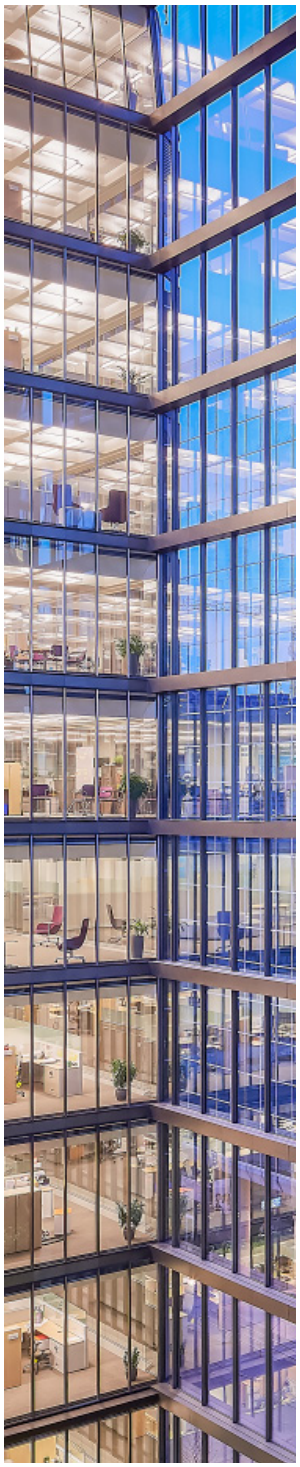
BANK OF CANADA
BANQUE DU CANADA

OSC ONTARIO SECURITIES COMMISSION

Staff Discussion Paper/Document d'analyse du personnel—2024-12

Last updated: July 11, 2024



The Ecology of Automated Market Makers

by Annetta Ho,[1] Cosmin Cazan[2] and Andrew Schrumm[2]

[1] Supervision Department, Bank of Canada
annettaho@bankofcanada.ca
[2] Ontario Securities Commission
ccazan@osc.gov.on.ca, aschrumm@osc.gov.on.ca

DOI: https://doi.org/10.34989/sdp-2024-12 | **ISSN** 1914-0568

Acknowledgements

Collaboration between the authors was made possible through a secondment arrangement between the Bank of Canada and the Ontario Securities Commission. We are grateful to the comments of many reviewers in shaping this paper and to the data vendors that provided insightful analysis. In particular, we wish to thank Melanie Achtemichuk, Paul Redman and Kevin Fine for their guidance and support.

This paper is intended for information purposes only. It does not include nor represent any formal legal analysis or opinion. Various commonly used terms are employed but interpretation of their potential legal definition is not the subject of this paper. We make no independent claim on the accuracy of the findings included from data providers and other external sources.

Abstract

This paper describes the ecology of automated market makers (AMMs), which are the most popular decentralized exchange model for the pricing and trading of crypto assets within decentralized finance. We use blockchain data to identify trends in user adoption and trading volumes of AMMs. Given the range of AMMs available and the diversity of their designs, we perform case studies on four platforms—Uniswap, Curve, Sushiswap and Balancer—to represent the AMM market. We describe the designs of these four AMMs in terms of their products or services, governance, incentives for participation and risks. Finally, we describe the characteristics of AMMs that require considerations with respect to the application of a regulatory framework to AMMs. Findings are presented for information and do not represent any formal legal analysis or opinion.

Topics: Digital currencies and fintech; Financial markets; Financial stability; Financial system regulation and policies
JEL codes: G, G1, G2

Résumé

Ce document décrit l'écosystème de la tenue de marché automatisée, qui est le modèle de plateforme d'échange le plus utilisé pour évaluer et négocier les cryptoactifs dans le secteur de la finance décentralisée. Nous utilisons des données sur les chaînes de blocs afin de cerner les tendances relativement à l'adoption de la tenue de marché automatisée et aux volumes de négociation sur ces plateformes. Étant donné l'éventail de protocoles de ce type offerts et la diversité de leur conception, nous avons effectué des études de cas sur quatre d'entre eux – Uniswap, Curve, SushiSwap et Balancer – que nous avons choisis pour représenter le marché. Nous décrivons la conception de ces quatre protocoles selon certaines caractéristiques : produits ou services, gouvernance, incitatifs à participer et risques. Enfin, nous définissons les propriétés des plateformes de tenue de marché automatisée qui doivent être prises en compte pour l'application d'un cadre réglementaire à cet écosystème. Les résultats sont présentés à titre d'information et ne constituent aucunement une analyse ou un avis de nature juridique.

Sujets : Monnaies numériques et technologies financières; Marchés financiers; Stabilité financière; Réglementation et politiques relatives au système financier
Codes JEL : G, G1, G2

Summary

This paper describes the ecology of automated market makers (AMMs), which are the most popular model of decentralized exchange (DEX) platform for the pricing and trading of crypto assets within decentralized finance (DeFi).[1] AMMs operate as unregistered entities and pose potential risks to investors, market integrity and financial stability. They may present regulatory arbitrage for crypto trading activity as regulators increasingly require centrally managed crypto trading venues, known as centralized exchanges, to register and comply with securities laws. This work includes efforts by the Canadian Securities Administrators (CSA) to have entities known as crypto asset trading platforms (CTPs) to register with the relevant provincial securities commission.[2]

Our paper intends to further understanding among policy-makers and regulators of the functions, operations and organization of AMMs. We collect blockchain data to identify trends in user adoption and trading volumes of AMMs. This work aligns with recommendations from the International Organization of Securities Commissions (IOSCO 2023) that securities market regulators analyze DeFi arrangements to assess any potential regulatory responses. Given the range of AMMs available and the diversity of AMM designs, we perform case studies on four platforms—Uniswap, Curve, Sushiswap and Balancer—to better understand their designs in terms of their products or services, governance, incentives for participation and risks. We conclude by identifying characteristics of AMMs that require consideration with respect to applying a regulatory framework, but this does not represent a formal legal analysis or opinion.

Our key findings are:

- **An AMM is a venue for primary and secondary trading of crypto assets, as well as custody and investment services to liquidity providers and liquidity and settlement to traders.** Any blockchain user can deploy the AMM code or protocol at a blockchain address to establish a pool. The user then determines what crypto assets can be traded in the pool, including tokens they created (for primary issuance or secondary trading) or pre-existing ones (for secondary trading). The pool relies on external liquidity providers to continuously add and remove crypto assets. In turn, the AMM locks these crypto assets and issues a token to the liquidity provider that entitles them to earn trading fees. Traders then swap their crypto assets with the pool, taking the AMM's quoted price as given, and pay a fee for each trade.
- **Crypto market participants continued to use large AMMs despite the broader crypto crash in 2022.** Data collected from the four AMMs—Uniswap, Curve, Sushiswap and Balancer—show that their activity levels in terms of volumes, values and number of participants in the first quarter of 2023 were about one-third of the peaks recorded in the fourth quarter of 2021, but still higher

[1] In the context of securities regulation, use of the term "exchange" is regulated and is permitted only when registered entities meet specific standards. DEXs operate as unregistered entities and accordingly may misuse the term exchange, potentially in breach of securities laws in Canada. For the purposes of this paper, we will employ the term DEXs in its commonly accepted usage.

[2] A list of CTPs that have registered or have provided a pre-registration undertaking is available on the Ontario Securities Commission's website.

than in the early years of DeFi. Uniswap and Curve have emerged as the leading AMMs. This may be due to Uniswap's first-mover advantage and Curve's focus on crypto assets known as stablecoins.[3] Our findings support data collected by others that show the usage of DEXs is stable or increasing compared with centralized exchanges (CEXs). For example, results from a recent Ontario Securities Commission (OSC 2023) survey show that 19% of Canadian crypto users interacted with a DEX to trade or hedge crypto, up from 16% in 2022.

- **Governance token holders can significantly influence the operating decisions of an AMM and may be connected to CTPs.** Governance token holders can vote on proposals about the platform's strategy and operations. A small number of blockchain addresses may wield significant influence by holding enough governance tokens to meet an AMM's thresholds for quorum and passing decisions. Examples of these address holders in our case studies included institutional firms and centralized crypto trading platforms or related parties. However, fully attributing governance token holders to specific identities is difficult because addresses are pseudo-anonymous.
- **AMMs create risks for investors, market integrity and financial stability through unique and complex channels.** Liquidity providers need to be aware that while they can receive stable trading fees, they are also exposed to losses from changes in the relative prices of the crypto assets they contribute. Traders need to be aware of sudden price changes, market manipulation and fraudulent pools. The risk of market manipulation is heightened on AMMs due to information leakage on public blockchains, the ability for anyone to issue new tokens on AMMs and the anonymity of users. The extent to which financial and operational vulnerabilities on AMMs can impact the real economy depend on the extent to which crypto assets and players on the platform are interconnected with the traditional financial system. We highlight that illiquidity and mispricing of, or runs on, fiat-backed stablecoins on AMMs is a potential channel for contagion that deserves more study.
- **Policy-makers and regulators may need to assess how existing regulatory frameworks would apply to AMMs.** Our paper does not assess whether securities laws or other regulatory frameworks apply to AMMs, but rather highlights activities provided by AMMs that are similar to those provided by regulated entities.[4] Our analysis of AMMs demonstrates the scale and nature of their interactions with crypto assets that may be considered securities or derivatives. Regulators will need to address data gaps while determining appropriate metrics to monitor the risks AMMs present to investors, market integrity and financial stability.

[3] Stablecoins are a type of crypto asset that attempt to reduce volatility by pegging its value to another asset, including USDC and Tether. In Canada, securities regulators have defined stablecoins as value-referenced crypto assets (VRCAs) because it is a type of "crypto asset that is designed to maintain stable value over time by referencing the value of a fiat currency or any other value or right, or combination thereof" (CSA 2023b). For the purposes of this paper, we will employ the term stablecoin in its commonly accepted usage.

[4] CTPs are generally required to be registered in Canada. Unregistered CTPs that continue to operate in Canada while pursuing applications for registration and related relief and satisfy eligibility criteria are expected to provide a pre-registration undertaking (PRU). A PRU commits an unregistered CTP to operate in a certain manner during the registration process (CSA 2023a).

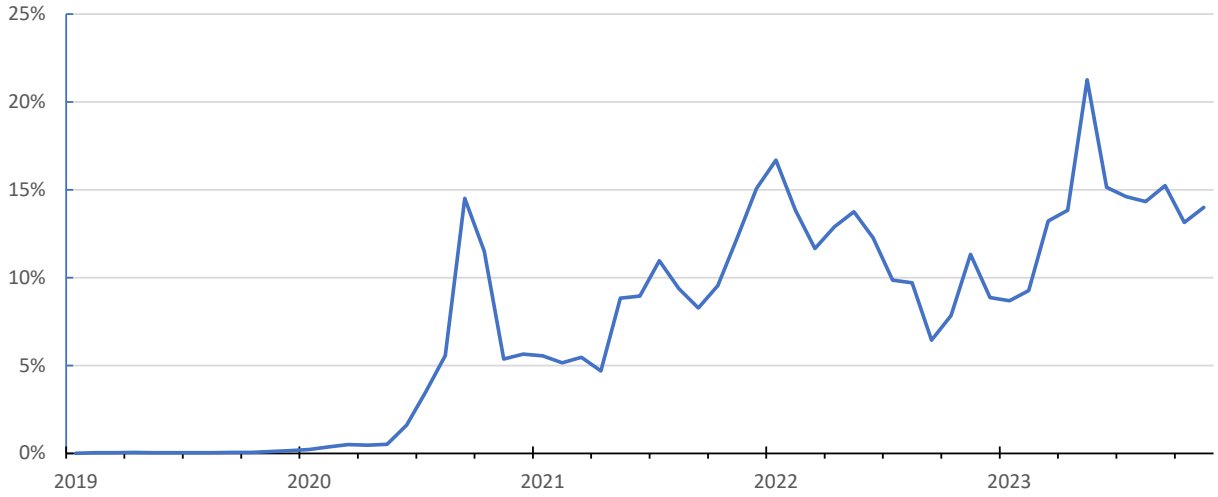
1. Introduction

DEXs facilitate the exchange of crypto assets through pieces of self-executing code on a blockchain known as smart contracts. These DeFi platforms are a way for users to trade without intermediaries. While trades are executed on a blockchain, the governance or decision-making around the design and operations of a DEX may be partially off-chain. Historically, the only way to trade crypto assets was on a bilateral basis with another user, so CEXs were developed to match orders and traders. These platforms effectively take control and custody of a user's crypto assets and set requirements and restrictions on trading activity, such as identification requirements and trading limits. CEXs include platforms like Mt. Gox and Quadriga, which respectively lost and stole their customers' crypto assets. Events like those accelerated the clarification of how existing regulations applied to CTPs, including the framework instituted by the CSA. However, DEXs have not yet sought registration in Canada or other jurisdictions.[5]

While CEXs remain much more popular than DEXs among users, participants also appear to be increasing their use of DEXs. Data collected by The Block show spot trading volumes on DEXs have been volatile but have hovered between 10% and 20% of CEX volume over 2022–23 (**Chart 1**). These global figures appear to mirror Canadian adoption: results from an OSC survey found that 20% of Canadian crypto users traded or hedged assets on a DEX in 2023, up from 16% in 2022 (OSC 2023). DEXs also appear to be quite important within the DeFi ecosystem, representing almost US$80 billion, or 42%, of total value locked in DeFi contracts at its peak in December 2021 (**Chart 2**).

5 Limited regulatory responses, as at March 2023, include minor rules introduced by the United Arab Emirates and limited enforcement action in the United States. For more, see D. Garcia Ocampo, N. Branzoli and L. Cusmano, "Crypto, Tokens and DeFi: Navigating the Regulatory Landscape," Bank for International Settlements *FSI Insights* (May 2023).

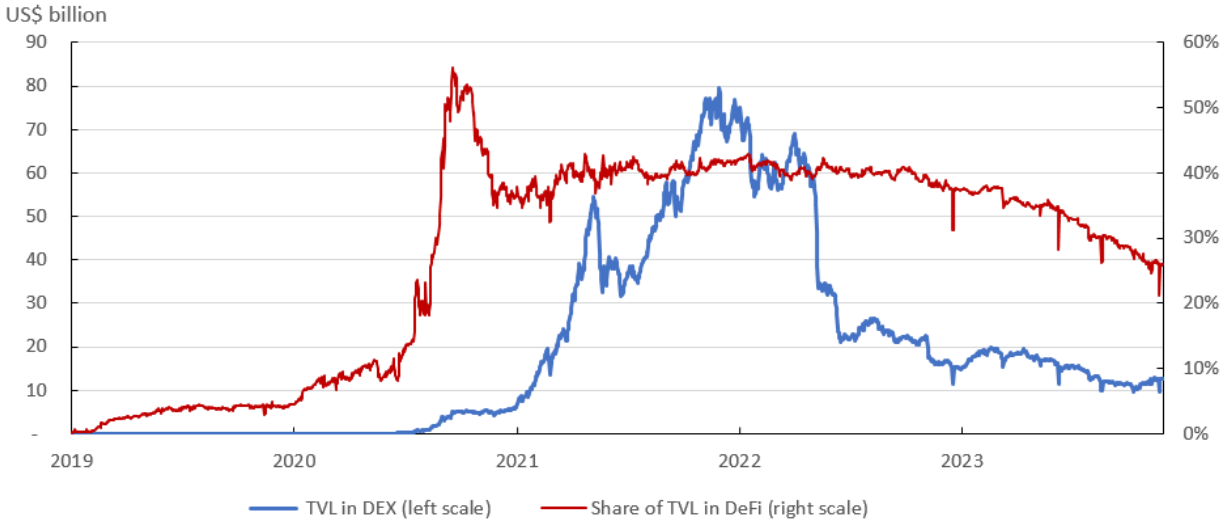
Chart 1: Spot trading volumes on decentralized exchanges as a share of centralized exchanges



Note: Percentages are calculated by dividing monthly decentralized exchange volumes by monthly centralized exchange volumes. Figures include the largest exchanges with trustworthy reporting of exchange volume metrics. All volume is filtered for flash trades, in which when a trader takes out a large loan to execute a high-volume trade and then quickly pays it back.

Sources: The Block, The Graph and Coingecko Last observation: November 2023

Chart 2: Total value locked in DeFi



Note: *TVL* is total value locked. *DEX* is decentralized exchanges protocols and *DeFi* is decentralized finance protocols. Data prior to January 4, 2019, are not plotted because of an unexplained structural break on that date.

Source: DeFiLlama Last observation: November 30, 2023

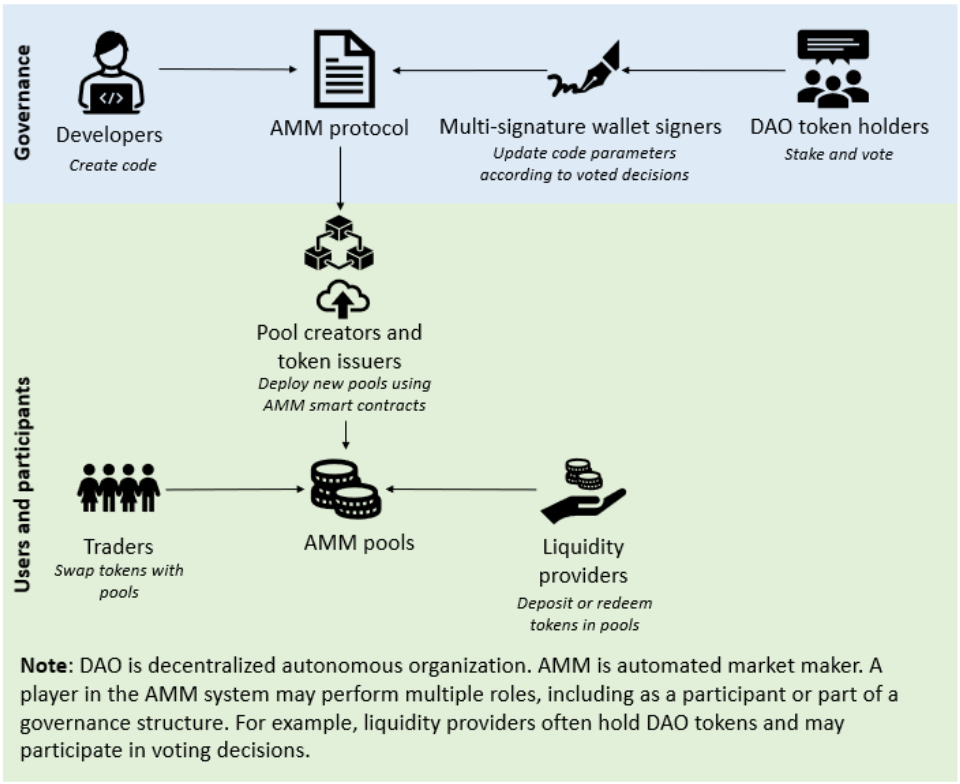
The dominant DEXs use smart contracts known as AMMs, which account for over 80% of total DEX volumes since February 2021. AMMs were intended to be DEXs with lower blockchain fees than DEXs with order book systems. Vitalik Buterin, the co-founder of Ethereum, first described the concept of an AMM in

a 2016 post on Reddit. Two years later, Hayden Adams implemented the first AMM in the form of Uniswap (Foxley 2020). We define an AMM as:

> A smart contract deployed at one or more blockchain addresses, each known as a pool, that uses a non-discretionary algorithm to set quotes for the purchase or sale of crypto assets within a two-sided platform of liquidity providers and traders.

The specific mechanics of AMMs distinguish them from any other platform for the trading of crypto assets. Developers, or blockchain users, deploy the AMM code or protocol at a blockchain address to establish a pool. They determine the crypto assets that can be traded in the pool, including newly created tokens (for primary issuance or secondary trading) or pre-existing tokens (for secondary trading). A nominal amount of crypto assets may initially be included in the pool. However, the pool relies on external liquidity providers (LPs) to continuously add and remove crypto assets. Traders then swap their crypto assets with the pool, taking the quoted price as given. LPs and traders may be retail investors, institutional firms or even protocols. In terms of governance, a community of market participants, an internal team of developers or both may control a DEX. **Figure 1** summarizes the various players and the roles that each can play in the AMM ecosystem.

Figure 1: Overview of automated market maker ecosystem



Note: DAO is decentralized autonomous organization. AMM is automated market maker. A player in the AMM system may perform multiple roles, including as a participant or part of a governance structure. For example, liquidity providers often hold DAO tokens and may participate in voting decisions.

This paper is divided as follows. Section 2 describes the methodology and data used for our research. Section 3 provides further details on the mechanics of AMMs. Section 4 covers adoption trends that motivate our work, with data on Canadian activity where possible. Section 5 and section 6 look at the

economic incentives and risks of participating in AMM governance arrangements and the platform itself. Section 7 and section 8 conclude with an analysis of AMM characteristics with respect to risks and applying a regulatory framework.

2. Methodology

2.1 Case study approach

Given the range of AMMs available and the diversity of AMM designs, we perform case studies on four platforms to represent the AMM market. We chose to study successful designs that are more likely to persist in the future and to understand a range of designs with different business models or features. The criteria we used to assess viability were:

- **Size**: The AMM must be relatively well adopted compared with its peers as measured by total value locked (TVL), which is the sum of all value in the AMM's pools. We did not consider AMMs with a TVL of less than US$100 million.
- **History**: The AMM must have existed for at least two years and have exhibited a level of operational stability.
- **Uniqueness**: The AMM must have a unique business model or unique features that helps us build a diverse sample of the AMM market. Specifically, it needed to have different types of crypto assets being traded or pool designs, or additional ancillary products or services.

Due to computational and data constraints (see section 2.2 for details), the evaluated AMMs also needed to have met the size and history criteria based on their presence on the Ethereum blockchain. Using these criteria, we selected four DEXs: Uniswap, Curve, Balancer and Sushiswap, and all their respective versions.[6] Other popular DEXs like PancakeSwap, Dodo and Trader Joe did not have sufficient size or history on Ethereum to be selected. We also excluded platforms where AMMs are not the core business. Future work on these applications may lead to other insights. **Table 1** summarizes an assessment of these platforms against our criteria.

[6] DEX developers, like other software developers, may create new versions of their protocol that ideally improve upon the previous version. The design changes between versions can be substantial.

Table 1: Case studies

Protocol (developer)	TVL (US$ billion)*		Created (no. of version)	Key features
	2021	2022		
Uniswap	8.2	3.1	Nov. 2, 2018 (3)	Basic, no frills: • First AMM launched • Pools consist of up to two crypto assets
Curve	20.3	3.3	Sept. 6, 2020 (1)	Stablecoin-focused: • Pools consist of stablecoins or similar assets (e.g., bitcoin and wrapped bitcoin) • Some pools automatically invest assets in external lending protocols (e.g., Compound) to generate higher returns for liquidity providers
Balancer	3.0	1.4	July 1, 2020 (2)	Multi-asset investing or diversification: • DEX platform where the number of assets in a pool can be very high (up to 50), exposing liquidity providers to a broader set of crypto assets • Operates a centralized exchange service that custodies traders' assets, known as The Vault, and matches trades off-chain to minimize gas fees under the Coincident of Wants Protocol
Sushiswap	3.1	0.3	Aug. 28, 2020 (1)	Full-service borrowing and lending: • Operates a borrowing and lending business called Kashi and offers yield instruments called BentoBox and Onsen Farms to users. Deposits in BentoBox can be pledged or used for multiple purposes simultaneously.

*Dollar figures are sums of all versions created on the Ethereum protocol and are as at December 31 of the respective years.
Source: DefiLlama

2.2 Data and information collection

We draw from multiple data sources. Information on the design and mechanics of each AMM case study were obtained directly from the AMM's websites, whitepapers and developer documents, unless otherwise noted.

In addition, we assess adoption trends by using raw blockchain data extracted and compiled by Inca Digital. To manage computational effort, we asked Inca to collect transaction data from the Ethereum blockchain only because it continues to be the leading blockchain for DeFi. Other blockchains have deployed the AMMs we consider, but the majority of their individual value is locked on Ethereum. The bulk of the raw data was collected between January 1, 2020, and June 30, 2022. This period covers the dramatic rise in crypto adoption and the initial phases of the crypto crisis that continued into 2023. In some cases, more recent data were collected for analysis. These data largely reinforce the downward trends in activity in 2022 and show even larger declines from the peak of activity.

Inca collected approximately 200 gigabytes of data that cover a wide range of adoption measures. Regarding market participation, the data include values and volumes of liquidity actions (add or remove) and trades (swaps), as well as the number of unique addresses interacting with the AMM protocols as LPs and traders. The top traders and LPs on each AMM are broken down by quarter. Regarding governance participation, Inca identified the top addresses holding AMM governance tokens at various points in time. Inca also collected data on web traffic data for each AMM platform website and application URLs to understand the possible geographic locations of users.

Unless otherwise indicated, values are presented in US dollars. Inca converted the values of every crypto asset into US dollars using daily prices available on various AMM pools that had a reference to a stablecoin (e.g., USDT or USDC) or to an asset traded on other centralized trading platforms (e.g., ETH) for which price information was readily available. For certain tokens, pricing in US dollars could not be collected or calculated because they were traded very thinly. We determined that the volume of these tokens is not material and would not significantly change the results presented in this paper.

Data and information about crypto market manipulation came from Solidus Labs, a global company that provides crypto market integrity solutions, including trade surveillance, transaction monitoring and threat intelligence.[7]

To calculate specific measures and metrics, we used data aggregation websites such as coinmarketcap.com for the market capitalization of governance tokens, defillama.com for total value locked in DeFi contracts and dune.com for impermanent loss. We also used commercially available crypto-asset tracing tools to determine if top traders and LPs could be identified or attributed to known individuals and firms.

3. How automated market makers work

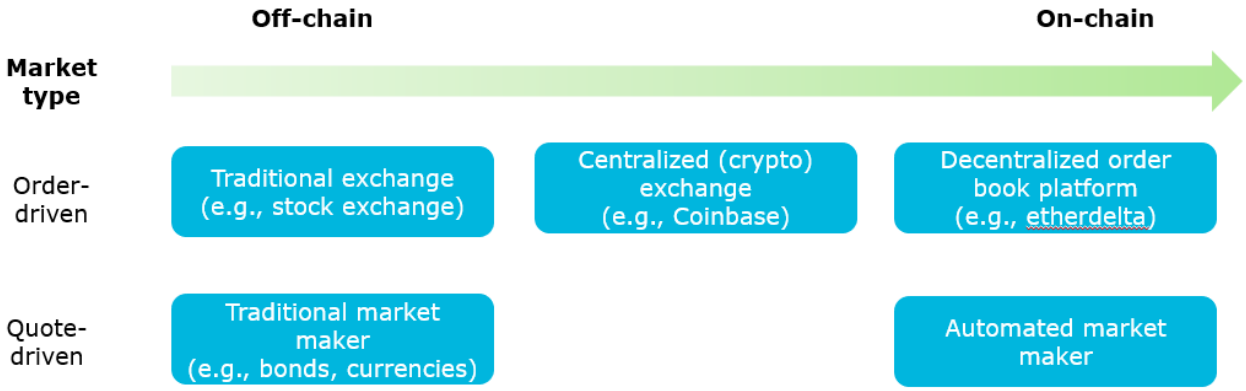
This section begins by comparing AMMs with traditional and other venues used for trading crypto assets. Different types of trading venues arise because the properties of an asset or the structure of the market for that asset make one venue more suitable than another for promoting efficient pricing and liquidity. Trading venues for traditional and crypto assets can be broadly divided into those that are:

- order-driven or quote-driven
- off-chain (settled on a central ledger) or on-chain (settled on a blockchain)

Figure 2 depicts examples of the various types of trading venues based on these two dimensions.

[7] Some of the data metrics in this document have been provided by Token Sniffer, a Solidus Labs product designed to detect problematic tokens by auditing tokens against a database of known malicious code.

Figure 2: Examples of trading intermediaries



The first dimension examines whether the venue is order- or quote-driven. An order-driven market is where buyers and sellers interact directly by submitting their orders to a central order book that performs matching. Unmatched orders, where the bid price is less than the ask price, are not filled. In a quote-driven market, a market maker holds an inventory of assets, quotes prices for trading those assets with the market and guarantees orders will be filled at their quoted prices, which can help improve liquidity. In traditional markets, stock trading is commonly order-driven while bond and currency trading is usually quote-driven because these assets are sometimes harder to trade (e.g., bespoke bond issues, unique currency pairs).

The second dimension examines whether trades are settled on-chain. Off-chain settlement involves recording the transfer and ownership of assets through entries on a central ledger. Users pay membership or other fees, usually in the form of fiat currency, to the central intermediary for settlement services. On-chain settlement, or settlement on the blockchain, involves a network of computers recording the transfer and ownership of cryptographic keys—which enable control of an asset—in a chain of computer events. Users pay fees in the form of the blockchain's native token to process their transaction requests.

Using these two dimensions, we compare blockchain usage by the computational memory required for trading and the associated blockchain fees between the three main types of trading venues used for crypto assets: CEXs, decentralized order book platforms and AMMs, noting that the latter two could be considered different models or subsets of DEXs (**Table 2**).[8] A more detailed comparison of these types of platforms requires further research and is beyond the scope of this paper.

[8] Currently, all CTPs in Canada that are registered under securities legislation are CEXs.

Table 2: Comparison of crypto trading venues

Trading venue	Blockchain computational memory required for trading	Explanation
Centralized exchanges (CEXs)	Low	CEXs use order books that require a large amount of computational memory for trading. However, a CEX operates an off-chain central ledger to record orders and the transfer and ownership of assets among its clients. Therefore, the blockchain is needed only for transferring crypto assets between addresses that a CEX does not control. This means the use of blockchain computational memory is low.
Decentralized order book platforms	High	Decentralized order book platforms involve a large amount of computational memory because they use order books, and all records of orders and settlement of those orders are recorded on-chain. For example, every order, modification of an order or cancellation of an order involves a blockchain transaction, an update to the blockchain ledger and a blockchain fee. This model is the most expensive and computationally intensive regarding blockchain usage.
Automated market makers (AMMs)	Medium	Blockchain usage is substantial since all trading operations are on-chain, but a trader submits an order to buy or sell only at the price quoted by the AMM. Therefore, trading through an AMM requires less computational memory and fewer blockchain transactions than decentralized order book platforms. As a result, AMMs can incur lower blockchain fees than decentralized order book platforms. This analysis does not consider computational memory used in the creation or redemption of liquidity tokens (see **section 3.1**).

To summarize, an AMM is unique because it is a quote-driven market and its trading operations are completely on-chain. The quote-driven nature of an AMM supports its viability on the blockchain, making it the dominant mechanism currently for DEXs.

3.1 Operations and services

Market participants can interact with an AMM by:[9]

- **Adding liquidity**: LPs deposit two or more crypto assets at the AMM's blockchain address, or pool, in proportions the AMM determines. The AMM issues or mints a token to the LP that

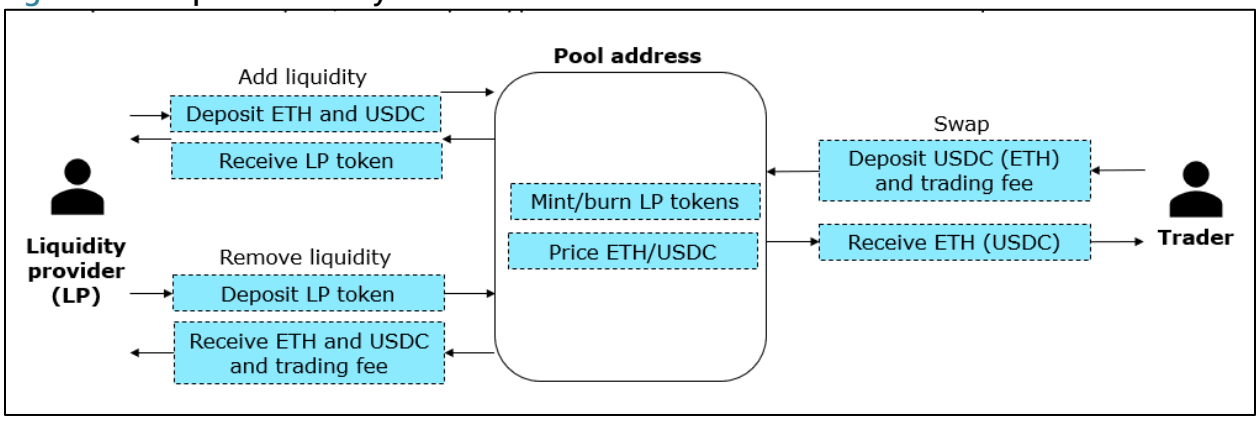
[9] These are known as calls to the contract in programming terms.

represents their proportional share of the pool, which is referred to as a liquidity provider token (LP token).

- **Removing liquidity**: LPs deposit their LP tokens into the pool. The AMM removes the LP token from circulation and returns the LP's corresponding share of the value of the pool plus any trading fees and rewards earned.
- **Swapping**: Traders exchange or swap one or more crypto assets for others in the pool, taking the price quoted or offered by the AMM. The traders pay trading or swap fees that the AMM protocol collects. These fees may be distributed to LPs and governance token holders or invested in the AMM's operations. Traders also pay blockchain transaction fees, such as gas fees on Ethereum.

The pool contract must keep an accurate accounting of both the LP tokens in circulation and the crypto assets in the pool. **Figure 3** illustrates the actions that market participants can take against a single AMM pool, using an example of a pool that swaps between the ether (ETH) and USD Coin (USDC) tokens.

Figure 3: Example of an ecosystem for an automated market maker



An AMM can potentially provide different services to different users (**Table 3**). To an LP, it may provide custodial services by locking crypto assets deposited in the pool and offer investment services by issuing an LP token that generates a return. To traders, it provides trading, liquidity and settlement services. To issuers of crypto assets, an AMM can help create primary markets by enabling issuers to create their own pool from which to distribute their newly created crypto asset.

Table 3: Services performed by an automated market maker

Beneficial user	Potential financial services
Liquidity provider	• **Custody**: Holds and pools crypto asset deposits on the blockchain • **Investment**: Provides variable and potentially an additional fixed rate of return. Trading fees collected depend on trading volumes, while additional rewards are typically paid in proportion to the amount of time assets remain deposited.
Trader	• **Liquidity**: Guarantees the purchase or sale of crypto assets at quoted price. • **Settlement**: Crypto assets traded are immediately cleared and settled using a blockchain.
Crypto asset issuer	• **Primary distribution**: Enables newly created crypto assets to be immediately traded against other crypto assets determined by the issuer. • **Secondary liquidity**: Creates secondary markets for crypto assets.

3.2 Pricing mechanism

An AMM quotes a single price that is provided continuously to the market and determined algorithmically. The quoted price is expressed as a relative price and based on the quantities of crypto assets in a pool. For example, in a pool that has $50 million of DAI and $50 million of ETH, the price of DAI is 1 ETH and the price of ETH is 1 DAI. The quantities of crypto assets in the pool must always satisfy some function or condition. In some cases, this means that the total amount of liquidity does not change across time, known as being liquidity invariant. Commonly, the pricing function is some form of either the constant product function or the constant sum function, described below.

- **Constant product function (CPF)**: The product of token quantities must equal a constant. Each token quantity can be written as an exponential function of the other token quantity. Therefore, the relationship between token quantities can be graphically represented as a curve, also known as a bonding curve.
- **Constant sum function (CSF)**: The sum of token quantities must equal a constant. Each token quantity can be written as a linear function of the other token quantity. Therefore, the relationship between token quantities can be graphically represented as a straight line. CSFs are used for highly correlated assets that are not expected to vary much in price, such as pairs of stablecoins with the same reference asset. In practice, CSFs are parameterized so that the function is some blend of a CPF and CSF depending on the degree of correlation between assets.

Pricing functions across AMM pools can vary regarding the formula, its parameters and even the inputs in that the functions may not be completely based on the quantities of crypto assets in the pool (e.g., some may use external prices or oracles). These functions are evolving as new versions of AMMs are created

and new AMMs are established. Our paper covers a small sample of pricing functions, but other literature such as Mohan (2022) provides a more comprehensive review.

Our case studies use CPF, CSF and their variants (see **Table B-2** in **Appendix B** for further details). As well, the price moves only when traders swap against the pool and change the balance of crypto assets. Because of this, the only way that pool prices match prices in the external market is through traders arbitraging away price differences. For example, if the price of ETH in the pool is lower than its external price, traders should be incentivized to buy ETH from the pool and sell to the external market. As the amount of ETH in the pool decreases, its price in the pool should increase to the external price.

3.3 Pool designs and permissionless issuance

An AMM may establish one or more pool designs. Designs vary by the maximum number of crypto assets that can be included and pricing function. Regardless of design, all AMMs in our case studies have a contract that can be used to deploy some or all of their pool designs. This contract is known as a factory. Factory contracts allow users to build their own pool, choose the tradeable crypto assets in the pool, set trading fees and provide additional rewards to LPs. Therefore, users can control the economic incentives for LPs and traders to participate in their pool.

No permissions are required to call the factory. This allows an AMM to offer primary market-making services for issuers of crypto assets. In traditional markets, issuers of securities (or derivatives) are required to provide specific disclosures prior to distribution, such as prospectus or registration statements. These requirements may apply to issuers of crypto assets in instances where the crypto asset could be a security or derivative, or subject to other regulations. Those in the business of trading securities are required to register under securities law. Currently, however, this is not standard practice among issuers of crypto assets. Some issuers provide no information and others use whitepapers to provide information on its characteristics, functions and risks.

Some AMMs deliberately design their factories or other services to address the needs of new crypto asset issuers. For example, Balancer intentionally designed its liquidity bootstrapping pools for initial coin offerings, allowing the pool's weight to shift from the new token to the other, collateral token over time (Balancer Docs, n.d.). SushiSwap has an offering called the Miso program that supports initial coin offerings and creates new pools on SushiSwap with the new token and proceeds from the initial token sale. In addition, SushiSwap has another offering called the Onsen program to support new coin projects by distributing its governance token, SUSHI, as a reward to LPs of project pools (SushiSwap Docs 2023).

4. Trends in Adoption

To assess user adoption and trading volumes of AMMs, we collected data on a variety of measures of size and activity level for both liquidity provision and trading. This is because AMMs are two-sided platforms that need both LPs and traders to operate sustainably. On the liquidity side, we collected data on:

- TVL
- the number of additions, removals and provider addresses

- activity of the top-20 liquidity provider addresses

On the trading side, we collected data on:

- the value traded or swapped
- the number of swaps
- the number of trader addresses
- activity of the top-20 trader addresses

To obtain insights on adoption by Canadians, we leveraged data collected by our vendors on web traffic from Canadian IP addresses.[10]

4.1. Liquidity trends

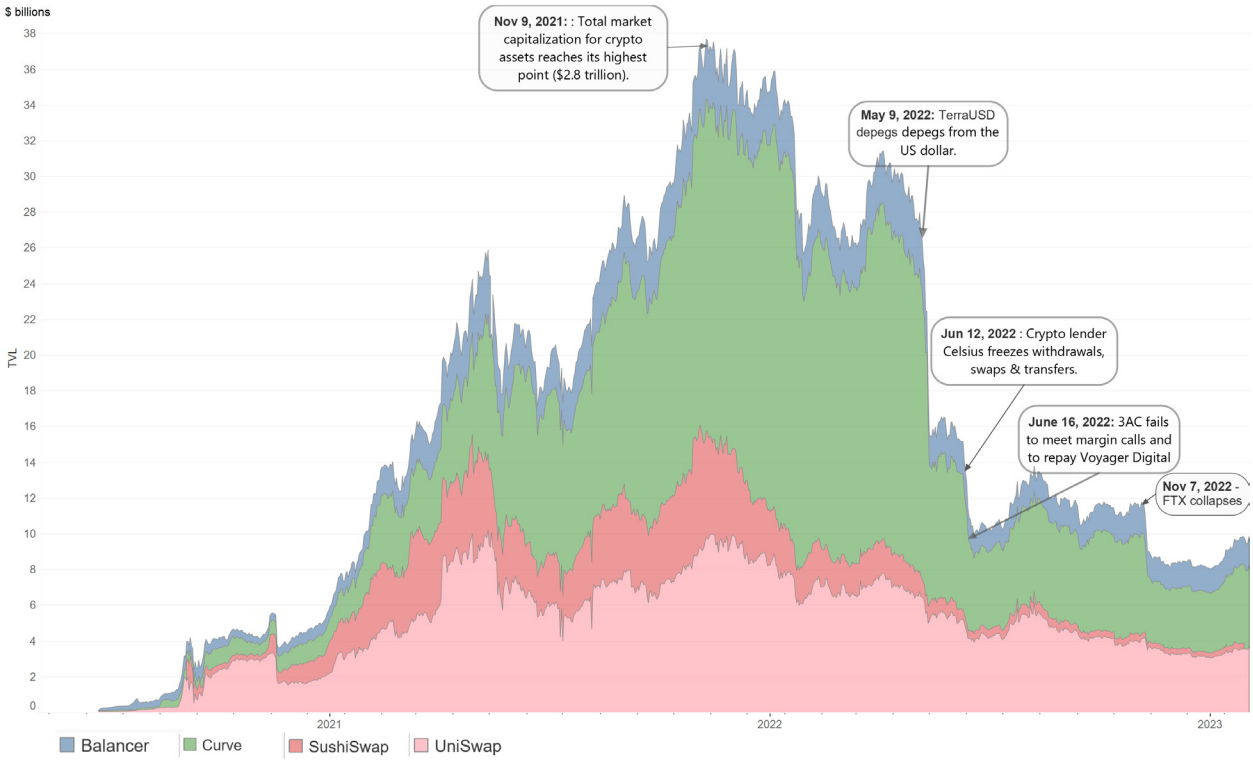
TVL measures the total value of assets locked at the AMM platform level or pool level, making it a key measure of liquidity for AMMs. In general, as TVL increases, so too does the depth of the market and liquidity in terms of lower price impacts from large orders.

The TVL in AMMs increased dramatically through 2021 and reached an all-time high in December of that year, one month after the peak in the total capitalization of the crypto market (**Chart 3**). Much of the run-up in TVL was on Curve, the stablecoin-focused platform that included TerraUSD. Following the collapse of TerraUSD in May 2022, TVL on Curve dropped by more than half, causing the combined TVL across our case studies to drop from a record of $37 billion to just over $15 billion in June 2022. Subsequent failures of large institutional crypto firms (e.g., Celsius, 3AC, Voyager Digital and FTX) caused TVL to fall further to levels seen at the start of the run up in 2021 before recovering somewhat in early 2023.

While growth in TVL has slowed, improved economic conditions, a migration away from CEXs and the introduction of new protocols could reverse this trend in the future.

[10] The authors do not have access to and did not store any IP addresses.

Chart 3: Total value locked in automated market maker case studies



Source: Inca Digital

With respect to volumes, total monthly liquidity transactions (additions and removals) across our case studies ranged from approximately 1,000 to 110,000 between January 2020 and April 2023, generally with more additions than removals or withdrawals (**Chart 4**). In early 2023, the total number of addresses for active liquidity providers each month had fallen to just over 5,000 (**Chart 5**). We also look at the total number of unique addresses that have contributed liquidity to the platforms since their respective launches. As at April 2023, the number of unique addresses were:

- 755,979 for Uniswap[11]
- 1,011,728 for SushiSwap
- 270,045 for Balancer
- 45,515 for Curve

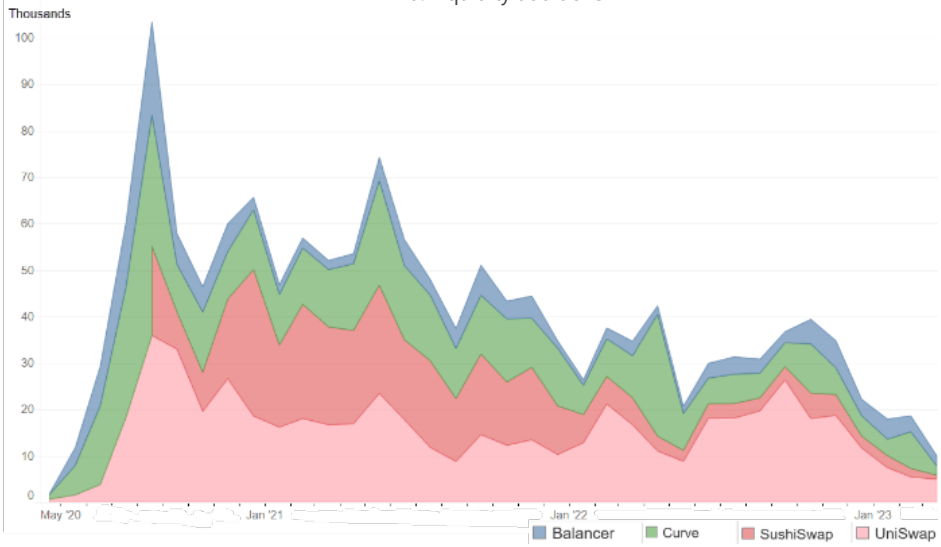
Compared with Uniswap, Curve has significantly fewer LP addresses but a similar amount of TVL. One explanation for this is that the average size of liquidity contributed per LP on Curve is higher than on Uniswap. If true, this could also mean that Curve's LPs are more likely to be institutional firms or aggregating protocols than retail traders. However, further data and empirical analysis are needed to verify this because multiple addresses may be attributable to the same individual or entity.

[11] Source: Dune.com dashboard: Uniswap Protocol Unique LPs Over Time (dune.com)

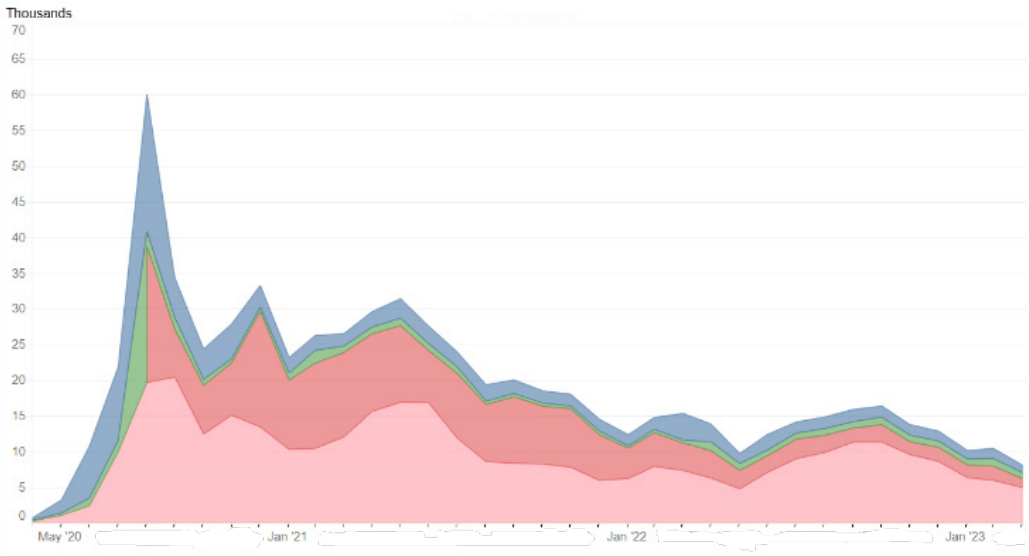
Chart 4: Monthly volumes of liquidity transactions

Monthly counts of liquidity additions and removal events

a. Liquidity additions

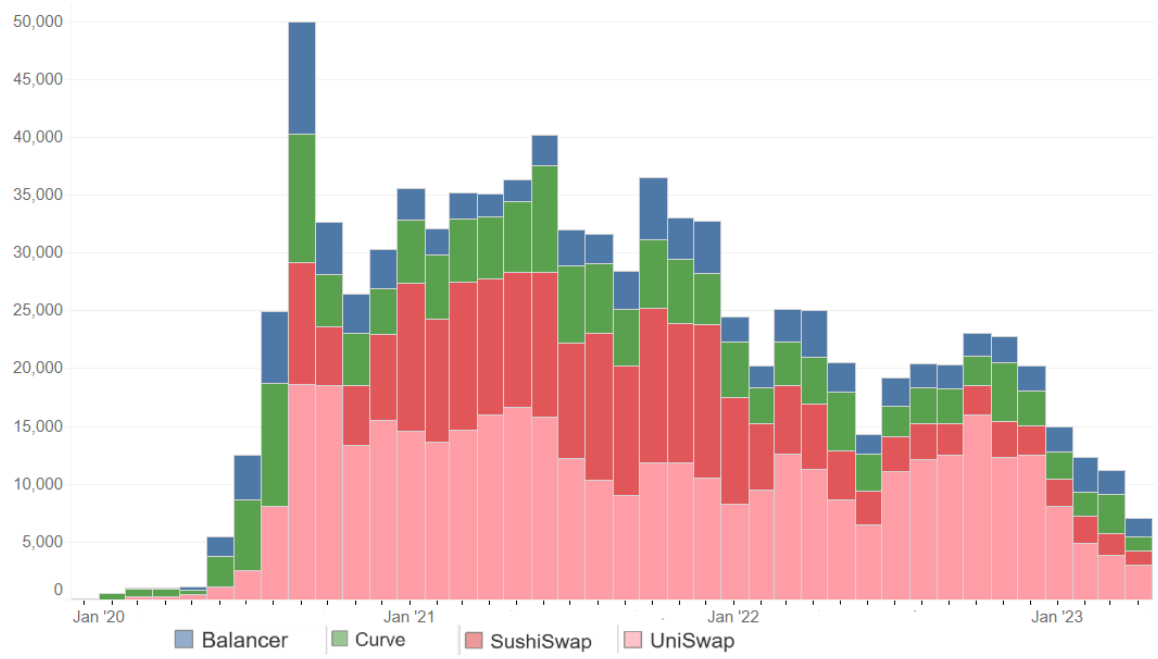


b. Liquidity removals



Source: Inca Digital

Chart 5: Unique addresses that added or removed liquidity from liquidity pools
Monthly counts

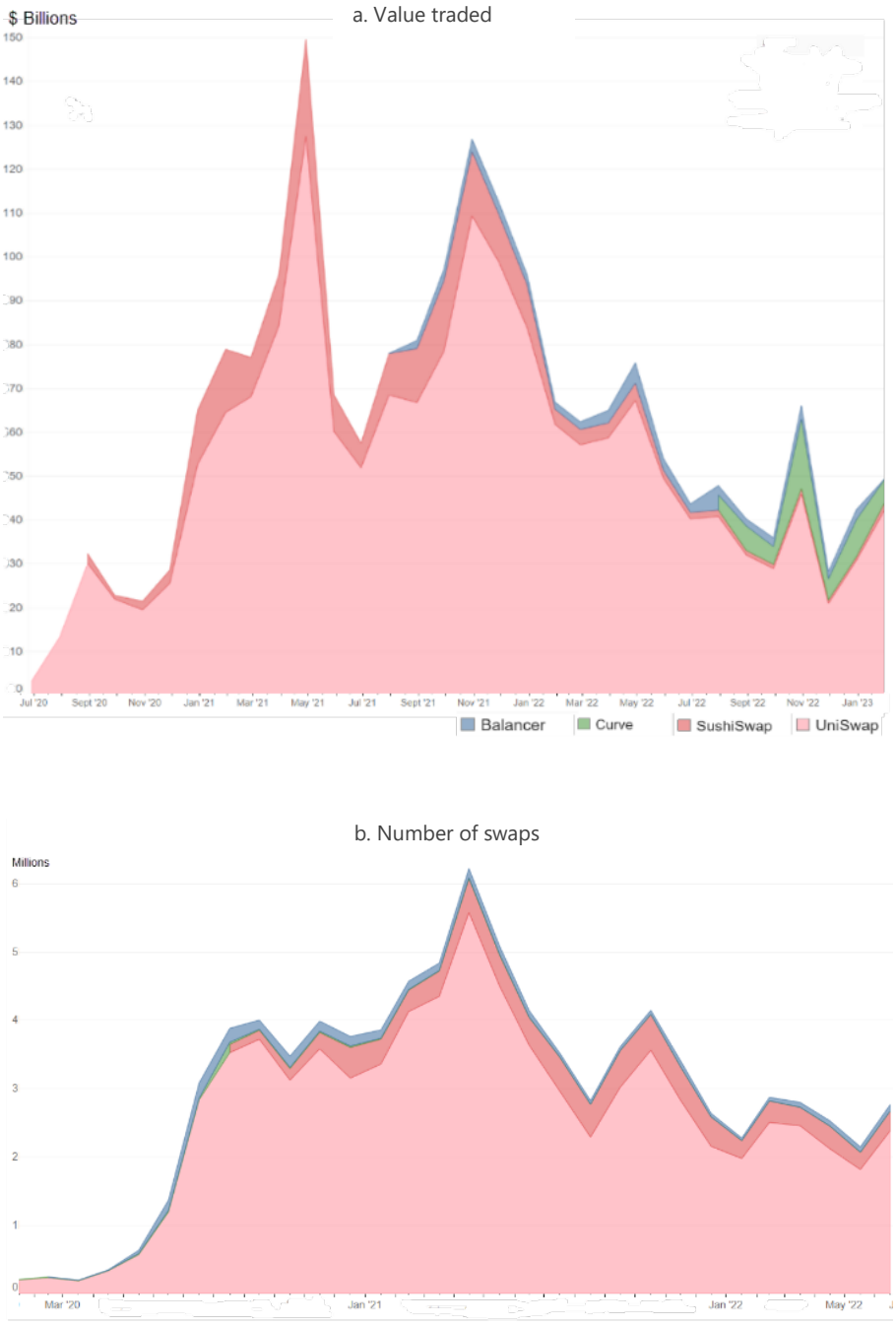


Source: Inca Digital

4.2 Trading trends

Trading or swap activity across our case studies peaked in 2021 with more than $8 billion in trades each day and more than 5 million swaps per month (**Chart 6**). More recently, those figures have fallen to less than $3 billion in daily value and less than 3 million swaps per month. Uniswap is the clear leader in trading activity with respect to value and volume unlike on the liquidity side where Curve posed a challenge to Uniswap.

Chart 6: Monthly value traded and volumes of trades



Note: Uniswap values include V1, V2 and V3. Balancer values include V1 and V2.
Source: Inca Digital Last observation: April 2023

The number of traders also reflects Unsiwap's popularity, with a peak of approximately 1 million unique addresses trading on Uniswap in May 2021 compared with only approximately 100,000 for the other platforms combined. This could be due to Uniswap having a first-mover advantage and a large number of

trading pairs. It could also indicate that an AMM builds more trust with the community of crypto traders the longer it operates.

Table 4: Top 20 addresses actively trading, January 2020–July 2022

Platform	Swaps by top 20 addresses	Total swaps	Top 20 share of total swaps
Uniswap	1,997,635	78,334,285	3%
Balancer	454,731	2,730,574	17%
Sushiswap	602,736	8,193,442	7%
Curve	37,788	268,611	14%

Source: Inca Digital

Uniswap has the lowest concentration of trading volume with 3% of all swaps being associated with the top 20 addresses between January 2020 and July 2022. Balancer had the larger concentration at 17%.

Some of the top 20 traders are common across two or more of our AMM platforms. Three addresses appeared in the top 20 for all AMMs. Using third-party crypto tracing tools, we found that one of these addresses could be linked to Wintermute Trading Ltd., a UK-based company that promotes itself as "a leading global algorithmic trading firm in digital assets."[12] Four addresses appeared in the top 20 for both Uniswap and SushiSwap, one of which appeared to be controlled by Alameda Research, the affiliate of crypto exchange FTX.[13] We could not find attribution data for the remaining common traders, although Balancer had three in its top 20 that also appeared in the top 20 of at least one of the other platforms.

Interestingly, one of the top 20 addresses on SushiSwap appeared to be attributable to Ethermine, a mining pool operated by Bitfly that also deployed front-running software for its miners. Ethermine ceased its operations after Ethereum moved to a proof-of-stake consensus mechanism on September 15, 2022.[14]

4.3 Canadian participation

Quantifying the extent of Canadian participation on AMMs is difficult using blockchain data alone because of the anonymity of blockchain technology and the limitations of crypto tracing tools. In the future, researchers may be able to obtain more information by tracing interactions of wallet addresses linked to registered CTPs in Canada with DeFi protocols, or from surveys about AMM usage by Canadians.[15]

[12] For more, see the Wintermute website at www.wintermute.com.

[13] FTX filed for bankruptcy in November 2022 after fraudulently investing and losing client funds in Alameda Research's projects (Morrow 2023).

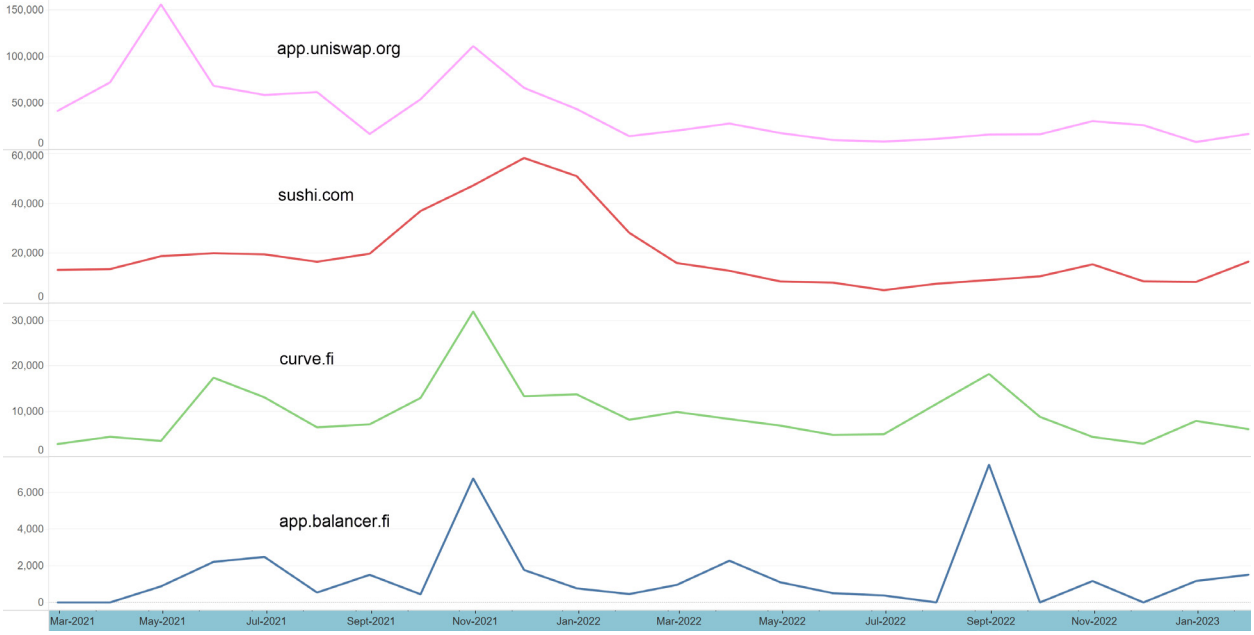
[14] Bitfly, "Important Announcement: End of Ethereum PoW Mining Phase" (August 27, 2022).

[15] CTPs that are registered or have provided a pre-registration undertaking with the CSA are required to provide a list of all blockchain addresses, except for deposit addresses, that hold crypto assets on behalf of clients, including all hot and cold wallets.

To obtain some insights on Canadian participation, we count the number of visits from unique Canadian IP addresses to the domains of the four AMMs between March 2021 and February 2023. We find that, on average, Canadian addresses represented about 3% of total traffic to these domains during the sample period. We provide a caveat that the IP address may not be the true address of the end user since addresses can be masked and appear to be of a different geographic location. Further, a visit to the website does not mean that the end user performed a liquidity action or swap. However, we find that the average visit by a Canadian IP address lasted between 10 and 15 minutes.

Canadian addresses visited in higher numbers in November and December 2021 than in any other time during our sample period, which coincides with when most prices for crypto assets reached all-time highs. During 2022, the number of visitors dropped to record lows, but we observe this trend reversing somewhat in 2023. **Chart 7** shows that Uniswap leads in popularity or awareness among Canadians, followed by Sushiswap and Curve.

Chart 7: Unique monthly visits by Canadian IP addresses



Source: SemRush

Overall, global activity levels at the four AMMs suggest that usage of AMMs remained persistent despite the broader crash in crypto prices in 2022. Activity levels in the first quarter of 2023 were significantly less than the peaks recorded in the fourth quarter of 2021 but are still higher than in the early years of DeFi. We find that activity levels appear to be normalizing around levels seen in the first quarter of 2021. We also see that Uniswap and Curve have emerged from the 2022 crypto market crash as the leading AMMs.

These CTPs are required to separate crypto assets of Canadian clients from their own property and place clients' assets in a designated trust account or in an account designated for the benefit of those clients with an acceptable third-party custodian.

This may suggest that Uniswap has benefited from its first-mover advantage, and that Curve's strategy of focusing on stablecoins and providing strong rewards to LPs is keeping it competitive.

5. Ownership and governance

Identifying if a person or entity is controlling or influencing an AMM is often difficult because of the anonymous nature of blockchains, unless the person or entity has identified themselves. The governance of AMMs is also fairly immature and continues to evolve to troubleshoot challenges. Broadly speaking, current AMM governance arrangements are not well-defined and often lack continuity. These observations contrast with traditional models of good governance where roles and responsibilities are clear, and mechanisms exist to ensure that those with authority or responsibility have the appropriate skills and incentives to fulfill their roles and the organization's objectives.

5.1 Decentralized autonomous organizations and governance tokens

Across our case studies, AMMs aim to use a decentralized autonomous organization (DAO) to govern their operations. In theory, DAOs are collectively owned organizations where all decisions are carried out by a democratic vote on-chain, thus achieving full transparency (Ethereum, n.d.).[16]

AMMs issue governance tokens that can be freely traded or invested on the AMM's platform or those owned by third parties. These tokens provide membership in a DAO but need to be staked or delegated (to one's own address or to a third-party address) for the token holder to have voting rights and receive any staking income or fees directly from the AMM. Therefore, a user may be a passive holder of governance tokens and not use them to vote or exercise any control.[17] Often after staking, the token holder is issued a staked version of the governance token, representing their claim on the original governance token. Sometimes AMMs may set up different staking programs for governance tokens that can change a token's voting weight over time (e.g., assign less than 100% or one vote per token).[18]

5.2 Distribution of decision-making authority

The distribution of a DAO's governance tokens and the staked versions determines the distribution of decision-making authority. All DAOs in our sample have plans to give majority control, or around 60% of their governance tokens, to the external community (i.e., mainly to LPs). The remaining 40% goes to insiders—such as founders, employees or contributors, advisors and investors—or to internal operations like the protocol itself as a form of reserve or treasury to finance projects on the platform. However, DAOs distribute these tokens at varying rates. For example, Uniswap plans to fully distribute its supply by

[16] For more details on the structure and operations of a DAO, see IOSCO (2022).

[17] We are not aware of any custodians that provide users the ability to stake or delegate their governance tokens. As well, some community members have voiced concerns that users that hold governance tokens in cold wallets, which are considered more secure than hot wallets, are generally unable to participate in the governance process. For more, see teoleibowitz, "Proposed Simplifications to the Uniswap Governance Process," Governance-Meta, Uniswap Governance (January 21, 2022).

[18] Tokens with voting weights that increase over time are not fully vested or earned. AMMs commonly provide these tokens to core developers or investors to incentivize retention. Tokens with voting weights that decrease over time are unique to DeFi and are used by DEXs that offer certain incentive programs (see **section 5.3** on incentives).

September 2024 (Uniswap Labs 2020). Balancer will take until 2090, a more cautious approach that the platform attributes to the significant experimentation still happening with decentralized governance (Balancer Docs, n.d.).

Available data suggest that token holdings are fairly concentrated across AMMs, with some more concentrated than others. Using data from August 2022, we find that the top 20 addresses for each AMM held at least 60% of the available supply of governance tokens. Curve had the highest concentration (88%) and Uniswap the lowest (62%). Except for Balancer, the level of concentration for staked versions of governance tokens appears to be the same or worse across platforms.[19] For example, the top addresses holding staked versions of governance tokens at Curve and SushiSwap have 66% and 95% of the available supply, respectively. These figures are misleading since the top addresses for these AMMs are aggregating protocols that hold tokens for multiple users. Identifying the owners of these tokens would require the computationally intensive task of reviewing transaction-level data to see who staked or sent their governance tokens to these contract or protocol addresses.

Ignoring these contract or protocol addresses, we still find a concentrated number of addresses with significant influence over an AMM. AMMs set quorums for passing votes that can be met by a small number of addresses. For example, Uniswap only requires 4% of UNI tokens to pass a vote, and four addresses had been delegated at least this amount in April 2023. Similarly, Balancer and SushiSwap require quorums of 2 million veBAL and 5 million SUSHIPOWAH to pass a vote, and five addresses and at least two addresses, respectively, exceeded these amounts. According to data collected by Inca and other sources, some of the largest holders have been institutional players: Andreessen Horowitz was one of the largest holders of UNI, and Binance and Alameda Research were two of the largest holders of xSUSHI as at February 2023.[20]

The number of members in multisignature, or multisig, wallets is another indicator of the concentration of authority. These wallets may be used to execute or implement proposals and require more than one private key to authorize a transaction or execute code.[21] They may have other special powers like the authority to disable all functionality of an AMM, such as in the case of Curve. Typically, the total number of signers for a multisig wallet ranges from 5 to 10. Unfortunately for governance token holders, little information may be available on who the signers are other than their pseudonyms or social media handles. The process for selecting signers is not usually transparent, although governance token holders can vote to change signers in some cases. Our expectation is that signers would be core developers or contributors who have intimate knowledge of the protocol's code.

---

[19] We use data from February 2023 for staked versions.

[20] In February 2023, Andreessen Horowitz (a16z) held 15 million UNI and delegated 40 million UNI to third parties that could theoretically be reclaimed, for a total of 55 million UNI. See S. Kessler, "Contentious Uniswap Vote Highlights the Opaqueness of Decentralized Governance," *CoinDesk* (February 8, 2023). For live information on top UNI delegates, see https://sybil.org/#/delegates/Uniswap.

[21] Multisig wallets can help create redundancy in case of a loss or theft of a private key and can reduce the risk of self-dealing by any single individual. The most obvious use case for multiple signatures is to control the disbursement of funds deposited at a single address.

5.3 Incentive structure

This section discusses the economic incentives for participating in AMM governance, such as by staking governance tokens. In traditional models of corporate governance, compensation is important for recruiting and retaining qualified talent. Compensation at the board or executive level usually includes a mix of cash and equity—to balance interests in the short- and long-term performance of the firm—with some element of deferred compensation to incentivize staying with the firm (Edmans 2014). In contrast, compensation schemes in a DAO governance model are evolving.

An AMM faces the challenge of incentivizing governance token holders to stake these tokens and vote rather than immediately transfer or sell them to the market for value. The market value from a staked governance token cannot be realized until a future date since these tokens are locked in a contract and cannot be sold immediately. As a result, AMMs have added or are adding economic incentive programs for staking.

Two common economic incentives or rewards that may be provided under staking programs for governance tokens are:

- **Governance or protocol fees**: An AMM charges traders a markup on trading fees, known as a governance or protocol fee, and distributes revenues to governance token holders who have staked their positions.
- **Additional liquidity mining rewards and voting rights over their distribution**: To make certain pools more attractive to LPs, an AMM can offer additional rewards for liquidity locked in those pools. These rewards can be in the form of governance or other tokens. Only LPs that have staked governance tokens are eligible to receive these rewards, and the amount of tokens received is typically a multiplier of the amount of governance tokens staked. Further, only holders with staked governance tokens may vote on which pools offer rewards and the reward rate.

Another incentive scheme, commonly known as a vote-escrow system, has created some negative consequences among the community of governance token holders. Curve and Balancer use this scheme, and SushiSwap was considering adopting it (0xMaki.eth 2021). This scheme allows governance token holders to influence a pool's relative liquidity or attractiveness. Because of this, issuers wishing to improve the liquidity of their token trading on an AMM can amass large amounts of governance tokens, stake them and vote to provide liquidity mining rewards to pools trading their token. The competition for liquidity on Curve became known as the Curve Wars. Similarly, a governance battle emerged on Balancer between a whale known as Humpy and other large players (**Box 1**).

5.4 Issues and challenges

Major challenges have been identified with the governance arrangements found in DeFi. We describe a subset of these challenges below and some of the potential solutions AMMs are experimenting with to

address them. Interestingly, addressing these challenges may require developing more off-chain organizational structures and processes.[22]

- **Unclear legal treatment**: A DAO may not be a recognized legal structure—or its structure may be interpreted differently between jurisdictions—and may not be registered as a legal entity with local authorities.[23] Ambiguity may exist where any rights and obligations of token holders and contributors set out by a DAO do not comport with laws in the jurisdictions where it operates. For example, the Commodity Futures Trading Commission filed a civil enforcement action against the Ooki DAO in September 2022, arguing that its members are liable for DAO debts (Frankel 2022). SushiSwap hired a law firm for advice on a structure that would better protect members from any liability. In December 2022, SushiSwap's members voted to restructure the AMM into three foundations: two in Panama and one in the Cayman Islands that would administer an on-chain governance process.[24]
- **Concentration of authority and conflicts of interest**: While the intent of a DAO is to have a more democratic form of governance, decision-making authority can still be concentrated because no restrictions exist on the number of tokens a single person or entity can hold or stake. For example, five entities reportedly controlled 88.5% of SushiSwap's governance tokens in December 2022 (Avan-Nomayo 2022). **Box 1** describes concentration issues that are unique to blockchains.
- **Informal accountability for off-chain decisions**: The AMM's core team or multisig signers typically execute off-chain decisions. These decisions may include business partnerships with external firms or agreements with third-party service providers—such as audit or security firms—and can be strategically and operationally important. Traditional firm structures have a set of legally binding contracts that enable the board to oversee management, determine executive compensation and receive regular reporting on performance. These mechanisms ensure that the management team is accountable for its decisions. For AMMs, these formal mechanisms rarely exist. Instead, governance token holders must trust that the core team is executing off-chain decisions according to the holders' best interests, which seems counter to the blockchain spirit of being able to operate in an environment where trust is not essential.

[22] For more, see A.Z. Lewis, L. Lotti and J. Pope, "The State of Uniswap Governance: A Paradox of Minimization," Other Internet (May 25, 2022).

[23] Some jurisdictions analyze DAOs as existing partnerships, joint ventures, associations, limited liability entities or similar structures. Other jurisdictions either recognize DAOs as legal corporate entities or are studying their legal status (e.g., Australia, the United Kingdom and certain states in the United States). For more, see IOSCO (2023).

[24] For more, see D. Nelson, "With Crypto Governance in CFTC Crosshairs, SushiSwap Mulls Legal Shakeup," CoinDesk (October 4, 2022); and 0xMaki.eth, "Sushi Proposal: oSUSHI [SIGNAL]," Snapshot, August 2021.

Box 1

Examples of concentration issues unique to blockchains

In October 2022, Binance delegated to itself 13 million UNI tokens, or 5.9% of the total supply of the token. Binance claimed this was unintentional and occurred automatically because of UNI's design when the company was transferring tokens between its own wallets (Copeland 2022). Although unintentional, the incident raises questions about the ability of automated market makers (AMMs) or members of its decentralized autonomous organization (DAO) to prevent large custodial wallet providers from accumulating a disproportionate amount of voting power. The situation also suggests that a trade-off exists between custody arrangements and governance participation. Since the majority of crypto users store their tokens with third-party custodians, they cannot participate in the governance process. This limits broad community engagement and exacerbates any asymmetric distribution of power.

AMMs that adopt vote-escrow systems of governance have experienced significant issues with users accumulating substantial amounts of governance tokens and voting for personal gain rather than for the long-term benefit of the AMM.

On the Curve platform, users who stake their CRV tokens for longer periods are rewarded with higher CRV emissions, which in essence are a liquidity premium. Yield aggregator protocols have emerged to capture this premium and are competing to attract CRV token holders with the promise of higher rewards without the lock-up periods. Instead of staking CRV tokens directly to Curve, users transfer them to a pool controlled by the protocol in exchange for a liquidity provider (LP) token. The protocol then stakes the collected CRV tokens at staggered durations, earning higher CRV emissions than users could have earned individually. The most successful of these protocols has been Convex, which has collected and controlled as much as 85% of Curve's total value locked. The protocol did this by attracting users to transfer it around 50% of the supply of CRV.[25] Convex has amassed significant voting power on Curve's DAO (66%) and has influenced the allocations of rewards to Curve's liquidity pools. [26] A consequence of this structure is an active secondary market for Convex's LP token, CVX. Users see acquiring CVX as a way to influence the governance of Curve. This ongoing competition for liquidity, and influence over the platform, is known as the Curve Wars.

Similarly, Balancer had a situation where a whale known as Humpy directed the distribution of BAL liquidity rewards to pools where the whale had deposited liquidity. In one case, Humpy issued its own token called CREAM, created a pool with those tokens and reportedly directed US$1.8 million of liquidity rewards to that pool (Kelly 2022). Other governance token holders, including smaller whales, attempted to counter Humpy's vote, leading to governance battles. In December 2022, Balancer, Humpy and other whales reached an agreement, known as the peace treaty, that required Humpy to cease accumulating veBAL tokens and only "vote for pools that are beneficial to the long-term growth of Balancer" (Kelly 2022).

[25] See Echidna Finance, "Curve & Convex," Medium (January 31, 2022).

[26] Convex held 66% of veCRV tokens, the staked version of the Curve governance token, in August 2022.

6. Economics of participation

This section identifies the economic benefits and risks of using AMMs. As benefits and risks can vary by type of participant, we provide an analysis from the perspective of an LP and a trader.

6.1 Liquidity providers

An LP should seek to maximize its net economic benefit, which can be formulated as:

$$Trading\ Fees - Blockchain\ Transaction\ Fees - Impermanent\ Loss + Other\ Compensation.$$

Trading fees are derived from a transaction fee charged to a trader for their swap or trade. Each AMM establishes its own fee structure. Fees are typically set and collected at the pool level and range from 0.01% to 1% of the swap value. An LP is entitled to a share of the fees in proportion to its relative contribution to the pool (e.g., it receives 10% of fees if it contributed 10% of the pool's value). An AMM needs to set trading fees high enough to attract more liquidity but not too high that they deter trading. Fees that are too high can reduce overall revenue for LPs, which is a product of both trading fees and trading volumes.

Blockchain transaction fees are incurred each time an LP makes a deposit to or withdrawal from an AMM pool, and amounts will differ depending on the blockchain. These fees are usually proportional to the computing power or resources required to process the transaction rather than the value of the deposit or withdrawal. This means that the cost of these fees increases with the number of transactions or amount of congestion on the blockchain. These fees can be substantial depending on the blockchain and can disincentivize an LP from withdrawing its assets.

Impermanent loss (IL) is a concept unique to AMMs. The loss represents the opportunity cost from locking liquidity in an AMM instead of holding the tokens outside the platform. IL can be calculated as the difference between the price gains from holding tokens outside the platform and any increase in the value of the LP's pool position. The latter is a function of changes in both pool price and token quantities since traders swap tokens with the pool.

Aoyogi and Ito (2021) show that a liquidity provider always suffers IL if relative prices change within the pool.[27] This occurs whenever an external price shock affects only one of the tokens in the pool and the token does not maintain its original relative price. The reason is that an AMM relies on traders to arbitrage the spread in prices between the AMM and the external market and equilibrate the two prices. If the AMM price is higher than the market price, an arbitrageur will buy the token in the external market and sell it to the AMM. Conversely, if the AMM price is lower than the market price, an arbitrageur will buy a token from the AMM and sell it to the external market. Since the LP is implicitly the counterparty to the arbitrageur's trades, the LP always buys too high or sells too low relative to the market price and suffers an unrealized loss.[28] In fact, the arbitrageur's profit equals the IL of the LP.

[27] Recall that the price provided by an AMM is expressed as a relative price and based on the quantities of crypto assets in the pool.

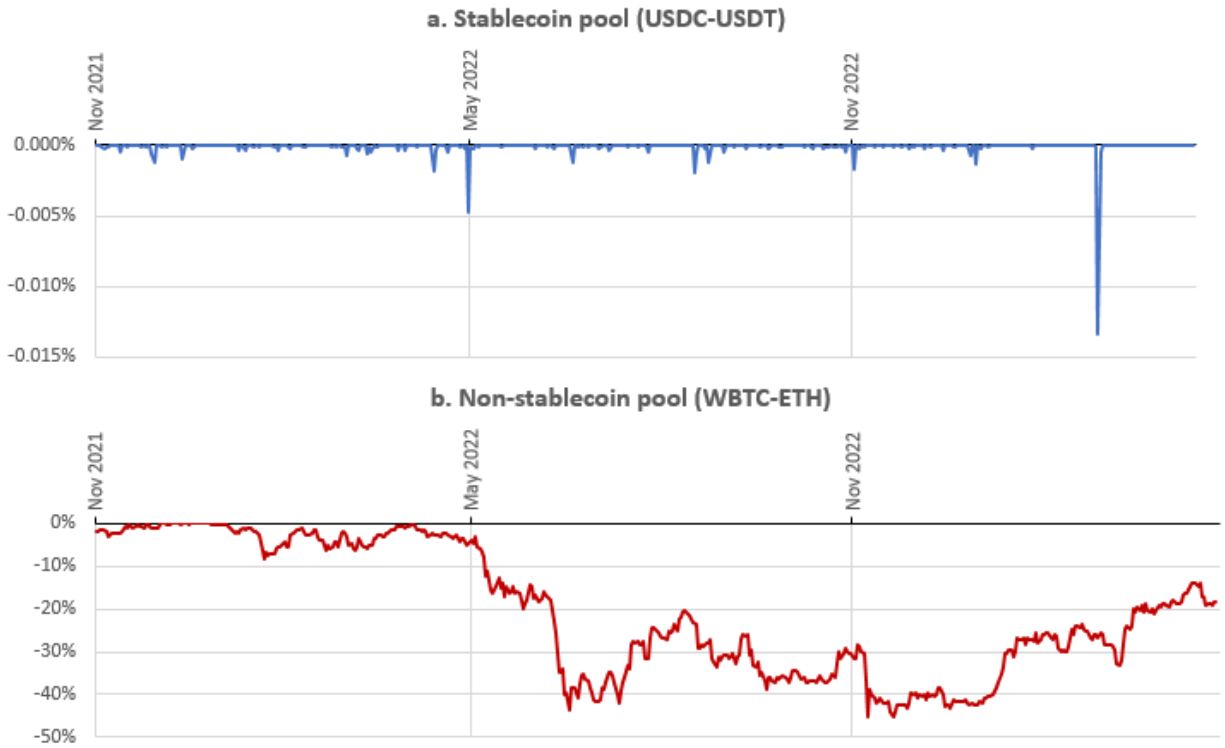
[28] Put differently, this loss comes from informed traders imposing an adverse selection cost on LPs unaware of the arbitrage. For more, see Aoyagi and Ito (2021).

IL can be minimized if LPs invest in pools composed of stablecoins with the same reference asset such as the US dollar. Conversely, IL increases if the volatility of the crypto assets in the pool are vastly different from one another (**Box 2**).[29] **Chart 8** compares the cumulative ILs of two Uniswap pools:

- one with stablecoins that seek to maintain the same value as the US dollar—USD Coin and Tether
- a second with non-stablecoins—wrapped Bitcoin and Ether

Since their inceptions, the maximum cumulative loss was 0.016% for the stablecoin-only pool and more than 45% for the non-stablecoin pool. To break even, the latter pool would need to increase trading fees and other rewards.

Chart 8: Cumulative impermanent loss in Uniswap pools



Note: Stablecoins in panel a include USD coin and Tether. Non-stablecoins in panel b include Bitcoin and Ether. Pool addresses are 0x3416cF6C708Da44DB2624D63ea0AAef7113527C6 for panel a, and 0xCBCdF9626bC03E24f779434178A73a0B4bad62eD for panel b.
Source: Dune Analytics Last observation: April 27, 2023

Other compensation is anything else the pool may offer through various incentive schemes like reward tokens, also known as liquidity mining rewards. We previously discussed how LPs who stake their governance tokens in value-escrow reward systems can receive additional governance tokens, and therefore greater voting power, when providing liquidity. The tokens traded in the pool may also be yield-bearing, although third-party protocols provide the interest, not the AMM itself, across our case studies. Nonetheless, the AMM does not prevent an LP from earning interest while the tokens are locked in a pool.

[29] This is well-documented in the literature (Wang, Heimbach and Wattenhofer 2021; Aoyagi and Ito 2021; Capponi and Jia 2021).

An AMM will not be viable if it cannot attract enough liquidity to its pools. To do this, it needs to appropriately compensate LPs for the substantial amount of risk they take. Most crypto assets are highly volatile, which means IL is usually very high. Early versions of AMMs, such as Uniswap and SushiSwap, fixed trading fees at 0.3%. Increasingly, AMMs have allowed these fees to vary according to the volatility of crypto assets in the pool. For example, pools consisting mostly of stablecoins, like those on Curve, tend to have lower trading fees. Balancer allows pool creators to dynamically set trading fees using a model developed by the Gauntlet, which is a company that helps DeFi protocols optimize capital efficiency and stakeholder rewards. However, most Balancer pools still have flat trading fees.

Box 2

Short volatility

A helpful analogy is to view a liquidity provider's (LP) position as a short straddle options strategy, which is a combination of a short call and a short put position, both with the same strike price and expiration. The payoff from a short straddle is the fixed premiums from writing the two call options minus any losses from the price of the underlying asset moving outside the strike price. The strategy is extremely risky because the rewards are limited (the price of the underlying asset can only fall to zero) and the losses can be unlimited (prices can rise infinitely). Options traders that use this strategy are trying to short volatility, which means they will incur losses if volatility increases in the price of the underlying crypto asset. Similarly, an LP's impermanent loss grows as the volatility of prices increases for the crypto assets deposited in the pool.

This is quite different from traditional market makers who do not bet on the underlying crypto asset maintaining a specific price but typically have a flat or neutral position. Traditional market makers also behave like arbitrageurs, buying low and selling high to generate revenue from the bid-ask spread (Fender and Lewrick 2015). Lehar and Parlour (2021) explain that LPs retain all the price impact revenue from supplying liquidity in order-book markets but earn only fees in AMMs because arbitrageurs (traders) obtain this benefit.

6.2 Traders

A standard trader seeks trading venues that will provide the best price and the lowest cost. To trade on an AMM, the trader must simultaneously buy one token and sell another (or several others), which is why these trades are also called swaps. Since a purchase is always made, a trader's objective is to minimize:

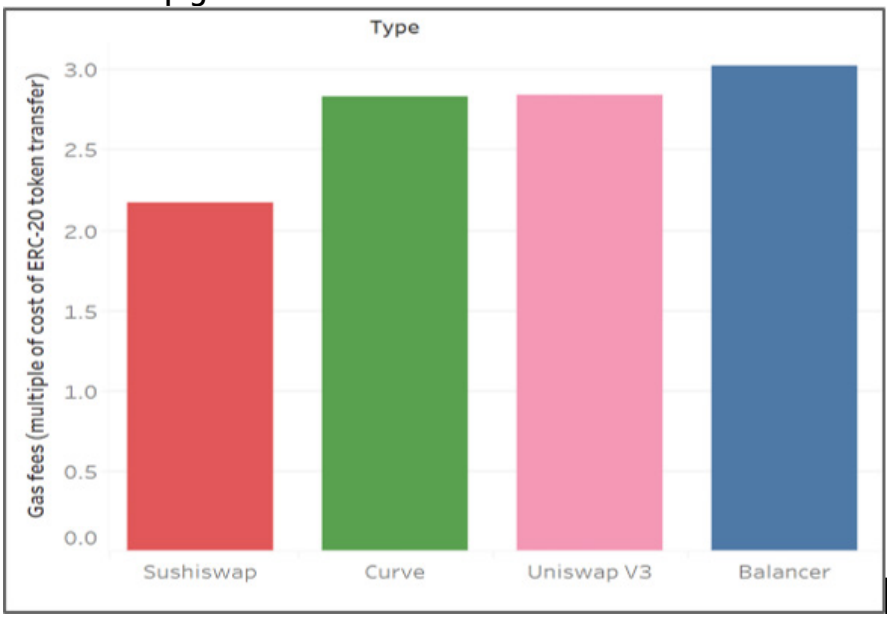
$$Trading\ Fees + Blockchain\ Transaction\ Fees + Execution\ Price.$$

Trading fees are transaction fees charged to a trader for their swaps or trades, as discussed above. These fees are paid into the pool and subsequently distributed to LPs, governance token holders or the protocol's related addresses (e.g., the DAO, treasury).

Blockchain transaction fees must be paid each time a trader swaps against the pool. These fees can be substantial and create a wedge between prices in the AMM and the external market. Traders are the only type of participant that can change the pool price through their trades, but equilibrating the AMM price to the external market may not be economical for them because of these fees. On Ethereum, blockchain transaction fees are known as gas fees and total gas costs depend on the computational resources

required to perform a transaction. The computational resources required to perform a swap can vary across AMMs, which suggests that AMMs could also compete on this factor to attract traders. A swap on the AMMs in our sample can cost two to three times more in gas fees than a standard token transfer on Ethereum (**Chart 9**).[30] At its peak in May 2022, the average gas fee was US$87 to transfer an ERC-20 token. Ten months later, fees dropped to less than US$5 (see **Chart A-3** for more details).

Chart 9: Swap gas fees relative to ERC-20 token transfer



Note: The gas limit used to calculate gas fees for a swap action on each AMM is expressed as a multiple of the gas limit for an ERC-20 token transfer as at March 4, 2023.

Source: Etherscan

The AMM algorithm determines the **execution price** based on the relative supplies of tokens in the pool, which change as traders swap against the pool to meet their demands. Larger pools that have deep supplies of all their constituent tokens help prevent sizable and adverse price impacts—also known as price slippage in crypto parlance—when a large trade is made. In other words, larger pools have better liquidity and tend to offer a better execution price than smaller pools. Aoyogi and Ito (2021) show that informed traders are more sensitive to the size of liquidity pools than traders who are unaware of the arbitrage. This suggests that institutional investors may be more attracted to AMMs with larger pools.

Blockchain scalability can also affect price slippage. Congestion on the blockchain can lead to delays in fulfilling orders. This can cause the executed price to deviate from the price quoted at the time the order was made. Most AMM wallet providers have mechanisms for traders to set a limit for price slippage, such as a percentage of price deviation, and will not execute the trade if the tolerance is exceeded.

[30] Most tokens on Ethereum follow the ERC-20 coding standard, which facilitates interoperability between tokens. A transfer is a simple transfer of tokens from one address to another.

Decentralized exchange aggregators have developed protocols that can help traders receive the best prices or pay the lowest costs by routing orders to different DEXs (**Box 3**).

Box 3

Decentralized exchange aggregators

Service providers known as aggregators split a single swap into multiple trades that can be executed on different decentralized exchanges (DEXs) and different pools within those DEXs. Examples of aggregators are 1inch, Kyberswap, Matcha, ParaSwap and OpenOcean.

Using aggregators does not prevent slippage. This is because transactions are executed on-chain where there can be congestion or delays to processing. Since trades may be executed at different times, and each trade could cause a price impact itself, slippage can arise. Aggregators are not yet sophisticated enough to anticipate price impacts from non-simultaneous trades and incorporate them into a trading strategy. Notably, DEX aggregators also provide wallet and custody services for traders, unlike DEXs, and are frequently a gateway to DEXs for users.

7. Risks to investors, market integrity and financial stability

In this paper, we attempt to provide readers with a detailed understanding of AMM activities, operations and governance that supports further consideration with respect to applying a regulatory framework. This work aligns with IOSCO's recommendations that securities market regulators develop a "holistic and comprehensive understanding" of DeFi activities within their jurisdictions (IOSCO 2023).[31]

In this section, we consider what AMM activities may pose a risk to a securities regulator's mandate.[32] We discuss:

- sources of investor harm
- risks to market integrity and broader confidence in capital markets
- potential channels for systemic risk

7.1 Investor harm

Users of DeFi products or services often face information asymmetries and may be susceptible to harm through a loss due to misconduct or market failure. Crypto assets offered or traded on AMM platforms have varying levels of risk that are likely not well-understood by investors and the terminology used in

[31] IOSCO (2023) provides nine policy recommendations that acknowledge the differences in domestic regulatory frameworks and encourages regulators to implement the recommendations based on their own analysis of DeFi activities or arrangements. The recommendations are principles-based and outcomes-focused. They are intended to assist IOSCO members as they apply existing or develop new regulatory frameworks to achieve regulatory outcomes for investor protection and market integrity in DeFi that are consistent with those in traditional financial markets.

[32] Anti-money laundering risk also exists on AMMs but is not discussed here given the scope of this section.

DeFi can be confusing. For example, the concept of IL for LP tokens is complex (see **section 6.1**). Even labelling the loss as impermanent is potentially misleading.

Further, trading decisions are complicated by the lack of standardized terms and functions of crypto assets as well as comparable historical data. Additionally, retail investors are unlikely to have the knowledge or capacity to independently assess whether the programming behind or the provisions within an AMM smart contract may be fraudulent or susceptible to exploit.

LP tokens represent claims on pools. For those pools consisting of uncorrelated crypto assets, the LP tokens are very risky and may be unsuitable for retail or less sophisticated investors. In contrast, the risk-return profile of governance tokens may be easier to understand. But the legal risk and liability of governance token holders who have certain control rights are unclear since the legal treatment of DAOs remains unsettled in many jurisdictions.

As well, AMMs are designed to be permissionless. They generally do not perform due diligence on new token offerings, nor have any requirements for the disclosure of information to investors.

7.2 Market integrity

Market integrity refers to markets without abuse that create an unfair advantage for one participant, unfair terms of trade or barriers to entry like excessive costs. Market integrity is considered important for fostering confidence and increasing participation in capital markets (Austin 2017).

We discuss three factors that increase the risk of market manipulation on AMMs:

- information leakage
- lack of listing standards
- anonymity

While some AMMs are developing mechanisms to address these risks, we do not cover these mechanisms in detail.

Information leakage leading to potentially unfair practices

Information asymmetries among market participants may lead to fairness concerns and questions about the integrity of the market. In some blockchain systems, all pending and successful transactions are public. Theoretically, this should give traders equal access to the same set of blockchain data and not allow for any information advantage. In practice, certain actors can still use high-frequency trading bots and validator nodes—which are known as miners in some blockchain designs—to gain an advantage over the typical investor (Daian et al. 2019).

Like in traditional finance, high-frequency trading bots constantly scan the blockchain for arbitrage opportunities. They can obtain a slight information advantage from building faster connections to access these blockchain data. We consider this form of information advantage somewhat less egregious since the information advantage is obtained through costly investment in infrastructure and because it can facilitate price discovery and equilibrium across fragmented trading venues. However, retail investors

typically do not have faster connections, leaving them at a disadvantage in DeFi where they can trade independently without the fast speeds or best execution efforts that a broker may provide.

We consider information advantages exploited by validator nodes—which are unique to blockchains—to be more egregious because the information advantage is obtained through privileged power. In a blockchain system, a network of validator nodes verifies transaction requests and updates the blockchain. Usually, a validator node is chosen through a pseudo-random process (proof-of-stake) or competes to select a set of pending transactions to add to the blockchain (proof-of-work). The node can then sequence those transactions within the new block in any way.[33] Validators nodes can insert their own transactions and re-order other users' pending transactions to extract value from market-moving trades, known as miner extractable value. Data collected by Auer, Frost and Pastor (2022) show that some nodes front run, back run and conduct sandwich trades. The latter involves executing trades both before and after a user, thus making profits without having to take on any longer-term position in the underlying assets. The total value extracted on the Ethereum network alone is estimated to be between US$550 million and US$650 million from 2020 to 2022 (Auer, Frost and Pastor 2022).

Complete data on the incidence of market abuse and loss to investors do not exist, but available data are concerning. Data from Flashbots (n.d.) show that value extracted by block proposers from the re-ordering, inclusion or censoring of transactions continues on Ethereum and had been fairly steady in 2023. After Ethereum moved to a proof-of-stake system, more than 500,000 of these realized extractable value, or REV, transactions occurred between September 2022 and June 2023 on certain AMM protocols, including Balancer V1, Curve, Uniswap V2 and Uniswap V3. The profits from these transactions totalled over US$70 million. Over 90% of these profits occurred on Uniswap V2 or V3, which we suspect have mainly retail participants (Flashbots Transparency Dashboard, n.d.).

A common way for AMMs to defend against information asymmetries is to adjust their pricing formulas so the formula does not immediately respond to the last trade. For example, the price may be a moving average of historical prices over a certain period, which makes manipulating the price more difficult because attackers would need to persistently attack the price over that period. This was one of the improvements made to Uniswap V2 and V3.

Lack of listing standards

The ethos of DeFi is to provide open, permissionless access to financial products and services. As a result, crypto assets are included in AMM pools without protections against unfair, improper or fraudulent practices. This environment makes it easier for bad actors to execute malicious schemes through AMMs.

Analysis in this area distinguishes between schemes that involve tokens that have built-in smart contracts designed to steal investor funds and schemes that involve tokens that do not have code integrity issues but are launched as part of a pump-and-dump scheme.

[33] In a proof-of-stake consensus mechanism, the probability of a validator being selected is usually based on a measure of the validator's proportional ownership of the blockchain's native token supply, or stake.

Research from Solidus Labs (2023) found that at least 9% of the ERC-20 tokens in pools and available for trading on the AMM platforms in our case studies may have code integrity issues.[34] **Table B-7** provides a breakdown of these tokens using Solidus Lab's taxonomy. The organization's research suggests that the most common types include honeypots, which is when a smart contract prevents the buyer of a token from reselling it, and hidden mint contracts, where buried code will execute minting and selling of new tokens that result in the original token becoming worthless. Generally, for listing problematic tokens for trading, bad actors are attracted to venues that provided higher liquidity and a variety of traded assets, which may obscure their malicious activity.

Several forms of pump-and-dump manipulations exist in crypto asset markets. One form is information-based and involves spreading false information about the asset.[35] Another is trade-based and involves rapidly buying and then selling a token at successively higher prices—known as wash swapping—before removing liquidity from the AMM asset pair. Finally, users of so-called pump groups openly orchestrate pump and dumps without any pretense of maintaining secrecy. Instead, administrators of pump groups publicly declare they will pump a coin, known as sending a pump signal, and call on others to join the pump (Dhawan and Putniņš 2022).

Chainalysis (2023) estimates that 24% of new tokens launched in 2022 were part of pump-and-dump schemes such as these, although we do not know which of these were launched on AMMs. This figure could be conservative because it looks at tokens that had some trading activity (i.e., 10 swaps and 4 consecutive days of trading). Further research and data are needed to better understand the extent of pump-and-dump schemes on AMMs since studies to date have focused on larger, unregistered order-book CEXs.

Anonymity leading to self-dealing or wash trading

The anonymity of traders makes it difficult to detect relationships between blockchain addresses and identify conflicts of interest, heightening the risk of manipulation from self-dealing such as wash trading. A trader can easily engage in self-dealing and wash trading by quickly buying and selling the same crypto asset from different addresses to generate fictitious volumes and temporarily inflate prices. A trader may also have conflicts of interest if they are simultaneously the LP and crypto asset issuer and would benefit from artificially higher trading volumes.

CTPs registered in Canada are required to know their clients and are better than AMMs at detecting this behaviour because they can attribute trading activity to individual traders. This allows registered platforms to place restrictions or prohibitions on those accounts. An AMM has information about the blockchain activity of specific addresses but would need to perform a forensic analysis to identify the users and the

[34] Solidus Labs (2023) scanned token codes for signs of malicious intent between September 2020 and April 2023 using its tool available at tokensniffer.com. Available tokens were obtained from thegraph.com and reflect numbers as at August 10, 2023.

[35] This requires uncertainty about the fair value of the asset and information asymmetry.

relationships between addresses.[36] This makes market surveillance of and deterrence or enforcement against bad actors more challenging and could impair an AMM's ability to comply with securities laws.

Solidus Labs (2023) finds that more than US$2 billion worth of wash trades have taken place on DEXs since September 2020. Almost half of this fictitious volume comes from token creators that use multiple crypto asset addresses to evade traditional methods to detect wash trading.

Attributing the observed declines in crypto activity or investment to concerns over the integrity of AMM markets is difficult, but some evidence shows that confidence in the broader crypto market is low and may be declining. Results from a survey by the OSC (2023) show a decline in the share of Canadian respondents that own crypto assets, falling to 10% in 2023 from 13% in 2022. Results also show a drop in the share of respondents who believe that crypto assets will play a key role in the future financial system, declining to 34% in 2023 from 49% in 2022. Similarly, results from a 2023 survey by the Pew Research Centre of over 10,000 Americans find that three-quarters of respondents were not confident in the safety and reliability of cryptocurrency. Responses to the survey also show that one-third of American adults who ever invested in, traded or used crypto assets had divested all their holdings, providing further evidence that confidence may be declining (Faverio and Sidoti 2023).

7.3 Systemic risk

Systemic risk refers to the potential for AMMs to adversely impact the functioning of the broader financial system and the real economy. While AMMs have vulnerabilities that can create a systemic risk, the potential for contagion to the real economy is likely low at this time.

- **Illiquidity and mispricing of crypto assets**: Fragmented and low liquidity in certain AMM pools can cause mispricing issues to persist or worsen. The complexity of pools, reward schemes and pricing algorithms may also make it difficult for investors to value LP tokens and provide liquidity support where needed. The mispricing vulnerability is also due to a lack of controls or mechanisms by platforms to detect or prevent market manipulation or to address downward spirals in asset prices, such as through trading halts. Combined, these factors can make AMMs prone to attacks on liquidity pools. One example of this occurred on May 7, 2022, when Terraform Labs withdrew US$150 million of TerraUSD from its 3pool on Curve to create a new 4pool on the platform. This temporarily made the 3pool more illiquid and prone to attacks. Indeed, large trades were then placed in the 3pool that caused TerraUSD to de-peg and then collapse (Barthere et al. 2022). Nonetheless, there were no adverse impacts on the real economy because TerraUSD was not commonly used to pay for real goods and services.
- **Financial interconnectedness**: The extent to which mispricing can lead to systemic risk or impacts on the real economy depends, in part, on the linkages between AMMs and traditional financial system participants and asset markets. Available data suggest that retail or institutional investors

[36] In contrast, tracing transactions on the blockchain becomes easy once the identities of and relationships between addresses are determined. Identifying these relationships could also help detect manipulation strategies that involve multiple marketplaces.

likely have low values of direct exposures to AMMs.[37] However, some assets traded on AMMs are linked to traditional financial markets, such as fiat-referenced stablecoins supposedly backed by a reserve of traditional assets. Issuers of these stablecoins could be forced to sell traditional financial assets at fire-sale prices if AMMs exacerbate selling pressures on their stablecoins. This makes having well-functioning markets desirable to support the pricing of these assets. Curve may be of most interest from a systemic risk perspective given its focus on stablecoins.

- **Operational vulnerabilities**: A failure or interruption of service at an AMM could lead to broader disruptions in capital-raising activity for crypto projects and reduce secondary market liquidity for traded crypto assets. The extent to which operational vulnerabilities can impact the real economy depend on how much crypto assets are interconnected with the traditional financial system. Operational vulnerabilities on AMMs arise from concentration risk with respect to people and technology. Certain AMMs, such as SushiSwap and Balancer, appear to have concentrated governance and ownership structures. Available data suggest key persons or entities involved in these structures are interconnected with other segments of the crypto ecosystem but not the traditional financial system. From a technology perspective, AMMs tend to rely on common blockchains and technology solutions, such as Ethereum, Snapshot and Discord. Service interruptions to these providers could lead to disruptions to other AMMs and the broader crypto ecosystem. However, the operational linkages between DeFi and the traditional financial system are opaque, and further data and research are needed in this area.

8. Regulatory considerations

The rapid proliferation of DeFi products and services reflects the level of financial innovation from market participants and technology developers. However, as we have explored in this paper, AMMs present common and unique risks to investors, market integrity, financial stability and the broader DeFi market. In this section we highlight a limited set of AMM activities that may already be captured within existing regulatory frameworks. We also recognize that DeFi entities, such as AMMs, have qualities such as decentralized decision-making and user anonymity that may present distinct challenges compared with centralized entities when applying regulatory expectations.

8.1. Select activities of automated market makers

Users engage with AMMs to perform a variety of activities with some conducted on- and off-chain. Accordingly, AMMs are not strictly peer-to-peer platforms. Analyzing where these activities may fall within the boundaries of securities regulation requires careful legal analysis by using the principle of same activity, same risk, same regulatory outcome.[38]

[37] A 2023 report by the Financial Stability Board concluded that interlinkages between DeFi, TradFi and the real economy appear to be limited so far. See Financial Stability Board, "The Financial Stability Risks of Decentralised Finance" (February 16, 2023).

[38] IOSCO (2023) affirms that where DeFi activities and arrangements mirror traditional financial markets, a "same activity, same risk, same regulation/regulatory outcome" approach should be adopted.

At a functional level, AMMs appear to:

- issue and engage with a variety of crypto assets that may be considered securities or derivatives
- perform some key functions comparable with centralized market structures
- encourage participation by retail and institutional users in trading activities and liquidity pool

As explored in **section 3.1**, we identify three core interactions that market participants—LPs, traders and crypto asset issuers—have with AMMs:

- adding liquidity
- removing liquidity
- swapping assets

Each of these activities—and potentially others—may have implications for securities regulation. In particular, AMMs may engage directly with crypto assets that are securities or derivatives. As well, AMMs may have arrangements and mechanisms that could result in the activity being considered as relating to securities or derivatives trading.

Tokens and other crypto assets

Thousands of unique crypto assets are issued, swapped, staked or locked across the liquidity pools on the AMMs explored in this paper. The structure and characteristics of each token may differ significantly, including the design, distribution and intentions of the issuer. Efforts are ongoing in many jurisdictions to determine which crypto assets may be a security, derivative or both.[39] Issuers, platforms and investors that engage with such assets must do so in compliance with securities legislation.

AMMs explored in this paper all use LP tokens, governance tokens and stablecoins (**Table 5**). A legal interpretation of these or other crypto assets is outside the scope of this paper. However, some tokens used on or issued by AMMs—or the key characteristics these tokens exhibit—may already be considered securities, derivatives or both.[40, 41]

---

[39] In some cases, specific crypto assets are subject to litigation between token issuers, trading platforms and regulators. For example, a US federal court judge ruled in favour of XRP token issuer Ripple, finding that its programmatic sales of XRP through digital exchanges and algorithms did not qualify as the sale of securities because investors could not have had a reasonable expectation of profits "from the entrepreneurial or managerial efforts of others" (*United Housing Foundation, Inc. v. Forman*, 421 U.S. 837 (1975), quoted in *Securities and Exchange Commission v. Ripple Labs, Inc.*, 1:20-cv-10832, 18 (S.D.N.Y. July 13, 2023)). Additionally, the same court in a different case dismissed a class action lawsuit to hold UniSwap accountable for scam tokens but went further and called ETH a commodity (*Risley v. Universal Navigation Inc.*, 1:22-cv-02780, (S.D.N.Y. Aug 29, 2023)).

[40] CSA (2023a) states that VRCAs or VRCA arrangements may be securities, derivatives or both. Additionally, recent regulatory action taken by the US Securities and Exchange Commission against crypto platforms Binance and Coinbase signals its decision that at least 19 coins should be considered securities. Notably, this includes SOL, the governance token for the Solana blockchain, and BUSD, the fiat-backed stablecoin issued by Binance. For more, see B. Rahma and M. Washburn, "The Full List of Cryptos Named Securities in SEC Lawsuits Against Binance and Coinbase," BeInCrypto (June 8, 2023).

[41] A study commissioned by the European Parliament (Zetzsche et al. 2023) suggests establishing a default rule where crypto assets are deemed transferrable securities unless exempted by a national authority. This study outlines potential futures for the Markets in Crypto Assets (MiCA) Regulation that came into force in June 2023. MiCA creates a licensing regime in the European Union for centralized CTPs and wallet providers and requires stablecoin issuers to hold sufficient reserves.

Table 5: Common characteristics of tokens

Type	Purpose	Key characteristics
Liquidity provider (LP) token	Acts as a receipt of claim on assets in a liquidity pool, which are locked in a smart contract, and as evidence of entitlement to any return or yield (e.g., liquidity fees or other rewards)	• Issued by automated market makers (AMMs) • Acts as a deposit note or guarantee on pledged crypto assets • Units represent user's proportionate share of pool's total liquidity and its value tied to pooled assets • Redeemable on demand • Users can stake the token to the AMM to gain a governance token • Users can stake the token to other yield platforms (e.g., Convex) or transfer it to other wallet addresses*
Governance token	Gives holder the right to vote on proposals that govern the development and operations of the AMM, and may act as evidence of entitlement to any return or yield (e.g., staking rewards)	• Issued by AMMs • Equity-like properties, including voting rights on AMM operations and secondary market liquidity • Can be earned through locking LP tokens, with added rewards for longer-dated holders • Users expect returns through rewards and fees, including the issuance of additional tokens
Stablecoins	Provide price stability and liquidity to facilitate trading of other crypto assets	• Issued by a crypto business (e.g., Circle and USDC) or a decentralized exchange (e.g., Curve and crvUSD) • AMMs may distribute, offer or sell stablecoins (and other crypto assets) • Pledged to liquidity pools • Generally viewed as highly liquid • Used to facilitate paired trades involving less liquid crypto assets

*LP tokens issued on the Ethereum network are ERC-20 tokens and can be transferred, exchanged or even staked on other protocols. Initiatives on secondary markets exist, including from Yield Bank, but compete with other yield-farming protocols. For more, see iYield, "Secondary Markets & Longevity in DeFi," Medium (January 27, 2021).

Stablecoins—also known as value-referenced crypto assets (VRCAs) in Canada—play a key role in facilitating DeFi activity. An estimated 80% to 85% of trading and lending on global crypto platforms involve stablecoins (Gensler 2022). Notably, Curve was exclusively designed to increase liquidity for stablecoin swaps.[42] Despite what their name implies, stablecoins are not without risks and have attracted regulatory attention in recent years. In particular, the CSA is of the view that VRCAs may constitute

[42] Regulatory attention toward stablecoins intensified after the collapse of the algorithmic TerraUSD/Luna ecosystem and the resulting de-pegging of fiat-referenced coin Tether (USDT) through confidence shocks in May 2022. Authorities including the Financial Stability Board, the Committee on Payment and Market Infrastructure, IOSCO, the Bank for International Settlements and the CSA have provided clarity on the uses of and risks from the multiple versions of these crypto assets.

securities, derivatives or both (CSA 2023a).[43] As an interim approach, the CSA has established certain terms and conditions that CTPs must satisfy to continue trading VRCAs (CSA 2023b).[44]

An AMM may also perform functions similar to a dealer by issuing and distributing its own tokens or facilitating the primary distribution and secondary trading of tokens from other issuers. We observe that these activities include few—if any—disclosures, including associations between the entities or the related fee structure. As well, the AMM may have conflicts of interest regarding tokens that the DAO decides to include on its platform. For example, voting power in a DAO may be used to prioritize fees and rewards for certain liquidity pools, accept a native token as collateral or provide preferential pricing to certain issuers.

Activities with respect to liquidity providers

Platforms incentivize market participants to become LPs through fees and other rewards gained by obtaining and staking LP tokens (see **section 5.3**). The token acts as a user's claim on the pool's future earnings, providing an opportunity to earn passive income on crypto assets. An AMM holds and pools crypto asset deposits on the blockchain. In doing so, an AMM may, in effect, provide custodial services to the LP and create a contractual obligation with the user by committing to store and protect the deposited crypto asset through a smart contract.

Such activity may be distinct from the trading function of the AMM, where swaps are executed automatically between users' wallet addresses. If the AMM does provide custody of the deposited crypto assets—potentially establishing a contractual obligation—it may need to register as a trust corporation with a prudential authority. This would result in operational and compliance obligations, including auditing and reporting requirements. In addition, a custodial AMM could be considered to be dealing in securities (e.g., being evidence of indebtedness or an investment contract under the definition of a security).

A liquidity pool may be created to help a primary market distribute a newly created crypto asset. Any entity that complies with the requirements of the pool's smart contract (e.g., holder of the desired crypto asset) may become an LP. In this way, AMMs may unwittingly enable bad actors to raise capital illicitly or perform illegal activities on the platform. As well, AMMs may lack the controls needed to report suspicious activity to the relevant authorities. AMMs are unlikely to consider the risk profile and past transaction history of an LP before permitting the provider to participate in the pool. Generally, AMMs do not implement any other conditions for participation unlike regulated market participants that use know-

[43] The CSA staff notice states that VRCAs backed by a reserve of a single fiat currency, also known as a fiat-backed crypto asset, generally meet the definitions of a security, derivative or both in several Canadian jurisdictions (CSA 2023a). Similarly structured VRCAs pegged to and backed by either non-fiat currencies or other types of assets may also generally be considered a security, derivative or both. These crypto assets may give digital evidence of indebtedness or a direct or indirect claim on the issuer.

[44] The CSA staff notice (CSA 2023b) sets out the interim terms and conditions for which the CSA would consent to a registered CTP—or to a CTP that provided a pre-registration undertaking—so it can continue allowing its clients to buy, deposit or enter into crypto contracts to buy or deposit VRCAs.

your-client (KYC) standards, anti-money laundering (AML) measures and combatting the financing of terrorism (CFT) controls.

Activities with respect to traders

AMMs appear to perform some key functions of traditional marketplaces since they can provide primary and secondary markets for various crypto assets as well as trade clearing and settlement services.[45] Commonly, regulations apply to a marketplace that brings together buyers and sellers of securities, derivatives or orders from multiple users employing common, established methods for orders to interact.[46] AMMs may also be in the business of trading in or advising on securities or derivatives. Despite the peer-to-peer nature of AMMs, where orders are executed on-chain between users' wallets, the various functions of the platforms may trigger regulatory attention.[47] The characteristics of each AMM may require specific consideration on its alignment with current definitions of marketplaces, exchanges and dealers in applicable legislation, including any legal obligations present in smart contracts.[48]

Presently, traders and LPs that engage in AMM activities do so with few protections and must inherently accept risks to their assets. Platforms generally conduct little or none of the following common risk practices for trade execution:

- KYC or product suitability standards for on-boarding users
- controls for AML or CFT
- transparency on swap or trading fees
- checks for creditworthiness
- uniform approaches to user leverage in trading activity

As mentioned in **section 7.2**, the potential for bad actors in DeFi is heightened and recourse for participants is often unavailable due to a platform's immediate settlement practices.

From our research, AMM users generally retain control of assets in their blockchain wallets and trades are executed through a smart contract directly with other users' wallets. Settlement of traded assets is generally immediate. Traders take ownership, possession and control of the traded crypto assets and

---

[45] DEXs may perform marketplace functions similar to those of CTPs (CSA 2020). CTPs are subject to registration and other requirements of securities laws to conduct business in Canada (CSA and IIROC 2021).

[46] See the OSC's website for more information on the general requirements for marketplace registration.

[47] Previous Canadian regulatory guidance may be applicable to these practices, including CSA Staff Notice No. 21-327, which states that CTPs would be subject to securities legislation if the traded crypto assets are securities or derivatives, or if the traded contracts or instruments are derivatives based on a crypto asset.

[48] The US Securities and Exchange Commission (SEC) proposed amending the Securities Exchange Act to revise the definition of "exchange" to include systems that "offer the use of non-firm trading interest and communication protocols to bring together buyers and sellers of securities" (Securities and Exchange Commission, "Amendments Regarding the Definition of 'Exchange' and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities," Release No. 34-94062, January 22, 2022). If realized, these changes may capture any platform that facilitates digital asset exchanges or swaps. At the time of writing, the SEC has conducted a second round of public consultations on the proposed changes from 2022.

likely have no ongoing obligation or relationship with an AMM. During execution, an AMM assumes no counterparty risk and passes other risks—including fraud, performance or proficiency—to the users. Authorities may need to consider the trader's relationship with—and expectations of—the platform, particularly regarding the timing of trade execution and whether an AMM has control over user assets (see CSA 2020).

8.2 Future monitoring and data gaps

Regulators may want to continue monitoring the AMM sector in terms of its size and interconnectedness, the risks to investors and efficient capital markets, and the sources of financial instability that it could amplify. For example, regulators could collect the number of traders and track trading volumes to measure activity on Uniswap since it appears to be retail-focused. In contrast, TVL and the number of LPs may be better measures for Curve because it focuses more on institutions due to its large stablecoin pools. **Table 6** provides examples of data that could be collected to monitor this sector, with some data serving multiple purposes or categories.

Regulators should monitor investor adoption, despite it not always being easy to quantify, because future changes to the DeFi technology stack could accelerate adoption.[49] Some of these changes could be desirable from a public policy perspective by reducing risks or costs, such as improving the back-end blockchain (settlement) layer to reduce congestion and fees for LPs and traders. Another example is enhancing a protocol's pricing mechanism to reduce the risk of market manipulation or to better incentivize designs for LPs and governance token holders that improve governance decisions and lead to more sustainable growth.

[49] The technology stack includes the following layers: application, smart contract, asset and settlement (IOSCO 2023).

Table 6: Examples of data for monitoring automated market makers and decentralized exchanges

Category	Examples of data
Size and interconnectedness	• Total value locked • Offered yields (for aggregators or liquid staking providers) • Swap and liquidity transaction volumes and values • Number of users (governance token holders, liquidity providers, traders) • Number of integrated DeFi applications, such as wallets, decentralized exchange aggregators, lending platforms or other financial services providers that could expand the points of entry to platforms* • Market capitalization of governance tokens • Governance structure and operations
Risks to investors and market efficiency	• Miner extractable value or other front-running activity • Pump-and-dump schemes • Links to addresses known to have received funds from or used funds for illicit activities
Vulnerabilities	• Number and size of pools by token • Linkages with other entities (i.e., blockchains, bridges, oracles, etc.) • Multi-signature thresholds for changing smart contracts • Activity by types of traditional financial intermediaries and investors • Market share for trading of fiat-referenced stablecoins and other tokens representing real assets • Concentration of (staked) governance token ownership, as well as the identity and roles or interests (e.g., token issuer, liquidity provider or trader) of major owners • Concentration of third-party service providers • Hacks or operational issues†

*Using IOSCO (2022) terminology, the DeFi application layer that faces users sits above the smart contract layer that includes AMMs.

†For additional metrics, see Annex C of IOSCO (2023).

While tools and strategies are being developed to address some of the key challenges associated with collecting DeFi data, further work is needed.[50] For example:

- The anonymity of blockchain addresses is a key challenge preventing assessments of interconnectedness and enforcement against bad actors. Tools exist to trace blockchain activity and attribute them to individuals or entities, but regulators across the financial sector may need to require regulated entities to report their blockchain addresses or DeFi activity to fully deal with this challenge.
- The lack of standardized coding parameters or language across AMM platforms makes it challenging to efficiently collect and aggregate data from multiple platforms. One interim solution is to focus on a manageable set of the more dominant platforms and blockchains, as we did in

[50] For a discussion about data challenges, see Financial Stability Board, "The Financial Stability Risks of Decentralised Finance" (February 16, 2023).

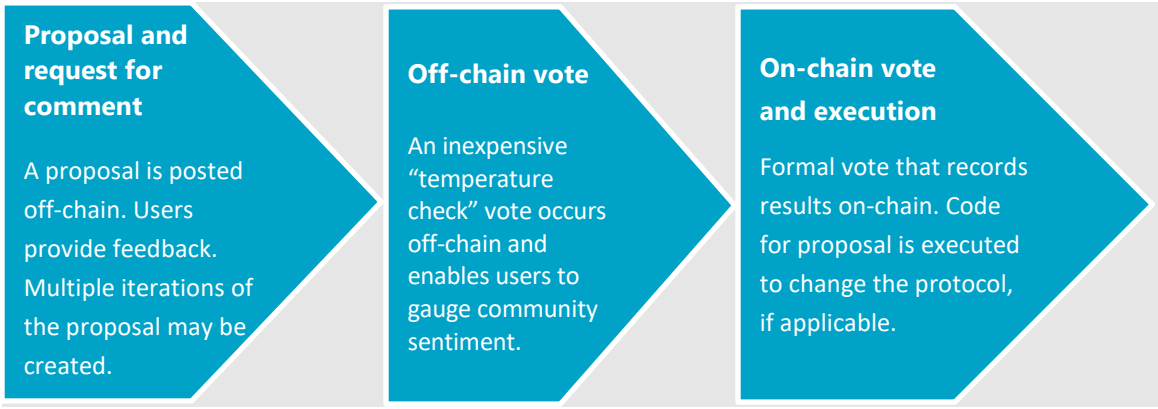
this paper. Ideally, a coordinating mechanism, such as standards or best practices from industry or regulators, would help platforms use the same language and terms.

- Cooperation and information sharing across regulatory agencies, both domestically and internationally, is difficult without effective mechanisms to do so. Agencies have different mandates and access to different regulatory data. This can make sharing data across agencies important to provide a system-wide view of the global DeFi market. Some progress is being made as regulators bring crypto firms into compliance with existing regulations and as international standard-setting bodies continue to place DeFi on their agendas and workplans. For example, IOSCO's Multilateral Memorandum of Understanding and Enhanced Multilateral Memorandum of Understanding capture information requests related to DeFi activity.[51]

[51] See IOSCO (2023).

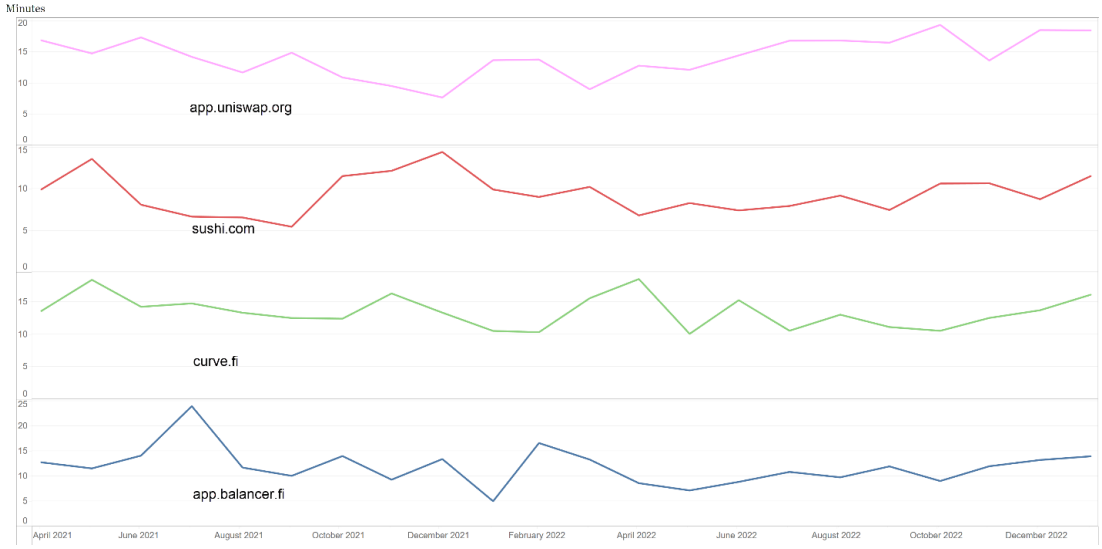
Appendix A: Figures and charts

Figure A-1: Governance process



Note: A pure decentralized autonomous organization (DAO) requires a democratic vote for every operational decision, which is then recorded on a blockchain for full transparency. Because casting votes on-chain can incur blockchain transaction fees (e.g., gas fees), most decentralized exchanges use a combination of off-chain and on-chain tools to govern their platform. For example, common off-chain governance tools are Discord, a forum for discussing proposals, and Snapshot, a voting platform spun off from Balancer and created specifically to support DAOs. A proposal will typically go through three stages, the first two of which occur off-chain.

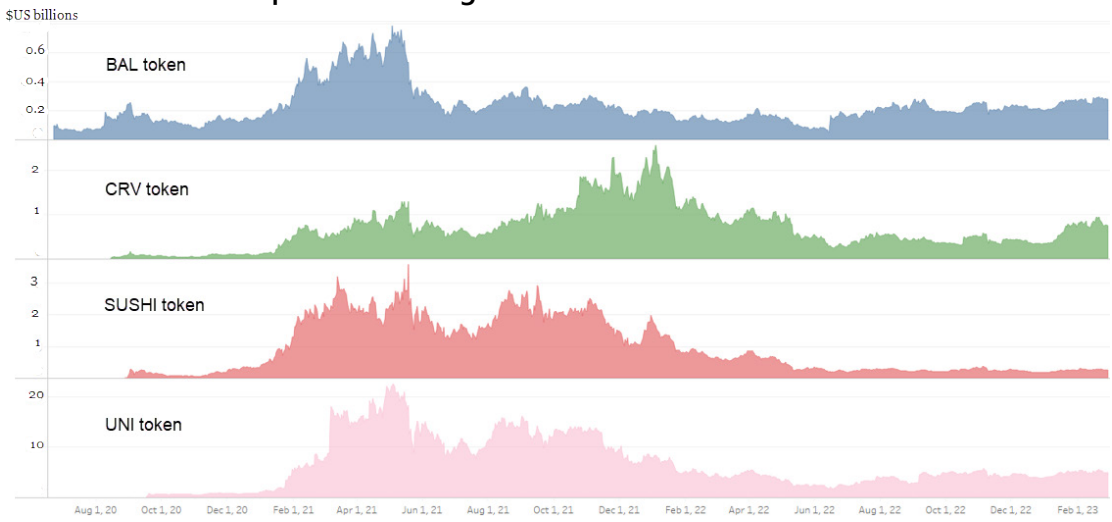
Chart A-1: Average duration in minutes of a visit to an automated market maker by a Canadian IP address



Source: SemRush

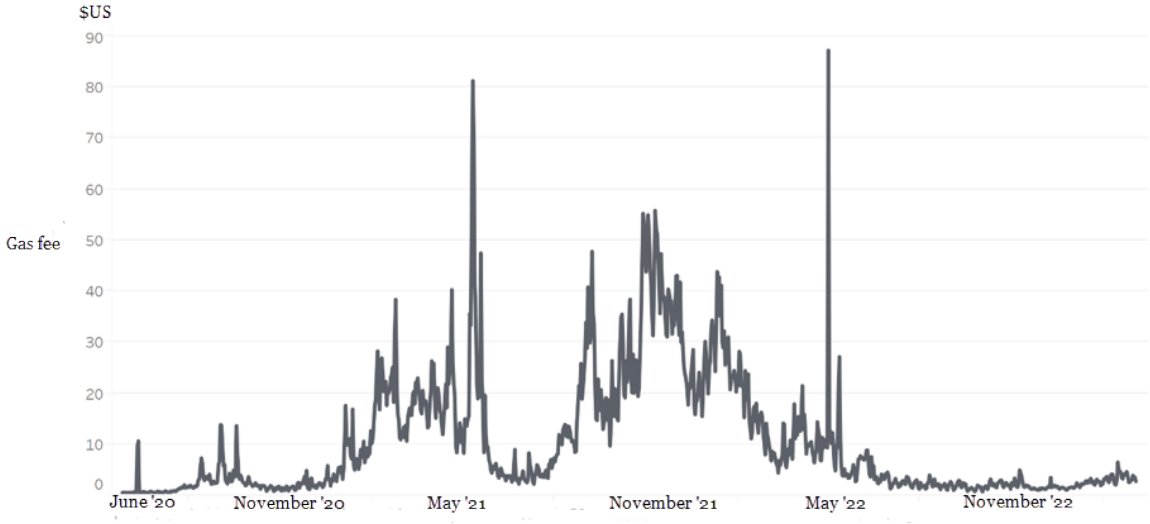
Last observation: February 28, 2023

Chart A-2: Market capitalization of governance tokens



Source: Coinmarketcap.com

Chart A-3: Average daily gas fee for transferring an ERC-20 token



Source: Etherscan and Bank of Canada calculations

Last observation: Mar 4, 2023

Appendix B: Tables

Table B-1: Summary of methodologies used by Inca Digital

Data	Methodology
Total value locked	Calculated the number of pools (count), related assets (symbols) and the total value locked in each asset. Converted amounts to US dollars.
Volume and value of liquidity events and trades	• Obtained a list of all pools on each AMM and their associated tokens. Each AMM typically has one or more pool factory addresses that are publicly available. Inca queried the factory addresses for calls used to create a pool (createPool or createPair). • Extracted from each pool the number of liquidity addition and removal transactions. Large variation exists across different AMMs in terms of the contract mechanics and terminology for liquidity actions. • Extracted the number of swap events in each pool with all relevant parameters. Converted the raw amount into the actual amount. The amount parameters for swaps (trades) and liquidity actions are in raw integer form instead of the actual amount (e.g., 1234 instead of 12.34). The associated decimal value for each token address was applied to each liquidity or swap amount (raw_amount / 10^decimal_value = actual_amount).
Number of liquidity providers and traders	Calculated the number of liquidity providers and traders using unique addresses that either added or removed liquidity or that traded on the four AMMs.
Top 20 liquidity and providers and traders by volume	• For top 20 liquidity providers, calculated the number of additions minus the number of removals for each address and for each pool, then aggregated by address for each AMM. • For top 20 traders, calculated the number of trades for each address and for each pool, then aggregated by address for each AMM.
Top 100 governance token holders	• Calculated the number of governance tokens and staked version of governance tokens, where applicable, held by unique addresses for each AMM. • Divided token holdings by total supply to arrive at a percentage of ownership. • Attributed addresses using etherscan.io where data were available.

Table B-2: Pool designs and factories

Decentralized exchange	Pools (Pricing function, maximum number of tokens)*	Factory for
Uniswap	Uniswap pool (CPF, 2)	Uniswap pool
Curve	• Base pool (CSF, 2+) • Metapool (CSF, 2+)	Metapool
Balancer	• Weighted (CPF, 8) • Linear (CSF, 2) • Stable or Composable Stable (CSF, 5) • MetaStable (CSF, 2) • Liquidity Bootstrapping (CPF, 4) • Managed (CPF, 50)	• Weighted • Linear • Composable Stable • Liquidity Bootstrapping
Sushiswap	SushiSwap pool (CPF, 2)	SushiSwap pool

*The two general types of pricing functions are constant product formula (CPF) and constant sum formula (CSF).

Table B-3: Governance token distribution

Decentralized exchange	Token name	Market cap* (US$ million)	Maximum supply (million) and schedule	Initial distribution
Uniswap	UNI	3,840	1,000 2020 to 2024	60% community; 20% core team and employees; 18% investors; 2% advisors
Curve	CRV	344	3,030 2020 to 2026	57% community + 5% early users; 26% core team; 4% investors; 3% employees; 5% reserve
Balancer	BAL	200	94 2022 to ~2090†	65% liquidity providers; 25% founders, advisors, investors; 5% ecosystem fund; 5% Balancer Labs
SushiSwap	SUSHI	177	250 2020 to 2023	No allocation scheme

* As at December 31, 2022.

† Amounts issued decrease exponentially over time starting with about 7.5 million per year at launch. The amount of Balancer governance token is less than 1 in 2091, so 2090 is selected as the end date.

Table B-4: Minimum thresholds for passing various governance stages

Decentralized exchange	Minimum thresholds	Number of addresses that exceed minimum thresholds*
Uniswap	• **Off-chain vote pass**: majority with minimum 10 million UNI (1%) voting yes • **On-chain proposal or vote call**: 2.5 million UNI (0.25%) delegated to proposer • **On-chain vote pass**: majority with minimum 40 million UNI (4%) voting yes	• > 1% supply: 42 • >0.25% supply: 50 • >4% supply: 4
Curve	**On-chain proposal or vote call**: 2,500 veCRV	> 2,500: 78
Balancer	**Off-chain vote pass:** majority with quorum of 2 million veBAL	Top 5 veBAL holdings exceed 2 million
SushiSwap	**On-chain vote pass:** majority with quorum of 5 million SUSHIPOWAH (vote unit in SushiSwap)	• > 2 million xSUSHI (each equivalent to 1 SUSHIPOWAH): 2 • Top 5 xSUSHI holders exceed 50% of xSUSHI outstanding

* As at January 7, 2023, for Uniswap (see https://sybil.org/#/delegates/uniswap) and February 3, 2023, for other decentralized exchanges. Note that *ve* means vote-escrow and is the staked version of the governance token in some AMMs.

Table B-5: Use of multi-signature wallets

Decentralized exchange	Description of Multi-signature (multisig) wallet	Number of signers required for authorization / Total number of signers
Uniswap	n/a*	n/a*
Curve	Emergency DAO: Disables all functionality in Curve pool contracts except for withdrawals when there is danger of loss of funds.	5/9 signers must vote and of those who vote, there must be 59.999% support†
Balancer	Governance multisig(s): Enacts on-chain decisions such as setting and use of fees. Each chain appears to have several multisigs that perform different duties. The community can substitute signers.	6/11 on Ethereum 3/5 on Polygon, Arbitrum
SushiSwap	• Developer fund (Devfund) multisig: Controls disbursement of funds for developing the ecosystem. • Operations multisig: Makes changes within the purview of the core team.	• Devfund multisig: 4/7 • Operations multisig: 3/6

* Uniswap does not use any multisig wallets for governance.

† Curve requires 51% quorum.

Table B-6: Incentives for staking governance tokens

Decentralized exchange	Staked token	Incentives
Uniswap	UNI	n/a[*]
Curve	veCRV[†]	• 50% of all fees (trading and protocol) • Voting over pool rewards • Eligible for pool rewards as liquidity provider
Balancer	veBAL[†]	• 75% of protocol fees • Voting over pool rewards • Eligible for pool rewards as liquidity provider

SushiSwap	• SUSHI
	• xSUSHI
		• SUSHI tokens staked in SushiSwap's SUSHI-ETH pool receive 2 votes for all decisions
		• SUSHI tokens staked in SushiSwap's SushiBar address are exchanged for xSUSHI and receive:
		  • 16.7% of all fees (trading)[‡]
		  • 1 vote for all decisions

[*] Proposal to switch on protocol fees was outstanding at the time of writing.

[†] *ve* stands for vote-escrow. The basic governance token of these staked tokens is locked in escrow and can be used to vote on pool rewards. Notably, holders in vote-escrow systems that have staked their governance token receive a vote-escrow version of their governance token in return. These governance tokens are assigned voting weights that decline to zero over their staked period. There is typically a maximum staking period (e.g., one year, four years). In theory, this should help limit the concentration of voting power since it cannot be easily accumulated over time. However, highly motivated actors have done so. For example, some third-party platforms have created their own yield or earnings programs for governance tokens to incentivize holders to stake with and transfer voting rights to them.

[‡] Trading fees on SushiSwap are 30 basis points (bps). Liquidity providers receive 25bps. Liquidity providers who stake their SUSHI tokens receive the remaining 5bps in the form of xSUSHI tokens.

Table B-7: Classification of tokens with code integrity issues found across case studies

Type	Count
Honeypot[1]	3,320
Hidden mint[2]	2,791
Fake ownership renounce,[3] hidden mint	2,545
Honeypot, external contract[4]	2,254
Honeypot, hidden mint	2,162
Fake ownership renounce	1,611
Fake ownership renounce, honeypot	803
Blocklist/allowlist[5]	772
Liquidity pool block,[6] honeypot	760
Hidden fee modifier[7]	510
Fake ownership renounce, blocklist/allowlist	481
Hidden balance modifier[8]	126
Hidden mint, hidden balance modifier	125
Mint to multiple wallets during creation	104
Hidden transfer[9]	43
Honeypot, hidden transfer	27
Unassigned	19
External contract	12
Honeypot, hidden fee modifier	10
Restricted selling[10]	5
Blocklist/allowlist, fee modifier	2
Total	18,482

Source: Solidus Labs

* Types and descriptions in this table come from Solidus Labs (2023).

[1] A honeypot involves a contract that prevents token owners from selling the token after they purchase it. This causes the token price to increase, creating the appearance of a so-called mooning token. In some cases, the creator's externally owned account address or other approved addresses are granted permission to sell. To exit the scheme, the creator removes liquidity, such as by draining the funds held in the liquidity pool, or mints or sells tokens when the funds are locked in the liquidity pool.

[2] A hidden mint contract provides one or more externally owned accounts the ability to mint new tokens using a hidden function within the token contract. After calling the mint function, these accounts can dump the extra tokens in the market. This leaves the originally minted tokens that users hold worthless and drains any potential liquidity for users. Sometimes a hidden mint capability accompanies a honeypot functionality.

[3] In a fake ownership renounce, the token creator encodes the impression that they have relinquished ownership over

the contract. In reality they maintain ownership and can still call sensitive owner-only functions within the contract, such as pausing trading, minting tokens or changing fees.

[4] In an external contract transfer, functionality is implemented in a separate contract for which source code is not available. The separate contract blocks token swaps for all addresses except for the deployer address.

[5] A blocklist or allowlist contract restricts selling to specific addresses. In most instances, the deployer address is in the allowlist as the only stakeholder with the ability to sell, and any unrelated externally owned accounts or users who purchase the token are automatically or manually added to a blocklist.

[6] A liquidity pool block prevents transfers to a token's liquidity pool contract, which is a necessary step in the swap of a token. Only purchases of a token are allowed since the contract is not sent tokens in the same manner.

[7] In a hidden fee modifier, the contract allows one or more externally owned accounts to change the fee amounts collected when buying and selling a token. Updating the fee modifier can lead to users unknowingly paying disproportionate transaction fees, such as a 100% sell fee. Alternatively, the fees can be set to greater than 100% to act effectively as a token mint to the fee wallet.

[8] A hidden balance modifier contract allows one or more externally owned accounts or the contract itself to modify the balances of token holders. Setting holder balances to zero makes selling impossible. The bad actor then removes liquidity or mints or sells tokens to exit the scheme.

[9] A hidden transfer contract allows one or more externally owned accounts or the contract itself to transfer tokens from users to the bad actors' wallet.

[10] In a restricted selling, the contract allows one or more externally owned accounts to set the maximum transaction or wallet amounts to a low or zero value, which prevents selling the token.

References

Aoyagi, J. and Y. Ito. 2021. "Coexisting Exchange Platforms: Limit Order Books and Automated Market Makers." Available at SSRN: ssrn.com/abstract=3808755.

Auer, R., J. Frost and J. Pastor. 2022. "Miners as Intermediaries: Extractable Value and Market Manipulation in Crypto and DeFi." Bank for International Settlements *BIS Bulletin* No. 58.

Austin, J. 2017. "What Exactly is Market Integrity? An Analysis of One of the Core Objectives of Securities Regulation." *William & Mary Business Law Review* 8 (2): 215–240.

Avan-Nomayo, O. 2022. "Sushi DAO Votes to Send All Fees to Treasury but It Was a Fight between Whales." *The Block*, December 19. Accessed July 10, 2023. www.theblock.co/post/196213/sushi-dao-votes-to-send-all-fees-to-treasury-but-it-was-a-fight-between-whales.

Balancer Docs. n.d. "Liquidity Bootstrapping Pools (LBPs)." Accessed July 9, 2023. docs.balancer.fi/concepts/pools/liquidity-bootstrapping.html.

Balancer Docs. n.d. "Multisig." Accessed July 9, 2023. docs.balancer.fi/concepts/governance/multisig.html#the-multisigs-and-their-addresses.

Barthere, A., B. Beraki, Y. Khoo, P. Grushyn, X. Lim and J. Ho. 2022. "On-Chain Forensics: Demystifying TerraUSD De-peg." Nansen.

CSA (Canadian Securities Administrators). 2020. "Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets." Staff Notice No. 21-327, January 16.

CSA. 2023a. "Crypto Asset Trading Platforms: Pre-Registration Undertakings — Changes to Enhance Canadian Investor Protection." Staff Notice No. 21-332, February 22.

CSA. 2023b. "Crypto Asset Trading Platforms: Terms and Conditions for Trading Value-Referenced Crypto Assets with Clients." Staff Notice No. 21-333, October 5.

CSA and IIROC (Investment Industry Regulatory Organization of Canada). 2021. "Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements." Joint CSA/IIROC Staff Notice No. 21-329, March 29.

Capponi, A. and R. Jia. 2021. "The Adoption of Blockchain-based Decentralized Exchanges." arXiv preprint, arXiv:2103.08842.

Chainalysis. 2023. "24% of New Tokens Launched in 2022 Bear On-Chain Characteristics of Pump and Dump Schemes." February 16.

Copeland, T. 2022. "Binance Didn't Intend to Delegate 13 Million UNI Tokens, Says CEO." *The Block*, October 20. Accessed July 10, 2023.

Daian, P., S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach and A. Juels. 2019. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges." arXiv:1904.05234.

Dhawan, A. and T. J. Putniņš. 2022. "A New Wolf in Town? Pump-And-Dump Manipulation in Cryptocurrency Markets." *Review of Finance* 27 (3): 935–975.

Edmans, A. 2014. "How Should CEOs Be Paid?" World Economic Forum *The Agenda*, November 13. www.weforum.org/agenda/2014/11/how-should-ceos-be-paid.

Ethereum. n.d. "Decentralized Autonomous Organizations (DAOs)." Accessed July 9, 2023. ethereum.org/en/dao/#what-are-daos.

Faverio, M. and O. Sidoti. 2023. "Majority of Americans Aren't Confident in the Safety and Reliability of Cryptocurrency." Pew Research Centre, April 10.

Fender, I. and U. Lewrick. 2015. "Shifting Tides—Market Liquidity and Market-Making in Fixed Income Instruments." Bank for International Settlements BIS Quarterly Review (March). https://www.bis.org/publ/qtrpdf/r_qt1503y.htm.

Flashbots Transparency Dashboard. n.d. "Flashbots Transparency Dashboard." Accessed July 14, 2023. transparency.flashbots.net.

Frankel, A. 2022. "Novel Action Against Ooki Crypto Collective Draws Rebuke from Commodities Trading Commissioner." Reuters, September 23.

Foxley, W. 2020. "Hayden Adams: King of the DeFi Degens." *CoinDesk*, December 8.

IOSCO (International Organization of Securities Commission). 2022. *IOSCO Decentralized Finance Report*. Madrid: IOSCO, March. http://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf.

IOSCO. 2023. *Final Report with Policy Recommendations for Decentralized Finance (DeFi)*. Madrid: IOSCO, December. http://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf.

Kelly, L. 2022. "How Balancer DAO Achieved Peace with a Clever Whale Named Humpy." *Decrypt*, December 19. decrypt.co/117590/how-balancer-dao-achieved-peace-with-a-clever-whale-named-humpy.

Lehar, A. and C. Parlour. 2021. "Decentralized Exchange: The Uniswap Automated Market Maker." Available at SSRN: doi.org/10.2139/ssrn.3905316.

Mohan, V. 2022. "Automated Market Makers and Decentralized Exchanges: A DeFi Primer." *Financial Innovation* 8 (20). doi.org/10.1186/s40854-021-00314-5.

Morrow, A. 2023. "Sam Bankman-Fried Found Guilty of Seven Counts of Fraud in Stunning Fall for Former Crypto Billionaire." *CNN*, November 2, 2023. https://www.cnn.com/2023/11/02/business/ftx-sbf-fraud-trial-verdict/index.html.

Ontario Securities Commission (OSC). 2023. *Crypto Asset Survey 2023*. Final report, November 29. https://www.osc.ca/sites/default/files/2023-12/inv-research_20231129_crypto-asset-survey-2023.pdf.

Solidus Labs. 2023. "The 2023 Crypto Market Manipulation Report Series." https://www.soliduslabs.com/reports/2023-crypto-market-manipulation-report.

Sushigov.eth. 2022. "Sushi Legal Structure [Implementation]." *Snapshot*, October. Accessed July 10, 2023. snapshot.org/#/sushigov.eth/proposal/bafkreibawm6u4tsq4e5lqwz5yo3rg2k4p6upg5eqaeen33ghmuwxttiaqm.

Sushiwap Docs. 2023. "Token Listings & Partnership Requests." May 4, 2023. https://docs.sushi.com/docs/Ecosystem/Token%20Listings%20&%20Partnerships.

The Block Research. 2022. *2023 Digital Asset Outlook*. https://www.theblock.co/post/196671/2023-digital-asset-outlook.

Uniswap Labs. 2020. "Introducing UNI." Uniswap Labs Blog, September 16. blog.uniswap.org/uni.

Heimbach, L., Y. Wang and R. Wattenhofer. 2021. "Behavior of Liquidity Providers in Decentralized Exchanges." arxiv.org/abs/2105.13822v1.

Zetzsche, D. A., R. P. Buckley, D. W. Arner and M. van Ek. 2023. *Remaining Regulatory Challenges in Digital Finance and Crypto-Assets after MiCA*. Report provided to the European Parliament Committee on Economic and Monetary Affairs (May). https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740083/IPOL_STU(2023)740083_EN.pdf.

0xMaki.eth. 2021. "oSushi [SIGNAL]." *Snapshot*, August. Accessed July 10, 2023. snapshot.org/#/sushigov.eth/proposal/QmfEqngSUDtZHgQf5U9wEpkskwK38zWKbyEeWp3pfz2hPE.