

# DeFi vs. TradFi: Institutions and Industrial Organization

Andreas Park

## Abstract

This paper analyzes the institutional and organizational differences between traditional finance and decentralized finance (DeFi), with a focus on public, permissionless blockchains. In traditional markets, intermediaries provide custody, authentication, settlement, and regulatory compliance. By contrast, the option of self-custody and open access on blockchains fundamentally reshapes the organization of financial services and challenges the foundations of current regulatory approaches. These structural differences alter trading, lending, and derivatives markets while introducing risks such as smart contract failures and infrastructure concentration. At the same time, DeFi's openness reduces entry barriers, improves transparency and access, and fosters competition and efficiency. Because self-custody removes intermediaries as enforcement points, regulation cannot simply extend existing frameworks. I conclude with policy recommendations emphasizing self-custody rights, privacy protection, adaptive regulation, and integration pathways for traditional intermediaries.



Andreas Park is a Professor of Finance at the University of Toronto, appointed to the Rotman School of Management and the Department of Management at UTM.

The **Wharton Initiative on Financial Policy and Regulation** is directed by **Itay Goldstein**, the Joel S. Ehrenkranz Family Professor and Professor of Finance at The Wharton School of the University of Pennsylvania. It commissions white papers from leading and emerging experts on a range of topics on financial policy and regulation. For more, see <https://wifpr.wharton.upenn.edu/>

# *DeFi vs. TradFi: Institutions and Industrial Organization*

Andreas Park

October 5, 2025

## **Abstract**

This paper analyzes the institutional and organizational differences between traditional finance and decentralized finance (DeFi), with a focus on public, permissionless blockchains. In traditional markets, intermediaries provide custody, authentication, settlement, and regulatory compliance. By contrast, the option of self-custody and open access on blockchains fundamentally reshapes the organization of financial services and challenges the foundations of current regulatory approaches. These structural differences alter trading, lending, and derivatives markets while introducing risks such as smart contract failures and infrastructure concentration. At the same time, DeFi's openness reduces entry barriers, improves transparency and access, and fosters competition and efficiency. Because self-custody removes intermediaries as enforcement points, regulation cannot simply extend existing frameworks. I conclude with policy recommendations emphasizing self-custody rights, privacy protection, adaptive regulation, and integration pathways for traditional intermediaries.

Economic interactions inevitably occur within a framework of institutional constraints shaped by both legal and technological factors. Regulatory interventions and institutional guardrails should, therefore, be understood as responses to existing technological and institutional conditions. Blockchain represents a fundamentally new technology, introducing its own set of constraints while potentially alleviating others.

This paper highlights economically significant differences in technological constraints that blockchain introduces. These differences shape business models, alter business opportunities, and redefine the roles of market participants in environments where blockchain is adopted.

For this paper, I focus on the setting that most sharply departs from traditional finance. In traditional markets, investors almost always hold assets through third-party custodians and can access, use, or trade them only by instructing intermediaries to act on their behalf. By contrast, I define a blockchain setting as one in which users (can) hold assets in self-custody, retain unrestricted control over their use, and where access

to the network is in principle open to anyone.<sup>1</sup> This distinction establishes a clear basis for analyzing four key organizational differences between traditional and decentralized finance: delegated versus self-custody; intermediated versus direct, pseudo-anonymous, and unvetted access to financial infrastructure; the ability to build on the infrastructure, including issuing new assets; and differences in transparency and privacy.

These organizational differences create significant economic and risk implications. Self-custody in decentralized finance and unfiltered access to financial infrastructure eliminate the need for intermediaries, but also broaden the competitive environment: users can access a wider range of services directly, and competing providers can reach customers without going through gatekeepers. As a consequence, no entity directly restricts access, provides protection, delivers information by default, or enforces compliance with regulations. Removing interme-

---

<sup>1</sup>Crypto-exchanges such as Binance, Coinbase, and Kraken, while significant participants in the crypto- and blockchain ecosystem, are custodial entities. Hence, for this paper, they belong to traditional finance.

diaries also eliminates conflicts of interest that arise when intermediaries make decisions on behalf of clients. Unvetted, pseudo-anonymous access allows users to create duplicate identities, complicating credit scoring and potentially enabling malicious actors. Furthermore, anyone can develop applications—legitimate or malicious—based on different standards and requirements.

Even though blockchain accounts are represented simply by alphanumeric addresses, all transactions, by default, are traceable back to their genesis. Consequently, once an account is linked to an individual or firm, all past and future transactions become identifiable, posing threats to privacy and raising substantial concerns for businesses. An overly restrictive regulatory “know-your-client” approach intended to eliminate criminal activity may negatively impact technology adoption and usage. Conversely, without associating accounts with specific individuals or entities, enforcing taxation and detecting money laundering is challenging.

Finally, although cryptographic tools generally ensure transactions cannot be manipulated or falsified, clearing and settlement processes on blockchains remain challenging for users and application designers because settlement participants may have the ability to interfere.

Traditional finance places significant emphasis on intermediaries. They guarantee essential functionality: intermediaries ensure assets exist and are authentic, confirm parties control their assets, and guarantee transaction settlement. Conceptually, blockchain replaces and simplifies these functions, as all assets are recorded on a single, publicly visible ledger. In the first part of this paper, I revisit these institutional arrangements and identify which intermediary roles blockchain supplants.

However, despite blockchain’s advantages, its applications must still address core economic challenges in finance, traditionally often facilitated by intermediaries. Participants must find counterparties; liquidity must exist to facilitate trades; arbitrage mechanisms must function effectively; traders remain concerned about front-

running, price manipulation, and trading against more informed parties; market manipulation can and will occur; parties entering future-oriented contracts must trust in eventual payment; investors require adequate disclosure and reliable data to make informed decisions; and issuers must manage ownership transparency and control risks.

In the second part of this paper, I contrast traditional and decentralized approaches to these core financial functions, highlighting challenges, emerging risks, and opportunities. Specifically, I examine how blockchain influences user and investor actions, how issuers of financial instruments leverage blockchain technology, how intermediary roles evolve or adapt to blockchain adoption.

Lastly, I discuss the role of and implications for regulators and regulation. Institutional frameworks evolve organically over time in response to existing technological constraints, and regulatory rules are often reactions to specific institutional arrangements. When new technology emerges, it is incorrect to assume that existing rules and institutional structures were universally optimal or that they should simply extend to new contexts. Likewise, it is suboptimal to force processes arising from new technology into frameworks designed for older technologies. Nevertheless, traditional regulatory frameworks serve important functions, and their underlying policy objectives —such as investor protection— remain relevant despite technological changes. The challenge is striking a balance: ensuring market fairness and investor protection while allowing efficient technologies and services to succeed.

One of the central regulatory challenges is convenience. In traditional finance, intermediaries are essential to financial transactions. Consequently, regulators can delegate compliance enforcement to a small number of institutions, rather than imposing complex regulations directly on numerous citizens who might fail to comply, often simply due to ignorance. However, when anyone can create tokens and sell them via blockchain, and when transactions are genuinely peer-to-peer, new regulatory challenges emerge.

## The Paperwork Crisis & the DTC: Will Blockchains bring the Certificate-less Society?

In the late 1960s, daily trading volume on the New York Stock Exchange (NYSE) rose from roughly 5 million to over 12 million shares. The surge overwhelmed manual back-offices because settlement still required the physical delivery of stock certificates. Brokers relied on couriers, which led to processing delays, misplaced or stolen certificates, and widespread failed trades. This paperwork crisis nearly halted market operations, caused numerous broker-dealer failures, and ultimately triggered the establishment of the Depository Trust Company (DTC) in 1973 as a centralized depository and book-entry system to replace physical transfers. However, both policymakers and the securities industry, wary of monopolist utility-style structures, regarded the DTC and the broader indirect holding model as a temporary, second-best solution to bridge the crisis until a fully certificate-less society could be achieved (see, e.g., SEC Historical Society archives and BASIC Committee records). If physical certificates were once the only legitimate ownership record, are tokens on a public blockchain the long-anticipated certificate-less technology?

As the proliferation of blockchain technology has demonstrated, these tools inevitably attract misuse by organized crime, fraudsters, and hostile state actors.

In my mind, the key innovation of a blockchain is that it is philosophically open in the sense that it serves as a platform for anyone to use and build on and explicitly does not seek to create “walled gardens.” In an ideal world, this approach fosters maximum competition among service providers and maximum liberties and choices for users. Therefore, in this paper, I focus on public, permissionless blockchains such as Ethereum, Algorand, and Avalanche. While I aim to remain technology-neutral, I place particular emphasis on Ethereum because it hosts the majority of decentralized finance applications and its Ethereum Virtual Machine has become the de facto standard for blockchain operations.

Private, permissioned blockchains also exist, but these largely resemble traditional private-sector arrangements. Technologically, such systems have been feasible for decades, as they require only a group of trusted parties to coordinate on a shared database and computational resource. Economically, these systems are just a different version of a walled garden that requires strong regulatory oversight and runs the risk of parties creating and then exploiting entrenched

network effects for rent extraction. Regulators and many financial institutions may instinctively favor these systems because of their closedness and because there is “someone in charge,” but, at least in my opinion, they resemble intranets relative to the internet: functionally limited and of little relevance to the transformative aspects of public blockchains, and I will not discuss such private networks here.

The paper proceeds as follows. Section 1 examines ownership arrangements in traditional finance and on blockchains. Section 2 considers Know-Your-Customer (KYC) and Anti-Money Laundering (AML) provisions. Section 3 analyzes differences in the trading and exchange of standard assets in traditional finance and on blockchains, including a discussion of blockchain-based trading, derivatives, and lending platforms. Section 4 reviews the “traditional” challenges outlined above and how they are addressed in blockchain networks. Section 5 compares risk factors in traditional and blockchain finance, and Section 6 highlights the resulting challenges for regulators. Section 7 describes existing and potential pathways for traditional financial firms to integrate with decentralized finance. Section 8 summarizes, and Section 9 sets out policy recommendations.

# 1 Ownership of Assets

## 1.1 Crypto vs. Traditional Assets

The central objective of this paper is to compare traditional and decentralized finance. This naturally raises the question of how to classify the assets used in decentralized finance—often called “digital assets”—and how they relate to traditional financial instruments. Over the past decade, new blockchain-based assets have emerged that, while functioning as financial instruments, do not fit neatly into existing regulatory taxonomies. Although such assets raise important economic and regulatory questions and significantly expand financial contracting possibilities, a thorough treatment of their nature and legal standing lies beyond the scope of this paper.

Instead, I focus on traditional financial instruments—such as equities, bonds, and derivatives. I implicitly assume that tokenized representations of existing assets can be used on blockchain systems and examine how their custody, ownership, and trading would operate on blockchain-based infrastructures. By examining institutional differences and overlaps systematically, I can thus provide insights to help policymakers identify new risks, recognize obsolete ones, determine where existing regulatory frameworks might apply, and assess the necessity of new regulatory measures for blockchain-based systems.

## 1.2 Accounts and Custody in Traditional Finance

Opening either a bank deposit account or a brokerage account requires providing proof of identity and other information for Know-Your-Customer (KYC) compliance. In the U.S., banks must implement a **Customer Identification Program (CIP)**, collecting at minimum the customer’s name, date of birth, address, and an identification number (such as an SSN for U.S. persons). Depositors then fund accounts with cash, checks, or electronic transfers.

Legally, a bank deposit becomes an asset of the bank, creating a debt owed to the depositor.

The depositor is thus an unsecured creditor of the bank. Deposits are essentially commingled on the bank’s balance sheet rather than held in segregated accounts. Banks typically hold only a fraction of deposits as reserves (vault cash or settlement balances with the central bank) and use the rest for loans or investments. Deposits in insured banks are **protected by the Federal Deposit Insurance Corporation (FDIC)** up to \$250K per depositor, per insured bank, per ownership category. If a bank fails, the FDIC, acting as receiver, arranges a transfer of deposits to a healthy bank or directly compensates depositors. Customer liability is also limited if accounts are compromised, provided issues are reported promptly.

Internationally, many banks offer USD-denominated accounts; these are typically backed by correspondent (nostro) accounts with U.S. banks, meaning the dollars ultimately reside in the U.S. banking system even if the legal claim is against a foreign bank.

Brokerage accounts differ in important ways. In brokerage accounts, customer funds and securities are held for investment purposes, not for institutional lending unless the customer explicitly permits it. U.S. securities laws require broker-dealers to segregate customer assets from their own. With margin accounts, funds and securities are also held as collateral. Under the SEC’s Customer Protection Rule (Rule 15c3-3), brokers must safeguard customer money and securities by maintaining fully paid and excess margin securities in their possession or a designated “good control” location, and by holding customer cash in a special reserve bank account (**Segregation of Assets**). Unlike banks, brokers cannot use client cash for their own business activities. Customer securities are usually registered in the broker’s nominee name (street name), often under “Cede & Co.,” the nominee for the Depository Trust Company, while the broker’s internal records show the investor as the **beneficial owner**. This arrangement simplifies trading but preserves investor rights to dividends, sales proceeds, and other entitlements. I explain the background of the DTC in a sidebar.

Cash balances in brokerage accounts are han-

dled differently from bank deposits. Uninvested cash is often “swept” into money market funds, FDIC-insured bank deposit programs, or held in the reserve account mentioned above. Brokerage accounts are not covered by FDIC insurance; instead, they are protected by the **Securities Investor Protection Corporation (SIPC)**, which covers up to \$500K per customer (including a \$250K cap on cash). SIPC doesn’t guarantee market value but aims to recover/replace missing securities/cash if a broker-dealer fails. In practice, segregation rules and SIPC protections usually ensure investors recover their assets.

In sum, a bank deposit is a debt claim against the bank, a brokerage account preserves customer ownership of securities, with cash balances held separately in trust. As discussed in the next section, blockchain-based asset ownership is conceptually closest to brokerage accounts rather than bank deposits. Accordingly, I abstract from bank-related arrangements.

### 1.3 Ownership with Blockchains

Blockchain technology comprises three core components: first, public-private key cryptography for securing individual transactions; second, hash-linked data structures that maintain consistent data and ensure historical blocks cannot be altered; third, a consensus protocol governing how new blocks are validated and added by competing validators. Since numerous papers describe blockchain mechanisms extensively, I will not repeat those details here.<sup>2</sup>

My focus is specifically on ownership attribution. Every crypto asset is associated explicitly with a blockchain address or account number by design. Ethereum defines two types of **accounts**:

---

<sup>2</sup>The first operational implementation of intermediary-free, peer-to-peer value transfers was the Bitcoin network, enabling decentralized transfer of a single asset: bitcoin. Fundamentally, a bitcoin transfer involves the network collectively executing specific operations. Ethereum generalizes this concept by allowing arbitrary sets of commands, enabling applications with potential capital market uses. Good resources for the workings of consensus are Harvey, Ramachandran, and Santoro (2021), Biais, Bisire, Bouvard, and Casamatta (2019), Saleh (2021), or Buterin (2022).

externally owned accounts (EOAs) and smart contract accounts (SCAs). An EOA resembles a conventional account number (on Ethereum, similar in length to a European IBAN), derived directly from a public key. This public key is, in turn, generated from a private key via public-private key cryptography. The private key grants control over crypto-assets and is required to sign transactions. When a user directly controls their private keys, the arrangement is termed *self-custody*; when a third party holds the keys, the arrangement is termed *custodial*.

In contrast, a smart contract account represents executable code registered on the blockchain. Its behavior is strictly determined by this code. Examples include decentralized applications allowing users to lend or borrow crypto assets or the code responsible for generating blockchain assets, such as tokens.

This paper emphasizes self-custody arrangements. Additionally, interactions with smart contracts involve users calling specific contract functions. The unrestricted ability to call these functions is a key characteristic of self-custodial blockchain environments. This feature is particularly important for decentralized finance applications that pool assets. In such applications, users “deposit” assets into pools via smart contract calls and later execute different smart contract calls to withdraw these assets.

Ultimately, ownership of assets on blockchain networks is always explicitly tied to an address, leaving no ambiguity regarding asset ownership.

Since a blockchain address can also represent a smart contract —such as a liquidity pool or blockchain bridge— and since users can hold claims on assets stored within these contracts, determining *beneficial* ownership ((i.e., identifying the ultimate individual or entity that economically benefits from holding the asset) is not straightforward. Furthermore, because anyone can generate a public-private key pair, the natural person or legal entity owning an asset is typically unknown by default. These characteristics complicate the direct application of traditional market rules (e.g., dividend payments or accrued bond interest) to blockchain environments because these rules rely on clearly knowing the as-

set holders at any point in time.

To illustrate these issues, I describe three common decentralized finance (DeFi) ownership attribution models. In each case, users deposit assets in a smart contract and receive a receipt token to signify their deposit. In each case, knowledge of who owns the receipt tokens is sufficient to determine ownership claims at any given moment, but the exact number of underlying tokens represented by a claim continuously changes. Notably, deposit and receipt tokens are transferable, tradable, and can be used as collateral.

The first model involves deposits in automated market maker (AMM) protocols like [UniSwap](#). A liquidity provider (LP) contributes a pair of assets to a liquidity pool, specifying the price range over which these assets will be available (mathematical details are omitted here). The LP receives a token encapsulating details of their liquidity position —formally an ERC-721 token (a non-fungible token or NFT)— which can be redeemed at any time for the original deposit plus any accumulated fee income. This receipt token does not represent a fixed quantity of tokens but varies according to the trades that liquidity demanders execute against the pool.

The second attribution model follows decentralized lending pools such as [AAVE](#). Here, upon depositing tokens, the liquidity provider receives a 1:1 allocation of corresponding a-tokens (e.g., depositing 2 USDT yields 2 aUSDT tokens), with balances tracked and updated by the liquidity pool’s smart contract. The LP accrues interest over time based on borrowers’ activity, reflected by an increasing a-token balance. Upon withdrawal, the LP exchanges their a-tokens back to the original tokens at a 1:1 ratio.

The third approach follows decentralized lending protocols like [Compound](#). In this model, depositors receive c-tokens representing fractional ownership of the pool at the time of deposit, calculated based on the circulating supply of c-tokens. The pool’s smart contract maintains aggregate deposits and interest accruals. When withdrawing, depositors receive an amount proportional to their fractional ownership, as indicated by their c-token balance.

## 1.4 Summary Comparison

In traditional finance, asset ownership involves complex intermediation, typically relying on centralized entities to simplify transaction settlement. This arrangement includes built-in information barriers that protect essential client information without revealing unnecessary details. A broker knows client identities and holdings held through them (but not at competitors), while a transfer agent tracks beneficial ownership, enabling issuers to identify asset holders when needed. No single entity typically knows all assets an individual owns or their complete activity history. With brokers’ assistance, transfer agents ensure information, dividends, and voting rights reach asset owners.

In contrast, blockchain accounts can be created freely and without restrictions. Asset ownership is attributed to pseudo-anonymous blockchain addresses, with the identity behind each account unknown by default. Furthermore, blockchain assets can be held by smart contract accounts, allowing multiple individuals to maintain separate claims on assets stored within the same smart contract. All actions involving an account are publicly visible on the blockchain network. By default, no transfer agent maintains beneficial ownership records, making it difficult for asset issuers to identify their owners. Distributing dividends or voting rights to blockchain accounts is also challenging, particularly for pooled assets held in smart contract accounts, as these contracts may not be designed to accept or relay such rights or payments to underlying owners.

## 2 Compliance with Know-Your-Customer and Anti-Money-Laundering Rules

### 2.1 KYC in Traditional Finance

most of the discussion on regulation in this paper considers preventative rules rather than the punitive and enforcement dimension following rules violations. Know-Your-Customer (KYC) rules stem from two distinct regulatory tradi-

tions. The first tradition focuses on investor protection, emphasizing suitability of investment products in relation to client objectives and risk tolerance. These practices originated in U.S. securities regulations in the 1930s, notably evolving through NASD rules requiring brokers to assess client financial situations for suitability purposes. Modern KYC rules, however, primarily emphasize customer identification and monitoring due to anti-money laundering (AML) laws, notably beginning with the 1970 U.S. Bank Secrecy Act (BSA).<sup>3</sup>

The Bank Secrecy Act of 1970 required financial institutions to maintain records of cash transactions and report suspicious activities to government authorities. Initially intended to deter tax evasion and financial fraud, the BSA evolved into a cornerstone of AML efforts. Subsequent amendments expanded reporting obligations, transforming financial institutions into active participants in law enforcement efforts against illicit financial flows.

Following the September 11, 2001 attacks, global financial regulation intensified, focusing heavily on preventing terrorist financing. The USA PATRIOT Act of 2001 significantly enhanced KYC and AML requirements, mandating financial institutions to implement Customer Identification Programs (CIP) and conduct continuous transaction monitoring. Concurrently, international organizations such as the Financial Action Task Force (FATF) promoted standardized measures against money laundering and terrorist financing (abbreviated as CFT for “combating the financing of terrorism”). Financial institutions became obligated not only to verify customer identities but also to closely examine transactions for potential illicit activity.

Today, KYC, AML, and CFT measures are fundamental components of financial regulation globally. Originally designed to protect customers from unsuitable investments, these mea-

asures now primarily function as tools for screening individuals and monitoring transactions and entities considered high-risk due to potential involvement in money laundering, terrorism, or other financial crimes. The regulatory burden and penalties for non-compliance have intensified. Although these measures have reduced illicit financial activities, they have also raised concerns about privacy, financial exclusion, and regulatory overreach.

## 2.2 KYC and AML with Blockchains

**Privacy and Secrecy.** Blockchain transfers occur directly between accounts. By default, all transactions are perfectly traceable, even if the identities behind blockchain addresses are unknown. For instance, when someone uses an online retailer to purchase goods with blockchain assets such as stablecoins, the retailer learns both the customer’s blockchain and physical addresses, enabling them to trace all blockchain-based activities associated with that address. Similarly, when a firm conducts a business deal on-chain, all related actions—including potentially sensitive contract terms or interactions with competitors—may become publicly visible.

If blockchain transactions were restricted exclusively to KYC-verified accounts, the KYC provider would know all activities of these accounts. For instance, if the KYC provider is a broker-dealer, they would in particular know the interactions of their clients with their competitors. For example, if a hedge fund enters a blockchain-based transaction, both the counterparty and the KYC provider could trace every trade and investment involving the hedge fund’s address. Moreover, financial institutions’ holdings would become publicly observable, increasing risks such as front-running or market squeezes.<sup>4</sup> If the KYC provider gets hacked or leaks information to an unauthorized party, substantial quantities of individuals’ private infor-

---

<sup>3</sup>Bank Secrecy Act of 1970 (31 U.S.C. §5311 et seq.); USA PATRIOT Act of 2001, Title III (International Money Laundering Abatement and Financial Anti-Terrorism Act); Financial Action Task Force (FATF) recommendations ([FATF Recommendations](#)); FINRA Rule 2111 (Suitability) ([FINRA Rule 2111](#)).

---

<sup>4</sup>An alternative perspective exists, noting that institutional solvency could be publicly verified in real-time. Following the FTX collapse, many crypto trading platforms adopted this approach to demonstrate asset reserves and liabilities transparently.

## The Bank “Secrecy” Act of 1970

The term “secrecy” in the BSA is misleading, as clarified by the 1976 Supreme Court case *United States v. Miller*. In this case, the Court ruled that individuals do not have a reasonable expectation of privacy for financial records held by third parties, such as banks. In *Miller*, federal agents obtained bank records, including deposit slips and checks, without a warrant, relying on BSA authority. The defendant, Mitchell Miller, argued this violated his Fourth Amendment rights against unreasonable searches and seizures. The Court rejected his argument, reasoning that Miller had voluntarily shared his financial information with the bank, thereby forfeiting any reasonable expectation of privacy in those records. This decision established the “third-party doctrine,” under which information shared with third parties (e.g., banks, phone companies) is not protected by the Fourth Amendment.

The *Miller* ruling provided the legal foundation for BSA-based financial surveillance, including requirements for banks to file Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) routinely, without warrants or probable cause. This precedent underpins the U.S. government’s authority to monitor financial transactions extensively.

It is noteworthy that the U.S. approach to privacy is not universal. For instance, a recent court ruling in Canada strengthened citizens’ privacy protections. This ruling emerged in response to the Trudeau government’s directive that banks freeze accounts of individuals associated with the “Convoy Protests” without court authorization, a measure aimed to disrupt financial support sustaining the protests. However, the Federal Court of Canada determined that freezing bank accounts and collecting financial information without judicial oversight constituted unreasonable search and seizure, violating Section 8 of the Canadian Charter of Rights and Freedoms.

This Canadian ruling contrasts with the U.S. Supreme Court’s decision in *United States v. Miller* (1976), where the Court held no reasonable expectation of privacy exists for financial records held by third parties. The Canadian court recognized a higher standard of privacy concerning financial information, particularly when government actions could be perceived as overreaching.

mation could be revealed, exposing the affected individuals or businesses to significant abuse and harm. Such transparency poses severe privacy concerns for individuals, and businesses would be reluctant to publicly disclose their dealings to this extent.

At the same time, organized criminals have leveraged blockchain technology to steal and move funds on an unprecedented scale, exemplified by the recent US\$1.4B [ByBit hack](#), allegedly carried out by North Korea’s Lazarus Group. There is clearly societal value to prevent criminals and terrorists from using the technology.

The big question is: can users be provided privacy without enabling criminal activity?

**Present Approaches to AML/CFT.** Currently, I am aware of six primary approaches aimed at curtailing criminal blockchain activities. The natural starting point to intercept illicit funds is at the crypto on- and off-ramps.

Most users initiate blockchain activity by purchasing crypto assets with fiat money, typically through a money services business (MSB) in Western countries. These MSBs must adhere to stringent regulatory standards. For example, transactions above \$1,000 require identity verification, likely to limit anonymous financial flows, those above \$3,000 must be recorded to keep transaction trails, and transactions exceeding \$10,000 trigger mandatory reporting to regulatory agencies such as FinCEN to flag large

scale suspicious activities.<sup>5</sup> Organized crypto-trading platforms generally require significant KYC procedures, similar to traditional finance.

Thus, barring theft or illicit dealers, most users leave identifiable trails in their crypto transactions.<sup>6</sup> Regular users typically undergo rigorous KYC processes; however, these individuals are generally not the primary target of AML and KYC regulations. Once blockchain assets leave regulated platforms, the situation becomes complex, and there are numerous ways legitimate funds might reach criminal entities.

The first approach to prevent money laundering involves limiting deposit amounts to prevent organized criminals from employing ordinary users as “mules” to funnel illegal funds into regulated systems. In this scenario, crypto on/off-ramps would impose transaction limits. While effective in restricting large-scale criminal activities, this approach could frustrate legitimate users and hinder practical capital-market operations on-chain.

A second approach involves blocking or disabling sanctioned addresses. Off-ramps would refuse funds originating from addresses identified as associated with criminal activities, or in stricter implementations, addresses that have interacted with criminal entities. For tokens (as opposed to native cryptocurrencies), the underlying smart contract tracks holder balances, making it possible to freeze or censor specific addresses. Indeed, Circle and Tether together have frozen holdings in over 2,000 blockchain accounts, presumably due to OFAC sanctions. Likewise, OFAC sanctions can also be implemented by block proposers: Wahrstätter, Ernstberger, Yaish, Zhou, Qin, Tsuchiya, Steinhorst, Svetinović, Christin, Barczentewicz, and

---

<sup>5</sup>Notably, the \$10,000 reporting threshold established by the 1970 Bank Secrecy Act has never been adjusted for inflation. In today’s dollars, the equivalent would be roughly \$75,000 - \$80,000, meaning that the law now applies to far more transactions than when it was enacted.

<sup>6</sup>Tinn (2024) develops a theoretical model for asymmetric privacy in payments, where money spent is fully anonymous whereas money received is not. This model was part of a digital currency design effort, commissioned by the Bank of Canada in 2021, and arguably the model is most suitable for customer-merchant interactions.

Gervais (2024) provide an empirical analysis of the censoring of Tornado Cash related transactions. They show that “46% of block builders are OFAC compliant, but this level of OFAC compliance is not effective at censoring transactions. In particular, transactions by OFAC sanctioned entities are only delayed but not censored.” They also raise concerns in that the presence of censorship slows down all transactions. A further downside of this approach is that it can harm innocent users who have unknowingly interacted with a bad actor’s address and whose legitimate funds may get locked.

Third, for tokenized real-world assets such as stocks, regulators might seek to enforce KYC rules comparable to traditional finance, in particular requiring firms to know their beneficial owners. However, this method resembles a “whack-a-mole” strategy, as criminals can easily generate new addresses. Moreover, blockchain users cannot prevent receiving funds from criminal addresses, causing inadvertent associations and numerous false positives.

Fourth, several private firms, such as Chainalysis and Integra FEC, offer blockchain analytics services that analyze on-chain data to flag suspicious actors. This approach, however, also tends to produce numerous false positives.

A fifth approach involves “whitelisting” addresses, creating a list of accounts that have undergone a formal KYC process. Such a whitelist could be stored using a distributed file system such as IPFS (InterPlanetary File System). Token or application designs could restrict transfers exclusively to whitelisted addresses. However, when a token permits only whitelisted blockchain addresses to receive or hold the token and rejects transfers outside this whitelist, then this list must contain any defi application that users want to use. The reason is that defi applications are smart contract addresses, and usage of the dapp requires the smart contract to hold token balances. This strict approach thus likely faces practical implementation challenges, and may restrict users’ ability to fully utilize DeFi applications and negatively impact market efficiency, particularly by limiting arbitrage bots that rely on rapid transfers. Furthermore, given

blockchain transaction traceability, enforcing a brute-force KYC regime raises significant privacy and business secrecy concerns.

The sixth approach is a more nuanced approach of KYC and involves so-called “association sets” or “proofs of innocence.” Like whitelists, these sets include addresses whose owners have completed a KYC process.<sup>7</sup> Using zero-knowledge cryptography, a user can prove their inclusion in an association set without disclosing their identity so that they can conduct transactions via temporary account numbers, preventing traceability. Problems would emerge, however, if malicious actors managed to be included in these sets, and trust in the list administrator would remain necessary.

A more sophisticated and related approach, encapsulated in the Labyrinth protocol, involves decentralized compliance networks. Such networks ensure transaction anonymity but allow selective de-anonymization when illicit activities are identified. These networks consist of independent “Revokers” and “Guardians,” structured without centralized control. Users select potential revokers in advance, who can initiate de-anonymization requests upon identifying suspicious activity. Revokers must publicly post verifiable requests to trigger the review process, ensuring transparency. Guardians then vote on these requests. Guardians themselves do not see transaction details; information is only disclosed to the revoker if enough guardians approve the request. This configuration reduces risks of malicious surveillance, allowing de-anonymization only with legitimate justification.

**Additional Thoughts.** Unsurprisingly, research into privacy and compliance continues. A fundamental difference between KYC in traditional finance and decentralized finance lies in the presence and central role of regulated intermediaries. In traditional finance, opening and maintaining accounts at regulated institutions is necessary to participate in finance, and the necessary involvement of intermediaries naturally ensures compliance with KYC rules. With-

---

<sup>7</sup>See also Duffie, Olowookere, and Veneris (2025) for a discussion on zkKYC certificates and the relation of zero knowledge proofs and KYC rules.

out automatic procedures provided by intermediaries, broad compliance in decentralized finance seems unlikely.

A more promising approach may involve designing incentive mechanisms that encourage voluntary compliance by offering clear benefits. For example, registries for tokenized traditional assets, as envisioned by Li, Singh, Veneris, and Park (2024), might include a KYC process and rewards compliant users in the sense of retaining rights such as shareholder voting, dividend distributions, and bond coupon and face value payments.

## 3 Transferring Assets and Financial Contracting

### 3.1 Traditional Finance

Once funds reside in a bank or brokerage account, an investor can acquire a range of financial assets. Here, I focus on four primary instruments—bonds, equities, options, and futures—to highlight the key functions that support markets: centralized clearing and settlement, custody and ownership records, and the mechanisms of margin and collateralization.

#### 3.1.1 Bonds and Equities

Corporate bonds and publicly traded stocks share similar infrastructures for execution, clearing, and settlement. Bonds may be acquired in the primary market through underwriters or in secondary OTC markets; equities are typically bought on organized exchanges. In both cases, trades clear through the National Securities Clearing Corporation (NSCC), which nets obligations and serves as central counterparty (CCP), and settle through the Depository Trust Company (DTC). DTC transfers securities in electronic book-entry form, with nearly all assets held in street name under its nominee, Cede & Co., while brokers maintain records of beneficial owners. Cash settlement occurs via NSCC netting and payment systems such as Fedwire, ensuring delivery-versus-payment (DVP).

Although bonds and equities differ in their economic features—bonds as debt contracts (with trustees protecting bondholders) and equities as residual ownership claims—both rely on custodians, transfer agents, and DTC/NSCC to manage ownership records, corporate actions, and investor rights. Transfer agents are especially important for equities, ensuring accurate records of shareholder ownership and managing dividends, proxy votes, and stock splits. Tokenized versions of both bonds and equities are beginning to circulate on blockchains (see Figures 1 and 2).

### 3.1.2 Options and Futures

Options and futures are standardized contracts traded through exchanges and cleared by centralized clearinghouses. The Options Clearing Corporation (OCC) clears equity and index options, while CME Clearing manages futures. In both cases, the clearinghouse novates contracts, acting as buyer to every seller and seller to every buyer, thereby guaranteeing contract performance.

Unlike bonds and equities, which involve custody of securities, options and futures rely on margin collateral. Investors post initial margin to brokers or futures commission merchants (FCMs), who in turn post to the clearinghouse. Positions are marked-to-market daily: variation margin credits gains and debits losses, ensuring that clearinghouses avoid accumulating credit exposures. If losses exceed posted margin, investors receive margin calls; failure to meet calls leads to liquidation. Contracts can typically be closed before maturity; those held to expiry may be cash-settled or physically delivered (e.g., futures contracts resulting in warehouse receipts).

Securities accounts have protections such as SIPC insurance, but derivatives accounts do not. Instead, investor protection relies on margin segregation rules and the clearinghouse’s guarantee fund. Derivatives arrangements highlight how risk management in modern markets depends on collateralization and daily settlement.

## 3.2 Decentralized Trading

The description of traditional financial assets highlighted the different arrangements for trading and roles, i.e., organized exchanges, clearing and settlement, OTC trading, options and future clearing, as well as the process for shorting and margins. The focus of this subsection is not on the assets themselves, but on how the functions that I identified for traditional assets functions emerge in decentralized finance.

### 3.2.1 Acquiring and Transferring Blockchain Assets

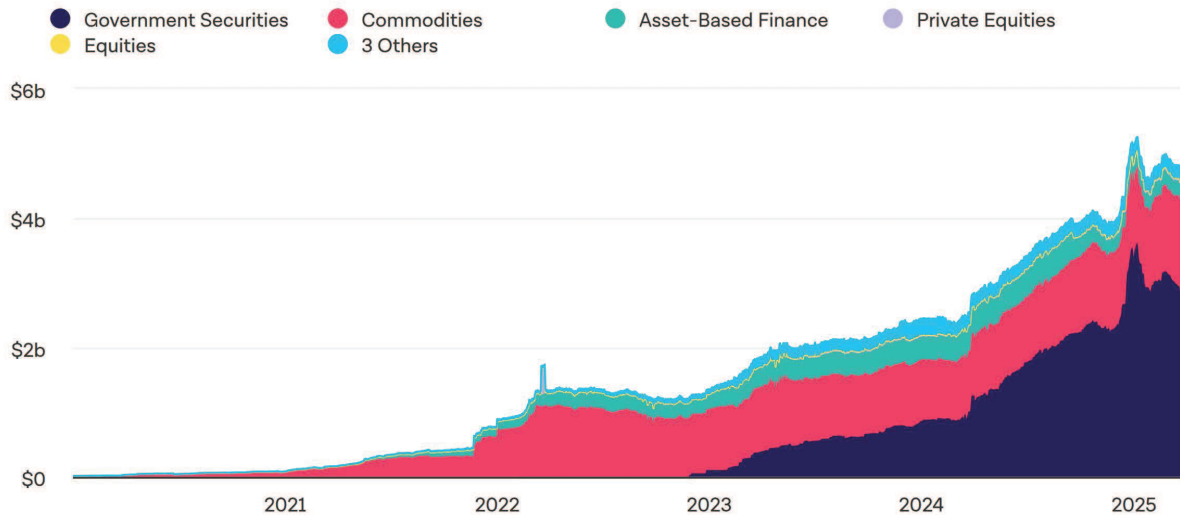
Presently, almost all new blockchain users use an “on-ramp” to obtain crypto-assets, meaning that they purchase crypto assets at a custodial exchange or related money business (including crypto ATMs). In principle, crypto-assets can be earned as coinbase or staking rewards for participating actively in the validation process, but for proof-of-stake blockchains—the primary focus of this paper—staking requires prior ownership of the asset. Users can also create new on-chain assets, but again this process requires paying the network fee in the native cryptocurrency which must therefore be acquired with an on-ramp. For this paper, I focus exclusively on transactions involving self-custody accounts. Therefore, I assume that users have moved their assets from an on-ramp provider to a self-custody account.

In blockchain networks, asset owners transfer assets by digitally signing transactions with their private keys, typically through software tools called crypto wallets. The wallet sends transaction details (including signatures and public keys for verification) and transaction fees to blockchain validators, who then include and process these transactions in blocks.

While interesting, I omit most underlying technical details and participants, except two key points. First, blockchain validator networks are borderless and permissionless: anyone meeting broad prerequisites—such as holding sufficient stake—can participate, regardless of jurisdiction or legal status. This creates a significant jurisdictional challenge: while a regulator may



## RWA Market Capitalization by Product Category (Daily)



SOURCE: 21CO VIA DUNE  
UPDATED: MAR 31, 2025

Figure 1: Traditional Assets on Public Blockchains

prohibit specific activity, anonymous or foreign validators may still process sanctioned transactions. For instance, after OFAC sanctioned Tornado Cash, permissionless validators (especially those outside U.S. jurisdiction) continued to process its transactions, despite growing reluctance among U.S.-based block proposers (Federal Reserve Bank of New York, 2024; Axios, 2024). Similarly, after the ByBit hack, platforms such as eXch and THORChain allowed the attacker to swap funds, despite ByBit’s urging not to. One may even ask what would happen if someone uses stolen funds to participate in proof-of-stake validation.

Second, cryptographic techniques ensure transactions cannot be altered during validation (for all practical purposes). However, transactions may fail if they violate smart contract conditions or may remain unprocessed if the attached fee is insufficient.

Peer-to-peer transactions are just one type of blockchain operation. General-purpose blockchains, like Ethereum, support arbitrary transactions, including creating new smart con-

tracts, tokens, applications, escrows, or accessing existing decentralized applications and tokens.

Traditional finance’s value chain arguably emerged to facilitate asset exchanges on existing markets: individuals gathered at specific physical locations (e.g., under New York City’s famous Buttonwood tree), organically giving rise to institutions that organize and support trading.

A blockchain, however, is fundamentally a general-purpose tool—not inherently a market nor initially designed to support an existing market. Though buyers or sellers can individually create smart contracts resembling limit orders, this method is costly (each order creation incurs transaction fees) and inefficient, as the entire network processes these contracts and counterparties must actively search for opportunities. Simply put, this method does not constitute an effective marketplace.

Yet blockchain technology enables the creation of decentralized marketplace applications, which I describe in the following sections.

## Ownership and Short Sales

Short sellers do not own the stock at the time of sale and must therefore borrow shares to ensure proper settlement. Before executing a short sale, brokers must locate available shares to borrow, a requirement mandated by SEC Regulation SHO. Shares are typically borrowed from institutional investors, mutual funds, pension funds, or margin account holders who have agreed to securities lending. The short seller must post collateral—such as cash or Treasury securities—with the lender.

To close the short position, the short seller repurchases shares in the market and returns them to the lender. Upon settlement of this repurchase, the broker delivers the shares to the original lender, concluding the securities loan and releasing the collateral. Although regulations address failures to deliver shares (FTDs) by settlement date, such failures still frequently occur, presenting challenges to market integrity.

A unique situation arises when an investor purchases shares on the cum-dividend date from a short seller. This investor becomes the new beneficial owner and, as of the dividend record date, will receive the dividend directly from the issuer as the registered shareholder. The original lender does not receive the dividend from the issuer despite owning the shares prior to lending.

To compensate, the short seller must provide the lender with a manufactured or “payment-in-lieu” dividend. This ensures that the lender does not incur financial loss due to lending shares. The practice of dividend compensation in short selling is governed by standard securities lending agreements and is well-established in market operations. See also Fabozzi and Mann (2005).

### 3.2.2 Non-custodial Trading Platforms

The most common blockchain-based trading mechanisms are automated market makers (AMMs).<sup>8</sup> Harvey, Hasbrouck, and Saleh (2024) discuss AMMs in detail. Briefly summarized, AMMs represent a novel type of trading institution based on a few core principles. Liquidity providers deposit assets into a liquidity pool, enabling traders (liquidity demanders) to trade against this pool by depositing one asset and withdrawing another. Exchange rates between assets depend deterministically on the pool’s liquidity at transaction time, without prioritizing individual liquidity providers. This design yields three key features. First, liquidity is continuously available for trading at any time. Second, a deterministic 1:1 mapping exists between traded quantities and prices. Third, all liquidity

providers collectively share trading risks and the collected fees.

As with all trading, liquidity providers face market risk, including adverse price movements leading to disadvantageous trades. In AMMs, this issue is particularly acute since price adjustments occur only through executed trades; thus, external price movements directly result in losses for liquidity providers. AMMs compensate providers for such adverse selection losses by charging liquidity takers a transaction fee.

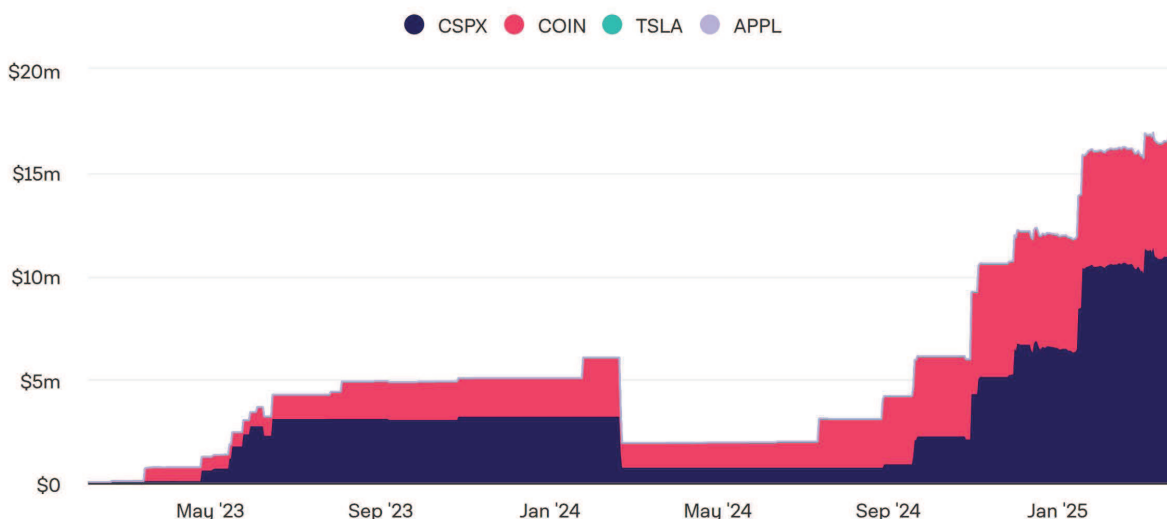
Various implementations of AMMs exist, differing in pricing algorithms and pool-access rules, and these systems have evolved into a diverse ecosystem. Several details merit highlighting. Users typically access AMMs in two ways: either by directly calling smart contract functions on the blockchain network or by using interfaces (websites or apps) that generate transaction requests for users and forward signed transactions to the blockchain. Early versions, such as UniSwap v2/v3 and SushiSwap, ran primarily on

---

<sup>8</sup>Non-custodial marketplaces resembling limit order books also exist; however, apart from early and now rarely used systems, these generally operate on layer-2 solutions to efficiently handle high transaction volumes.



## Equities Market Capitalization by Underlying Asset (Daily)



SOURCE: 21CO VIA DUNE  
UPDATED: MAR 31, 2025

Figure 2: Tokenized Equities of Public Blockchains

blockchain mainnets; today, increasingly many applications move to rollups or layer-2 solutions to benefit from higher throughput and lower fees. For instance, Uniswap recently launched a specialized layer-2 solution designed explicitly to reduce trading costs and latency. A main technological challenge at this point is the interoperability of the many emerging layer-2 solutions so as to avoid a world with captive audience which can ultimately lead to rent extraction and economic inefficiency. Innovation in AMM themselves is ongoing: Aggregators like 1Inch operate similarly to smart order routers in traditional trading and split user trade orders across multiple AMMs to optimize execution prices. UniSwap v4 now allows developers to create customized AMM variants tailored to specific client needs, such as optimized fee structures or enhanced liquidity-provider protection.

Compared to traditional finance, several distinctions stand out. First, although AMMs charge transaction fees—similar to traditional marketplaces—these fees primarily represent transfers from liquidity takers to makers, gen-

erating negligible or no direct revenue for platforms themselves. Additionally, AMMs typically do not charge data-related fees.

A substantial and growing literature examines AMMs, as reviewed by Harvey, Hasbrouck, and Saleh (2024). To highlight key insights, Lehar and Parlour (2023) show that AMM and centralized-market prices generally move in unison. Empirically, Barbon and Ranaldo (2025) compare liquidity between decentralized exchanges (DEXs) and centralized platforms, concluding that DEX prices are less efficient. Malinova and Park (2024) conduct a thought experiment, calibrating trading costs for an optimally designed AMM applied to U.S. equities, suggesting that AMMs could theoretically reduce trading costs by 18–30% relative to current equity market structures.

### 3.2.3 Non-custodial Lending Platforms

Trading frequently involves short-selling or margin buying, necessitating active lending markets for cash and assets. In traditional finance, bro-

kerages facilitate this process, relying on capital-intensive structures and supervised entities capable of sourcing assets internally or via broker networks. In decentralized finance, no broker organizes margin lending or short-selling, but specialized applications exist to facilitate borrowing and lending.

Decentralized lending platforms primarily include two application types: liquidity pool-based lending and minting protocols. In pool-based platforms, depositors contribute assets to non-custodial liquidity pools on public blockchains, earning interest income when borrowers access these assets. Both deposits and loans may involve multiple assets. Interest accrual is linked to transferable tokens received by depositors representing their pool contributions.

Because blockchain interactions are pseudo-anonymous, traditional credit mechanisms relying on credit scores are not applicable. Thus, all loans require collateral exceeding the loan value.<sup>9</sup> Procedurally, borrowers first deposit assets into a lending pool. Borrowing becomes available once part of this deposit is designated as collateral. Each asset eligible as collateral receives a collateral factor determined through protocol governance, specifying the maximum loan-to-value ratio. For instance, a collateral factor of 0.8 allows borrowing up to 80 cents for each dollar of collateral.

Borrowers receive loan proceeds from the general pool directly into their wallets. The protocol continuously tracks the outstanding loan balance and accrued interest. Loans are repaid by returning the borrowed amount plus accrued interest to the pool. Interest accrues block-by-block, with rates determined by pool utilization (the ratio of total borrowing to total deposits).

Minting protocols (such as Maker, recently rebranded as Sky Protocol) offer an alternative lending model. Here, users deposit collateral into a smart contract and subsequently “mint” new stablecoin tokens based on the collateral pro-

vided, where the minted quantity depends on collateral specifics and protocol parameters.

A crucial feature common to both minting and pool-based lending protocols is the liquidation mechanism. If collateral value falls below a predetermined threshold, third parties can repay the borrower’s loan and initiate collateral liquidation, thus preventing under-collateralization and reducing default risk.

Overall, a clear distinction between tradfi and defi management of counterparty risk emerges: traditional clearinghouses manage counterparty risk through guarantee funds, or collateral and regulation. Blockchain settlements instead relies on collateral pools and auto liquidation mechanisms.

### 3.2.4 Non-custodial Options Platforms

Cash markets for on-chain assets involve simple exchanges of one asset for another. Options are more complex since they involve future exchanges, requiring assurance that the option writer can deliver the underlying asset at expiration. In pseudo-anonymous environments, this creates similar challenges as with lending.

Multiple implementations of non-custodial options markets exist. Generally, the writer of an option acts as a liquidity provider (LP) or market maker. Though implementation specifics differ, these platforms typically incorporate elements of standard automated market maker (AMM) designs. For instance, consider Lyra Finance, which operates on several Ethereum layer-2 solutions. The lifecycle of an option on Lyra begins when an option writer deposits collateral into a liquidity pool, termed a Market Maker Vault (MMV). MMVs are asset-specific, akin to lending pools in that liquidity provider funds are pooled, and each MMV supports multiple option contracts simultaneously, differing by strike prices and expiration dates. Options are then traded via an AMM that dynamically prices and issues various options from this pooled collateral. Throughout the option’s life, collateral remains locked in the MMV, and liquidity providers accrue premiums paid by traders. At expiration, in-the-money options settle automat-

---

<sup>9</sup>An exception is “flash loans,” riskless by design. Flash loans, as offered on Aave, require borrowing and repayment within the same blockchain block, eliminating counterparty and liquidity risks; see, e.g., Lehar and ParLOUR (2022). Flash loans are excluded from our analysis.

ically against the collateral pool through Lyra’s smart contracts. After settlement, LPs can withdraw unused collateral along with accrued premiums. The protocol thus operates without margin or leverage beyond full collateralization, ensuring options remain fully backed.

The AMM serves as a pricing and risk-management algorithm layered on top of the collateral stored in the MMV. While the MMV provides pooled collateral backing multiple option contracts, the AMM dynamically determines premiums, manages trading, and hedges risk. The AMM itself does not store assets; rather, it interacts with liquidity held in the MMV. Its pricing mechanism effectively aims to identify the implied volatility balancing option supply and demand, adjusting premiums explicitly based on volatility.

In addition to the MMV (also referred to as the collateral pool), Lyra maintains a separate “delta pool,” dedicated explicitly to hedging delta exposure from option positions. Funds in the delta pool initially originate from liquidity providers but are allocated specifically for hedging. The delta pool actively trades underlying assets externally to maintain the desired risk profile, with resulting profits or losses flowing back into the delta and not the collateral pool.

When a liquidity provider on Lyra wishes to withdraw collateral before expiration, the process depends on the MMV’s current risk profile. First, there is a mandatory three-day waiting period before withdrawals can occur. Since the collateral pool supports multiple open option positions simultaneously, early withdrawals may impact the vault’s overall risk exposure.

If an LP requests early withdrawal, Lyra assesses existing positions to determine liquidity availability. Withdrawals potentially increasing the pool’s delta or vega exposure may incur penalties or fees. The AMM dynamically adjusts these penalties to discourage withdrawals that negatively affect the pool’s risk profile.

If sufficient liquidity exists and risk is unaffected, the LP may withdraw immediately, typically receiving their collateral share plus earned premiums, net of hedging costs or fees. Otherwise, the LP may have to wait or accept reduced

amounts reflecting the AMM’s hedging adjustments and the pool’s prevailing risk exposure.

### 3.2.5 Non-custodial Futures Trading Platforms

At the time of writing, the most actively used decentralized futures platform is Hyperliquid, operating on a dedicated, EVM-compatible blockchain capable of high throughput (claimed up to 200,000 transactions per second). This infrastructure enables an on-chain limit order book. Liquidity providers (LPs) deposit funds into an on-chain liquidity pool, making them available within the decentralized order book for perpetual futures trading.

Traders opening long or short positions deposit collateral into margin accounts. A trader in a long position profits from rising asset prices and incurs losses from declining prices, while short traders profit from price decreases and suffer losses when prices rise. A defining feature of blockchain-based futures markets is their perpetual nature: positions remain open indefinitely, with traders paying or receiving periodic funding rates to reconcile differences between the futures market price and the underlying spot price (usually sourced from external markets through an oracle).

Specifically, when traders open long positions, they effectively purchase perpetual futures contracts from liquidity provided in the on-chain order book. LPs deposit funds into this order book, collectively acting as counterparties by assuming short exposure proportional to their deposits. The trader’s collateral secures their position, while funding rates regularly align the futures prices with underlying spot prices.

Liquidity providers withdrawing funds can typically access their liquidity once associated open positions are settled, subject to current liquidity conditions. Withdrawals is immediate if ample liquidity is available or delayed if significant liquidity is committed to active positions.

Unlike fully collateralized options markets, Hyperliquid’s perpetual futures allow leveraged trading. Traders deposit collateral covering only a fraction of the total position size, borrowing

the remainder from liquidity providers. LPs collectively bear the exposure resulting from traders’ leveraged positions, facing both counterparty and market risks.

Collateral (margin) deposited by traders on Hyperliquid is structured to cover typical price movements. Margin requirements ensure collateral remains adequate. If market prices move adversely, collateral diminishes. Before collateral depletion, an automatic liquidation mechanism closes positions to protect LPs from absorbing losses exceeding traders’ collateral. Under normal circumstances, this mechanism effectively limits LP counterparty risk.

### 3.2.6 Ownership Transfers and the Role of Blockchain Settlement Process

Users create blockchain transactions, typically using wallet software, and send them to a network of validators. Below, I describe Ethereum’s process, noting that other approaches exist and Ethereum itself has evolved over time. Submitted transactions enter a pool of unsettled transactions (the “mempool”) where they await inclusion in a block, effectively representing final settlement.

Originally, validators handled the entire process: verifying transactions, selecting them, and assembling blocks. Over time, however, specialized service providers have emerged at various stages of the validation process. For example, a *searcher* identifies profitable transactions in the mempool and assembles bundles of transactions that are jointly profitable. Searchers submit these bundles to a *builder*, who constructs a block from multiple bundles. In essence, builders provide infrastructure services for assembling and transmitting new blocks, whereas searchers specialize in transaction bundling—though some entities combine both roles. The *block proposer*, selected to propose the next block, typically relies on builders to supply ready-made blocks, effectively delegating their proposal power.

Ideally, this process would be neutral and mechanical—as is generally the case in traditional finance—but in practice, at least for Ethereum, it is not. One might expect searchers

(or builders) simply to select transactions paying the highest fees. However, blockchain operations can be contingent upon one another, potentially creating profit opportunities. For instance, a transaction on one decentralized exchange may trigger an arbitrage opportunity elsewhere. A searcher recognizing this arbitrage opportunity will insert their own arbitrage transaction alongside the user’s original transaction, creating a profitable bundle. This incremental profit is known as maximal extractable value (MEV), and it is a highly controversial activity; see Daian, Goldfeder, Kell, Li, Zhao, Bentov, Breidenbach, and Juels (2020). Identifying and capturing MEV is challenging, requiring extensive data access, deep knowledge of decentralized applications, sophisticated analytical capabilities, and substantial resources. Indeed, MEV has driven the emergence of specialized roles and participants, significantly influencing the validation microstructure. Consequently, blockchain settlement infrastructure is not neutral; application designers and blockchain users must carefully navigate the potential pitfalls arising from these institutional arrangements.

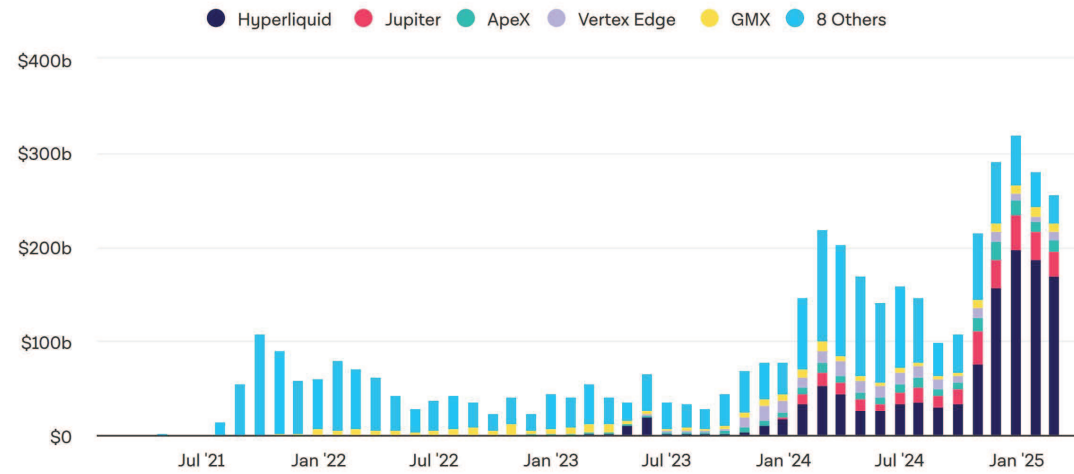
### 3.3 Why DeFi? The Benefits

Traditional finance relies on a complicated network of specialized intermediaries for its operation, all with separate databases and functionalities, bound together in a complex operational process. Even though components have been updated to databases instead of stacks of paper, this current market’s “plumbing” evolved organically over decades but is still rooted in markets that relied on shouted orders. A simple stock trade requires broker-dealers, trading platforms, custodian banks, clearing agencies, asset depositories, transfer agents, and the payments network to work in unison, with multiple reconciliation steps along the way. Arguably, if we could build a financial infrastructure from scratch, the operationally most efficient one would be a shared, single, centralized system for all assets.

And that’s what a blockchain is: as I outline in this section, it is a single system for asset creation, servicing, transfers, trading, pledging,



## Perpetual Protocol Trade Volume



SOURCE: DEFiLLAMA  
UPDATED: APR 2, 2025

Figure 3: Trading Volume of On-Chain Perpetual Futures

borrowing and lending, and any other form of financial contracting including arbitrary derivatives. These functions are no longer a possibility, numerous solutions already exist, albeit work on improving systems is ongoing.

More specifically, as illustrated by the traditional financial infrastructure, current capital markets exhibit considerable frictions and persistent inefficiencies, particularly in cross-border transactions. Blockchain technology presents several distinct comparative advantages: First, blockchain transactions are structurally atomic in the sense that all parts of the transaction either complete at the same time or fail altogether, eliminating certain forms of counterparty risk and simplifying liquidity management. Second, multiple asset types coexist on the same infrastructure, significantly easing and making more transparent processes such as asset pledging (using assets as collateral) and re-hypothecation (reusing pledged collateral for numerous transactions). This latter feature makes the technology particularly attractive to firms like Blackrock that would benefit from reducing their backoffice costs associated with managing assets across the various different systems. In his 2025 “[Annual](#)

[Chairman’s Letter to Investors](#),” Blackrock CEO Larry Fink further praises the tokenization of existing asset as a key mechanism to foster the democratization of investing, as a means to “helping current investors access parts of the market they’ve previously been restricted from” and “by enabling more people to become investors in the first place.”

Third, liquidity pooling enhances risk-sharing and reduces trading costs. Specifically, well-designed pool-based applications can incentivize non-intermediary market participants to contribute liquidity directly. Fourth, blockchain technology simultaneously provides greater transparency (by maintaining publicly verifiable transaction records) and improved privacy (through cryptographic techniques to protect sensitive user information), enhancing supervisory effectiveness and reducing regulatory costs. Fifth, as an open infrastructure, blockchain lowers entry barriers for innovators to introduce new financial products and technologies, thus fostering competition. Sixth, publicly available transaction data eliminates data monopolies, thereby reducing information costs for all market participants. Overall, a well-designed

blockchain environment can decrease operational costs, improve transparency, enhance systemic resilience, and significantly advance risk management through sophisticated digital analytics. Consequently, capital markets appear to be a prime candidate for blockchain adoption.

## 4 Challenges for DeFi

In the introduction, I outlined several ongoing challenges in decentralized finance. While some have been implicitly discussed in previous sections, I restate key insights here for clarity.

### **Finding Counterparties, Information Asymmetries, and Market Manipulation.**

A fundamental challenge involves finding trading counterparties. Although blockchains themselves are not inherently marketplaces, the decentralized finance community addresses this by developing new market institutions, notably liquidity pools. Rewards to liquidity providers can be structured to compensate adequately for trading with potentially informed counterparties. Early approaches were somewhat ad hoc, but recent innovations, such as UniSwap v4, enable more sophisticated and dynamically optimized reward systems.

**Arbitrage.** Another critical requirement is effective arbitrage. When multiple marketplaces operate on a unified blockchain infrastructure with atomic settlement, arbitrage tends to function efficiently. However, three concerns arise around current blockchain infrastructures:

First, the presence of multiple blockchain platforms (e.g., Ethereum, Avalanche, Algorand, Solana, Celestia) hosting separate capital market operations complicates arbitrage. Efficient arbitrage across these platforms requires temporary capital deployment on multiple chains, increasing costs. Bridging technology is continually improving, however, and settling arbitrage positions across chains is increasingly rapid, often taking mere minutes.

Second, arbitrage involving simultaneous trading on defi and traditional platforms requires the

bridging of two disconnected infrastructures. A similar concern applies when assets are traded on defi and tradfi simultaneously. Arbitrage here too requires the bridging of two systems, and speeds of traditional finance may not be compatible. Nonetheless, empirical work by Lehar and Parlour (2023) and Barbon and Ranaldo (2025) for the trading of crypto-assets on Binance vs. UniSwap suggests pricing discrepancies between decentralized and centralized markets diminish significantly after initial adjustment periods.

Third, the rise of layer-2 solutions introduces another dimension of complexity, as these also require additional capital commitments, thereby raising arbitrage costs. Ongoing development of bridging technologies—such as the Hop protocol—already enables seamless asset transfers across different layer-2 platforms, significantly mitigating this issue.

Lastly, comprehensive systems such as Crossmint offer integrated platforms that support stablecoins (and potentially other tokenized assets), providing wallet infrastructure, fiat on- and off-ramps, payment capabilities, tokenization services, and compliance solutions across multiple networks. Such integrations aim to facilitate smoother interactions and arbitrage opportunities between decentralized and traditional finance.

**Liquidity.** A valuable feature in decentralized finance (DeFi) is the availability of minting protocols, where users deposit assets into smart contracts and mint stablecoin tokens as loans against these assets. For major assets, this process is straightforward, transparent, and designed to ensure adequate collateralization. However, minting protocols constitute a narrow use case for stablecoins.

For broader asset classes, borrowers require willing lenders. In traditional finance, financial intermediaries managing accounts and market access serve as natural coordinators. These intermediaries attract depositors and borrowers by adjusting interest rate spreads, leveraging existing capital to offer incentives, or cross-subsidizing across different business lines.

Decentralized finance, by contrast, aims to replace intermediaries with peer-to-peer financial service platforms. The peer-to-peer model, however, depends critically on DeFi platforms successfully building liquidity on both sides of a decentralized market. Liquidity suppliers participate only if sufficient demand is expected, and demanders join only if liquidity supply is adequate. Given capital constraints and intense competition among platforms, DeFi application designers thus face the substantial challenge of simultaneously attracting both liquidity suppliers and borrowers.

Unlike traditional financial intermediaries, DeFi applications neither capture interest spreads nor possess direct access to capital for monetary incentives. Platforms have addressed the liquidity bootstrapping problem innovatively by rewarding users with protocol-native tokens. These tokens confer multiple benefits, such as governance rights over key platform parameters or implicit and explicit claims on future protocol revenues. Ideally, token distribution fosters a self-reinforcing growth cycle: early adopters support the platform, enhancing token value, which attracts additional participants, further strengthening protocol viability. This mechanism, known as “liquidity mining,” has emerged as a central strategy for many DeFi protocols to attract both capital and activity.

Designing these incentive programs is challenging. In a recent study, Park and Stinner (2023) examine liquidity mining programs on Ethereum’s two largest decentralized lending platforms at the time, AAVE and Compound. They find that introducing or increasing rewards significantly boosts user deposits and borrowing activity. However, this liquidity proves transient: reducing or terminating incentives triggers rapid capital outflows and declining borrowing activity. Such outflows raise concerns, as platforms cannot indefinitely sustain incentive programs. Ideally, platform activity should remain robust even after incentives diminish.

Additionally, a subset of users displays curious behavior by simultaneously depositing and borrowing the same asset. Although this pattern could establish leveraged positions, in practice

it predominantly occurs with stablecoins, where leverage provides no economic advantage. Instead, as Park and Stinner argue—supported by evidence that yield aggregators explicitly promote this strategy—users create these positions to maximize liquidity incentives from both deposits and borrowings, which are heavily concentrated (over 85%) in stablecoin pools. Because these borrowed funds are immediately re-deposited, they artificially inflate platforms’ balance sheets without providing genuine liquidity accessible to other users. Park and Stinner refer to this as “phantom liquidity,” since it is effectively unavailable to market participants.

A helpful analogy is pricing on ride-hailing platforms like Uber, which requires simultaneous participation from drivers and passengers. To stimulate participation, Uber occasionally subsidizes both sides. Phantom liquidity is analogous to a driver hiring themselves as a passenger to collect both subsidies, artificially inflating supply and demand metrics without adding genuine value. Although similar to wash trading (generally viewed as manipulative), Park and Stinner argue that, on balance, such opportunistic behavior contributes positively to overall welfare, though the benefits accrue unevenly.

Another factor contributing to phantom liquidity is the emergence of “yield aggregators,” a new class of blockchain-based asset managers. Yield aggregators are automated systems that continuously scan blockchain platforms to identify and exploit optimal returns, dynamically allocating user funds through smart contracts. Or, in the language of traditional finance, they take the role of decentralized, non-custodial asset managers. By overcoming information frictions and behavioral biases—such as limited attention and inertia—these aggregators rapidly shift capital between platforms in pursuit of the highest returns. While aggressive yield-seeking is typical in finance and can serve the important function of providing liquidity when needed, the speed and scale at which capital moves within blockchain systems intensifies competition. Consequently, blockchain-based platforms must design incentive programs capable of quickly establishing robust network effects; otherwise, these

## Liquidity Mining and Sushiswap’s Vampire Attack on UniSwap

The Uniswap -SushiSwap liquidity mining episode was a notable event in decentralized finance (DeFi) in late 2020, highlighting the dynamics of liquidity mining incentives, so-called “vampire attacks,” and competition among automated market makers (AMMs). Uniswap, a leading decentralized exchange (DEX) built on Ethereum, relies on liquidity pools where users deposit tokens to facilitate trading. In return, liquidity providers (LPs) earn trading fees. By mid-2020, Uniswap had emerged as the dominant AMM with substantial liquidity. In August 2020, SushiSwap launched as a fork of Uniswap, adopting an aggressive strategy to rapidly bootstrap its liquidity. Unlike Uniswap, SushiSwap introduced a governance token (SUSHI) offering additional incentives to LPs, going beyond Uniswap’s existing fee structure. Furthermore, SushiSwap implemented a liquidity migration strategy termed a “vampire attack,” incentivizing Uniswap LPs to move their liquidity to SushiSwap by offering them additional rewards in the form of SUSHI tokens. The process unfolded as follows:

First, SushiSwap introduced liquidity mining incentives, granting SUSHI rewards to LPs who staked their Uniswap LP tokens on SushiSwap. Second, this allowed LPs to simultaneously earn Uniswap trading fees while accumulating SUSHI tokens, creating a highly attractive opportunity. Third, at a predetermined date, SushiSwap migrated all staked liquidity from Uniswap to SushiSwap, effectively transferring over \$1 billion of liquidity from Uniswap in a single transaction. This vampire attack successfully bootstrapped SushiSwap’s liquidity at Uniswap’s direct expense, although the incentive structure temporarily boosted liquidity on Uniswap as well.

Initially resistant to issuing a governance token, Uniswap quickly responded to the vampire attack by launching its own governance token (UNI). Uniswap distributed UNI as rewards to liquidity providers and retroactively airdropped tokens to past users, significantly enhancing user loyalty and community support.

incentive programs risk becoming unsustainable “flash-in-the-pan” phenomena.

In related work, Gudgeon, Werner, Perez, and Knottenbelt (2020) analyze liquidity provider behavior and platform stability in defi lending. They find that that periods of illiquidity are common, often shared between protocols and that liquidity reserves can be very unbalanced. As Park and Stinner they find strong concentration of deposits, in their case with as few as three accounts controlling 50% of the total liquidity. They further report that realized interest rates concentrate around the “kink” in the interest rate function.

**MEV, Front-running, and Squeezes.** A persistent concern for market participants is the risk of competitors anticipating their trades

or exploiting knowledge of their positions to manipulate prices. This issue also arises in blockchain systems. The inherent transparency of blockchain transactions significantly increases visibility, potentially exposing sensitive asset positions—especially problematic when asset holders can be identified. Privacy-enhancing technologies may mitigate some of these risks.

Experienced finance professionals also recognize issues stemming from the non-neutrality of blockchain settlement infrastructure, as discussed earlier: submitting transactions to a public mempool reveals intentions and exposes users to front-running. Certain solutions exist, such as private mempools. Additionally, specific layer-2 solutions like UniChain aim explicitly to address these concerns. Alternative blockchain networks, including Avalanche and Solana, are of-

ten argued to be inherently resistant to front-running. Nevertheless, more extensive development and safeguards are likely necessary before capital market participants become comfortable conducting multi-million dollar transactions on blockchain systems.

**Solvency of Counterparties.** As discussed earlier in the context of borrowing, lending, and derivatives, decentralized finance platforms generally incorporate explicit mechanisms ensuring adequate collateralization of positions. Arguably, collateral requirements sometimes exceed optimal levels, but existing mechanisms effectively mitigate counterparty risk.

**Adequate Disclosure and Beneficial Ownership.** Clearly, numerous blockchain-based assets circulate with insufficient, misleading, or fraudulent disclosures—a natural consequence of a system allowing unrestricted asset issuance. For this paper, however, I focus specifically on legitimate issuers, where disclosure concerns mirror those in traditional finance, albeit with critical differences.

In traditional finance, issuers must notify asset holders of material developments, and investors are entitled to offering prospectuses or memoranda upon purchasing securities. Importantly, stocks typically confer dividends and voting rights, while bonds involve coupons and principal repayments.

In pseudonymous peer-to-peer blockchain transactions, requiring sellers (particularly liquidity pools) to provide buyers with prospectuses is impractical. Additionally, although blockchain asset ownership clearly corresponds to specific blockchain addresses, dividends or voting tokens cannot be straightforwardly distributed when ownership resides with smart contract accounts.

Therefore, representing traditional securities—such as stocks or bonds—on blockchains necessitates rethinking existing regulatory frameworks and redefining the role of transfer agents. One useful approach to mitigate these challenges is discussed in Ma-

linova and Park (2023a) and implemented by Li, Singh, Veneris, and Park (2024). This approach involves investors registering their ownership with a centralized registry (similar to a traditional transfer agent). The registry determines aggregate ownership balances at critical cutoff points (measured in blocks rather than calendar dates), including positions within liquidity pools, and distributes dividends or voting rights in a manner compatible with standard externally owned accounts (EOAs). Moreover, blockchain-based communication protocols could enable the registry to disseminate required disclosures directly to asset holders.

However, this registration system would be opt-in, shifting the responsibility onto individual investors. While issuers benefit from immediate clarity regarding their beneficial owners, the voluntary nature of this system means it is not fail-safe and could raise privacy concerns.

**Scaling Challenges.** A persistent issue for blockchain-based financial systems is limited throughput on mainnet blockchains such as Ethereum. Ethereum’s current transaction capacity (roughly 15-40 transactions per second) is insufficient for the scale required by global financial markets. A related issue is the growing blockchain state size—the amount of stored data required to process transactions correctly—which poses challenges for node operation and decentralization, as validators require increasingly substantial resources to maintain a copy of the network state.

Efforts to address scaling primarily involve so-called layer-2 (L2) solutions, particularly rollups. Rollups bundle numerous transactions in a separate system and then submit minimal verification data back to the Ethereum mainnet. Recent Ethereum protocol upgrades (such as proto-danksharding and the introduction of “data blobs” in EIP-4844) significantly improve the efficiency and reduce the costs associated with posting this verification data, allowing rollups to scale Ethereum’s throughput dramatically. Future developments, such as full danksharding (layer-1 data availability scaling), promise fur-

ther significant improvements.

Alternative layer-1 approaches also exist. Solana, for example, achieves much higher throughput (thousands of transactions per second) by reducing decentralization and requiring parallel processing. However, parallel execution poses complex technical challenges, such as avoiding transaction conflicts and managing state consistency. Another emerging architecture, exemplified by Celestia, separates consensus, execution, and data availability into distinct layers. This modular design allows specialized chains to handle execution more efficiently and independently, potentially enhancing scalability and flexibility at the cost of introducing complexity in system integration and inter-chain security dependencies.

**Concentration.** The promise of blockchains as open infrastructures is that they foster competition and promote Schumpeterian “creative destruction” by allowing entrepreneurs to challenge incumbents whose entrenched network effects otherwise stifle entry. In the best of worlds, blockchains could dramatically lower the cost of financial services and extend access to underserved or excluded populations worldwide. Yet, as in many digital industries—and especially in financial intermediation—significant economies of scale and scope risk producing concentration in a few dominant players.

We already see such tendencies in the blockbuilding business, where a small number of builders (currently Titan and Beaverbuild) construct most Ethereum blocks. Similarly, large stablecoin issuers such as Circle or payment platforms like Stripe have recently announced to be pursuing their own blockchains, potentially leveraging the network effects of money itself to entrench their positions. More broadly, the financial industry has long displayed a “walled garden” mentality: banks often resist open banking reforms with the argument that they should not “let anyone get between them and their clients”—a sentiment that, while common, is arguably anti-competitive and anti-trust in spirit. There is thus a risk that, rather than dismantling

barriers, blockchain infrastructures could be repurposed by powerful firms to replicate closed ecosystems and shield customers from competitors.

This creates an ongoing challenge: ensuring that the competitive potential of blockchain infrastructures can unfold rather than be suppressed. Regulators face a delicate balance. It is administratively easier for them to oversee a small number of large players, and such efficiency may be tempting. But regulatory convenience is not equivalent to social optimality: what is easier to supervise may reinforce concentration, while society at large benefits more from an open and contestable financial infrastructure.

**Crime.** The open and permissionless nature of blockchains inevitably attracts illicit use alongside legitimate activity. High-profile incidents include direct hacks—such as the Bybit theft—and sophisticated smart-contract exploits that drain user funds. Beyond these direct attacks on crypto holders, cryptocurrencies are playing a role as another payment rail for ransomware gangs, as documented by (Cong, Harvey, and Rabetti 2023). They are also linked to human trafficking, “pig-butcher” scams, and other forms of organized fraud, where, as (Griffin and Mei 2024) note, the tragedy lies on both sides: criminal syndicates often enslave the scammers themselves while also exploiting unsuspecting individuals in the developed world. The law is the law, and the legitimate crypto ecosystem must take crime more seriously if it seeks broader adoption and regulatory trust. Hacked or stolen funds can circulate freely on blockchains, raising the prospect that illicit proceeds may at some point be used for infrastructure-level participation—for instance, if stolen assets from a major hack were used to operate Ethereum validators. This possibility underscores the urgency of establishing minimum standards for the treatment of illicit funds in decentralized systems.

**Further Readings.** A growing literature explores the mechanisms and economic implica-

tions of decentralized finance, and as I outline above, many functions from traditional finance find their way to the decentralized finance eco-system, such as trade and yield aggregators. Harvey, Ramachandran, and Santoro (2021), John, Kogan, and Saleh (2023), Makarov and Schoar (2022) provide overviews and feature various elements of DeFi. One strand of literature focuses on decentralized trading markets, e.g., Lehar and Parlour (2023), Capponi and Jia (2021), or Park (2023). DeFi trading and lending also interact in loan liquidations and arbitrage operations; see, e.g., Lehar and Parlour (2022).

A number of papers study the performance and architecture of yield aggregators and decentralized asset managers, e.g., Coussaert, Xu, and Matsui (2022), Augustin, Shin, and Chen-zhang (2022). Several papers study decentralized lending markets. Rivera, Saleh, and Vandeweyer (2023) argue that DeFi protocols have inelastic rates at full utilization, leading to inefficient capital allocation and thus a welfare loss. Based on an equilibrium interest rate model, they propose a step-wise rising function that sharply increases near full utilization. Chaudhary, Kozhan, and Viswanath-Natraj (2023) examine interest rate determinants, suggesting a weak link between rates and future premiums on the underlying cryptocurrencies. They argue that lending markets predominantly serve to assemble speculative positions. Carre and Gabriel (2023) develop welfare-maximizing pricing rules of DeFi lending platforms operating in Proof-of-Stake blockchains. Cornelli, Gambacorta, Garratt, and Reghezza (2023) study why individuals use Aave and argue that depositors seek an investment return while borrowers speculate and seek participation in platform governance. De Simone, Peiyi, and Rabetti (2024) point to tax avoidance as an additional motive. Heimbach and Huang (2023) examine leverage in Aave and Compound, finding that users do not fully exploit their leverage potential. Lehar and Parlour (2022), Qin, Zhou, Gamito, Jovanovic, and Gervais (2021), Chiu, Ozdenoren, Yuan, and Zhang (2022) address the inherent robustness of the lending and liquidation process. While we do not feature liquidations in this paper, the

level of pool deposits influences risks related to borrowing/lending. Yield seekers’ stablecoin-to-stablecoin activities resemble wash trading, as identified by Cong, Li, Tang, and Yang (2023) on centralized crypto exchanges, albeit wash-lending arguably has no manipulative intent.

Attracting a critical mass of participants poses a major challenge, which has been studied in various industries (e.g., Rysman (2009), Evans and Schmalensee (2010), Cabral (2011)). In this context, liquidity mining has emerged as an instrument with distinctive advantages for competing platforms. Moreover, several papers study externalities in markets facilitated by digital platform firms, e.g., Kamepalli, Raghuram, and Luigi (2019), Liu, Brynjolfsson, and Dowlatabadi (2021), Reisinger, Ressler, and Schmidtke (2009).

There is also a significant literature that studies the general role of tokens in platform finance; Canidio, Danos, Marcassa, and Prat (2021) and Li and Mann (2021) provide overviews. Recent contributions that study the financing of blockchain-native projects, taking into account specific features such as platform building are Chod, Trichakis, and Yang (2022), Gan, Tsoukalas, and Netessine (2021), Catalini and Gans (2018), Shakhnov and Zaccaria (2021), Lee and Parlour (2022) (for crowdfunding), Malinova and Park (2023b), Gryglewicz, Mayer, and Morellec (2021), and Goldstein, Gupta, and Sverchkov (2024).

## 5 Risks

### 5.1 Risks for Users

I have already discussed several risks inherent in blockchain applications in prior sections. Here, I discuss those not previously covered.

*Custody risks* differ substantially between DeFi and traditional finance. Traditional finance utilizes regulated intermediaries—such as banks and brokerages—which face regulatory oversight and typically offer deposit insurance or other safeguards, reducing user exposure to asset loss. In contrast, DeFi custody inherently requires users to manage private keys directly, exposing

them to permanent asset loss due to errors, key theft, or lost access. Users bear direct responsibility for wallet security without institutional protections. However, direct user control over assets eliminates third-party custodial risks.

*Fraud risks* manifest differently between DeFi and traditional finance. Traditional financial institutions rely on regulatory oversight, consumer protection frameworks, and robust enforcement mechanisms to mitigate fraud. Institutions verify user identities and monitor transactions, significantly curbing malicious activity. Reporting requirements for issuers further reduce the likelihood of fraud, and users implicitly expect institutions to screen out scammers. In DeFi, there are no formal barriers to entry or usage, which unfortunately also removes barriers for fraudsters. Blockchain platforms and digital currencies have thus become prevalent tools in various scams, including phishing (via malicious websites), rug pulls, Ponzi-like schemes, “pig-butcher” scams, and impersonation fraud (as documented by Griffin and Mei (2024)).

*Faulty transaction risk* in traditional finance is typically mitigated through institutional mechanisms such as transaction reversals, customer support, and regulatory protections. Mistaken or unauthorized transactions can often be corrected through institutional intervention. By contrast, DeFi transactions executed on public blockchains are generally irreversible. Errors—such as incorrect wallet addresses, incorrect token amounts, or misconfigured contract interactions—result in permanent loss without recourse.

*Defective smart contract risk* is unique to DeFi. Smart contracts autonomously control asset interactions and transfers, introducing vulnerability to software bugs, security flaws, and exploitation. Unlike traditional finance, which relies on human oversight and established legal protections, smart contracts depend solely on code execution. Exploited vulnerabilities have resulted in significant losses, underscoring the critical need for thorough auditing, formal verification, and secure coding practices. Figure 4 illustrates a time series of major blockchain-related hacks, though not all relate exclusively

to DeFi or smart contracts (e.g., the largest recent attack involved the custodial exchange Bybit). Smart contract auditing has thus become a **growing business**.

*Fraudulent smart contracts* also exist. For example, tokens may misleadingly adopt the “ticker” symbol of legitimate tokens (see Lehar and Parlour (2023) for documented instances of such deceptive tokens on UniSwap). Another notable scam involved tokens with hidden restrictions, such as the infamous **Squid Game token**, which prevented users from reselling tokens at a certain point. Users primarily rely on personal due diligence, increasing vulnerability to scams. Recent developments in wallet software, particularly smart contract wallets, aim to mitigate such risks by alerting users to known fraudulent addresses or contracts. Additionally, DeFi applications like UniSwap incorporate functionality that warns users about interactions with tokens that the system does not recognize.

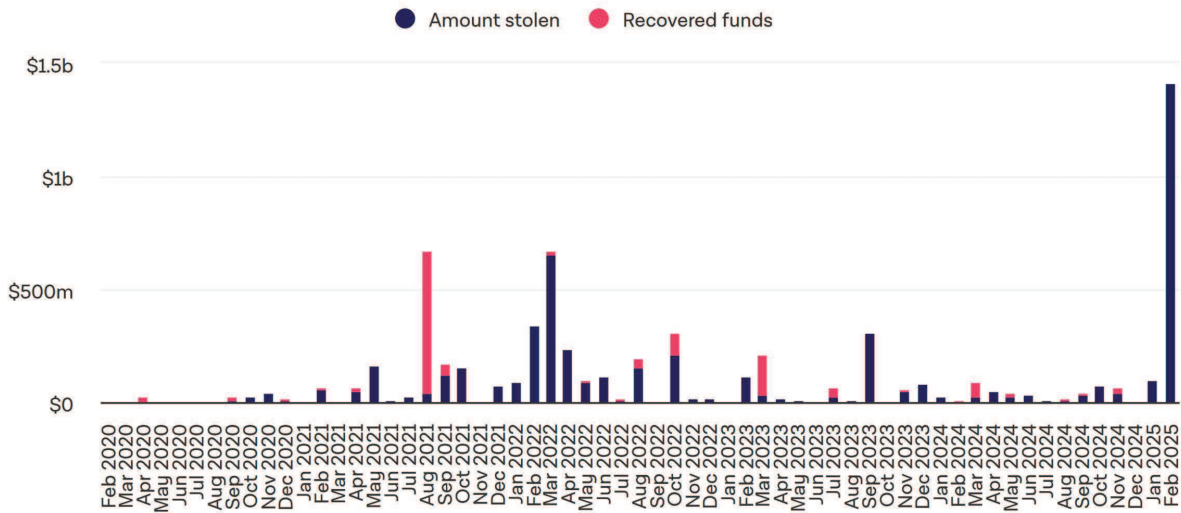
Finally, users face *protocol governance risk*. Some smart contracts, such as UniSwap v2, run autonomously and cannot be modified after initial deployment. Others can be altered via on-chain governance processes, typically through decentralized autonomous organizations (DAOs), where smart contracts automatically implement the outcomes of on-chain votes. The voting process itself introduces risks, as participants’ motivations may conflict with those of other users. More broadly, decentralized protocols depend implicitly on participants following established rules. Changes to protocol rules—even in response to clear problems—may be slow, inadequate, or ineffective. Furthermore, decentralized governance could lead to unforeseen alterations affecting the economic properties of tokens or user rights, and there is the risk of concentration of power and influence with DAOs; see Peña Calvin, Arroyo, Schwartz, and Hassan (2024).

## 5.2 Risks and Challenges for Issuers

*Hidden takeovers* present a prominent risk in tokenized stocks due to pseudonymous or anonymous ownership. Issuers may lose visibility into



## Stolen vs Returned Funds in DeFi Attacks



**SOURCE: THE BLOCK**  
**UPDATED: APR 8, 2025**

Figure 4: Funds Stolen in DeFi Hacks

beneficial ownership, complicating the identification and management of accumulating controlling stakes. In traditional finance, disclosure requirements and shareholder reporting obligations typically enable issuers to detect takeover attempts early and respond appropriately.

*Servicing shareholders* in terms of dividend management and enabling shareholder voting present distinct challenges for tokenized equities. Dividend distributions via blockchain require issuers to navigate crypto-based payment mechanisms, exposing them to blockchain congestion, volatile gas fees, and potential smart contract errors. Similarly, shareholder voting on-chain demands secure yet transparent governance mechanisms, making the administration of proxy votes more complex than centralized, regulated processes in traditional finance.

*Ownership by politically exposed persons* (PEPs) introduces compliance and reputational risks for issuers of tokenized equities. Due to pseudonymity on decentralized platforms, issuers may inadvertently allow PEPs or sanctioned individuals to acquire significant stakes,

resulting in potential regulatory enforcement risks. Traditional finance addresses this through rigorous know-your-customer (KYC) and anti-money laundering (AML) frameworks that mandate identifying ultimate beneficial owners.

Implementing token ownership registries, as envisioned by Li, Singh, Veneris, and Park (2024), could mitigate some of these concerns.

Further issuer risks in tokenized equity include jurisdictional ambiguity and regulatory uncertainty. Tokenization often involves multiple jurisdictions, each potentially lacking clear regulatory guidelines or having conflicting requirements. This situation generates legal risks regarding securities registration, investor rights, and enforcement.

### 5.3 Systemic Risks

Systemic risks differ fundamentally between blockchain-based systems and traditional finance. For blockchain networks secured through proof-of-stake (PoS), systemic risk arises from their reliance on token value for network secu-

ity. The validation process requires prospective validators to lock up capital in the network’s native cryptocurrency. Consequently, validators demand compensation for their capital costs through rewards, including fixed per-block payments (the “coinbase” reward), a share of user-paid fees, and value extracted by block builders.

A severe decline in token prices can undermine economic incentives for network security, potentially enabling attacks—such as consensus disruption or compromised transaction validity—if an adversary acquires control over more than 33% of staked tokens. Additionally, the intrinsic value of the cryptocurrency derives directly from user willingness to pay for network access. Therefore, network scaling strategies require careful consideration. John, Rivera, and Saleh (2020) highlight that scaling can enhance network security if it attracts more users, thereby increasing demand and token value. Conversely, scaling through layer-2 solutions may threaten network security by reducing mainnet demand, as emphasized by Harvey, Saleh, and Sverchkov (2025).

If a systemically important national sector, such as finance, becomes heavily dependent on a public blockchain, that network may become a target for hostile nation-states, necessitating a national security perspective on blockchain operations.

In traditional finance, analogous systemic risks emerge from centralized infrastructure dependencies—such as clearinghouses, payment systems, or custodians—whose failure or compromise could significantly disrupt financial markets.

Meme tokens and tokenized personal assets introduce risks of financial bribery or covert influence. Foreign entities or governments could manipulate prices of tokens linked to influential individuals by purchasing large quantities, indirectly transferring wealth and exerting hidden influence. Such covert price manipulations have no direct analog in traditional finance, where regulatory disclosure requirements and anti-bribery laws reduce the likelihood of undisclosed financial inducements or conflicts involving public figures.

Finally, governments reliant on capital gains taxation face potential erosion of their tax base. While concerns about individuals hiding capital gains using blockchain pseudonymity are common, another less-recognized issue is the potential use of blockchain assets to manufacture artificial capital losses, offsetting taxable gains. For instance, Cong, Landsman, Maydew, and Rabetti (2023) document investor behavior involving tax-loss harvesting via non-fungible tokens (NFTs).

## 6 Challenges for Regulation

There are too many regulatory objectives and rules to comprehensively cover in this survey, so I will broadly focus on topics relating to investor protection and market integrity.

Existing financial fraud laws already provide strong investor protections, prompting the question: what additional value does regulation offer beyond these existing laws? From an economic perspective, several arguments justify further regulation to enhance investor protection and promote market integrity.

First, regulation raises the barriers for fraud, making it more difficult for fraudulent schemes to reach unsuspecting investors. In traditional finance, one cannot simply issue and list an asset without oversight. On blockchain networks, however, anyone can easily create a “vaporware” asset and sell it via decentralized exchanges to a large audience.<sup>10</sup> Clearly, this lowers barriers for fraudulent actors.

Second, regulation establishes minimum standards of acceptable business conduct above mere fraud prevention. Higher standards improve market functioning by reducing investor uncertainty about certain investment aspects, thereby lowering collective investor costs.

Third, relatedly, regulation shifts responsibility for harm prevention to parties best positioned to mitigate risks. For example, publicly listed companies face mandatory reporting and gover-

---

<sup>10</sup>While selling “vaporware” assets was possible before blockchains, practical issues such as authenticity verification and double-spending made such frauds uncommon.

nance standards, making executives directly accountable to regulators for misconduct.

Fourth, intermediaries often efficiently solve collective-action problems, such as disseminating critical information or matching investors with suitable products. This allows effective implementation of broader public policy objectives.

These regulatory rationales remain valid even when new technologies emerge. However, three important questions arise in this context. First, which regulations are specifically necessary due to and only within the existing institutional structures? Second, which regulatory functions can (or cannot) be adapted to decentralized environments? Finally, how can public policy goals, such as investor protection and market integrity, be effectively pursued within decentralized and borderless blockchain ecosystems?

Since some regulatory considerations have been addressed earlier, I now focus explicitly on these broader issues.

**Regulating Standard Operations.** In traditional finance, extensive supervision ensures that custodial financial institutions safeguard client assets. On blockchains, cryptographic methods and consensus protocols ensure asset safety. Digital signatures, generated via wallet software, ensure that only rightful owners control their assets. Consensus protocols facilitate transactions and prevent transactions from disappearing or being altered retroactively.

Since users manage their private keys, there is no custodial third party requiring regulatory oversight. User protection might instead be implemented at the wallet software level, though achieving protection without compromising user autonomy remains challenging. Direct regulation of validators in decentralized networks is nearly impossible, as their physical locations are generally unknown, except in cases involving custodial crypto-exchanges.

In contrast, block builders—entities that assemble transaction blocks for validators—are specialized firms. On Ethereum, the market for block builders is currently concentrated, which makes regulation feasible by a regulator in the

same jurisdiction as the builder. Overbearing regulations, however, could prove counterproductive because builders can relocate to less regulated jurisdictions and circumvent oversight. For domestic builders operating within jurisdictions with robust fraud enforcement (e.g., the U.S.), users benefit from legal protections and enforcement threats. Conversely, aggressive regulation that pushes builders offshore to where there are not even fraud protections could unintentionally increase user risk.

More broadly, jurisdictional issues are going to be a challenge for enforcement as it can be difficult to determine which court has authority, how to handle court rulings across borders, and especially how to coordinate regulation across borders, especially given how fast assets can move; see also Silvers (2019).

A closely related question is whether validator regulation is justified in the first place. Network rules are transparent, and little evidence currently suggests systematic violations by network participants. In fact, blockchain protocols inherently penalize and deter systematic misconduct. Individual instances of misbehavior, such as the case of two brothers **indicted** for manipulating and exploiting MEV bots by submitting invalid transactions, have occurred. Nonetheless, isolated incidents alone may not warrant broad regulatory intervention.

Moreover, application designers actively address emerging issues like maximal extractable value (MEV). Economic mechanisms have already been developed to mitigate specific risks, such as sandwich attacks, as discussed by Park (2023).

**Applications.** Once deployed on a blockchain, smart contracts typically run autonomously, making it difficult to hold designers and developers accountable, as exemplified by the **case** involving OFAC sanctions against Tornado Cash. Because smart contracts can be deployed from any jurisdiction, mandatory pre-deployment reviews are practically unenforceable even if they may be desirable. Nevertheless, application developers have strong incentives to attract users;

consequently, misbehavior or malfunctions in one application can harm the reputation of all others. Pre-release smart contract audits have become standard practice. Likewise, Nimalendran, Pathak, Petryk, and Qiu (2024) report that many blockchain onramp services voluntarily register as money services businesses. An additional measure could involve voluntary certification and the formation of self-regulatory organizations (SROs), as also explored in Nimalendran, Pathak, Petryk, and Qiu (2024). Bourveau, Brendel, and Schoenfeld (2024) provide evidence on the usage of smart contract audits and the positive market reaction to them. These organizations would voluntarily undergo audits to enhance security standards. This approach requires clearly defined accountability frameworks and certification procedures, akin to traditional financial software audits.

**Tokenized Assets.** Direct Connections between Traditional Finance and Blockchains arise prominently when traditional assets are tokenized. Custodial stablecoins exemplify this connection, with companies issuing digital tokens representing dollar-denominated assets held off-chain. This arrangement is widely understood and has led to the recent adoption of the **GENIUS Act**. Thus, I will omit detailed coverage here. For the purposes of this paper, the essential regulatory concern is ensuring trust in the existence and value of backing assets, as required by the GENIUS Act. Currently, major stablecoin issuers already rely on periodic attestations from high-profile accounting firms (for instance, Circle Inc. uses Deloitte). Regulators will play a crucial role in establishing appropriate (audit) standards to verify asset existence and to ensure backing asset quality.

Rules developed for stablecoins will likely become blueprints for regulating tokenized assets, though important differences exist as outlined in Section 1. Specifically, regulators must carefully address the absence of traditional transfer agents that verify ownership, manage distributions, and facilitate communication, and determine implications for issuers' obligations in

blockchain-based environments. As discussed in Malinova and Park (2023a), placing responsibility on token holders to actively register with entities serving transfer-agent roles (such as the registry proposed by Li, Singh, Veneris, and Park (2024)) can help ensure investor rights. Altering these traditional arrangements, however, may significantly impact the usage of tokenized assets. For instance, tokenized securities could become widely used as incentive payments or rewards, something that has proven controversial and challenging in traditional finance, exemplified by regulatory concerns around **Robinhood's** "gamification" practices.

More broadly, tokenized assets highlight that there is a difference between investor's rights and abilities. Traditional securities explicitly provide legal rights (such as dividends and voting) enforceable through established legal channels. In contrast, tokens often confer only practical functionalities (such as governance participation or platform access) without explicit legal protections. Regulatory frameworks must therefore clearly delineate enforceable investor rights from mere technological capabilities, specifying investor-protection obligations. This topic relates to the discussion in Cohen, Strong, Lewin, and Chen (2022) who argue that crypto-assets give owners abilities, but not rights.

Financial intermediaries are usually tasked with ensuring suitability checks, meaning that users do not interact with financial products that are unsuitable for their risk profile. Blockchain platforms lack access restrictions, allowing users to interact with assets that might fail traditional suitability checks. Consequently, individuals may face exposures to risks they do not fully understand. Furthermore, blockchain technology enables the creation of arbitrarily complex derivative instruments related to tokenized assets, blurring traditional distinctions among securities, commodities, and hybrid instruments. This complexity significantly complicates regulatory classification, oversight, and enforcement of investor protection measures.

Lastly, tokenized equity poses market structure related challenges. In the early 2000s, the U.S. established the National Market System

(NMS), a regulatory framework to align and unify the trading of equities across the multiple, newly emerging electronic trading platforms of their time. The regulation around NMS is stringent and has numerous technological requirements to ensure that markets can integrate. There are too many rules to cover here, but let me highlight two. First, trades and quotes are disseminated in real time via the Securities Information Processor (SIP), a unified system. DeFi markets have natural delays when trades await inclusion in a block, and blockchains generally operate on their own time and it's not at all clear how a genuinely decentralized systems can be integrated with fundamentally centralized, and very fast markets. Second, a key requirement of Reg NMS is trade-through prohibition, meaning that a marketplace cannot process a trade at a price that is worse than the best-offered price at a protected market. Prices in automated market maker systems are determined only at the time when a trade executes within a block, and given the block building process, it would be close to impossible to prevent situations where trades of tokenized equities violate trade-through prohibitions.<sup>11</sup> With all that being said, one reason for Reg NMS is to ensure that intermediaries operate in a manner than reasonably ensures that their clients get served well and trade at “good” prices. In a market where users control their assets themselves, users can reasonably be expected to finding the best price themselves.

There are numerous other challenges not covered here, including classification issues for crypto-assets whose form or function may shift

---

<sup>11</sup>Setting aside the specific rules, one may wonder whether the forces of arbitrage are sufficient to ensure that prices reasonably align, or, put differently: is there evidence that the market itself forces its integration? The evidence from crypto markets is mixed: Makarov and Schoar (2020) report that for (custodial and centralized) bitcoin markets, there were significant deviations and arbitrage opportunities, often associated with the physical locations by country. Lehar and Parlour (2023) on the other hand report that after an initial transition period, prices between UniSwap, the largest automated market maker, and Binance, the largest custodial exchange aligned very closely; Barbon and Ranaldo (2025) make similar observations.

over time—initially resembling securities but later commodities or utilities—as well as know-your-customer rules (previously discussed) and broader tax policy implications.

**Summary and the path forward.** Many regulatory justifications persist despite the transition of assets from traditional to decentralized finance. However, the absence of intermediaries complicates applying traditional regulatory processes directly to decentralized finance. Given blockchain technology's borderless nature, imposing similar regulatory structures—for example, by directly regulating builders—could produce unintended negative consequences. Similarly, restricting asset ownership or mandating comprehensive KYC could severely hinder smart contract functionality, lead to privacy violations and excessive surveillance, and hinder beneficial capital market innovations.

Another practical challenge arises from regulators' limited resources: intermediaries traditionally provide scalability and efficiency in enforcing compliance, whereas regulators lack capacity to enforce broad compliance directly among a large, decentralized user base.

Ultimately, all regulatory interventions involve trade-offs; pursuing public policy goals incurs costs. For new technologies, these costs manifest as direct implementation expenses and potential losses from foregone future innovations. In some instances, regulatory costs may outweigh their intended benefits. Thus, exploring alternative regulatory pathways—such as voluntary certification frameworks or encouraging the establishment of self-regulatory organizations—may offer more effective means of achieving essential public policy goals, including investor and user protection, while minimizing innovation constraints.

## 7 Pathways for Traditional Financial Intermediaries to Blockchain Integration

Financial institutions can interact with blockchain technology and its users in various ways. The following list provides examples,

ordered loosely from superficial to deep forms of integration:

- Banking services to crypto firms for routine operations, such as payroll or receiving customer funds.
- Banking services for crypto on-ramp firms such as crypto exchanges.
- Crypto custody services for investors and crypto-related businesses, including ETF providers.
- Crypto trading services without direct fiat on-ramping (brokerage only).
- Tokenization and KYC services, including creating and maintaining association sets.
- Customer on-ramp services with wallet-to-bank account integration.
- Layer-2 (L2) integrations and direct on-chain capital market services.

I elaborate on these points below.

**Banking services to crypto firms and investors.** Crypto-related businesses, such as development labs or specialized law firms, have standard banking needs: payroll, rent payments, and fee collection for services. Such interactions are generally uncontroversial as long as business activities remain legal, and regulators typically avoid discriminating against specific legal industries. Similarly, individual crypto investors have ordinary banking needs. However, as TD Bank [painfully discovered in 2024](#), financial institutions must exercise caution with crypto investors who may receive illicit funds via offshore crypto exchanges. In TD Bank's case, multiple customers received substantial transfers from Colombian crypto exchanges without adequately documenting or reporting them.

Providing banking services to crypto on-ramp firms is more challenging. Here, a bank would offer a crypto trading platform an account specifically for managing customer funds. These accounts can experience significant inflows and outflows, especially during periods of market stress,

requiring banks to implement extra liquidity management precautions. Banks typically handle these accounts similarly to brokerage sweep accounts.

**Crypto Custody Services.** Historically people have sought the help of banks to keep their valuables and assets safe, and many blockchain users would likely appreciate the option of such a service. Following [S.E.C. Staff Accounting Bulletin 122](#), financial institutions can now offer crypto custody services similarly to traditional custody offerings. The business case depends primarily on a financial institution's willingness to engage with the crypto industry and adopt blockchain technology. Currently, most retail crypto investors hold their assets at exchanges and may welcome custody services provided by their banks. Particularly as asset tokenization becomes widespread, financial institutions could naturally integrate crypto custody into their existing customer offerings.

**Crypto Trading Services.** Early forays by financial institutions into crypto primarily provided customers with exposure to crypto-assets without direct asset control. For example, the Canadian fintech firm Wealthsimple initially offered Bitcoin and Ether exposure without allowing users to transfer assets into self-custody wallets. Over time, Wealthsimple expanded its platform to fully integrate crypto trading and cash account operations. Similarly, Revolut in the UK enables users to seamlessly move and exchange value between crypto wallets and traditional bank accounts.

Coinbase, originally a crypto trading platform, approached this integration in reverse. It partnered with Bridge, a subsidiary of Stripe, to now offer customers access to traditional bank accounts, facilitating easier movement between decentralized and traditional finance.

A more substantial solution would be for banks to offer comprehensive integration with customers' crypto wallets. A crucial consideration in such integration involves converting bank deposits into blockchain based as-

sets. Crypto trading platforms typically operate affiliated markets that facilitate these exchanges internally. Without such internal markets, banks would need to rely on external markets to convert blockchain assets into fiat currency, creating temporary inventory risk. Such deposit-to-crypto conversions inherently make banks slightly riskier and crypto-assets somewhat safer, raising an important question about the optimal balance between these two effects.

**Tokenization and KYC Services.** In traditional finance, the custody and ownership chain typically flows from issuer to broker-dealer to custodian, then to a clearing and settlement registry, and ultimately to a transfer agent. Asset tokenization involves taking custody of traditional assets and issuing new blockchain-based claims on them. A prominent analog in traditional finance is the issuance of American Depositary Receipts (ADRs), primarily handled by institutions such as BNY Mellon. In this arrangement, the ADR issuer acts as an intermediary between the original asset issuer and ADR holders, also managing administrative functions like voting rights and dividend distribution.

Tokenizing traditional assets onto a blockchain would follow a comparable structure. As discussed earlier, however, blockchain-based tokenization presents challenges if the tokens are intended for use in decentralized finance (DeFi) applications and self-custody solutions. For instance, Li, Singh, Veneris, and Park (2024) suggest establishing a centralized beneficial-ownership registry similar to a traditional transfer agent. Such an entity would require significant technological expertise to accurately record and track ownership.

A closely related service involves Know-Your-Customer (KYC) procedures. Financial institutions are well-positioned for this task, as they have already conducted thorough KYC checks and regularly update customer records. Consequently, traditional financial institutions are ideal candidates for creating and maintaining the “association sets” described in Section 2. However, the business model remains uncertain,

primarily because it is unclear how institutions would be compensated for providing these KYC services.

**L2 Integration and Service Offerings.** The shortest path toward blockchain adoption for traditional financial institutions involves layer 2 or rollup solutions. These can be organized in various ways; one approach involves an institution—or consortium of institutions—appointing a sequencer (the term for rollup validators) and deploying a suite of smart contracts and tokens operating exclusively on the rollup. Under this arrangement, institutions can maintain control by issuing (smart contract) wallets, restricting user access through KYC requirements, and running applications at high speed and low gas costs. For example, the Canadian fintech firm Tradewind has developed an L2 solution specifically for trading tokenized gold. This solution involves partnerships with the Royal Canadian Mint (a Canadian Crown corporation) for custody of the physical gold and the prominent brokerage Kitco for customer onboarding and KYC.

However, beyond narrow use cases, this model requires institutions either to agree collectively on the design or to follow the specifications of a lead institution. Given the typical difficulty of development-by-committee, there’s a significant risk that such L2 solutions become isolated silos rather than interoperable infrastructures.

There is also examples where the integration is initiated from the crypto side. Crypto trading platforms have started developing L2 rollups as execution environments that extend their services; prominent examples include Coinbase’s Base rollup (built on Optimism) and Kraken’s Ink. Similarly, the decentralized exchange UniSwap recently introduced its own rollup, UniChain, which also connects to traditional finance through fintech providers such as MoonSwap.

## 8 Conclusion

A defining feature of traditional finance is that investors and customers hold their financial instruments through intermediaries, with cash being the only common exception. Several practical reasons underpin this arrangement. First, safekeeping: financial assets represent significant value, and individuals typically prefer not to manage security themselves. Specialized institutions offer secure storage at scale—though poorly designed digital systems can also amplify security risks. Second, authenticity: when trading financial instruments, buyers must trust that assets are genuine. Establishing authenticity traditionally requires sophisticated physical measures like watermarks and stamps. Institutions provide authentication and validation, facilitating transfers among themselves. Finally, institutions acting as central custodians can efficiently deliver additional services, leveraging network effects. Notably, historically assets were still held decentrally at intermediaries in physical form; only since the 1960s have changes in beneficiary ownership been administered centrally at and by the DTC.

Blockchain-based finance allows new models of direct ownership and disrupts this traditional arrangement. Individuals can directly control their assets through self-custody, transferring them independently of intermediaries. Asset authenticity derives inherently from cryptographic proof embedded in the blockchain, though the link between blockchain tokens and external assets may still require trust. Self-custody fundamentally changes financial institutions' roles by eliminating their necessity. Financial institutions may remain beneficial but face altered competitive dynamics: existing network effects change, yet blockchain allows institutions to offer services beyond their traditional client base, competing or collaborating in new ways.

Self-custody and direct network access also re-define regulatory roles. Regulators find it more challenging to enforce rules broadly on individuals than on specialized intermediaries. A key regulatory challenge involves imposing rules within an open, self-custodial environment where many

users remain unaware or indifferent to compliance. Compliance performed by intermediaries behind the scenes is typically perceived as less intrusive. Additionally, blockchain's borderless nature constrains national regulators, raising unresolved questions about enforcing traditional compliance standards effectively.

Equity trading exemplifies these differences. In traditional finance, investors access public equity markets through broker-dealers who arrange trading, custody, clearing, and settlement. Broker-dealers must invest in technology, purchase data from trading platforms, and can offer customers additional services or generate income from lending client assets. Regulators rely on broker-dealers for investor information dissemination, market manipulation prevention, and tax compliance enforcement. Issuers similarly leverage broker-dealers to distribute information, dividends, and market new issues. Investors receive comprehensive services, including asset safekeeping, but face barriers to changing brokers and accessing alternative services.

In blockchain-based finance, custodial entities providing comprehensive services still exist, but this paper emphasizes decentralized, blockchain-native solutions (including rollups or other Layer 2 solutions). Custody resides directly with users, and financial platforms are open-network applications, accessible to all and governed solely by their code. Traders access blockchain-native applications typically through websites or portals, which may also offer order routing and optimization across platforms. Relationships are transactional and ad hoc.

Crucially, a single blockchain application can be accessed simultaneously by numerous websites or other applications, with no restrictions on who can develop applications or on their nature. While commonplace in software development, this openness sharply diverges from nearly a century of financial tradition. Another distinctive feature is cost recovery: in traditional finance, intermediaries such as broker-dealers, exchanges, and clearinghouses impose complex fee structures to recoup operational costs.

In decentralized finance (DeFi), platform fees are typically minimal or nonexistent, with trad-

ing data freely accessible. The primary fees involve transfers between liquidity providers and traders. Though attractive initially, decentralized markets depend critically on attracting liquidity providers, a complex challenge. Users also incur transaction fees paid to network validators, historically substantial but increasingly minimal with blockchain scaling solutions. However, DeFi users must rely on anonymous validator networks and potentially flawed applications, introducing significant risks. Issuers, meanwhile, must develop new channels to reach investors and mechanisms for identifying beneficial owners of tokenized securities.

## 9 Policy Views

### **Self-Custody as a Fundamental Right.**

The ultimate purpose of this discussion paper series is to provide insights for better policy. I view a blockchain in finance as a value management infrastructure built on two principles: openness and universal access. These imply, crucially, that individuals can directly control the value they own on a blockchain.

The U.S. Constitution protects property rights, most notably through the Fifth Amendment, which prevents government from depriving individuals of property without due process or just compensation. Property is a prerequisite for independence, and property rights imply not only the ability to hold assets but also the practical capacity to use and exchange them. In the physical world, this is straightforward: cash can be held and transferred without restriction.

By contrast, participation in today’s digital economy typically requires intermediaries. The problem is that there is no constitutional right to a bank account: access to banking services is contractual, not guaranteed. Blockchains change this by enabling individuals to own and transfer digital assets without relying on financial institutions. In this sense, self-custody and peer-to-peer exchange on open blockchains extend constitutional property rights into the digital realm. My view is that participation in the digital economy—the right to own and pay for things

in digital form—should receive the same constitutional protections as traditional property ownership.

An analogy helps: should individuals (a) be free to access the internet directly, or (b) only through vetted gateways after identity checks? In a free society, most would agree with option (a). Yet in finance, ownership and transfer of assets are possible only after authentication by intermediaries. Blockchain technology makes this gatekeeping unnecessary, offering a “certificateless” society where individuals can directly own and control digital assets. My first policy recommendation therefore is to enshrine this ability in law: citizens must have the fundamental right to use public, permissionless blockchains without undue restrictions.

**Privacy.** My second recommendation is closely tied to the question of rights: there must be a clear discussion of the rights of individuals and firms to privacy and confidentiality in financial transactions. Zero-knowledge technologies now make it technically feasible to protect personal and transactional data while still complying with regulatory requirements, and advances in this field are rapid. It is important to acknowledge that people will seek to use such technologies to safeguard their privacy. Rather than resisting this trend, regulators and policymakers should recognize the underlying demand, and design frameworks that grant individuals these liberties while embedding appropriate compliance mechanisms. In this way, privacy-preserving technologies can coexist with effective oversight, ensuring both the protection of individual rights and the integrity of financial markets.

**Regulation and Innovation.** The past decade has revealed a deep cultural clash between financial regulators and technology innovators. The promise of blockchains as open infrastructures is that they can dismantle entrenched networks and foster competition, attracting innovation and offering users greater choice. Yet this very process of creative destruc-

tion stands in tension with the regulatory priority of “financial stability.” A dynamic landscape of small, fast-moving firms that innovate without permission is nearly incompatible with today’s regulatory approach, in which new technologies are typically sanctioned only after approval by supervisors (or by financial institutions’ internal compliance departments).

One insight of this paper is that blockchain technology can render parts of the regulatory process unnecessary. For example, the structure of token smart contracts can make the total supply of assets fully transparent, eliminating the need for separate registration and record-keeping. Similarly, blockchains are not walled gardens in which service providers must be closely monitored to prevent rent extraction from captive users. Openness and programmability themselves provide safeguards that reduce the need for layers of traditional oversight.

My third recommendation is therefore that regulators systematically review their rules to identify which requirements are no longer necessary in a blockchain environment. In short, regulators should articulate a clear “do less” agenda, acknowledging where technology itself already achieves the policy objective.

**Self-Regulation and Incentives.** My fourth recommendation is to allow and, if necessary, strongly encourage the blockchain community to develop self-regulatory standards. Some of these, such as independent smart contract audits, are already becoming common practice. Others could involve incentive-based KYC frameworks, where users gain additional benefits or access to services when they verify their identity. Because self-custody reduces the role of traditional intermediaries, regulators often lack direct points of enforcement. Policymakers should therefore explore whether aligning incentives for good behavior may achieve public policy objectives more effectively than attempting to impose traditional compliance models.

**Crime and Illicit Finance.** Blockchains have enabled new forms of abuse, such as direct hacks

and smart-contract exploits, and they used as payment rails for ransomware, human trafficking, and large-scale fraud schemes. Hacked or stolen funds can circulate freely and even be staked or otherwise deployed on permissionless infrastructures, raising the troubling possibility that illicit proceeds could underpin critical system functions. It is therefore important for the blockchain community to take crime seriously and find ways to combat it. Examples are establishing minimum standards for how stolen or tainted funds are identified and treated, so that the legitimate crypto ecosystem can distance itself clearly from criminal activity.

**Systemic Resilience and National Security.** Proof-of-stake systems derive their security from token values and validator incentives; sharp price declines or concentration of stakes in hostile hands could weaken consensus and expose critical markets to attack. Once major sectors of the financial system rely on public blockchains, these networks will become attractive targets for adversarial states. Regulators and policymakers must therefore monitor validator concentration, foreign influence, and systemic interdependencies, and ensure that contingency planning and supervisory frameworks reflect the strategic importance of these infrastructures.

**Risks of Permissioned Systems.** I also urge regulators to be skeptical of permissioned blockchain systems. Economically, such “walled garden” structures risk industry concentration, allowing a handful of players to develop entrenched network and extract rents from users. While regulators may find these systems attractive because they offer a clear entity to supervise, this convenience comes at the cost of openness, competition, and user choice.

**Need for Legal Clarity.** Finally, recent years illustrate the dangers of inconsistent regulatory direction. The Biden administration took steps that many interpreted as attempts to choke off blockchain development, while the Trump administration is now actively promoting the mi-

gration of financial services onto blockchains. Such swings are destabilizing: both approaches claim grounding in law, yet entrepreneurship cannot thrive when there is always the threat from the winds of politics. Legal clarity and durable commitments are therefore paramount if innovation is to flourish.

## References

- Augustin, Patrick, Donghwa Shin, and Roy Chen-zhang, 2022, Reaching for Yield in Decentralized Financial Markets, *SSRN Electronic Journal*.
- Barbon, Andrea, and Angelo Ranaldo, 2025, On the quality of cryptocurrency markets: Centralized versus decentralized exchanges, *Management Science* Forthcoming, accepted for publication.
- Biais, Bruno, Christophe Bisire, Matthieu Bouvard, and Catherine Casamatta, 2019, The blockchain folk theorem, *Review of Financial Studies* 32, 1662–1715.
- Bourveau, T., J. Brendel, and J. Schoenfeld, 2024, Decentralized finance (defi) assurance: early evidence, *Review of Accounting Studies* 29, 2209–2253.
- Buterin, Vitalik (edited by Nathan Schneider), 2022, *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains* (Seven Stories Press: New York).
- Cabral, Luís, 2011, Dynamic price competition with network effects, *Review of Economic Studies* 78, 83111.
- Canidio, Andrea, Vincent Danos, Stefania Marcassa, and Julien Prat, 2021, Tokens and icos: A review of the economic literature, in Agustin Fernández Anta, Christos Georgiou, Maurice Herlihy, and Monica Potop-Butucaru, ed.: *Principles of Blockchain Systems* (Morgan & Claypool).
- Capponi, Agostino, and Ruizhe Jia, 2021, The Adoption of Blockchain-Based Decentralized Exchanges, *Working Paper*.
- Carre, Sylvain, and Franck Gabriel, 2023, Security and Efficiency in DeFi Lending, *SSRN Electronic Journal*.
- Catalini, Christian, and Joshua S Gans, 2018, Initial coin offerings and the value of crypto tokens, Working Paper No. 3137213 National Bureau of Economic Research and Rotman School of Management.
- Chaudhary, Amit, Roman Kozhan, and Ganesh Viswanath-Natraj, 2023, Interest Rate Parity in Decentralized Finance, *SSRN Electronic Journal*.
- Chiu, Jonathan, Emre Ozdenoren, Kathy Yuan, and Shengxing Zhang, 2022, On the Inherent Fragility of DeFi Lending, *Working Paper*.
- Chod, Jiri, Nikolaos Trichakis, and S. Alex Yang, 2022, Platform tokenization: Financing, governance, and moral hazard, *Management Science* 68, 6355–7064.
- Cohen, Lewis, Greg Strong, Freeman Lewin, and Sarah Chen, 2022, The ineluctable modality of securities law: Why fungible crypto assets are not securities, SSRN working paper SSRN.
- Cong, Lin, Xi Li, Ke Tang, and Yang Yang, 2023, Crypto Wash Trading, *Management Science* 69, 6427–6454.
- Cong, Will, Campbell R. Harvey, and Daniel Rabetti, 2023, Ransomware and cryptocurrencies, *Management Science* 70, 104–123.
- Cong, Will, Wayne Landsman, Edward Maydew, and Daniel Rabetti, 2023, Tax-loss harvesting with cryptocurrencies, *Journal of Accounting and Economics* 76.
- Cornelli, Giulio, Leonardo Gambacorta, Rodney Garratt, and Alessio Reghezza, 2023, Why defi lending? evidence from aave v2, *BIS Working Paper*.
- Cousaert, Simon, Jiahua Xu, and Toshiko Matsui, 2022, SoK: Yield Aggregators in DeFi, *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022*.

- Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels, 2020, Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability, *2020 IEEE Symposium on Security and Privacy (SP)* pp. 910–927.
- De Simone, Lisa, Kin Peiyi, and Daniel Rabbetti, 2024, Tax Avoidance with DeFi Lending, *SSRN Electronic Journal*.
- Duffie, Darrell, Odunayo Olowookere, and Andreas Veneris, 2025, A note on privacy and compliance for stablecoins, Discussion paper, Stanford University, York University, and University of Toronto Working Paper.
- Evans, David S., and Richard Schmalensee, 2010, Failure to launch: Critical mass in platform businesses, *Review of Network Economics* 9.
- Fabozzi, Frank J., and Steven V. Mann, 2005, *Securities Finance: Securities Lending and Repurchase Agreements* (Wiley) 1st edn.
- Gan, Rowena, Gerry Tsoukalas, and Serguei Netessine, 2021, To infinity and beyond: Financing platforms with uncapped crypto tokens, *Working Paper*.
- Goldstein, Itay, Deeksha Gupta, and Ruslan Sverchkov, 2024, Utility tokens as a commitment to competition, *Journal of Finance* 79, 4197–4246.
- Griffin, John M., and Kevin Mei, 2024, How do crypto flows finance slavery? the economics of pig butchering, SSRN working paper SSRN.
- Gryglewicz, S., S. Mayer, and E. Morellec, 2021, Optimal financing with tokens, *Journal of Financial Economics* 142, 1038–1067.
- Gudgeon, Lewis, Sam M. Werner, Daniel Perez, and William J. Knottenbelt, 2020, Defi protocols for loanable funds: Interest rates, liquidity and market efficiency.
- Harvey, Campbell R., Joel Hasbrouck, and Fahad Saleh, 2024, The evolution of decentralized exchange: Risks, benefits, and oversight, WIFPR working paper, Wharton Initiative on Financial Policy and Regulation White Paper.
- Harvey, Campbell R., Ashwin Ramachandran, and Joey Santoro, 2021, *DeFi and the Future of Finance* (John Wiley & Sons: Hoboken, NJ).
- Harvey, Campbell R., Fahad Saleh, and Ruslan Sverchkov, 2025, An economic model of the 11-12 interaction, SSRN working paper SSRN.
- Heimbach, Lioba, and Wenqian Huang, 2023, DeFi leverage, *SSRN Electronic Journal*.
- John, Kose, Leonid Kogan, and Fahad Saleh, 2023, Smart Contracts and Decentralized Finance, *Annual Review of Financial Economics* 15, 523–542.
- John, Kose, Thomas Rivera, and Fahad Saleh, 2020, Proof-of-work versus proof-of-stake: A comparative economic analysis, SSRN working paper SSRN.
- Kamepalli, Sai Krishna, Rajan G. Raghuram, and Zingales Luigi, 2019, Kill Zone, *NBER Working Paper*.
- Lee, Mina, and Christine Parlour, 2022, Consumers as financiers: Consumer surplus, crowdfunding, and initial coin offerings, *The Review of Financial Studies* 35, 1105–1140.
- Lehar, Alfred, and Christine A. Parlour, 2022, Systemic Fragility in Decentralized Markets, *SSRN Electronic Journal*.
- , 2023, Decentralized Exchange: The Uniswap Automated Market Maker, *Journal of Finance* 80, 321–374.
- Li, Jiasun, and William Mann, 2021, Initial coin offerings: Current research and future directions, in Rau Raghavendra, Robert Wardrop, and Luigi Zingales, ed.: *The Palgrave Handbook of Technological Finance* . pp. 369–393 (Springer).

- Li, Reina, Shrisht Singh, Andreas Veneris, and Andreas Park, 2024, On tokenizing securities in contemporary decentralized finance ecosystems, in *IEEE Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*.
- Liu, Meng, Erik Brynjolfsson, and Jason Dowlatabadi, 2021, Do digital platforms reduce moral hazard? The case of uber and taxis, *Management Science* 67, 4665–4685.
- Makarov, Igor, and Antoinette Schoar, 2020, Trading and arbitrage in cryptocurrency markets, *Journal of Financial Economics* 135, 293–319.
- , 2022, Cryptocurrencies and Decentralized Finance (DeFi), *NBER Working Paper Series*.
- Malinova, Katya, and Andreas Park, 2023a, Tokenized stocks for trading and capital raising, *Research Policy*, accepted for publication.
- , 2023b, Tokenomics: When tokens beat equity, *Management Science* 69, 6417–7150.
- , 2024, Learning from DeFi: Would automated market makers improve equity trading?, SSRN working paper SSRN.
- Nimalendran, Mahendrarajah, Parag Pathak, Mariia Petryk, and Liyang Qiu, 2024, Informational efficiency of cryptocurrency markets, *Journal of Financial and Quantitative Analysis* pp. 1–30.
- Park, Andreas, 2023, The conceptual flaws of decentralized automated market making, *Management Science* 69, 6731–6751.
- , and Jona Stinner, 2023, Phantom liquidity in decentralized lending, SSRN working paper SSRN.
- Peña Calvin, Andrea, Javier Arroyo, Andrew Schwartz, and Samer Hassan, 2024, Concentration of power and participation in online governance: the ecosystem of decentralized autonomous organizations, in *Companion Proceedings of the ACM Web Conference 2024* pp. 927–930.
- Qin, Kaihua, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais, 2021, An empirical study of DeFi liquidations: Incentives, risks, and instabilities, in *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC* 1.
- Reisinger, Markus, Ludwig Ressner, and Richard Schmidtke, 2009, Two-sided markets with pecuniary and participation externalities, *Journal of Industrial Economics* 57, 32–57.
- Rivera, Thomas J, Fahad Saleh, and Quentin Vandeweyer, 2023, Equilibrium in a DeFi Lending Market, *SSRN Electronic Journal*.
- Rysman, Marc, 2009, The economics of two-sided markets, *Journal of Economic Perspectives* 23, 125143.
- Saleh, Fahad, 2021, Blockchain without waste: Proof-of-stake, *Review of Financial Studies* 34, 1156–1190.
- Shakhnov, Kirill, and Luana Zaccaria, 2021, (R)Evolution in entrepreneurial finance? the relationship between cryptocurrency and venture capital markets, *EIEF Working Paper*.
- Silvers, Roger, 2019, Cross-border cooperation between securities regulators, *Journal of Accounting & Economics* p. 69 Forthcoming; preprint available at SSRN.
- Tinn, Katrin, 2024, A theory model of digital currency with asymmetric privacy, SSRN working paper SSRN.
- Wahrstätter, Anton, Jens Ernstberger, Aviv Yaish, Liyi Zhou, Kaihua Qin, Taro Tsuchiya, Sebastian Steinhorst, Davor Svetinović, Nicolas Christin, Mikolaj Barczentewicz, and Arthur Gervais, 2024, Blockchain censorship, in *Proceedings of the ACM Web Conference 2024 (WWW 24)* pp. 1632–1643.

# Contents

<b>1</b>	<b>Ownership of Assets</b>	<b>4</b>
1.1	Crypto vs. Traditional Assets . . . . .	4
1.2	Accounts and Custody in Traditional Finance . . . . .	4
1.3	Ownership with Blockchains . . . . .	5
1.4	Summary Comparison . . . . .	6
<b>2</b>	<b>Compliance with Know-Your-Customer and Anti-Money-Laundering Rules</b>	<b>6</b>
2.1	KYC in Traditional Finance . . . . .	6
2.2	KYC and AML with Blockchains . . . . .	7
<b>3</b>	<b>Transferring Assets and Financial Contracting</b>	<b>10</b>
3.1	Traditional Finance . . . . .	10
3.1.1	Bonds and Equities . . . . .	10
3.1.2	Options and Futures . . . . .	11
3.2	Decentralized Trading . . . . .	11
3.2.1	Acquiring and Transferring Blockchain Assets . . . . .	11
3.2.2	Non-custodial Trading Platforms . . . . .	13
3.2.3	Non-custodial Lending Platforms . . . . .	14
3.2.4	Non-custodial Options Platforms . . . . .	15
3.2.5	Non-custodial Futures Trading Platforms . . . . .	16
3.2.6	Ownership Transfers and the Role of Blockchain Settlement Process . . . . .	17
3.3	Why DeFi? The Benefits . . . . .	17
<b>4</b>	<b>Challenges for DeFi</b>	<b>19</b>
<b>5</b>	<b>Risks</b>	<b>24</b>
5.1	Risks for Users . . . . .	24
5.2	Risks and Challenges for Issuers . . . . .	25
5.3	Systemic Risks . . . . .	26
<b>6</b>	<b>Challenges for Regulation</b>	<b>27</b>
<b>7</b>	<b>Pathways for Traditional Financial Intermediaries to Blockchain Integration</b>	<b>30</b>
<b>8</b>	<b>Conclusion</b>	<b>33</b>
<b>9</b>	<b>Policy Views</b>	<b>34</b>

## About the Author



Andreas Park is a Professor of Finance at the University of Toronto, appointed to the Rotman School of Management and the Department of Management at UTM. He serves as the Academic Director at the FinHub, Rotman's Financial Innovation Lab. He has served as a lab economist for the Blockchain stream at the Creative Destruction Lab (a world-leading start-up accelerator program) and advised various entities such as regulatory agencies, FinTech start-ups, and large banks. Andreas teaches undergraduate, graduate, and executive courses on payments innovation, blockchain and cryptocurrencies, decentralized finance, and financial market trading, and his current research focuses on the economic impact of technological transformations such as blockchain technology. He co-authored a design proposal for a central bank-issued digital currency, commissioned by the Bank of Canada. He serves on the Ontario Securities Commission's Market Structure Advisory Committee and currently heads the Canadian Securities Administrators Data Fee Methodology Committee.