coinbase INSTITUTE

Why the Future of Finance Calls for a Permissionless Architecture

coinbase INSTITUTE

The global financial system is ready for an update. This paper sets out a vision for a more responsive, effective, and resilient infrastructure, built on permissionless systems. At the center is tokenization—turning assets into digital records that can be exchanged as easily as sending a text. When built on open systems, tokenization gives users more control over their money and data, helps financial institutions with compliance, and allows developers to create new products and services. This will transform how we do business today, bringing new opportunities for growth and innovation.

Table of Contents

01 — Toward a Tokenized Economy

Leading organizations and central banks around the world agree that the financial system needs an update.[1] Despite decades of improvements in digital technology, many systems remain outdated and disconnected. Transactions can take days to finalize, relying on slow and complex messaging, clearing, and settlement processes.

The deficiencies of the current financial system are sometimes masked by consumer-friendly innovations, such as the introduction of mobile payments apps. But while they are digital, and may feel instant, they still rely on traditional banks and settlement rails to actually move money. And because they are closed systems, they limit users to sending money within their own networks. For example, a PayPal user cannot send directly to a CashApp user, just as WhatsApp users cannot message Apple's iMessage users.

Tokenization of assets on permissionless blockchain networks can change this. Rather than just adding new interfaces to old systems, permissionless networks rebuild financial services from the ground up with open, programmable rails—bringing everyone and everything onchain. This enables true peer-to-peer transactions and direct connectivity between all participants—regardless of which provider they use.

Tokenization is the process of digitally recording the ownership of an asset on a shared ledger, and it can be for any type of asset, not just financial. This includes stocks, bonds, treasuries, commodities, intellectual property, digital art, collectibles, real estate, and more. Ownership, when recorded on a permissionless network, is both immutable and public.

Once an asset is tokenized, its owner can securely transfer it as easily as sending an email. The transaction does not require an intermediary. This innovation allows the linking of previously disconnected parts of the financial system, much like the internet did for communications. And by enabling onchain ownership, tokenization puts holders in direct control of not only their financial assets but also their personal data. BlackRock's tokenized money-market fund, BUIDL; Société Générale's use of tokenized assets for stablecoins; and Siemens' issuance of digital bonds with automated settlement highlight how tokenization is transforming mainstream financial operations.

This vision of an improved financial architecture holds significant promise, but achieving it depends on one key condition: it must be built on a permissionless system—one that anyone can access and use. Time and again, history has shown that open systems encourage innovation, create fair competition, and deliver benefits to everyone. This was true of the protocols that underpin the internet, like TCP/IP

[1] Carstens, A. & Nilekani, N. *Finternet: the financial system for the future, BIS Working Paper No. 1178* (April 15, 2024), https://www.bis.org/publ/work1178.html.

Understanding Permissionless Networks

Permissionless networks are open systems that anyone can join and use without special permission. These networks are built on what is called a "base layer"—the foundation that provides security and basic transaction capabilities, similar to how a city's infrastructure (roads, power lines) supports everything built on top of it. These networks have four essential components:

1. **Core Protocol**
   The fundamental principles that govern how the system works. Participants help maintain the network's accuracy and security, following clear rules about how to verify and record information on a shared ledger. They receive rewards for this work.
2. **Nodes**
   A globally distributed network of computers that maintains copies of the shared ledger, validates transactions, and ensures network security. Anyone can run a node, contributing to the network's infrastructure.
3. **Smart Contracts**
   Some networks allow for automated agreements—digital instructions that execute automatically when specific conditions are met.
4. **Cryptocurrency**
   Each system has its own digital currency that rewards those who help maintain and secure the network.

for moving data and SMTP for sending emails; they were instrumental in creating a level playing field and encouraging experimentation in the early days of the technology. For example, by enabling email exchange between competing providers, such as Gmail and Outlook, SMTP provides a universal "language" for global messaging.

However, tech companies built private, closed platforms—from social media to commerce—on top of the internet's open protocols, limiting how users could connect across different services. This led to the centralization of user data, content, and digital services under the control of a few dominant players, which in turn led to the problems we face online today: misuse of personal data, compromised privacy, and platforms with the power to instantly cut off access to essential services.

The ethos of openness and interoperability of the early internet is essential for updating our financial system and counterbalancing centralization in digital platforms. Permissionless architectures break down barriers to entry by allowing any innovator to create new products and services. In contrast, closed systems privilege their owners, allowing them to set the rules of participation and limit competition. By keeping the system open, we ensure more opportunities for innovation, growth, and inclusivity.

Without this ethos, the vision of a new, more competitive financial system is at risk. There are and always have been strong economic incentives for creating closed systems—just as there were in the 1990s when major players tried to control the emerging internet. Companies like America Online, Microsoft, and Apple sought to create closed ecosystems that limited users, businesses, and developers to proprietary content and features. However, with government support, the open internet prevailed.

Governments are once again in a position to shape the future. They have the opportunity to not only allow but actively support a new generation of open protocols—permissionless blockchain networks. While cryptocurrencies like Bitcoin are often simply viewed as advances in computer science, the underlying technology offers a far greater transformation in how society organizes economic activity and designs markets.[2]

Realizing this vision will reduce reliance on single points of failure, foster competition, and balance the market power of established players. These features are also crucial for creating a more user-centric financial system—one that empowers individuals with greater control over their assets and data. Enabling these features may, of course, introduce novel risks and policy considerations, which will need to be addressed as the new systems evolve and scale. Striking the right balance will unlock benefits that extend far beyond finance, driving transformative changes across mainstream commerce and other industries. Just as the internet transformed every aspect of society and the economy, permissionless blockchain networks are now redefining the very foundations of how value is created, exchanged, and managed.

[2] Catalini, C., & Gans, J.S. *Some simple economics of the blockchain*, Communications of the ACM 63.7, 80-90 (2020), https://dl.acm.org/doi/abs/10.1145/3359552.

02 — What is Tokenization and Why Does It Matter?

Tokenization is the process of digitally recording the ownership and attributes of assets on a distributed ledger. In the context of open networks, tokenization enables asset owners to send them to someone else without the need for a trusted intermediary. Moreover, these transfers can be preprogrammed to execute upon specific conditions by using smart contracts—software code that embeds instructions directly in the blockchain itself. This is not possible with our existing market infrastructure.

The impact of tokenization extends well beyond financial products and services. In addition to stocks, bonds, loans, treasuries, commodities, and derivatives, tokenization can unlock value and generate liquidity for assets like intellectual property, gaming items, and digital content. It can bring similar benefits to physical goods and real-world assets, like real estate and collectibles.

Tokenization even extends to the creator economy. For example, when art is tokenized on a distributed ledger as a non-fungible token (NFT), its identity as both a creative artifact and a transferable form of value become inseparably linked. This differs from traditional art markets, where transactions require organized auctions and art dealers. This enables new possibilities; for example, customizable rights, such as royalties, can give creators and owners more ways to share or exchange value.

This new paradigm relies on the type of universal interoperability that can only be achieved through an open system, supported by shared frameworks and standards for seamless communication and interaction. And the consequences are far reaching.

Tokenization on permissionless blockchains will fundamentally change the roles of historically critical intermediaries like transfer agents, settlement and clearing agents, custodians, and brokers. Many of these intermediaries are no longer required because information about an asset's ownership is encoded in the asset itself, onchain. Separate ownership records for the purpose of settling, netting, or clearing transactions are not needed. This allows financial activities to be handled more securely and automatically while still complying with traditional regulations.

Intermediaries will still play a role in tokenized transactions but with a new value proposition. Just like today, market participants may still prefer centralized services like custody, exchange, and regulatory compliance. However, on an open blockchain network, centralized intermediaries will not have exclusivity over providing these services. They will need to compete based on the quality of their products and services, lowering barriers to entry and renewing competition in long-stagnant sectors of the economy.[3]

[3] Catalini, C. *Forget antitrust, regulate to let tech disrupt itself,* a16z crypto (April 30, 2024), https://a16zcrypto.com/posts/article/forget-antitrust-regulate-to-let-tech-disrupt-itself/.

Ultimately, realizing a tokenized future will require well-crafted regulatory frameworks, guided by the principles we discuss in Section 4. When designed and implemented effectively, these frameworks will ignite a transformative wave of innovation in financial services and beyond. Just as sending an email or a picture online is now easy and nearly free, moving money or updating ownership of assets could soon become just as simple and affordable.

Tokenization: The Start of a Global Transformation in Financial and Non-Financial Sectors

Global Embrace of Tokenization

Governments and institutions worldwide are embracing the potential of open systems for programmability, faster settlement, and accessibility.

- **Singapore's** Project Guardian integrates blockchain with institutional finance, exploring tokenized foreign exchange and government bonds with real-time settlement and reduced counterparty risk.[4]
- **European Investment Bank's** €100M Ethereum-based bond[5] highlights permissionless networks' potential for capital markets.
- **Philippine** startups and real estate companies are exploring tokenization in the real estate sector, which will democratize investment and expand inclusion.[6]
- **Switzerland's** Lugano promotes blockchain for urban services via the "Plan ₿ initiative."[7]
- **Broadridge** processes $4T/month[8] in tokenized repos, improving liquidity and efficiency.
- **Apollo** and **JPMorgan** are exploring automated portfolio rebalancing.[9]
- **Société Générale** leverages tokenized assets for stablecoins and liquidity pools.[10]
- **Siemens** issued digital bonds with automated settlement.[11]
- **Christie's** 3.0 enabled fully on-chain NFT auctions, showcasing tokenization's reach beyond finance.[12]
- **BlackRock** launched a tokenized money-market fund, BUIDL.[13]

---

[4] Project Guardian, https://www.mas.gov.sg/schemes-and-initiatives/project-guardian.
[5] EIB, *EIB issues its first ever digital bond on a public blockchain* (April 28, 2021), https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain.
[6] Prime Investments Philippines, *From Bricks to Blockchain: The Rising Trend of Real Estate Tokenization* (Aug. 22, 2024), https://primeinvestments-ph.com/2024/08/22/from-bricks-to-blockchain-the-rising-trend-of-real-estate-tokenization/.
[7] Lugano's Plan ₿, https://planb.lugano.ch/.
[8] Broadridge, *DLT in the Real World 2024*, https://www.broadridge.com/resource/capital-markets/dlt-in-the-real-world-2024.
[9] JP Morgan, *Revolutionizing Asset & Wealth Management*, https://www.jpmorgan.com/kinexys/content-hub/project-guardian.
[10] Société Générale, *Société Générale-Forge elevates its stablecoin to accelerate its distribution and free use* (July 8, 2024), https://wholesale.banking.societegenerale.com/en/news-insights/all-news-insights/news-details/news/societe-generale-forge-elevates-its-stablecoin-to-accelerate-its-distribution-and-free-use/.
[11] Siemens, *Siemens remains a pioneer – Another digital bond successfully issued on blockchain* (Sept. 4, 2024), https://press.siemens.com/global/en/pressrelease/siemens-remains-pioneer-another-digital-bond-successfully-issued-blockchain.
[12] Christie's 3.0, https://nft.christies.com/.
[13] Yahoo Finance, *BlackRock Launches Its First Tokenized Fund, BUIDL, on the Ethereum Network* (March 20, 2024), https://finance.yahoo.com/news/blackrock-launches-first-tokenized-fund-222700828.html.

03 — The Benefits of a Permissionless Architecture

3.1 Core Benefits

Tokenized assets on permissionless blockchains have the power to improve economic outcomes across several critical dimensions. The first is instant settlement. Tokenized transactions are highly efficient, requiring a simple update to a shared digital ledger to transfer ownership or update the status of an asset. This enables near-instant settlements without the need for manual processes or third parties. The results are lower transaction costs, broader accessibility, and lower counterparty risk.

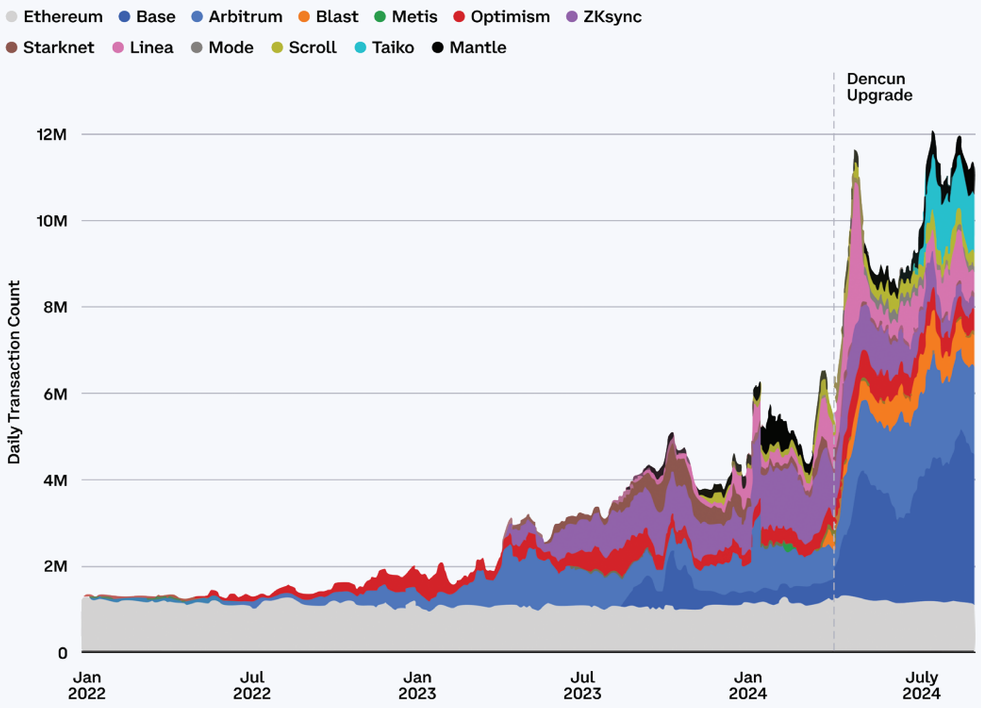
Second, tokenization eliminates many outdated processes tied to legacy systems. Transactions no longer require extensive digital or physical paperwork because the necessary information is contained within the token itself. For example, a tokenized loan can be issued with covenants and terms of repayment attached directly to the loan—no offchain paperwork required. This reduces reconciliation across different systems, streamlines communication, and simplifies audits.

Third, tokenization on permissionless networks enables self-custody (see Section 4.5), allowing individuals to have direct control over their digital assets and data. This shift from institutional custody to personal control brings important benefits for privacy, portability, and user autonomy.

Fourth, distributed ledgers offer unprecedented transparency. Assets are at all times visible and their transaction history never disappears. The process of verifying and monitoring the ownership and status of an asset can be automated, eliminating the need for trust in and reliance on an intermediary. Automation streamlines transactions, reduces delays, and minimizes the operational overhead associated with traditional verification.

Fifth, while there is unprecedented transparency on some blockchains, users can also operate with an appropriate level of privacy without compromising regulatory compliance. Solutions using advanced cryptographic techniques such as zero-knowledge proofs (ZKPs) allow participants to prove the validity of information without revealing the underlying data. For example, a user can demonstrate compliance with financial regulations without exposing sensitive personal information. This improves privacy, reduces the friction of traditionally invasive verification methods, and minimizes the risk of creating centralized stores of personally identifiable information (PII) that could attract hackers and identity thieves.

Figure 01 — Daily Transactions on Ethereum



Sources: growthepie.xyz and Coinbase. Metrics are taken on a 10-day rolling average.

Daily transactions in the Ethereum ecosystem. While transactions on Ethereum's foundational base layer have remained relatively stable, transactions on Layer 2s have surged dramatically. Today, these scaling solutions process over 90% of all transactions.

Sixth, the speed of onchain transactions on permissionless networks continues to improve. Recent advances in scalability have put to rest a common misconception that maintaining and securing a distributed ledger is prohibitively expensive due to throughput limitations and high transaction (i.e., gas) fees. These solutions entail additional settlement systems, often referred to as Layer 2s, that operate on top of the foundational base layer, or Layer 1. This shift reflects how onchain technology has responded to the growing demand for transactions, fueled by the rise of decentralized finance (DeFi) applications, stablecoins, and non-fungible tokens (NFTs).

Seventh, these benefits rely on the unique governance properties of permissionless systems. While proponents of permissioned blockchains and technology-agnostic approaches argue that achieving these benefits is possible without embracing openness, the inevitable question arises: Why has this yet to materialize on a global scale, beyond incremental improvements to domestic payment systems? The answer: Far too often, the governance of international or industry consortia and standard-setting bodies is slow, complex, and stalls under the weight of divergent interests and objectives.

Open and permissionless networks solve the consortia governance problem by deploying technology that is equally accessible to all. Complex coordination is replaced with standardized software interfaces, similar to the APIs that have revolutionized much of software production over the last decades. These interfaces are available on the same terms and conditions to incumbents and new entrants alike. This is a fundamental strength of the technology. Just as Bitcoin operates as a digital store of value independent of any central bank while remaining globally accessible, permissionless networks enable market participants to efficiently transact without requiring coordination on a unified solution and its ongoing governance.

Finally, permissionless networks can be implemented in ways that fully meet the needs of highly regulated environments. Much in the same way that financial services participants adapted to use of the internet, controls can be implemented at the application layer, on top of a permissionless architecture, where an intermediary uses discretion in ways similar to traditionally regulated activities. This approach lets institutions maintain essential oversight and critical controls while leveraging the openness, interoperability, and dynamism of the technology. It mirrors the model followed by the internet's evolution, which combined foundational openness at the protocol layer with controls and oversight at the application layer.

The Important Role of Self-Custody

Self-custody means having direct control over your assets, identity, and data through private keys, removing the reliance on intermediaries like custodians. While some users will continue to custody digital assets through intermediaries, others already welcome the benefits that self-custody affords, including portability and privacy.

As this technology enables direct user control of digital assets, policymakers and regulators are developing new frameworks that preserve the benefits of self-custody while ensuring appropriate oversight. Self-custody can be entirely compatible with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) goals. In fact, chain analytics solutions—powered by AI and machine learning models—are positioned to meet and exceed traditional financial systems in detecting illicit activity.

This is important because self-custody is a prerequisite for user-centricity – i.e., giving users control of their participation in mainstream commerce and digital interactions. Self-custody also reduces dependency on service providers by minimizing lock-in and enabling seamless data portability. It has the added benefit of mitigating the risks of data breaches and misuse that arise in the current system, where private data is duplicated across multiple institutions. And it enables entirely new approaches to know your customer (KYC) and identity verification that prioritize privacy and security while complying with regulatory requirements.

Transforming Cross-Border Payments Through Permissionless Networks

The adoption of stablecoins—tokens pegged to fiat currencies—for cross-border payments highlights how permissionless networks are solving long-standing frictions in global value transfer. Traditional payment systems are often slow, expensive, and restricted by limited operating hours, leaving significant room for improvement.

Data from the first half of 2024 underscores the transformative impact of stablecoins: they settled over $2.6 trillion in value, translating to an annualized rate exceeding $5.3 trillion. This volume reflects adoption that extends beyond speculative trading—particularly in emerging markets.

A survey of 2,541 early adopters across Brazil, India, Indonesia, Nigeria, and Turkey reveals multiple use cases for stablecoins: 47% of respondents rely on them to save in U.S. dollars, 43% to secure better exchange rates, and over 30% for international money transfers.[14] Notably, more than 20% of respondents indicated that their use of stablecoins was to enable transactions that would otherwise be impractical.

Stablecoin adoption is also reshaping key remittance corridors, such as the U.S. to Mexico one. According to Visa, stablecoin transaction volume to exchanges in Mexico has grown by 30% per month, recently exceeding $100 million in monthly transfers.[15] Bitso, a leading regional exchange, reports facilitating 10% of the remittances volume between the two countries. New consumer experiences, such as those offered by Félix Pago and Sling, aim to revolutionize cross-border payments with user-friendly and low-cost solutions. By cutting fees by 50% or more compared to traditional options, these platforms have seen rapid growth. Similarly, startups like Onboard are using stablecoins to provide seamless global payouts to creators and freelancers.

The efficiency gains delivered by stablecoins stem from the foundational properties of permissionless networks. These networks facilitate instant settlement, automated payment processes, and transparent verification. The elimination of traditional correspondent banking delays is particularly advantageous for markets historically underserved by conventional financial infrastructure.

[14] Castle Island Ventures & Brevan Howard Digital, *Stablecoins: The emerging market story* (2024), https://castleisland.vc/wp-content/uploads/2024/09/stablecoins_the_emerging_market_story_091224.pdf.
[15] DuneCon2024, *View on Stablecoins: On-Chain Insights and Payment Implications* (Nov. 27, 2024), https://www.youtube.com/watch?v=jl6QZ62zi9s.

3.2 Interoperability

Open and permissionless networks help overcome one of the biggest challenges to commerce and finance—the purposeful lack of interoperability among proprietary systems. Financial institutions, payment apps, and digital platforms often restrict interoperability, creating closed systems that lock in customers and prevent them from interacting or transacting with users on competing platforms. For example, payment apps such as PayPal or WeChat Pay restrict transactions to their own networks, preventing seamless exchanges with rival services. Similarly, financial institutions might make it difficult for customers to switch providers or integrate services from competitors.

This lack of interoperability limits customer choice and can stifle innovation. New entrants struggle to offer equivalent or complementary services because they are effectively excluded from the ecosystems and services controlled by the incumbents. For customers, this leads to higher costs, fragmented experiences, and the inconvenience of maintaining accounts on multiple platforms to access the functionalities they need.

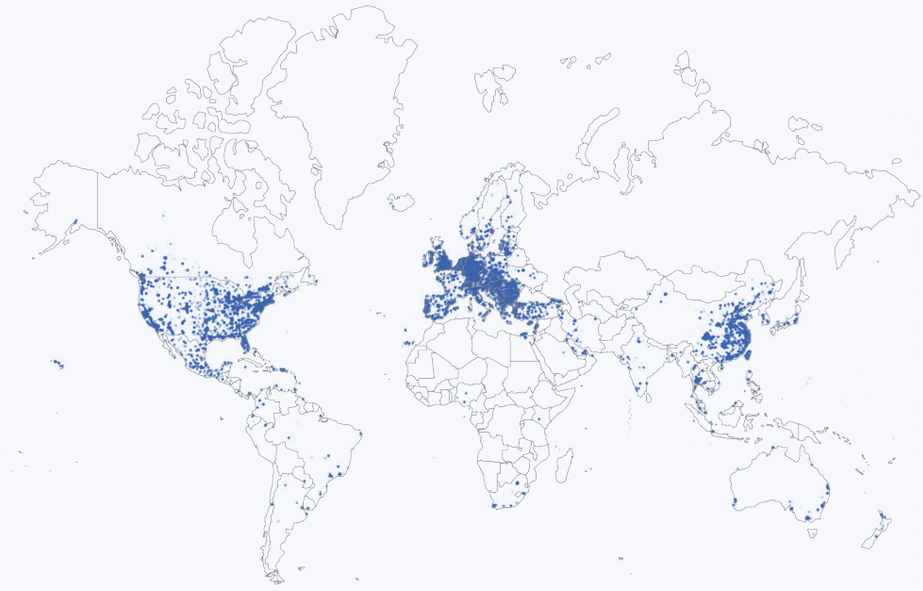
Providers often support interoperability with other products or services in the early stages to attract users and grow their market presence. However, once they achieve significant market share, their priorities can shift, and instead of focusing on delivering value to customers, they begin extracting value by raising fees and limiting access by, and interoperability with, competitors. And once challengers face higher barriers to entry, dominant providers face little pressure to innovate. As a result, service quality deteriorates, leaving customers with fewer choices and diminished benefits.

Tokenization on permissionless networks shifts the power of network effects away from individual companies and places it in the hands of the broader participants in a system—a user-centric model.[16] Moreover, ownership and control of tokenized assets reside directly with the owner, and participants can switch service providers with minimal friction. The ability to switch keeps dominant players accountable and fosters a more dynamic, competitive market—one that prioritizes delivering high-quality, reliable, and cost-effective services over exploiting market dominance.

This outcome is possible only with an irrevocably open system for developers and builders. If a single entity were permitted to unilaterally alter the rules of a blockchain network, then it would not be truly open and would be merely a different type of closed network. Such "decentralization theater" does little to change the economic dynamics of the system and fails to offer any meaningful improvement over existing technologies.

[16] Catalini, C., & Kominers, S.D. *Can Web3 Bring Back Competition to Digital Platforms?,* Antitrust Chronicle, (Feb. 2022), https://www.competitionpolicyinternational.com/wp-content/uploads/2022/02/6-Can-Web3-Bring-Back-Competition-to-Digital-Platforms-Christian-Catalini-Scott-Duke-Kominers.pdf

Helium Network: Reimagining Interoperability in Telecommunications Through Permissionless Networks



Source: https://explorer.helium.com/

The Helium Network shows how permissionless networks can transform traditionally closed ones into open, interoperable systems. Helium has created a new model for deploying and operating wireless networks that challenges conventional assumptions about telecommunications. Traditional telecommunications infrastructure requires significant capital investment and operates as a closed system, with single operators maintaining exclusive control over their infrastructure and user base. This model has historically limited competition and left many areas underserved. Helium's decentralized approach challenges this by enabling users to deploy infrastructure directly. Helium has seen rapid growth with over 350K active hotspots between mobile devices and Internet-of-Things (IoT)[17] devices. Real-world implementations demonstrate the network's versatility:

Urban Resilience

In Portugal, Greenmetrics.ai[18] leverages the low-cost network for flood prevention. Their sensors detected a critical 10x increase in underground water levels during a May 2023 flood event, providing authorities with crucial advance warning.[19]

Museum Sensors

By deploying low-cost, connected environmental sensors in museums and libraries, Heliotics maintains optimal preservation conditions through real-time monitoring of temperature and humidity.[20]

Maritime Connectivity

Through Skynet, the network extends coverage to the otherwise challenging maritime environment along the North Sea and Florida coast.[21]

Telecommunications Integration

The network's partnerships with Telefónica[22] and T-Mobile[23] enable seamless integration with traditional cellular infrastructure. Mobile subscribers can automatically transition between networks, effectively extending carrier coverage without additional capital investment.

Helium's economic model aligns infrastructure deployment with demand through tokenized incentives. Operators earn rewards based on the utility they provide to the network, creating direct correlation between service quality and economic returns. This structure has driven growth in areas of highest demand, leading to more efficient resource allocation compared to traditional top-down planning. Helium's progress has catalyzed similar initiatives across other sectors, including distributed computing and environmental sensing networks. These Decentralized Physical Infrastructure Networks (DePIN) demonstrate how permissionless protocols can reshape critical infrastructure deployment and expand accessibility while maintaining interoperability with legacy systems.

[17] Helium, *Network Stats*, https://explorer.helium.com/stats.
[18] greenmetrics, https://www.greenmetrics.ai/.
[19] greenmetrics, *Success Case: Ultra-Early Flood Detection in Downtown Lisbon During Intense Rainfall* (July 14, 2023), https://www.greenmetrics.ai/post/success-case-real-time-flood-detection-in-lisbon-during-intense-rainfall.
[20] heliotics, *IoT in Museum: Smart Ambience Monitoring* (Jan. 19, 2024), https://www.heliotics.com/blog/iot-in-museum-smart-ambience-monitoring/
[21] Business Wire, *The Helium Foundation Announces SkyNet IoT's Roaming Integration with Helium* (March 7, 2024), https://www.businesswire.com/news/home/20240307676524/en/The-Helium-Foundation-Announces-SkyNet-IoT%E2%80%99s-Roaming-Integration-with-Helium.
[22] Telefonica, *Telefónica and Nova Labs launch Helium Mobile Hotspots in Mexico* (Jan. 24, 2024), https://www.telefonica.com/en/communication-room/press-room/telefonica-and-nova-labs-launch-helium-mobile-hotspots-in-mexico/.
[23] Hardesty, L. *T-Mobile allows the Helium Mobile 'crypto carrier' to ride on its 5G network,* Fierce Network, (Sept. 20, 2022), https://www.fierce-network.com/5g/t-mobile-allows-helium-mobile-crypto-carrier-ride-its-5g-network.

3.3 Programmability and Modular Innovation

Programmability and modular innovation at the protocol layer of blockchains are essential to fostering a dynamic and competitive landscape.

Programmability allows rules and logic to be built directly into the network's operations using smart contracts. Smart contracts are self-enforcing code that execute specific operations when invoked by a user, application, or another smart contract. Once triggered, they perform these operations based on pre-specified conditions, and can also incorporate data from external sources, such as price feeds—also referred to as "oracles"—to ensure accurate and more flexible execution.

In financial services, smart contracts can be used to automate critical compliance, risk management, governance, audit requirements, and other operational or regulatory requirements. On permissionless networks they can also establish transparent incentivization and governance rules to reward desired behaviors, such as contributions of capital or other resources, and discourage actions that could undermine the security, stability, or fairness of the system.

Modulary innovation relies on the principle of composability—allowing different applications to be combined to create more advanced products and services. When protocols are designed in an open

architecture, anyone can deploy them without requiring permission. This allows simple financial primitives—such as exchanging, lending, and borrowing assets—to be combined to create more advanced instruments and services. It also facilitates the reuse of successful components, enables seamless upgrades to individual components, and reduces duplication of effort. While service providers may still choose to bundle services for user convenience, the underlying services would also be available in unbundled form, facilitating user choice in the ecosystem.

The Potential of DeFi and Composability

One recent example of the growth of permissionless networks is Decentralized Finance (DeFi). In DeFi, individual smart contracts can be recombined, like money lego blocks, significantly lowering barriers to entry—a property often referred to as "composability." Multiple providers compete to offer the most effective access to the underlying markets, driving a relentless focus on user experience, meeting user needs, and achieving cost efficiency. The fast-paced innovation in DeFi has only been possible because of a permissionless architecture.

Traditional financial institutions have started to develop significant interest in using DeFi to meet new and existing client needs. As a recent EU Commission report concluded, "early experiments often relied on permissioned ledgers" but "the success of [DeFi] [...] led many organizations to recognize that this technology's true potential is realized only when the blockchain functions as a broadly shared ledger."[24]

DeFi also shows how the value created by an open network can be shared with its participants. For example, Aerodrome enables liquidity providers to deposit stablecoins, earn a proportional share of the revenue, and actively shape operations through voting. This model ensures that the value created is distributed to participants rather than intermediaries. By streamlining currency exchange between stablecoins such as USDC and EURC at a fraction of the cost (0.1% fee) and near-instant settlement (1–5 seconds, 24/7), Aerodrome dramatically outperforms traditional finance's slow, costly FX operations—unlocking more efficient global payments.

[24] Schär, F. *Enhancing Financial Services with Permissionless Blockchains,* European Commission, (Oct. 2024), https://data.europa.eu/doi/10.2874/8306042.

Self-Custody and User Control: Decentralized Social Media

The development of decentralized social networks on permissionless architecture demonstrates how tokenization can fundamentally reshape ownership and control of digital identity. Two implementations—Lens Protocol and Farcaster—illustrate distinct approaches to achieving this transformation while highlighting the flexibility of permissionless networks in supporting diverse technical solutions.

Lens Protocol encodes user social profiles as non-fungible tokens. This design ensures that all social connections and interactions are recorded onchain, with users maintaining control over their profile and data. The protocol's architecture enables ownership of not just identity, but the entire social graph—including followers, content, and engagement history. This tokenization approach allows for modular innovation, as applications built on top of Lens can reuse different components of it.

Farcaster employs a hybrid model that separates identity management from social media content. The protocol records user identities on the Ethereum blockchain while storing social data in a distributed network of storage nodes. This architectural decision optimizes for performance and scalability while preserving the core benefits of self-custody. Users retain control of their identity and social relationships, enabling portability across applications. This means, for example, that users can seamlessly switch between different clients for interacting with their social feed, as well as applications that build on the social graph for diverse purposes such as content curation, event organization, and more. For instance, a user might engage with their social feed using a microblogging client like Warpcast, participate in community discussions through a platform like Lemmy, and manage events using a tool like Eventcaster. This interoperability fosters a dynamic ecosystem where users have the freedom to choose applications that best suit their needs without being confined to any single platform.

Traditional digital platforms maintain centralized databases that define user relationships, content, and access by third-party applications. This creates lock-in, as users cannot easily transfer their social graph and experiences. By encoding these relationships on blockchains, Lens and Farcaster ensure that social connections become portable assets controlled directly by users.

This transformation extends beyond data portability. This architecture enables new models for content monetization too. Smart contracts can automatically enforce revenue sharing, manage content licenses, and facilitate direct creator-audience relationships without platform intermediation. This programmability allows for innovation in how social platforms generate and distribute value.

3.4 Onchain Security, Privacy, and Risk Management

Permissionless networks offer capabilities that are not possible with the recordkeeping methods of traditional finance. Transactions are recorded on immutable ledgers, ensuring that changes cannot occur without network consensus. Data can be encrypted to protect sensitive information, and the properties of a tokenized asset can be verified by a third party without revealing all the underlying information.

The distributed nature of permissionless networks eliminates single points of failure and ensures that no individual participant can alter the rules of operation, whether through malicious intent or as a result of being compromised. This ensures that records cannot be tampered with and assets can only be transferred with the owner's unique authorization key.

When unexpected or bad events do happen, blockchain explorer tools available to any market participant provide audit trails and information about token movements, facilitating the real-time detection of anomalies, fraud, and financial crime. This is in contrast to traditional financial systems, which are not only more opaque but also fragmented across multiple organizations, making such oversight significantly more challenging, even by regulators with special authority.

Technology also exists to balance the privacy of users with compliance needs. Participants across sectors such as finance and healthcare often need to verify transactions and demonstrate compliance without exposing sensitive information. Despite the public nature of blockchain transactions, this can be achieved with cryptographic techniques like zero-knowledge proofs (ZKPs). ZKPs enable participants to prove the validity of transactions or asset properties without revealing the underlying data. For example, a company can demonstrate regulatory compliance without disclosing sensitive business details, or an individual can confirm eligibility for a service without revealing their full identity.

Finally, smart contracts offer new methods for risk management. For example, they can dynamically enforce risk-reduction measures when triggered by a market participant, an external price feed, or another smart contract. In decentralized finance (DeFi), smart contracts can automatically initiate the liquidation of undercollateralized positions during periods of market stress. By automating liquidations, smart contracts help maintain stability and minimize the impact of individual defaults on the broader system. This level of automation is challenging in traditional financial systems where participants often lack access to all relevant information, leading to delays and increased risks.

Experiments in Digital Identity and Reputation

The emergence of new digital identity solutions demonstrates how open systems can improve both security and privacy.

California DMV's Mobile Driver's License

The California DMV's partnership with SpruceID illustrates how traditional identity documents can be modernized. Their mobile driver's license (mDL) solution creates digital credentials that offer greater security and privacy than traditional, physical documents.[25] The system allows users to selectively share specific credentials—for instance, proving they are over 21 without revealing their exact birthdate or address. These credentials ensure authenticity while giving users control over their information.[26] In the future, they could also be extended to seamlessly integrate with permissionless networks.

Coinbase Verifications via Ethereum Attestation Service

Coinbase Verifications,[27] built on the Ethereum Attestation Service (EAS),[28] enable Coinbase customers to create onchain attestations tied to attributes like their trading account status and country of residence. These attestations can be linked to any self-custodial wallet, serving as trusted certifications that the broader ecosystem—not just Coinbase—can leverage to develop applications and offer unique functionality for verified users. By recording only the attestations onchain, the system prioritizes privacy and security, ensuring that personal data remains protected while fostering trust and interoperability. Widespread adoption of onchain attestations could drastically simplify distinguishing legitimate users from fake accounts and bots.

Proof of Personhood

World ID[29] tackles the challenge of proving human uniqueness while preserving privacy. The system uses biometric verification to create a unique identifier for each user. This identifier is then transformed into a zero-knowledge proof that allows individuals to perform "proof of personhood" without revealing their biometric data.[30] Once verified, users can prove their humanity across various applications without revealing their identity or additional biometric scans. The technology could help limit inauthentic behavior from AI-generated content.[31]

Decentralized Reputation

Karma3 Labs focuses on building decentralized reputation systems that enable users to establish and use onchain reputations. Karma3 Labs builds reputation through onchain activities and peer validation. This enables developers to create applications where users can engage in transactions, from voting to lending, based on verifiable reputation scores.

These examples show how permissionless networks and related technologies such as digital credentials can address diverse identity and reputation needs. The California DMV solution upgrades identity systems with privacy enhancements, Coinbase Verifications create trusted attestations for onchain ecosystem participants to rely on, World ID focuses on establishing human uniqueness at a global scale, and Karma3 Labs builds decentralized reputation systems. Despite differing use cases, all leverage new forms of verification and user-controlled data, pointing to a future of secure, private, and user-driven identity models.

---

[25] Maercklein, E. *Credible: Introducing Mobile Driver's Licenses,* SpruceID, (Dec. 8, 2022), https://blog.spruceid.com/credible-introducing-mobile-drivers-licenses/.
[26] SpruceID, *SpruceID Partners with California DMV on the Mobile Driver's License* (Oct. 25, 2023), https://blog.spruceid.com/spruceid-partners-with-ca-dmv-on-mdl/.
[27] Coinbase, *Verify your wallet to unlock onchain experiences*, https://www.coinbase.com/onchain-verify.
[28] Ethereum Attestation Service, https://attest.org/.
[29] World ID, https://world.org/world-id.
[30] World, *Intro to zero-knowledge proofs, Semaphore and their application in World ID* (Aug. 17, 2023), https://worldcoin.org/blog/worldcoin/intro-zero-knowledge-proofs-semaphore-application-world-id.
[31] World, *Proof of personhood: What it is and why it's needed* (Feb. 21, 2024), https://world.org/blog/worldcoin/proof-of-personhood-what-it-is-why-its-needed

3.5 Onchain Governance

Trust removes friction in human interaction, exchange, and commerce. One way to build trust is through a robust legal system. Advocates for the Finternet argue that "trust in the financial system does not come from technology but from the legal and regulatory framework that underpins it."[32] However, decades of progress in economic research and behavioral science have shown us there are many ways to generate trust and reduce transaction costs.[33] Technology is a powerful tool in this regard, complementing legal frameworks to promote more efficient forms of exchange.

Permissionless networks are already reducing friction and transaction costs, automating contracts, and reshaping how markets operate.[34] For example, DeFi protocols like Aave have attracted billions of dollars in value to their lending ecosystem by offering secure, smart-contract-enabled loans with low fees and high transparency. In DeFi, smart contracts execute with a level of precision unattainable in traditional markets, where ownership and control rights are often constrained by slow, costly, and imperfect proxy voting processes.

However, smart contracts and onchain governance may face last-mile frictions, such as ensuring onchain information aligns with real-world conditions. For example, while a smart contract can automatically execute trades between tokenized assets, the initial onboarding of users still requires traditional know your customer (KYC) verification to comply with regulations—a process that involves manual checks of government IDs, proof of address, and other offline documents that cannot be automated onchain. This creates friction where the efficiency gains of onchain technology meet the practical constraints of real-world identity verification and regulatory compliance.

Many of these challenges can be addressed by integrating governance practices from traditional markets. The most effective approach combines the strengths of legal frameworks with the automation capabilities of smart contracts and onchain governance, ensuring fairness, security, and alignment with societal norms.

Most notably, in permissionless networks, key parts of the legal and regulatory frameworks needed to govern activity shift to the application layer. Issues beyond the scope of smart-contract automation, such as consumer protection, dispute resolution, and systemic stability can be addressed at this layer. This ensures permissionless networks can scale while maintaining the oversight required for trust and adoption. By incorporating smart contracts, traditional contracts can also be streamlined,[35] saving time and resources. This hybrid approach merges the efficiency and transparency of onchain technology with the robustness of traditional governance systems.[36]

The same result is not achievable with unified ledgers alone, as permissioned systems fail to address the competitive and security side effects of centralized control. Without the decentralization made possible by permissionless networks, the same power imbalances,

[32] Carstens, A. & Nilekani, N. *Finternet: the financial system for the future, BIS Working Paper No. 1178 at 29* (April 15, 2024), https://www.bis.org/publ/work1178.htm.

[33] See, e.g., Coase, R. H., *The nature of the firm*, Economica, 4(16), 386–405 (1937), https://doi.org/10.1111/j.1468-0335.1937.tb00002.x; Jensen, M. C. & Meckling, W. H., *Theory of the firm: Managerial behavior, agency costs and ownership structure*, Journal of Financial Economics, 3(4), 305–360 (1976), https://doi.org/10.1016/0304-405X(76)90026-X. Their research, which frames firms as a nexus of contracts, is particularly relevant for understanding the transformative potential of smart contracts and programmability when combined with a neutral base layer.

[34] Catalini, C., *The firm as a nexus of smart contracts: How blockchain and cryptocurrencies can transform the digital economy*, Yale Journal on Regulation (June 7, 2017), https://www.yalejreg.com/nc/the-firm-as-a-nexus-of-smart-contracts-how-blockchain-and-cryptocurrencies-can-transform-the-digital-economy-by-christian-catalini/.

[35] See, e.g., International Swaps and Derivatives Association, *Building Smart Contracts*, https://www.isda.org/2024/04/08/building-smart-contracts/.

barriers to entry, and opportunities for established players to control the market persist, leaving the potential for meaningful transformation of the financial system unrealized.

Today, the governance of many essential financial and digital platforms is concentrated in the hands of a few large companies. These entities wield substantial influence over markets, the content we consume, the products we buy, and the connections we form. Their dominance has grown over time due to network effects and the natural tendency of digital platforms to gravitate toward winner-take-all dynamics.

Onchain governance offers a powerful counterbalance to this concentration of power, redistributing ownership and decision-making among key stakeholders. Automating governance through permissionless protocols ensures that interoperability and open access to the base layer cannot be revoked as ecosystems scale. This approach fosters a level playing field, promoting competition and innovation while curbing the ability of dominant players to exploit network effects to stifle new entrants.

[36]See, e.g., U.S. Securities and Exchange Commission, 17 CFR Parts 240, 270, 274, and 275, *Concept Release on the U.S. Proxy System*, https://www.sec.gov/files/rules/concept/2010/34-62495.pdf.

Ethereum's Transition from Proof of Work (PoW) to Proof of Stake (PoS): A Governance Perspective

Ethereum's shift from Proof of Work (PoW) to Proof of Stake (PoS), completed in September 2022 with "The Merge," is a prime example of how open-source communities govern and navigate significant protocol changes.

Ethereum's transition was not decided by a central authority but shaped through a decentralized and participatory governance process. Key governance mechanisms included Ethereum Improvement Proposals (EIPs) that enabled community members to propose, debate, and refine changes. These proposals were publicly accessible, allowing for transparent deliberation and broad input. Developers, researchers, validators, and users participated in discussions across forums and community calls. Achieving consensus required balancing differing opinions and addressing technical, economic, and ethical considerations.

Throughout the transition, effective communication was critical, with regular updates from developers and the Ethereum Foundation keeping the community informed about progress and challenges. This fostered trust and reduced uncertainty.

Ethereum's transition to PoS not only implemented breakthrough technical capabilities but also highlighted the potential of decentralized governance to drive innovation and consensus in permissionless networks.

04 — The Path Forward: Policy Considerations and Regulatory Principles

Public policy has a key role to play in fostering an environment that enables the transformative potential of permissionless networks. This potential is made possible by regulatory frameworks that are appropriately tailored to the underlying technologies. Doing so will help ensure a level playing field for services built on open networks, paving the way for a new era of experimentation and innovation—much like we experienced with the commercial internet.

Realizing this outcome requires market participants—new entrants and incumbents—to have the same level of access and same obligations. Interoperability between new and legacy systems can facilitate seamless integration and extend the capabilities of existing infrastructure. And new entrants would benefit from fair and equal access to payment and banking rails, avoiding the kind of gatekeeping that could hinder their ability to compete.

Public policies that ensure the neutrality and interoperability of permissionless networks must be actively promoted and safeguarded, both within individual networks and across them. Without these principles, a unified ledger system would amount to little more than a backend infrastructure upgrade, offering minimal benefits to consumers and businesses.

Regulatory frameworks should also consider policies that do not treat all assets and activities involving permissionless blockchains as financial. Tokenization serves diverse purposes, such as granting access to resources, enabling governance participation, or representing ownership of digital and physical goods like NFTs. Recognizing the difference between finance and commerce can avoid the risk of misclassifying products and services that do not fit traditional financial categories.

In the sections that follow, we lay out the importance of base layer neutrality and share key requirements for the technology to thrive.

4.1 Ensuring Base Layer Neutrality

Base layer neutrality is essential for realizing the benefits of permissionless networks. It ensures that the underlying technology operates impartially, without favoring specific participants or prioritizing one type of activity over another, much like how net neutrality supports internet traffic. This means, for example, that infrastructure providers, like node validators, need to treat all participants and applications equally when processing transactions.

Neutrality promotes healthy market dynamics, fosters inclusivity, and enables the technology to act as a trustworthy and unbiased foundation for a wide range of applications. A neutral base layer empowers developers and enterprises to innovate on a shared set of standards, free from arbitrary interference, hold-up, or expropriation. This creates a dynamic where success is determined by merit rather than technological gatekeeping.

Importantly, base layer neutrality does not imply that all participants operate with the same level of access to the network infrastructure. Service providers can—and often must for regulatory compliance—impose restrictions on the services they offer and the types of customers they serve, much like financial intermediaries in traditional market systems. Permissioning at the application layer, when intermediaries use discretion commensurate with traditional services, preserves the ability of policymakers to exert oversight with these specific activities.

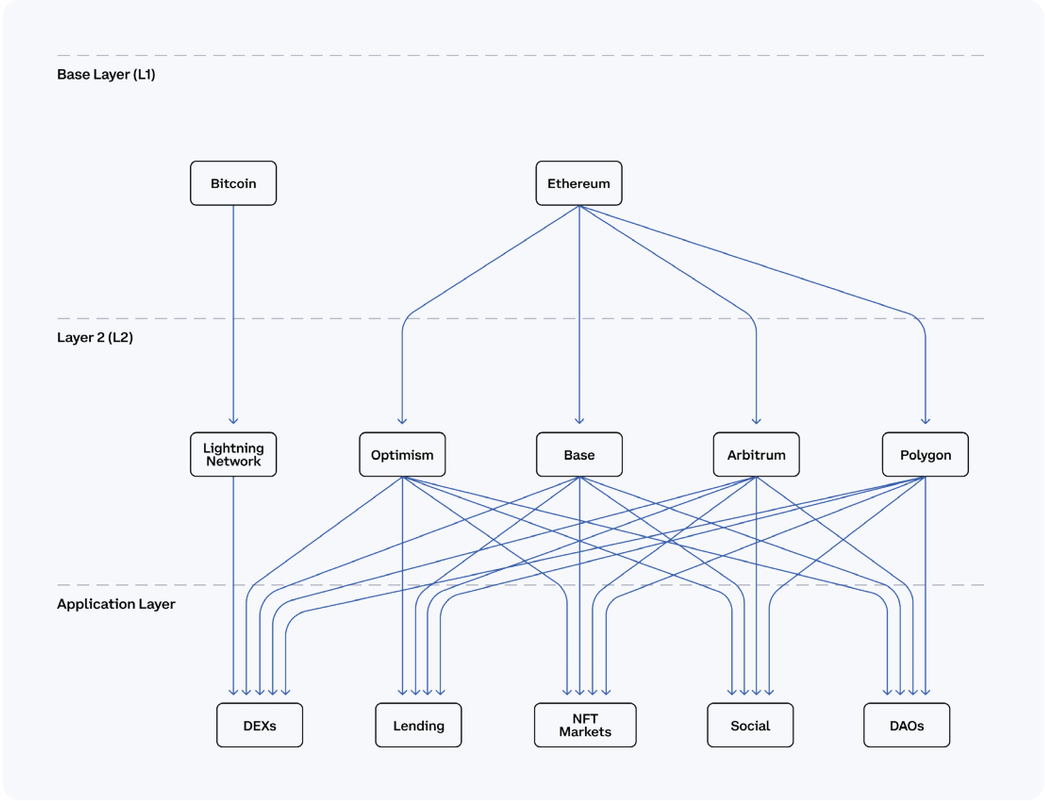
Base layer neutrality can also facilitate transparent governance of technological upgrades. In permissionless networks, a diverse ecosystem of builders actively contributes to the upgrade process, improving the likelihood of detecting and resolving bugs, errors, and other issues.[37] Using this approach, the Bitcoin and Ethereum networks have maintained continuous operation 24/7/365 since their inception, demonstrating remarkable reliability. This collaborative model stands in contrast to closed financial systems, where a central operator dictates the need for and implementation of upgrades for everyone, often resulting in outages that have caused substantial economic harm—such as the recent global disruption linked to a CrowdStrike employee mistake.[38]

Regulators can play a key role in preserving base layer neutrality by avoiding rules that undermine its impartiality, such as mandating transaction prioritization or filtering based on factors like geographic location or institutional affiliation. Instead, key compliance concerns can be addressed by targeting intermediaries operating at the application layer—such as exchanges and custodial services—where oversight is essential for consumer protection and fraud prevention. With neutrality of the base layer, policies can balance fostering innovation with addressing concerns, like combating market abuses and financial crime.

[37] Fracassi, C., Khoja, M., & Schär, F. *Decentralized Crypto Governance? Transparency and Concentration in Ethereum Decision-Making (2024)*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4691000.

[38] Fung, B., CNN, *We finally know what caused the global tech outage - and how much it cost,* CNN, (July 24, 2024), https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html.

Figure 02 — Crypto Layers Infrastructure



Base Layer (L1) protocols like Bitcoin and Ethereum serve as the foundation, providing core security and consensus mechanisms while processing and validating network transactions. Layer 2 (L2) solutions build on top of these base layers to improve scalability while inheriting the security of L1s. The Application Layer sits at the top, where user-facing applications leverage both L1s and L2s to deliver services to participants.

4.2 Combatting Illicit Finance

A common concern among many policymakers is the use of cryptocurrencies for illicit finance. However, permissionless networks actually offer new tools for combating illicit finance as well as significant benefits for user privacy.

New and effective tools for combating illicit finance are possible because of the fundamental features of permissionless blockchains—pseudonymous transparency and traceability of transactions. A growing industry of blockchain analytics firms has emerged, offering advanced solutions that complement traditional methods to enable faster, more precise identification, tracking, and prevention of illicit financial activity onchain.

For example, institutions, regulators, and law enforcement can analyze transactions carried out on a blockchain regardless of the specific platform on which they took place. In contrast, a traditional

financial institution is largely limited to reviewing its own ledgers, and law enforcement must piece together information from different institutions to trace illicit activity. This is a challenging and slow process. Permissionless networks overcome these limitations, offering advanced tools that address the weaknesses of traditional surveillance and monitoring methods. These innovations provide regulated institutions and law enforcement with a more comprehensive view of customer activities across the network.

Tracing and Recovering Funds on Permissionless Networks

Halting Theft

In 2022, over $500,000 was traced and recovered after being stolen from an elderly man in North Carolina. The scammers had gained access to the man's personal accounts and used his personal information to buy Bitcoin. FBI and Coinbase traced the funds to a scammer in India and returned the stolen money to the victim.[39]

Stopping Social Scams

A criminal group hacked high-profile social media accounts in 2019–2020, extorting funds through blackmail. The suspects were identified by tracing crypto transactions, leading to the extradition and guilty plea of a U.K. suspect.[40]

Recovering Funds from Phishing Scams

Coordinated efforts with Homeland Security helped identify a major phishing scam targeting over 1,000 users. This collaboration led to the recovery of $28.6 million in stolen funds and the arrest of the perpetrator.[41]

Recovering Chargeback Fraud

In 2020, a Florida fraud ring stole $3.6 million from a U.S. crypto exchange through chargeback scams. The exchange worked with the Secret Service to trace and recover the funds, leading to the arrest of five suspects and restitution of over $3.5 million by one guilty party.[42]

---

[39] Contreras, I. *Crypto Crime Stopper: How Coinbase Foiled The Theft Of A Half Million From An Elderly Man's Bank Accounts,* Forbes, (Jan. 7, 2022); https://www.forbes.com/sites/isabelcontreras/2022/01/06/crypto-crime-stopper-how-coinbase-foiled-the-theft-of-a-half-million-from-an-elderly-mans-bank-accounts/.

[40] U.S. Dept. of Justice, *U.K. Citizen Extradited and Pleads Guilty to Cyber Crime Offenses* (May 9, 2023), https://www.justice.gov/opa/pr/uk-citizen-extradited-and-pleads-guilty-cyber-crime-offenses.

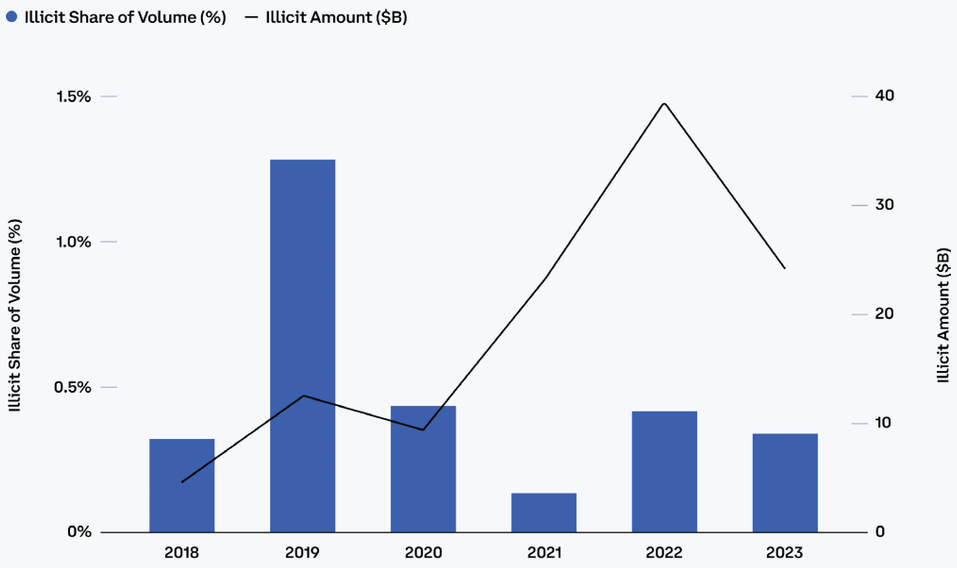
[41] Martin, P. *When it comes to crime, crypto is a powerful tool for law enforcement,* Fortune, (Aug. 23, 2024), https://fortune.com/crypto/2024/08/23/when-it-comes-to-crime-crypto-is-a-powerful-tool-for-law-enforcement/.

[42] United States Attorney's Office, *Leader Of Miami Crew Pleads Guilty To Defrauding Banks And Cryptocurrency Exchange Of More Than $4 Million* (April 26, 2023), https://www.justice.gov/usao-sdny/pr/leader-miami-crew-pleads-guilty-defrauding-banks-and-cryptocurrency-exchange-more-4.

The digital assets ecosystem continues to develop new solutions that address diverse transaction types, typologies, and emerging threats. Figure 3 illustrates this dynamic, showing decreases in illicit activity over the past five years despite growth in the value of assets on permissionless networks that underpin this activity. In 2023 less than one-half of one percent of cryptocurrency transaction volumes were attributed to illicit finance.[43]

[43]Chainalysis, *2024 Crypto Crime Report at 5*, (Feb. 2024), https://go.chainalysis.com/crypto-crime-2024.html.

Figure 03 — Illicit Share of Cryptocurrency Transaction Volume



Source: Chainalysis 2024 Crypto Crime Trends.

Consumer privacy is another key consideration in the fight against illicit finance. Privacy interests are often overshadowed in the pursuit of strong law enforcement against criminal money laundering and sanctions evasion. This creates a key challenge for policymakers: how to safeguard user privacy on permissionless networks while effectively enabling the detection and prevention of illicit activities.

Fortunately, innovations have emerged that enhance user privacy. This includes solutions like zero-knowledge proofs (ZKPs), which safeguard private data while allowing for effective screening of illegitimate activity. ZKPs enable users to prove specific information—such as age, account balance, or country of residence—without disclosing the full underlying data. This results in better protection

of user data and lower risks for service providers, who no longer need to maintain sensitive user data for identity and authorization reviews.

The future success of ZKPs and other innovative approaches to fighting illicit finance while protecting user privacy will also depend on public sector adoption and use. Embracing these technologies will help policymakers better address the difficult tradeoffs between user privacy and the risk of illicit finance and other forms of misconduct.

4.3 Supporting Integration with Traditional Finance

Globally integrated financial markets provide significant economic benefits. By creating seamless connectivity between banking, capital markets, and payment systems across jurisdictions, financial integration can improve resource allocation, enhance productivity, and foster innovation.

Obstacles to financial integration include inconsistency across legal and regulatory frameworks, geopolitical and macroeconomic risks, divergent tech stacks, and disparities in economic development. These can all lead to market fragmentation and structural differences that impede the potential benefits. An open, permissionless financial infrastructure can, by design, overcome many of these challenges.

This hinges on three key initiatives. First, national authorities and international regulatory bodies should be open to building and using financial infrastructure on permissionless networks. This has not yet happened. For example, the Basel Committee on Banking Supervision (BCBS) has recommended capital requirements for banks holding crypto assets at a risk rate—1250%—that effectively discourages their participation. In the United States, the lack of a comprehensive regulatory structure for crypto firms has created uncertainty for businesses in the space.[44]

Second, policymakers should reevaluate the prudence of regulation intended to ringfence traditional finance to insulate incumbents from all risks, and assess whether those regulations also insulate them from progress and competition. Integration and experimentation offer benefits to both traditional and new participants, within longstanding requirements for safety and stability applied equitably based on activities and the associated risks.

Realizing these benefits would require policies that permit cryptoasset products and services to rely on traditional financial services, while also allowing traditional financial services firms to broadly

[44] See, e.g., *Joint Guidance on Crypto Asset Risk to Banking Organizations* (Jan. 3, 2023) https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf; *SEC Staff Accounting Bulletin 121*, (April 11, 2022), https://www.sec.gov/regulation/staff-interpretations/accounting-bulletins/old/staff-accounting-bulletin-121.

engage with permissionless blockchain infrastructure. Examples include stablecoins relying on traditional custody services for reserve backing, conventional exchange-traded funds relying on crypto custody technology when holding digitally-native assets like Bitcoin and Ether, and most critically, the integration of bank fiat onramps and offramps with cryptoasset services providers.

Finally, financial regulators should actively engage with and learn from developers of permissionless architectures and the market participants building on them. Such engagement could help ensure that well-meaning regulation does not inadvertently violate base layer neutrality, and that our future financial infrastructure accommodates the needs and values of all participants. This interaction is critical for balancing trade-offs—such as privacy versus security, and speed versus censorship resilience—in ways that reflect the interests of a broad range of stakeholders. Only through active dialogue can financial integration create an inclusive, adaptive, and resilient ecosystem that benefits everyone.

4.4 Enabling Tokenization of Traditional Financial Assets

To date, digital asset policy has primarily focused on digitally-native assets like Bitcoin and Ether (ETH). Jurisdictions like the EU have passed and implemented comprehensive regulation for the treatment of cryptoassets that is separate from securities regulation. Other jurisdictions like the U.S. are still establishing the classification of cryptoassets for the purpose of regulatory oversight.

There has been far less focus on the tokenization of traditional securities. Yet digitally-native crypto assets represent only $3.8 trillion, a small portion of the global financial economy. In contrast, global equities and fixed income markets are each estimated to be greater than $100 trillion.[45] Bringing these assets onchain, along with the funds that make these investments available to millions of investors globally, represents an unprecedented opportunity for capital market efficiency. Recent studies have concluded that using decentralized exchanges for tokenized equity securities could save U.S. investors over 30% in transaction costs.[46]

Sandboxes are one approach to encourage the tokenization of securities and other traditional financial products, but the pace of development under those efforts is often slow, and jurisdictions often restrict the participation of new entrants—entities not already registered under traditional rules. In contrast, the technology to tokenize securities and trade them on permissionless networks, with appropriate compliance and controls, already exists.

[45] Securities Industry and Financial Markets Association, *Capital Markets Fact Book* (July 2024), https://www.sifma.org/wp-content/uploads/2023/07/2024-SIFMA-Capital-Markets-Factbook.pdf.

[46] Malinova, K. & Park, A. *Learning from DeFi: Would Automated Market Makers Improve Equity Trading?* (Aug. 7, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4531670.

Assessing new ways to promote this tokenization, particularly across jurisdiction and types of market participants, will give regulators an opportunity to rethink how established practices such as broker distribution, custody, and exchanges—born out of a paper-based society—can be improved. For example, atomic settlements forgo the need for centralized counterparties to net and settle transactions on a T+1 or 2-day cycle. Compliance engines built using smart contracts can passport KYC credentials across a broker-dealer network to give asset managers new ways to distribute their products. Tokenized commercial paper has the potential to transform money markets, freeing cash and collateral to be used more easily.

4.5 Recognizing the Right to Self-Custody

The ability of individuals to self-custody digital assets is a foundational principle of the digital asset ecosystem, built on the permissionless ethos of open access, equality, security, and low cost. And self-custody is, conversely, required for the digital asset ecosystem to exist.

Unlike securities or other financial claims, native tokens in permissionless networks are essential to their functioning, acting as the economic and operational backbone of these systems. In networks like Bitcoin and Ethereum, native tokens play a critical role by incentivizing participants, such as miners or validators, to secure the network, process transactions, and maintain decentralized consensus. To achieve this, users must have control over private keys to sign transactions and transfer ownership of assets. For instance, unlike owning a share of Apple, which is not required to use an iPhone, interacting with the Ethereum network requires holding ETH to execute smart contracts or perform other onchain actions.

Self-custody of assets on permissionless networks has many benefits. It gives users maximum control over their financial assets. It eliminates the risks of centralized control and reduces dependency on external entities that may be prone to failures, hacks, or regulatory overreach, including the risk of loss of sensitive personal information, which is all too commonplace at traditional service providers. It also facilitates greater financial inclusion and flexibility, as many individuals worldwide lack access to traditional banking services due to geographical, socio-economic, or political barriers.

In traditional financial markets, regulators have sought for decades to prohibit bearer instruments, primarily to combat financial crimes including money laundering, tax evasion, and fraud. Bearer instruments were historically problematic because ownership and transfer

of these paper-based instruments were hard to trace and regulate. As a result, over the years, regulatory frameworks have emerged to actually or in effect prohibit bearer instruments and requiring regulated intermediaries (e.g., bank and broker dealer custodians or transfer agents) to oversee financial transactions.

Permissionless networks challenge this paradigm by mitigating the types of self-custody risk that resulted in the historical phase-out of bearer instruments. While intermediaries in permissionless networks may not act as gatekeepers—and thus will not be responsible for deciding who has access to the system or monitoring all transactions—key features of permissionless networks help to address any new gaps. And new tools to address illicit finance risk, as well as other risks such as fraud and tax evasion, can be applied to self-custody transactions. The possibility of new and better approaches to addressing these serious risks should be viewed as an important opportunity, both by the private sector and by policymakers.

05 — Conclusion

In this paper we presented a vision for an updated financial system based on open and permissionless networks. An open architecture removes barriers to entry and empowers innovators to create new products and services. At the heart of this transformation is base layer neutrality, a prerequisite for any meaningful change in competition. Without it, distributed ledgers risk replicating the same centralized dynamics that have historically stifled competition and limited innovation in closed financial systems and digital platforms.

We also explained why base layer neutrality is essential: It ensures that the core technology operates impartially, treating all participants and transactions equally, much like net neutrality does for internet traffic. This impartiality prevents dominant players from using the infrastructure to block competitors or control market access. Without this foundation, the potential of tokenization would be limited, and financial systems would continue to operate with the inefficiencies and challenges that exist today.

If realized, this vision will enable a user-centric model, empowering users with self-custody over their assets, identity, and data, while enabling them to switch providers with minimal friction. This can enhance privacy and security, reducing reliance on intermediaries and the replication of user information across providers.

coinbase INSTITUTE

coinbase INSTITUTE