable identities and verifiable attestations to participate in the ecosystem	***Identities***: Passport, national (digital) ID card, driver's license, birth certificate, social security number/card, bank cards, etc ***Attestations***: Investor accreditation, educational degrees, employment history, professional licenses /certifications, health /financial records, criminal background checks, social

[9] Finternet: the financial system for the future

		media, etc
3	Could authenticate myself and authorize transactions on any ledger of my choice	PIN, biometric verification, hardware token, SMS/email based, authorization chains, etc
4	Could create personalized integrated financial workflows	Rule-based transactions (i.e. pre-defined limits/caps on the amount/volume), transaction interlinking, delegation, etc
5	Could choose what data to reveal, how, and to whom	virtual addresses, aliases based on time/payee/amount, zero-knowledge proofs of personal data, etc
6	Could use any device for authorizing transactions	mobile phone, laptop, desktop, mixed reality headset, Internet-of-Things device, NFC tag and other form factors
7	Could send and receive any thing of value in any unit, any amount, to anyone, anywhere	Any asset (registered/ unregistered, regulated/ unregulated, attested /unattested), any amount, anyone (any natural or legal person), anywhere
8	Could manage my assets with any asset manager of my choice	Banks, brokers, asset management companies, depositories, etc
9	Should be protected from fraud, abuse, and bad actors	Know-your-customer and anti-money laundering, fraud monitoring/alerts, encryption and other secure cryptographic mechanisms, two-factor authentication, regulatory compliance checks, sanctions checks
10	Should be able to adhere to established legal norms	Banking law, securities law, taxation law, dispute resolution mechanisms, etc

3.2 Unified: across sectors, asset types, geographies, and time

Any to any, anyone, anywhere, anytime. In our diverse world, the convergence of technology with various systems and cultures calls for an approach that unites without enforcing homogeneity. By embracing diversity within systems, we ensure flexibility and robustness, preparing them to evolve sustainably in response to new challenges.

Internationally, the effort to connect disparate financial systems across geographical borders presents a complex challenge. It requires integrating varied

legal, technological, and operational frameworks to create a seamless international financial environment. This architecture must promote strong governance and efficiency without depending on uniform standards or centralization, thus accommodating the diverse regulatory needs of international stakeholders.

Ultimately, we must consider building a financial ecosystem that is internationally interconnected yet responsive to local needs, fostering economic activities that surpass geographical and sectoral boundaries, and nurturing continuous innovation and growth.

Below, we explore the essential attributes and capabilities that need to be unified.

1. **Any verifiable identity:** users can provide several digital identities for different purposes, enhancing privacy while maintaining accountability.
2. **Multi-layered proofing:** ability to dynamically apply proofing with differentiated strengths (user account, token, workflow, etc). This means user accounts at the core ledger layer need not have all the complexities of KYC and other proofing, rather these can be implemented at the flow allowing users to be onboarded easily and various attestations can be incrementally brought in based on the type of transactions they do.
3. **Any currency:** the ecosystem must support transactions in any form of currency and across currencies as determined by the respective regulatory authorities.
4. **Any asset:** allowing any type of asset, from physical goods to digital assets across sectors, from user-generated assets to regulated ones.
5. **Any jurisdiction:** any geographical region, country, or sector should be able to use the infrastructure and participate in flows that enable geographic or sectoral rules.
6. **Any form factor:** the system must be accessible across various devices, from mobile phones to no phones, accommodating different form factors and user contexts.
7. **Varied purpose:** the system must accommodate a multitude of objectives, from personal finance management to complex institutional operations, ensuring versatility and adaptability.
8. **Multiple asset managers and trust service providers:** users must be able to use any asset manager of their choice and layer on any additional trust service provider (like custodians, guarantors, verifiers, etc)
9. **Multiple legal norms:** the system must adhere to established legal norms and laws and any new norms that may be created over time
10. **Multiple standards for data:** there's no need to create one universal

standard for all data types, multiple data standards can be supported in an interoperable manner.

3.3 Universal: open technology, accessible to all

The vision of universal technology access is crucial. It requires the creation of open technology systems that enable the regulation of specific activities, similar to how financial activities are managed independently of the underlying technology like smartphones. Regulating the flows and activities atop a universally accessible technology balances regulation and innovation. If the technology infrastructure is not universally accessible, it could limit participation across different sectors or countries, adversely impacting both users and the stability of the overall system.

Like the Internet, we must ensure the technology infrastructure has no artificial boundaries or constraints that limit its use. To realize the vision of the Finternet, universal, unrestricted access (by users, organizations, adopters, application developers, etc) to infrastructure is essential. At the same time, financial flows, especially of the regulated asset types, can have rules and regulations applied at the flow level.

4. Asset types within the Finternet

There are diverse asset types that exist today, including cash and cash equivalents, stocks, bonds, mutual funds, ETFs, derivatives, commodities, foreign currencies, REITs, InVITs, cryptocurrencies, carbon credits, agricultural assets, infrastructure, precious metals, real estate, intellectual property, collectibles, and digital assets. Each of these varies based on their governance model, we've defined the 4 categories below:

A. **User-Controlled Assets**: Assets that users themselves create, manage, and transact among other users. Examples include Non-Fungible Tokens (NFTs), digital credentials, and personal physical/digital assets that are directly controlled and managed by the user.
B. **Attested Assets**: These assets are user-controlled assets but include additional attestations from third-party verifiers (like a gallery-attested painting), insurers, or guarantors to enhance trust and reliability.
C. **Registered Assets**: Assets that are officially registered with a public authority, like land or vehicles, which help confirm ownership and facilitate legal and regulatory processes.

D. **Regulated Assets**: These include assets like money and publicly traded securities, which are under strict regulatory oversight to ensure compliance with financial laws and to protect the interests of stakeholders.

We imagine the universal infrastructure of the Finternet can unify all the above four types under user control, still ensuring the application of rules and regulations as necessitated within type C and type D assets. This unification is essential to create combinatorial across types and sectors (e.g., a type B asset such as painting which is fully user-created and managed while still having the ability to interoperate with formal systems within the ledger to, say, obtain a loan).

4.1 Assets may have multiple types of ownership

Ownership structures for assets can vary significantly, accommodating different investment and management needs. Sole ownership grants one individual or entity complete control over an asset. Joint ownership divides rights among two or more parties, commonly used in real estate, enhancing collaboration. Multi-stakeholder ownership involves shared rights among several parties, suitable for corporate or community assets, facilitating collective decision-making. Lastly, fractional ownership breaks down assets into smaller portions, making high-value investments like art or property accessible to more investors.

4.2 Management of assets goes beyond ownership

Management of assets extends well beyond the scope of traditional ownership, embracing a broader array of property rights and claims. This includes real and personal property rights for tangible assets, intellectual property rights for creative works, resource-based rights for natural resources, usage rights such as easements for specific property uses, and financial claims like mortgages or liens. Such diversity in property rights enhances asset management flexibility, allowing for more nuanced legal and practical control, and can accommodate various innovative financial arrangements without the necessity of owning the asset directly. This approach not only simplifies transactions but also promotes broader market participation and liquidity.

In the realm of managing different types of assets, tokenization allows each right associated with an asset to be represented as a separate digital token, providing specific claims, entitlements, or responsibilities. This granular approach not only enhances precision and flexibility in managing asset-holder rights but also facilitates the independent management of these rights. For example, investors can

hold tokens for developmental rights or tenancy without owning the actual property, simplifying transactions, increasing liquidity, and opening up innovative financial opportunities. This system encourages broader participation in asset markets by allowing distinct and separate control over various property aspects.

4.3 Assets can be managed across jurisdictions

The borderless open architecture is designed to facilitate asset management across various jurisdictions, transcending traditional geographic and sectoral boundaries. This versatile framework supports:

1. **Cross-Sector and Cross-Border Regulation**: It allows for seamless asset flows not only between countries but also across different sectors within a single country, implementing a unified approach for the user that ensures high innovation, high efficiency, and high compliance regardless of jurisdictional nuances.
2. **Customizable Regulatory Enforcement**: Public authorities can apply specific rules based on the asset type and the jurisdiction or sector involved, including:
    - **Access Restrictions (who)**: Defining which entities can participate based on their role, location, or sector, utilizing mechanisms like whitelists or blacklists.
    - **Sector-specific and asset-specific Requirements (what)**: Tailoring rules to address the unique regulatory demands of different sectors, and asset types, ensuring that all transactions adhere to the relevant legal frameworks.
    - **Transactional Controls (how much)**: Limits on the size and frequency of transactions.

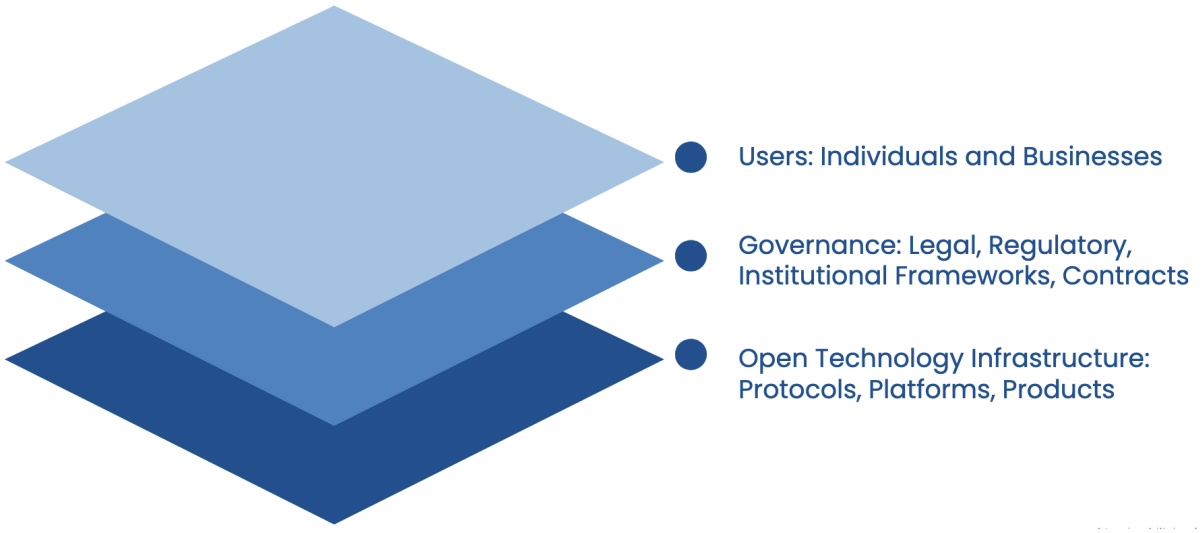
This framework enhances the interoperability and regulatory compliance of asset transactions, promoting a secure and efficient environment for the movement and management of assets across diverse legal and economic landscapes.

4.4 Balancing regulation and innovation with users at the center

To cultivate an ecosystem where regulators can govern and innovators can thrive, the Finternet must integrate open, universally accessible technology with regulated flows that permit the tokens, entities, and their activities tailored to specific asset types. Moreover, the implementation of strong certifications for the technology

guarantees reliability, security, privacy, and consumer protection based on rigorous testing and adherence to technical compliance standards.

Open Infrastructure, Regulatable Flows



10

In the realm of regulated and registered tokens, the enforceability of rules is paramount for consumer protection. Therefore, implementing the concept of "safe by design" embodies a foundational principle that prioritizes inherent safety and compliance within the financial ecosystem. This entails a programmatic enforcement of rules where the system architecture itself prevents non-compliant actions from being executed, effectively ensuring that only permissible activities take place.

Additionally, governance mechanisms can be individualized, allowing users to set their own rules, much like a person can with credit card settings—placing the person at the center of financial control. This capability speaks to the concept of "calibrated adoption," where the uptake of these financial instruments can be asynchronous, depending on individual comfort levels and regulatory landscapes.

However, it must be acknowledged that not all aspects of governance can be intrinsically embedded into the technology itself. Therefore, regulators, judiciary systems, and other public statutory authorities are essential in maintaining trust

[10] This diagram has been incorporated from the "Finternet: the financial system for the future" (2024) by Agustín Carstens and Nandan Nilekani.

within the ecosystem. These bodies are responsible for upholding standards and resolving disputes, effectively unbundling rules and regulations from the technological framework to make them accessible and equitable for all users. Such delineation also helps address risks, prevent exclusion, and combat fraud while ensuring consumer protection through established guardrails and enforcement mechanisms.

In this framework, all transactions and events between verified actors create a non-repudiable credentialed audit trail. This trail ensures accountability, as it provides incontrovertible evidence of actions taken within the system, supporting transparency and trust in the financial ecosystem. It also forms the basis of an automated model-based resolution system, which can handle disputes and irregularities efficiently, minimizing the need for manual intervention. When disputes do arise, mechanisms such as spot assessment, arbitration, and mutual negotiation come into play. These processes are designed to resolve conflicts swiftly and fairly, often leveraging an independent network of online dispute resolution providers. This network, established to complement the ecosystem, can leverage existing arbitration and mediation rules, as well as other legal norms, to provide at-scale grievance redressal and dispute management. This system aims to resolve conflicts effectively without overburdening the state's judicial capacity, thus ensuring a streamlined and efficient dispute resolution process that upholds the integrity and trustworthiness of the financial asset ecosystem.

5. Technology vision

5.1 Three traps to avoid

When implementing systems at the population scale in diverse environments, we strongly recommend avoiding three common pitfalls:

1. Standardization: Instead of imposing a single international standard or putting every stakeholder into one room to design a common standard, embrace multiple standards that allow for the coexistence of various data schemas. This approach respects the complexities and needs of diverse stakeholders and environments. This also allows evolvability into the future as these standards evolve.

2. Centralization: Rather than centralizing data and functionalities within a single system, opt for a decentralized network structure. This ensures better privacy, security, and governance by distributing control and responsibilities. This

also balances the power and control structures and ensures the technology infrastructure is truly universal.

3. Synchronization: Allow for asynchronous (at their own pace and point in time) integration of users, organizations, geographies, and use cases. This flexibility enables entities to engage with the system on their own schedules, accommodating different operational timelines and reducing friction during adoption.

Building on our understanding of the pitfalls in the implementation of population-scale systems—specifically the challenges of over-standardization, centralization, and synchronization—our next section outlines the guiding design principles and key technical characteristics. These principles are crafted to foster a resilient, scalable, and user-centric architecture. By emphasizing decentralized control, flexible integration, and diverse compliance standards, we aim to detail a robust framework that supports dynamic and inclusive digital ecosystems.

5.2 Guiding design principles and key technical characteristics

In the evolving landscape of digital ecosystems, the design principles we adopt are pivotal in shaping systems. This section delves into the core principles and key technical characteristics that should guide the development of the Finternet and equip it to meet current needs and anticipate future challenges.

Guiding Design Principles
As outlined in the Finternet: the financial system for the future (2024)[11], here are the guiding design principles that we must adopt: 1. **Users at the center:** The key rationale for developing the Finternet is to offer individuals and organizations access to the greatest possible range of financial services, in the most flexible way and at the lowest possible cost. The best way to achieve this goal is to prioritize the needs and wants of the system's users. In most cases, user priorities should guide technological and regulatory choices, not the other way around. 2. **Interoperability:** It is neither feasible nor desirable to build a single unified ledger to encompass all financial assets and transactions. Accordingly, unified ledgers will need to be interoperable with other parts of

[11] Finternet: the financial system for the future (2024) published by Agustín Carstens and Nandan Nilekani: https://www.bis.org/publ/work1178.pdf

the financial system. Ideally, such interactions will be seamless, enabling functionality across different protocols, platforms, and products. Interoperability will facilitate the creation of a "network of networks" to connect the diverse array of specialized networks that characterize modern financial systems. Such an interconnected framework significantly enhances the functionality and reach of each participating network. The emergence of such a complex system requires the development of consistent standards and protocols to enable interoperability while preserving the autonomy and integrity of each subsystem. This strategic, interconnected model aims to foster a financial ecosystem that is both more integrated and resilient, effectively responding to the sophisticated demands of modern finance.

3. **Evolvability:** The technological advances that motivate the development of unified ledgers will eventually be superseded. Accordingly, the Finternet should be able to evolve to accommodate future technological advances, while maintaining backward compatibility with existing systems where necessary. Such evolvability will facilitate continuous improvement and open avenues for innovation, by enabling new entrants to contribute meaningfully to the ecosystem's development. Adopting a pragmatic "+1" approach by leveraging existing systems as a foundation ensures a seamless transition towards more sophisticated technologies, balancing innovation with practical implementation.
4. **Modularity:** This principle highlights the importance of endowing the architecture with the capacity to evolve through discrete, independently modifiable layers, minimizing disruption across the ecosystem. Further, providing extensive programmability within the infrastructure is essential, enabling users to tailor functionalities to their unique requirements, and fostering a highly personalized and flexible environment.
5. **Scalability:** The scope and range of participants on the Finternet is likely to expand over time. Conceivably, this growth could be non-linear, as the introduction of new users and products enhances the value of the entire network, encouraging further growth. Accordingly, unified ledgers need to be able to accommodate such growth without compromising security and functionality.
6. **Division of labor and competition:** Public and private sector institutions both have roles to play in developing the Finternet. For the public sector, a key objective is to provide the "rails", which could include the core infrastructure, rules, and regulations on which private financial

institutions can operate. A key objective will be to promote healthy competition between private actors through open platforms, and a level playing field can support innovation and lower costs for end users by reducing rents. In this regard, policymakers should bear in mind that in today's system, inefficiencies are often someone's profit; accordingly, some resistance is to be expected and will require careful compromises. Creating an innovation-friendly atmosphere that supports combinatorial innovation allows for the blending of different technologies and methodologies, paving the way for breakthrough advances.

7. **Inclusiveness and accessibility:** Innovators are keen to leverage infrastructure with the ultimate goal of making financial activities universally accessible, affordable, and inclusive, ensuring no one is left behind. In the current financial services ecosystem, several constraints have emerged, presenting unique challenges yet opening avenues for innovation and improvement. Notably, the implementation of new technologies and systems has been met with high costs and operational delays, contributing to a slower pace of adoption across the board. This situation has inadvertently limited the empowerment of individuals within the financial ecosystem. The potential for widespread network effects – which could significantly enhance user empowerment and system efficiency – remains largely untapped. Such challenges underscore the need for a re-imagined approach that prioritizes affordability, flexibility, and inclusiveness in digital financial services. The architecture should aim wherever possible to serve any sector, be accessible on all devices, and cater to a wide range of purposes (from personal finance to institutional operations) while offering a choice of custodial services. It should support multiple data standards and integrate methods for determining the quality of assets, and respect existing legal norms.
8. **Security and privacy:** Last but certainly not least, the security of the infrastructure is a fundamental design principle. This pertains to security both vis-à-vis users and of the infrastructure at large. For one, a digital financial infrastructure should have adequate safeguards for data privacy and commercial secrecy, while ensuring system integrity by guarding against money laundering, financing of terrorism, and fraud. Moreover, strong institutional and legal safeguards to ensure operational and cyber resilience of the infrastructure should remain always and everywhere a first-order concern.

Complementing the design principles, here is a set of important technical characteristics:

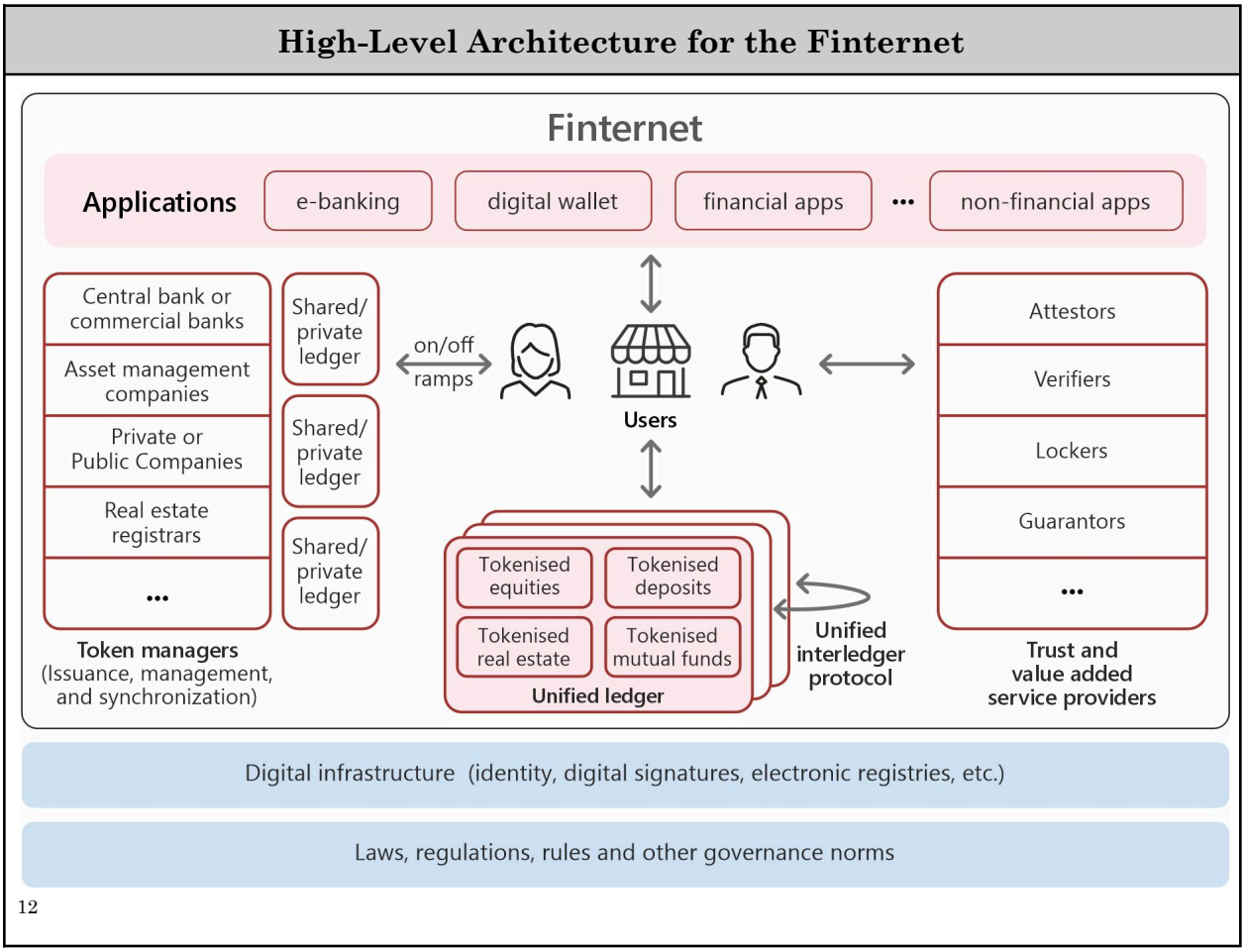
A. **Business Confidentiality**: provides an assurance that sensitive business information is accessed only by authorized parties, protecting trade secrets, strategies, and client details from competitive and unauthorized exposure.
B. **Composability**: is the capacity to combine different transactions or operations on a programmable platform.
C. **Enforceability**: is the mechanism by which a system, at the specific flow level, can ensure adherence to legal agreements, policies, or regulatory requirements, reducing the need for manual enforcement.
D. **Finality**: is the moment at which funds or assets, transferred from one account to another, officially become the legal property of the receiving party.
E. **Immutability**: is the characteristic of a system that prevents alteration or deletion, ensuring permanent and tamper-proof record-keeping.
F. **Multiplicity & Co-Existence**: ensures the support of simultaneous operation and interaction of multiple solutions and entities to cater to a spectrum of needs and scenarios.
G. **Non-Alterability**: The feature of a token that prevents any modifications post-creation, ensuring integrity.
H. **Non-Repudiability**: ensures that users cannot deny the authenticity of their actions, supported by irrefutable evidence such as digital signatures or tamper-proof transaction logs.
I. **Non-Tamperability:** ensures transactional data, environment data, and metadata cannot be modified by an unauthorized user.
J. **Observability**: provides visibility into necessary transactions and operations, essential for policymakers, regulatory agencies, and participants to effectively monitor for operational efficiency and compliance, detect fraud, and ensure accountability across the ecosystem.
K. **Portability**: The ability to easily transfer information from one environment. Portability is essential for interoperability between different systems and for the convenience of users who navigate multiple networks.
L. **Producibility**: The capacity to independently create one's token and at the same time no one can create a token in another's name.
M. **Programmability**: A feature of platforms and other technologies whereby actions can be programmed or automated.
N. **Replicability**: The ability to create exact copies of a token.
O. **Self-Describing & Self-Contained**: It refers to technical artifacts that contain sufficient information within themselves to be understood without

needing external references or additional data. This means the technical artifacts should inherently contain or convey key information about the entity they represent, such as their attributes, rights, or roles in the network. This characteristic aids in efficiency and clarity in transactions and interactions.

P. **Verifiability**: The ability to confirm the accuracy and authenticity of information or processes, allowing for trust and reliability in the outcomes.

Building on these characteristics will unleash massive network effects, allowing for the unbundling into a core set of primitives and rebundling of services by entrepreneurs across the Finternet. We propose in the next section a high-level architecture for the Finternet that incorporates these principles and characteristics.

5.3 High-level technology architecture



[12] This diagram has been incorporated from the "Finternet: the financial system for the future" (2024) by Agustín Carstens and Nandan Nilekani.

5.4 Key technical building blocks of the architecture

5.4.1 Tokens

Token Characteristics and Security Tokens in the digital realm are programmable digital representations of claims on an asset, with each possessing a unique identifier that ensures traceability. Their non-alterable nature enhances the security and integrity of digital transactions. Programmability facilitates the automated execution of transactions, streamlining the process and bolstering security.

Trusted Proof Chains Tokens can incorporate third-party attestations and credentials, boosting their credibility and detailing usage terms via metadata. This clarifies the conditions under which tokens can be used, enhancing trust among transaction participants. The chaining together of tokens, their credentials and attestations, and metadata of every event results in the creation of proof chains that can be made portable so that subsequent actors have all the information to decide without having to capture and verify all over again.

Transactional Triggers and Holder Authentication Transactions with tokens can trigger various actions at different stages, such as pre-insert (KYC checks), real-time (fraud checks), and post-transaction activities. Tokens are linked to user accounts and are updated or transferred depending on their type and quantity. Each token has a Holder, which establishes authentication and authorization chains. Transactions are executed only with explicit authentication and authorization proof of the user.

Tokenization and De-tokenization Tokenization is the process of converting assets along with the rights and rules into a self-containing and self-describing digital representation (token), while de-tokenization refers to the reverse process, converting tokens back into their original form. This may be facilitated by an ecosystem of service providers that offer a bridge between the existing world and the Finternet (on-ramp during tokenization, off-ramps during de-tokenization).

5.4.2 Token managers

Token managers are integral to maintaining the integrity and compliance of

tokenized assets within the Finternet. They may operate their own private or shared ledgers, ensuring that these ledgers synchronize with the Finternet's unified ledger. This structure supports the independent issuance of tokens and offers solutions for token reproduction and recovery. Users also can manage their self-created tokens (for type A and type B assets), reinforcing autonomy while the system safeguards against the unauthorized creation of tokens on behalf of others.

The Finternet ecosystem also includes registrars who ensure the security of asset transactions. They provide recovery options for registered and regulated assets, enhancing trust in the system. The architecture caters to various asset types, from user-controlled and attested assets to registered and strictly regulated assets, each with its degree of user autonomy and compliance requirements. This multifaceted approach aims to make the digital economy more inclusive and user-centric while ensuring necessary oversight and safety.

5.4.3 Verifiable and portable credentials and attestations

Verifiable credentials and attestations digitally encapsulate key information about individuals, entities, or assets in a secure format that is readily shareable through QR codes, enhancing the verification process across devices and platforms. These credentials, by being easily verifiable, improve user experience and access to digital services. Verifiable attestations add another layer, bringing in third-party verification to bolster the credentials' trustworthiness.

Portability and interoperability are critical for these credentials and attestations, allowing for seamless integration and use across different systems. Moreover, their design must accommodate both dynamic and static information—dynamic credentials can be updated or revoked to reflect changes, while static ones maintain consistency over time. This adaptability ensures that credentials remain both relevant and reliable, supporting a wide range of uses in a connected digital environment.

Incorporating the concept of portability into verifiable credentials and attestations is crucial, particularly across different ledgers. This portability ensures that the proof chain, which enables the verification for transaction completion, remains intact when credentials are transferred or accessed across various systems. The seamless transfer of these credentials and attestations, supported by open standards, is vital for maintaining their validity and trustworthiness in a diverse technological landscape. This approach not only facilitates easy verification but also

enhances the overall security and usability of digital credentials in multi-ledger environments.

Issuance, sharing, and verification of credentials and attestations. The lifecycle of verifiable credentials and attestations, encompassing the creation, notification, sharing, transport, and verification stages is as follows:

1. **Creation**: The process begins with the 'issuer' creating the credential. This involves the issuer's information, the holder's details, the actual credential data, relevant metadata, and the issuer's digital signature to ensure authenticity and integrity.
2. **Notification**: Upon storing the credential, the system notifies the holder via SMS or email, indicating that their credential is ready for use.
3. **Transport**: The credential can be shared with a verifier directly by the holder through various means:
    - **Print**: The holder can physically print the credential.
    - **Export**: The holder may export the credential for use in different formats or applications.
    - **Download**: The credential can be downloaded to the holder's device.
    - **3rd Party Apps**: The holder can use third-party applications, such as a user's digital wallet, to manage and share the credential.
4. **Verify & Accept**: The final stage involves the acting party verifying the authenticity and accepting it within their workflows.

Throughout this lifecycle, the holder controls their verifiable credentials, choosing when and with whom to share them. Additional layers of privacy-enhancing techniques can be applied as necessary. The process ensures that credentials are securely created, stored, and transported while allowing verifiable attestations to be efficiently made by verifiers who can trust the validity of the information they receive. Verifiable Credentials and Verifiable Attestations must leverage existing digital signature and public-key cryptography (PKI) infrastructure. Digital signatures are cryptographic mechanisms used to verify the authenticity and integrity of electronic data.

Public Key Infrastructure (PKI) is at the heart of digital signatures.

1. **Key Pairs:** PKI uses two related cryptographic keys: a private key (kept secret by the owner) and a public key (shared openly).

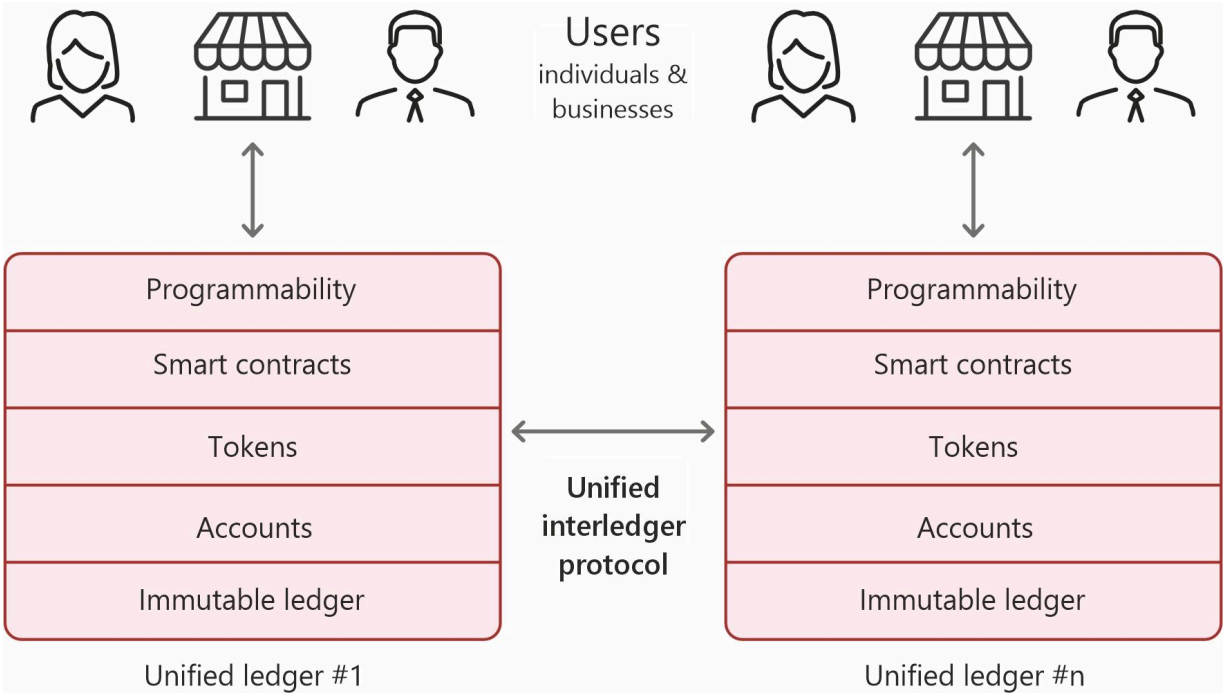
2. **Signing:** When data needs to be signed, the owner's private key is used to generate a unique digital signature for that data. This process often involves creating a hash of the data and encrypting it using the private key.
3. **Verification:** Anyone can verify the signature using the corresponding public key. They decrypt the signature to retrieve the original hash and compare it against a new hash of the received data. If they match, the data is unchanged and verified.

While individuals and organizations are common entities using digital signatures, other entities like websites, servers, or software can also use them.

5.4.4 Ledger design considerations

At its core, users leverage this ecosystem to perform a spectrum of financial activities, from transactions to asset management, facilitated by an array of user-friendly interfaces and applications made possible by the unified ledgers. The core components of the unified ledger include programmability that enables applications, account management, tokens, smart contracts, and interoperability with other ledgers.

High-level architecture of the unified ledger[13]



Authentication, authorization, and addressing in unified ledgers. The first step is that a user can create their account in any ledger of their choice. When they create an account, they can define their own authentication, authorization, and addressing schemes. Authentication and authorization work in tandem to secure digital transactions. Authentication verifies user identities, while authorization grants them specific access based on their roles. In complex scenarios, such as joint or multi-stakeholder holdings and maker/checker workflows, building authentication chains is crucial when transactions require two-factor authentication. Similarly, authorization chains are necessary when actions need approvals from multiple authenticated users, ensuring thorough control and security in transaction processes. Each of the authentication chains and authorization chains must be converted into a set of proofs that can be passed on as metadata for a transaction, all security characteristics must be unbundled and embeddable as code. This sets the stage for user-defined addresses.

User addressing within the Finternet system plays a crucial role in simplifying and securing the interaction with unified ledger accounts.

[13] This diagram has been incorporated from the "Finternet: the financial system for the future" (2024) by Agustín Carstens and Nandan Nilekani.

These are the core features of user addresses:

1. **Human Readable:** the account addresses must be designed such that they are easily understandable and memorable for individuals, as opposed to being just a complex series of numbers and letters. This feature enhances usability by making addresses more approachable and easier to communicate.
2. **QR codeable and shareable**: account addresses, attached to every unified ledger account, can be encapsulated in QR codes, making them easily shareable and scannable. This streamlines the process of initiating transactions or sharing account details.
3. **Abstracted from token managers' identity**: Addresses are designed to function independently of any specific token manager, ensuring compatibility and flexibility across different systems and entities.
4. **Deep-Linking**: Account addresses support deep linking, allowing direct navigation to specific functionalities or actions within applications, enhancing the user experience and interaction efficiency.
5. **Management of the address**: Addresses can be transient, one-time, or revocable, providing users with control over the duration and permanence of their address visibility. Users can set up aliases for their addresses, facilitating easier management and recognition.
6. **Differentiation of address usage**: There is a distinction between viewable and buyable links, akin to the difference between reading and transacting endpoints, which delineates the purpose and function of the address interaction.
7. **Discovery and Routing**: A robust discovery and routing mechanism must be integrated, allowing users to find and interact with accounts seamlessly, akin to how people use email and website addresses in the broader digital space.
8. **Brand and Procedural Guidelines**: Ledger providers must adhere to specific brand and procedural guidelines for using the address system, ensuring consistency and reliability in user interactions.
9. **Dynamic Resolution and Management**: The system includes a Discovery API and mapper to facilitate the dynamic resolution of addresses, providing updates and managing the flow of information between users and ledger systems.
10. **User Onboarding**: The Unified Interledger Protocol (UILP) Onboarding API is an integral part of the system, ensuring that new users and entities can integrate and participate in the ecosystem smoothly and effectively.

In the admin/account management app of a ledger application, certain rules are paramount to ensure the integrity and functionality of the system. Firstly, without explicit authorization proof, the ledger is prohibited from executing any transactions, ensuring that only verified actions are processed. This principle enforces strict adherence to security protocols, where the ledger acts only upon validated requests. Secondly, the rule of "what you see in the proof is what gets executed" applies, particularly in the context of transfer rules. This ensures that the transaction details provided in the authorization proof directly correspond to the actions performed by the ledger, thereby maintaining transparency and predictability in transaction processing.

In the user's account, multiple user-controlled, attested, registered and regulated tokens can be attached. This flexibility in ledger technology is reinforced by the point that all of a customer's tokens do not need to reside on the same ledger but their management is made interoperable across ledgers via the unified interledger protocol.

While there may be infinite workflows and representations for any financial interaction involving individuals and organizations, the contexts in which assets are managed and the governance structures surrounding them may differ internationally, they can all be built based on a primitive set of building blocks:

The core ledger technology is structured into two functional layers to enhance the system's flexibility and control:

1. **Ledger Layer:** generalized technology layer providing core ledger functionalities such as user and account management, authentication, Unified Interledger Protocol (UILP) adherence, core ledger operations, immutability, security, availability, and so on.
2. **Descriptor Layer**: This foundational layer handles the representation of assets and tokens, including all associated data, metadata, and credentials. It integrates transient attestations, such as guarantees for transfers or balance proofs, as well as permanent credentials, effectively setting the trust levels and defining the asset's characteristics. The descriptor layer contains four primitives that have been outlined below:
    a. **Actions**: This category covers the primary interactions within the system, including reading, creating, updating, and transferring assets. These actions define how users engage with the ledger.
    b. **Holders**: This refers to the entities that possess or control tokens within the system, outlining their roles and responsibilities.

   c. **Consensus**: This involves the mechanisms through which decisions are made, such as different voting rules (any, at least, all, veto) that dictate how consensus is reached among stakeholders.
   d. **Conditions**: This encompasses the criteria or stipulations required for transactions to proceed, which are verified through the proof chain. Conditions ensure that all required parameters are met before an action is finalized, also aiding in dispute resolution and enforcing compliance.
3. **Programmability Layer**: This layer offers varying degrees of composability, programmable workflows, and automation (from minimal to fully automated processes), enabling application developers and users to construct complex workflows. This enables composability across multiple types of asset types, and transactions, and supports open innovation, allowing anyone to launch applications without prior permissions. However, the operation of specific tokens may require the authorization of holders and involved parties and the application of necessary rules and regulations.

It is possible to think about a next-gen non-mining ledger architecture without forcing everything to a single native token of the ledger provider. A ledger implementation that contains the key technical characteristics, is compliant with the UILP protocols, and architecture we have outlined but doesn't involve any form of mining and native tokens.

Today, most efforts are either focused on private ledgers (within a financial institution), or shared ledgers (between a set of financial institutions coming together), but we now need to build unified ledgers that meet all the user-centric requirements, are universal and open to all, and can unify across diverse asset types and environments.

Lastly, the issue of replicability, especially pertinent in digital contexts and even more so in offline-offline transactions, is acknowledged as a significant challenge. The system must be designed to prevent unauthorized duplication of transactions, addressing the unique vulnerabilities of digital and offline interactions to uphold integrity and trust in the ledger's operations.

Advances in cryptographic and ledger technologies[14]

[14] This has been reproduced from Finternet: the financial system for the future (Carstens and Nilekani, 2024)

The financial sector has extensively leveraged cryptographic technologies, particularly encryption, to safeguard sensitive data, secure online transactions, and ensure the confidentiality and integrity of financial communications. Encryption protocols like SSL/TLS are used to protect data transmitted over the internet, preventing unauthorized access and data breaches. The Advanced Encryption Standard (AES) secures data at rest, ensuring that stored financial information remains confidential and tamper-proof. Public Key Infrastructure (PKI) has played a pivotal role, serving as the backbone for both encryption/security and the integrity of digital records. PKI utilizes a two-key asymmetric system, where a public key is used for encryption and a private key for decryption. This framework secures sensitive data in transit and also underpins the authenticity and integrity of digital records through digital signatures.

Digital signatures, enabled by PKI, inherently facilitate non-tamperability in digital transactions and records. By providing a secure means to verify the identity of transaction participants, they ensure that any data or records involved remain unaltered after signing. This verification process is key to maintaining data integrity, as any tampering with the content would invalidate the digital signature. Consequently, this mechanism not only protects against unauthorized modifications but also establishes non-repudiation, making it impossible for the signatory to deny their action or the authenticity of the signed document, thereby reinforcing trust and security in digital interactions.

Leveraging digital signatures, verifiable credentials, and attestations, as standardized by the World Wide Web Consortium (W3C), bolsters the non-tamperability and verifiability of digital transactions. These credentials, which include examples like digital passports, educational degrees, and professional certifications, are signed by trusted issuers and can be verified easily across platforms. Verifiable attestations, such as employment history confirmation for credit score validations, support these credentials by providing trusted evidence of the claims made. This system ensures secure, reliable identity verification and data integrity, streamlining the verification process, reducing fraud risks and enhancing efficiency in digital ecosystems.

Recent advances in identity data-sharing, such as Self-Sovereign Identity (SSI), empower individuals to control their personal identity data, enabling them to share it securely and as needed. Beyond identity data, technologies like zero-knowledge proofs (ZK proofs) and multi-party computation (MPC) could also help to safeguard privacy and confidentiality in data-sharing. ZK proofs allow one party to prove to another that a statement is true without revealing any information beyond the validity of the statement itself. MPC enables multiple parties to jointly compute a function over their inputs while keeping those inputs private, enhancing the security and confidentiality of data-sharing.

Going beyond data-sharing, we can incorporate concepts such as tokens, programmability, composability and, in some cases, immutability into the regulated financial system, drawing from technological developments with hashing, Merkle trees, smart contracts, and various distributed ledger technologies (such as Hyperledger, Ethereum, etc).

In sum, these developments represent a transformative shift in the way trust is established, enabling massive network effects and unlocking new interactions across various sectors, thus redefining the dynamics of digital and economic exchanges. This is an indicative list, and we are at the threshold of many more advances. As technologies continue to evolve, it is critical not to get locked into specific solutions but instead design for evolvability, ensuring adaptability to future changes and innovations. Moreover, we must look to leverage the best technological advances while keeping in mind consumer protection, balancing innovation with the safeguarding of users' rights and interests.

5.4.5 Contracts within the Finternet

In the evolving landscape of digital transactions, smart contracts represent a continuum of programmable workflows, mirroring the shift from traditional to digital processes similar to early internet adaptations like internet banking. Each technological shift—from the adoption of paper to its eclipse by digital technologies—has radically altered workflows. Examples include the shift from queuing in line to apply for services at a physical location to the ease of executing the same tasks online. This technological evolution is not just a replacement but a foundation for entirely new forms of business interactions.

Yet, the conventional notion of smart contracts as fully self-contained rule systems (codifying every single rule, regulation, and other legal norms) is flawed. Reality dictates that not all rules and regulations can be effectively translated into codified data within contracts. Instead, these should be viewed as part of a broader spectrum of digital workflows that incorporate various levels of business logic and ledger interactions. These levels include basic transaction protocols, complex business automation (like automated leasing workflows in banking), and cross-border transactions, emphasizing the need for automation and efficiency.

In a multi-ledger world, the challenge amplifies as innovators must consider interoperability without coding for every specific ledger system. This necessitates a

shift towards universal constructs—ledger-independent and language-independent models focusing on the fundamental 'Nouns' (data models) and 'Verbs' (actions). This approach leverages automatic triggers and executable protocols, moving beyond the limitations of traditional smart contracts to a more flexible and scalable framework suitable for the diverse and dynamic nature of international digital transactions.

Enabling Network Effects through contracting. The transition from traditional bilateral contracts to a network-based model marks a pivotal evolution in business operations, enhancing scalability, flexibility, and interoperability across various sectors internationally. This evolution can be illustrated through three models:

1. **Pipe Model**: Resembling a traditional pipeline, this model involves a linear process where laws and regulations are translated into contracts and then into code, guiding all transactions from start to finish. While highly structured, it lacks the flexibility to swiftly adapt to market changes or scale across different jurisdictions—akin to early telecommunications systems that were rigid and operator-dependent.
2. **Platform Model**: Similar to online marketplaces, this model centralizes transactions on a platform that mediates between consumers and producers. It simplifies compliance and contract management but restricts direct interaction between the parties, centralizing control and potentially stifling direct peer-to-peer engagement.
3. **Network Model (NxM)**: This innovative model functions like the internet or an electricity grid, where any participant can interact directly with any other participant in a regulated, trustworthy framework. It supports extensive interactions free from the linear constraints of the Pipe Model or the central oversight of the Platform Model. Leveraging network effects, the model's value increases as more participants join, much like how the internet gains utility with more connected users. This model encourages a seamless, efficient, and transparent ecosystem, facilitating international, cross-industry transactions, reducing costs, and increasing transaction speed.

These models collectively illustrate a shift towards more dynamic and interconnected systems, advocating for an approach that significantly enhances the adaptability and efficiency of international economic activities.

This shift paves the way for on-the-fly contracting, where agreements and transactions can be initiated and concluded in real-time, tailored to the immediate

needs of the parties involved. This capability is vital for the Finternet, as it supports a seamless, efficient, and user-centric digital economy, enabling participants to engage economically in a manner that is as spontaneous and fluid as everyday conversations. Such a dynamic environment is crucial for fostering innovation and rapid adaptation across different sectors and geographies.

5.4.6 Unified Interledger Protocol (UILP)

The Unified Interledger Protocol (UILP) is a set of open protocols that define the messaging specifications between different ecosystem participants: token managers, trust service providers, applications, and unified ledgers to ensure interoperability and the finality of transactions between them. It serves as a fundamental framework designed to facilitate seamless transactions between disparate systems. UILP's core is built around the concept of "proof chains," which ensure the integrity and verifiability of transactions across these ledgers.

These non-repudiable proof chains (consisting of tokens, credentials, and attestations chained together) are critical as part of on-ramp/off-ramp operations or interledger operations to prevent man-in-the-middle attacks. In addition to building trust in transactions and addressing fraud, the proof chains also enable compliance. For example, the Bank Secrecy Act (BSA) "Travel" rule, as specified in 31 CFR 103.33(g), mandates that financial institutions involved in certain transmittals of funds must pass on specific information about the transaction to the next financial institution. This rule is crucial for tracking and preventing illicit financial activities across borders. Complementing this, the IVMS101 messaging standard, developed by the Joint Working Group on interVASP Messaging Standards, establishes a uniform data model for transmitting originator and beneficiary information. The proof chains enable the sending institution to attach a signed packet using the IVMS101 data model, enhancing the security and compliance of cross-border transactions, and the receiving institution to verify it locally.

At the heart of UILP is the ability for two distinct ledgers to not only initiate a transaction but also to verify the endpoints, establish the necessary handshakes, execute the transaction, and finalize it. This comprehensive process ensures that each step is securely and efficiently managed, maintaining the consistency and reliability of the interledger transactions.

The pre-initialization phase of a UILP transaction involves discovery and information exchange, facilitated by a suite of APIs designed for this purpose. These include discovery APIs, verification APIs, and other metadata APIs, which

collectively enable the identification and understanding of the transaction parties and their capabilities. Additionally, key exchange and registry APIs play crucial roles in establishing secure communication channels and maintaining a record of participating entities and their transaction histories.

Following this, the transaction phases of initialization, execution, and finalization are managed through a structured set of operations. Each transfer within this process is mirrored by an update on both sides of the transaction, ensuring that the state is consistently maintained across the ledgers. The proof chain mechanism comes into play here, where the accepting party bears the responsibility of verifying the transaction's integrity, independent of any intermediary or bridge.

The negotiation process between the two participating ledgers involves asynchronous handshakes, allowing for the dynamic exchange of additional data that may be required to proceed with the transaction. This flexibility is crucial in addressing the diverse and often complex requirements of different ledger systems.

Finally, UILP mandates a standardized request/response structure for retrieving asset and transaction information, ensuring a uniform and predictable interface for interacting with the protocol. This standardization is pivotal in facilitating interoperability and enabling the diverse ecosystem of ledgers to interact seamlessly through the UILP framework, thus fostering a more connected and efficient digital transaction landscape.

5.4.7 Application use-cases and design considerations

Looking to the future, digital tokenization presents exciting possibilities across various sectors, offering innovative and flexible financial solutions. It could streamline income management and investment for freelancers, provide artists with access to international markets, and enhance strategic planning for small businesses. Tokenization might also democratize real estate investment through fractional ownership and improve transparency in nonprofit operations. Additionally, it could stabilize agricultural markets and simplify access to healthcare and education through tokenized vouchers, contributing significantly to sustainable and equitable economic development.

In the realm of climate action, tokenization might support the issuance of green bonds for sustainable projects, manage carbon credits more effectively, or facilitate the distribution of subsidies for energy-efficient technologies. These applications could significantly enhance transparency and accountability in environmental

efforts. Additionally, tokenization offers promising applications in RegTech (regulatory technology) and SupTech (supervisory technology), which could strengthen trust in financial systems by improving compliance tracking and enhancing the supervision of regulatory processes. This broader adoption could lead to more robust and trusted frameworks in financial and environmental regulation.

This moment in technology could usher in an era where the full spectrum of possible applications has yet to be fully imagined, laying the groundwork for unprecedented advancements and opportunities. The applications developed will interact with the user's ledger account (which will be the source for authentication and authorization of transactions).

5.5 Tackling fraud

Addressing financial crimes like money laundering, and terrorist financing, preventing other illegal activities, enhancing consumer protection against financial harms, and preventing the build-up of systemic risks requires a further evolution in the ability to observe, supervise, regulate, and enforce actions. Currently, the detection and prevention of such crimes are challenging due to their often hidden nature within complex paperwork, making human detection difficult and statistically improbable.

The reliance on extensive paperwork in current financial systems often leads to inefficiencies that can be exploited to conceal financial crimes. This systemic inefficiency can cause services to grind to a halt, leading to a denial of service in critical financial operations, thereby necessitating a move towards more streamlined, digital solutions. The current systems are hampered by the use of disputable and easily manipulated evidence, along with outdated methods like manual, randomized sampling, and retrospective audits.

To overcome these limitations, we need to shift towards an ecosystem based on irrefutable facts and evidence, where transaction details are transformed into unassailable proofs. This shift will enable a move from traditional, paper-based responses to more efficient, algorithmic solutions. Bridging cross-sectoral gaps is also critical, as assets frequently move across different systems. Establishing a consistent, digital, and tamper-proof system across all sectors is key for combating financial crimes effectively, protecting consumers, and ensuring adherence to regulations.

Finternet: the financial system for the future (Carstens and Nilekani, 2024)[15] provides a framework to think about the various types of fraud. This has been detailed in the box below.

Categories of Fraud

In the complex landscape of financial fraud, practices like impersonation, circumvention, and compromise highlight the multifaceted challenges faced by individuals and institutions alike (FinCen (2024))[16]. Impersonation frauds exploit personal identities, circumvention tactics bypass established standards and protocols, and compromises breach the security of accounts and systems. These categories encompass a broad range of fraudulent activities, from altering records and identity theft to cyber incidents and the abuse of insider access, each exploiting vulnerabilities for illicit gain. Against this backdrop, the Finternet stands as a formidable defense, offering advanced mechanisms to counteract these challenges.

Fraud at entry: preventing unauthorized access

- Identifiability and traceability: The unified ledger enhances the ability to identify and trace transactions and user activities, making it significantly

[15] Finternet: the financial system for the future (Carstens and Nilekani, 2024)
[16] Identity-Related Suspicious Activity: 2021 Threats and Trends (January 9, 2024)

harder for impersonators to gain unauthorized access. By embedding advanced identity verification mechanisms that leverage biometric data, real-time authentication, and digital signatures, the system ensures that only legitimate users can enter.

- Embedding of regulatory rules into code: Automating compliance through smart contracts prevents circumvention of entry controls. Regulatory requirements, such as Know Your Customer (KYC) and Anti-Money Laundering (AML) standards, are programmed into the system, ensuring that all users meet strict criteria before being granted access.

Fraud once within the system: safeguarding against internal threats

- Observability and auditability: Once users are within the system, continuous monitoring and real-time alerts for unusual activities help in detecting internal fraud. The system's observability ensures that any attempt to manipulate transactions or records is immediately flagged, while auditability allows for detailed examination of all actions, enhancing accountability.
- Immutability and verifiability: The immutable nature of records within the unified ledger prevents alterations, ensuring that once a transaction is recorded, it cannot be changed or deleted. This verifiability deters insider fraud and abuse, as any fraudulent attempt to alter records will be easily detected and irrefutably traced back to the perpetrator.

Social engineering attacks

- Educational programs and behavioral analytics: While technological safeguards are vital, educating users on the risk of social engineering attacks is equally important. Behavioral analytics can be employed to detect patterns indicative of social engineering, such as unusual transaction requests or atypical access patterns, triggering additional verification steps.
- Multi-factor authentication and dynamic permissions: Implementing multi-factor authentication and dynamic permission settings for transactions can mitigate the risk posed by social engineering. By requiring additional authentication for sensitive actions and adapting permissions based on risk assessment, the system can prevent unauthorized transactions even if a user is manipulated.

In addition to applications for users, we expect entrepreneurs to build many types of applications in broader categories such as regulatory tech, supervisory tech, compliance management, and fraud management thus providing the tools to token managers and public authorities to safeguard the system better.

6. A unique opportunity that empowers everyone

In conclusion, the journey toward tokenization presents an important pathway for the international economy, promising to unlock a multi-trillion-dollar economic opportunity over the next decade. With the potential to affect more than 8 billion individuals, 300 million businesses, and numerous other organizations across over 193 countries,, the scale and scope of this revolution are unprecedented. We stand at a critical window of opportunity, where the convergence of technology, market readiness, and international connectivity has set the stage for rapid and inclusive growth.

To harness this potential, we must embark on a mission mode to implement the Finternet, crafting a rollout architecture that embodies the principle of "seeing is believing." It's crucial to create tangible experiences, allowing individuals and organizations to touch and feel the benefits of tokenization, thus accelerating adoption and integration into the economic fabric of societies worldwide. The formation of communities and alliances is pivotal in this context, signifying a collaborative effort to weave financial inclusion and digital innovation into a cohesive network that spans the globe.

When selecting use cases for deployment within the Finternet, one should employ a framework that navigates the landscape of abundance and alignment while respecting established habits and routines. First, identify the areas where data or technology is abundant and can be harnessed to provide value without overhauling existing systems. Next, consider the habitual incentives that drive user behavior, selecting use cases that integrate seamlessly with these daily practices to reduce friction and encourage adoption. It is important to discern which stakeholders stand to gain from the transition and those likely to resist, tailoring strategies to engage both groups constructively.

Required changes must be carefully balanced with the fears and concerns of individuals about privacy, regulators' focus on oversight, and market players' emphasis on operational continuity. Use cases that align with the common

intentions of efficiency, transparency, and security across all parties are more likely to succeed. Therefore, the ideal use cases should leverage abundant resources, correspond with existing user habits, accommodate the concerns of various stakeholders, and capitalize on the shared objectives of individuals, regulators, and market players, thus ensuring minimal habit disruption and maximal intent alignment.

To fully harness the potential of the Finternet and ensure its effective integration across various sectors, it is essential to engage in extensive prototyping and experimentation of protocols, specifications, and standards. Establishing dedicated sandboxes will enable the safe testing of diverse use cases, allowing us to iterate and refine solutions in controlled environments.

As we stand on the brink of this monumental shift, the call to action is clear: we must collectively drive the momentum to ensure that the benefits of tokenization are realized universally, bridging divides and fostering a world where every individual and business can thrive. This is not just an economic imperative but a moral one, where accelerating the pace of change and innovation through tokenization becomes our shared mission for the betterment of all humanity.