EUBlockchain
Observatory and Forum

Decentralised Finance (DeFi)

A Thematic Report Prepared By
The European Union Blockchain Observatory & Forum

An initiative of the European Commission

About this report

This is the sixth of a series of reports that will be published addressing selected topics in accordance with the European Commission priorities. The aim is to reflect on the latest trends and developments and discuss the future of blockchain in Europe and globally.This report, prepared by the new team leading the EU Blockchain Observatory and Forum, aims to present a comprehensive overview of the rapidly expanding field of Decentralised Finance (DeFi).

This report has been produced by the EU Blockchain Observatory and Forum Experts Panel and team.
EU Blockchain Observatory and Forum team:

- George Giaglis, Lambis Dionysopoulos, Marianna Charalambous, Aliki Ntouzgou, University of Nicosia;
- Nikos Kostopoulos, Tonia Damvakeraki, Netcompany-Intrasoft
- Alexi Anania, Íñigo Moré, Marcin Pawłowski, Matthew Niemerg, Amit Joshi, Miquel Gouarré Baró, Iwona Karasek-Wojciechowicz, Stefan Loesch, Daniel Szegö, EU Blockchain Observatory and Forum Expert Panel.

Special thanks to **Jacek Czarnecki,** Global Legal Counsel at MakerDAO for his insightful interview.

Special thanks to **Scope** for the editorial review and language proofing.

Note

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this report.

Total Value Locked (TVL) figures sourced from DeFiLlama and DeFiPulse between January 2022 and May 2022.

Disclaimer

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission’s behalf may be held responsible for the use which may be made of the information contained therein.

EUBOF: Decentralised Finance

Contents

Acronyms and abbreviations

AML	Anti-money laundering
AMM	Automated market maker
BFT	Byzantine fault tolerant
BSC	Binance Smart Chain
CDO	Collateralised debt obligation
CDP	Collateralised debt position
CEX	Centralised exchange
CSH	Cash
CTF	Counter-terrorism financing
DAG	Directed acyclic graph
DAO	Decentralised autonomous organisation
DEX	Decentralised exchange
DL	Divergence loss
DLT	Distributed ledger technology
DOS	Denial of Service
DPoS	Delegated PoS
EVM	Ethereum Virtual Machine
Ewasm	Ethereum WebAssembly
GDP	Gross domestic product
GDPR	General Data Protection Regulation
HPoS	Hybrid PoS
ICO	Initial coin offering
IoT	Internet of things
KYC	Know your customer
LP	Liquidity provider
MEV	Miner-extractable value
NFT	Non-fungible token
OR	Optimistic rollup
P2P	peer-to-peer
PBFT	practical Byzantine fault tolerance
PCV	Protocol-controlled value
PoA	Proof of Authority
PoH	Proof of History
PoS	Proof of Stake
PoSA	Proof of Staked Authority
PoW	Proof of Work
RSK	Risk
RVM	RSK Virtual Machine
SME	Small and medium-sized enterprise
TLV	Total value locked
UTXO	Unspent transaction output
WASM	WebAssembly
wETH	Wrapped ETH
wBTC	Wrapped Bitcoin
ZK	Zero-knowledge
ZKP	Zero-knowledge proof
ZKR	Zero-knowledge rollup

Chapter 1: Introduction to Decentralised Finance

SECTION 1.1: DEFI DEFINED

Decentralised Finance (DeFi) is an umbrella term for a collection of financial products which rely on smart contracts and blockchains to enable open, peer-to-peer (P2P) financial services and automate specific procedures. DeFi applications aim at decentralisation, although the degree to which they are varies. Decentralisation is quantified from multiple perspectives (starting from the base-layer blockchain, e.g. Ethereum, Solana, Avalanche, Cardano and Polkadot) and the code base of the protocol (e.g. Uniswap, Curve.fi and SushiSwap), and includes factors such as governance structures, voting procedures and more. While we will not be analysing the degree of decentralisation of the concepts included in the report, we note that it plays an important role when evaluating their characteristics and differences, especially in the context of conventional financial products.

Due to its open, decentralised and P2P nature, DeFi also enables ‘money Legos’. The term refers to the interoperability of applications in the space, and it is often cited as one of the aspects responsible for the rapid innovation in the space.

Naturally, DeFi can also be considered as a subset of fintech. By studying the similarities and differences of DeFi and traditional or conventional finance (TradFi), we can get a better sense of the prospects of this new form of finance. In this introductory chapter, we have chosen the following four main areas.

- **Intrinsic characteristics:** topography and nature of the underlying systems or embedded protocols.
- **Functional differences:** occurring as a result of the underlying intrinsic characteristics.
- **Operational differences:** exploring interface/platform, including expectations and the user experience.
- **Regulatory landscape:** comparing the outlook of policymakers and regulators in addressing those differences.

While this is not an exhaustive list, our findings will serve as the basis for exploring the more advanced DeFi concepts.

1.1.1 Intrinsic characteristics

The intrinsic characteristics predominately resulting from the (infra)structural differences between centralised TradFi systems and (quasi)decentralised systems lead to the former being permissioned finance, while its latter counterpart is permissionless. Permissionless systems have characteristics of inclusion and a degree of immutability where anyone can participate. By contrast, TradFi is a permissioned, tightly controlled and managed environment, resulting in it often being more exclusive. Read/write attributes for transactions and any financial action require a hierarchy of separate permission. As a result, TradFi is more segmented, requiring multiple intermediaries with various levels of permission to action a chain of events. Often a simple financial transaction (e.g. remittance) can take T+5 days. DeFi, by contrast, bypasses this stage by automating it through smart contracts, allowing DeFi practitioners to trade P2P in real time. DeFi is also often referred to as ‘trustless’ and ‘immutable’ (to varying degrees), meaning that unlike TradFi, no single entity (or collection of entities) must be present to guarantee its good performance. This is possible, as DeFi applications inherent (to some extent) the decentralised trust and censorship resistance generated by their open blockchain foundations. Finally, whereas TradFi uses data to record (nominal) value often linked to real-world assets/currencies, DeFi transactions consider data as value.

1.1.2 Overview of intrinsic characteristics

Table 1 – Overview of Intrinsic characteristics

Features	TradFi	DeFi
Access	Permissioned models	Permissionless models
Data integrity	Read/write access is controlled, managed, gated, exclusive	Inclusive, immutable
Interoperability	Segmented, dependent on multiple intermediaries	Composability, money Legos
Settlement	Timely chain of events, T+day(s)	Immediate settlement
Value	Uses data to record (nominal) value	Data does not record value, but is value in itself

1.1.3 Functional differences

TradFi and DeFi have many similarities in principle, and although the end goal is similar — to provide services to individuals and organisations — functionally, the differences are vast.

One contrasting functional area is the accounting method. TradFi utilises double-entry accounting, which revolutionised the field of financial bookkeeping during the Renaissance, 600 years ago. This refers to the accounting practice of using balance sheets (with two entries in a book, a credit that corresponds to a debit, and vice versa). In TradFi, every party keeps their own respective books to report the same transactions therein. Any discrepancies need extensive audits and administration. DeFi bypasses this by making use of an economy-wide accounting system, first referred to by Ian Grigg as triple-entry accounting. This means that the accounting entries are cryptographically sealed by a third system (blockchain) that's verifiably congruent and serves as both the transaction and the receipt (proof that a financial transaction took place between two counterparties). Triple entry does away with the need for manually recording and cross-reference transactions and state transitions, as those are already verified and stored in an immutable and independent ledger.

Another fundamental difference is identity. In DeFi (and on public blockchains more broadly), participation is pseudonymous. There's no underlying requirement for trust in individuals, as smart contracts and blockchains operate by strict rules that apply to every participant and are sceptical of anything else. The counterparty can be any individual human or device, so long as it can send and receive valid information. This extends to financial services for internet-of-things (IoT) devices and lays the groundwork for a new machine economy.

TradFi, on the other hand, is firmly rooted in the procedures of conventional systems, and has exhibited less capacity for innovation due to technical, regulatory and cultural factors. However, unlike DeFi, conventional financial services are often more accessible, convenient and easy to use for most banking-accustomed users. Moreover, regulation largely mitigates technical and financial risks for the end users. That is unlike services in DeFi that necessitate a high level of technical competency, are poorly integrated with existing deployments, and often come with ill-understood financial risks.

1.1.4 Overview of functional differences

Table 2 - Overview of functional differences

Feature	TradFi	DeFi
Accounting	Double-entry accounting bookkeeping.	Triple-entry accounting bookkeeping.
Trust	Trusted. Identity-based systems.	Mostly trustless.
Data availability	Transaction history is private. User is known.	History of financial transactions is publicly open. User is (pseudo)anonymous.
History and characteristics	Established. Slow and rigid in terms of innovation.	Nascent. Incrementally/radically innovative. Constantly changing, often faster than regulation can keep up with.
User experience	Easy to use. Embedded in everyday life.	Often difficult to use. More technical competency is required.
Risk	Risks are managed and thoroughly regulated.	Requires an individual understanding of the underlying risks.
Reversibility	Reversible transactions. Amend permissions.	(Mostly) irreversible transactions. Append only.

1.1.5 Operational differences

TradFi services rely on intermediaries who are also in custody of consumer assets. However, DeFi is (mostly) non-custodial, as participants can be in control of their own assets. TradFi services providers are also regulated, supervised and licensed entities that offer standardised financial services to identified users. Conversely, DeFi involves unregulated, unsupervised, unlicensed unknowns that offer unstandardised services to pseudonymous users, whether humans, organisations or other smart contracts and machines. This means that participating as a financial service provider or user in DeFi is accessible to everyone. Finally, TradFi is mostly operationally opaque, especially for end users, as entities are required to disclose only specific aspects of their operation to certain competent authorities. By contrast, DeFi's operation is publicly open and transparent, as all details are available in the blockchain for inspection.

1.1.6 Overview of operational differences

Table 3 - Overview of operational differences

Feature	TradFi	DeFi
Custody	Mostly custodial	Mostly non-custodial
Entities	Involves regulated, supervised and licensed entities that offer standardised services to identified users	Involves unregulated, unsupervised, unlicensed entities. Unknowns offer unstandardised services to anyone
Access	Gated access for supply and demand	Inclusive; anybody can offer or receive DeFi
Transparency	Mostly operationally opaque	Public and transparent operation

1.1.7 Regulatory landscape

TradFi is ruled by various legal and regulatory provisions, from financial services regulations to service contracts. DeFi applications are (technically speaking) ruled by code, as the functionality and boundaries of each application are limited to what has been specified in the smart contracts executing the application. This does not mean that DeFi is not ruled by law, as existing regulations are naturally applicable to DeFi applications, too. However, the automatically enforced execution of smart contracts, once they are deployed on a public blockchain, has certain implications regarding the applicability of existing legislation and the potential need for new rules governing the DeFi field. In this section, we briefly explore potential implications in the areas of transparency, investor protection and asymmetric information.

Beginning with transparency and openness, financial records in TradFi are maintained in accordance with regulations and are typically confidential (they can be accessed by authorised parties only). Conversely, in DeFi, records are typically immutable and can be accessed by anyone, since they live on-chain. In other words, the openness and transparency of financial record-keeping in DeFi is unprecedented, while at the same time there can be no provisions for data modification, deletion or transaction reversal after transactions have been included in verified blocks. This difference may have implications for data management and General Data Protection Regulation (GDPR)-related applications in DeFi, among other things.

With regard to consumer protection, this is also enforced in TradFi through regulatory and legislative measures. The same measures may or may not be applicable or enforceable in DeFi. For example, there is no method of filing a complaint against a company, as most interaction with DeFi applications happens through decentralised protocols and smart contracts not controlled by a central counterparty. This does not mean, of course, that consumers are entirely unprotected, as criminal behaviour in DeFi can still be dealt with through existing law enforcement. However, it is not always easy, especially for inexperienced users, to know their rights or the best course of action in unfamiliar situations.

Furthermore, in TradFi, specific regulations exist to deal with the asymmetry of information between retail users and professionals, especially for complex products. For instance, the need for a detailed prospectus for securities issuance, required by Regulation (EU) 2017/1129, governs what information and in what form must be disclosed to investors prior to making an informed investment decision. In DeFi, it can be argued that such asymmetry of information between common users and professionals does not exist, since everything is published on the blockchain. However, that is not the case in the initial stages of token issuance, for example, when developers have full knowledge of token economics and other details not known to investors – hence the perceived need to follow existing regulations or adapt them specifically for DeFi to address this asymmetry of information and protect users.

1.1.8 Overview of regulatory landscape

Table 4 - Overview of regulatory differences

Feature	TradFi	DeFi
Regulation	Ruled by law	Ruled by law and code
Record-keeping	Governed by regulation; confidential	Openly accessible
Consumer protection	Governed by regulation	Unclear whether existing regulations apply or new ones are needed

1.1.9 DeFi vs TradFi

TradFi – and to a certain extent DeFi – are umbrella terms encompassing technologies, user preferences and procedures. In generalising their similarities and differences, some important aspects are lost. For the sake of comparison, however, TradFi and DeFi differ in at least three major ways: ideology, infrastructure and innovation. At the same time, they present similarities in their human and consumer aspects, such as marketing, recruitment and even governance.

Table 5 – differences between DeFi and TradFi

Feature	TradFi	DeFi
Ideology	Efficiently allocate resources and facilitate commerce, investment and development	Make financial services accessible to everyone
Infrastructure	Private database	Open blockchain/DLT
Innovation	Incremental and sustaining	Radical and disruptive
Human-facing aspects	Brick and mortar; Web 2.0	Web 2.0 transitioning to Web 3.0

The underlying ideology of DeFi, i.e. making financial services available to everyone, stems from the realisation that besides money and simple payments, public, open, decentralised blockchains can also make more complex financial services available to all. As a result, the choice of technologies is important, and besides ideology, represents DeFi's biggest difference from TradFi. Whereas the latter opts for efficient solutions that comply with existing systems and procedures (despite artificially inflated costs and settlement times), protocols in DeFi opt for solutions that make financial services accessible to most, sometimes at the expense of efficiency. The DeFi technology stack (explored later) includes public blockchains for transaction and state transition settlement, protocols build on top, as well as Web 2.0 interfaces for interacting with the protocols. TradFi, on the other hand, mostly relies on private databases, Web 2.0 applications and brick-and-mortar branches.

Decentralisation is another important component of DeFi. In contrast to TradFi, where centralised procedures facilitate compliance and economies of scale, DeFi protocols aim for a more decentralised approach, from the way they are built, maintained and governed, again at the expense of efficiency. However, as highlighted in the Bank of International Settlements' recent report, creating contracts that cover all possible eventualities is very difficult, if not impossible. This contrasts with the deterministic and immutable nature of smart contracts. To mitigate this, certain aspects of some DeFi protocols, predominately governance and admin key access, present some degree of centralisation. Specifically, most DeFi protocols rely on a governance scheme, where governance token holders vote on certain decisions, which are then usually implemented either through forks or administration keys, meaning smart contracts that can update/modify the protocol in certain ways. Although admin keys often are time-locked multi-signature deployments, they represent a centralised component. Protocols with no admin keys, such as Uniswap, are in practice non-upgradable. While no gold standard for decentralisation exists, the degree of decentralisation of DeFi protocols mostly relies on the aspects described above, namely the distribution and ownership of governance tokens, as well as ownership and management of admin keys.

TradFi and DeFi also differ in the types of innovations they produce. Innovation is a well-defined concept, but for our analysis we draw upon the works of Clayton Christensen and Greg Satell, who broadly recognise four types of innovation: (1) incremental, (2) sustaining, (3) disruptive, and (4) radical. TradFi, for the most part, produces and relies on incremental and sustainable innovations. Incremental innovations constitute gradual and continuous improvements on existing financial products and services. Sustainable innovations are substantial improvements that aim to sustain the position of a provider in an existing market. Incremental improvements on existing financial services fall under the incremental innovations, whereas newer concepts, such as fintech, represent sustainable innovation. On the contrary, DeFi represents a radical advance, producing disruptive innovations. Radical innovations are technological breakthroughs that transform industries and create new markets, such as the untapped market for offering financial services to the unbanked and underbanked, and the capturing by DeFi of individuals previously uninterested in traditional investments. At the same time, disruptive innovations are new technologies or business models that disrupt existing markets. Numerous examples exist within DeFi, from automated market makers (AMMs) to flash loans, protocol-owned liquidity and more.

Finally, DeFi and TradFi are most similar in their user-facing and human-reliant aspects. Both TradFi and DeFi rely on human beings for the development and promotion of their applications. As a result, there is some overlap in how TradFi and DeFi fund, recruit, market and offer their services. Both TradFi and DeFi promote their services online (although outright advertising is less common in DeFi), and recruit employees through online forms and forums. At the same time, most of their services are offered through standard Web 2.0 interfaces. However, it is important to note that DeFi is moving towards Web 3.0 community-governed-and-maintained solutions, for funding, promotion and recruitment.

SECTION 1.2: DEFI FUNDAMENTALS

The technology stack on which DeFi is built can be separated into five major components: (1) settlement layer, (2) asset layer, (3) protocol layer, (4) application layer, and (5) aggregation layer.

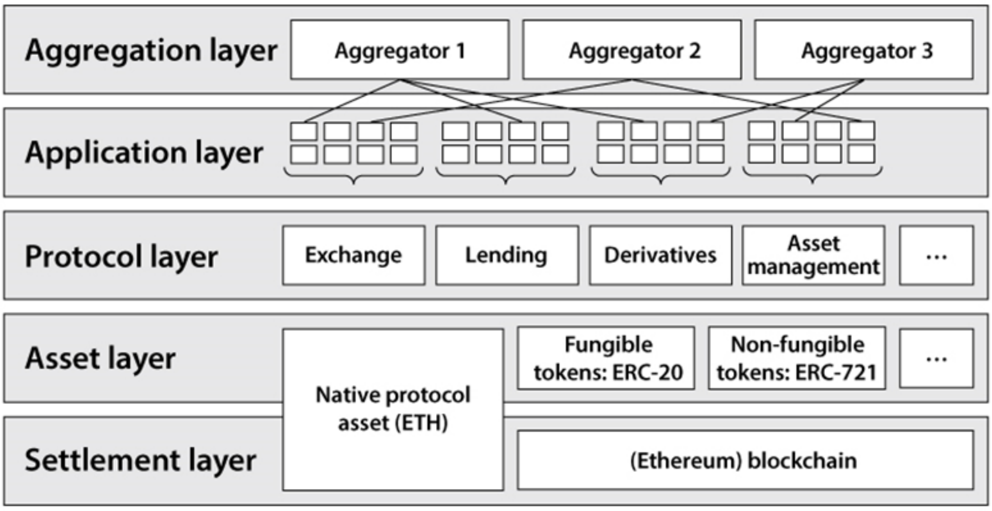


Figure 1 – The DeFi Stack

The foundational layer on which all distributed ledger technologies rest (and transitively, all of DeFi) is the settlement layer. In this report we will also refer to it simply as 'blockchain' or Layer 1. At its core, the settlement layer or blockchain consists of a means to agree on the order of valid transactions that cause an update to a local state to achieve state machine replication in a distributed system. The state of a distributed system consists of the current set of unspent transaction outputs (UTXOs) or the current account balances of the native asset, depending on whether the model is UTXO or account based. In blockchains that support smart contracts, the overall state also includes the state of all smart contracts, meaning their on-chain logic, associated account balances and data for authorised queries. The settlement Layer 1 is also defined as a distributed system that uses its own consensus protocol as the ultimate source of truth for the validity of a transaction. Layer 2s (L2s), on the other hand, use an L1 and its underlying consensus mechanism for determining the validity and finality of transactions that occur on the L2. Smart contract functionality is a necessary component needed for both the asset and the protocol layers of the DeFi stack. The asset layer consists of different types of tokens that have various functionalities. The purposes of these assets range from utility or governance tokens of a protocol to tokens that represent the receipt of a deposit into a smart contract to non-fungible tokens (NFTs). These assets are created using a standardised smart contract specification, such as the ERC-20 or ERC-721 standards, which are used throughout the Ethereum and compatible ecosystems. The internal logic of any DeFi application is defined by the protocol layer which consists of one or more independent smart contracts that dictate the rules of the protocol.

The application layer consists of a standard Web 2.0 user interface that connects a wallet, such as MetaMask or Phantom, to a smart contract, and creates a user-friendly way to interact with the DeFi protocol, by signing, creating and submitting valid transactions.

DeFi protocols that attempt to achieve the same type of functionality, such as AMM protocols (further explained in Section 2.2), can often benefit from aggregation. The aggregation layer combines the application layers of different protocols of the same type into a single interface. In the instance of an AMM aggregator, the assets deposited in liquidity pools across different protocols are combined to provide users with better quotes when trading one asset in a pool for another.

The aggregation layer is a minor example of composability or money Legos. In general, different DeFi applications can be combined to achieve functionality beyond the original design of a protocol. Composability naturally allows for smart contracts to interact with other smart contracts in a streamlined fashion, or when automation does not exist natively, can allow users to manually compose different DeFi primitives themselves.

For example, automated secured lending protocols (further discussed in Section 2.1), such as Compound or AAVE, or protocols that issue collateralised debt positions (CDPs), such as MakerDAO, can be composed with an AMM protocol such as Uniswap, to allow for leveraged trading, which is not a feature immediately available to users of an AMM.

Composability can be as simple as aggregating liquidity across liquidity pools in different AMMs or can consist of numerous different money Legos. Nonetheless, it allows developers and users to treat DeFi primitives as independent building blocks, which are the pillars of open financial systems.

In Subsections 1.2.1 and 1.2.2, we expand upon the role of the settlement and asset layers and the interactions between each. In addition, we describe several families of L1s in Subsection 1.2.1, different types of assets and their roles in DeFi in Subsection 1.2.2, the blockchain trilemma in Subsection 1.2.3, and present several off-chain scaling solutions to address the blockchain trilemma in Subsection 1.2.4.

1.2.1 The settlement layer

From an overall perspective, the settlement layer of blockchain systems can be considered a 'black box'. This black box uses a consensus or Byzantine agreement protocol to achieve consensus on the order of valid transactions that change the underlying state of the distributed system. Nodes of the network then apply the state transitions in this agreed format to store and track a local copy of the blockchain. As such, one settlement layer can theoretically be swapped for a different settlement layer with little impact on the way the DeFi works. Yet we must bear in mind that altering the underlying settlement layer can change the security properties of all abutting deployments.

The different settlement layers and their associated consensus protocols fall broadly within various families of Byzantine agreement protocols. The first classification that can be applied is whether a settlement layer operates as a permissioned or a permissionless protocol. A permissioned protocol restricts the authorised set of parties who have the ability to approve valid transactions and their corresponding order. On the other hand, a permissionless protocol allows parties to voluntarily participate in the consensus with the ability to enter or leave the network at will. In keeping with DeFi's goal of openness and decentralisation, most applications utilise permissionless settlement layers.

Most permissioned platforms, such as Ethereum Enterprise, employ a slightly modified classical Byzantine agreement protocol termed Proof of Authority (PoA) to reach consensus. In the simplest case, PoA has a static set of nodes operating a Byzantine agreement protocol, such as Paxos or PBFT, and is not different from the classical understanding of consensus. In a more complex scenario, a centralised authority could update the authorised nodes participating in the consensus protocol between rounds. Alternatively, PoA could operate in a manner where there is a larger pool of authorised nodes determined by a governing authority and a fixed-size subset of the nodes are chosen from this pool to operate a consensus protocol in rounds. Broadly, in any PoA design, block production is limited to an authorised set of nodes that is determined by a governing body.

The innovation of the Nakamoto protocol is that it is the first permissionless Byzantine agreement protocol. The Nakamoto consensus and its different variants are based on the longest-chain rule. They work by combining economic incentives to encourage honest behaviour by block producers who are chosen using an anti-Sybil mechanism that requires access to a limited resource, e.g. computing power in Proof of Work, coins in Proof of Stake, hard drive space in Proof of Capacity, etc. In this way, a participant becomes an authorised block producer after winning a randomised lottery (where tickets are based on the scarce resource used for achieving Sybil resistance) and has the complete authority to choose transactions to include in a block. However, the Nakamoto protocol and all the longest-chain rule Byzantine agreement protocols are probabilistic. In other words, a transaction or a block of transactions does not have the same guarantee of being final and officially committed to the log of transactions as is the case with permissioned Byzantine fault-tolerant (BFT) protocols. Practically, this has not been a major security concern as controlling the scarce resources used for the anti-Sybil mechanism of well-established networks is quite cost-prohibitive. However, one downside with settlement layers that use a Nakamoto protocol variant is reduced latency and throughput capacity. This limitation can be considered a result of the blockchain trilemma (see Subsection 1.2.3) and has led to innovations in the design of improved L1s or using L2s (described in more detail in Subsection 1.2.4) for off-chain scaling solutions.

More recently, hybrid consensus models have been proposed as solutions to address scalability issues. In this model, an anti-Sybil scheme is used to select multiple lottery winners to act as a committee that operates a classical BFT protocol for a brief period of time. The advantage of a hybrid consensus model is that the key properties of the chosen BFT protocol – namely finality and throughput capabilities – extend to the settlement layer. Even within the hybrid consensus family, lots of variations exist since both the choices of the anti-Sybil mechanism and the Byzantine agreement protocol that can be used are independent.

Further classifications of BFT protocols can be broken down into network assumptions regarding synchrony, whether the protocol is leader-based or leaderless, communication and latency complexity, or whether the protocol employs directed acyclic graphs (DAGs). Many of the L1s that currently operate hybrid consensus models primarily use practical Byzantine fault tolerance (PBFT)-like (Solana and Cosmos) or DAG-based classical Byzantine agreement protocols (GRANDPA, Hashgraph, AlephBFT, Lachesis) combined with Proof of Stake. Two notable Layer 1s, Algorand and Avalanche, do not fall under either of these two sets for the choice of the BFT protocol. Algorand uses a leader-based Byzantine agreement protocol that differs from PBFT. While Avalanche employs the use of a DAG, the protocol uses a polling mechanism to probabilistically determine the state of a transaction (Rocket et al., 2019), which differs significantly from classical consensus protocols.

Table 6 – Consensus algorithms and smart contract language of major DeFi blockchains

Project name	Consensus algorithm	Smart contract language support
Aleph Zero	Hybrid: PoS + aBFT: AlephBFT	WASM
Algorand	Hybrid: PoS + BA	AVM
Avalanche	Snowman	EVM
Binance Smart Chain	Proof of Staked Authority	EVM
Cardano	PoS + Ouroboros	Plutus
Cosmos	Hybrid: PoS + Tendermint	WASM
Ethereum	PoW	EVM
Ethereum 2.0	PoS	Ewasm
Fantom	Hybrid: PoS + aBFT: Lachesis	EVM
Harmony	Hybrid: PoS + fastBFT	EVM
Hedera	PoA + aBFT: Hashgraph	EVM
Polkadot	Hybrid: PoS: GRANDPA + BABE	EVM or WASM
Polygon	Hybrid: PoS + Tendermint	EVM
Solana	Hybrid: PoS + PoH	LLVM

1.2.2 The asset layer

With the use of smart contracts, new assets can be created for a variety of purposes, particularly within DeFi. Within blockchain systems, the asset layer ‘sits’ on top of the settlement layer and all assets have an associated database that stores account balances of the asset; as previously described, changes to an account balance are made by processing transactions at the settlement layer.

DeFi-specific tokens are vital for virtually every kind of application. Indicatively, in AMMs, liquidity pool tokens allow for the exchange of two or more assets held by the liquidity pool smart contract at an algorithmically determined rate. When the correct ratio of assets is deposited into the liquidity pool, new liquidity tokens are issued. Likewise, when liquidity is removed, liquidity pool tokens are ‘burned’, or removed from the circulating supply and exchanged for the assets held by the liquidity pool smart contract at the prevailing rate. Tokens can also represent protocol debt issued in the form of CDPs. Utilising oracle price feeds, protocols remain solvent by monitoring the value of all the assets used as collateral relative to the current value of the loan for any given account.

1.2.3 The blockchain trilemma

There are three key concepts that are shared by any blockchain design.

1. Decentralisation: network control takeover resilience; capacity to spread the control over many nodes.
2. Security: network immunity on internal and external threads; ability to continue operation despite being under an attack.
3. Scalability: network ability to expand and to process more transactions.

Historically, the first blockchain designs focused on decentralisation and security as their main objectives. Later, when networks started to proliferate, the problem of scalability arose, i.e. networks were unable to process enough transactions in a given time.

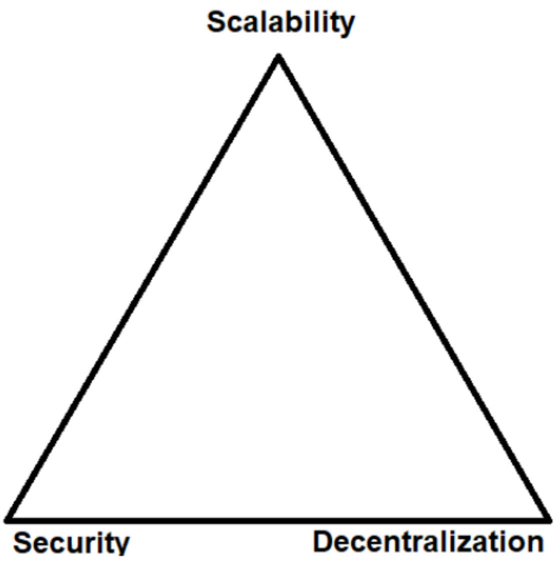


Figure 2 – Blockchain trilemma

Trying to describe the fundamental difficulties faced by blockchain developers working on improving the scalability of their blockchains, one of the key founders of the Ethereum blockchain project, Vitalik Buterin, posed the following trilemma. By design, a blockchain can be scalable and secure, but not decentralised; or secure and decentralised, but not scalable; or scalable and decentralised, but not secure. It is an open question if the trilemma is true. One of the difficulties of proving the trilemma lies in defining decentralisation, security and scalability in an objective manner. Empirical observations from industry indicate that practical implementations of blockchain technologies require trade-offs to be made in one of the three properties to improve any of the other two.

1.2.4 Off-chain scaling solutions

Recently, L2 scaling solutions have been seen as a promising solution to overcoming the scalability aspect of the blockchain trilemma. In this paradigm, the execution of a transaction is decoupled from its commitment of being finalised on-chain. This separation allows for off-loading transactions to a secondary layer in a way that reduces the full node requirements from verifying and executing every transaction, which can be a major bottleneck and minimises the information that is provided to the main chain. In addition, this type of approach allows for incremental improvements of pre-existing chains that have substantial market share and value, scale poorly and cannot be easily changed, as in the case of Ethereum. Alternatively, new blockchain ecosystems can adopt this architecture from the beginning.

One notable approach that falls under the shared security model, which is to say that the scaling solution inherits or shares the security of an extended L1, is the use of rollups. Side chains are another scaling solution that do not fall under the shared security model. Rather, side chains maintain their own Layer 1 security and bridge to other Layer 1s. Finally, state channels offer a third approach to scaling an L1.

Side chains address the scalability problem by running a parallel L1 chain to another L1 chain. Therefore, the side chain should be treated as a separate and independent blockchain with security provided by itself. As such, transactions made on the side chain are protected only by the consensus mechanism of the side chain, and the side chain does not inherit the security of the other L1 chain. Furthermore, side chains rely on a bridge construction, which enables the transferring of assets between the L1 and the side chain. The design of a bridge is paramount to the security of the side chain, as it governs the transfer of assets between two independent blockchains.

State channels enable the direct update of a state between two or more blockchain users, which occurs off-chain. Setting up a channel requires locking the state in a dedicated smart contract. Only the state that is locked can be updated in the channel and only by the parties that participate in the channel. The state updates can happen instantly without any limitations to the number of transactions, but the channel is constrained only by the parties in the initial setup. However, state channels with more than two persons are generally more difficult and less flexible than other scaling techniques.

Rollups protocols allow transactions to be executed, collected and rolled into a batch off-chain; after finalisation, only a brief confirmation of what happened off-chain is sent to the L1. The rolling into a batch may be optimistic or zero-knowledge (ZK). Optimistic rollups (ORs) assume that every transaction is valid until proven invalid. Therefore, every transaction is added to the rollup; if any user finds the transaction invalid, a fraud proof is submitted to the network. However, if the proof is correct, the transaction is then removed from the rollup. This fraud proof must be submitted during a challenge period, after which all transactions in the rollup are considered valid and the rollup is published on the L1. Zero-knowledge rollups (ZKRs) rely on zero-knowledge proofs (ZKPs), which mathematically guarantee that the transaction is valid. These validity proofs are generated with only a small subset of information related to transactions and can therefore limit the amount of data posted on the L1 chain. ZKRs require more computation power to generate proofs than the ORs, which at the same time eliminates the waiting period for publishing optimistic fraud proofs.

Table 7 – DeFi scaling technologies

Project name	Scaling technology	Smart contract language support	Intended use case	L1
Arbitrum	Optimistic rollup	EVM	General purpose	Ethereum
Celestia	Optimistic rollup	WASM	General purpose	Cosmos
Hydra	Isomorphic state channel	Plutus	General purpose	Cardano
Immutable X	Zero-knowledge rollup or Validium zero-knowledge proof	–	NFT	Ethereum
Lightning Network	State channel	–	Payments	Bitcoin
Loopring	Zero-knowledge rollup	–	Trading and payments	Ethereum
Optimism	Optimistic rollup	EVM	General purpose	Ethereum
Raiden	State channel	–	Payment	Ethereum
RSK	Side chain	RVM	General purpose	Bitcoin
StarkNet/StarkEx	Zero-knowledge rollup	Cairo	General purpose	Ethereum
xDai	Side chain	EVM	General purpose	Ethereum

SECTION 1.3: THE DEFI MARKET SIZE

The first sparks of DeFi started in 2017 with the EtherDelta experiment, which despite being less successful than anticipated, paved the way for what was to come in the years ahead. In December 2017, with the launch of MakerDAO, avenues of financial application (apart from just money transfers) were opened. This was carried further with the launch of Uniswap (which enabled trading via user capital pooled in the protocol's smart contracts in 2018) and Synthetix (which enabled incentivising of users to contribute to liquidity pools in 2019). More DeFi protocols were launched on the Ethereum Mainnet between 2018 and 2019 including Compound, REN, Kyber and 0x; some of them are leading DeFi service providers now. However, their adoption was limited in the first 12 months. In February 2020, the total value locked (TVL) in all DeFi protocols surpassed USD 1 billion for the first time. Interest in the DeFi space was just picking up when the young sector then suffered heavy losses during the 12 March 2020 global market crash due to the COVID-19 pandemic. This was followed by a period of hesitancy until the Compound protocol issued its token, which was a major contributor in starting the summer of DeFi in 2020. Other protocols which further accelerated this movement were Yearn Finance and SushiSwap which were able to attract high liquidity. This was capped by the issuance of Uniswap tokens (UNI) with added functionalities of liquidity mining. This resulted in Uniswap's monthly volume going from USD 169 million in April 2020 to over USD 15 billion in September 2020.

1.3.1 Market size

As mentioned in the previous sections, the DeFi market has grown exponentially since its early days in 2020, with the TVL and wallets in use being the most important metrics in understanding the DeFi market size and user base engaged in the DeFi space. TVL is a measure of the amount of capital locked inside DeFi protocols. It has been increasing at a breakneck speed, surpassing USD 1 billion in May 2020 and lately surpassing USD 250 billion in November 2021.

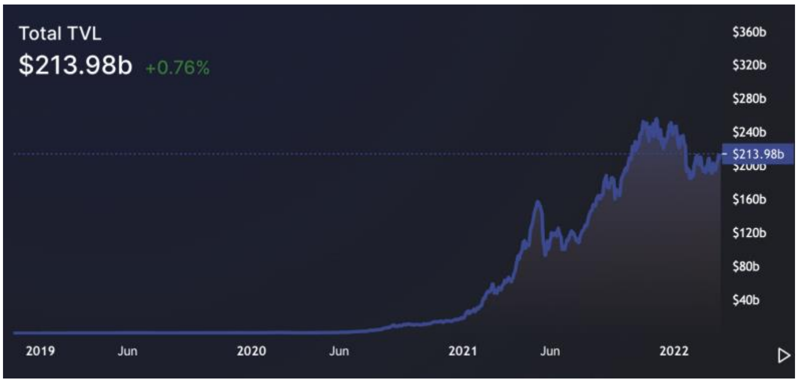
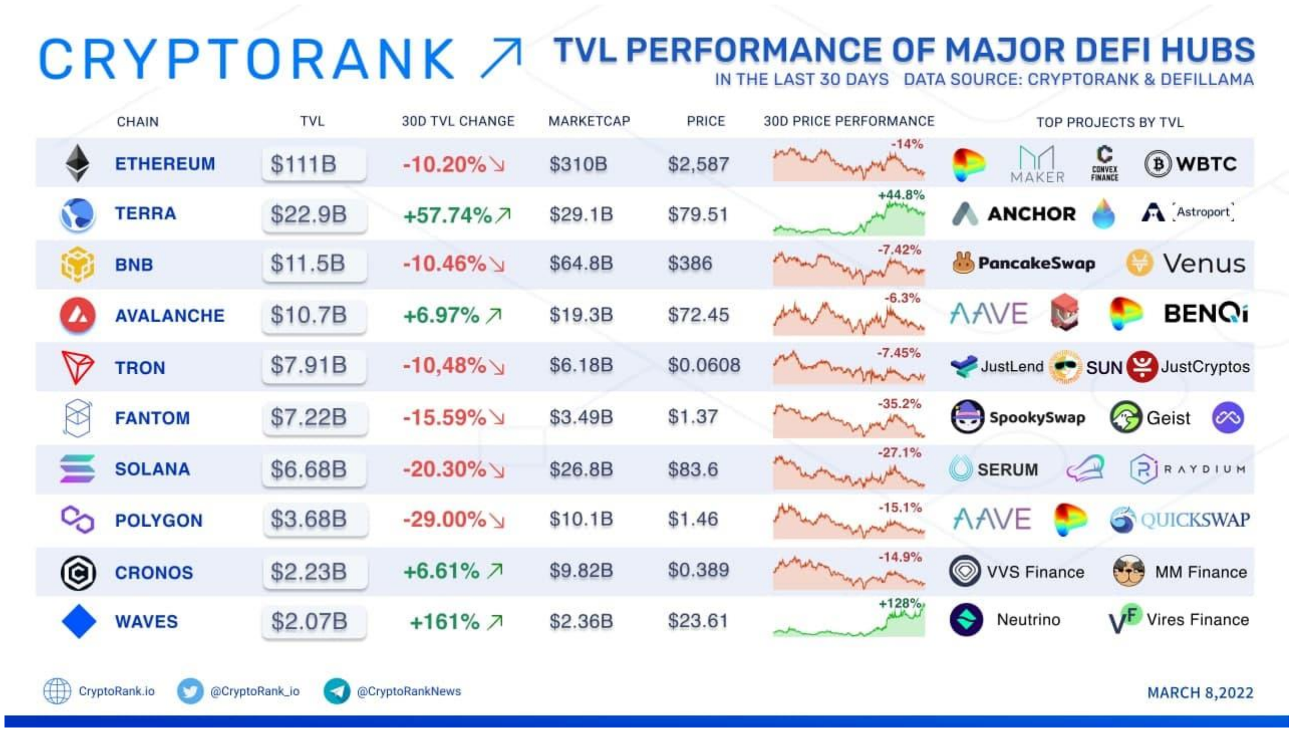


Figure 3



CRYPTORANK ↗ TVL PERFORMANCE OF MAJOR DEFI HUBS

IN THE LAST 30 DAYS DATA SOURCE: CRYPTORANK & DEFILLAMA

CHAIN	TVL	30D TVL CHANGE	MARKETCAP	PRICE	30D PRICE PERFORMANCE	TOP PROJECTS BY TVL
ETHEREUM	$111B	-10.20%↘	$310B	$2,587	-14%	MAKER, CONVEX FINANCE, WBTC
TERRA	$22.9B	+57.74%↗	$29.1B	$79.51	+44.8%	ANCHOR, Astroport
BNB	$11.5B	-10.46%↘	$64.8B	$386	-7.42%	PancakeSwap, Venus
AVALANCHE	$10.7B	+6.97%↗	$19.3B	$72.45	-6.3%	AAVE, BENQI
TRON	$7.91B	-10,48%↘	$6.18B	$0.0608	-7.45%	JustLend, SUN, JustCryptos
FANTOM	$7.22B	-15.59%↘	$3.49B	$1.37	-35.2%	SpookySwap, Geist
SOLANA	$6.68B	-20.30%↘	$26.8B	$83.6	-27.1%	SERUM, RAYDIUM
POLYGON	$3.68B	-29.00%↘	$10.1B	$1.46	-15.1%	AAVE, QUICKSWAP
CRONOS	$2.23B	+6.61%↗	$9.82B	$0.389	-14.9%	VVS Finance, MM Finance
WAVES	$2.07B	+161%↗	$2.36B	$23.61	+128%	Neutrino, Vires Finance

CryptoRank.io @CryptoRank_io @CryptoRankNews

MARCH 8,2022

Figure 4 – TVL performance of major DeFi hubs

The dominance of TVL on Ethereum has dropped from a mammoth 94 % in August 2020 to a still formidable 66 % with 185 billion in TVL in November 2021 and it has dropped further to $111 billion in TVL in March 2022. It is distinctly followed by Terra (22.9 billion in TVL), Binance (11.5b in TVL), Avalanche (10.7b in TVL), Tron (7.91 billion in TVL), the other members of the top 5 DeFi TVL club.

The major applications across DeFi include DEXs, lending protocols, yield farming protocols, and aggregators.

- When we look at the current DEX landscape, Curve with USD 16+ billion in TVL tops the charts, followed by Uniswap with USD 5+billion in TVL, SushiSwap with almost USD 4 billion in TVL, PancakeSwap with USD 36+ billion in TVL, and Balancer with USD 2+ billion in TVL, which all make up the top 5 DEXs in the market.
- In the case of lending protocols, AAVE with USD 9+ billion in TVL, Anchor with USD 7+ billion in TVL, Compound with USD 5+ billion in TVL, Abracadabra with almost USD 4 billion in TVL, and Venus (USD 1+ billion in TVL) are the top 5 lending protocols in the market.
- For yield farming, Convex Finance with USD 14+ billion in TVL, Yearn Finance with USD 3+ billion in TVL, Alchemix with almost USD 1 billion in TVL, Beefy Finance with almost USD 1 billion in TVL as well and Tokemak with USD 900+ million in TVL make up the top 5 of the yield farming list.

N.B: *Due to the high volatility of the DeFi space, these lists keep changing as per market performance. The values shown here were observed in the last week of January 2022.*

1.3.2 DeFi user base over the years

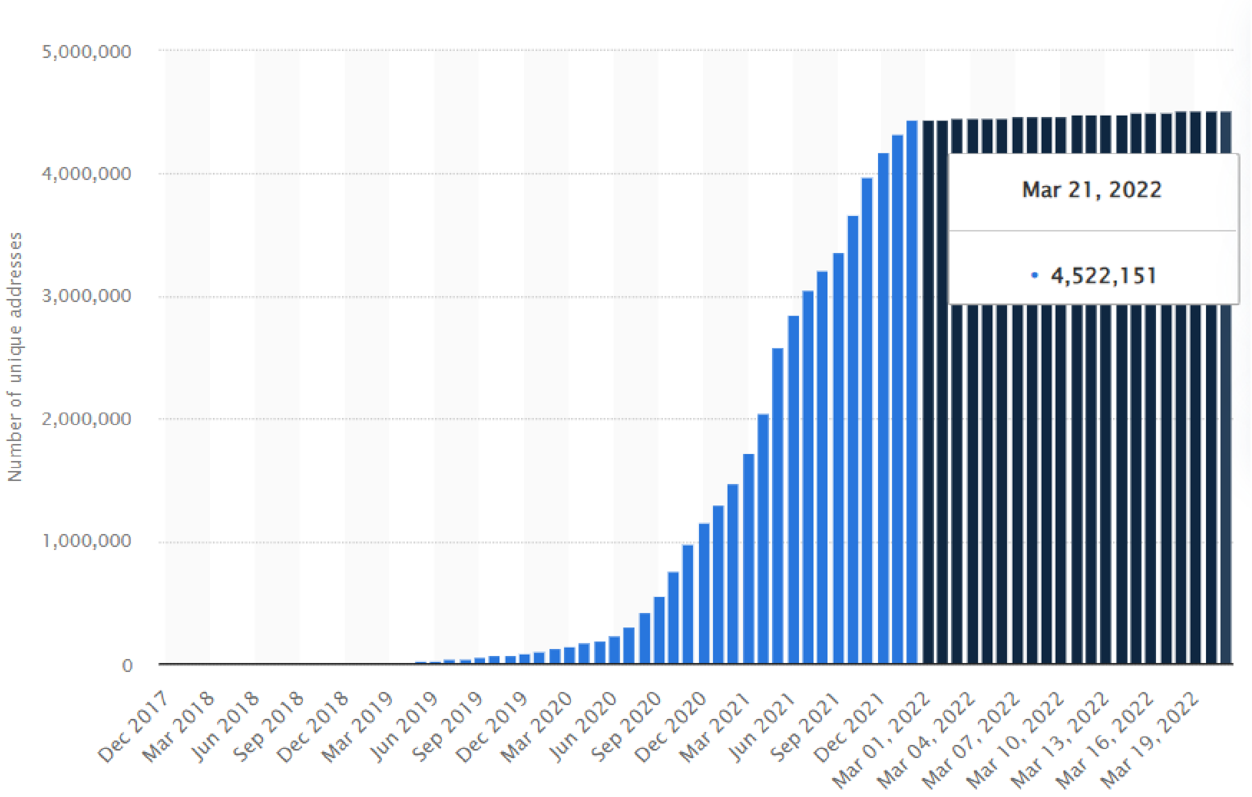


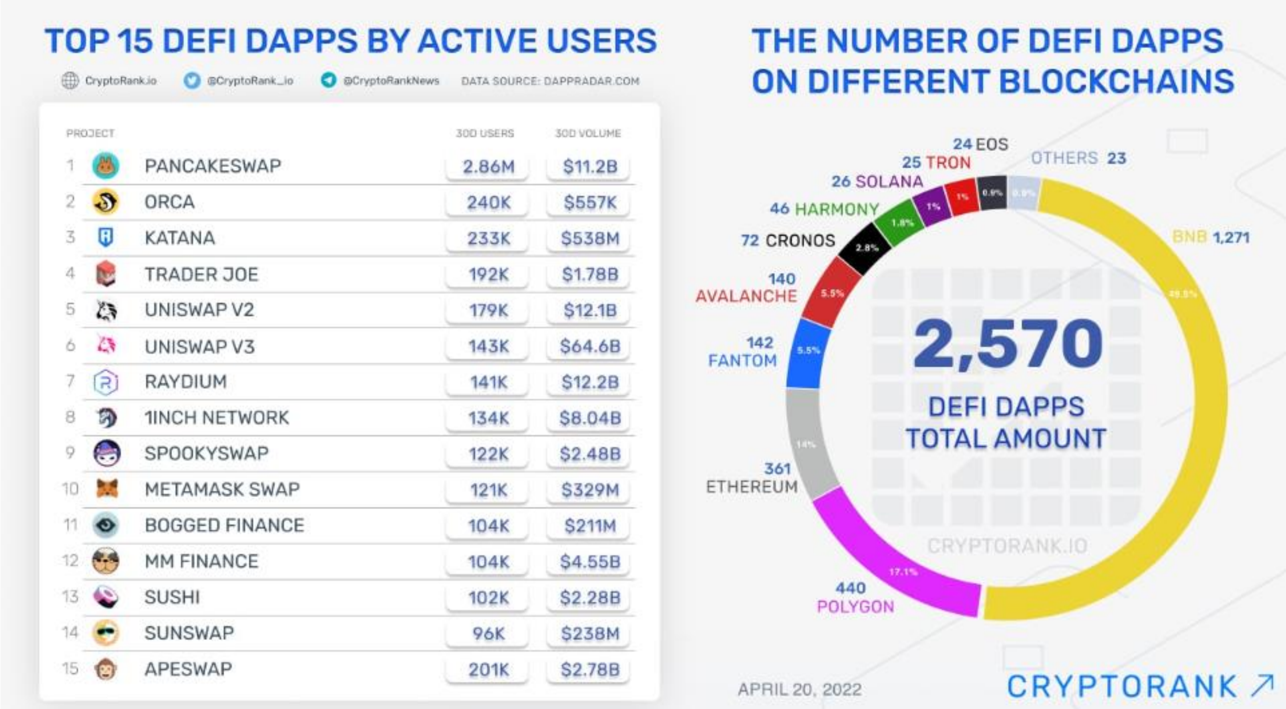
Figure 5 – DeFi address growth

By March 2022, the active DeFi address base had increased to more than 4 000 000 with DeFi protocols such as Compound, SushiSwap and Uniswap expanding their portfolio of functions and providing token airdrops. The number of addresses engaged in DeFi has grown ever since. We can estimate the number of users actively participating in DeFi by referring to the amount of monthly active users of DeFi (non-custodial) wallets such as MetaMask. The address base of MetaMask grew by 1 800 % between July 2020 and August 2021, which is nothing short of astounding. In numbers, it translated to an increase in user base from 545 080 monthly active addresses in July 2020 to 10 354 279 in August 2021.

August to December of 2021 has seen an even more accelerated growth, with MetaMask reaching the milestone of 21 million active addresses in November 2021 and now supporting applications across Ethereum and Ethereum-compatible chains such as Polygon, Arbitrum and Optimism.

The numbers depicted in the chart below of the address engagement in the month of November across DeFi protocols shows a high level of activity across different DeFi protocols.

With the crypto address base already exceeding 300 million, DeFi growth still has a lot of room to grow. The speed of the rise will be supported by development of DeFi protocols on other prominent blockchains such as Polygon, Solana, Polkadot, Cosmos and Avalanche, which envision providing faster and cheaper transactions at scale without compromising security. But that will take time and we will see Ethereum being the major hub for DeFi for some time. It is worth noting that addresses do not necessarily translate to users, as multiple addresses can be owned by the same individual person or organisation.



TOP 15 DEFI DAPPS BY ACTIVE USERS

CryptoRank.io @CryptoRank_io @CryptoRankNews DATA SOURCE: DAPPRADAR.COM

	PROJECT	30D USERS	30D VOLUME
1	PANCAKESWAP	2.86M	$11.2B
2	ORCA	240K	$557K
3	KATANA	233K	$538M
4	TRADER JOE	192K	$1.78B
5	UNISWAP V2	179K	$12.1B
6	UNISWAP V3	143K	$64.6B
7	RAYDIUM	141K	$12.2B
8	1INCH NETWORK	134K	$8.04B
9	SPOOKYSWAP	122K	$2.48B
10	METAMASK SWAP	121K	$329M
11	BOGGED FINANCE	104K	$211M
12	MM FINANCE	104K	$4.55B
13	SUSHI	102K	$2.28B
14	SUNSWAP	96K	$238M
15	APESWAP	201K	$2.78B

THE NUMBER OF DEFI DAPPS ON DIFFERENT BLOCKCHAINS

APRIL 20, 2022

CRYPTORANK ↗

Figure 6 – Top DeFi apps by address activity as of April 2022

Chapter 2: DeFi applications

In this chapter, we provide an overview of prominent DeFi applications.

SECTION 2.1: STABLECOINS

What arguably hinders the ability of decentralised cryptocurrencies' utility in the context of DeFi is their failure to serve as an effective unit of account and as a widely used medium of exchange, two of the three basic functions of money. This is largely due to their decentralised issuance and high exchange-rate volatility. To combat those 'shortcomings', a new form of digital currency emerged, commonly known as stablecoins. Stablecoins aim to address the volatility of cryptocurrencies and constitute a blockchain-native unit of account. At the same time, they maintain most of the desirable characteristics of their non-stable cryptocurrency counterparts, and most importantly for DeFi, composability and programmability.

In addition, stablecoins are digital currencies that aim to maintain a stable value against a set target price. This set price can be that of any financial or real asset, or even of a collection of assets. Since most stablecoins aim to serve as an effective unit of value, the elected target price is usually that of the United States dollar. Price parity between the stablecoin and the external asset can be achieved either through collateralisation or algorithms. While algorithmic stablecoins employ elastic supply mechanisms and rely on market forces to maintain parity, collateralised stablecoins are instead backed by either traditional assets, such as fiat currencies and commodities, or digital currencies. Notable fiat-collateralised stablecoins include USDT, TrueUSD and USDC, while popular DAI is backed by digital assets. The algorithmic stablecoin space is less populated. The interest of the public in stablecoins has grown over the years. In 2020 specifically, following the March 2020 market instability, increasing retail appeal and interest-bearing use cases emerged from the DeFi space and the need for stablecoins increased. Within a year, from January of 2020 to January of 2021, the collective market capitalisation of the 12 stablecoins included in the Messari Index increased by more than five times from USD 5 billion to over USD 25 billion. The rising need for stablecoins has remained constant, having increased by another factor of 5, from January 2021 to approximately USD 125 billion in September of 2021.

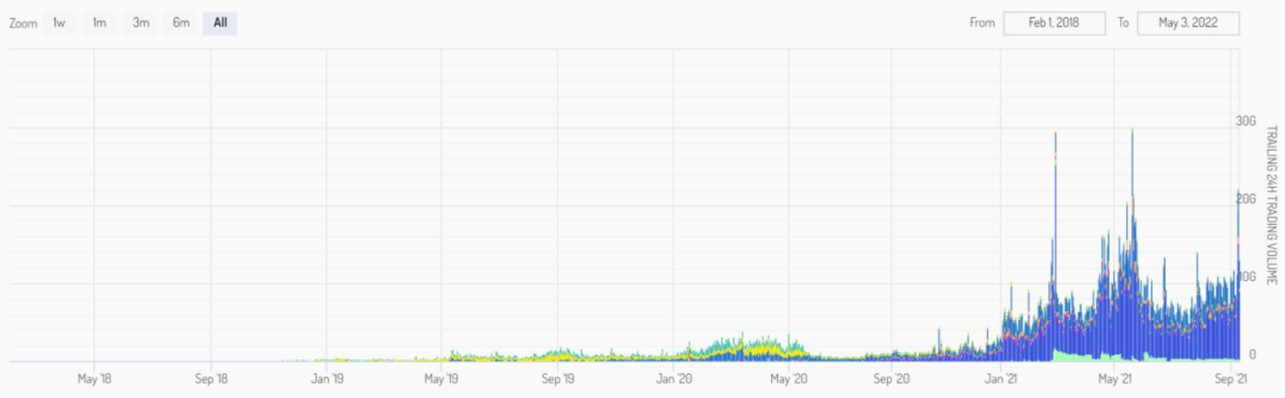


Figure 7 – Stablecoin 24h trading volume between February 2018 and February 2022 – Messari Index

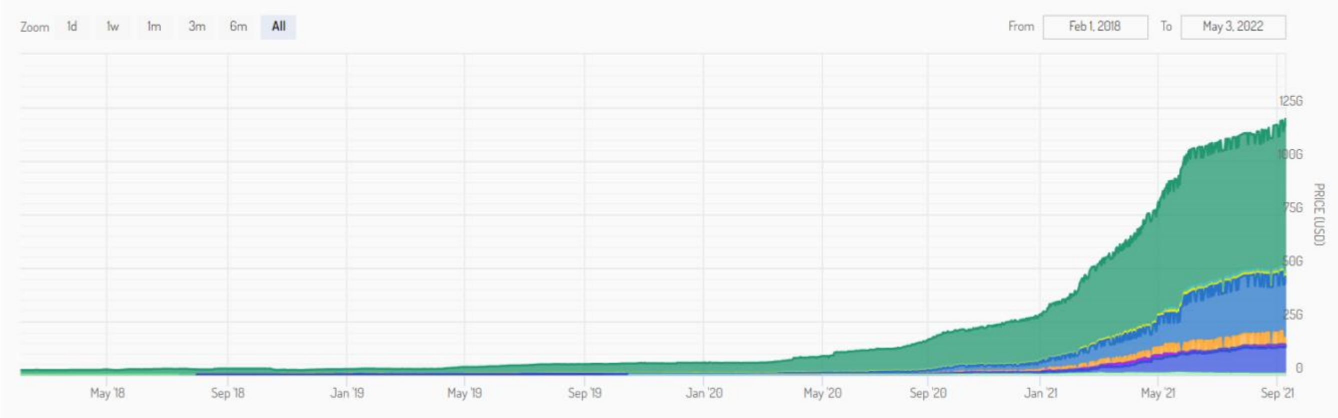


Figure 8 - Stablecoin market capitalisation between February 2018 and February 2022 – Messari Index

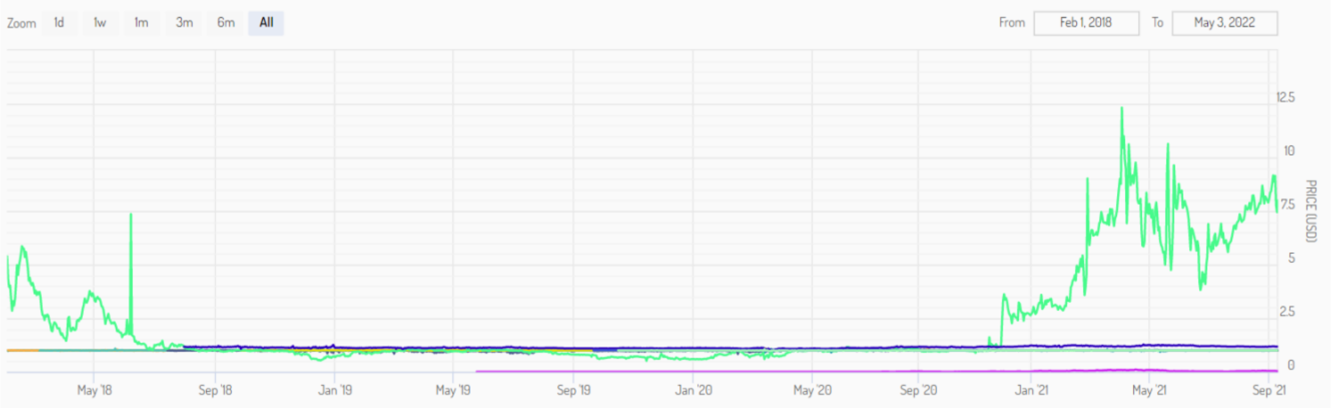


Figure 9 - Stablecoin trading volume between February 2018 and February 2022 – Messari Index

2.1.1 Stablecoin taxonomy

As noted, stablecoins use a variety of techniques to minimise volatility and maintain a stable price against their target. They can also be issued either by centralised custodians or in a decentralised manner.

We can thus broadly categorise stablecoins based on:

(1) their degree of (de)centralisation
(2) their mechanism for maintaining their peg.

In terms of decentralisation, we identify:

(1.1) custodian, or centralised stablecoins
(1.2) non-custodian, or decentralised stablecoins.

In terms of mechanisms, we identify:

(2.1) reserve-backed
(2.2) collateral-backed
(2.3) algorithmic
(2.4) mixed-approach stablecoins.

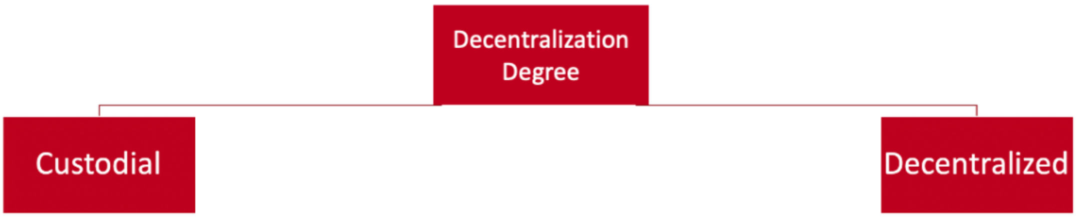


Figure 10 - Stablecoin degree of decentralization

For custodial stablecoins (1.1), centralised entities, often in the form of company consortia, maintain off-chain collateral backing the stablecoin. The collateral usually includes money and money equivalents, and the stablecoin is essentially an on-chain representation of this collateral. Such custodian deployments come with the usual benefits and drawbacks of centralised systems: being efficient, but at the same time prone to censorship, single points of failure, as well as lack of transparency and auditability. However, it should be noted that unlike fintech deployments sharing some similarities with custodian stablecoins, the latter are deployed on open blockchains and are composable, programable and accessible by anyone. Finally, custodial stablecoins introduce holders to counterparty risk since they essentially operate as IOUs. Decentralised stablecoins (1.2), on the other hand, rely on on-chain collateral and smart contract-backed algorithms to maintain their peg. Collateral-based stablecoins closely resemble traditional risk-transfer instruments such as collateralised debt obligations (CDOs). As a result, decentralised stablecoins are less capital efficient (for similar reasons as DEXs and lending/borrowing in DeFi is inefficient), but are transparent, censorship resistant and accessible to everyone, on top of being composable and programmable.

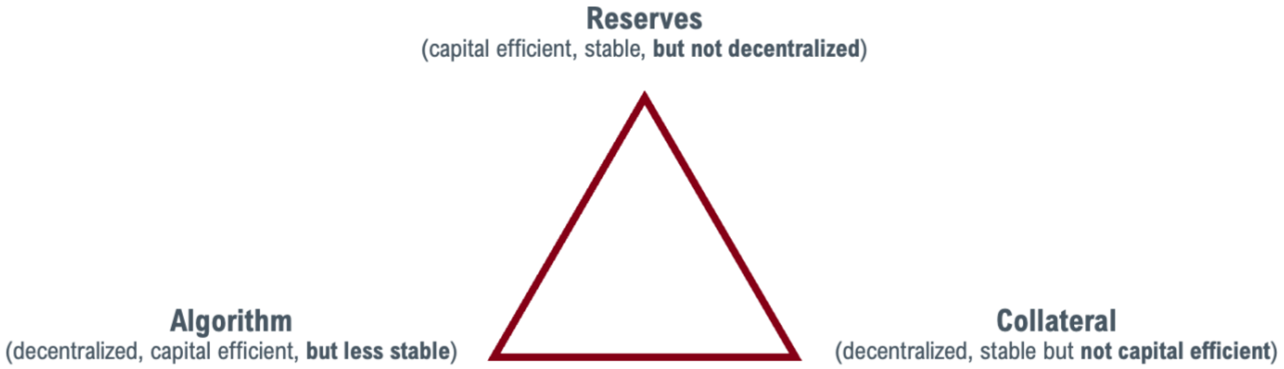

Reserves
(capital efficient, stable, but not decentralized)
Algorithm
(decentralized, capital efficient, but less stable)
Collateral
(decentralized, stable but not capital efficient)

Figure 11 – Stablecoin trilemma

We already touched upon the mechanisms through which stablecoins achieve price stability against their target. Centralised stablecoins are almost exclusively reserve backed, whereas decentralised stablecoins can rely on algorithms or utilise on-chain collaterals. Combinations of the above also exist. Those three distinct options also imply mutually exclusive trade-offs. Reserve stablecoins (2.1) are, for the most part, capital efficient, stable but not as decentralised. Collateral stablecoins (2.2) are capital decentralised, stable, but capital inefficient, whereas algorithmic stablecoins (2.3) are decentralised, capital efficient, but less stable.

Reserve stablecoins (2.1) work in three main steps: (a) a user deposits fiat collateral (exogenous collateral) with a custodian, (b) the custodian mints an on-chain representation of the deposit (stablecoin), and (c) the stablecoin can be returned in exchange for the initial deposit. This straightforward method ensures price parity between the initial collateral and stablecoin. It must be noted, however, that the custodian must be trusted to maintain the collateral as promised and not engage in fractional reserve activities.

Collateralised stablecoins (2.2) work in a similar way but utilise smart contracts in place of centralised custodians: (a) a user deposits cryptocurrency collateral (endogenous collateral) with a smart contract, (b) another smart contract mints an on-chain representation of part of the collateral (stablecoin), and (c) the stablecoin can be returned in exchange for the initial deposit. As with DeFi loans, stablecoins are overcollateralised to ensure that they maintain their peg even in volatile markets.

Algorithmic stablecoins (2.3) operate differently to their reserve and collateral counterparts, in that they do not require the lock-up of capital. Instead, they rely on oracles and algorithms to influence the supply and demand of the stablecoin, and thus its price. Using a theoretical euro-denominated stablecoin (zEUR) we explain the basics of this mechanism. Assuming that the desirable outcome is 1 zEUR = 1 EUR (1), if the price of zEUR ≈ 1 EUR, then nothing happens. If the price of zEUR > 1 EUR, then the supply of zEUR expands, whereas if zEUR < 1 EUR, the supply contracts instead. This contraction or expansion of supply can happen with a rebase or seigniorage mechanism. In a rebase model, the supply of the stablecoin is influenced directly. Conversely, seigniorage models work by introducing an incentive mechanism in the form of coupons bought and sold in the native stablecoin or other token native to the application.

SECTION 2.2: DECENTRALISED LENDING AND BORROWING

Lending and borrowing were the among the first DeFi applications to gain popularity. Decentralised lending and borrowing are simply transactions of transferring and returning cryptocurrencies at a fixed or variable interest rate, which use smart contracts. The transactions are carried out by dedicated protocols, interfaces at the first or second layer of a blockchain, with which users interact through standard Web 2.0 interfaces. Since DeFi is open, public and permissionless, there is no central authority to decide who participates and mediates the whole lifecycle of lending and borrowing. There is no need (or ability) for credit history or other financial records, as loans are either overcollateralised or issued in a way that ensures that they are repaid. Anyone can lend their assets and earn interest or deposit collateral with which to borrow against. Decentralised lending and borrowing aims to disintermediate money markets to achieve efficiency and cost reduction. Their open and permissionless nature (in principle) eliminates exclusion. However, to some degree, the above are achieved at the expense of interconnection with established money markets and related procedures, including regulation, anti-money laundering (AML) and investor protection. The latter is nowadays regulated according to the assumption that money markets rely upon vetted intermediaries that are obliged to comply with specific regulations (e.g. know your customer (KYC)) and subject to supervision by national and international bodies.

2.2.1 Characteristics of centralised and decentralised lending and borrowing

Lending and borrowing in DeFi differ from TradFi in seven ways:

(1) nature of creditor
(2) nature of debtor
(3) setting of interest rate
(4) collateral amount and type
(5) loan maturity
(6) risk to lender
(7) risk to borrower.

(1) In TradFi, creditors are, for the most part, vetted financial service providers such as banks or other appointed institutions. Unformalised P2P lending between individuals also exists in some limited capacity. This is unlike DeFi, where anyone can be a creditor, including non-human agents: they simply need to have funds to borrow, a valid address, and a way to send and receive valid information from a protocol.
(2) Similarly, anyone can be a debtor in DeFi; this is again in contrast to TradFi, where regulations and procedures can limit the access of certain individuals in financial services. The latter is true beyond lending and borrowing.

(3) Interest rates in TradFi are determined by the decisions of influential institutions such as central banks or politicians, in the form of forward guidance, and also by consumer and interbank demand. In DeFi, interest rates are set algorithmically by the protocol, and while influenced by wider market conditions, they rarely, if ever, fall in line with the interest rates of banks.

(4) The methods for mitigating financial damage stemming from defaults represents another difference between the two approaches in finance. In DeFi, this is mainly achieved through overcollateralised loans. TradFi uses a plethora of techniques, often in combination to achieve the same result. More specifically, this occurs over two stages; first, minimise the probability of default, and second, ensure that even in the event of a default, the lender will not suffer (severe) damages. The former is usually achieved through credit scores, which assess a borrower's ability to repay credit. Credit scores are used by banks as a way to measure risk and can influence their decision on issuing credit, as well as other factors like the amount or the rate of interest. KYC and AML regulation is also often used to limit access to credit, much to the consternation of the decentralised community. Once a bank decides to issue a loan, they can request collateral (such as a mortgage) below, at or above the value of the loan as an extra measure to minimise damages, in case of default. Regulations, courts and police provide further guarantees that debts will be repaid. Blockchains, however (and to that extent lending/borrowing protocols), comprise pseudonymous participants and lack centralised institutions to enforce standardised procedures for credit scores. In such a system, moral hazard is rampant, as it would be reasonable to assume that if the value of the collateral fell below the value of the loan, there would be no incentive to pay back the debt. As a result, the only viable way for ensuring that a borrower repays their debt is through over-collateralisation or technical means, both of which are utilised in practice.

(5) Maturity in TradFi loans is usually mostly fixed, whereas in DeFi it is often undefined.

(6) In TradFi, lenders face two main types of risks, these being default risks and systemic risks, whereas DeFi lenders face a plethora of other risks such as platform, protocol, governance and volatility risks.

(7) Borrowers in TradFi risk bankruptcy, loss of financial flexibility – and in extreme circumstances – loss of freedom, whereas in DeFi, they stand to lose their collateral through liquidation or exploits.

2.2.2 On collaterals and liquidation

We have already established that most loans in DeFi are overcollateralised. As a result, a question arises, why borrow funds when the collateral must always be of higher value? Another, lesser question also arises: Why do lenders provide funds for borrowers in the first place? Starting with the latter, in exchange for providing their funds, lenders receive compensation in the form of interest, and sometimes even governance tokens that can be sold on the open market.
The situation is more complex for lenders, who have the following main motives:

(1) leverage
(2) capital efficiency
(3) rewards
(4) taxation.

Regarding (1), it is important to note that borrowers don't lose exposure to their collateral, unless they fail to repay their loan and there is a liquidation event (collateral sold to cover a lender's losses). For this reason, they can post collateral in Asset A, whose value they think will appreciate, take out the loan in Asset B, and switch Asset B for Asset A to effectively lever their position. They can then, once again, deposit the borrowed asset as additional collateral, take out another loan, and repeat the process to multiply their leverage in a process called 'folding a position'. Naturally, with every iteration, they can borrow less and move more towards the liquidation ratio.

Table 8 – Loans in TradFi vs DeFi

Features	TradFi	DeFi
Creditor	Banks or appointed institutions	Anyone including smart contracts
Debtor	Vetted individuals or businesses	Anyone including smart contracts
Interest rate	Set by central bank, financial institutions and lenders	Set algorithmically by the protocol
Default damage mitigation	Laws, police, possibility for collateralised or unsecured debt	(Mostly) through overcollateralised debt
Maturity	Fixed	Fixed or undefined
Risk to lender	Default risk, systemic risks	Platform risk, protocol risk, volatility, governance risk, rug pulls
Risk to borrower	Bankruptcy, loss of financial flexibility	Liquidation/loss of collateral

(2) While antithetical at first, users can use DeFi borrowing for capital efficiency. As of late, some lending/borrowing protocols (discussed further in our coverage of DeFi 2.0)w users to use collateral that would otherwise be unproductive.

Overall, besides leverage, other reasons for lending and borrowing in DeFi are as follows:

- lenders and borrowers maintain exposure to the funds they lend or use as collateral;
- lenders receive interest on the funds they lend;
- lenders and borrowers may receive additional rewards in the form of governance tokens that can be sold in the market;
- depending on the jurisdiction, users might avoid or delay paying capital gains taxes through lending/borrowing.

2.2.3 Lending/borrowing metrics and key players

Table 9 – Lending/borrowing metrics and key players

Name	Description	Availability	€ TVL
Anchor (ANC)	Decentralised money market protocol	Terra, Avalanche	16 153 500 000
AAVE (AAVE)	Decentralised borrowing/lending platform	Ethereum, Avalanche, Polygon	10 685 700 000
Compound (COMP)	Decentralised borrowing/lending platform	Ethereum	5 309 700 000
JustLend (JST)	Decentralised fund pool protocol	Tron	1 649 700 000
Venus (XVS)	Decentralised stablecoin borrowing/lending platform	BSC	1 621 200 000
AAVE V3 (AAVE)	Decentralised borrowing/lending platform	Avalanche, Polygon, Arbitrum, Fantom, Harmony, Optimism	1 336 900 000
Benqi (QI)	Decentralised borrowing/lending platform	Avalanche	881 800 000
Vires Finance (VIRES)	Decentralised borrowing/lending platform	Waves	677 140 000
Parallel DeFi Super App	Decentralised protocol to protocol borrowing/lending platform	Parallel	650 887 000
Iron Bank (IB)	Decentralised protocol to protocol borrowing/lending platform	Ethereum, Fantom, Avalanche	604 893 000

The top 10 lending and borrowing protocols in DeFi collectively account for EUR 38 billion in TVL. 3 of these are available on Ethereum, with AAVE, AAVE3 and Iron Bank also available on Avalanche. Polygon and Fantom's Opera are the third most popular chain, counting two protocols (AAVE and AAVE3 for Polygon, AAVE3 and Iron Bank for Fantom). Overall, the protocol available on most chains (6 in total) is AAVE3.

SECTION 2.3: DECENTRALISED EXCHANGES (DEXs)

The emergence of DEXs can be traced back to one of Ethereum's killer application, 'tokens', i.e. transferable records of ownership of something, often unspecified, just like Ethereum and Bitcoin itself.

Tokens were the main actors of the initial coin offering (ICO) boom of 2017/18, where over USD 15 billion were raised within just over a year, with all these tokens living on the Ethereum – in October 2018, there were reportedly more than 800 tokens trading. The only trading venues at the time were centralised exchanges (CEXs), which presented two issues. First, they were centralised, in contrast to the decentralisation philosophy driving the blockchain movement. At least equally important, for tokens to be traded on an exchange, whoever was running the exchange had to list them first. For a plethora of legal, technical and reputational reasons, only a small fraction of all ICOs were listed on a CEX, and then there was a significant delay between the ICO and the listing, during which the token was effectively stranded.

Therefore, the idea of decentralised exchanges (DEXs), which live on Ethereum and act autonomously, was born. Initially the ideas concerned order books but this proved unworkable at the time for several reasons including transaction costs. Bancor created the concept of utilising the *k=x*y* 'bonding curve' algorithm in place of an order book. Bancor initially did not allow for external liquidity providers (LPs) through the user interface;

only the projects themselves could place their tokens in the pool in this way. Uniswap entered the market quickly thereafter with an AMM that allowed anyone to easily provide liquidity. This proved extremely successful and they have dominated the AMM market ever since.

2.3.1 DEX metrics and key players

Table 10 – DEX metrics and key players

Name	Description	Availability	€ TVL
Curve (CRV)	Decentralised exchange liquidity pool for stablecoin trading	Ethereum, Avalanche, Fantom, Polygon, Arbitrum, Gnosis, Harmony, Optimism	17 685 800 000
Uniswap (UNI)	Decentralised protocol for automated liquidity provision	Ethereum, Polygon, Arbitrum, Optimism	7 074 300 000
PancakeSwap (CAKE)	Decentralised protocol for automated liquidity provision	BSC	4 362 100 000
Balancer (BAL)	Protocol for programmable liquidity	Ethereum, Polygon, Arbitrum	3 005 900 000
SushiSwap (SUSHI)	Decentralised protocol for automated liquidity provision	Ethereum, Avalanche, Polygon, Arbitrum, Fantom, Harmony, BSC, Moonriver, Celo, Gnosis, Fuse, Telos, OKExChain, Palm, Heco	2 892 000 000
Astroport (ASTRO)	The meta AMM of Terra	Terra	1 602 300 000
VVS Finance (VVS)	Simple platform for token swaps and yield generation	Cronos	1 061 900 000
SunSwap (SUN)	Decentralised trading protocol for automated liquidity provision	Tron	986 090 000
Osmosis (OSMO)	Customised AMM protocol with sovereign liquidity pools	Osmosis	885 400 000
DefiChain DEX (DFI)	Decentralised platform for token swaps	DefiChain	856 300 000

The top 10 DEXs account for EUR 40.4 billion TVL. 4 of them are available on Ethereum and its various second-layer scaling solutions, the most popular of which are Polygon and Arbitrum. Besides Polygon and Arbitrum, the exchanges Curve and Sushiswap are also available on Avalanche, Fantom and Optimism. Gnosis also counts in the same 2 of the top 10 DEXs. PancakeSwap and SushiSwap are available on BSC, , whereas SushiSwap operates on Avalanche and Harmony, but not on BSC. PancakeSwap can only be found on BSC. DEXs are also available on Terra and DefiChain, whereas at least 1 of the top 10 exchanges is available on Celo, Fuse, Telos, OKExChain, Palm Heco, Aurora, Tron, Cronos, Osmosis and Moonriver. Overall, the protocol available on most chains (15 in total) is SushiSwap and Curve econd (8 chains).

Of the above, 13 utilise a Proof of Stake (PoS) or variant. Avalanche, Fantom's Opera, and (in part) Telos rely on proprietary DAG consensus mechanisms called Avalanche Consensus, Lachesis and EOSIO, respectively. Harmony, Celo, Telos and (in part) Lachesis rely on BFT consensus algorithms. Ethereum and Heco are the only chains relying on Proof of Work (PoW). Ethereum has announced plans to move away from PoW: this change will take place when the execution (using PoW) and consensus (using PoS) layers merge. This change is expected to take place in 2022. Heco partially relies on PoW for the generation of new blocks, with validation executed by PoS validators.

Table 11 – Major DeFi platforms and consensus mechanisms

Chain	Consensus
Ethereum	PoW (Soon PoS)
Avalanche	Avalanche Consensus
Fantom	Lachesis
Polygon	PoS (relies on ETH)
Arbitrum	AnyTrust Guarantee
Gnosis	PoS
Harmony	Fast Byzantine fault tolerance (FBFT)
Optimism	PoS (ETH is the parent blockchain)
Binance Smart Chain	PoSA
Moonriver	DPoS (delegated PoS)
Celo	BFT (Byzantine fault tolerant)
Fuse	DPoS (delegated PoS)
Telos	EOSIO (DPoS + aBFT)
OKExChain	Tendermint (PoS variant)
Heco	HPoS (hybrid PoS)
Aurora	Themis
Tron	DPoS (delegated PoS)
Cronos	PoA (Proof of Authority)
Osmosis	Tendermint (PoS variant)

SECTION 2.4: OTHER NOTABLE DEFI CONCEPTS

This section presents some emerging DeFi concepts, namely, derivatives, insurance and the collection of novel applications collectively referred to as DeFi 2.0.

2.4.1 Blockchain derivatives

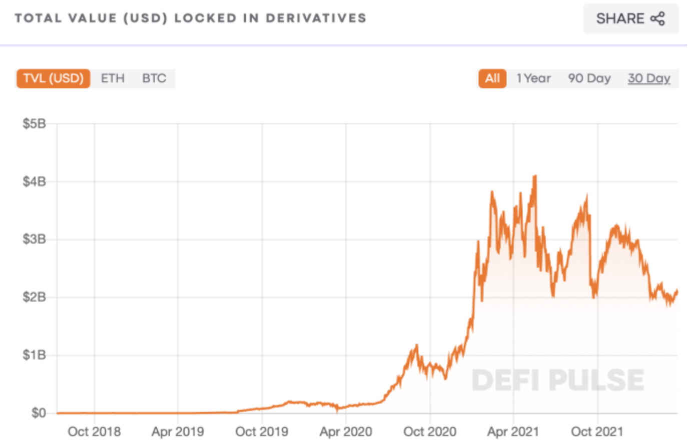


Figure 12 – Blockchain derivative volume

DeFi began by replicating financial services offered in TradFi. However, as it continues to grow, novel applications have emerged that go beyond conventional financial services. These innovations rely on the unique attributes of blockchains (deterministic, programmable, etc.), the comparatively relaxed regulatory requirements and even cultural differences between DeFi and TradFi. One of the most sophisticated elements of the classical financial markets are the different kinds of derivatives, like futures or options. The term derivative refers to ‘a type of financial contract whose value is dependent on an underlying asset, group of assets or benchmark. Derivatives are mainly used for two reasons: hedging, which allows for managing financial risk, while speculation focuses on rather short-term yield maximisation by providing liquidity to the market. It is estimated that the global derivative market is 10 times bigger than the total gross domestic product (GDP) of the world. Importantly for the open finance landscape of DeFi, derivatives only emulate the underlying asset(s), without providing a right or ownership rights. They thus represent an attractive option for bringing conventional financial products on-chain. At the same time, the composable nature of the space allows for the creation of highly sophisticated financial assets that follow unorthodox rules.

When referring to derivatives in DeFi, we often mean one of the following.

- **Wrapped tokens,** which are special and narrow-focused derivative applications, usually representing an on-chain asset for interoperability purposes. A notable example is wBTC, or wrapped Bitcoin, which is an ERC20 token on the Ethereum blockchain representing Bitcoin.
- **Synthetic assets**, which are more akin to conventional derivatives as they use oracles and other techniques to track the price of an underlying real or financial asset, usually fiat, crypto and stocks, or some physical commodity.
- **Blockchain-based derivative markets**, which are a form of DEX specialising in derivatives trading, including forwards, futures or options.

Although the blockchain-based derivative market is relatively new, it has recently achieved increased traction, resulting in an enormous increase in the total value locked (TLV) of derivative protocols.

As suggested above, wrapped tokens and synthetic assets share many similarities from a purely financial perspective; however, they have a technological basis. Wrapped token technologies have emerged to address the need for cross-chain interoperability and thus increase the utility of DEXs and lending/borrowing protocols.

Wrapped tokens operate on two basic levels.

- **The Wrapping,** where tokens from Blockchain 1 (e.g. Bitcoin) are held by a centralised or decentralised custodian like a smart contract or a multi-signature wallet, and tokens representing these holdings are minted (issued) on Blockchain 2 (i.e. wBTC) using a standard token protocol such as the ERC20.
- **The Unwrapping,** where wrapped tokens are removed from circulation on Blockchain 2 by being burned (become provably unspendable) with the simultaneous release of the tokens held in custody on Blockchain 1.[4]

Notable examples for wrapped token protocols are:

- wBTC being the first virtual Bitcoin on the Ethereum blockchain;
- renBTC providing a much more decentralised way of wrapping tokens without focusing only on Bitcoin;[5]
- tBTC working with an over-collateralised debt position scheme;
- wETH representing ether as an ERC20 token.

As noted, the main difference between wrapped coins and synthetic assets is that the latter follow the price of another asset without holding the underlying asset. As these protocols focus on tracking a price of an asset rather than holding it, more complex derivatives can be created. One such example is following the inverse price of an underlying asset, as with the iTokens in Synthetix, They usually work with an over-collateralisation in a protocol token, like an SNX token. If the collateralisation ratio drops below a certain threshold for the core asset whose price is being followed, the position is liquidated, meaning that the issued synthetic token is burned. Two notable examples are synthetics and UMA. Synthetix works with a large over-collateralisation ratio (1:5) and external oracles for following the price of the underlying asset.[8] By contrast, UMA operates with an intelligent liquidation scheme, so it requires no blockchain oracles and less collateralisation.

General blockchain derivative markets aim to provide the opportunity to trade with classical derivative constructs of crypto assets. These come in the form of special DEXs and enable the trading of the following.

- **Futures**: ‘Futures are derivative financial contracts that obligate the parties to transact an asset at a predetermined future date and price
- **Options**: an option is like a future and provides only the possibility to buy or sell an asset at a future price; it is not an obligation.
- **Perpetual contracts**: perpetual contracts are a particular form of futures that do not have an expiration or settlement date.
- **Spot trading**, **swap trading**, **margin trading** and more.

Among the notable protocols, Hegic specialises in decentralised option trading of different assets in a non-custodial permissionless way,[11] dY/dx is a general-purpose DEX which also provides different types of derivatives (like spot or margin trading) and more classical financial constructs (like lending), while Perpetual Protocol focuses on perpetual contracts.

From an architecture point of view there are many variations on the implementation of these DEXs. Some are fully on-chain solutions, while others integrate external oracles, cross-chain interoperability or Layer 2 solutions. Indicatively, dY/dx relies on an off-chain order book for efficiency purposes, while keeping the settlement on Ethereum.[12] By contrast, Hegic utilises an AMM. Some platforms integrate external oracles for importing price feeds while others rely on on-chain mechanisms. The two common frameworks used for external data integration are Chainlink and Provable. Platforms like UMA, on the other hand, utilise on-chain mechanisms. Another strong trend emerges with the development of L2 solutions, like optimistic, ZK rollups or off-chain ERC20 channels. The previously mentioned protocols are continuously developed further by integrating the latest technical innovations. As a result, most platforms investigate or already implement part of their protocol with L2 scaling. Finally, it should be noted that initiatives also exist for decentralised derivative protocols on non-Ethereum based settlement layers. Although the field is still in its infancy, we may expect rapid development in the near future.

2.4.2 Derivatives metrics and key players

Table 12 – Blockchain derivatives metrics and key players

Name	Description	Availability	€ TVL
DYdX (DYDX)	Decentralised derivatives trading platform	Ethereum	957 596 100 000
Synthetix (SNX)	Protocol for synthetic assets	Ethereum, Optimism	878 700 000
Mirror (MIR)	Protocol for synthetic assets	Terra, Ethereum	655 300 000
GMX (GMX)	Decentralised derivatives trading platform	Arbitrum, Avalanche	313 967 000
Keep3r Network (KP3R)	Decentralised network for external devops and keeper jobs	Ethereum	150 654 800
Perpetual Protocol (PERP)	Decentralised perpetual contracts for every asset	Optimism, Gnosis, Ethereum	39 447 000
Drift	On-chain, cross-margined perpetual futures to Solana	Solana	13 705 700
Tracer (TCR)	Smart contract protocol for derivatives	Arbitrum	11 185 500
Linear Finance (LINA)	Cross-chain compatible, delta-one asset protocol	BSC	9 619 200
Jarvis Network (JRT)	Decentralised derivatives protocol	Polygon, BSC, Ethereum, Gnosis	8 819 900

Unlike the most popular applications of DeFi, such as DEXs and lending/borrowing, Ethereum's network effects and dominance over other blockchains is evident in lesser popular applications such as derivatives, insurance and even options, since the majority of the top 10 derivatives protocols are available on Ethereum. Popular Synthetix and Perpetual Protocol are also available on Optimism, whereas Linear Finance and Jarvis Network are also available on BSC and. The TVL of the top 10 derivatives protocols amounts to EUR 3.04 billion.

2.4.4 Decentralised insurance

There are at least two ways that insurance can be interpreted in a decentralised context. The broader interpretation covers insurance against everything that is a possible event happening on-chain, off-chain, online or offline. This is realised with the help of decentralised prediction markets for creating possible outcomes for a future event and selling shares for these outcomes. Shares can be traded until the event happens. As most of these events are off-chain and even offline, there is usually a decentralised protocol for reporting these events in a way that ensures no individual reporter can cheat the system. Such protocols usually have game theory background. Decentralised prediction markets can be easily used in different insurance scenarios as well, as with betting against bad weather or bankruptcy of a centralised partner company. However, there must be sufficient liquidity for the outcome of the event, otherwise prediction markets are inefficient in such use cases. Well-known blockchain-based prediction market examples are Augur or Gnosis.[15]

Decentralised insurance can be interpreted within a narrow context as well, focusing only on events for the DeFi space. The narrow interpretation tries to insure against different failures/risks of other DeFi protocols. These failures/risks can usually be divided into the following major categories.

- **Technical risks**: for smart contract and protocol failures and exploits.
- **Liquidity or financial risks**: some of the DeFi protocols can behave unexpectedly in extreme market conditions: a sharp price drop can cause the mass liquidation of CDPs resulting in a domino effect in other protocols as well.
- **Admin key risks**: some protocols are not fully decentralised, meaning that the stealing master serves as a risk point.

One of the prominent examples of the DeFi insurance space is Nexus Mutual, which provides insurance against technical risks and bugs of other smart contracts on the Ethereum blockchain. Users can buy insurance, a coverage, for a period of time for a smart contract that specifies a cover period and a cover amount. In the case of a smart contract bug being exploited, a claim assessment process will commence, whereby independent claim assessors evaluate the smart contract incident. In the case of approval, the cover amount will be paid. The price of the insurance is identified by risk assessors evaluating the technical implementation of the smart contract, and it is paid in the native NXM token of the protocol.

Another popular DeFi insurance protocol is Opyn, which provides insurance not only for smart contract failures but liquidity, financial and admin key risks. Opyn utilises options to hedge against unexpected events. As an example, through Opyn, users can buy a put option on stablecoin deposits on Compound, like the right for selling cDAI for DAI in the future for a certain exchange rate. In case of a Compound failure, economical, smart contract hack or even admin key theft, the option guarantees to cover most of the loss.

Finally, insurance in DeFi, for the most part, does not follow the following main principles of insurance of conventional offerings.

- **Insurable interest**: the insurer must have a legal and valid interest in the item being insured.
- **Utmost good faith**: each party must reveal all relevant information, in the interest of good faith.
- **Proximate cause**: the cause of loss must be related to the insurance policy.
- **Indemnity**: the insured must not be compensated in an amount exceeding their economic loss.
- **Contribution**: where multiple insurances apply, the total may not exceed the total amount of loss.
- **Subrogation**: the transfer of an insurance claim to third parties.

Specifically, due to the permissionless nature of DeFi, anyone can insure against any event without necessarily having an insurable interest. Moreover, due to the lack of KYC/AML requirements, users can breach utmost good faith by relying on asymmetric information for profit. The contribution and subrogation principles do not apply, either. This means that DeFi insurance can also be used as a novel form of gambling.

2.4.5 Insurance metrics and key players

Table 13 – Blockchain insurance metrics and key players

Name	Description	Availability	€ TVL
Armor (ARMOR)	Decentralised insurance protocol	Ethereum	432 632 800
Nexus Mutual (NXM)	Decentralised cover against smart contract failure	Ethereum	405 976 200
Risk Harbor	Decentralised detection mechanism to secure liquidity providers and stakers against smart contract risks, hacks, and attacks	Terra, Ethereum, Arbitrum	201 052 300
Unslashed (USF)	Decentralised insurance protocol	Ethereum	54 674 000
InsurAce (INSUR)	Decentralised lending and insurance protocol	Polygon, BSC, Ethereum, Avalanche	51 533 800
Sherlock	Decentralised insurance protocol	Ethereum	19 837 500
Guard (Helmet) (GUARD)	Decentralised insurance protocol	BSC, Polygon	12 960 100
Tidal Finance (TIDAL)	Decentralised insurance protocol	Ethereum	8 176 500
Bumper Finance (BUMP)	Decentralised insurance against volatility	Ethereum	7 347 200i
iTrust Finance (ITG)	Decentralised insurance protocol	Ethereum	3 437 700

All but 1 (Guard Helmet) of the top 10 insurance protocols are available on Ethereum, with Guard Helmert, available on BSC and Polygon. Risk Harbor is also available on Terra and Arbitrum, while InsurAce is also available on Polygon, BSC and Avalanche. The top 10 protocols collectively account to EUR 71.2 billion in TVL.

2.4.6 Options metrics and key players

Options are financial instruments often used for hedging purposes and can be considered a novel form of insurance.

Of the top 10 options protocols, 8 are available on Ethereum, 4 on Avalanche, 3 on BSC, 3 on Solana and 1 on Fantom's Opera and Aurora. They collectively account for EUR 925 million of TVL.

Table 14 Blockchain options metrics and key players

Name	Description	Availability	€ TVL
Opyn	Options market	Ethereum, Avalanche	330 146 400
Ribbon Finance (RBN)	Structured products protocol	Ethereum, Avalanche, Solana	282 211 000
Friktion	Crypto-asset portfolio management platform	Solana	108 316 600
Dopex (DPX)	Maximum liquidity and minimal exposure options protocol	Arbitrum, Avalanche, BSC, Ethereum	57 002 700
ThetaNuts	Decentralised structured products and options strategies protocol	Ethereum, Avalanche, Fantom, Polygon, Aurora, BSC, Boba	49 630 600
Lyra (LYRA)	Decentralised options protocol	Optimism, Ethereum	45 077 600
Katana	Automated option strategies yield generation protocol	Solana	21 319 600
FODL Finance (FODL)	‘Money Lego’ decentralised leverage trading platform	Ethereum	13 444 000
Premia (PREMIA)	Automated options market	Arbitrum, Ethereum, BSC	10 778 000
Hegic (HEGIC)	Non-custodial options trade	Ethereum, Arbitrum	6 845 800

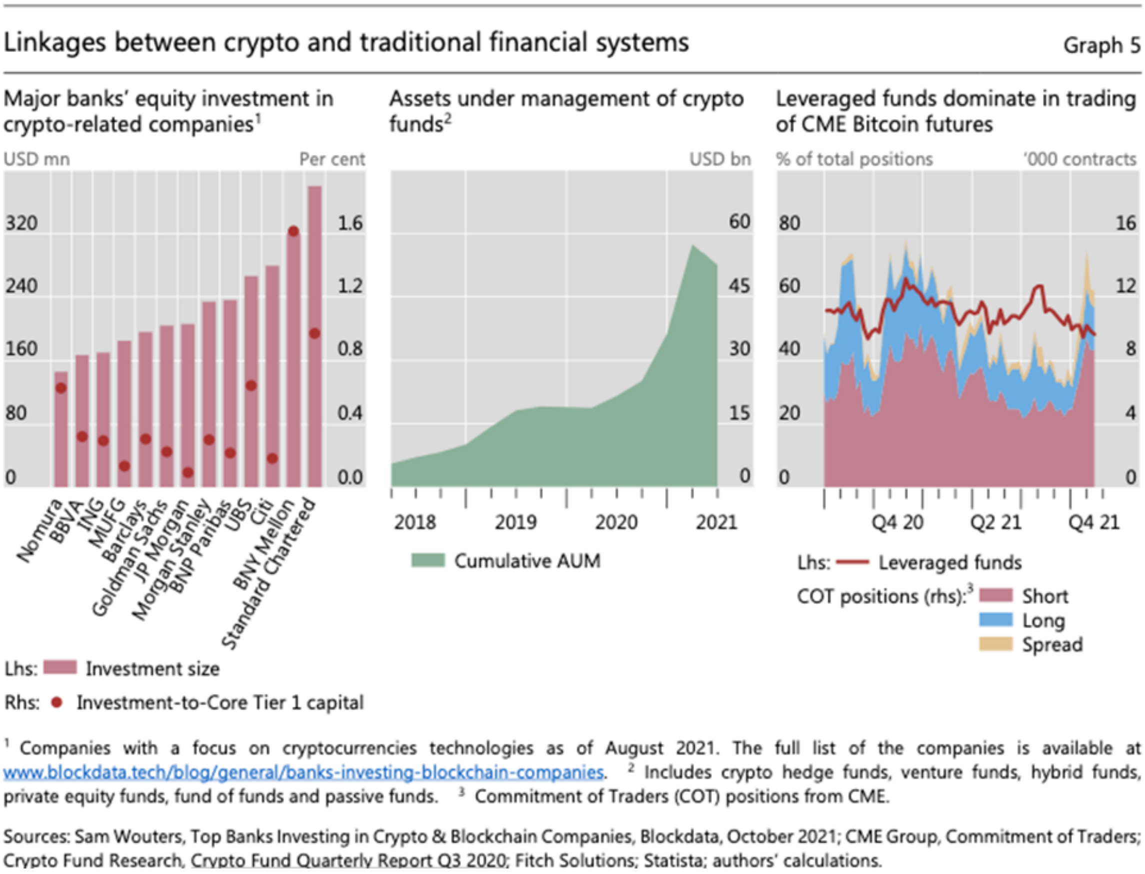
Section 2.5: DeFi risks

2.5.1 Technical risks

Throughout our analysis of the various components of DeFi, we have covered some of its risks. This section expands upon those by categorising them into technical, financial and procedural risks. Technical risks concern failures of DeFi protocols stemming from their underlying technological infrastructure at a protocol, or Layer 1 level. Financial risks are related to projects failing due to either the idiosyncrasies of the cryptocurrency market or the economic modelling of the service. Finally, procedural risks refer to hacks that rely on the exploitation of specific procedures within the decentralised space.

Starting with technical risks, DeFi protocols rely on an underlying L1 blockchain/DLT infrastructure and are thus affected by its technical limitations and vulnerabilities. This shared risk profile between L1s and DeFi can manifest in several ways, but most importantly through consensus failures, or other Denial of Service (DOS) and Sybil attacks. As a result of disruptions at the L1, transactions in DeFi can be double-spent and even censored.

In circumstances of extreme stress at the L1, DeFi applications running atop might even become non-operational, as was recently the case with Solana. This DeFi-L1 interdependency feeds into other forms of



Linkages between crypto and traditional financial systems

Graph 5

[1] Companies with a focus on cryptocurrencies technologies as of August 2021. The full list of the companies is available at www.blockdata.tech/blog/general/banks-investing-blockchain-companies. [2] Includes crypto hedge funds, venture funds, hybrid funds, private equity funds, fund of funds and passive funds. [3] Commitment of Traders (COT) positions from CME.

Sources: Sam Wouters, Top Banks Investing in Crypto & Blockchain Companies, Blockdata, October 2021; CME Group, Commitment of Traders; Crypto Fund Research, Crypto Fund Quarterly Report Q3 2020; Fitch Solutions; Statista; authors' calculations.

Figure 13 – Linkages between cryopto and traditional financial systems - BIS

risks, such as front-running, discussed in the chapters above. Besides this ‘blockchain risk’, DeFi applications can only be as secure as their underlying smart contracts/code. Protocol risk refers to the risk stemming from bugs in a DeFi protocol’s smart contracts that can lead to exploits.

For its various operations, DeFi protocols have also become increasingly reliant on oracles. Oracles overcome the isolated and sandboxed nature of blockchains by retrieving and delivering off-chain data to smart contracts, writing data to external systems, and even executing off-chain operations. This means that faulty oracles or oracle manipulation can affect DeFi protocols directly. Finally, besides oracles, interoperable bridges between L1s and even L2s have become increasingly common for users that want to transfer their tokens. However, some bridge solutions have proven unreliable, as was the case recently with Wormhole, leading to another DeFi risk factor.

2.5.2 Financial risks

Financial risks in DeFi stem mostly from the volatility of cryptocurrencies. A prime example of this is impermanent loss, covered in the previous chapters. Besides impermanent loss, price volatility is responsible for liquidity problems and price slippage. The two concepts are related. Liquidity risk refers to the inability of obtaining sufficient cryptocurrencies in a given timeframe or for a reasonable price. Slippage refers to a situation where the actual price of a trade deviates from its expected price. Those deviations can range from minor to extreme, depending on the liquidity available in the market (pool), as well as the size of the trade. Generally, there is a negative relationship between the size of the pool and slippage, and a positive relationship between the size of the order and slippage.

2.5.3 Procedural risks

As noted above, procedural risks are a broad category that describes threats stemming from the idiosyncrasies of DeFi, and these risks include:

(1) loss of a private key
(2) admin key risk
(3) governance risk
(4) the risks of rug pulls
(5) the risk of liquidity draining attacks such as the vampire attack.

(1) Due to a lack of KYC and appointed entities controlling access to decentralised applications, the loss of a private key means loss of access to all funds, with no way of retrieving them. Moreover, as blockchains and DeFi protocols are agnostic to users’ intentions, custody of a private key translates to complete access to its corresponding assets.

(2) The admin key risk is similar and refers to the risk of the key owner(s) modifying the underlying protocols in a way that benefits them, without taking into consideration the impact this might have on the users. This can be mitigated entirely if the keys are ‘burned’ (destroyed), or partially through multi-signature deployments that might also be governed by a decentralised autonomous organisation (DAO). However, as highlighted in the previous chapters, if admin keys for a DeFi protocol are burned, the protocol cannot be upgraded or altered. Uniswap, for example, mitigates this by deploying entirely new versions of its protocol on-chain.

(3) Governance risks refer to the exploitation of protocols underlying DAO and voting procedures to enforce decisions that are beneficial to certain users. This risk is especially high when voting power in the form of governance tokens is concentrated in certain individuals or entities. Protocols usually impose minimum requirements for submitting, voting and passing governance requirements that can be exploited by large token holders.

(4) Besides governance, rug pulls are another risk vector in DeFi. The term is used to refer to a collection of techniques with which a minority of users can manipulate a token's value or utility for their own benefit, at the expense of most users. Indicatively, developers of a protocol can increase fees, and impose other technical limitations to restrain trading at their platforms, allowing them to offload cryptocurrencies before their market price crashes. Additionally, most DEXs, lending/borrowing, and derivative protocols also rely on liquidity pools for their operation. Malicious actors can coordinate the removal of liquidity from those pools in a way that benefits them at the expense of the majority of users. Finally, the term can also refer to developers abandoning a project and leaving with the investors' money. In essence, rug pulls are akin to exit scams and are relatively rare in established protocols.

(5) Another DeFi risk, this time affecting liquidity-dependent protocols instead of users, comes in the form of a vampire attack. A vampire attack usually involves two steps. First, a new DeFi protocol, usually a fork (copy) of an existing implementation, incentivises LPs of another protocol to stake their liquidity tokens to a new platform. Since liquidity tokens represent ownership of the underlying liquidity in a pool, the new protocol essentially becomes the custodian of those positions. After enough liquidity is attracted, the LP tokens are migrated to a new protocol, effectively 'draining' the liquidity from the first, hence the term 'vampire attack'. This attack was successfully executed by the then nascent SushiSwap, on Uniswap in August of 2020.

Table 15 – DeFi risks

Technical risks	Financial risks	Procedural risks
Blockchain risk	Liquidity risk	Loss of private key
Protocol risk	Slippage	Admin key risk
Oracle manipulation	Front-running (and variations)	Governance risk
Bridge disruption	Impermanent loss	Rug pulls
-	-	Vampire attacks

Chapter 3: Conclusions

DeFi represents a paradigmatic shift in financial services provisioning and promises to be one of the most disruptive applications of blockchain-fuelled decentralisation. The ability to transact P2P (i.e. without intermediaries) remotely and trustlessly (at least as far as trusting one's counterparty is concerned) is a novel phenomenon, which is still maturing. The plethora of DeFi applications already in existence may be just the tip of the iceberg compared to the wave of innovation we expect in the near future.

The Directorate-General for Financial Stability, Financial Services and Capital Markets Union of the European Commission has dedicated a comprehensive reference to the Decentralized Finance market. The European Financial Stability and Integration Review, an annual publication which investigates the recent financial developments, expands on issues about the financial sector that might pose challenges to financial integration and stability and potentially raise policy issues. The 2022 edition expands on three chapters i) The Macroeconomic developments, the real estate in the aftermath of the pandemic, and finally focusing on Decentralized Finance state of the art and policy challenges. The report highlights that the Decentralized Finance sector could potentially increase the security, efficiency, transparency, accessibility, openness, and interoperability of financial services compared to the traditional financial system. The report provides a very strong case for the sector. It suggests that the Decentralized Finance ecosystem "could provide substantial opportunities to foster cross-border financial integration," an important policy objective of the European Union. The report is deepening also on the financial stability and expands on complex concepts for regulators, such as decentralised governance and liquidity provision.

According to the researchers, the real impact of the Decentralized Finance market has so far the minimal impact on the real economy, and use-cases are only artificially limited in the cryptocurrency markets. Nevertheless, the editors make clear that the Defi ecosystem is prone to numerous risks, and more effort should be committed to identifying operational risks. The lack of regulation, along with the pseudonymous culture of Defi culture, constitute the operational risks more vital. The report similarly indicates that the Commission has announced a pilot project on embedded supervision in 2022.

We will quickly refer to the highlights of the report:

- Despite the potential values and characteristics of the Defi ecosystem, it still remains an open question if it could substitute or complement the traditional financial ecosystem. Although Defi replicates many of the functionalities, its impact and contribution to actual economic activity are minimal.
- A new approach toward regulatory framework might be required focus. A potential solution could be regulating the DeFi actors based on their activity rather than their entity-based one.
- Regulation of smart contracts might be required, given the fact that are substituting regulated intermediaries.
- The report is emphasizing the benefits of public blockchains regarding transparency and auditing, which constitutes an advantage for researchers and supervisors who can have access to the entire time series of historical and real-time trading data. In turn, it is expected to facilitate a better understanding of the risks that "often remain obscure in the traditional financial systems".
- The report suggests that the DeFi potentially could lead to lower financial audit costs and open borders in terms of financial cooperation.

The authors conclude that is already clear that supervisors will have to invest considerable resources in improving their data processing capabilities if they are aiming to stop updated with the pace of digital innovation in the financial sector. The size of the Decentralized Finance ecosystem remains limited in scale, and already European regulators take a proactive approach to better understand the industry.

While decentralised financial solutions are expected to contribute to digital transformation and competitiveness for the European economy, as well as introduce new forms of financing for small and medium-sized enterprises (SMEs) and European citizens, they are also politically important, as they can support Europe’s ambitions to make financial services more accessible and transparent, while contributing to long-term job creation and economic growth.

However, such services will require a clear and favourable regulatory framework, which will allow centralised and decentralised services (TradFi and DeFi) to co-exist, without distorting competition or hindering innovation growth for new types of services. The global (borderless), trustless (disintermediated) and self-enforcing (automated) nature of DeFi services may present regulatory and policy challenges that should be addressed proactively so that innovation can flourish in Europe and not move to other jurisdictions which may adopt more friendly or favourable approaches.

One dimension of such challenges has to do with the global (borderless) nature of DeFi applications and services: any applicable regulation must address the fact that there is an inherent difference between TradFi and DeFi in terms of both the physical location of providers of DeFi services (or lack thereof) and the location of the users of such services.

Another dimension concerns the legal enforceability of smart contracts in general and DeFi smart contracts in particular: questions related to legal protection and liability should be addressed in a way that not only covers existing solutions but is also general enough to anticipate future innovations in this fast-moving field. The extent to which existing regulations are applicable to DeFi as well, or whether clarifications, modifications or new regulatory initiatives are needed, must be assessed. This is also related to AML, counter-terrorism financing (CTF) and KYC regulations, which must be considered in the context of DeFi with a view to achieving adequate levels of protection without putting onerous, unnecessary or unenforceable burdens on DeFi application providers.

Finally, it is crucial that existing and future DeFi innovators have a clear view of which regulations they will need to follow if they base or provide their services within Europe. Currently, the European regulatory landscape for DeFi is largely unclear, and hence Europe may risk losing access to talent, applications, revenues and growth stemming from unclear or inadequately addressed aspects of setting up and operating DeFi services within the European Union. The following areas must be assessed.

- Legal entity requirement: DeFi projects typically self-organise as community DAOs and/or run autonomously as automatically enforced smart contract code. How will these forms of organisation be addressed in the absence of a specific legal entity (European or otherwise) operating the DeFi service?
- Underlying technology risks: DeFi applications may be affected through no fault of their own, when the underlying blockchain on which they operate (sometimes referred to as Layer 1 or Layer 2) is affected, resulting in compromised security, downtime or other problems. The same can happen at other levels of the DeFi application stack, for example when oracles fail to fetch the right information or when stablecoins lose their peg, thereby affecting the operation of a DeFi service through no apparent fault of the service itself. How will liability be assessed and attributed in such cases?
- Stakeholder risks: DeFi protocols are typically governed through ownership of their native governance token. However, token holders may be pseudonymous, and tokens may be trivially transferred to new owners across the globe. How will stakeholders be identified and held legally responsible for decisions they have made in the context of exercising their governance rights? Conversely, how will stakeholders know which rules they have to follow when making such governance decisions?
- Investor protection: given the novel nature of DeFi, fraud can be a significant risk, especially in the absence of clear regulatory frameworks. Developers may abandon projects, running away with customer funds (‘rug pulls’ in the DeFi jargon) or DeFi smart contracts may prove to be insecure, exposing users to risks of fund loss. How will investors be protected, while at the same time ensuring that protocols do not face insurmountable obstacles in operating?

The above examples point to the differences between blockchain-based and traditional structures, which in turn pose challenges for regulating DeFi. Regulators will be faced with the challenging task of devising rules that do not view DeFi through the lens of TradFi requirements, while at the same time allowing DeFi to be accessible to European citizens and businesses in a legally compliant manner. Authorities will need to upskill, both in terms of adopting and using appropriate software tools to monitor DeFi activity and with regard to employing appropriately skilled staff to audit smart contracts or perform on-chain analytics. Regulatory sandboxes, which allow projects to operate in a controlled environment, is a potentially effective way for DeFi developers to work together with regulators.

Generally, it is hoped that regulators and policymakers will choose a technologically neutral approach to balancing the need for promoting innovation and meeting supervisory objectives. As with any regulation, measures should be fair, efficient, effective and enforceable. A combination of self-regulation and supervisory enforced regulation will gradually give rise to a more regulated DeFi 2.0 emerging from the current nascent DeFi 1.0 ecosystem.

Annex

A1 How AMMs work – constant product formula

The modern AMM is based on the principle of the ‘bonding curve’, although a more accurate term would be ‘indifference curve’. An AMM is a smart contract that has at its disposal tokens of two kinds, for example CSH (for ‘cash’) and RSK (for the ‘risk asset’). In the k=x*y formula, the x represents the number of RSK tokens, and y the number of CSH tokens, and k is determined by the current holdings of the AMM. The AMM is a passive market participant, which means that the AMM does not engage in trading itself, but is willing to trade with everyone. The rule is that **the AMM will accept any trade that, not considering fees, keeps k constant.** In reality, k will go up at every trade as does the AMM when the fees are accounted for.

The chart below shows an example indifference curve for a specific k (in red). The current state on the curve is indicated by the red dot. The tangent at this point (in dotted grey) determines the exchange ratio between CSH and RSK the AMM offers for an infinitesimally small trade. In other words, the tangent shows that **marginal** price. The actual price of a trade is given by the secant, like the one shown in the chart (solid grey).

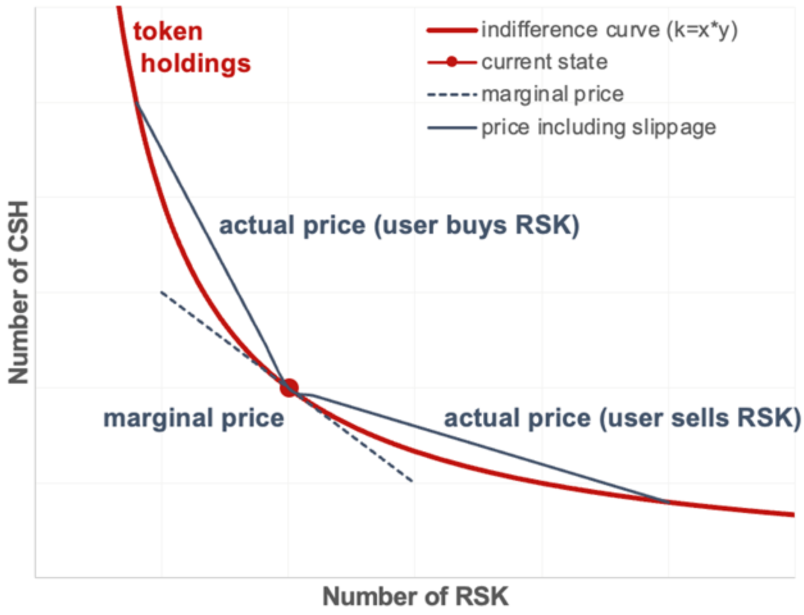


Figure 14 Constant product formula

The difference between the marginal price and the actual price is referred to as slippage. Translated to market parlance, the price including slippage is the (trade-volume dependent) bid or offer, whereas the marginal price is the midpoint, and slippage is the bid-offer spread. It is easy to see that in market equilibrium, arbitrageurs will ensure that the AMM portfolio composition is such that the marginal price offered by the AMM is equal to the market price. For the k=x*y AMMs specifically, this implies that in equilibrium, the monetary value of the AMM’s CSH holdings is equal to that of its RSK holdings. For historical reasons, and because this is what is needed to implement an AMM, people tended to focus on the indifference curve and on analysis along the lines above. This is somewhat unfortunate as micro-economics has a well-developed framework for analysing market makers and other market participants: the so-called ‘supply curve. Translated into a supply curve, the k=x*y AMM with k=100tn appears as follows.

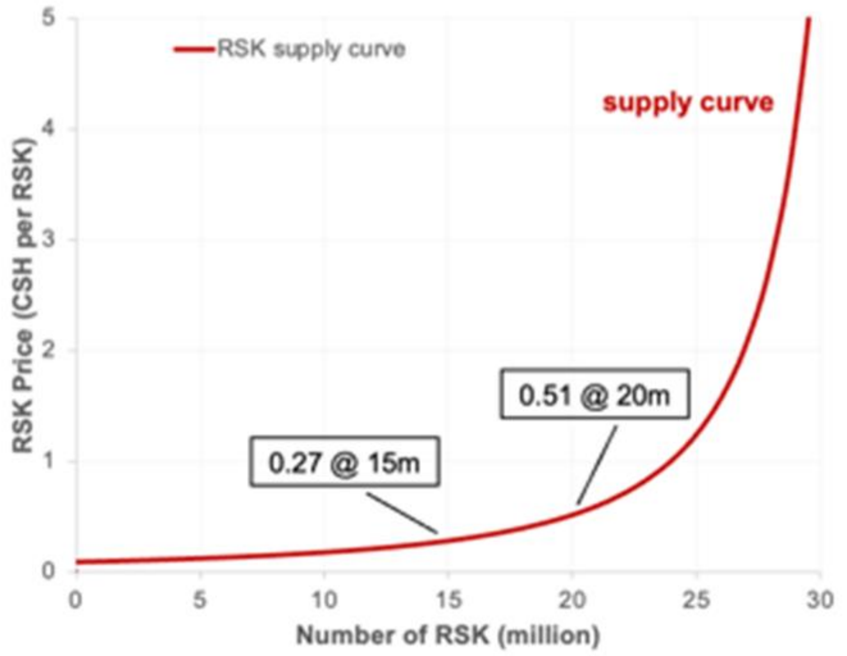


Figure 15 – Price and supply curve

This is a bulk standard supply curve, which offers a straightforward explanation of how AMMs function. For example, at a price of 0.27, the AMM will have supplied RSK 15 million to the market. At a price of 0.51 it will have supplied a total of RSK 20 million. In other words: **between 0.27 and 0.51, this AMM releases RSK 5 million to the market**.

A2 Modified-weigh models

We have seen that the k=x*y indifference curve leads to a specific form of the supply curve. We also know that any increasing curve is a valid supply curve, so evidently the space of possible AMM indifference curves is equally large. It is beyond the scope of this report to go into details, but it is worth noting the $k = x^a \times y^{1-a}$ family of AMMs. The alpha parameter determines the collateral composition of the AMM. At a value of 0.5, we find our original AMM with half the assets in each of the two constituent assets, while for other values this ratio shifts.

Another important model is the stable swap model, which is especially designed to swap stable coins with the same based asset (e.g. USDC and USDT) against one another. While they are generally described in terms of their indifference curve, it is much easier to describe them in terms of their supply curve, which is concentrated around the unity exchange rate, and away from which they cease trading.[2] In other words, they are a special form of the concentrated, leveraged liquidity model, which is discussed below.

A3 Concentrated, leveraged liquidity model

Uniswap recently introduced their version v3 which introduces the concept of concentrated and leverage liquidity. It is based on the k=x*y model, but then it (a) restricts the AMM to only trade in a certain price range (‘concentrated’), and (b) then removes all the collateral that can no longer leave the AMM (‘leveraged’). The mathematics of this is beyond the scope of this report, but the principle is simple in terms of the supply curve. If, in the example above, the liquidity is restricted to the price range 0.27 to 0.51, all the supply below 15 million and above 20 million disappears – the AMM provides RSK 5m of liquidity in the price range 0.27 to 0.51. Uniswap v3 allows LPs to choose their range on range and amount, so the aggregate Uniswap v3 supply curve is the aggregate supply curve of those constituents, just like a commodity supply curve is the aggregate of the individual producer supply curves.

A4 Concentrated, leveraged liquidity model

The original AMM design only had two constituent assets. In a world of N tokens, we either need point-to-point pools allowing us to trade in one hop, or we designate one asset as base asset and establish $N - 1, where\ 0.5N(N - 1)$ pools against it. This is highly capital inefficient unless a protocol-controlled asset that can be minted and burned on demand is used as the AMM's base asset.

An alternative to this model is the multi-asset-pool model where all assets reside in a single pool. The most natural indifference curve in this case is the equal-weight curve which leads to all constituents having equal monetary value in equilibrium, and a modified weight of this curve also exists.

$$\boldsymbol{k = x1 \times x2 \times \ldots \times xN}$$

A5 Impermanent loss

AMMs are two-sided marketplaces, bringing together LPs who offer the trading collateral and earn the fees, and traders who use the AMM and pay fees. Trading economics is straight forward, except for front-running issues. LP economics is more complex as they suffer divergence losses (or 'impermanent loss' as it is misleadingly known). Strictly speaking, the divergence loss (DL) is an opportunity cost – it is the difference in portfolio value, had the LP held on to the initial portfolio, compared to the value of the actual AMM portfolio.
As the name implies, the DL depends on the **price divergence** of the assets in the pool. The designation 'impermanent' is derived from the fact that if the divergence reverts back to zero, so does the DL. The value of the DL is shown in the chart below (Figure A3).

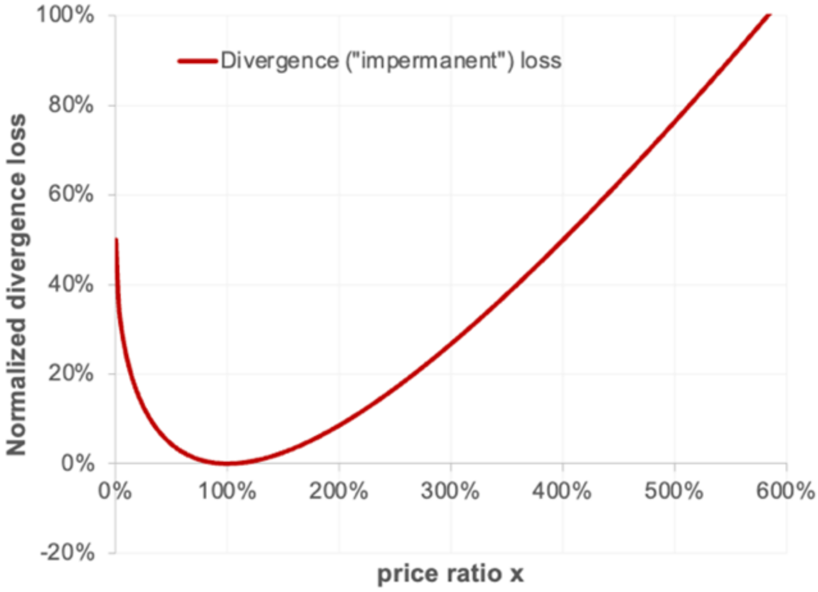


Figure 16 Impermanent loss

As we can see, at original price levels (100 %), the DL is 0. For moderate price movements (up 100 %, down 50 %), it stays well within the 10 % range. However, when the risk asset breaks out, the DL becomes substantial and at a 600 % divergence, the DL is as large as the initial investment. DL is an opportunity loss, i.e. foregone profits. When an asset goes up, the AMM reduces its exposure to it and thus profits less from subsequent price rises. Therefore, the LP might still make money, just significantly less than they would have had they held on to the initial portfolio in the outset. Recent research into Uniswap v3 data suggests that in current markets, in aggregate, the DL is significant and of the same order of magnitude as the fees.

A6 Miner-extractable value (MEV)

On Ethereum, the miners chose which transactions to include, their order, and whether to add transactions on their own. AMMs are trading infrastructures and it is well-known from traditional finance that the ability to front-run trades can yield significant profits. In this report we will focus on two specific opportunities to illustrate this point, but there are many others.

Front-running LPs (flash liquidity)

In a flash liquidity transaction, the miner (or a bot working with them) scans the transactions in the mempool for significant trades on an AMM. If it finds them, they add a significant amount of liquidity before the trade and remove it right after it. While in principle possible on any AMM, a concentrated AMM like Uniswap v3 lends itself particularly well to this, because of the leverage provided by a very narrow position just around the current price range. The effect of this is that a significant portion of the fees generated from this trade is diverted to the flash LP, leaving the permanent LPs with less.

From one perspective, it can be seen that flash LP is simply an active market maker who takes the other side of a trade, earning maker fees in this process, and this is correct. On the other hand, the flash LP takes away fees from the permanent LPs (most likely on the most profitable trades), which means they have less capacity to cover their DL risk. This in turn means that they may be encouraged to leave the market; unless the flash LP is willing and able to provide liquidity for all trades (effectively disintermediating the AMM), this would constitute a market failure.

Front-running traders

Front-running traders is a more traditional method of making money from knowing the order flow. As in the previous example, the miner or bots are scanning the mempool. When they find a suitable trade for a specific AMM, they (1) source the assets at the current market price via another route, (2) put a large trade ahead of the trade they identified that pushes the price against it, and after it executes, they (3) reverse their own trade. The miner or bots make money from the targeted trade because it is executed at an off-market price, at the price of some additional fee payments. Depending on whether this becomes prevalent, trading customers may no longer choose to trade with AMMs, which would constitute a market failure.

Private execution (flashbots)

The way for AMM users to avoid these front-running issues is to not submit their trades to the mempool where everyone can view them, but instead submit them confidentially to a miner for private execution, or ‘flashbot’ execution, as it is known, after the name of the protocol that provides this service. This solves the issue at hand, but at the cost of increased latency because the transaction will only be executed (at the then prevailing price) when the miner finds a block.

A7 DeFi 2.0

DeFi 2.0 is an initiative to overcome some of the technical and financial limitations of existing DEX and lending/borrowing deployments.

One of the largest problems of the previously mentioned protocols is that they ‘rent’ their liquidity from users. To bootstrap liquidity and mitigate impermanent loss, LPs are rewarded by a percentage revenue of the underlying protocol, usually paid in the form of native protocol tokens which also serve as votes in governance proposals. The primary issues regarding this incentivisation mechanism are that even with lock-up periods, liquidity is ultimately free to move between protocols; this is especially true if better yields can be earned. This liquidity migration puts downwards pressure on the price of the protocol’s token, which in turn results in a lesser incentive for new LPs. These imperfect incentives can even be exploited through attacks. In an indicative example, SushiSwap managed to get its initial liquidity by draining it from Uniswap with a so-called vampire attack. This model of liquidity provision makes it hard to identify and appropriately reward individuals that use the platform either for its services or because they truly believe in it. Moreover, those kinds of users are hurt the most, as yield farmers remove their liquidity (thus deprecating the protocol) and sell their tokens for profit. The explosive growth of DeFi has encouraged new solutions that attempt to mitigate those problems. New protocols in DeFi 2.0 introduce the idea of protocol-controlled value (PCV). Instead of relying on LPs to bootstrap and maintain liquidity, DeFi 2.0 protocols own their own liquidity.

One prominent application enabling this is OlympusDAO, a decentralised reserve currency protocol with its own native token, OHM. The OHM token is backed by a basket of assets that is stored in the Olympus treasury. The underlying logic is that since OHM is backed by assets that have utility and value outside of OlympusDAO, this creates an implicit price-floor for OHM that is at least equal to the value of the assets backing it. Users can earn OHM either by purchasing OHM-denominated bonds, or by staking their OHM. In the first scenario, OlympusDAO sells OHM at a variable discount in exchange for other cryptocurrencies. OHM acquired in this way is locked for a short period. In the second scenario, users stake OHM acquired through bonds or the open market in exchange for rebase rewards. Importantly, the reserve assets of the OlympusDAO treasury include liquidity provider tokens that represent popular OHM pairs in DEXs. This results in the treasury, and thus the OlympusDAO, owning up to 99 % of its own liquidity. Through Olympus Pro, OlympusDAO makes this bond system available to other protocols. A year later, after the all-time high of OHM’s price, its value has decreased by 97 %. While the decentralised community has grown sceptical of OHM's proposition as a new reserve currency, the concept of protocol-owned liquidity remains innovative and influential.

Another interesting use case emerging from DeFi 2.0 are self-repaying loans, and the abutting concept of yield-bearing collateral. In the latter case, new protocols allow for interest-bearing crypto to be used as loan collateral. This means that otherwise illiquid tokens can be used to generate additional yield, thus making decentralised borrowing more capital efficient. A notable example of such implementation is Abracadabra Money. Finally, self-repaying loans operate on a similar principle. In that scenario, yield generated from interest-bearing tokens posed as collateral is used to gradually repay the loan. An example of this implementation is Alchemix. Another notable DeFi 2.0 application is Tokemak which creates sustainable liquidity through a decentralised market-making and liquidity governance mechanism. All signs point to DeFi's innovations continuing in 2022 and beyond.

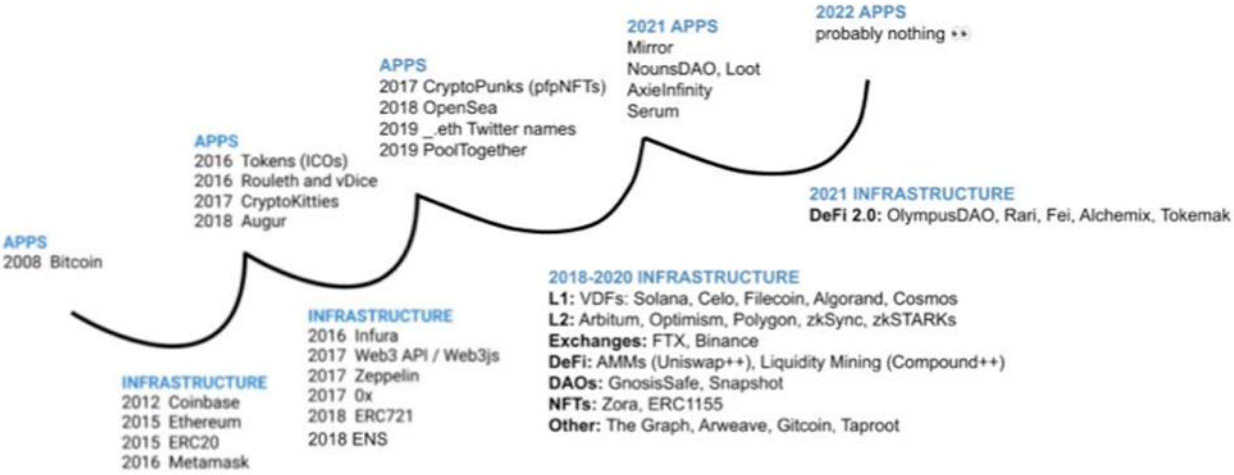


Figure 17 Innovation curves

A8 Interview with Jacek Czarnecki, MakerDAO

The European Blockchain Observatory and Forum interviewed Jacek Czarnecki, Global Legal Counsel, MakerDAO for some insights on DeFi and regulation.

EU OBSERVATORY: What are the main regulatory initiatives for DeFi at the moment, especially in EU and the US? Could you present some of the main challenges of regulating DeFi?

JC: *I think that the main regulatory initiatives are well-known. In the EU, it's mainly MiCA (with the entire uncertainty in terms of to what extent DeFi is covered), TFR, the new AML package, and potential future initiatives directed at DeFi mentioned by the EU institutions from time to time. In the US, we should expect that some crypto bills will get more attention and support in Congress, perhaps as a result of the UST and Luna catastrophe in the last few days. It is also possible that some agencies such as FinCEN will return to some ideas on how to approach DeFi.*

The challenges are also quite well identified, and they include:

- *Very complex technical and governance aspects of DeFi products and organizational frameworks*
- *Knowledge gaps between regulators and the market concerning technological and business developments*
- *Global and cross-border nature of DeFi*
- *Regulatory arbitrage among DeFi creators and projects (common use of offshore jurisdictions)*
- *The fact that some crypto-assets do not easily fit traditional definitional boundaries of regulated products, especially in civil law jurisdictions (including the EU)*
- *Unwillingness by policymakers and regulators to recognize permissionless blockchains as financial market infrastructures, due to perceived flaws*
- *Unclear definition, meaning, and criteria for "decentralization" and its legal consequences*
- *Uncertain legal and regulatory standards*

EU OBSERVATORY: What will be the impact of the Markets in Crypto-Assets (MiCA) regulation on DeFi if implemented in its current form? What, in your opinion, could be improved?

JC*: I think that everyone is awaiting the final draft after the trilogue, as it is entirely unclear whether and to what extent MiCA will cover DeFi. The current discussions make it clear that as far as DeFi is considered, MiCA creates more issues than solutions and creates massive legal uncertainty, which will be bolstered by differences among specific member states.*
In my opinion, MiCA should apply exclusively to well-defined centralized models built around certain clear concepts (such as e.g., centralized order books or centralized custody). At the same time, the EU should launch a separate effort directed at DeFi (which could be about amending MiCA to its "2.0" version).

EU OBSERVATORY: How important is the degree of decentralization when it comes to applying existing and future regulations to specific DeFi protocols? How can the level of decentralization be assessed by regulators?

JC: Very important. The degree of decentralization should directly translate into the applicable regulatory obligations and should be one of the critical factors in determining their addressees. A simple example is Bitcoin: there are not many regulatory doubts regarding this asset, and its current regulatory treatment (e.g., a non-security status in all key jurisdictions) stems directly from the high degree of its decentralization. Regulators should adopt functional decentralization testing frameworks (covering technical, operational, governance, and economic factors), which should be used from time to time as projects evolve. This is the major challenge faced by policymakers in the coming years, but the problem is not theoretical anymore and attempts at solving it should be made.

EU OBSERVATORY: Given the global and borderless nature of blockchains, is it possible to effectively regulate DeFi at a national level? The FATCA and GDPR regulations by the US and EU respectively, are two recent examples of extraterritorial regulation. Do you predict that policy makers in the EU and US will approach DeFi regulation in a similar manner?

JC: It is challenging but not impossible. The example of the US and its securities law doctrine and enforcement shows that it is possible for a major jurisdiction to impose certain standards even on decentralized models. I do predict significant differences in the US and EU approaches.

EU OBSERVATORY:Could you provide a framework of what you would consider exemplary DeFi regulation? In particular, would you focus on regulating the so called "on-ramps" to DeFi, or the protocols and their underlying technologies and why?

JC: I would need a bit more space and time to fully elaborate on this. In short, I would consider the rollout of DeFi regulation in a few phases:

1. *Addressing on-ramps and other interaction points such as user interfaces.*
2. *Creation of frameworks for "hybrid" products and projects (by this, I mean products that are on the verge of the regulatory frameworks today, e.g., by being centralized yet non-custodial) by building a more modular regulatory framework.*

3. *Providing incentives (of tax and regulatory nature) for developers and protocols to go in directions intended by the policymakers.*

EU OBSERVATORY: Help us understand what is at stake if DeFi regulation falls in either of the following extremes: (1) proves insufficient and ineffective, or (2) proves overwhelming for DeFi and related stakeholders.

JC: 1: risks to retail investor protection, increased financial crime, risks to financial stability.
2: emergence of a shadow unregulated financial system, which will create similar risks as above.