# Tokenized Stocks for Trading and Capital Raising

*By Katya Malinova, McMaster University and Andreas Park, University of Toronto*

## Executive Summary

The market for crypto assets has seen a tremendous boom and an equally impressive bust cycle in less than two years. Despite the goldrush and scams that emerged during this time, the underlying blockchain technology holds immense promise for the financial industry. As a new infrastructure, this technology could simplify and streamline back-office operations, enable new interactions between issuers, financial firms, and investors, and allow novel service models in digital asset issuance and management.

The term "digital asset" includes all representations of value, financial assets, and instruments, and related claims. Digital assets have a wide range of applications, including payments, investments, and the transmission or exchange of funds. Regardless of their label, digital assets are primarily financial instruments akin to securities, commodities, and derivatives, and they can embed links to non-digital assets. Our goal is to provide a focused view on the tokenization of existing assets using blockchain technology and the issuance of digitally native assets that mimic existing assets. Covering the entire universe of digital assets and their applications, in particular, as far as the emerging area of government-issued digital assets is concerned, is beyond the scope of any individual report. Moreover, the underlying technology, its applications, the surrounding service sector, and the public sector's response evolve rapidly and in real-time. Thus, a report can be no more than a snapshot in time.

We examine asset tokenization using public permissionless blockchains such as Ethereum, Algorand, or Avalanche. Although assets can be tokenized on private networks, the database tools to build such systems have existed for two decades, yet there has been no promising private sector initiative. Instead, the excitement, promise, and innovation stem from the developments in the public, permissionless blockchain space.

We begin by reviewing the core principles and components of public blockchains in Section 1, using Ethereum as the primary example. Ethereum is the most widely used blockchain to date, and examining its features is instructive for most other public blockchain networks. We focus on the details that are important for asset tokenization, such as ownership attribution and efficient and private transaction processing. A few crucial insights emerge from our review. A blockchain is a communally built, operated, and governed infrastructure that anyone can use. As a protocol, it allows multiple parties to agree on a set of assumptions so that the network can run decentralized applications for value transfers. Digital assets are pieces of code that are registered and deployed on the network. These so-called smart contracts define tokens and can provide them with functionality that goes far beyond simple asset ownership. An important insight for the

financial industry is that ownership attribution on a blockchain is traceable yet complex. Tokens are always owned by a blockchain address. However, an address need not signify an individual or a business entity but can also belong to a smart contract (a piece of code, e.g., a blockchain application). For investors to take advantage of the novel opportunities that the blockchain infrastructure offers, they must be able to transfer tokens between user accounts and between applications.

If the legal framework for digital assets restricts transfers to users that have gone through a KYC (Know Your Customer) process, asset holders may not be able to use blockchain applications, and the assets would lose value.

In Section 2, we discuss the functions and potential usage of tokens, and we provide a characterization of crypto tokens already in circulation. This review allows us to highlight conceptual similarities and differences between traditional and digital assets. One insight is that blockchain tokens can decouple the functions of traditional assets. For instance, an equity share typically offers its owner dividend and voting rights. Digital assets can unbundle these two functions. Further, the transparency and traceability of the blockchain environment can support alternative funding models for firms. For instance, tokens can serve as claims on revenues or cash flows from specific projects.

In Section 3, we discuss the mechanisms for token issuance, using tokenizing equities as an example. In addition to blockchain-native digital assets, we examine the usage of existing assets as tokens on a blockchain. Conceptually, tokenizing existing assets is similar to the process for American Depository Receipts (ADRs). Using the ADR approach as a blueprint for blockchain-based token issuance, we discuss the potential issues that may arise. We conclude our analysis by suggesting several best practices and requirements for token issuance, including a token registry, standards for backed or asset-linked tokens, and a failsafe reconciliation process if the blockchain fails.

Next, in Section 4, we discuss the challenges and advantages of digital assets for implementing traditional asset functions such as dividend payments, shareholder voting, and shareholder communications. One critical issue is ownership attribution. On a blockchain, ownership is based on pseudo-anonymous addresses, and there is currently no registry that links addresses to individuals. Furthermore, users may need to transfer assets to an address of a blockchain application when using it, posing further challenges for ownership attribution. We describe several blockchain solutions, such as roll-ups and wallet messaging tools, that can enable standard asset functions more conveniently and efficiently than in the traditional world of finance.

Sections 5 through 8 of our report cover the usage of tokenized assets and the potential effects of smart contract services on existing financial service providers. In Section 5, we discuss the types of crypto trading platforms and the projected evolution of these platforms as traditional assets transform into digital assets. Section 6 provides an overview of the usage of tokenized assets in other blockchain applications such as borrowing and

lending protocols. In Section 7, we discuss capital raising, in particular, public offerings, in a blockchain environment. We describe several services that have emerged in the blockchain space and identify the advantages and challenges for these services and their users.

Finally, in Section 8, we speculate on how the emergence of digitally native and tokenized assets would impact traditional financial firms. A critical feature of blockchain infrastructure is that investors may hold custody of their assets. This means that they have the ability to store and manage their own digital assets directly on the blockchain, without the need for a traditional financial institution to hold them on their behalf. This can change the traditional relationship between investors and financial institutions and also change the way of protecting and managing assets. It also affects the service options for individuals, the relations between financial service providers and investors, the competitive landscape of the financial industry, and the reach and applicability of regulations.

In summary, asset tokenization will have significant implications for issuers, investors, financial institutions, regulators, and other government authorities. The blockchain world is evolving rapidly, many innovations are yet to come, and we are only beginning to understand the opportunities of blockchain infrastructure for financial markets. Our report identifies novel ideas and developments and highlights several areas that require further study. Many of the applications and tools that we identify as crucial for asset tokenization do not yet exist, and many legal and regulatory challenges remain. We hope our report can serve as a starting point that spurs future work and helps shape the discussion.

# Section 1: Review of Blockchain Technology

## 1.1 Overview

The purpose of this section is to provide a high-level overview of blockchain technology. We will highlight the features and limitations of technology to frame the opportunities and challenges of asset tokenization. We will closely review the features of the technology that affect the usage of tokenized assets.

Our paper examines asset tokenization using public permissionless blockchains such as Ethereum, Algorand, or Avalanche. Assets can also be tokenized on private networks. In our opinion, however, most such networks are merely variations of long-standing private sector arrangements. They have no direct relation to crypto-assets and the developments in the blockchain space.

Permissioned networks may become more prominent if developed by the central banks for their digital money (central bank-issued digital currencies or CBDCs). If the CBDC platforms are designed as general-purpose infrastructures, they will likely mimic the functions of public blockchains, albeit in a permissioned environment. We believe that the insights we offer in the context of an open, permissionless approach would carry over to such permissioned environments.

Our goal is to provide a tech-neutral perspective beyond some general stylized features of the technology and the philosophy behind these networks. That said, our review is biased toward the Ethereum network because we identify functionality, limitations, and challenges representative of permissionless networks in reviewing its setup and features. Furthermore, the Ethereum network to date hosts the bulk of decentralized finance applications and attracts most innovators. The workings of these applications provide valuable insights into the opportunities that blockchain brings.

## 1.2 Key Components of a Blockchain

As a first step, we will review the basics of blockchain technology to "level the playing field" for the reader. An expert in blockchain technology may skip this section.

Value transfers without the involvement of a trusted third party have eluded computer scientists and engineers for decades. That changed with the publication of Satoshi Nakamoto's White Paper in 2008. It is the first concept of a decentralized peer-to-peer value transfer system. Nakamoto's key innovation is to combine a technology invented in 1991 known as blockchain with a mechanism introduced in 2002, known as proof of work. Moreover, transactions in this system employ "standard" private-public key cryptography.

The first working implementation of this innovation is the bitcoin network which allows the decentralized value transfer of a single asset, bitcoin. Fundamentally, a value transfer in the bitcoin network involves the network agreeing to run a specific set of operations. The Ethereum network generalizes the idea and allows the network to run arbitrary sets of commands. This development enables decentralized applications, with possible applications in finance and beyond.

There are three key technologies:

1. Public-private key cryptography to secure individual transactions
2. Hash-linked data structures, which ensure that the data is consistent so that data in past blocks cannot be tampered with
3. The consensus protocol for new blocks created from a group of competing validators.

**Cryptography** is a branch of computer science based on well-understood mathematical tools from number theory. Blockchain networks process transactions that have been cryptographically signed based on public-private key cryptography. As an intuitive analogy, a private key is like an email address; the private key is like a password. Users sign transactions using their private key. They then send the transaction, the signature, and the public key to the network for processing. The network uses the public key and the message to verify that the transaction has been signed with the private key associated with the public keys. This verification operation is simple and fast, and it does not require knowledge of the private key, nor is it possible to derive the private key from the signature. Therefore, these tools are secure, and signed transactions cannot be tampered with.

**Hash-linked databases** are common in distributed systems, for instance, for time-stamp servers, to ensure the integrity of the data. These databases work as follows: Multiple operations are bundled together in blocks. Each block links to the previous block by including a cryptographic hash or unique digest of that block. The blocks are then added together in chronological order to the blockchain network's row, or chain, of data blocks. This sequencing is the origin of the term "blockchain." Since each block contains a link to the previous block, the n-th block is directly linked to the n-1st block, and since that block is linked to the n-2nd block, the n-th block is also linked to the n-2nd and so on all the way to provenance.

A cryptographic hash is a mathematically produced output of fixed length based on an arbitrary length input that is unique (for all practical purposes) for a given input. Any change to the input text changes the hash fundamentally and unpredictably. Therefore, if someone were to tamper with block n, the digest of that block would change. Consequently, the digest of the n+1st block would have to change, too; the network would discover this inconsistency and reject the change to the past block. A hash-linked database is therefore secure from tampering.

**Consensus.** The consensus protocol describes the process by which new blocks are added to the chain. Hash-linked databases are traditionally used in a permissioned network where nodes are trusted,[1] so the consensus is comparatively simple. The premise of public blockchains is that they are trustless, i.e., anyone can contribute to the running of the network. Therefore, the critical component of network operation is finding a mechanism that achieves consensus on new operations.

**Preventing Double-Spending.** A hash-linked data structure with public-private key cryptography ensures that transactions cannot be forged and that the data cannot be changed after the fact. However, it does not solve the critical issue of trustless value transfers, the "double-spending" problem. A double-spending "attack" occurs when the network is convinced to ignore a past transaction so that the attacker can spend the same amount twice. How is this possible? The attacker cannot alter a block committed to the chain but can convince the network to forget an entire block (or sequence of blocks). For this, the attacker must create a series of blocks that the network accepts as a valid blockchain, which excludes the block with the transaction the attacker wants to double-spend. Metaphorically, the attacker would create a "new reality" that replaces the actual reality of blocks to circumvent the hash-link protocol. This process becomes more challenging as the chain after the double-spending block becomes longer.

Blockchain consensus protocols have two key features that mitigate the double-spending issue. The first is the remuneration for block creators, which provides economic incentives to ensure that all created blocks are valid. The block creator receives payments that are only valuable if future validators build on their block. The second component is the randomness of block creation. To build the new reality that allows for double-spending, the attacker must be able to create new blocks on the blockchain predictably. Therefore, all blockchain protocols have mechanisms in place that prevent predictability in block creation by randomly selecting block producers among a large group of validators.

Bitcoin and Ethereum (until September 14, 2022) achieve randomness through the proof-of-work protocol. Proof of work requires block producers to find a rare cryptographic hash, which can only be discovered by random guessing. Metaphorically, the proof-of-work protocol can be thought of as rolling a complex dice with many sides. If the right side comes up, the creator gets to produce a new block. Proof-of-work "mining" is essentially akin to miners rolling the dice as often as possible to increase the chance of the right side coming up. The "rolling of the dice" requires that miners expend computing power. An attacker can tilt the playing field and create more blocks by buying more

[1] "Notably, trust encompasses not only knowing the party that operates a node, but also trusting that the node runs correctly. A trustless network, therefore, in principle ensures that a faulty node cannot threaten the integrity of the database.

computing power, but this comes at a (very high) cost.[2] This latter feature adds further economic disincentives.

here are other consensus mechanisms as well. The Avalanche protocol uses a repeated voting mechanism developed by Emin Sirer. Algorand, developed by Silvio Micali, uses Verifiable Random Functions. Economic incentives for these protocols arise from a so-called proof-of-stake mechanism, where validators must commit cryptocurrency or a stake to make themselves available to be randomly selected as block proposers. The key idea is that validators commit large enough stakes because the probability of being chosen is proportional to the stake, and they do not cheat because they would lose their stake. The mechanism also gives rise to staking-as-a-service, where a validator can improve their chances of being selected by collecting stakes from third parties."

**Proof-of-Work vs. Proof-of-Stake.** The Ethereum network began as a proof-of-work blockchain, but it transitioned to proof-of-stake in September 2022. On the other hand, the Bitcoin blockchain continues to use the proof-of-work mechanism and is unlikely to change its approach. The issuance of tokens and the running of applications on the Bitcoin blockchain is technologically challenging, so it hosts very few tokens. Most blockchain tokens and applications to date have been created on Ethereum (see, for instance, DappRadar). Therefore, for the discussion of tokenization, the Bitcoin blockchain is not relevant.

Both under Proof-of-Work and Proof-of-Stake, block validators have two sources of income. The first is fees paid by the users to validators. For bitcoin, this amount is about 10 BTC per day or 0.1 BTC per block.[3] Notably, in bitcoin fees are entirely voluntary, and in the first years of the network's existence, fees were rarely ever paid. In networks like Ethereum, the fees are essential, as we explain in the next section.

The second is a "coinbase" reward: upon creation of a new block, the validator gets to assign itself newly minted cryptocurrency. There are some subtle differences regarding coinbase rewards depending on the network. For instance, the bitcoin coinbase reward declines over time so that the total number of bitcoins is limited. In Ethereum, the cumulative coinbase reward is infinite. At the time of writing, the "coinbase" reward for a bitcoin block is 6.25 BTC (about $110K at $17.5K per BTC).

[2] This cost is in the billions of dollars. One can estimate the magnitude of the cost by dividing the current hash rate of the network by the has rate that a single graphics card produces and multiplying it with the cost of such a graphics card.

[3] https://www.blockchain.com/explorer/charts/transaction-fees

The coinbase reward system leads to dilution and a shift in network value from token holders to validators. Essentially, the creation of new blocks is financed by all owners of the cryptocurrency. Again, there are some subtle differences between proof-of-work and proof-of-stake consensus mechanisms. Under proof-of-work, validators do not need to hold any cryptocurrency, resulting in value shifting from owners to non-owners. In contrast, under proof-of-stake, rewards to stakers simply transfer network value from non-stakers to stakers. If all network participants were to stake all the time, staking would not generate any income and over the long term, coinbase rewards would be similar to stock splits.[4] However, as not all participants stake and validators also receive fees from users, staking does in fact create revenue in practice.[5]

### 1.3 The Role of a Cryptocurrency

There is a widespread view that cryptocurrencies are merely digital stickers created out of thin air with no fundamental value. Although there is some truth to this in regards to Bitcoin, the same cannot be said about the native token in second-generation blockchains such as Ethereum, where the cryptocurrency is a critical component for the operation of the blockchain network and serves a particular purpose.

Specifically, second-generation blockchains are software protocols that allow multiple parties to operate under shared assumptions and data without any institutional reason to trust each other. These data can be anything from the destination information for items in a supply chain to account balances for a particular token. Therefore, a blockchain is best thought of as a distributed network of computers that provides the guaranteed execution of code. The processing of code requires computational cycles, and a cryptocurrency is the blockchain-native means to pay validators for the provision of the code execution service. To the extent that users value this service, a cryptocurrency has value.

Furthermore, for proof-of-stake systems, validators need to lock up holdings to participate in validation, and cryptocurrency that is available to network users as liquidity cannot be used in staking. Supply of the cryptocurrency is therefore driven by the opportunity cost

---

[4] Mathematically, stakers receive coinbase tokens in proportion to their stake, and if all owners stake, the ownership shares of the network follow a Martingale process; see Rosu and Saleh (2020). Over time, this process converges to a distribution that mimics the initial distribution. For instance, imagine there are two stakers who own 60 and 40 tokens respectively. Suppose over a year, the network issues 100 new tokens. The holder of the 60 tokens will receive 60% of the new tokens (in expectation), the holder of the 40 tokens will receive about 40%. By the end of the year, in expectation, the owners will hold 120 and 80 tokens, which signify the same 60%/40% ownership splits as at the beginning of the year.

[5] Income taxes on staking may, however, cause a long-term deterioration of value: to pay taxes, stakers would have to sell coins to new investors who, at the margin, have lower valuations of the network than current holders

of lost staking rewards. Demand for usage, therefore, drives demand for the cryptocurrency.

Cryptocurrency coinbase rewards and fees are therefore central to the operation of blockchain networks. One interesting change that occurred on Ethereum in 2021 is the so-called EIP-1559 upgrade (as part of the "London" fork). After this upgrade, users had to pay a baseline fee for each operation, but the baseline fee was "burned", i.e., the associated coins were taken out of circulation. Although validators continue to receive coinbase rewards, when the burned fees exceed the reward, the cryptocurrency ETH can be deflationary.

### 1.4 The Philosophy of Decentralization and Scaling Challenges

There is much confusion in the business world about the blockchain community. Ethereum is not a company that set out to build an enterprise-level product that they want to sell to the financial sector. The Ethereum founders, in fact, explicitly opted against the corporate path and rejected a multi-million dollar offer from a large tech firm in the early development stage. Instead, Ethereum and almost all other blockchain networks rely on community contributions and are built with open-source code. There is effectively no IP in the blockchain world, no patents, and no walled gardens.

Instead, the core philosophy of decentralization is that anyone with a laptop should be able to participate in the network. This philosophy creates scaling challenges. Ethereum blocks have a limit on the number of computational cycles that they can process. An average laptop takes 10-15 seconds to process these cycles, effectively constraining the Ethereum network to about 30 transactions per second. The transition to proof-of-stake in Ethereum will increase the possible throughput substantially -- proof-of-stake networks such as Algorand and Avalanche can process 4,000-8,000 "mainnet" transactions per second. However, even these higher numbers cannot support a global digital economy of thousands of decentralized applications.

Moreover, there is a second, possibly more significant problem. The processing of transactions becomes more challenging over time because of the size of the "state," i.e., the amount of information that a network validator needs at the ready to process transactions. The state grows with the number of past transactions. Although it may be possible to alleviate the problems by relying on more advanced and powerful computing tools, such an approach would arguably lead to a high concentration of computing power and network operation. The Solana network follows yet another direction: it allows increased throughput by delegating data to cold storage. However,

the Solana network has been down several times for hours,[6] which is unacceptable for a worldwide financial network.

Development and research on Ethereum-scaling are ongoing, and a few instructive solutions have emerged. Since Ethereum has no government or formal leader, changes are always tentative and never formal promises, and there are no regulatory filings. Instead, upgrades are a community effort and are commonly discussed on social media and at conferences. The website https://ethereum.org/en/upgrades/ regularly publishes the outcomes of the discussions. The most prolific Ethereum co-founder, Vitalik Buterin, recently revealed his vision for the Ethereum roadmap on Twitter. In what follows, we discuss the scaling solution that, in our opinion, is immediately relevant for asset tokenization.

### 1.5 Scaling through Roll-ups

A rollup is a process that efficiently bundles or rolls up many transactions into one. There are several different approaches to this process, and they are best explained by example. Consider a traditional limit order book. In principle, it is possible to maintain a limit order book directly on the blockchain because a limit order is merely a set of instructions that can be encoded as a set of commands to be kept and processed by a blockchain network. However, running such an exchange would be expensive because the limit order submitter would need to pay a fee for each limit order submission, including all order modifications, even if the order does not execute. Moreover, all 10,000+ blockchain nodes would need to process each limit order submission, and they would need to store the information, which is computationally inefficient.

The decentralized exchange dYdX, for instance, resolves this using rollup technology. It collects cryptographically signed but unexecuted limit orders off-chain, builds a limit order book off-chain, and only commits the executed orders and transactions to the mainnet. This approach resembles end-of-day netting via CCPs or CSDs. In addition to saving on fees for orders, a rollup is also very efficient when posting (bundling) transactions. Theoretically, according to Buterin (2021), a rolled-up transaction should use less than 1% of the gas (the measure for computational cycles on blockchains) of a normal transaction.

Notably, a rollup can do much more than transaction processing. It can host entire payment systems or complicated derivatives contracts, and it would accommodate asset tokenization. A rollup can offer privacy-protecting transactions, and it would allow a financial institution to establish a new token and disseminate it to known entities.

---

[6] The websites status.solana.com and https://statusgator.com/services/solana track network up-/downtime. For instance, in 2022, Solana had major outages in January and April.

Rollup technology leverages the mainnet's security through either validity or fault-proof processes; therefore, there is no need to trust the rollup operator.

A rollup can also solve another critical complication of blockchain usage: any transaction on the blockchain requires a payment in the native cryptocurrency. This arrangement implies that users must acquire the cryptocurrency before using a blockchain. For instance, a user who wants to make a remittance payment on the Ethereum blockchain using a digital representation of the USD, such as USDT, has to acquire USDT tokens and ETH to make the transfer. A rollup operator can, in principle, perform this operation and charge the user in USDT (or in a different currency).

### 1.6 Wallets, Addresses and Public-Private Keys

Public blockchains such as Ethereum have two types of accounts: externally owned accounts (EOAs) and smart contract accounts (SCAs).

Crypto-asset ownership is associated with EAOs; these are public addresses, similar to account numbers. The public address is derived from the public key, and the latter is generated from a private key as part of public-private key cryptography. The private key controls the crypto-assets and is used to sign transactions.

A crypto **wallet** is a software tool that stores private keys and enables the signing of transactions. There are many forms of wallets, the most common being browser plugins or smartphone apps. In these so-called "hot" wallets, the private key is stored on a desktop computer or a smartphone. There are also hardware wallets that store the private keys in a separate device which, in some cases, never "touch" an online device.

The terms "wallet" and "public address" are often used interchangeably, even though that is technically incorrect because a single wallet can handle many addresses. When the user controls the private keys, a wallet is referred to as self-custody; when a third party controls the private key, a wallet is referred to as custodial.

The standard wallet setup requires that a single entity sign a transaction. It is also possible to set up multiple-signature ("multi-sig") wallets, in which case multiple parties must sign a transaction cryptographically to initiate a transfer. Such an arrangement provides greater security against password theft or malicious use of, for instance, third-party assets that a financial institution holds in custody. There is a set of applications for asset tokenization where multi-sig wallets can play an important role in compliance. We will discuss this more in Section 2.

Most users purchase their first crypto assets on a centralized exchange. To trade on a centralized venue, users must first register with the platform, which now almost always involves a KYC process that requires a photo, government-issued ID and proof of residency. Centralized exchanges then commonly issue their users a unique public address, but the custody of the private keys for this address rests with the exchange. These

public addresses are, therefore, also referred to as custodial wallets because the exchange has custody of the private keys. When a user purchases crypto-assets on a centralized exchange, however, these assets are typically not transferred into the user's custodial wallet but are kept in the exchange's omnibus wallet. Out-transfers from exchanges, therefore, usually occur from an omnibus wallet. In-transfers are sent to the custodial wallet address and are then transferred to the exchange's omnibus wallet in the second implicit step. After that, all transactions are arranged and recorded on the centralized exchange's proprietary infrastructure and not on the blockchain. For this reason, assets in omnibus wallets are often referred to as "off-chain."

Note that the usage of a centralized exchange differs from a rollup because transactions within a rollup require the user to sign a transaction cryptographically, the user can withdraw funds when they want, and they can challenge the activities of a rollup validator on-chain. When using a centralized exchange, users hand the control over to the exchange.

From a compliance perspective, custodial wallets are associated with a real person that went through a KYC process, whereas self-custody wallets are entirely user-controlled and established without any KYC process. The European Parliament recently passed legislation that requires crypto exchanges to know the owner of non-custodial wallets when they transfer funds out, allowing the KYC process to stretch one step beyond custodial wallets. Of course, users can transfer funds further, negating the expansion of KYC, and the policy-makers considered a restriction that would prevent centralized exchanges from sending crypto-assets to *any* non-custodial wallet.

Although this proposal was made with the best intentions, it would have had significant downstream consequences if adopted. By not allowing transfers to non-custodial wallets, policy-makers would have effectively diminished these assets' functionality, made using DeFi applications all but impossible, and prevented users from being able to protect their privacy.

Smart contract accounts, or SCAs, differ from externally owned accounts (EOAs) in that they are not controlled by private keys, but by their intrinsic code. SCAs are, in a broad sense, pieces of code that EOAs can interact with and that run on the Ethereum blockchain. Examples of SCAs include decentralized applications and digital tokens.

### 1.7 Ownership Attribution

Every crypto asset is associated with a blockchain address by design. However, an address is not synonymous with an account that belongs to a person or firm – it can also be a smart contract such as a liquidity pool or a blockchain bridge.

Knowledge of the owner address of a crypto asset is thus often insufficient to attribute beneficiary ownership to an end-owner. Likewise, assigning accrued earnings (e.g., in the form of accrued interest) based on addresses alone may be problematic. Pseudo-

anonymous and unattributable ownership is a challenge for know-your-customer compliance rules, and it is a challenge for token issuers who keep track of the beneficiary owners of their tokens.

Firms that want to comply with KYC rules may be tempted to develop workarounds, but these may not be effective and may limit digital assets' usability. For instance, one might consider creating a so-called whitelist that contains addresses that went through a KYC process. Such a list could be stored in a distributed file system such as IPFS (InterPlanetary File System), and the token design can restrict transfers to be among whitelisted/registered addresses.[7] However, the problem is that this list would also have to contain smart contract addresses, and this process may limit the ability of users to take advantage of DeFi applications. It may also hamper market efficiency because arbitrage bots may not be able to operate as desired when whitelist checks are always necessary.

### 1.8 Personal Privacy and Business Secrecy

Blockchain addresses are pseudo-anonymous: by default, transactions are perfectly traceable, but the identity behind an address is unknown. Financial institutions that offer blockchain services would know their customers. They would also be able to follow what the customer is doing with the crypto-assets, at least to the extent that they can trace the activities of known addresses.

The downside is that all of the person's or business' activities on the blockchain are publicly visible. Many of these activities may be of a non-financial nature and may reveal information about their behavior, preferences, and relationships that they prefer to keep private and secret. Being linked to an identity means that these activities are no longer private/secret to their bank. Furthermore, when a user's addresses and identity are linked and known to a government agency, this user may face state surveillance of their blockchain-related activities.

Likewise, a firm that uses the blockchain for business activities would give up at least some part of the secrecy of its operations, at the very least to direct counterparties of blockchain transactions. The potential misuse of individual private information and business proprietary knowledge is a concern.

Against this backdrop, ideally, blockchains users should be able to authenticate themselves as legitimate people/firms without revealing either their identity or their blockchain address. The Indian government has created a digital ID solution (the Adhaar system) within its jurisdiction for such a purpose. There are also several blockchain

[7] Circle has a somewhat related approach which is to maintain a list of addresses to which USDC cannot be transferred.

community-based attempts to establish a form of digital ID. Users' desire to protect their privacy will likely give rise to a business service sector in the future.

Arguably, investors in tokenized assets will have a strong interest in preserving their privacy, for instance, to protect their investment strategies. Therefore, privacy-preserving technology is of first-order importance for a successful tokenization strategy.

### 1.9 Cross-Chain Bridges

Blockchain networks can be linked using cross-chain bridging services such as Shuttleflow or Wormhole. These services lock tokens on one platform in an escrow account and then release a new token on a different platform. This process is also known as "wrapping." For instance, it is possible to trade wrapped bitcoin on the Ethereum network. The insight for tokenization is that tokens deployed on one platform can potentially be used on a different platform. Using these services, however, exposes investors to additional risks, for instance, due to cyberattacks.[8]

### 1.10 General Legal Issues Around the Usage of Public Blockchains

Tokenization and value transfers on a permissionless blockchain may require regulatory changes to ensure that a particular blockchain may legally serve as the recording technology. Blockchains are conceptually borderless, not domiciled in any specific country, and not controlled by a single entity. Instead, they are a communally built, operated, and governed infrastructure that anyone can use. It is unlikely that a specific country or region in isolation can impose nor enforce their regulations on blockchain usage in a worldwide community. Blockchain technology offers many opportunities, but the borderless, communally governed infrastructure and many of its applications do not fit existing regulatory frameworks. Ideally, lawmakers and regulators would recognize the potential of the new infrastructure and design regulations that would allow the community to take advantage of the technology's novel features and global reach.

Of course, laws in any specific country would also need to cover contingency and fallback plans should the recording technology come under the control of a foreign government or cease to exist for economic or political reasons.

[8] See, for instance, https://blog.chainalysis.com/reports/wormhole-hack-february-2022/ for a description of a hacker attack on Jump Trading's Wormhole service.

## Section 2: Forms of Tokenizations

### 2.1 Overview

This section covers the type of assets that a blockchain can host. We begin by reviewing tokens already circulating on blockchains; most of these are self-referential in the sense that these assets are related to a blockchain-specific platform or applications. As a value transfer infrastructure, however, a blockchain can serve as a platform for any assets, including stocks, bonds, or property. In the second part of this section, we discuss processes and best practices for issuing tokens that are linked to the non-blockchain world.

### 2.2 Crypto-Assets and Tokens.

There are two types of crypto-assets: first, the native means of payment for a blockchain, the cryptocurrency, and second, tokens built on top of the chain. For this paper, we are interested in the latter.

A token is a type of smart contract, a piece of code and data that reside at a specific address (or account number) on the Ethereum blockchain. A token can represent almost anything: reputation points in an online platform, a character's skills in a computer game, financial assets such as a share in a company, or real-world physical assets such as oil or gold.

The community has agreed to specific standards for token contracts. Standards for the Ethereum protocol community developed, based on the Ethereum Improvement Proposal process. The most common one is the ERC-20 standard for fungible tokens (ERC=Ethereum Request for Comment), ERC-721 for non-fungible tokens, and ERC-1155 for "mixed tokens."[9] These contract features allow users to transfer tokens from one account to another, establish the current token balance of an account, obtain the total supply of the token available on the network, and approve spending by a third-party account. Non-fungible tokens allow links to metadata that specify, for instance, a digital piece of art or the VIN of a car.

As smart contracts, a token's functions are not controlled by a user but are deployed to the network and run as programmed. Users interact with a token smart contract by submitting transactions that execute a function defined in the token code. Tokens may contain functions beyond those of the ERC standard.

---

[9] There are several other accepted and still-debated standards, such as ERC-4519 for Non-Fungible tokens tied to physical assets, or ERC-3525 for semi-fungible tokens. Token invention and standardization remains an active research and development field.

A blockchain can serve as a value-transfer platform for assets, including traditional ones such as bonds, stocks, gold, carbon, and title to the property in digital form.

However, blockchains work seamlessly only when they are self-referential in that they host assets that operate on their own platforms in applications. In this self-referential world, the network performs all functions, and control is decentral and trustless. Using blockchain technology for real-world assets requires a connection beyond the data natively available on the network, which in turn requires trust.

Examples of successful implementations of an outside link are fiat-back stablecoins such as USDT (issued by Tether Inc.) or USDC (issued by Circle Inc.); both firms are regulated by U.S. state banking regulators. However, there are ongoing rumblings as to whether these stablecoins are fully backed.[10] Another example is NFTs which link to non-blockchain items of value. Conceptually, NFTs and fiat-backed stablecoins are tokenized assets.

### 2.3 A Taxonomy of Blockchain Tokens

The landscape of blockchain tokens is continuously evolving. As pieces of computer code, tokens can include any custom features and be deployed in an infinite number of applications. It is therefore impossible to put forth a precise classification. Instead, this paper presents an overview of the main functions we have seen in tokens over the last few years.

From a legal viewpoint, two broad representations have emerged in two leading jurisdictions.

In the U.S., President Biden's executive order defines digital assets as follows: "The term "digital assets" refers to all CBDCs, regardless of the technology used, and to other representations of value, financial assets and instruments, or claims that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof, that are issued or represented in digital form through the use of distributed ledger technology. For example, digital assets include cryptocurrencies, stablecoins, and CBDCs. Regardless of the label used, a digital asset may be, among other things, a security, a commodity, a derivative, or other financial product. Digital assets may be exchanged across digital asset trading platforms, including centralized and decentralized finance platforms, or through peer-to-peer technologies."

In the European Union, the European Commission put forth several definitions in its recent publication of "Markets in Crypto-assets, and amending Directive (EU) 2019/1937" (MiCA). Title I defines a "crypto-asset" as a "digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or

[10] For example, see this New York Times article from June 2022. During an episode from Bloomberg's Odd Lots podcast, Bennett Tomlin, co-host of the Crypto Critics' Corner, explained the history of Tether as well as the concerns in an accessible manner.

similar technology." An "asset-referenced token" is a type of crypto-asset that "purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets. The Commission further defines "electronic money tokens/e-money tokens" for stablecoins, and "utility tokens" as a crypto-asset needed to obtain digital access to a blockchain-based good or service that is only accepted by the issuer of that token.

Before we discuss our own, more nuanced taxonomy of token types and applications, we want to outline several important facts about blockchain tokens:

1. Issuing a standard token is not difficult and does not require the issuer to have coding skills. One can use websites to issue an ERC-20 token by filling out a simple form. Services such as the Colony protocol allow the development of more complex token designs for governance tokens.

2. There are also no technological restrictions or limitations on who can and cannot issue a blockchain token, for lack of such restrictions is the essence of a permissionless system.

3. Tokens allow a re-imagination of value, ownership, use, and rewards.

4. Tokens live on a single infrastructure and can interact with other tokens.

5. Tokens are immediately transferable & usable in applications.

6. Token can be programmed to have many features and different uses.

7. Not all tokens are primarily investments, but people can buy tokens as investments.

With these issues in mind, in our opinion, the following are the most common types of blockchain tokens.

1. Payment tokens:
   These are tokens that are used strictly as a means of payment. The simplest example is native cryptocurrencies.

2. Stablecoins:
   These are digital representations of fiat currencies, most commonly the USD, but there are also solutions for the EUR, the CAD, or the CNY. Stablecoins can be (over)collateralized or un-/under-collateralized; they can be centralized or decentralized. Collateral can be in the form of traditional financial assets such as cash-like securities, commodities such as gold, or crypto-assets, most commonly bitcoin or ether.

A *centralized* stablecoin is issued by a single entity that also manages the collateral; examples are USDT and USDC. A *decentralized* stablecoin is issued based on a blockchain protocol/smart contract, and the management of collateral follows a set of rules. An example is a MakerDAO protocol which manages the stablecoin DAI. Finally, so-called *algorithmic* stablecoins aim to create a 1:1 exchange rate to a fiat currency using a monetary policy of issuing tokens or bonds, usually without being fully collateralized. There is no example to date of an algorithmic stablecoin that is empirically (and, arguably, theoretically/mathematically) run-proof; the 2022 collapse of the UST coin underscores potential issues with this approach. Figure 1 shows the time series of the dollar-value of stablecoins in circulation.

3. Asset tokens:
   These tokens represent ownership of an asset, collection of assets, or an item. Examples include a securities token that represents ownership of a firm, a non-fungible token, a claim or receipt token for a liquidity pool deposit, or fractional ownership in a fund such as those issued under the Set Protocol or Enzyme Finance.

4. Derivatives tokens:
   These tokens link to the prices of other crypto-assets or traditional assets, similarly to derivatives in traditional finance. Examples are perpetual bitcoin futures.

5. Utility tokens:
   These tokens are required to access or use a particular blockchain protocol. Examples are the filecoin token, which is necessary to use decentralized storage, or the Synthetix token, which is required to access and use the derivatives protocol by the same name.

6. Governance tokens:
   These tokens allow their holder to participate in the governance of a decentralized autonomous organization or blockchain protocol. One example is voting tokens, which enable the holder to vote on changes to the parameters of a smart contract. For instance, the UNI token allows users to vote on changes to the fees charged by the UniSwap decentralized trading protocol.

Notably, many tokens in circulation straddle multiple functions. For example, governance or DAO tokens may accumulate cash-flow rights and resemble traditional equities.

Tracking the issuance of new tokens is a challenge. Lyandres, Palazzo, and Rabetti (2022) compile a comprehensive dataset up to 2019 using almost 20 different data sources. However, new tokens are created each day. Some tokens, such as NFTs, are issued on known platforms such as OpenSea, making their issuance easily trackable. However, the multitude of tokens and blockchains makes tracking a Sisyphean task.

## 2.4 Money on the Blockchain

Cryptocurrencies in their current state are not money, but they serve the critical function of the internal means of payment for the usage of the system.

Many assets in traditional finance require some form of cash transfer. These transfers involve complex linking of different ledgers to ensure that beneficiary owners obtain the payments and to avoid overpayments or duplicate payments. Furthermore, payments often occur in a single, domestic jurisdiction, so foreign owners must initiate costly international transfers.

The main advantage of using a blockchain as the recording and value transfer infrastructure for assets is that it can automate and simplify back-office processes. To realize its full potential, however, blockchain would have to accommodate cash transfers, e.g., for dividend or coupon payments.

At the time of writing, several solutions exist for fiat-backed digital representations of fiat currencies; all of these are by private firms, not chartered banks. Examples include the USDT token by Tether Inc. and the USDC token by Circle Inc. These two tokens are backed by cash deposits at chartered banks or cash-like instruments. The two firms are overseen by state banking regulators, similarly to PayPal Inc. Despite these tokens' fungibility to fiat currencies, to the best of our knowledge, these stablecoins are not legal tender. Therefore, it is unclear whether these tokens can be legally used in dividend or coupon payments.

Furthermore, the existing stablecoins are subject to counterparty risk, which adds significant relative costs for low-margin trades (e.g., in fixed income markets).

For asset tokenization to unfold its potential across securities, the existence of payment tokens recognized as legal tender is vital. Arguably, the proliferation of stablecoins on Ethereum contributed to the boom of the decentralized finance ecosystem.

There are several paths forward. The first is to enable commercial/chartered banks to issue their own stablecoins and to mandate that users can redeem the different stablecoins at any chartered bank. Another approach is to designate a small number of (narrow)[11] banks that can issue generally accepted tokens. Lastly, central banks themselves could introduce central bank issued digital currencies, or CBDCs.

[11] The term "Narrow Bank" formally refers to a financial institution that provides only monetary (aka payments) services and invests its depositors' funds in safe assets only (such as treasuries). For early descriptions see Litan (1987), Pierce (1991), or Kobayakawa and Nakamura (2000).

For the remainder of our discussion, we assume that a legal tender stablecoin exists. In its absence, token issuers and holders would need to rely on workarounds that link the traditional payments network with the blockchain world.

### 2.5 Economic Benefits and Costs of Token-Innovation

The economic impact, costs, and benefits of various types of tokens are an ongoing area of academic research. We will highlight a few findings from the literature on token offerings. Notably, these academic papers study tokens with genuinely novel economic characteristics; they are not concerned with tokens that are merely digital representations of existing assets. The first strand of the literature focuses on the technology's more business-related application and service layers, where a firm offers a product and uses the underlying miner-enabled blockchain infrastructure.

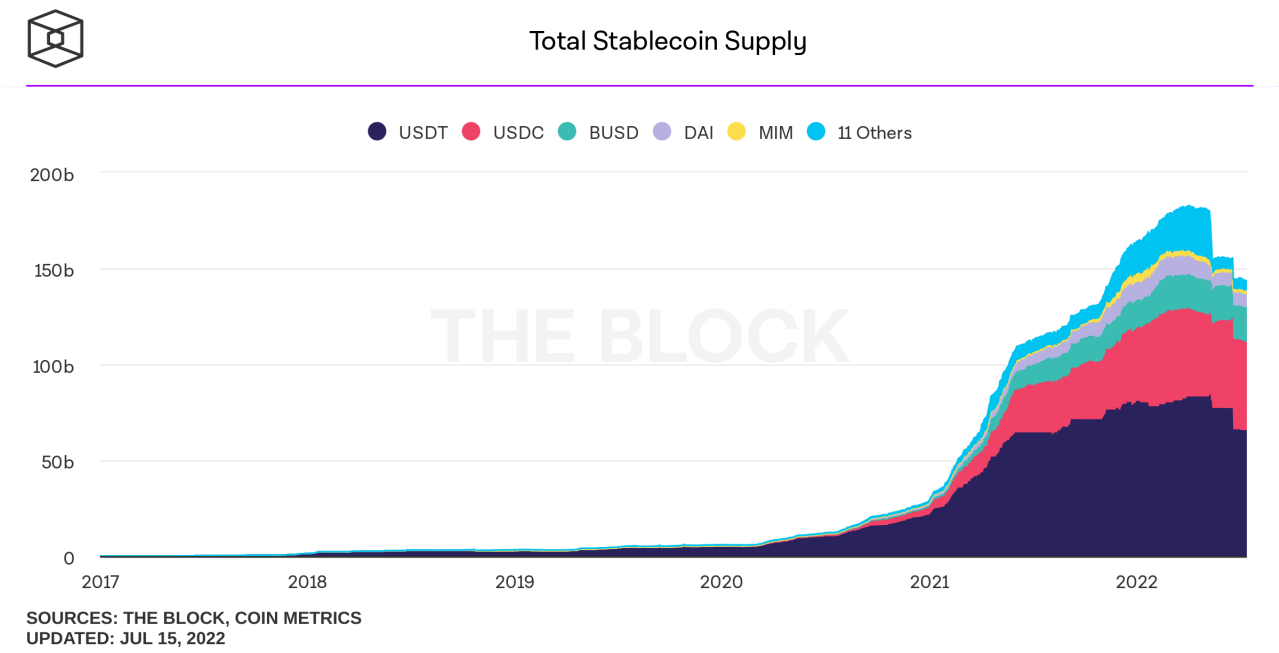
Catalini and Gans (2018) show how token issuers' monetary policy ---the issuance of future tokens--- affect investors' willingness to provide funds. Chod and Lyandes (2020) and Gan, Tsoukalas, and Netessine (2021a) model a token sale as a pre-sale of a fraction of future revenue, which leads to underinvestment relative to a venture capitalist or equity financing. Davydiuk, Gupta, and Rosen (2021) develop a model to study the signalling effect of issuers' token retention policy; in their model, the issuer knows the value of its business. Gan, Tsoukalas, and Netessine (2021b) focus on whether token issuers should commit to an upper bound of token issuance. Chod, Trichakis, and Yang (2019) study the role of revenue-sharing tokens in platform financing under moral hazard. Prat, Danos, and Marcassa (2021) develop a model to determine the fundamental value of utility tokens.

Lee and Parlour (2022) study crowdfunding in a competitive product market, where crowdfunding strongly relates to the pre-sale of utility tokens. They show that crowdfunding allows consumers to pay their surplus; in turn, firms finance projects that would otherwise have negative NPVs because of post-production product market competition. Malinova and Park (2020) study tokens as a financing tool and demonstrate that a utility token offering structured as a pre-sale of future service and one structured as a revenue sharing/royalty arrangement lead to different production decisions. Combining these two approaches offers optimal incentives and can finance more projects than a traditional equity contract.

The second strand of literature addresses whether tokens or platform-specific cryptocurrencies can spur platform adoption. Sockin and Xiong (2018) examine the role of cryptocurrency as a platform "membership token" in that only this token is accepted for transactions and as a miner compensation fee. Li and Mann (2018) and Bakos and Halaburda (2019) demonstrate that tokens can overcome possible coordination failures during platform operation, establish strong network effects, and support equilibria that favour a particular platform.

**Figure 1: Stablecoins in Circulation**

The figure shows the total supply of stablecoins across the major public blockchains. The drop in mid-2022 is due to the collapse of the stablecoin UST.




Cong, Li and Wang (2021a) and Cong, Li and Wang (2021b) develop asset-pricing models of tokens. They show that by facilitating transactions as a means of payment and by allowing community members to benefit from future growth, tokens can coordinate and accelerate adoption, platform growth, and improve economic welfare. Shakhnov and Zaccaria (2021) compare the value of venture capital advice with the possibly superior ability of tokens to spur network adoption. Candido (2019) and Li (2018) study the role of cryptocurrencies in platform adoption.

## Section 3: Linking the Blockchain and the Non-Blockchain World

To simplify the exposition, our discussion in this section assumes that the token represents an equity share in a firm. We note that this is merely a starting point for the debate. This approach is instructive, however, because the choice of tokenization mechanism affects the dissemination of dividends, the recording and tracking of beneficiary ownership, and shareholder voting. We will discuss fixed income instruments separately.

Equity shares can be tokenized in several ways by various entities, and conceptual, economic, and legal questions arise for each approach.

### 3.1 Blockchain-native issuance

The most straightforward approach is a **blockchain-native issuance.** In this scenario, the issuing firm or original owner registers the tokens as the native form of its equity, i.e., the deployed token signifies the stock certificate.

Even in this simple case, there is a need for a reliable process. Although tokens are uniquely identified by their blockchain address, these addresses are difficult to work with, and investors rely on ticker symbols. Ticker symbols on decentralized trading systems are not protected exposing users and investors to copycats. Anyone can register a new token and give the token a symbol that mimics the ticker symbol of the listed firm. For instance, for the popular token of the Yearn Protocol, YRI, at one point, there were 17 copycat tokens (see Lehar and Parlour 2022). Company websites can also be copied or hacked.[12]

### 3.2 Issuance by an intermediary depository or custodian institution

The second tokenization approach involves an intermediary that keeps the original stock certificates for an existing, publicly listed firm in a dedicated repository or with a custodian. This **intermediary depository or custodian institution** links two infrastructures: that of the original issue and a blockchain.

This approach resembles the issuance of depository receipts such as American Depository Receipts (ADRs), and we believe it instructive to revisit the ADR process.

According to the Securities and Exchange Commission (SEC), an ADR represents the shares of a non-U.S. company held by a U.S. bank outside of the United States. The infrastructures for company shares, such as depositories and custodians, generally reside in a single jurisdiction, and ownership transfers of any kind, including trading on exchanges, can only occur within that jurisdiction. As a result, U.S. investors are only able to purchase shares of a foreign company if they have an account in that foreign jurisdiction or if the foreign company lists its shares on a U.S. exchange. ADRs serve as a workaround, allowing private institutions such as U.S. depository banks with foreign representation to bridge the gap between the foreign and domestic settlement ledgers, making it possible for U.S. investors to purchase shares of a foreign company without having to open an account in that foreign jurisdiction.

To create an ADR, the foreign firm (in the case of a "sponsored" deal) or an investor (in the "unsponsored" case) delivers the shares to a depositary bank or its custodian in the firm's home jurisdiction. The U.S. bank then issues the ADRs to the investor in the U.S.,

[12] For instance, within hours after the blockchain of the Conflux Network with its internal cryptocurrency CFX went live, a group of fraudsters had built an exact replica of Conflux's original website under a slightly different name and with an offer to purchase a fraudulent ERC-20 token on Ethereum under the symbol CFX.

allowing the investor to trade the securities further in the U.S. The S.E.C. governs a registration process for ADRs: Form F-6 contains information about the original deposit, and there are additional forms, rules, disclosure and reporting requirements, and regulations if the foreign firm seeks to raise financing with ADRs.

J.P. Morgan and BNY Mellon dominate the ADR creation market, and the S.E.C. registration process ensures that investors who purchase ADRs know that the original deposit occurred and is legitimate. Therefore, the ADR process follows a set of well-established and well-understood rules. The depository banks usually handle all shareholder communications, dividend payments, and other recording-keeping services. Their custody fee is typically paid from the dividends that pertain to the original shares. If there are no dividends, the ADR-creating bank charges the broker-dealers who handle ADRs for their customers, and these entities pass on the costs to their clients.

The institutional arrangement for ADR issuance provides a blueprint for a reasonable approach to the intermediary issuance of blockchain tokens for shares:

- Shares are deposited at a custodian or depository bank in the jurisdiction of the underlying company.
- The custodian/depository issues the tokens on the blockchain and files a registration with the domestic securities regulator to indicate the terms of the arrangement.

The custodian/depository would also have to develop the technology to distribute the tokens and accept payment.

It is worth noting that collecting a maintenance fee for this service may be challenging if there are no dividends. In contrast to the ADR arrangement where the intermediary charges brokers who manage client accounts with ADRs, in the blockchain world, investors can hold assets in self-custody, making it difficult to collect fees.

After the distribution and sale of the tokens, the issuer (for blockchain-native issuance) or the custodian (for intermediated issuance) would have the following obligations:

1. Tracking beneficiary ownership
2. Distributing dividends and
3. Providing shareholder communications.
4. Custodians also commonly facilitate proxy and voting rights on behalf of ADR holders.

In what follows, we will discuss possible approaches to these tasks.

### 3.3 Tracking Beneficiary Ownership

Once tokens are in circulation, dividends must be distributed, and communications must reach shareholders. For this, one must know the beneficiary owners. In traditional finance, tracking beneficiary owners is straightforward (subject to settlement delays): a central

securities depositories record holdings at the broker level, brokers know beneficiary owners based on their internal records, and the two databases can be used together to assemble a complete list of beneficiary owners. Although easy to describe, this process is expensive and cumbersome in practice.

In the blockchain world, there is no central depository and no brokers who record ownership. Instead, token ownership is attributed to blockchain addresses, and at each point in time (measured in block-time, i.e., by the number of the last-processed block), a token is owned by a unique address. Obtaining ownership information is straightforward because it is recorded on the blockchain. Moreover, (any)one can acquire this information in real-time using the API of blockchain explorers such as Etherscan using GraphQL.

Determining the beneficiary owner behind an address is, however, more challenging. By default, tokens can be transferred to any address. Anyone, including legitimate investors, minors, and criminals that may not have gone through a KYC process, can have a blockchain address and own a token. Furthermore, a blockchain address need not always correspond to an individual's wallet: it could also be an omnibus account of a blockchain exchange or a smart contract that forms a liquidity pool. A naive approach to mitigate problems would be restricting the transfers to authenticated users. However, as we discussed earlier, such a restriction could prevent investors from using the DeFi applications and deny them the opportunities and convenience offered by the DeFi ecosystem. In turn, this would significantly decrease the value of a token. Creating lists of authenticated addresses may cause further downstream problems, such as antitrust, continuity, and the selling of addresses.

### 3.4 Suggested Best Practices for Token Issuance

To ensure the integrity of the token market, it is necessary for there to be reliable outlets such as regulatory filings where firms can register and display their token's address. Such a repository should contain details about the token, such as the number issued and its functions.

Based on the discussion in this section, we believe that the following is a reasonable set of best practices for issuers of tokenized assets.

1. Token registry: issuers or depositories/custodians should register the token name, address, quantity, date, and other features of tokens that they issue.
2. Process for "backed" tokens: depositories/custodians should register the number of deposited tokens and outline the redemption process. Regulators should establish an oversight framework for these backed tokens.
3. Shareholder information process: issuers and regulators should establish shareholder communication process by blockchain address and define it as

legally binding and sufficient. There should be relief for liquidity pool and wrapped token arrangements.

4. Dividend and voting process: issuers and regulators should establish a smart contract (possibly roll-up-based) dividend dissemination and voting process.
5. Failsafe process: issuers and regulators should develop a reconciliation process in case the blockchain fails.
6. Ownership restrictions: legal changes to who can own securities may be necessary. Careful consideration should be applied when tokenizing assets that have constraints on ownership.

## Section 4: Features of Tokens/Tokenized Assets

### 4.1 Functions of Traditional Assets

Most traditional assets have standardized features: Equity shares entitle their owners to voting rights and board-approved dividend payments. Bonds provide regular coupon payments and a face value repayment at maturity; commercial paper has a single maturity cash payment. Options have standardized terms and are commonly settled for cash at maturity.

Traditional financial assets in their current form are database entries, and any functionality such as annual meeting voting rights for equities derive from the underlying legal framework.

In the traditional world, some entity has to enable the functions such as reaching shareholders and distributing dividends. For ADRs, which are conceptually similar to asset-linked tokens, the issuing depository bank oversees shareholder information dissemination and dividend distribution.

Crypto assets can offer additional, pre-programmed functions that interact directly with the underlying blockchain and require less organizational overhead. Moreover, a blockchain allows firms to process any number of payments and business relations using the technology. Therefore, blockchain technology allows firms to issue new assets that segment and sell cash flows or to use tokens to incentivize users and employees.

Although tokenized assets can assume some of these functions, there are caveats and complications, and it may not be possible to translate all functions and roles from traditional finance to the blockchain world. For instance, there is no direct ownership attribution for tokens in liquidity pools.

In this section, we first discuss features of existing, traditional assets. We then discuss some of the new functions that may emerge for blockchain-based assets, and we outline how the choice of tokenization affects the applicability of the new functions.

The additional functions that we discuss here apply to natively issued tokens. Asset-linked tokens would require that the original assets have the same functionality, which they cannot. Finally, we note that there is a token standard in Ethereum, ERC-2222, for tokens that have a fund distribution mechanism.

### 4.2 Ownership Attribution: Blockchain vs Traditional

Ownership for traditional assets is based on the holder of record. However, there can be uncertainty as to who has rights to dividends or voting rights at a given point in time, due to the delay between trades and settlement and the delivery of assets, such as after a short-sale. The cum-ex tax scandal in Europe highlighted these issues. Typically, investors purchase traditional assets through a broker-dealer, who then arranges record-keeping with custodians. This arrangement allows issuers and regulators to rely on broker-dealers for various ownership-related functions, such as processing dividend payments.

Beneficiary ownership attribution with blockchain-based assets is both simpler and more complex. On the one hand, the ownership of blockchain-based assets does not require the involvement of a third party, as assets can be owned directly by the investor and held in self-custody. Attribution is simpler because blockchain-based tokens are always uniquely owned by an account at any given point in time. For instance, while traditional assets may have uncertainty of ownership when short sales are involved, this uncertainty does not arise for blockchain-based assets as short sellers must own an asset before they can sell it. Short sellers can borrow assets from lending protocols, but when borrowing the asset, the ownership formally transfers to the borrower.

On the other hand, beneficiary ownership attribution for blockchain-based assets can be complicated because the owning account can be a smart contract account. Two common types of smart contract accounts that hold tokens are lending protocols and automated market makers (which will be explained in detail in Section 5). Both these applications involve the creation of a liquidity pool to which investors can deposit their tokens (e.g., to earn interest or trading fee income). When they do, they formally transfer ownership from their account to the smart contract account. They receive a receipt token that they present later when they withdraw their deposit. However, a receipt token is not a derivative claim on a specific asset, it is an ownership share of the value of the liquidity pool. When an automated market maker pool sells a token or a lending pool makes a loan, ownership of the tokens immediately transfers to the purchaser/borrower.

Taken at face value, a smart contract deposit may appear similar to the arrangement that a client has with their broker-dealer. Very loosely, the broker-dealer effectively issues a receipt to the investor (the account balance), the investor holds a claim on the broker, as far as the security depository is concerned, the owner of the asset is the broker-dealer, but the broker-dealer is merely a custodian (with obligations) for the investor. However, this similarity is only superficial because a pool depositor is no longer the beneficiary owner of an asset. Additionally, smart contract accounts are limited and precisely

defined by their code, which may prevent them from accepting payments from an issuer or submitting shareholder votes.

### 4.3 Dividend and Coupon Payments

A key question to address when issuing tokenized assets is how token owners will receive dividend or coupon payments and additional shares in a stock split. There are several options to consider.

One approach is to have the depository institution create a smart contract in which owners who deposit their tokens into this contract at a specific time would receive dividends or coupon payments. These dividends and coupons would be paid in stablecoins so that when depositors withdraw from the contract, they receive their tokens plus a stablecoin payment.

An alternative approach is to send dividends, coupons, or new shares from stock splits directly to blockchain addresses. However, this implementation presents several potential issues. First, smart contract accounts, such as liquidity pools, would need to build functionality to receive payments on behalf of pool depositors and distribute the dividends when depositors withdraw from the pool. This is not a trivial task as the pool would need to be able to process an additional token (the payment currency). Second, crypto exchanges with omnibus accounts would need to develop systems to correctly distribute dividend payments, which presents functional challenges in a 24/7/365 environment. Third, it is very likely that the number of payments would exceed block capacity, opening the door to manipulations.

Fixed income tokens can be designed as bearer instruments at their inception. Such tokens could include a coupon function: at pre-determined intervals, the contract would create a new token, the coupon, and issue it to the current holder. The bond issuer would have to simultaneously create a pool where cash is deposited. Coupons are claims against this pool.

Buybacks can be easily arranged with a repurchase smart contract that users can access over a defined period of time.

Since blockchain tokens can be designed to trade at almost arbitrary granularity, stock splits or reverse splits appear to be an outdated concept for such assets, and it is unclear what a split operation would accomplish for blockchain native assets. Non-native assets, however, may undergo splits. There are two perspectives on this. Firstly, the issued token represents a claim on a different number of underlying assets, for example, in a 2:1 split, a blockchain token after the underlying splits is a claim on two underlying assets. Alternatively, the issuer could create new tokens and "airdrop" them to all accounts that hold tokens. Reverse splits are more complex as a token issuer cannot simply reduce the number of tokens in circulation. One solution is to issue a new token and declare the old token to be invalid from a certain date. The new tokens can be distributed to existing

owners at a pre-specified time via an "airdrop" or the firm can arrange an exchange program through a smart contract. However, airdrops can be problematic for smart contract accounts as they may not be able to receive or recognize the new token.

Two key considerations when designing dividend and coupon payments are cost and efficiency. Blocks have limited capacity, and for firms with many tokens and tokenholders, the number of dividend/coupon transactions may exceed the capacity of individual blocks. Rollups may be an appropriate solution because the batch processing of transactions is cheap. Furthermore, when requiring that users deposit tokens in the rollup, firms can ensure that their owners receive their dividends. Finally, shareholder voting can also be arranged in rollups.

### 4.4 Shareholder Communications

Shareholder communication is more challenging than the receipt of payments. First, smart contract accounts are pieces of code that cannot easily pass on information to pool contributors. Nor is it clear that they should – arguably, such a functionality is an add-on service, it is not clear that it should be an entitlement.

Second, blockchain addresses have no name attribution, and firms cannot mail owners invitations to annual meetings or other material information. However, it is possible to send information to blockchain addresses. For instance, chat.blockscan.com allows sending messages to any blockchain address, provided the user has signed up for this service. Since it is possible to get almost real-time information on who owns a firm's assets, firms can reach all their users, provided these users have signed up for the service. To take advantage of the options that blockchains offer, it may be necessary that firms receive relief and are allowed to disseminate information using specific protocols such as blockscan. This would put the onus on the owner to subscribe to a service.

Allowing shareholder communications based on blockchain accounts may require legal changes.

Likewise, smart contract accounts are not legal entities communication with or via such entities may require legal changes. It may be reasonable to grant firms relief because the granular divisibility of blockchain assets allows an investor to retain a nominal interest in a self-custody wallet and thus receive information: those who want to remain informed can keep a nominal amount of the token in their wallet and thereby ensure that they receive relevant shareholder information.

### 4.5 Shareholder Voting

Shareholder voting can be arranged similarly to receiving a dividend: shareholders deposit their token in a specific contract and receive voting tokens. They then submit these tokens for their respective decisions. Once the vote is complete, token holders

receive back their original token. As with dividend payments, organizing voting in a rollup is more efficient.

When assets are formally owned by smart contract accounts, voting can be more difficult because it is may not be possible or practical for a smart contract to exercise voting rights on behalf of its depositors. At the same time, without such a functionality, activities in liquidity pools around important events such as shareholder votes could distort market liquidity and prices, e.g., when investors withdraw funds to vote.

### 4.6 Direct Shareholder Engagement for Blockchain Assets

Most public firms are organized with agent representation: shareholders vote for the board of directors who appoint and monitor the chief executive officer. The CEO makes decisions on behalf of the shareholders, sometimes subject to board and general shareholder assembly approval. Shareholder involvement is organizationally difficult and costly.

With blockchain tokens, shareholder votes and engagement can be arranged directly. For instance, it is possible to arrange votes on-chain for standard votes such as those during annual meetings. Firms can also deploy the same mechanism for other types of arrangements, and it is possible for firm to change its corporate charter to expand the range of issues for which they seek shareholder input.

Furthermore, tokens can be designed to allow shareholders to flip the table and initiate a vote. The Decentralized Autonomous Organizations (DAOs) that have emerged over the past few years provide an idea of how these ideas can carry over to traditional firms:

- Anyone can make a proposal and post it in a public governance portal.
- There is a multi-stage process to "take the temperature" on a proposal; each stage has quorum and pro-vote thresholds.
- After the preliminary stages, proposals open to on-chain voting, conducted via a smart contract.

For DAOs, votes can be binding because the DAOs smart contracts automatically accept changes (e.g., in terms of fees) following the on-chain vote. In non-blockchain businesses, the corporate charters would likely need to be adjusted to make the results of unsolicited shareholder votes binding.

### 4.7 Cash Flow Contingencies for Blockchain Assets

When a blockchain hosts a legal tender payment token (i.e., a stablecoin or CBDC), firms can organize all payments using the blockchain that their token is listed on. They can then use this blockchain for hedging, contingent contracts, subscription arrangements, and memberships (encapsulated in non-fungible tokens (NFTs)).

Such an arrangement would also allow token issuers to tie token features to specific cash flows and costs. For instance, a larger firm may be able to link a token to a single project's stream of cash flows, or they could provide employee reward tokens for achieving income targets. Ultimately these more comprehensive options allow firms to change their internal organization if they so choose.

### 4.8 Customer Engagements

A common feature of blockchain projects is that they reward service users with their tokens. This model may not be suitable for all firms or in all circumstances. However, it can be fruitful for situations where user participation creates network effects critical for a business's success. Examples are social networks, user-created content platforms, or liquidity pools.

### 4.9 Potential Legal Changes

The discussion in this section highlights that the tokenization of assets on blockchains may requires several legal changes pertaining to sending payments and communications to stakeholders. Namely:

1. Issuers should not be responsible for knowing their investors' identities. Instead, they could be required to implement an opt-in process to reach investors, e.g. through a communication tool such as blockscan.
2. Investors should be responsible for using dividend, voting, and interest dissemination services.
3. Providers of custodial wallets such as crypto exchanges must be required to provide information dissemination and payment distribution mechanisms.
4. The legal status and obligations of smart contract accounts to its depositors/users must be clarified.

## Section 5: Trading of tokenized assets

Blockchain tokens and coins can be traded on centralized platforms and with decentralized protocols. A platform is *centralized* if trades are arranged and processed in a firm's proprietary system. D*ecentralized* trading utilizes a blockchain's decentralized processing capacity to arrange and process transactions.[14]

[14] This section contains portions of a review paper that the second author of this report recently circulated as "A 2022 Primer for Crypto Trading."

### 5.1 Centralized Trading Platforms

Prior to the summer of 2020, most crypto tokens that had been issued on the various decentralized platforms, such as Ethereum, could only be traded on centralized venues such as FTX, Poloniex, Binance, OKX, Kraken, Huobi, or Coinbase.

There are two main types of centralized exchanges: fiat-connected and crypto-only. Fiat-connected exchanges link to the payments rails of traditional finance; examples are Coinbase, Upbit, Kraken, and Bitbuy.

However, most crypto exchanges are not directly connected to the world's traditional payments networks and, therefore, are also not connected to the traditional world of finance. Examples include Poloniex, Binance, OKX, Huobi, and Kucoin.

For venues that are connected to the payments network, users can fund their account by wiring fiat currency to the exchange, similar to what one would do when opening an account with a traditional investment brokerage. Crypto-only venues do not accept wire transfers. Although some allow users to fund their accounts through the expensive workaround of a credit card transaction, in most cases, users need to transfer blockchain assets to the exchanges.

There are two ways for users to buy crypto assets. First, many venues allow users to purchase cryptocurrency directly from the exchange, either from their fiat account or using a credit card. This service is like a money exchange business, and users do not interact with one another.

Second, crypto exchanges have a trading platform typically organized as a public limit order book where users can submit market and limit, as well as specialized orders, and trade with one another rather than with the exchange. Some token issuers additionally enlist specialized market-making firms to ensure that there is always liquidity in the book.

Users can trade crypto assets directly against fiat currencies on fiat-linked venues, whereas on crypto-only platforms, all trades are between crypto assets. Typically, one of the two crypto assets in a traded pair is a stablecoin, a digital representation of a fiat currency such as the U.S. dollar.

Since trades are arranged and recorded on the exchange's proprietary infrastructure, these venues are referred to as *centralized*.

**Fees.** Deposits and withdrawals from centralized exchanges involve fees, and these can be substantial. For instance, Interac transfers in and out of Canada's first regulator-approved venue, Bitbuy, cost 150 basis points, wire transfers cost 50 basis points, and withdrawals to the Ethereum blockchain can cost around $15-$20, depending on the price of the cryptocurrency ETH. When using the order book for trading, users have to pay trading fees similar to those on stock exchanges. When buying from the venue for cash, users pay an implicit fee through the markup that the exchange charges.

**Token Listings.** Centralized exchanges determine which tokens are traded on their platform and typically only enable trading for a limited number of tokens. For example, on Canada's first regulator-approved venue, Bitbuy, users can trade sixteen out of the thousands of blockchain tokens in circulation. A key consideration for listing a token is whether the token is considered a security, as exchanges may avoid listing an unregistered security to avoid regulatory action from their domestic regulator. Some centralized exchanges, such as Binance, charge token issuers a substantial fee for enabling trading of a token on their platform. Despite this, centralized exchanges can be attractive for crypto projects because exchange listings generate liquidity and allow users to obtain the project's tokens.

**Custody Risk.** As we discuss in Section 1.6, to trade on a centralized venue, users register and KYC with the platform. They usually transfer custody of their assets to the venue, which is why an exchange wallet is referred to as a *custodial wallet,* and why custodial wallets are associated with known individuals. Therefore, a centralized crypto exchange is similar to an investment broker.

By now there is a body of evidence showing that it is risky to keep tokens at a centralized exchange. For instance, QuadrigaCX sold customers crypto-assets that the platform did not own. FTX used Alameda Research (both owned by the CEO and founder of FTX) as a market maker, and then allegedly used their customers' assets to cover losses of their market maker. In both of these prolific cases, the exchange had control over customer assets and co-mingled its own assets and liabilities with their customers. A key concern, therefore, is the custody arrangement. Wealthsimple in Canada, for instance, uses a third party custodian for its clients' cryptoassets. Coinbase raised concerns in its May 2022 quarterly filing (p. 83) where they stated that "custodially held crypto assets may be considered to be the property of a bankruptcy estate, in the event of a bankruptcy, the crypto assets we hold in custody on behalf of our customers could be subject to bankruptcy proceedings and such customers could be treated as our general unsecured creditors."

**Regulatory Implications.** In the wake of the dramatic collapse of the crypto asset trading platform FTX in 2022, regulators worldwide have intensified their scrutiny of centralized exchanges. Recognizing that centralized crypto exchanges are similar to investment brokers, regulators in Canada require crypto asset trading platforms to register as investment dealers. There are still many questions to be answered.

Crypto exchanges operate trading platforms for items that often look like securities, and investors may reasonably expect orderly, non-manipulative conduct. However, there is no uniform regulation regarding trading conduct for crypto platforms that is comparable to those on traditional equity and derivatives trading venues. Almost all investors access stock exchanges via their brokers, where professional traders oversee trading behavior. In contrast, on crypto exchanges, individuals interact directly with one another, and, being untrained and unlicensed, may display behavior that professional traders would

be sanctioned for. Regulation, therefore, may need to address what trading conduct platforms need to require of untrained individuals.

Moreover, centralized exchanges make listing decisions and often charge substantial fees for listings. Platforms also invest in the crypto assets that they list, and such investments are not always transparent but should be, lest the venues engage in touting. One can argue that a listing decision endorses a crypto asset as an investment vehicle. Yet, making investments and charging for listings while creating credibility for investors may create substantial conflicts of interest, which are rightfully regulated in traditional financial markets. Therefore, platforms should be required to disclose their listing process, standards, and criteria, as well as their own investments and holdings.

Blockchains are borderless by design and aim to serve a worldwide clientele. In principle, crypto exchanges can and want to serve a worldwide clientele. However, there are many regulators worldwide, often with idiosyncratic and conflicting requirements. Dealing with a single regulator usually ties up several lawyers for months. Worldwide compliance is extremely costly.

In practice, threats of regulatory action have prompted many venues to exclude users from countries or regions such as Canada/Ontario and the U.S., e.g., by blocking IP addresses or requiring proof of residence in a non-blocked country. Anecdotally, for many Ontario-based Binance users, this led to the unfortunate situation where they had to close their accounts with Binance. Many of them moved their assets to the second largest venue at the time: FTX.

Furthermore, excluding investors from geographic regions may not be enough for compliance. The S.E.C.'s chairman Gary Gensler has stated that an exchange may fall under the S.E.C. jurisdiction because users can find ways to circumvent its self-protective measures. Therefore, even with the best intentions and solid, well-thought-out systems, it is expensive and risky for a crypto exchange to serve a worldwide audience.

**Regulatory Scrutiny and the Future of Centralized Exchanges.** According to Coinmarketcap, there are over 500 crypto-trading platforms worldwide, many of which offer a similar product. At the same time, according to data from The Block, Binance accounts for 75% of non-fiat-linked volume, and Coinbase, Upbit, and Kraken account for 75% of fiat-linked trading volume. Therefore, centralized crypto trading is highly concentrated.

Coinbase and Kraken are already regulated in the U.S., and Upbit is regulated in South Korea. Despite significant pressure, Binance has yet to submit itself to regulatory scrutiny. For instance, Binance's response to the Canadian OSC's demand for compliance was not to comply but to cease offering services to Ontarians. The fundamental problem for Binance (and other crypto-only venues) is that it is unlikely that they can continue operating their business as they do now when they are under regulatory scrutiny. They may likely have to cease trading in many crypto-assets, they may have to unwind their

stablecoin offerings, and they may have to divert resources from product development to compliance. If they can't maintain their business activities, but customers continue to want these services, then another unregulated venue will take their spot.

Regulators, therefore, have a related fundamental problem: if their compliance demands require a centralized platform to give up on products that consumers want, then forcing a platform into compliance may simply shift users to another platform. If the alternative platform is worse, for example, in terms of custody compliance, then forcing regulation onto a platform can make investors worse off.

Arguably, the collapse of FTX in November 2022 spooked many investors and brought to the forefront the custody risk of centralized exchanges. Many trading platforms responded by regularly publishing proof of reserves for their assets to mitigate their investors' concerns. Although this is a useful attempt to self-regulation by using the transparency of blockchains the approach is incomplete because reserves must be compared to liabilities. Going forward, probably the best outcome for crypto-only exchanges is that, under the leadership of the largest ones, they develop an approach to self-regulation that respects the technological innovation and satisfies the big countries' regulators (and maybe, by association, those in smaller jurisdictions).

In an alternative scenario, crypto-asset trading and token issuance moves entirely on-chain, so that centralized exchanges all but disappear. Users would still need to exchange their fiat money for crypto money, but they do not need a high-powered limit order book for this simple task. Instead, specialized service providers or even traditional financial institutions may offer users to swap digital representations of fiat currency for real fiat currency directly from their deposit account. In this scenario, traditional financial institutions would likely absorb the technology from centralized exchanges.

### 5.2 Decentralized Trading

It is possible to organize crypto-asset trading on a blockchain, similar to a traditional stock market. A limit order is a set of instructions for a conditional exchange of a stock for cash. These instructions can be cast into a "smart contract" and registered on the blockchain. However, this approach is not practical because each new limit order submission costs a fee to blockchain validators. Unexecuted orders also waste resources as all 10,000+ nodes must process the order.

Because of this difficulty, blockchain-based tokens traded almost exclusively on centralized, "off-chain" exchanges until mid-2020, thus reducing the blockchain to just yet another settlement infrastructure. Matters changed in 2020, however, with the development of two types of decentralized trading mechanism.

The first are **rollup based** systems such as dYdX. The idea of these systems is simple: users first deposit funds into a rollup-contract. They can then submit limit orders within the roll-up setting. These are essentially just signed transactions that become active when the

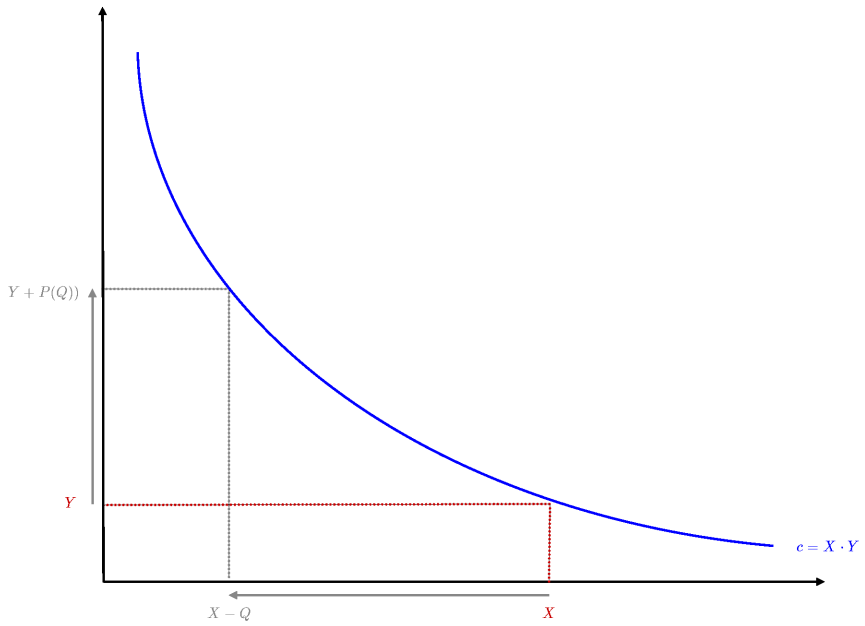
system can match a willing buyer and seller. In contrast to on-chain processing where all nodes must process and store information for such orders, in a rollup only the validator handles the signed orders. In contrast to a centralized exchange, there is no single third party that has control over the assets in the rollup, making them more secure. Although the rollup validator processes the transactions, as part of the protocol users can challenge and revert demonstrably wrong/fraudulent transactions. Rollup technology also allows for a much more efficient processing of transactions so that blockchains with their limited capacity can process up to 500 times the transactions even with current technology.

The second and most commonly used decentralized trading system are **Automated Market Makers (AMMs)**, such as UniSwap, SushiSwap, and PancakeSwap. These systems have seen tremendous user uptake and process billions of dollars' worth of transactions daily. An AMM is merely a "smart contract," a piece of code registered on a public blockchain. AMMs have several novel institutional arrangements that are not present in most traditional markets. In the latter, proprietary trading firms make billion-dollar investments to gain nano-second speed advantages so that they are at the "top of the order book" whenever and only when it is opportune. An AMM "pools" liquidity so that a liquidity demander trades against the supplied liquidity in a pro-rated manner; liquidity providers do not compete for speed or price at all. This setup allows retail investors to earn passive income from contributing their assets to a liquidity pool because liquidity provision does not require specialized skills or expensive equipment. Crucially, AMMs are not periodic auctions that require coordination in time, but they offer trading in continuous time. AMMs do not directly rely on a market mechanism that equilibrates demand and supply and determines an order's cost. Instead, they use a hard-coded pricing rule that depends deterministically on the amount of liquidity in the pool.

**How do AMMs work?** A swap exchange creates a liquidity pool by combining deposits of pairs of tokens A and B from liquidity providers. To provide liquidity, a user transfers a set quantity of both tokens to the AMM smart contract. Usually, the user will receive a receipt token in exchange for their contribution, and they can use this receipt in other applications, e.g., as collateral for a loan. A liquidity demander can trade against a liquidity pool by sending one token and receiving the other token in an atomic swap. The exchange rate is determined by a pre-coded rule that maintains the “invariance” of the pool’s aggregate liquidity. When a liquidity demander removes one token from the pool, they must deposit a quantity of the other token such that the aggregate liquidity of the pool defined by a “bonding curve” remains unchanged.

**Figure 2: Illustration of an Automated Market Maker Bonding Curve**

The blue curve is the bonding curve and describes a level of liquidity based on the product of the quantities of the two tokens, *c=XY*. For instance, for the ETH-USDC contract, in early 2022, this product was 38,100 x 118M. In this example, a trader withdraws *Q* of the *A* tokens from the contract (indicated on the horizontal axis). The value of the function (measured on the vertical axis) at the horizontal position *X-Q* is the number of the *B* tokens that must be in the pool to maintain the same liquidity level, and the change *P(Q)* is therefore the price for the quantity *Q*.




Although there are theoretically endless options for bonding curves, almost all AMMs use the same functional form that we illustrate in Figure 2. This bonding curve is referred to as a "constant product" pricing rule. Suppose the liquidity pool contains X units of token A and Y units of B. The ratio Y/X is the implicit marginal price of an A token measured in B tokens. If the B token is a stablecoin, i.e., a digital representation of a fiat currency, then the exchange rate Y/X is the cash price of an infinitesimal amount of A tokens. Under constant product pricing, the aggregate liquidity c is determined by the bonding curve *c=X·Y*. The number Q of A tokens that a buyer receives for *P* of the *B* tokens must be such that the liquidity level remains invariant: c=(X-Q)·(Y+P).

For instance, at the beginning of February 2022, the UniSwap (V2) token pair ETH (the native cryptocurrency of Ethereum) and USDC (a digital representation of the US dollar) contained approximately 38,100 ETH and 118M USDC; the implied marginal price of 1 ETH was thus 118M/38,100 = 3,097 USDC. Larger trades create a price impact. For instance, a liquidity demander who wanted to buy 100 ETH from this contract would pay approximately $3,105 USDC per ETH, one who wanted to buy 1,000 ETH would pay $3,181 per ETH.

**Table 1: Comparison of centralized and decentralized exchanges**

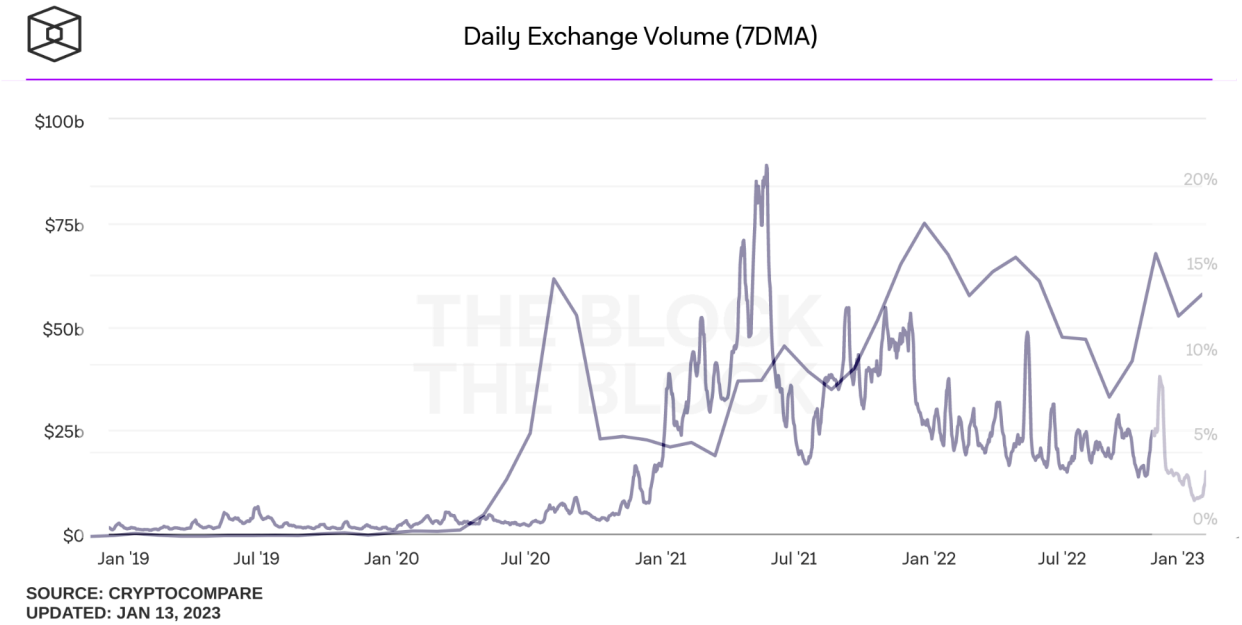
| | centralized exchanges | | decentralized exchanges |
|---|---|---|---|
| | fiat-connected (regulated) | crypto-only (unregulated) | (automated market makers/swap exchanges) |
| wallet | custodial | | non-custodial (full user control) |
| trading fees | maker-taker, bid-ask spreads | | liquidity demander pays supplier, slippage |
| withdrawal/deposit fees | significant | | none |
| gas fees for trading | none | | yes |
| ownership/governance | domesticized corporations | | decentralized autonomous organizations |
| traceability | within-system traceability, flows through payments follow AML rules | | full traceability of movements between pseudonymous wallets |
| user error handling (e.g., lost passwords) | support provided by platform | | user responsibility |
| malicious behavior by exchange | legal process but funds may be lost | | user can withdraw funds |
| AML enforcement | as per host country's rules | | none, but full traceability |
| wash trading | low | medium to high | Unknown |
| exchange solvency | supervised | possibly proved on-chain | by design |
| hacks | significant but possibly insured | significant | none |
| wire transfer fiat deposits | yes | no | no |
| credit card fiat deposits | yes | yes | yes (for dYdX) |
| KYC | yes | usually | no, access direct from pseudonymous wallet |
| token listings | often regulator-approved/tolerated | determined by exchange | user determined/unrestricted |

A full comparison of the different trading systems goes beyond the scope of this report. Table 1 briefly summarizes the some of the headline differences between the different types of exchanges along critical dimensions such as types of access, KYC, manipulations, AML enforcement, listings, and ownership. Figure 3 plots the time series of the fraction of crypto-asset trading that traded on decentralized exchanges. More details can be found in Park (2022a).

**Summary and Outlook.** Centralized exchanges create the market for tokens, and they are essential in the crypto ecosystem. Yet they also present significant problems and challenges, and seemingly every crisis in the crypto markets uncovers more concerns. Conceptually, centralized exchanges are no longer necessary, and decentralized

**Figure 3: Evolution of DEX vs. CEX Trading**

The figure displays the ratio of decentralized to centralized trading over time as well as the monthly level of exchange volume.




trading facilities are becoming increasingly liquid and convenient. It is possible to envision a future in which centralized exchanges no longer exist. Instead, crypto trading in the future may occur exclusively on-chain.

Arguably, traditional financial institutions would be better suited than exchanges to serve as on- and off-ramps for crypto-users and investors. For FIs to play this role, however, governments and regulators must facilitate FIs' engagement, develop digital ownership, and establish fail-safe systems.

Over time, most traditional financial assets, including fiat money and property registries, may be either tokenized or directly re-issued as new vehicles on blockchains to be listed, used, and transferred without borders.

A key innovation of AMMs is a novel approach to liquidity provision. Lack of liquidity is one of the biggest problems in securities markets, especially outside equity markets. Low liquidity makes trading more expensive and raises the risk of not finding a counterparty, making it difficult for investors to adjust their risk exposure. In turn, issuers face considerable challenges in raising funds and incentivizing employees with stock options. A key innovation of automated market makers is the pooling of liquidity, which could improve liquidity and lead to better-functioning capital markets.

### 5.4 Economic Implications of Tokenization

In Section 2, we highlighted some of the economic implications of firms using tokens with novel features as a form of financing. Here, we will review the role and impact of the underlying technology features, irrespective of the token design.

Blockchain technology brings several innovations, including smart contracts, atomic swaps/immediate settlement, peer-to-peer trading, liquidity pooling, and transparency of transactions and holdings.

Lee, Martin and Townsend (2022) study the impact of settlement immediacy. They examine the allocations achieved in a decentralized market with either the legacy settlement system or a token system. The authors show that asset tokenization can facilitate commitment and improve allocational efficiency (the "who gets what and when"). When counterparties regularly and strategically create failures to deliver, an auto-enforced smart contract can force delivery and improve efficiency. However, the authors also show that increased transparency that comes with tokenization can exacerbate existing "hold-up" problems (strategic delivery delays by one party to "squeeze" the other). This problem arises because the willingness to agree to a contract reveals information about the proposing party.

Malinova and Park (2016) identified a related problem in the peer-to-peer trading of large institutions because a high level of transparency can create front-running opportunities for counterparties.

Atomic swaps compare to traditional trading as real-time gross settlement (RTGS) does to large-value transfer systems (LVTS). The latter relationship has received significant attention in the literature. For instance, Martin and McAndrews (2008) examine how real-time gross settlement systems improve liquidity by eliminating resolve counterparty and credit risk. Koeppl, Monnet, and Temzelides (2012) explore the liquidity tradeoffs for different settlement speeds. Khapko and Zoican (2020) study how settlement speed affects market makers and find that fast settlement can cause inefficiencies.

Garratt, Lee, Martin and Townsend (2019) shed light on the effect of post-trade transparency that blockchain technology brings. They argue that trading platforms may choose inefficient disclosure policies.

### 5.5 The Costs and Benefits of AMM Liquidity Provision

A market maker provides capital and receives a fee income in return. However, the value of the assets may change over time, in which case the market maker may incur a loss. The implicit assumption of automated market makers is that liquidity provision is passive because liquidity providers do not adjust their positions. Arguably, they are designed for use by unsophisticated investors who want to earn incremental income on their assets. The blockchain community measures the costs of liquidity provision conditional on a price

movement by what they refer to as "*impermanent loss*." The "impermanent loss" is the difference in the value of assets held inside the AMM liquidity pool relative to those held outside of the pool.

We follow the description from Binance and UniSwap. Assume liquidity providers collectively made deposits of $X_0$ of the $A$ tokens and $Y_0$ of the $B$ tokens (which we will assume to be the numeraire) in an automated market maker liquidity pool. The price $P_0$ is the marginal price of an $A$ token measured in $B$ tokens, $P_0 = Y_0/X_0$, and since the $B$ token is assumed to be cash, the value of the deposit measured in cash is $P_0 \cdot X_0 + Y_0 = 2P_0X_0$. Suppose now the price moves permanently from $P_0$ to $P_1$. This move could be triggered either because of a trade against the pool or because the price in the broader market moved and the arbitrageurs traded against the pool. If liquidity providers held their tokens outside the pool, following the change they would own $P_1 \cdot X_0 + Y_0$. If instead, they provide liquidity in the pool, the pool holdings of the tokens adjust, $X_0 \to X_1$ and $Y_0 \to Y_1$, so that the new holdings satisfy $P_1 = Y_1/X_1$. Liquidity providers with token holdings in the pool then own $P_1 \cdot X_1 + Y_1$ in cash. The difference between the in and out of the pool holdings is the *implicit dollar loss* (IDL) of providing liquidity:

$$\text{IDL}(P_0, P_1) = P_1 \cdot X_1 + Y_1 - (P_1 \cdot X_0 + Y_0).$$

The *impermanent loss* of a price movement from $P_0$ to $P_1$ is expressed as the implicit loss relative to the initial holdings:

$$\text{IPL}(P_0, P_1) = \frac{\text{IDL}(P_0, P_1)}{2XP_0}.$$

Liquidity providers usually receive an additional fee for a trade that depends on the transaction value. In practice, they keep their deposits in the pool for long periods of time while fee income accumulates. Assume that the fee rate $f$ is collected on the dollar volume $v$ of transactions that occur between the time when the price was $P_0$ and when it moved to $P_1$. Then liquidity providers receive $v \times f$. The ratio of volume to initial pool holdings, $\nu = v/(2P_0X)$, is the *velocity* or turnover of the pool's liquidity over a time horizon. We can then write the impermanent loss as

$$\text{IPL}_f(P_0, P_1, \nu) = \frac{\text{IDL}(P_0, P_1)}{2XP_0} + f \times \nu.$$

For the *constant product* bonding curve that we described above, the impermanent loss can be expressed in closed form, using the gross return $R = P_1/P_0$[15]

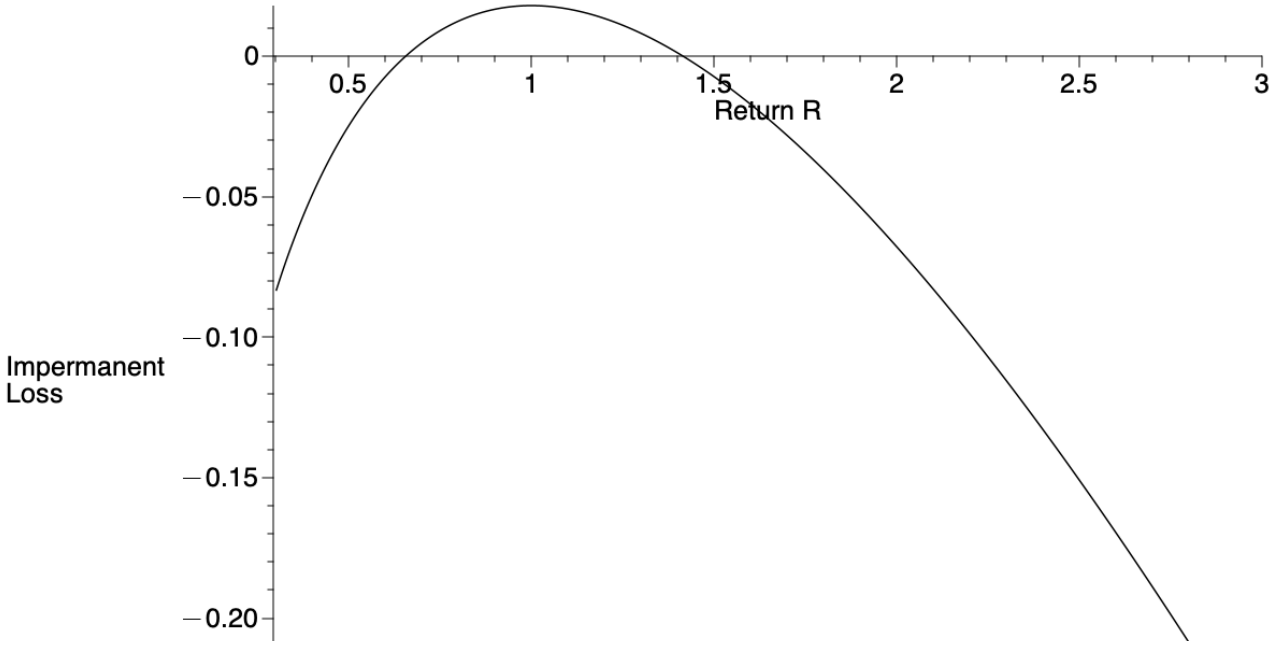
$$IPL^{constant\ product}(R) = \sqrt{R} - \frac{1}{2}(1 + R) + f \times \nu.$$

To put these numbers into perspective, we use the wETH-USDT pool in UniSwap v2 as a stylized example. The gross return for wETH to the USD for that time horizon was 0.7 (the

[15] For details of the derivation see Park (2022b).

**Figure 4: Impermanent Loss for Constant Product Pricing**

The figure displays the impermanent loss as a function of the gross return, $R = P_1/P_0$. This figure plots gross returns in the range of return 0.3 (the price drops by 70%) to 3 (the price triples), it includes a fee of 30bps and it assumes a turnover of 6 (over the deposit time horizon, dollar volume is 6 times the deposited amount.




exchange rate of ETH/USD dropped from \$3,724 to \$2,598), implying an impermanent loss of 1.3%, not accounting for fees. At the beginning of January 2022, the pool contained $2 \times \$118M$ worth of tokens. The total dollar-volume for January was \$1.6B, implying a turnover $\nu = 6.8$. For the 30bps fee, the total impermanent loss including fees therefore was 6.7 bps, i.e., liquidity providers earned 6.7 bps relative to holding the same amount of tokens in their portfolios.

Figure 4 plots the impermanent loss function assuming a turnover rate of 6 to illustrate that when the price does not move excessively for high volume (there are on average as many buyers as sellers, so that the price is approximately mean reverting), liquidity providers can earn a positive income relative to only holding the asset. The loss occurs only when prices move directionally. Loosely speaking, the fee that liquidity providers collect in "normal times" compensates them for the risk of directional moves. The above example highlights that this mechanism works even if the market price moves against the liquidity providers.

# Section 6: Usage of Tokenized Assets in the DeFi Stack

## 6.1 An Overview of Decentralized Finance Applications

From 2019 to 2022, there was a boom in service provision to the crypto space, with many services aimed at investors. Two types of services emerged: centralized and decentralized. A centralized service is provided by a firm, and control over the service provider's actions is at the discretion of individual firm managers or committees. A decentralized service, on the other hand, is a smart contract deployed on the blockchain, operated by blockchain validators, and is beyond the control of an individual manager or a firm's policy. For example, although the now-defunct Celsius.Finance is often mistakenly referred to as a DeFi service, it made centralized lending decisions and is therefore a centralized entity.

According to dappradar.com, there are close to 2,800 decentralized finance applications, or DeFi apps, across major blockchains, with around 400 of them being on Ethereum. Despite the large number of apps available, most of them see little usage. The ones that do see usage typically cover decentralized trading and borrowing/lending. In the borrowing/lending aspect, it is common to see over-collateralization of loans, although there are protocols that allow for under-collateralized loans, albeit few and only for known parties. These applications generate revenues, as Figure 5 illustrates. It is important to note that the majority of revenues flow from liquidity demanders to suppliers, with very little going to the protocols themselves.

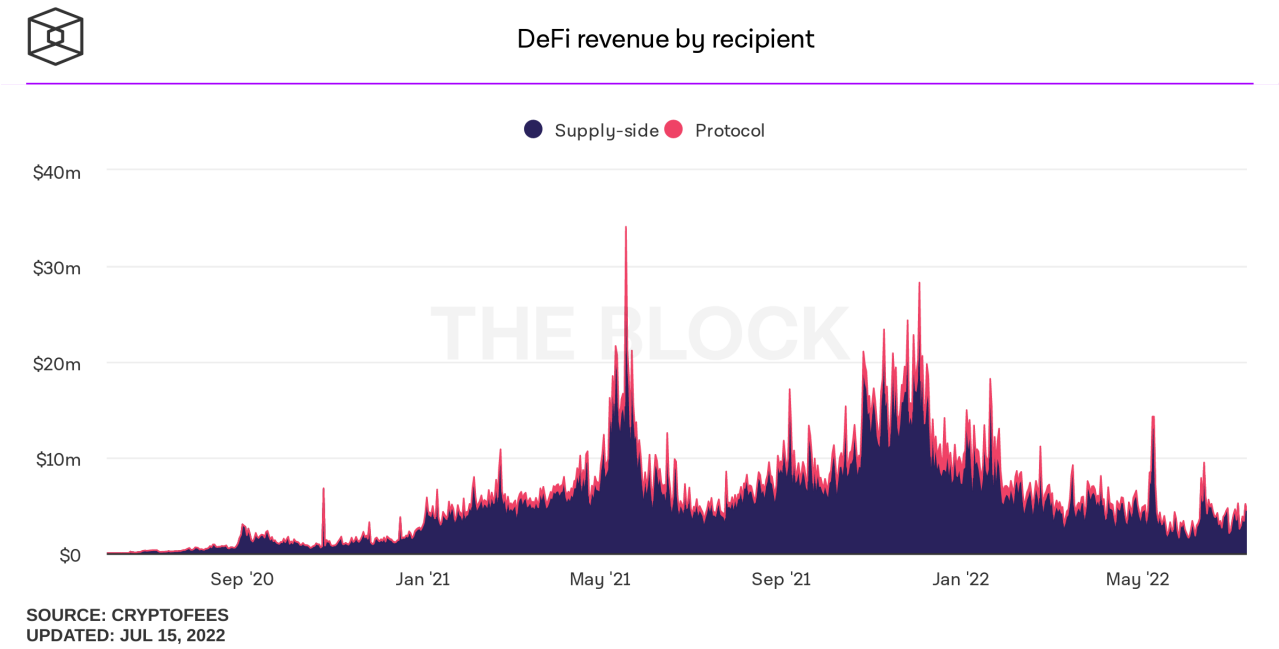
For instance, the operation of the UniSwap protocol ensures that liquidity demanders pay liquidity suppliers a fee; depending on the liquidity pool, this fee can be 1, 5, 30, or 100 basis points of the transaction value. In December 2022, UniSwap processed around $100 billion of volume and collected approximately $22 million in fees. Although the protocol could also include a fee that would pertain to the owners of the UNI token, such as a dividend, this feature is currently disabled.

A key feature of many DeFi protocols is that they establish liquidity pools. These pools allow users to earn rents on the re-use of their assets directly. In traditional finance, these rents typically go to intermediaries, such as a broker who lends shares to short sellers, while the original depositors may benefit indirectly, for example, through lower commissions.

Users create liquidity pools by interacting with the respective DeFi protocols' smart contracts, and developers can establish protocols for any token with pre-specified

**Figure 5: DeFi Revenues**

The figure displays the daily dollar-value of revenues earned across all DeFi protocols. "Supply side" refers to payments from liquidity demanders to liquidity suppliers; "protocol" refers to revenues that are collected for the underlying protocol (usually, these revenues can be claimed by the owners of DAO tokens, who control the features of the smart contract that provides the service).




properties, usually the ERC-20 standard. Therefore, any token deployed on Ethereum can be used for borrowing/lending, trading, and other DeFi applications.

## 6.2 DeFi "Legos"

A key feature of DeFi protocols is that they interact with one another in the sense that users can construct a sequence of transactions that string together across different DeFi applications; hence the term DeFi-Lego.

Let us explain the process with two examples. In the first, imagine that there is a price dislocation or arbitrage opportunity between two trading venues. To trade in DeFi, one needs to own the respective token -- there is no short-selling. However, many investors deposit their assets at lending platforms to earn interest. Short sellers may then borrow from such a platform with a flash loan: such a loan would be taken up and repaid within a string of transactions that are processed within the same block. Notably, the loan is only taken up if it also gets repaid. In the example, suppose there is a dislocation in the wrapped bitcoin (WBTC) to USDT price between Sushiswap and UniSwap. An arbitrageur with ETH could take up a flash loan on the lending protocol Aave for USDT against ETH

collateral, buy WBTC on protocol, sell WBTC on the other and then repay the Aave flash loan. These four transactions would be bundled together and processed as one, and each is contingent on the next.

A second example is loan liquidations. In DeFi protocols, loans are typically over-collateralized (except for flash loans, which have no credit risk) because the absence of borrower identities makes it impossible for lenders to seek recourse. Loans are commonly backed by cryptocurrency assets, with generous over-collateralization bounds. These bounds are pre-specified and take into consideration various factors such as the volatility of the underlying tokens. For instance, stablecoins typically have minimal over-collateralization bounds. Loans of the stablecoin DAI generated in the MakerDao protocol have over-collateralization bounds that vary with fees/interest rates and assets: for an interest rate (dubbed "stability fee") of 1.5%, the collateralization ratio for ETH is 145%, while for USDC it is 101% (data as of January 2023). When the collateral value drops below the prescribed bound, the loan becomes under-collateralized. To maintain the integrity of the system and the liquidity pool, it is critical that the collateral ratio is brought back above the collateralization bound. The standard process allows anyone to trigger a forced (partial) loan liquidation. The liquidator repays (a portion of) the loan to bring the remaining amount above the collateralization amount, and in return, receives a portion of the collateral at the market price minus a liquidation discount.

To take advantage of an under-collateralization opportunity, a liquidator would take up a flash loan for the repayment token, repay the under-collateralized loan, collect the collateral, trade this collateral in an automated market maker protocol for the borrowed coin, and then repay the flash loan. All of these transactions are bundled together and contingent upon one another.

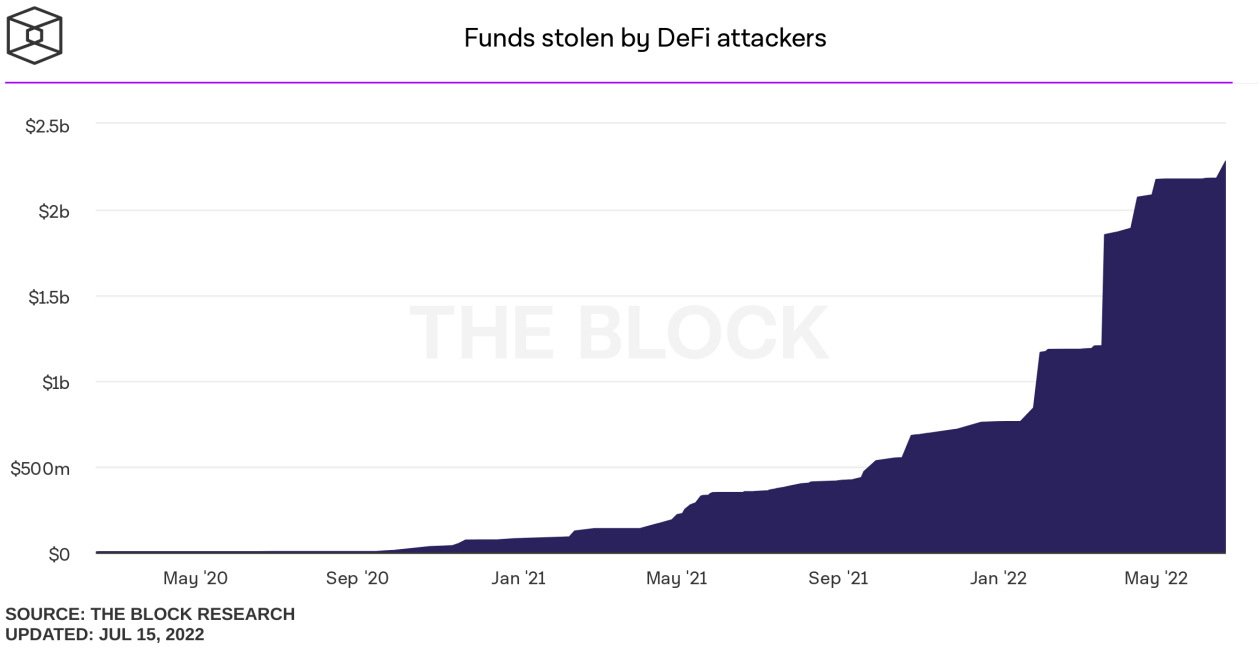
### 6.3 Tokenized Assets in DeFi

There are two key insights from the earlier discussion in this section that are relevant for asset tokenization: First, in traditional finance, an intermediary may use depositors' assets to earn extra income, for example, by lending shares to short sellers. In contrast, in DeFi, users have control over their assets. They can earn income as liquidity providers in trading or lending protocols.

Second, DeFi protocols are specialized and usually offer one type of service. For markets to work properly, users need to be able to combine transactions across various protocols. For example, when there is a price dislocation in one DeFi trading platform, the forces of arbitrage should ensure that prices re-align quickly. This realignment may involve the borrowing of assets, the trading of these assets on multiple platforms, and then the repayment of the loan. Each of these transactions occurs on a separate platform, and for greatest efficiency, a user would string together these trades.

**Figure 6: DeFi Exploits**

The figure displays the cumulative dollar-value of funds that were stolen from DeFi related protocols.




However, the interaction of various protocols creates risks. First, poorly coded or designed smart contracts may allow users to steal funds. Design flaws are often not obvious and may only surface when attackers find clever manipulations. For example, in the attack on Cream Finance, the attacker manipulated the market price of an illiquid asset that a smart contract used as an input, allowing the attacker to buy the asset at a dramatically reduced price. In the exploit of the Indexed Finance protocol, the attacker donated instead of sold one type of token into a contract, tricking the contract into believing that the value of its holdings was much lower than the market value and causing it to sell assets significantly underpriced. In the Beanstalk exploit, the attacker used a flash loan, a tool that borrows and repays a loan as part of the same (string of) transaction(s), to accumulate tokens and manipulate the protocol's governance process. Contrary to what some members of the blockchain community believe ("code is law" or "codeslaw"), crypto markets are subject to the law. For example, the attacker of the Mango protocol which yielded a profit of $114M, was recently charged with market manipulation by the CFTC.

Figure 6 displays the cumulative value of funds stolen from DeFi protocols between May 2020 and May 2022. Notably, most of the exploits are very large. The largest amount was the Ronin Network hack in March 2022, which resulted in $600 million being stolen; the network is a side-chain of Ethereum that was built to support the game Axie Infinity. The

second largest hack affected the Wormhole bridge from the Ethereum to the Solana blockchain, resulting in $323 million being stolen in February 2022. Beanstalk, Cream Finance, and Harmony saw losses of $181 million, $131 million, and $100 million, respectively. Notably, the Wormhole bridge is a tool that was developed by Jump Trading, one of the world's most sophisticated high-frequency trading firms.

In the future, we will likely see new types of attacks. For example, activist investors may borrow short-term to influence a firm's governance processes, influencing decisions without accountability. Investors may deposit assets in automated market-making platforms to earn fees, but shareholder votes or dividend payments may disrupt liquidity provision. In return for deposits, investors usually obtain receipt tokens, creating a new, specialized secondary market for the same underlying firm. Each innovation creates new uses and re-uses of capital and brings risks that the market has not yet seen.

## Section 7: Capital Raising

### 7.1 The Issuance-Trading Cycle

In the traditional world of finance, capital raising follows a standard process: a company enlists a broker-dealer's services, which then works to find investors for the issuing company. In a private placement, the broker-dealer helps prepare the offering documents (if applicable) and identifies suitable accredited investors, often with the help of investment advisors. In a public offering, the broker-dealer helps prepare the prospectus, performs due diligence, identifies a listing venue, and organizes a roadshow for the company to meet institutional investors. Whether the asset "lives" on traditional infrastructure or a blockchain has little impact on this process. However, ownership and the ability to transfer and use assets do.

As we outline in the previous sections, blockchain technology allows firms to issue tokens with various functions. Tokens can mimic traditional assets such as equity shares, bonds and commercial paper, preferred shares, or warrants. Tokens do, however, offer many additional novel features that are logistically challenging or not possible with traditional assets. For instance, tokenization can facilitate revenue-based royalties or claims tied to specific cash flows, separation of voting and dividends rights, or fractional ownership.

### 7.2 Public Offerings

A crucial component of the public offering is the sale process and determining the first listing price. A broker-dealer, or a syndicate, typically underwrites public offerings at a specific price and sells the shares in its initial public offering. Debt offerings, too, are commonly underwritten by a syndicate of financial institutions. The listing price can be an outcome of an auction process, but most commonly, it emerges from conversations between the underwriter and prospective investors.

A typical asset-linked tokenized offering would not involve the sale of new securities.

To issue a blockchain-native token, a company can follow a process similar to a traditional offering. However, the novel features of token trading enable alternative approaches. In the traditional financial system, a company must be listed on a stock exchange to be traded in public markets. In contrast, the blockchain world allows investors to hold tokens in self-custody and trade them peer-to-peer or through decentralized trading platforms. This eliminates the need for an exchange or broker-dealer's involvement in a token offering from an operational and functional perspective. An issuer can contact investors directly in a crowd sale or use the services of an online crowdfunding platform such as Coinlist or a crypto exchange for a so-called Initial Exchange Offering (IEO). Several major crypto exchanges have created crowdfunding platforms, such as Binance ("Launchpad"), Kukoin ("Spotlight") or Gate.io ("Startup"). According to cryptorank.io, there have been 454 such offerings since 2019, on average they raised $1 million ($144,000 median) per offering.

Finally, an issuer can also sell tokens directly through Initial DeFi Offerings (IDOs) by making them available in an automated market maker. According to cryptorank.io, there have been 1072 such offerings since 2021, with an average raise of $528K ($140K median) per offering. This approach eliminates the need for finding a distribution mechanism or setting up a separate website. Instead, the issuer creates a token pair, and investors can trade it using the established AMM mechanism. This is possible because anyone can "list" a token on an AMM simply by creating a liquidity pool for a toke.

The funds raised in these offerings are relatively small, so much so that most brokerages would likely not be willing to offer their services. To put this in perspective, over the same time period, 690 Special Acquisition Companies (SPACs) have been listed on U.S. markets, with an average market capitalization of $242 million. This highlights the stark contrast in the scale of these types of offerings.

Currently, capital raises using IEOs and IDOs are suitable for niche applications only. However, in the future, DeFi options for raising capital may change the competitive landscape for issuance services.

For now, investment dealers will likely continue to play a role for most firms as they have existing relationships with investors, providing a comparative advantage over new platforms. Dealer involvement may also provide additional safeguards for investors. Similarly, centralized exchanges have a role to play. Token holders value liquidity, and it may be beneficial for an issuer to list a token on a major centralized exchange. Due to their custody arrangements, it is possible that centralized exchanges will eventually subsume the roles of both stock exchanges and broker-dealers in the investment-issuance cycle, raising concerns about antitrust and monopoly.

**Regulatory Implications.** The recent European Union's Markets in Crypto-assets regulation MiCA mandates that issuers register a "whitepaper" that contains prescribed minimum

information (outlined under Article 5(1)) before issuing tokens. Our view is that MiCA's requirements fall short of what token-investors need to make informed decision and do not recognize the multi-function design possibilities of digital assets. MiCA's whitepaper requirements merely mimic those of traditional offering prospectuses, e.g., risk assessments, reasons for seeking public funding, etc. We believe that it is critical that whitepapers contain more specific information on the key economic and technological functions of the digital tokens. A few of the questions that a whitepaper should address are the following:

- Are there cash flow and voting rights?
- How are payments and voting organized?
- How will information be disseminated?
- What steps do investors have to take to receive information, dividends/coupons, and to vote?
- How and when are tokens distributed? Do they serve as an incentive?

### 7.3 Special Considerations for Private Markets with Accredited Investors

Investing in early-stage firms is often not suitable for the general public and only available to accredited investors. Although a blockchain token is available to anybody by default, it is possible to design a workaround that mimics the private markets.

Early-stage firms typically do not require immediate liquidity or other advantages of the public markets. If assets of such firms are issued on a blockchain, only a few investors will likely own these tokens, and transfers will be rare occurrences. Therefore, at an early stage, investors are unlikely to benefit from the novel opportunities offered by the blockchain technology, such as the DeFi infrastructure. Instead, blockchain will serve merely as a recording technology.

For this special case, it may be reasonable to restrict transfers to validated addresses. The starting point is establishing a whitelist of authenticated accredited investors' addresses. Then there are two options. The first is to hard-code into the token contract that transfers may occur only between whitelisted addresses. The concern is that the programming process may be complex and that there is an onus on the investor to ensure that their counterparty is on the list.

A second approach is restricting transfers between specific multi-signature wallets, where one signatory is a financial institution. In this case, an investor may initiate and cryptographically sign a transaction and send it to its broker-dealer for further processing. The broker-dealer will then be obliged to make the requisite check against the whitelist before adding their cryptographic signature. If, at genesis, all tokens are issued to such multi-sig wallets, then this process will restrict ownership to accredited investors.

# Section 8: Effects on the Industrial Organization and Regulatory Oversight of the Financial Services Industry

## 8.1 The Role of Traditional Financial Services

Capital markets and the investment process require many functions and services:

- Issuers and investors must be matched in the primary market.
- Investors require a secondary market with high integrity and ample liquidity.
- Market participants may need new securities and derivatives to implement investment and hedging strategies.
- Issuers and investors rely on third-party record keeping for transactions and ownership.
- Investors require investment advice and rely on third parties to perform due diligence on offerings.
- Market integrity is predicated on trading rules, acceptable trading conduct, and rules enforcement.
- Markets require an infrastructure, and investors need access to that infrastructure.

In traditional finance, intermediaries such as banks and broker-dealers (henceforth: FIs) play a central role. They provide investors with recording keeping, custody of assets, and access to the financial infrastructure.

An FI's key advantage is scale: a few intermediaries can service many investors. Because of their central position, issuers can employ intermediaries to find investors, provide information to investors, and disseminate funds. Moreover, regulators have a go-to entity to implement and enforce rules. For instance, broker-dealers are responsible for their clients' trading behavior, and they enforce risk controls.

Furthermore, secondary service providers such as marketplaces need only to connect with intermediaries to provide services to investors. In traditional finance, investors instruct their broker to buy or sell a security on their behalf, and the broker then chooses a trading venue. The trading venue merely processes information and, if a trade occurs, sends the result to the financial infrastructure to facilitate clearing and settlement. Panel A in Figure 7 illustrates this process.

The role of FIs as "gatekeepers" in financial markets is not without downsides. For instance, clients may find it difficult and costly to change service providers. Further, even though exchanges provide services for investors, their customers are the intermediaries. This business relationship may create conflicts of interest for intermediaries. Finally, intermediaries may derive income solely from their position and not only from the services they provide, or, in economic terms, they may also extract rents (which, by definition, is economically harmful).

### 8.2 Traditional Financial Services in a Blockchain Environment

A blockchain as a financial infrastructure changes the hierarchy of the investment process. The architecture of the traditional financial infrastructure is complex. Stock ownership is recorded in a central depository. Changes in ownership are initiated by intermediaries; therefore, the central depository records often contain ownership only at the intermediary level. The intermediaries keep records of ownership at the investor level. In essence, there are two ledgers, which are connected via intermediaries.

A blockchain effectively merges the two ledgers. It also permits third parties to deploy programs that run operations directly on this single ledger. Additionally, the recording-keeping is not centralized but distributed. A blockchain arrangement eliminates the structural need for intermediaries. Users can access the infrastructure and own a token in self-custody. They can also use blockchain deployed codes for trading.

In the most extreme scenario, intermediaries disappear, all secondary trading occurs peer-to-peer or by automated market makers, and primary markets rely on social media type matching. Although regulators may continue to be able to enforce rules on issuers, enforcing trading and risk regulations on individuals may prove technologically infeasible, particularly in a pseudo-anonymous environment. Enforcing the rules for decentralized, automated trading protocols will also likely be beyond the scope of regulatory agencies.

We do not believe, however, that this extreme scenario will emerge in practice.

For instance, although decentralized trading has seen significant uptake for crypto-assets, centralized venues continue to play a major role in the trading of crypto assets, and many users keep their assets on these systems. Even if investors can choose self-custody and direct control over their assets, many will likely continue to seek expert advice and support for their financial market activities.

Against this backdrop, we believe that broker-dealers will play an important role. Blockchain users need on and off ramps to exchange their fiat money (which they receive in bank accounts) for digital assets.[16] In the current crypto-asset space, centralized crypto-exchanges perform this function. However, with the creation of tokenized digital assets, existing financial institutions will be much more natural, better-suited providers for this service.

Furthermore, existing FIs may be well-suited to keep their clients' funds safe in a cyber-security sense. They could offer custody services and custody wallets for their clients. FIs can continue to apply appropriate risk controls to limit investors' exposure to investment

[16] This assessment may need to be revisited if genuine digital government money is available on public blockchains and if people and businesses accept payments and salaries transfers in this digital money.

losses. Additionally, they may be able to detect malicious applications and prevent their clients from inadvertently transferring assets to such applications.

Therefore, we believe that individual investors will continue to seek the support of financial institutions for their investment and trading activities and that financial institutions will continue to play an important role in the investment process.

### 8.3 Stock Exchanges and ATSs in the New Infrastructure

Crypto exchanges maintain user accounts and process trades. They therefore amalgamate the roles of broker-dealers and exchanges. Settlement is the investor's choice and requires them to transfer assets to a self-custody wallet.

On the other hand, traditional stock exchanges and alternative trading systems are primarily information processors, and their current infrastructure is not suitable for trading blockchain-based assets. Figure 7 illustrates the differences in the processes. To accommodate the trading of crypto tokens, existing exchanges and ATSs would have to operate similarly to centralized crypto trading venues and become completely different institutions. This would fundamentally change their business model and clientele: currently, their clients are broker-dealers and select trading firms, but as centralized crypto exchanges, they would provide services to the general public and would need to become broker-dealers themselves.

In addition to processing and overseeing trading, stock exchanges have a quasi-regulatory role in managing public listings. They serve the investment community by ensuring that listed firms provide information in an orderly fashion and that they abide by specific standards. This validation role will continue to be important in the world of tokenized assets. For instance, blockchain projects often seek listings on centralized crypto exchanges, indicating that listing decisions still hold significance in the blockchain ecosystem, even though fully decentralized markets exist.[17]

### 8.4 Trading Regulations in Traditional vs. Blockchain Finance

Traditionally, investors can access the market only through a broker-dealer, and this broker-dealer may face conflicts of interest. A strict set of rules is, therefore, necessary to ensure that broker-dealers act in the best interest of their clients. Implementations differ among jurisdictions. In Europe, brokers must provide best execution in the sense that they seek the best trading conditions for their clients. In North America, the same rule applies,

[17] Even tokens for which there is no intended investment value need to be available for users to buy (e.g., so users can apply a token in a game). A listing on a centralized crypto-exchange allows these projects to establish a marketplace for their token.

and in addition, brokers and trading venues must obey order protection rules and route orders to the venue with the best-priced visible price.

The organization of trading in a blockchain environment is different, and the differences are key for regulation. First, investors have more control over when and where their orders trade: they can choose between peer-to-peer, various DeFi applications, and centralized exchanges. Second, technologically, trading on traditional venues involves only sending messages. In the blockchain world, using a (centralized) trading system requires the transfer of assets, which is costly and time-consuming.

The first point is important for best execution regulations. In a blockchain world, investors can choose to be in control and avoid the costs that stem from potential conflicts of interest. Brokers who want to manage accounts for investors will compete and have an incentive to provide and advertise their best execution practice.

Order protection rules are more complex conceptually and technologically. The idea behind these rules is twofold. First, the rule ensures that those who post orders publicly get their orders filled first. Second, it effectively ensures that a national market is integrated because brokers need to monitor and access all markets (that display quotes). In a blockchain environment, order protection would need to be imposed on those with custody of the assets. It is hard to imagine that it can be enforced for individuals who hold assets in self-custody. It is also not evident that crypto exchanges can be required to forward orders to another venue because it would involve high costs and a transfer of custody.

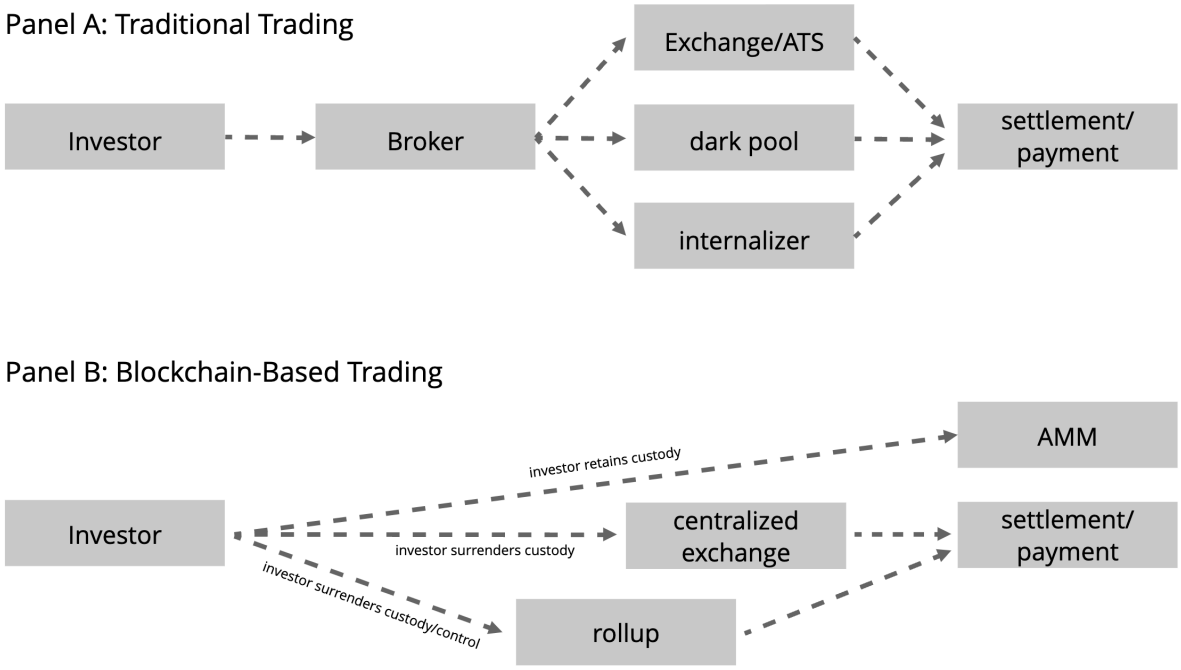
A further concern, particularly in Europe, is dark trading and the services of internalizers. The question that arises is whether brokers keep trades, especially retail trades, away from the public market to the detriment of the investor and the market as a whole. For instance, Comerton-Forde, Malinova and Park (2018) discuss the problems that arise when withholding retail order flow from public markets in Canada; Ernst and Spatt (2022) highlight the conflicts of interest that arise due to payment for order flow arrangements in US markets. Dark trading and internalization can be facilitated in a blockchain world, but the investor would have control over the choice of a trading arrangement. Moreover, the operation of a blockchain-based venue requires that users deposit funds into the system, and these deposits are visible. In other words, market participants can glean insights into trading interests from the blockchain itself. Firms that organize dark pools as centralized venues can be compelled to limit trading or deposits. However, dark pools can also be organized in decentralized rollups, and rollup initiation and activities cannot be restricted easily.

Crucially, when investors control their asset fully, they achieve exactly the routing outcome that they want. Therefore, the role of regulators in this environment requires rethinking.

**Figure 7: Order Submission, Trading, and Settlement**

**Panel A** illustrates the trading and settlement process in traditional finance: investors instruct their broker to buy or sell a security on their behalf, and the broker then chooses a trading venue such as an exchange, alternative trading system, a dark pool, or an internalizer. The trading venue merely processes information and, if a trade occurs, sends the result to the clearing and settlement system.

**Panel B** illustrates the process for blockchain based trading. The investor can choose to trade with a centralized exchange in which case they need to transfer their assets from their self-custody wallets to the exchange, which takes custody. After the trade, the investor can choose to transfer assets back to their self-custody wallet if they want full control. They can also use an on-chain AMM which facilitates an atomic swap to and from the self-custody wallet. Finally, they can use a trading system in a rollup in which case they deposit in the rollup and later withdraw.



## References


Bakos, Yannis, and Hanna Halaburda, 2019, The role of cryptographic tokens and ICOs in fostering platform adoption, Working paper New York University https://ssrn.com/abstract=3207777.

Canidio, Andrea, 2018, Financial incentives for open source development: the case of blockchain, Working paper IMT Lucca, INSEAD.

Capponi, Agostino and Jia, Ruizhe and Wang, Ye, The Evolution of Blockchain: From Public to Private Mempools (2022). SSRN: https://ssrn.com/abstract=3997796

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 https://ssrn.com/abstract=3137213.

Chod, Jiri, and Evgeny Lyandres, 2021, A theory of ICOs: Diversification, agency, and information asymmetry, Management Science Forthcoming.

Chod, Jiri, Nikolaos Trichakis, and S Alex Yang, 2019, Platform tokenization: Financing, governance, and moral hazard., Discussion paper, Boston College https://ssrn.com/abstract=3459794.

Comerton-Forde, Carole, Katya Malinova, and Andreas Park, 2018 Regulating dark trading: Order flow segmentation and market quality, Journal of Financial Economics, Volume 130, Issue 2, November 2018, Pages 347-366

Cong, Lin William, Ye Li, and Neng Wang, 2021a, Token-based platform finance, Journal of Financial Economics Forthcoming.

Cong, Lin William, Ye Li, and Neng Wang, 2021b, Tokenomics: Dynamic adoption and valuation, The Review of Financial Studies 34, 1105–1155.

Cong, Lin and Li, Xi and Tang, Ke and Yang, Yang, Crypto Wash Trading (July 2021). SSRN: https://ssrn.com/abstract=3530220

Cong, Lin and Landsman, Wayne R. and Maydew, Edward L. and Rabetti, Daniel, Tax-Loss Harvesting with Cryptocurrencies. SSRN: https://ssrn.com/abstract=4033617

Davydiuk, Tetiana, Deeksha Gupta, and Samuel Rosen, 2021, De-crypto-ing signals in initial coin offerings: Evidence of rational token retention, Discussion paper, Carnigie Mellon University https://ssrn.com/abstract=3286835.

Ernst, Thomas and Spatt, Chester, 2022, Payment for Order Flow and Asset Choice, NBER Working paper 29883

Gan, Rowena, Gerry Tsoukalas, and Serguei Netessine, 2021a, Initial coin offerings, speculation, and asset tokenization, Management Science 67, 914–931.

Gan, Rowena, Gerry Tsoukalas, and Serguei Netessine, 2021b, To infinity and beyond: Financing platforms with uncapped crypto tokens, Discussion paper, Boston University.

Garratt, Rodney, Michael Junho Lee, Antoine Martin, and Robert M Townsend, "Who sees the trades? The effect of information on liquidity in inter-dealer markets," The Effect of Information on Liquidity in Inter-Dealer Markets (July 2019). FRB of New York Staff Report, 2019, (892).

Griffin, John M. and Shams, Amin, Is Bitcoin Really Un-Tethered? (October 28, 2019). SSRN: https://ssrn.com/abstract=3195066

Khapko, Mariana and Marius Zoican, "How fast should trades settle?," Management Science, 2020.

Koeppl, Thorsten, Cyril Monnet, and Ted Temzelides, "Optimal clearing arrangements for financial trades," Journal of Financial Economics, 2012, 103 (1), 189–203.

Lee, Mina, and Christine Parlour, 2021, Consumers as financiers: Consumer surplus, crowdfunding, and initial coin offerings, The Review of Financial Studies 2022

Li, Jiasun, 2020, Profit sharing: A contracting solution to harness the wisdom of the crowd, Working paper George Mason University https://ssrn.com/abstract=2844335.

Li, Jiasun andWilliam Mann, 2018, Digital tokens and platform building, Working paper George Mason University https://ssrn.com/abstract=3088726.

Evgeny Lyandres, Berardino Palazzo, Daniel Rabetti (2022) Initial Coin Offering (ICO) Success and Post-ICO Performance. Management Science 68(12):8658-8679. https://doi.org/10.1287/mnsc.2022.4312

Martin, Antoine and James McAndrews, "Liquidity-saving mechanisms," Journal of Monetary Economics, 2008, 55 (3), 554–567.

Michael Junho Lee, Antoine Martin, and Robert M. Townsend, "Optimal Design of Tokenized Markets," working paper 2022.

Malinova, Katya and Andreas Park, "Market Design with Blockchain Technology", working paper, 2016.

Malinova, Katya and Andreas Park, "Tokenomics: When Tokens Beat Equity", working paper, 2020.

S. Kobayakawa and H. Nakamura, "A Theoretical Analysis of Narrow Banking Proposals," Monetary and Economic Studies, vol. 18, pp. 105–118, May 2000.

Lehar, Alfred and Parlour, Christine, Systemic Fragility in Decentralized Markets (January 1, 2022), working paper

Lehar, Alfred and Parlour, Christine A., Decentralized Exchanges (August 14, 2021). SSRN: https://ssrn.com/abstract=3905316

Li, Tao and Shin, Donghwa and Wang, Baolian, Cryptocurrency Pump-and-Dump Schemes (February 10, 2021). SSRN: https://ssrn.com/abstract=3267041

R. Litan, "What should banks do?," tech. rep., Brookings Institution, 1987.

Park, Andreas, A 2022 Primer for Crypto-Trading (2022b). Available at SSRN: https://ssrn.com/abstract=4148717 or http://dx.doi.org/10.2139/ssrn.4148717

Park, Andreas, The Conceptual Flaws of Decentralized Automated Market Making (2022b). SSRN: https://ssrn.com/abstract=3805750

J. Pierce, The Future of Banking. Yale University Press, 1991.

Prat, Julien, Vincent Danos, and Stefania Marcassa, 2021, Fundamental pricing of utility tokens, Working paper. CREST, Ecole Polytechnique.

Ioanid Roşu, Fahad Saleh (2020) Evolution of Shares in a Proof-of-Stake Cryptocurrency. Management Science 67(2):661-672. https://doi.org/10.1287/mnsc.2020.3791

Shakhnov, Kirill, and Luana Zaccaria, 2021, (R)Evolution in entrepreneurial finance? The relationship between cryptocurrency and venture capital markets, Discussion paper, University of Surrey https://ssrn.com/abstract=3613261.

Sockin, Michael, and Wei Xiong, 2018, A model of cryptocurrencies, Working paper Princeton University A Model of Cryptocurrencies.

## About the authors

**Katya Malinova** is an Associate Professor and holds the Mackenzie Investments Chair in Evidence-Based Investment Management at the DeGroote School of Business, McMaster University. Prior to joining DeGroote in July 2018, Katya was an Associate Professor at the University of Toronto. Katya's research focuses on financial market structure, including the impacts of maker-taker pricing, dark trading, high frequency trading (HFT), and new technologies such as blockchain technology. She has received major research grants from the Social Sciences and Humanities Research Council of Canada, she has collaborated with IIROC on research studies. Katya currently also serves on the Ontario Security Commission's Market Structure Advisory Committee. Her research has been published in, for instance, the *Journal of Finance*, the *Journal of Financial Economics*, and the *Journal of Financial and Quantitative Analysis*. She is currently an Editor of the Journal of Financial Technology and an Associate Editor of the Journal of Financial Markets. She teaches courses in corporate finance and FinTech.

**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, and he currently holds the Canadian Securities Institute's Research Foundation Limited-Term Chair. He currently serves as the Research Director at the FinHub, Rotman's Financial Innovation Lab, he is the co-founder of the LedgerHub, the University of Toronto's blockchain research lab. He has served as a lab economist for the Blockchain stream at the Creative Destruction Lab (a world-leading start-up accelerator program), an economic advisor to Conflux Network (a third generation blockchain network), and as a consultant to the Ontario Securities Commission (OSC) and the Investment Industry's Regulatory Organization of Canada (IIROC). Andreas teaches undergraduate, graduate, and executive courses on payments innovation, 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.