A 2022 PRIMER FOR CRYPTO-TRADING

JUNE 2022

Author: Andreas Park, *Research Director, Rotman FinHub, University of Toronto*

GLOBAL RISK INSTITUTE

A blockchain's core function is storing, processing, and transferring digital value, and the ability to exchange tokens is a central function of these networks. In this paper, I review the different forms of trading blockchain tokens to provide clarity on the tools and processes available and to highlight the risks and opportunities in this space.

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

CENTRALIZED TRADING PLATFORMS

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

There are two main types of centralized exchanges: crypto-only and fiat connected ones. Namely, some crypto exchanges are connected to the payments' rails of traditional finance; examples are Coinbase, Upbit, FTX, Kraken, and Bitbuy, and Figure 1 shows the monthly trading volumes measured in USD that these venues processed in the last few years.

However, most crypto exchanges are not directly connected to the world's traditional payments networks, and they are, therefore, not directly connected to the traditional world of finance. Examples for these markets are Poloniex, Binance, OKEx, Huobi, or Kucoin, and Figure 2 displays their trading volume over the last few years. What is remarkable is that these venues process more than twice the volume of the fiat-connected venues.

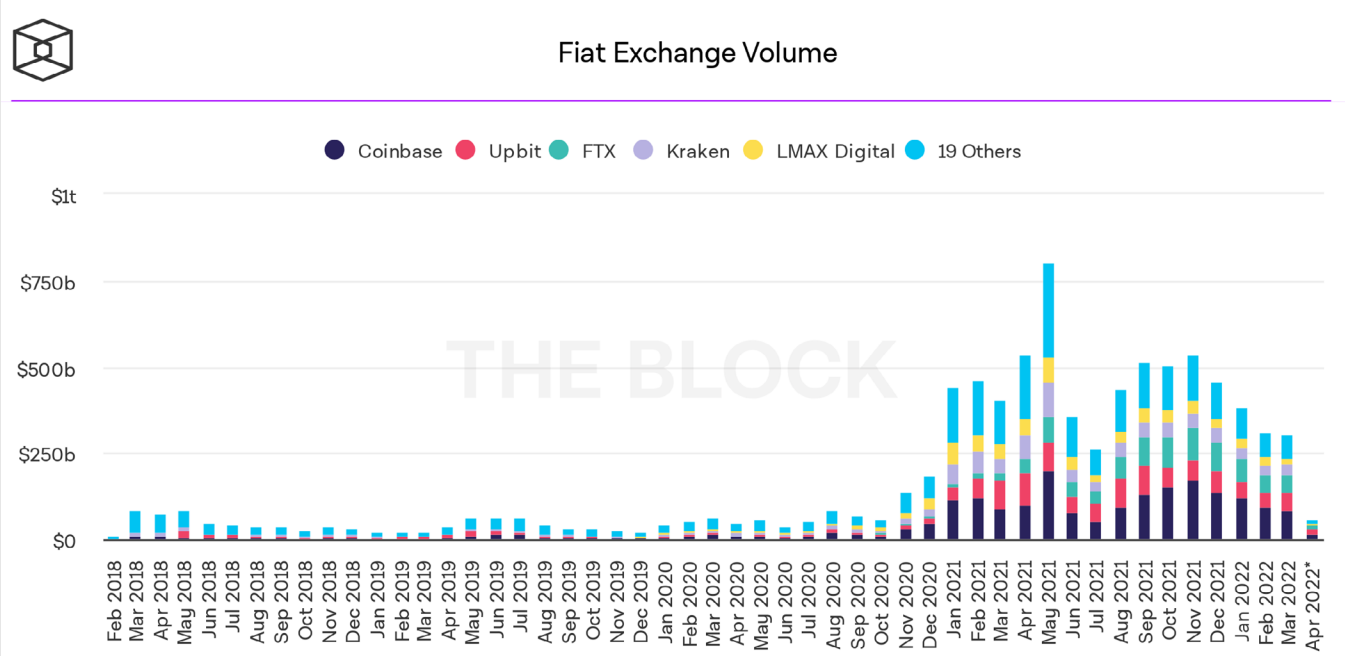
For venues that are connected to the payments network, users can fund their account by wiring fiat currency to the exchange, similar to what one would do when opening an account with a traditional investment brokerage. Crypto-only venues do not accept wire transfers, although some allow users to fund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

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

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

On fiat-linked venues, users can trade crypto assets directly against fiat currencies whereas, on crypto-only platforms, all trades are between crypto assets. Most commonly, however, one of them is a *stablecoin*, a digital representation of a fiat currency such as the US dollar; examples for stablecoins are USDT (issued by Tether Inc.) or USDC (issued by Circle Inc.). Notably, Ontario-based platforms are currently not allowed to facilitate trades with stablecoins.

Figure 1: Evolution of Trading Volume for Centralized, Fiat-Linked Crypto-Exchanges



Source: *CRYPTOCOMPARE Updated: April 6, 2022*

Crypto-Venue Custody. To trade on a centralized venue, users must first register with the platform, which now almost always involves a KYC process that requires a photo, government-issued ID and a proof of residency.

Wallets. On public blockchains, crypto-asset ownership is associated with a public address, similar to an account number. The public address is derived from the public key which is generated from a private key as part of public-private key cryptography. The private key controls the crypto-assets and is used to sign transactions. A wallet is a software tool that stores private keys and enables the signing of transactions. There are many forms of wallets, the most common being browser plugins or smartphone apps. The terms "wallet" and "public address" are often used interchangeably, though technically a single wallet can handle many addresses. When the user controls the private keys, a wallet is referred to as *self-custody.*

To use a crypto asset at a centralized exchange, users need to transfer the asset to the exchange. To facilitate this operation, centralized exchanges issue its users a unique public address, but the custody of the private keys for this address rests with the exchange. These public addresses are, therefore, also referred to as *custodial wallets* because the exchange has custody of the private keys.

After a user transfers crypto assets to their exchange/custodial wallet, there is usually a second step whereby the assets are transferred from the custodial wallet to one of the exchange's omnibus wallets. After that, all transactions and transfers are recorded only in the exchange's own siloed system and not on the blockchain. For this reason, assets in omnibus wallets are often referred to as "off chain." Since trades are arranged and recorded on the exchange's proprietary infrastructure, these venues are referred to as *centralized*.

Fees. Deposits and withdrawals from centralized exchanges involve fees, and these can be substantial, particularly in Canada. For instance, Interac transfers in and out of Canada's first regulator-approved venue, Bitbuy, cost 150 basis points, wire transfers cost 50 basis points, and withdrawals to the Ethereum blockchain cost around $15-$20, depending on the price of the cryptocurrency ETH. (The native cryptocurrency of Ethereum)

Token Listings. The centralized exchanges decide for which tokens they enable trading on their platform. Using Bitbuy as an example, users can trade sixteen of the many thousands of blockchain tokens that are in circulation. For crypto projects, exchange listings can be important to create liquidity for their projects and to enable users to obtain their tokens. Some, though not all, exchanges (e.g., Binance) charge token-issuers a substantial fee for enabling the trading of a token.

Custody Risk. Legally and functionally, using a centralized exchange requires a transfer of custody of the crypto assets from the user to the exchange. In a sense, a centralized crypto exchange is therefore closer to an investment broker than a stock exchange because the latter never handles assets directly.

Almost all centralized crypto-exchanges are startups that operate on shoe-string budgets. As "children" of the 2017-18 crypto boom, they grew fast and were riddled with problems. Keeping tokens at an exchange proved to be risky, as demonstrated by the numerous hacking, fraud, and theft scandals such as Mt. Gox, QuadrigaCX, or Thodex. Notably, even the biggest brand in crypto-trading, Binance, has been hacked repeatedly.

Moreover, it is often unclear how crypto exchanges handle assets in their omnibus wallets, if users have real-time 365-24-7-access, and if exchanges separate their own assets neatly from their customers'.

Crypto Wash Trading. There are numerous websites that publish information about the trading activities at the various crypto trading venues. Since liquidity begets liquidity, venues that want to attract users may be tempted to overstate their volume. Wash trading is one practice that, allegedly, many crypto exchanges either directly engaged in, or at least tolerated to create fake volume. Cong et al (2022) report that up to 70% of the volume on unregulated crypto exchanges was fake, although they also report that regulated venues, such as Coinbase and Kraken, did not engage in such behaviour.

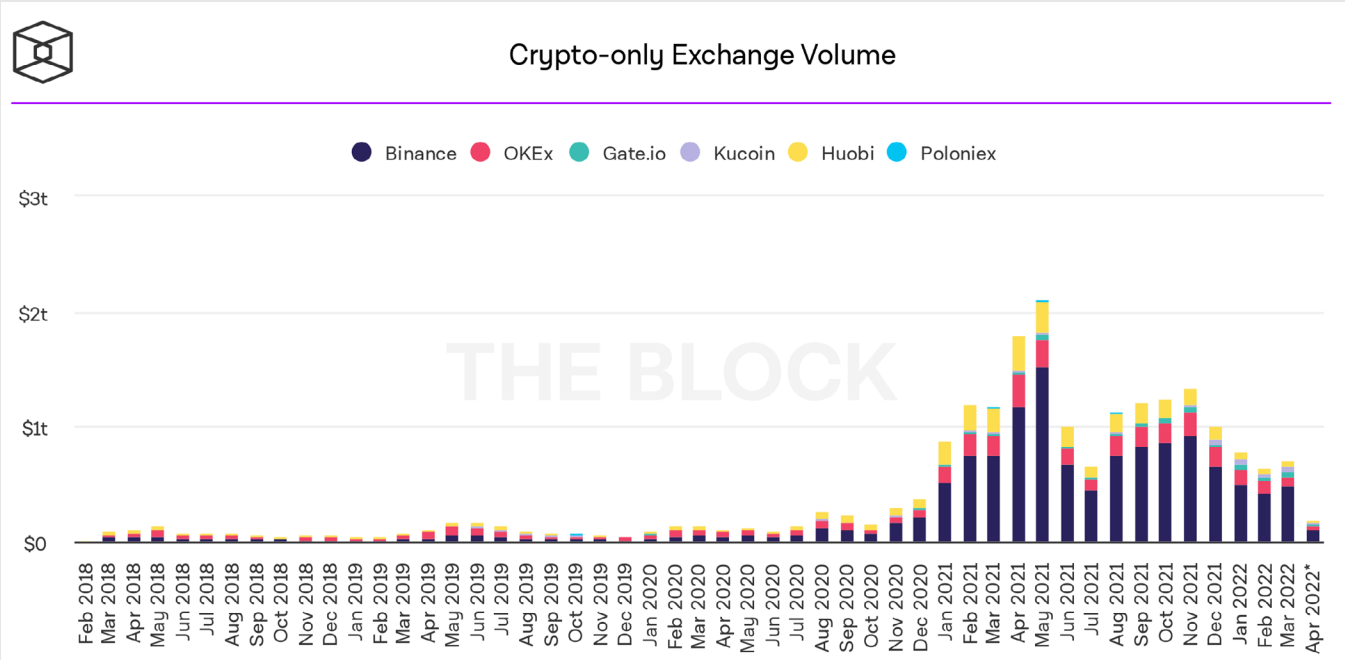
Price Manipulations. Another concern relates to the general propensity of price manipulations at venues that have no regulatory oversight. One alleged scheme involves the stablecoin issuer Tether and is part of the lore on the backing (or lack thereof) of the stablecoin USDT. The premise of USDT is that each token is backed by a USD or cash equivalent in a bank account, but for years Tether refused having their books audited. Tether issues coins using the exchange Bitfinex, a crypto-only venue. Griffin and Shams (2019) document, however, that USDT issuances were not followed by subsequent fiat outflows, raising the question as to the source of the funds to back these newly-issued coins. Moreover, they show that, instead, USDT issuance curiously coincides with massive price rises in Bitcoin's price. In other words, it appears that USDT issuance may well have been used to pump up the price of Bitcoin.

Pump-and-Dumps. One common allegation in the crypto world is that there are plenty of pump and dump schemes. Indeed, as Li, Shin, and Wang (2021) document, there are Telegram groups, open to anyone (but also with a premium subscription), that coordinate pump-and-dump activities of particular coins on selected exchanges.

The above developments related to wash trading, price manipulations, and pump-and-dump attacks were all documented during the 2017-2018 boom, and boom-times are often rife with shenanigans. A case in point is the 1999 Dot-com Boom which had its fair share of scams, frauds, and unethical behaviours – often facilitated by the world's most prestigious financial institutions under the watchful eyes of powerful regulators.

Tax Loss Harvesting: The latest trend, documented in Cong et al (2022), is tax loss harvesting: using trading strategies and crypto assets, such as specialized non-fungible tokens (NFTs), investors can create capital losses that they can use to offset capital gains. In traditional markets, a capital gain arises when a trader locks in the price appreciation of a firm's stock, presumably obtained because the firm retained and

Figure 2: Evolution of Trading Volume for Centralized, Crypto-Only Exchanges



Source: *CRYPTOCOMPARE Updated: April 6, 2022*

reinvested its earnings. Governments contributed to enabling these earnings by providing infrastructure, education, security, et cetera, and so it is fair that some funds flow back to the public when the firm and its investors do well. Many tokens, on the other hand, have explicitly no relation to economic activity, nor do they serve any economic purpose. One example is the Shiba-Inu coin, which its creator invented as a meme. Yet capital gains from trading these tokens fall under tax law just as much as cap gains from mining or banking stocks. Tax loss harvesting turns the law against the government in that specially-designed crypto-assets, or strategies that also fit the current law, create made-up capital losses that offset capital gains. One can argue that governments that seek to collect rents from hot potato, trading-induced, made-up price rises of meme coins also must accept equally made-up losses – but in some jurisdictions, losses can offset gains in traditional markets. With the large losses in the crypto markets in 2022, I predict that we will see fierce taxation-related discussions in 2023 and beyond.

Regulations and Reach. The above discussion has indicated that there are numerous problems and concerns regarding centralized crypto exchanges: they hold assets in custody, and investors therefore have the reasonable expectation that their funds are available when they want them. But are they?

During the May 2022 crypto crash, Coinbase revealed that they are not always separating their own and their customer funds, exposing their customers to loss of funds should Coinbase go bankrupt. Is this a risk that customers can be expected to accept?

Crypto exchanges operate a trading platform of items that often look like securities, and investors may reasonably expect orderly, non-manipulative conduct. Are exchanges enforcing orderly conduct and, if so, how?

Centralized exchanges make listing decisions and often charge substantial fees for listings. They also invest in the crypto assets that they list, and such investments are not always transparent. One can argue that a listing decision endorses a crypto asset

as an investment vehicle. Yet charging for listings and making investments, while creating trust for investors, possibly creates substantial conflicts of interest that are rightfully regulated in traditional financial markets.

Lastly, centralized exchanges are important on-and off-ramps from the crypto world to the traditional world of finance. Therefore, do they have to abide by the same Know Your Client (KYC) rules as traditional financial institutions?

Let me also outline the perspective of crypto exchanges. Blockchains are borderless by design and aim to serve a worldwide clientele. In principle, crypto exchanges can, and want, to serve a worldwide clientele, too. There are many regulators in the world, often with idiosyncratic, conflicting requirements. Dealing with one regulator usually ties up several lawyers for months, and there are many regulators in the world. Therefore, worldwide compliance is costly.

In practice, threats of regulatory action have prompted many venues to exclude users from countries or regions such as Canada/Ontario and the U.S., e.g., by blocking IP addresses or requiring proof of residence in a non-blocked country. For many Ontario-based Binance users, this allegedly led to the unfortunate situation where they lost all access to their crypto-assets in early 2022 after threats and pressure by the OSC.

And yet excluding investors from troublesome regions may still not be enough: the Securities and Exchange Commission (SEC)'s chairman, Gary Gensler, has stated publicly that, because users can find ways to circumvent its self-protective measures, an exchange can still fall under the SEC's jurisdiction. Therefore, even with the best intentions and with solid, well-thought-out systems, it is expensive and risky for a crypto exchange to serve a worldwide audience. They can be in legal jeopardy even if they never did harm.

Notably, in the mid-1990s, with the advent of the internet, U.S. policy makers took a very different, bi-partisan approach towards regulating internet start-ups: first and foremost, do no harm. Arguably, this attitude helped create Silicon Valley, the world's leading region for digital economy innovation.

An Outlook for Centralized Exchanges. Going forward, the likely best scenario for centralized venues is one where we see consolidation in the centralized venue space: a few international brands will remain and service a possibly worldwide clientele. Their pockets are deep enough to make it worth their while to absorb the compliance costs from satisfying the big countries' regulators. Alongside these big brands, we will see smaller venues that only serve a clientele in their national jurisdiction and deal only with a single regulator. These will be the jurisdictions that are too small, and insignificant, for the large exchanges to deal with, and the large brand venues may simply exclude users from these countries.

Personally, I would find such an industrial organization problematic because it is concentrated and has large institutions that may become systemic points of failure, and because residents of smaller countries are missing out on opportunities. The big question is whether the benefit of the regulation is worth the cost of the risks and missed opportunities that it creates. We take regulation of the existing world as given. But the emergence of a new eco-system like DeFi provides opportunities to rethink processes and rules to address and find an acceptable level of risk and cost of regulations.

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

This scenario brings me to the second part of this paper.

DECENTRALIZED TRADING

It's ironic that, until recently, the trading of deliberately borderless, *de*centralized digital items could only be exchanged in *centralized* venues. Although blockchains can facilitate the exchange of crypto assets, a blockchain is not a marketplace. It is possible to organize crypto-asset trading on a blockchain, similar to a traditional stock market, by registering limit orders as a "smart contract." But – this approach is not practical because each new limit order submission costs a fee to blockchain validators. Unexecuted orders also waste resources as all 10,000+ nodes must process the order. The volume of trades on decentralized crypto exchanges has increased since the summer of 2020 (Figure 3).

That's why trades of blockchain-based items or tokens most often occurred on centralized, "off-chain" exchanges, thus reducing the blockchain to just yet another settlement infrastructure.

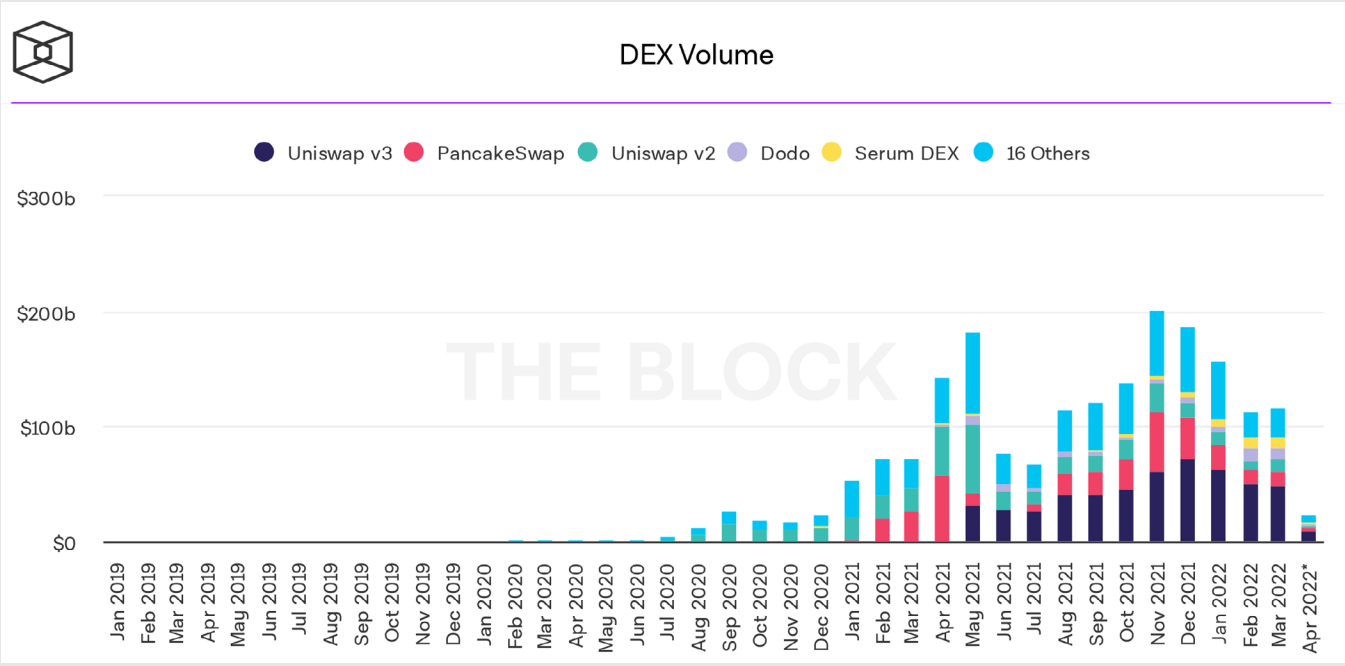
Automated Market Makers. However, matters changed by mid-2020 with the development of so-called Automated Market Maker (AMM) systems, a novel trading process that uses the blockchain's inherent ability to process code. Leading protocols, such as UniSwap, SushiSwap, and PancakeSwap, have seen tremendous user uptake and now process billions of dollars worth of transactions every day, often more than the largest centralized exchanges, Binance and Coinbase.

AMMs are interesting, beyond their user uptake, because they contain several novel institutional arrangements. First, an AMM is merely a "smart contract", a piece of code that is registered on a public blockchain. Once deployed, this code is accessible by anyone who has access to the blockchain for as long as the blockchain itself exists. The code is operated by the blockchain validators who follow the protocol, and not by the entity that has submitted it.

Changes to the code are usually governed by a so-called Decentralized Autonomous Organization (DAO), and governance is DAO-token based, blockchain-organized voting that can affect only a very limited set of contract parameters.

These tokens are often used in many ways. For instance, sometimes users of a protocol get rewarded with DAO tokens. That's as if Canadian Tire rewards its customers with its stock. DAO token holders sometimes receive a share of the fees that the protocol generates.

Figure 3: Evolution of Trading Volume for Decentralized Crypto Exchanges



Source: *COINGECKO Updated: April 6, 2022*

Overall, the arrangement presents many challenges for interested investors and regulators. When is a DAO token a security? When it is, who is responsible for reporting and compliance once the token has been issued and the protocol has been deployed? Who is liable if something goes wrong? What's the value of voting?

AMM Trading. The AMM trading process itself has several interesting trading-related features, too. First, AMMs combine or pool liquidity so that liquidity providers do not compete for order flow, a stark contrast to stock exchanges where proprietary trading firms make billion-dollar investments to gain nano-second speed advantages. This setup allows retail investors to earn passive income from contributing their assets to a liquidity pool because providing liquidity does not require specialized skills or expensive equipment. Second, AMMs do not directly rely on a market mechanism that equilibrates demand and supply and determines an order's cost, but instead use a hard-coded pricing rule, thus creating a constraint against which users optimize. Third, the pricing function employed by almost all AMMs has never been used in traditional financial markets (to the best of my knowledge). Therefore, this novel setup raises questions about the functioning of these markets, the informational efficiency of prices, and the possible emergence of arbitrage.

How do AMMs work? A swap exchange creates a liquidity pool by combining deposits of pairs of tokens A and B from liquidity providers. To provide liquidity, a user transfers a set quantity of both tokens to the AMM smart contract (usually, the user will receive a receipt token in return that they can then use in other applications, e.g., as collateral for a loan). A liquidity demander can trade against this pool by sending one type of token and receiving the other token in an atomic swap. A pricing rule determines the exchange rate of tokens. The objective of the rule is to keep the pool's liquidity invariant in the sense that, when a liquidity demander removes one type of token from the pool, they must deposit a quantity of the other type of token such that the aggregate liquidity of the pool defined by a "bonding curve" remains unchanged.

Although there are theoretically endless options for bonding curves, almost all AMMs use the same functional form that I illustrate in Figure 4. This bonding curve is referred to as a "constant product" pricing rule. The concept is best explained formally. Suppose the asset pool contains X units of token A and Y units of B. The ratio Y/X is the implicit marginal price of an A token measured in B tokens. If the B token is a stablecoin, i.e., a digital representation of a fiat currency, then the exchange rate Y/X is the cash price of an infinitesimal amount of A tokens. Under constant product pricing, liquidity c is determined by the bonding curve $c=X.Y$. The number Q of A tokens that a buyer receives for P of the B tokens must be such that the liquidity level remains invariant: c=(X-Q).(Y+P).

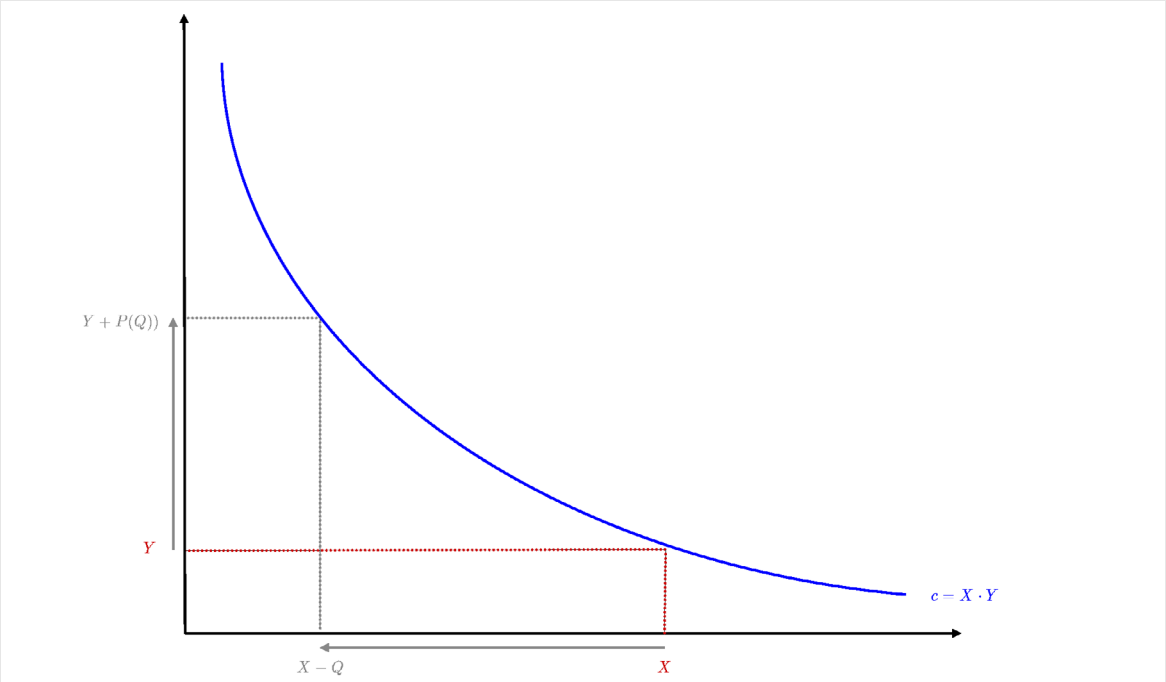
Let's look at some concrete numbers: At the beginning of February 2022, the UniSwap (V2) token pair ETH and USDC (a digital representation of the US dollar) contained approximately 38,100 ETH and 118M USDC; the implied marginal price of 1 ETH was thus around $3,097. A liquidity demander who wants to buy 100 ETH from this contract would pay approximately $3,105 per ETH.

The Problem: Sandwich Attacks. Suppose a speculator manages to inject a same-sized trade before this 100 ETH trade and then reverses it immediately after the original trade. What would this speculator earn from "sandwiching" the original trade? The initial trade would cost the speculator $3,105 per ETH, and reversing the trade yields $3,121 per ETH, for a total profit of $1,639 - value extracted from the original trader. Although this is a lot of money, for this $311K trade, it is only a 5 basis points excess cost that may be bearable. But it gets worse: had the attacker submitted a "sandwiching" trade of 1,000 ETH, the value extracted would be almost $17K, and had they attacked with a trade for 10,000 ETH, it would have been $261K.

This problem is pervasive: as I show in a recent research paper (Park 2022) for a general class of pricing functions that are based on liquidity invariance (such as the constant product rule), under a mild convexity assumption, these sandwich attacks are profitable for any trade (modulo fees), and the attacker's profits are unbounded.

The next question is how an attacker can find a sandwich-able trade. The answer lies in the inherent transparency of blockchain transaction processing. Namely, signed and processed blockchain transactions wait in publicly visible "mem-pools" for validators to include them in a block.

Figure 4: Illustration of an Automated Market Maker Bonding Curve



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

A front-runner can always add a new pair of transactions to the mem-pool to sandwich a trade. Crucially, the trade price is not fixed when it is submitted, nor when it is added to the mem-pool. What determines the price of a trade is the pool's liquidity at the precise time when a validator processes it within a block. A trade's cost thus depends even on its position within a block, which allows a sandwich attack to be successful and profitable. Figure 5, reproduced from my paper, illustrates the mechanics and different steps of a sandwich attack.

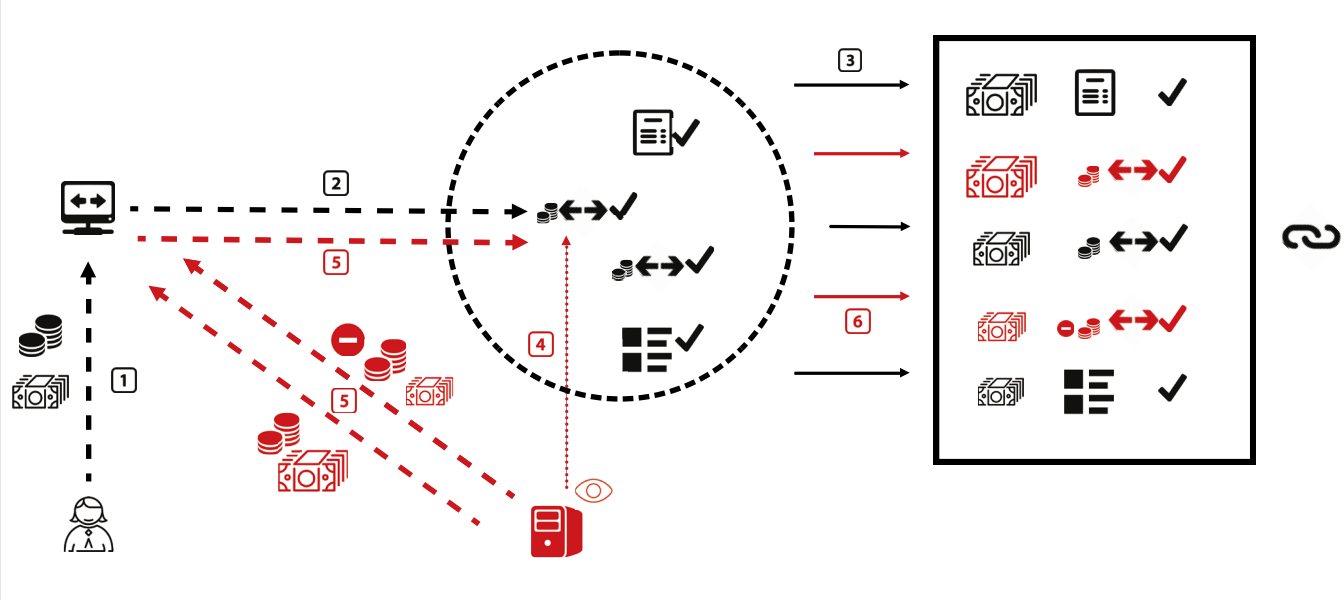
The Flashbots[1] protocol documents that traders have lost over $600M in these and related attacks over the last two years. Park (2022) provides an illustrative, real-world example from the Ethereum blockchain for one such attack. The problem is pervasive.

Technological Solutions. There are several examples of technological solutions that seek to address sandwich attacks. The first is the approach taken by the aggregator protocol 1Inch, which does not allow one to submit opposite-direction trades for some time after a trade has been submitted. A sandwich attacker would want the return leg of a sandwich trade to be executed right after the sandwiched trade. Since the attacker must wait, the profits from the return leg are uncertain, which is a significant disincentive.

A second approach is the Flashbots mining protocol: validators that follow the protocol receive AMM trades "privately," and they commit to not include them in the public mem-pool and not to front-run them. Users can connect their wallet to this protocol and when they use

1 https://explore.flashbots.net/

Figure 5: Illustration of a Sandwich Attack



The possibility of front-running is an intrinsic feature of blockchains. The schematic works as follows. A user who wants to perform a swap transaction submits the tokens she or he desires to exchange to the constant product market making contract (1). The contract submits an atomic swap to the blockchain network, and upon verification this transaction enters the mem-pool (2). Verified transactions get ordered in a block based on the fees that they offer (all else equal) (3). An attacker (likely a bot) observes the mem-pool and sees a transaction that can be front-run profitably (4). The bot sends two off-setting swap transactions to the contract, when the front-running trade has a higher fee than the original, front-run transaction (5). In the block, the transactions now get re-ordered according to their mining fees and, upon inclusion on the chain, the transactions in the automated market making contract are executed in the order of the fees (6).

an AMM, their trade would be submitted only to miners who follow this protocol. However, Agostino et al (2022) show that the approach is not bullet-proof either, and that attackers even submit their sandwiched trades, using this protocol, to protect themselves from attacks.

Economic Solutions. In practice, users can blunt the impact of sandwich trades via a built-in feature of many systems whereby traders can limit the price impact or "slippage" of their trade. The trade will not go through if its price impact exceeds a threshold.

Using this feature is, in fact, crucial because, for the common pricing rule, sandwich attack profits are theoretically unbounded.

Although limiting slippage may help prevent bad cases of front-running, there are practical concerns. First, users need to understand how much their trade moves prices naturally because of the shape of the pricing function. If they set a limit that's too conservative, their trade cannot go through. They also need to account for the possibility that the price moves, even in the absence of front-running, before validators include their trade. By being too cautious, a trader may have to resubmit their trade multiple times. This process can be costly because a validator can include a trade in the block and collect the gas fees even when no tokens change hands (e.g., the contract fails because the price impact or "slippage" was too large). In other words, a trader may have to pay gas fees even if the transaction does not go through.

Table 1: Comparison of centralized and decentralized exchanges

	centralized exchanges		decentralized exchanges (automated market makers/swap exchanges)
	fiat-connected	crypto-only	
wallet	custodial		non-custodial (full user control)
hacks	significant		none
wash trading	low	medium to high	Unknown
fiat deposits	yes	no	no
KYC	yes	usually	no, access direct from pseudonymous wallet
trading fees	maker-taker, bid-ask spreads		LP demander to supplier, slippage
withdrawal/deposit fees	significant		none
gas fees for trading	none		yes
token listings	often regulator-approved	controlled	In principle unrestricted
ownership/governance	domesticized corporations		decentralized autonomous organizations
traceability	within-system traceability, flow through payments follow AML rules		full traceability of movements between pseudonymous wallets
AML enforcement	as per host country's rules		none, but full traceability

Finally, limiting slippage alone cannot prevent sandwich trades altogether because a front-runner can still attack with a trade that maxes out the slippage that the original trader allows.

Role of AMMS in DeFi. AMMs play an important role in the DeFi eco-system: as Lehar and Parlour (2022) show, AMMs are often used in the strings of transactions that are needed for the liquidation of DeFi loans that breach a collateralization bond. These multistep transactions, which also often involve so-called Flashloans, are one of the reasons why DeFi holds such promise to yield a more efficient financial system.

Well-functioning AMMs are, therefore, crucial for the long-term viability of the DeFi ecosystem.

Initial DeFi Offerings (IDOs). Recently, AMMs, particularly PancakeSwap, have been used to issue new tokens in so-called Initial DeFi Offerings (IDOs). These offerings solve the problem of having to find a distribution mechanism or having to set up a separate website. Instead, an issuer creates a token pair, and investors simply trade this pair using the established AMM mechanism. This feature implies that anyone can "list" a token on an AMM simply by creating a token pair.

Frauds. Investors are used to trading crypto assets by ticker symbol, but these symbols are not unique or protected. A general problem is that scammers can create a fraudulent token that "impersonates" the symbol of a popular coin. Scammers can then set up a trading pair on an AMM using this scam token and invite investors to buy the scam token. Although this issue is not widespread, it does occur as Lehar and Parlour (2021) document in their paper.

Manipulation. There is not much academic work on wash trading or price manipulations on decentralized exchanges. Clearly, both these activities are possible. The purpose, however, is unclear: Centralized venues engage in wash trades to pump up their volume. But traders care about liquidity, and for AMMs, volume is not synonymous with liquidity. Rather, AMM liquidity is directly measurable and visible. Furthermore, there are numerous aggregator protocols that optimize liquidity demand. Liquidity providers can also add and withdraw liquidity instantaneously. Using wash trades to attract future volume therefore appears pointless. IDO issuers, of course, want to manipulate the price of their issue to ensure a stable price. I am not aware of research that studies price manipulations on decentralized venues.

Summary Comparison of centralized and decentralized exchanges. Table 1 briefly summarizes the differences between the different types of exchanges along important dimensions such as types of access, KYC, manipulations, AML enforcement, listings, and ownership.

Summary and Outlook. A blockchain itself is a value transfer infrastructure, not a marketplace. Centralized exchanges create the market for token exchange, and they are therefore an important ingredient in the crypto-ecosystem – for now. Yet they also present significant problems and challenges and, seemingly, every crisis in the crypto markets uncovers more concerns. Conceptually, they are no longer necessary, and decentralized trading facilities are becoming increasingly liquid and convenient. It is possible to envision a future in which centralized exchanges no longer exist. Instead, crypto trading in the future may occur exclusively on-chain.

Arguably, traditional financial institutions would be better suited to serve the role of on- and off-ramps for crypto-users and investors, provided governments have the vision to develop ways for FIs to engage, to develop digital ownership, and to establish fail-safe systems.

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

For all the issues that I identified with decentralized trading, blockchain-based trading has enormous promise. Recent developments in so-called optimistic rollups may solve many of the issues around AMMs, and they may also enable the same trading options that venues such as Binance offer without increased security risks and without the costs of regulatory oversight.

A key innovation of AMMs is that they are a novel approach to liquidity provision, where lack of liquidity is one of the biggest problems that plagues securities markets for most assets. Lack of liquidity makes trading more expensive and raises the risk of not finding a counterparty, making it harder for investors to adjust their risk exposure. This makes it harder for issuers to raise funds and reward and motivate employees with stock options. A key innovation of automated market makers is the pooling of liquidity, which could improve the situation, particularly for less liquid investments, and lead to much better capital markets.

References

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

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

Park, Andreas, The Conceptual Flaws of Decentralized
Automated Market Making (August 18, 2021). SSRN: https://ssrn.com/abstract=3805750

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

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

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

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