CAPCO

DEFI EXPLAINED

THE CASE OF DECENTRALIZED EXCHANGES

IN COOPERATION WITH

ABC RESEARCH

Austrian Blockchain Center

a wipro company

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Promising to enhance access and efficiency within financial services, Decentralized Finance (DeFi) has gained significant attention – and some traction in the marketplace – in recent years. In essence, DeFi uses secure distributed ledger/blockchain technology to facilitate peer-to-peer financial transactions, including borrowing, lending and trading.

DeFi seeks to disintermediate and decentralize the traditional financial services industry by automating complex financial processes. The functional roles of trusted third parties such as brokerage firms, banks, and other centralized financial institutions, are replaced by smart contracts – simple, self-executing programs that automatically carry out those functions.

Although from a big picture perspective DeFi is still a niche phenomenon whose long-term impact on the financial services industry is yet to be ascertained, that potential for disintermediation means it is important that established financial institutions understand how it might reshape the operational landscape and how they might themselves embrace the concept of decentralization.

Certainly, a major market correction is currently underway in the digital assets space. That said, the ongoing travails of DeFi challengers present an opportunity for traditional financial institutions to become more active in the space, stepping in to offer robust solutions that draw upon on their core strengths of security and trust.

To this end, this paper aims to support practitioners in two ways: first, we offer an overview of DeFi, its promises and key foundational principles to provide a broad framework to support firms as they assess the DeFi phenomenon. Second, we deep dive into one of the most promising areas of DeFi – Decentralized Exchanges (DEX) and the perceived benefits of DEXs over the more liquid centralized exchanges on which the majority of digital assets are currently traded.

1. WHAT IS DECENTRALIZED FINANCE?

At its core, DeFi aims to provide financial products and services based on blockchain technology. The term is used rather broadly to describe the decentralized applications (DApps) providing the necessary business logic for transactions as well as the underlying blockchain networks and digital assets. The combination of decentralized, smart-contract-based business logic solutions with a blockchain-based settlement layer facilitates the creation of financial services in a decentralized way.

In contrast to what their name implies, smart contracts are neither smart, nor are they contracts in a legal sense. Rather, smart contracts are executable code stored on layer 1 blockchain protocols like Ethereum. These small software applications are used to automatically execute program logic or rules written in the code. If the conditions of the smart contract are fulfilled, the code will self-execute its set of instructions. With no institution needed to execute the business logic, this enables participants to execute transactions in a 'trustless' environment.

In the DeFi world, intermediaries are replaced through a set of automated smart contracts. Functional roles of trusted third parties such as brokerage firms, banks, and other centralized financial institutions, are replaced by smart contracts which fulfil these functions automatically. In this sense, DeFi (similar to other DLT based use cases) seeks to disintermediate and decentralize the traditional financial services industry.

There is already a broad range of financial services or products available in the DeFi space including trading, lending, investing, deposits, and payments services. Furthermore, decentralized applications are highly modular. This means, that very often they can be combined and are interoperable to create new applications.

DeFi's rise in popularity can be partly explained by real and perceived structural issues with the current financial services industry. DeFi arose out of a desire to free financial services from the control of centralized institutions and governments thereby providing financial inclusion for more people. Proponents of DeFi argue that traditional financial services are dominated by large institutions and often characterized by tightly controlled access, leading to organically grown inefficiencies, high and opaque fees as well as financial exclusion. In addition, they point to the high level of regulation fostering an environment that is generally hostile to disruptive technologies or innovative business models. While some industry commentators have cast doubt on the sustainability of fully decentralized financial services, others believe that DeFi has real potential as a disruptor of traditional financial services markets.

1.1 DeFi from a technical perspective

A basic understanding of the different layers of technology used for DeFi applications will establish a mental map that is helpful in analyzing and evaluating specific DeFi implementations (Figure 1).

Protocol, asset, and settlement layers form the core of the DeFi technology stack. The protocol layer consists of DeFi applications that offer some sort of financial service functionality such as trading or lending. The asset layer defines which digital assets can be processed by a DeFi protocol. It is important to keep in mind that normally a specific DeFi protocol is offering its services for only a few specific digital assets such as one fungible token or a pair of fungible tokens. Finally, the settlement layer forms the underlying infrastructure. DeFi applications as well as digital assets reside on Layer-1-protocols (e.g., Ethereum). This Layer-1-protocol is of crucial importance, as it represents the execution and settlement layer for any transactions.

In addition to these core layers, three additional layers can play a role. First, at the bottom of the stack, the interoperability layer allows different settlement layers to directly communicate with each other. It can be used to allow DeFi applications to incorporate different Layer-1-protocols into their functionality. At the top of the stack, an application layer normally provides user interfaces. Finally, an aggregation layer allows to aggregate the functionality of multiple DeFi applications.

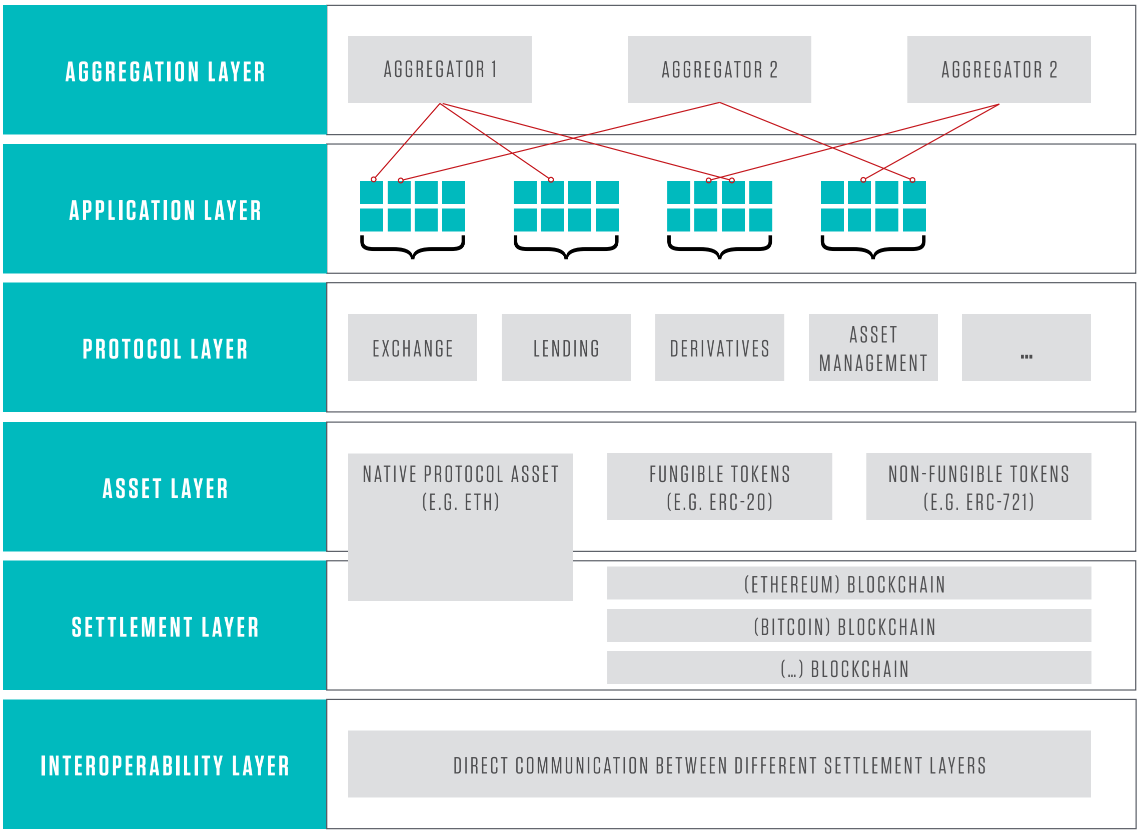


Figure 1: The DeFi Stack (based on IOSCO 2022 and Schär 2021)

1.2 The Promise of DeFi

Decentralized applications are the core building block of DeFi. They make DeFi services fundamentally different to traditional financial services: being built on public, permissionless blockchain networks, DApps operate in a trustless environment. This means that responsibility for the security of operations and assets need not fall to a central intermediary, but is instead provided by the underlying blockchain network. Furthermore, with assets stored and transactions settled on a public blockchain infrastructure, users are able to hold the cryptographic keys to their assets directly without using a custodian.

It is important to note that the primary goal of DeFi remains to facilitate existing financial services such as trading or lending. While DeFi for the most part does not change the functionality of the services, it does modify how the services are provided, delivered and used. From a user's perspective, this promises various benefits, including:

- **Real-Time Execution and Settlement:** Execution and settlement is more tightly integrated in DeFi applications. After executing a trade, the underlying blockchain is usually automatically updated.

- **Transparency:** Transactions are transparent for most DeFi projects, and this ensures that users can check and audit all activities.

- **Accessibility:** Regardless of people's location, they can access DeFi services if they have an internet connection, a crypto wallet, and a smartphone.

- **Disintermediation:** Assets are normally directly held by users in non-custodial wallets or in smart-contract-based escrow accounts. This eliminates the need for expensive intermediaries.

- **Programmability:** DApps offer the opportunity to integrate business logic into a system. This way, rules can be automatically executed with no need for intermediaries or human intervention.

- **Low Fees / High Interest Rates:** Since two individuals can transact directly, with no need for intermediaries, transactions normally become less expensive.

However, it is important to also consider the risks involved. Although DeFi solutions succeed in reducing some risks, such as counterparty risk associated with trading partners and intermediaries, they also add new risks such as software bugs or more general smart contract risk (e.g., token contracts, domino effects, dependency on off-chain data, etc.). Furthermore, from an institutional perspective, regulatory risks have to be considered. Important questions – such as concrete implementations for AML or KYC policies – are still under discussion.

1.3 DeFi applications

DeFi solutions exist for major functions such trading, lending, investing, deposits, and payments (see Figure 2) with more services being added on an ongoing basis. Figure 2 gives an overview of financial services verticals, with examples of solutions across traditional finance (TradFi), Centralized Finance (CeFi)[1] and Decentralized Finance (DeFi).

When comparing TradFi with CeFi and DeFi, it is important to distinguish infrastructures from assets. DeFi (and CeFi) solutions currently focus on the processing of digital assets such as cryptocurrencies, whereas TradFi handles traditional assets such as bonds or equities. However, it would also be conceivable that DeFi solutions process digitalized versions of traditional assets (e.g., tokenized bonds).

	Traditional Finance (TradFi)	Centralized Finance (CeFi)	Decentralized Finance (DeFi)
TRADING	Exchanges / Brokers (e. g. Xetra)	Crypto Exchanges (e. g. Binance)	Decentralized Exchange (e. g. UNISWAP)
LENDING	Secured and unsecured (e. g. term loans)	Lending Platforms (e. g. BlockFi)	Lending Protocols (e. g. AAVE)
INVESTING	Investment Funds (e. g. ETFs)	Crypto Funds (e. g. Grayscale)	Decentralized Asset Mgmt. (e. g. Set)
DEPOSITS	Savings Account (e. g. Commercial Banks)	Staking Pool (e. g. Coinbase)	dStaking Services (e. g. COSMOS)
PAYMENTS	Payment Platforms (e. g. SEPA, T2)	Centralized Stablecoins (e. g. USDC)	DeFi Stablecoins (e. g. DAI)

Figure 2: Main financial services categories in Traditional Finance, Centralized Finance and Decentralized Finance

[1] Centralized Finance refers to financial services for digital assets that are largely comparable to traditional financial services offerings from an organizational and procedural perspective. However, CeFi also uses blockchain for the settlement of net positions.

As noted, DApps are currently available for users in financial services such as trading, lending, investing, deposit, and payment solutions.

- **Trading:** In DeFi, decentralized exchanges (DEXs) perform the function of centralized exchanges by using smart contracts. DEXs enable users to exchange digital assets without having to use or trust intermediaries or use custodians. Major DEX protocols include Uniswap and Sushiswap.

- **Lending:** DeFi lending protocols offer loan services. These solutions normally come in one of two varieties. With pool-based lending protocols interested individuals provide liquidity or funds to a pool that others can borrow from. Users putting their assets into the pool can earn interest-like income in return. With peer-to-peer based lending, individuals borrow directly from a particular lender. In this case, decentralized lending protocols enable borrowers to take out loans with minimum barriers. Major DeFi lending protocols include Aave, Maker and Compound.

- **Investing:** DeFi DApps can also be used to execute automated trading strategies. For example, TokenSets is a DApp-based platform for portfolio management. Users provide the boundary conditions and investment objectives and then TokenSets trades, balances, and implements strategies to achieve the users' goals automatically. This enables users to gain exposure to a basket of digital assets, without the need to buy individual assets.

- **Deposits (Staking):** While there are no deposits in the traditional sense in the DeFi ecosystem, a very similar mechanism – 'staking' – exists. Staking refers to the process of locking up digital assets for a fee, and as such is comparable to depositing money at a bank. Just as a bank deposit represents a short-term loan that is given to the bank, staked cryptocurrencies can be seen as a short term loan to a protocol. For the time that assets are staked, they earn a small income, but cannot be sold or otherwise used by their owners. Rather, digital assets locked up in this way are used for adjacent processes, such as supporting the transaction validation mechanism of the underlying blockchain network.

- **Payments and Stablecoins:** The extreme volatility of cryptocurrencies such as Bitcoin and Ether inhibits their use for payment purposes. This problem is addressed by stablecoins – digital assets that are pegged to fiat currencies or some other stable asset. They aim to be a means of payment with a similar volatility as fiat currencies. As stablecoins are digital assets, they can be seamlessly integrated into other DeFi applications. Users can quickly conduct on-chain transactions with these coins without the need for using traditional financial infrastructures. Stablecoins come in two varieties. Asset backed stablecoins are blockchain-based tokens that have their value pegged to a reserve asset such as another digital currency, fiat money or a commodity. In contrast, algorithmic stablecoins try keep a stable value by managing the supply of the coin based on demand from users. However, the recent collapse of Terra (Luna) has shown that algorithmic stablecoins may not always be able to retain their stable value making them unsuitable as a means of payment.[2] Also, the adequacy of reserves of asset backed stablecoin projects have recently been publicly challenged.[3] Some of the most popular stablecoins include Binance USD (BUSD), USD Coin (USDC), and Dai (DAI). In additon to these private sector-driven initatives, central banks around the world are looking into the opportunities of Central Bank Digital Currencies (CBDC).

While the above examples represent the main solutions currently observed in the DeFi space, there are a host of other DeFi financial services that are being discussed and experimented with. These include insurance services, derivatives, and prediction markets (e.g., Augur).

[2] https://www.bloomberg.com/graphics/2022-crypto-luna-terra-stablecoin-explainer/

[3] https://www.wsj.com/articles/biggest-stablecoin-issuer-tether-switches-accounting-firm-to-bdo-italia-11660795062

2. DECENTRALIZED EXCHANGES

One of the fastest growing areas in DeFi is Decentralized Exchanges (DEX). With the rise of cryptocurrencies and other digital assets after the financial crisis of 2008, people soon searched for service offerings that enabled them to trade these new assets.

With traditional financial services providers not offering services for owners of digital assets, a new class of financial intermediaries emerged, initially in the shape of 'centralized exchanges' (CEXs) that replicate within the digital asset space the services provided by traditional exchanges. In order to use the services of a CEX, a users needs to sign up with the CEX and then, before being able to buy or sell digital assets, has to fund their account using either cryptocurrencies (e.g., Bitcoin) or some traditional form of payment (e.g., bank transfer).

However, this also means giving up control over any assets that are held by the CEX in a user's account.[4] Users need to trust the exchange with their money, making them vulnerable to some degree of counterparty risk. This was especially problematic given most CEXs were newly established entities with untested operations and minimal to zero oversight from financial markets authorities. As a results, hacks, scams, and other illegal activities have been common in the early years of the CeFi space, often leading to a loss of capital for users of these services.

Decentralized exchanges (DEX) emerged to solve this problem. The primary goal of a DEX is full disintermediation via the elimination of middlemen and allowing every user to deal directly with other users on a P2P basis. By migrating trading functionality directly onto the blockchain via smart contracts, a DEX serves as a trustless platform for the trading of digital assets. Much like traditional exchanges and CEX, these platforms coordinate supply and demand from many users. However, assets either remain in the custody of the user or – for a limited time – in an escrow account of the fully automated smart contract.

[4] Practically, the ownership of digital assets is represented by owning the private key to the address where the assets are stored. Sharing the private keys with third parties, enables these parties to fully control the asset. "Not your keys, not your asset" is a familiar quote in the crypto community.

2.1 Market size, major players, and market share

While CEXs might dominate the digital asset trading space for a long time, we are witnessing an increase in the popularity of DEXs. Available reports indicate that by late 2021, the largest DEXs have already started challenging some of the oldest CEXs in terms of their trading volume.

Generally, the size of a DEX can be evaluated using two metrics: trading volume and market capitalization. From a trading volume perspective, Uniswap (V3) is the largest DEX, with an average trading volume of close to $1.25 billion per day as of August 2022. Other large DEX include dYdX and Pancake swap (V2). Figure 3 gives an overview of 24h trading volumes.

In comparative terms the 24h trading volume as on 15 August 2022 for Uniswap (V3) was $1.25 billion whereas that of Binance (the largest CEX) on the same date was $17.52 billion.

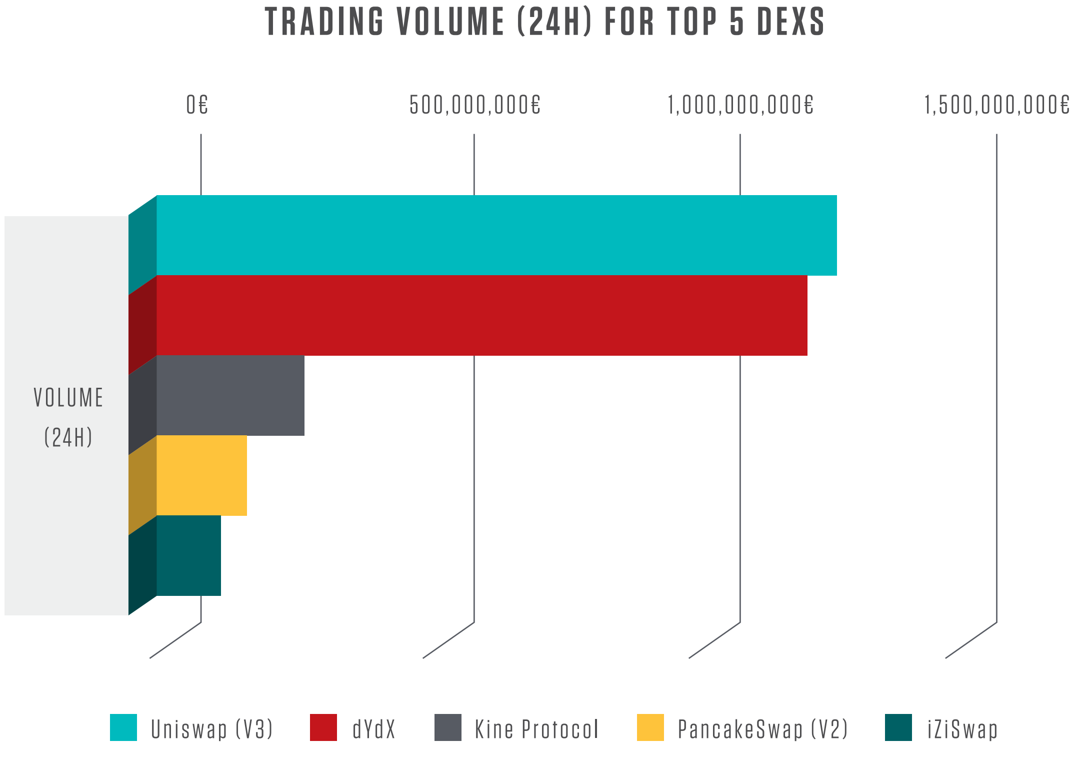


Figure 3: Trading Volume (24h) for top 5 DEXs[5]

[5] Data obtained from coinmarketcap.com on Aug. 15th, 2022

2.2 Main Types of DEXs

DEXs come in a variety of forms. Over the years, several designs have been suggested and implemented, all in an effort to improve on previous attempts and further streamline the functionality of the solution and its user experience. Generally, there are three major types of DEX.

- Automated Market Makers based DEXs
- Order book based DEXs
- Hybrid / Alternative Platforms

Automated Market Makers (AMMs) based DEXs: AMMs use pools of digital assets (sourced from so-called 'liquidity providers' – see Filling the Pool in section 2.3.1) to enable trading services for its users. Prices are quoted automatically by the underlying smart contract, hence the name automated market maker. The main purpose of creating an AMM is to ensure liquidity at all times. Given the prevalence of the term AMM for AMM-based DEXs, we use the terms interchangeably in the following.

Order Book based DEXs: Order book DEXs compile the details of all open buy and sell orders for a particular pair of digital assets. A buy order implies that a trader desires to bid for an asset at a given price. A sell order on the other hand is an indication that a trader is willing to sell a specific asset at a particular price. Much like traditional exchanges, order book DEXs match these orders.

Hybrid / Alternative Platforms: Though most DEXs can be classified as either as AMM or order book, a growing number of platforms are beginning to merge the concepts of both these types to create new, hybrid DEXs. This is mostly done to enable additional functionality such as allowing users to seamlessly trade their assets across multiple blockchains etc. An interesting example for such a hybrid approach is Raydium.

In addition, a noteworthy phenomenon has been the rise of DEX aggregators, which allow users to search for prices and liquidity across multiple DEXs.[6] As the name implies, they aggregate liquidity from different DEXs to provide the users with the best execution price available within the shortest time, while lowering the level of slippage on large orders and optimizing fees.

[6] Strictly speaking DEX aggregators are not a type of DEX, therefore they are not covered in this report.

2.3 Automated Market Makers – the current market leader

At present, the most common type of DEX is the Automated Market Maker. The main feature of traditional exchanges is to match supply and demand for a given asset and determine a price at which parties are willing to exchange assets. Automated Market Makers operate in a fundamentally different way.

An AMM does not match trades as in the case of a centralized or decentralized order-book, but rather provides a liquidity pool to trade against. The two major components of an AMM are its liquidity pool and a smart contract that manages the liquidity pool by determining trading prices as well as fees and rewards for the service.

The liquidity pool in its simplest form contains units of two digital assets. This asset pair can either consist of two risky assets (e.g., Ether and Bitcoin) or a risky asset and a base asset such as a stable coin (e.g., Ether and USDC). From a technical perspective, the pool is an address on the Layer-1 settlement infrastructure (e.g., Ethereum). The liquidity pool is controlled and managed by a smart contract that automatically, based on the pool's composition, generates prices for which a trader can exchange the assets.

2.3.1 How do AMMs work

Trading via AAMs is broken into multiple phases (see Figure 4).

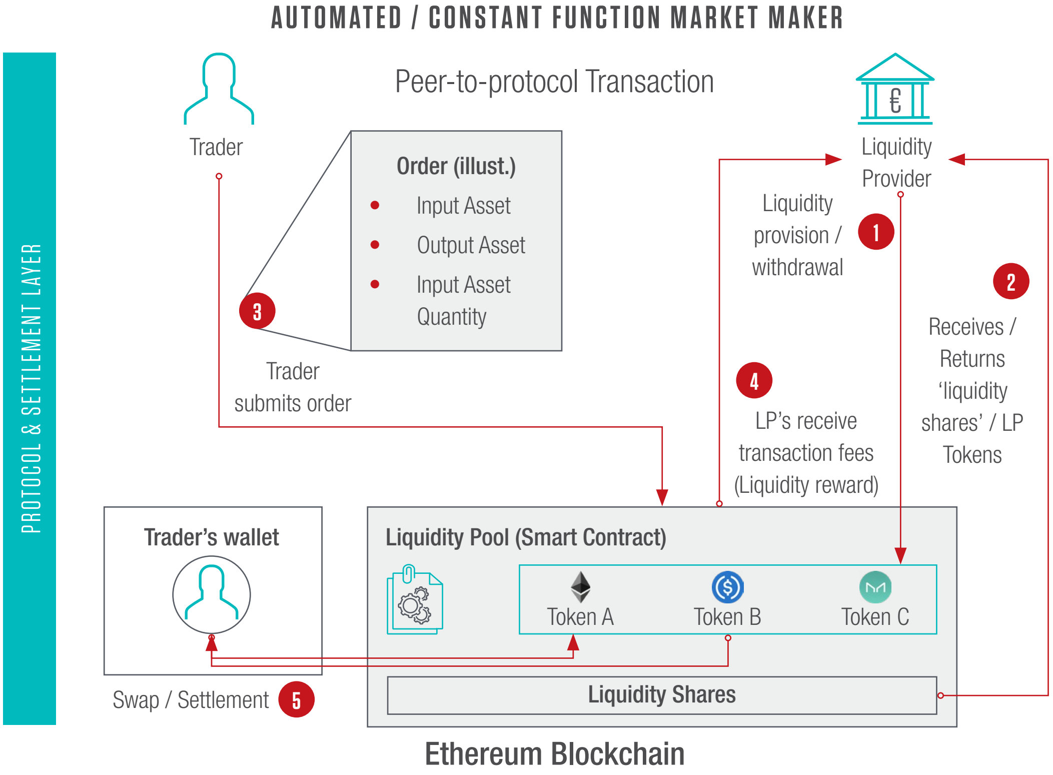

AUTOMATED / CONSTANT FUNCTION MARKET MAKER
PROTOCOL & SETTLEMENT LAYER
Peer-to-protocol Transaction
Trader
Order (illust.)
Input Asset
Output Asset
Input Asset Quantity
3
Trader submits order
Liquidity Provider
Liquidity provision / withdrawal
1
2
Receives / Returns 'liquidity shares' / LP Tokens
4
LP's receive transaction fees (Liquidity reward)
Trader's wallet
Swap / Settlement
5
Liquidity Pool (Smart Contract)
Token A
Token B
Token C
Liquidity Shares
Ethereum Blockchain

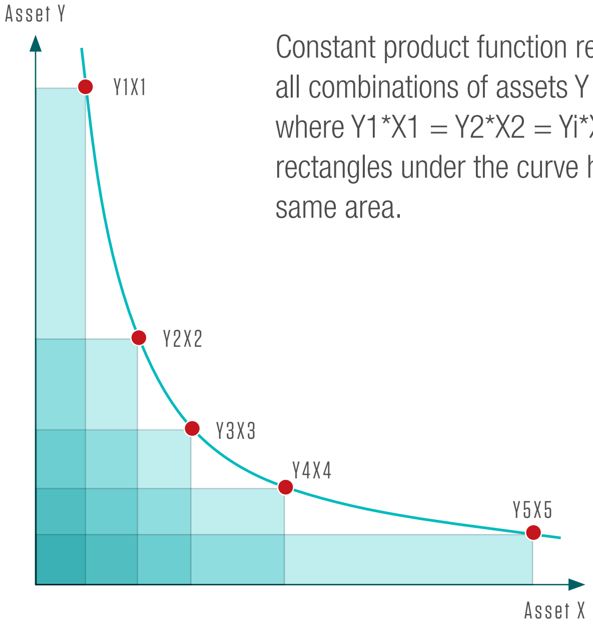
Figure 4: AMM – Process overview (numbers represent sequence of process steps)

Filling the pool: Initially the digital assets in a liquidity pool are provided by liquidity providers, including long-term holders of digital assets who provide their assets to the pool in order to earn income on otherwise non-earning assets. In exchange for bringing in their assets, the liquidity provider receives pool shares (also known as liquidity provider shares) in the form of special 'pool tokens'. These tokens represent a claim of the liquidity provider on the portfolio of assets in the pool and can be used to withdraw the liquidity provided. In addition to entitling the holder to a share in the pool assets, pool tokens also give the holder a claim on any trading fees earned by the pool.[7]

Trading assets: Once funds are available in the liquidity pool, traders can send their orders. An order consists of the input and the output asset as well as the quantity of one of the assets (e.g., 100 Ether against Bitcoin). On receiving the order, the AMM automatically quotes a price at which the trade can be instantly executed.

Determining the price: Prices are automatically determined by the AMM for traders who wish to trade the digital assets in the pool. The AMM generates its quotes according to a pre-determined formula (so-called conservation function or bonding curve). The conservation function prices the two pool assets relative to each other, making the asset that is in high demand automatically costlier, and vice versa.

One common function to determine prices is the constant product function. This function keeps the product of the amount of the two assets in the pool constant (i.e., amount of token X * amount of token Y = constant). Mathematically, such a function determines a curve containing all ratios at which an AMM is willing to exchange the assets of the pool (see Figure 5).



Constant product function represents all combinations of assets Y and X, where Y1*X1 = Y2*X2 = Yi*Xi. All rectangles under the curve have the same area.

Figure 5: Constant product bonding curve

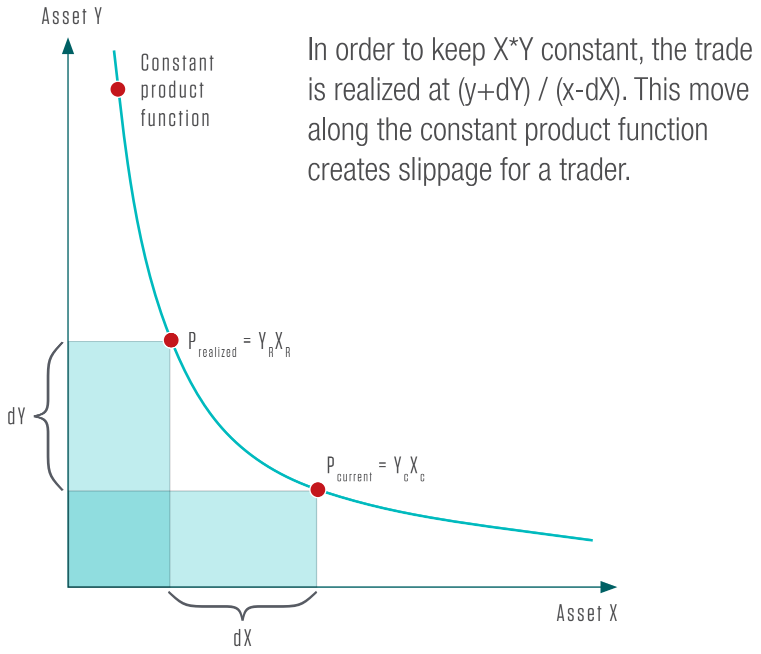
[7] With some DEX-applications, a liquidity provider might also receive so-called "protocol tokens" which grant the right to vote on decisions concerning the governance of the protocol (e.g., fee structure, code updates etc.).

While constant product functions are one of the most frequently used functions to determine prices for the assets in a pool, they are by no means the only one. Other functions that can be found implemented or discussed include Constant Mean Market Makers, Constant Sum Market Makers, Hybrid Function Market Makers and, Dynamic Automated Market Makers.

Example: If the liquidity pool AB consists of 100 units of digital asset A and 100 units of digital asset B, the product A*B is 10,000. If someone wanted to sell 10 units of A (against B) he would supply 10 A to the pool and receive an amount of 9.0909 units of B. This keeps the product constant at 10,000 (110 A * 90.909 B = 10,000).

As can be seen from this example of a constant product function, the price that the trader receives is not 1 unit of B for 1 unit of A (as implied by the ratio of the quantities of the two assets, 100/100 = 1) but only 0.90909 units of B. This price impact of trades (so-called 'slippage', in this case equal to -0.0909) depends on the size of trade relative to the size of the pool. The bigger the trade relative to the total size of the pool the higher the slippage. Figure 6 gives an exemplary illustration of the interplay between conservation functions and slippage.

Arbitrage Opportunity: As can also be seen from the example above, the price quoted by the AMM reflects the ratio of the assets in the pool. Every trade changes this ratio. If the slippage is large enough, this could result in a price deviation from a fair ratio of exchange between the two assets. If the assets in the pool are also traded on other markets, this in turn could lead to potential arbitrage opportunities. An arbitrageur would take advantage of this price difference and bring the price ratio back to its fair value.



In order to keep X*Y constant, the trade is realized at (y+dY) / (x-dX). This move along the constant product function creates slippage for a trader.

Figure 6: Constant product function and slippage (simplified, based on Mohan 2022)

2.3.2 Benefits of AMMs

AMMs offer several benefits to traders as well as liquidity providers.

For traders, the benefits are instant execution and continuous liquidity for otherwise illiquid assets. Another benefit lies in the operational setup. In contrast to centralized exchanges, traders do not have to store their digital assets with the exchange – instead, trades are instantly and automatically executed against the liquidity pool. This eliminates counterparty risk which has been an issue with lightly regulated centralized crypto exchanges.

For liquidity providers, the main benefit lies in generating income for otherwise non-earning assets. From this perspective, providing liquidity to a DEX can be compared to traditional securities lending of long-term portfolio positions. This can be quite profitable as the below example shows.

	POOL ASSET 1		POOL ASSET 2		POOL TOTAL	NOTE
	ETH	$-Value	USDC	$-Value	$ Value	
Pool Total	9	$9,000	9,000	$9,000	$18,000	Constant Product (9*9k= 81k)
Liquidity provision	+1	+ $1,000	+1,000	+ $1,000	+$2,000	Liquidity Provider owns 10% of Pool = $2,000
Pool Total	10	$10,000	10,000	$10,000	$20,000	Constant Product (10*10k = 100k)
BUY 1 ETH vs. USDC	(10-1)		10,000+x			Constant Product must stay at 100k
Pool after Trade	9	$9,000	11,111	$11,111	$20,111	Solving for X; Constant Product = 100k, Liquidity Providers owns 10% of Pool = $2011,1

Table 1: Example for trade via an AAM (Assumptions: 1 USD Coin (USDC) = 1$, 1 ether (ETH) = $1,000; example based on BIS 2021 p34)

2.3.3 Risks and drawbacks of using AMMs

Alongside the benefits of an AMM, it is also important to take an detailed look at the potential risks and drawbacks for traders as well as liquidity providers.

For traders, the main disadvantage of using an AMM is the potential for high slippage (see Figure 6). As AMM prices follow a curve, there will always be slippage, and that slippage depends on the conservation function of the AMM. The main factors driving slippage are the size of the trade relative to the pool size, as well as the current composition of the pool.

A second risk traders face is frontrunning. In order for a trade to settle it needs to be recorded on the underlying blockchain (e.g., Ethereum). Generally, the Layer-1-blockchain of a DeFi protocol stores transactions in a public transaction pool. Validators / miners then group these transactions into blocks, which are subsequently written onto the blockchain. Once written onto the blockchain, a trade is executed and settled at the same time. While this process seems pretty straight-forward, validators / miners have large discretion with regards to the order in which they process transactions from the transaction pool.

In a largely unregulated market, this opens up the risk of frontrunning, which exists even if validators / miners automatically group transactions according to predefined rules. By structuring transactions smartly, malicious third-party traders might be able to sandwich an order (buy and sell order before and after the order of the AMM) in order to profit from a price impact.

Thirdly, traders also face some uncertainty with regards to the total cost of their trade. While direct fees of the DEX are known and comparatively small, settling a trade requires recording the trade on the underlying blockchain. This normally also incurs fees. Most Layer-1 protocols used for DeFi have dynamic fee structures based on the demand for the protocol's services (e.g., Ethereum). This can lead to prohibitively high settlement fees. The extent of this risk is protocol dependent.

Lastly, from a trading perspective AMMs have very limited functionality when it comes to permissible order-types, as normally only market orders are supported.

For liquidity providers, the main risk for providing liquidity to an AMM lies in the possibility of a so-called 'divergency loss'. As described above, liquidity providers do not have a claim on the exact amounts of digital assets they have initially provided to the pool but rather claim on a share of the pool's total assets at a given time plus any fees earned by trades (see the above example in the Table).

If the price of an asset pair on external markets moves away from the price quoted by the AMM, this opens the opportunity for arbitrageurs to trade against the liquidity pool and profit from these price differences. This can lead to situations where the value of the liquidity provider's share in the pool is worth less than the value of the original positions provided to the pool. In other words, it would have been better for the liquidity provider not to have provided the liquidity. This loss is sometimes euphemistically referred to as 'impermanent loss', as it only is realized when a liquidity provider chooses to exit the pool.

2.4 Beyond Automated Market Makers

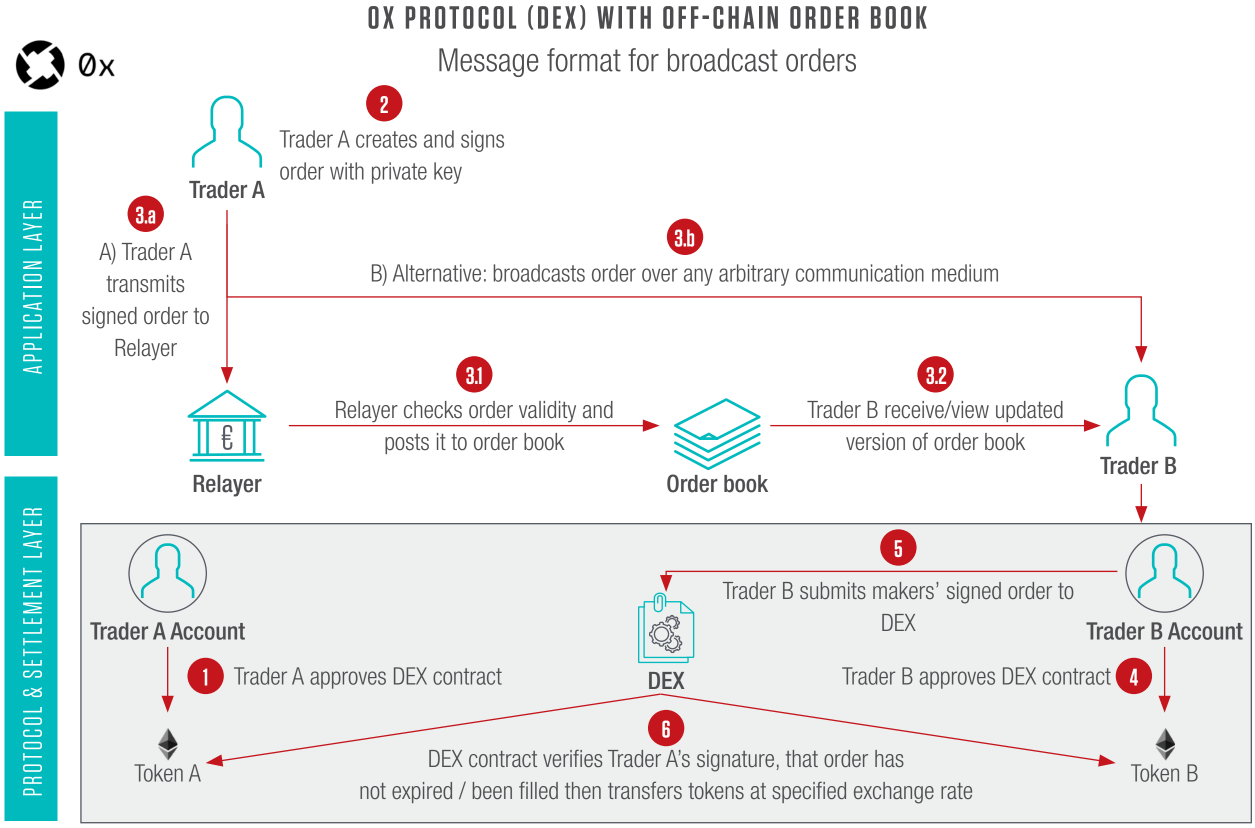
Currently, the majority of DEXs are based on the AMM model. This is noteworthy because – as discussed above – that model has several drawbacks when compared to an order book model. However, the major reason for the dominance of AMMs lies in the difficulties associated with implementing an order book on a blockchain infrastructure.

Maintaining a central limit order book on-chain means that every quote needs to be recorded as a transaction on the underlying blockchain settlement layer. This requires the underlying infrastructure to be able to processes transactions in both a fast and cheap way. Both these requirements were not met by early Layer-1-protocols (e.g., Ethereum). This made a normal quoting process – and hence maintaining an order book – prohibitively expensive and practically infeasible.

However, over time new approaches and new Layer-1 protocols have provided new impetus to projects working on blockchain-based order book DEXs. Several approaches can be identified.

DEXs with off-chain orderbooks: In order to combine the benefits of limit-order-book markets with the advantages of DEXs, one solution is to move the order book off-chain.

The 0x protocol is one example for such a solution. In this set-up, a party wishing to place an order sends a signed order to a 'relayer' who enters the order into the order book. This way, a party looking for liquidity can check their order against the order book. On finding an appropriate matching order, the relayer forwards the order to the DEX. The smart contracts of the DEX then verify the validity of the order and execute the asset transfer (Figure 7).



0X PROTOCOL (DEX) WITH OFF-CHAIN ORDER BOOK
Message format for broadcast orders
0x
APPLICATION LAYER
PROTOCOL & SETTLEMENT LAYER
Trader A
2 Trader A creates and signs order with private key
3.a A) Trader A transmits signed order to Relayer
3.b B) Alternative: broadcasts order over any arbitrary communication medium
3.1 Relayer checks order validity and posts it to order book
3.2 Trader B receive/view updated version of order book
Relayer
Order book
Trader B
Trader A Account
1 Trader A approves DEX contract
5 Trader B submits makers' signed order to DEX
DEX
Trader B Account
Trader B approves DEX contract 4
6 DEX contract verifies Trader A's signature, that order has not expired / been filled then transfers tokens at specified exchange rate
Token A
Token B

Figure 7: DEX with off-chain order book – Process overview (numbers represent sequence of process steps)

In addition to 0x, DEXs with such a set-up include IDEX and EtherDelta.

The off-chain order-book approach has two main advantages. First, it leads to higher performance when compared to purely blockchain-based order books, as the underlying Layer-1 protocol ceases to be a limiting factor. Furthermore, it normally also leads to lower overall costs, as no fees for the use of layer 1 must be paid in the quotation process.

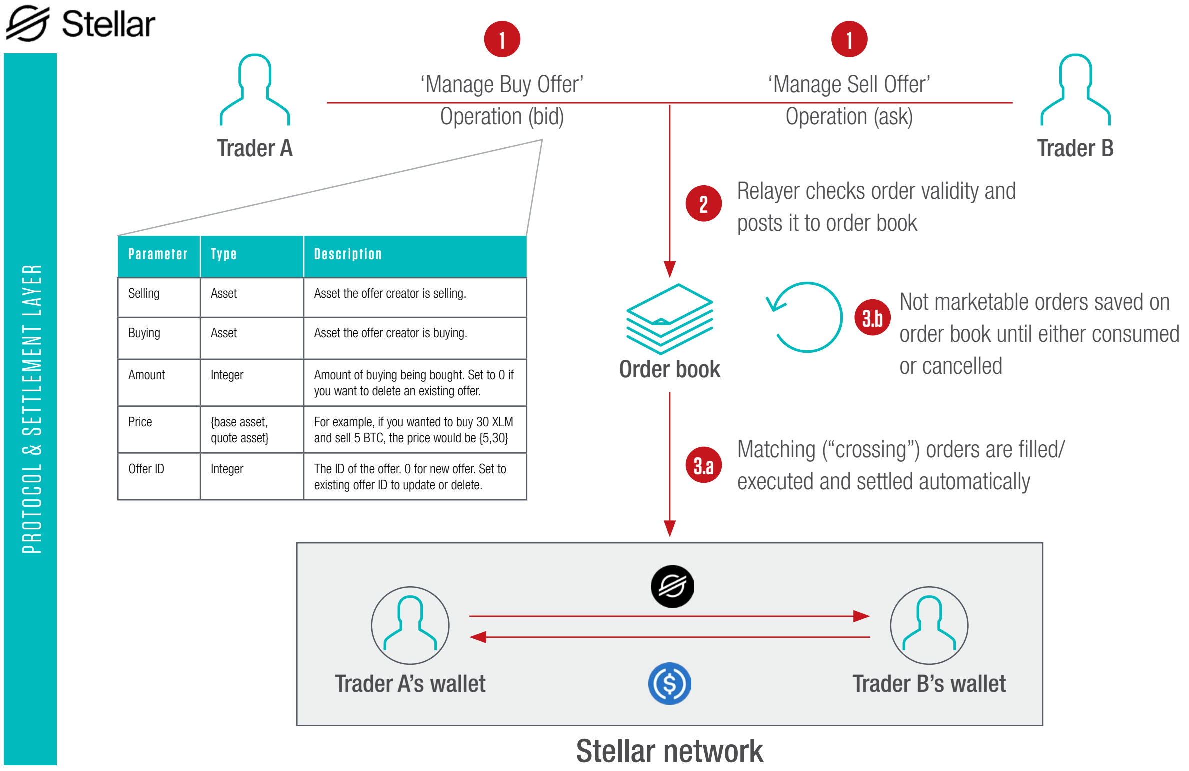
On the downside, the approach introduces a centralized element in the whole structure. While the settlement infrastructure is still based on blockchain, the order matching is done off-chain. This represents a single point of failure, as the centralized order book can be compromised. In other words, this solution requires trust in the central relayer to act properly on behalf of its users. However, in contrast to a CEX, the relayer does not take custody of the asset nor executes orders.

DEXs with on-chain order books: DEXs with on-chain order books look to combine the advantages of limit order books (e.g., order functionality, slippage) and a secure blockchain infrastructure for the order book (e.g., resistance to censorship, no need for central intermediaries). However, this requires every order and every quote to be recorded on the blockchain.

The requirement to record every action as a transaction on the underlying blockchain-infrastructure made this type of DEX very hard to implement on early Layer-1 protocols such as Ethereum. As discussed above, transaction recording on these Layer-1 protocols was simply too expensive and too slow. However, newer Layer-1-protocols (e.g., Solana) enable fast and low-cost execution of transactions on the underlying blockchain, therefore enabling decentralized order books as a pricing mechanism.

DEXs using an on-chain order book approach include for example Stellar and Serum.

STELLAR PROTOCOL WITH ON-CHAIN ORDER BOOK


Stellar
PROTOCOL & SETTLEMENT LAYER
Trader A
1
'Manage Buy Offer' Operation (bid)
1
'Manage Sell Offer' Operation (ask)
Trader B
2
Relayer checks order validity and posts it to order book
Order book
3.b
Not marketable orders saved on order book until either consumed or cancelled
3.a
Matching ("crossing") orders are filled/ executed and settled automatically
Trader A's wallet
Trader B's wallet
Stellar network

Parameter	Type	Description
Selling	Asset	Asset the offer creator is selling.
Buying	Asset	Asset the offer creator is buying.
Amount	Integer	Amount of buying being bought. Set to 0 if you want to delete an existing offer.
Price	{base asset, quote asset}	For example, if you wanted to buy 30 XLM and sell 5 BTC, the price would be {5,30}
Offer ID	Integer	The ID of the offer. 0 for new offer. Set to existing offer ID to update or delete.

Figure 8: DEX with on-chain order book – Process overview (numbers represent sequence of process steps)

3. CONCLUSION AND OUTLOOK

DEXs in their various forms are still a niche phenomenon in the emerging digital asset space. Therefore, it would be easy to dismiss them as largely irrelevant. However, from a bigger picture perspective, several trends support the growth potential of DeFi in general and DEXs in particular.

First, DeFi has the potential to be a key component of the ongoing trend of improving financial services processes. At its core, DeFi promises to make financial services more efficient mainly through automation and by cutting out middlemen – objectives achieved by building on the specific properties of blockchain technology. This could enable, for example, a tighter integration and automation of execution and settlement processes.

Second, while the crypto asset space has emerged out of the crypto community, in recent years we have seen increasing interest in the space across broader target groups. Not only have institutional investors become more interested over the past few years but established financial service providers have started initiatives and offerings for digital assets. We are starting to see a similar development in the DeFi-sector. While most DeFi-solutions are driven by the technology affine crypto community, there are first examples of regulated financial institutions becoming active. The engagement comes in a variety of forms including stable coin offerings (e.g., by JP Morgan[8]) and active participation in DeFi-protocols by established institutions (e.g., Societe Generale in MakerDAO[9]) to name two examples. Given the development of firm regulation of digital assets in various jurisdictions (e.g., Europe or Switzerland), there is an expectation that DeFi will persist and mature in the coming years.

Third, DeFi and DEXs should profit from the ongoing drive to digitalize traditional securities and assets. Such fully digitalized assets will require new processes and infrastructures, which DeFi is already offering today, such as the integration of the securities and the cash leg within one infrastructure.

Finally, the technology and solutions underlying DeFi are developing rapidly. New Layer-1 blockchains such as the emergent Solana ecosystem or the Binance Smart Chain, as well as innovative Layer-2 solutions (e.g., Polygon) promise better performance at a lower price while building on the key advantages of a decentralized system. This in turn creates a basis for newer and better DeFi solutions – the DEX space in particular has benefitted from constant work on major protocols, resulting in tremendous improvements to the available solutions.

While new disruptive solutions come with risks, they also offer opportunities. With regards to DEXs, traditional financial service providers can identify opportunities at various levels of the technology stack. Naturally, their expertise means trading-oriented financial institutions have an opportunity to become active players in DEXs as liquidity providers, traders or arbitrageurs. However, banks could also become more deeply involved by offering their own DEX or DEX-based services and solutions, built on their strong expertise in financial markets. Lastly, opportunities exist to become active in providing infrastructure services for the settlement layer of DeFi (e.g., staking).

[8] https://www.jpmorgan.com/onyx/coin-system.htm

[9] https://www.thedefiant.io/makerdao-members-vote-on-issuing-30m-loan-to-societe-generale

How do I become active in the space?

We are currently seeing a major market correction in the digital assets space. Such corrections should be expected with new technologies – and as with previous financial crises, such corrections typically lead to a shakeout of weaker companies and solutions. They also present long-term participants with an opportunity to learn from their own and others' mistakes.

When considering engaging with DEXs, market participants should consider the following aspects:

- **Customer segment:** A commercial bank with a strong retail service offering might be inclined to offer its customers secure and easy-to-use access to DEXs while a provider of traditional exchange services might focus more on creating infrastructure solutions.

- **Regulatory requirements:** The integration of existing DEX solutions into your own offering can have a potentially negative impact on your standing with regulators. With supervisory authorities globally casting an eye on DeFi, it is important to follow regulatory developments closely.

- **DEX business case:** Due to the dynamic nature of DeFi, such a business case should ideally consider numerous branching scenarios.

- **Implementation plan:** Typically new DLT components will have to be integrated with existing internal systems. In most cases, four components will be required. Depending on the positioning and the new service offering, these include:

  – a custody solution

  – an 'intermediate layer' (custody integration layer) that serves as an interface between the standardized DLT applications and legacy systems

  – specific trading software

  – an anti-money laundering solution

- **Build or buy:** Whether components are built or bought, the know-how and capabilities for operating the DLT components should be established internally to ensure both independence and sustainability.

Capco and ABC Research support the individual implementation path end-to-end with comprehensive technical and methodological knowledge of capital markets as well as DLT expertise, from digital asset strategy to the implementation of new business models.

REFERENCES

- 21Shares Research Team. (2022). State of Crypto. Our Insights into Web3, The Future of The Internet. [Industry Report]. https://21shares.com/research
- Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralization illusion. BIS Quarterly Review, December 2021, pp 21-36.
- Aspris, A., Foley, S., Svec, J., & Wang, L. (2021). Decentralized exchanges: The "wild west" of cryptocurrency trading. International Review of Financial Analysis, 77, 101845. https://doi.org/10.1016/j.irfa.2021.101845
- Barbon, A., & Ranaldo, A. (2021). On The Quality Of Cryptocurrency Markets: Centralized Versus Decentralized Exchanges (arXiv:2112.07386). arXiv. http://arxiv.org/abs/2112.07386
- Capponi, A., & Jia, R. (2021). The Adoption of Blockchain-based Decentralized Exchanges (arXiv:2103.08842). arXiv. http://arxiv.org/abs/2103.08842
- ConsenSys. (2021). DeFi for Institutions (Insight Report) [Industry Report].
- Deshmukh, S., Warren, S., & Werbach, K. (Eds.). (2021). Decentralized Finance (DeFi) Policy-Maker Toolkit. In collaboration with the Wharton Blockchain and Digital Asset Project [White Paper]. World Economic Forum.
- FATF. (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html
- Fidelity Digital Assets (2021). The Institutional Investor Digital Asset Survey. September 2021. Avaliable at: https://www.fidelitydigitalassets.com/research-and-insights/2021-institutional-investor-digital-assets-study
- Han, J., Huang, S., & Zhong, Z. (2021). Trust in DeFi: An Empirical Study of the Decentralized Exchange. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3896461
- IOSCO. (2022). Decentralized Finance Report (OR01/2022; p. 45pp). The Board of the International Organization of Securities Commissions.
- Kitzler, S., Victor, F., Saggese, P., & Haslhofer, B. (2021). Disentangling Decentralized Finance (DeFi) Compositions (arXiv:2111.11933 [cs]; arXiv:2111.11933). arXiv. http://arxiv.org/abs/2111.11933
- Lehar, A., & Parlour, C. A. (2022). Decentralized Exchanges. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3905316
- Meyer, E., Welpe, I. M., & Sandner, P. (2021). Decentralized Finance—A systematic literature review and research directions. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4016497

REFERENCES

- Mohan, V. (2022). Automated market makers and decentralized exchanges: A DeFi primer. Financial Innovation, 8(1), 20. https://doi.org/10.1186/s40854-021-00314-5

- Moncada, R., Ferro, E., Favenza, A., & Freni, P. (2021). Next Generation Blockchain-Based Financial Services. In B. Balis, D. B. Heras, L. Antonelli, A. Bracciali, T. Gruber, J. Hyun-Wook, M. Kuhn, S. L. Scott, D. Unat, & R. Wyrzykowski (Eds.), Euro-Par 2020: Parallel Processing Workshops (Vol. 12480, pp. 30–41). Springer International Publishing. https://link.springer.com/10.1007/978-3-030-71593-9_3

- Paruch, K. (2012). SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols [Working Paper].

- Quinlan, B., Chung, J., & Trehan, E. (2021). Cracking the Code. The Evolution of Digital Assets to the Mainstream. [Industry Report]. Quinlan & Associates.

- Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis REVIEW, 103(2), 153–174. https://doi.org/10.20955/r.103.153-74

- Wang, Y., Chen, Y., Wu, H., Zhou, L., Deng, S., & Wattenhofer, R. (2022). Cyclic Arbitrage in Decentralized Exchanges (arXiv:2105.02784). arXiv. http://arxiv.org/abs/2105.02784

- Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). SoK: Decentralized Finance (DeFi) (arXiv:2101.08778). arXiv. http://arxiv.org/abs/2101.08778

- Wharton Blockchain & Digital Asset Project. (2021). DeFi Beyond the Hype [Working Paper]. The Wharton School, The University of Pennsylvania.

- Zhou, L., Qin, K., & Gervais, A. (2021). A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges (arXiv:2106.07371). arXiv. http://arxiv.org/abs/2106.07371

AUTHORS

Vinzenz Treytl, ABC Research
Jan-Michael Steiner, Capco
Arindam Bhaumik, Capco
Gerald Hessenberger, Capco

CONTACTS

Alexander Eisl, ABC Research, alexander.eisl@abc-research.at
Christoph Ruth, Capco, christoph.ruth@capco.com

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, finance, risk & compliance, and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

ABOUT ABC RESEARCH

The Austrian Blockchain Center (ABC), located in Vienna, is a COMET competence center with the mission to be Austria's first scientific contact point for Blockchain and related technologies. Blockchain is a technology for secure cooperation between different participants with a wide range of use cases, not only as a digital currency, but also in industry, finance, energy, logistics, and public administration.

ABC is an interdisciplinary and application-oriented research institution dedicated to all aspects of blockchain research. Technological, economic, and legal topics are the focus. Projects with a high practical relevance, which directly lead to innovations in the economy, are made possible by the experts of the ABC and its scientific partners - Austrian and international universities, universities of applied sciences and research institutions.

CAPCO
a wipro company

ABC RESEARCH
Austrian Blockchain Center

WWW.CAPCO.COM