Decentralized Finance (DeFi) 101

Description

Decentralized Finance (DeFi) is redefining the future of finance. There is a major shift going on in the underlying infrastructure powering financial applications, and it's changing the way we think about permission and control, transparency and risks.

DeFi is a developing market sector within the intersection of blockchain technologies, digital assets, and financial services. According to DeFi Pulse, the value of digital assets locked into DeFi applications grew 10X from less than $1 billion in 2019, to over $10 billion in 2020, and over $80 billion at its peak thus far in 2021. Yet the DeFi applications and underlying infrastructure are still in its nascent stage of development.

The goal of this report is to provide an introduction of the new emerging area of DeFi infrastructure powering DeFi apps today. While it's easy to get caught up in the hype and speculation within the space, I'll focus on the key components of DeFi applications, their key differentiation compared to traditional finance, potential risks, and longer term implications these DeFi apps are causing.

Major Structural Commonalities Across DeFi Apps

DeFi apps are financial applications with no central counterparties. In practice this means there is no institution (e.g. banks) you are interfacing with to access these financial applications; instead users interface directly with the programs (e.g. smart contracts) on top of the protocol itself. For more of a DeFi 101 primer I highly recommend this report.

The major categories of DeFi apps include decentralized exchanges, lending platforms, stablecoins, synthetic assets, insurance, among others. While diverse in scope, all of these DeFi apps share a major set of commonalities including:

1. Using underlying blockchains as the core ledger
2. Open source and transparent by default
3. Interoperable and programmable (composability)

4. Open and accessible to all (permissionless)

Using Underlying Blockchains as the Core Ledger

Compared to traditional financial applications which use core banking systems (Fiserv, Jack Henry, FIS, etc.) as the underlying ledgers of record, DeFi apps use blockchains as their underlying core ledger.

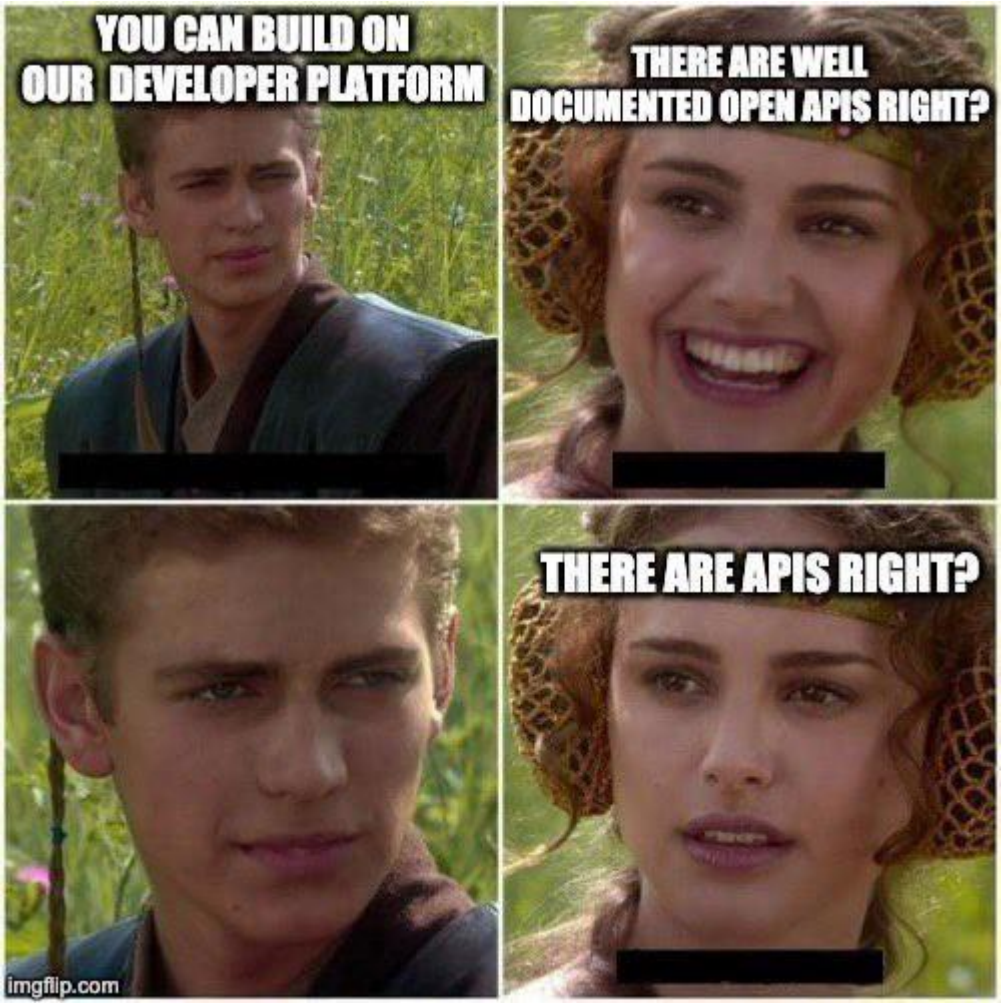
A few of the most prominent blockchains used to build DeFi apps include Ethereum, Solana, and Binance Chain, etc. These underlying blockchains store the ledger state of what is deposited into the DeFi apps, what is stored within the smart contracts, all of the transactions, and withdrawals.

All of the core accounting functions to ensure matching inputs and outputs are handled by the blockchain itself, the DeFi apps don’t need to create external systems to reconcile balances, because all of the transactions are queryable across the various block explorers.

In addition, compared to the traditional system there is no separate process of settling & clearing transactions. The transaction processing, clearing, and settling all happen at the same time when the transaction is broadcasted. Although it is advisable to wait around ~21 blocks or more to ensure finality on the blockchain itself.

Open Source and Transparent by Default

Compared to traditional financial applications which are all closed-source and built on top of proprietary systems, DeFi applications are typically entirely open sourced and built on top of open underlying blockchains.



Banking "APIs"

This causes three interesting properties:

1. *Composability* — The DeFi app itself can be forked, remixed, and reused in many other applications (more on this below).
2. *Transparency* — Since the DeFi app is open source, it is completely auditable to know exactly what the smart contract is doing in terms of functions, user permissions, and user data.
3. *Auditability* — Since the underlying blockchain itself is open sourced, the entire flow of funds is completely auditable including collateral in the system, trading volume, defaults, etc.

Unlike the traditional financial system (which is opaque), runs on a fractional reserve system, and is prone to market shocks — the DeFi system is completely transparent and over-collateralized — which allows DeFi companies to weather downturns much more efficiently.

Interoperable and Programmable

In order for developers to gain the trust of users, the majority of the DeFi apps are completely open source — including the front end and the smart contracts themselves. In addition, since DeFi apps all

run on top of a common platform (the underlying blockchain) these DeFi apps are completely interoperable with each other and can be programmed to work with any other DeFi app in the ecosystem.

This is commonly referred to as the "money legos" or "composability" aspects of DeFi. All of these DeFi apps are like individual lego pieces which can be remixed to work with other lego pieces to build something new.

Contrast this to the traditional financial system where;

- *Infrastructure Fragmentation* — Traditional financial apps are not built on top of common infrastructure.
- *Siloed Applications* — Traditional financial apps are typically proprietary to one banking institution. For example, all of Wells Fargo's "fintech apps" work together but not across different banking institutions.
- *Developer Unfriendly* — Traditional financial apps are not made for other developers to build services on top of.

The traditional financial system does have common standards; however, it's extremely hard to reach consensus across market participants because financial institutions view their software as their competitive moat instead of using products as a differentiating factor.

One of the biggest reasons why we have seen so much innovation within the DeFi space is because the systems are interoperable, it allows the developer ecosystem to have more creative expression on the products and services they create. On top of this, developers don't need to waste time reinventing the wheel, but rather can build upon common frameworks and focus on the things that make their products special.

Open and accessible to all

With traditional financial applications, new users typically need to go through a lengthy onboarding process, income verifications, credit checks, or even in person meetings — just to be able to use a given financial product.

Because of these arbitrary rules set by financial institutions, these onboarding processes are prone to bias including lending descrimination, denial of basic banking services, opening credit lines without consent, charging illegal fees, etc.

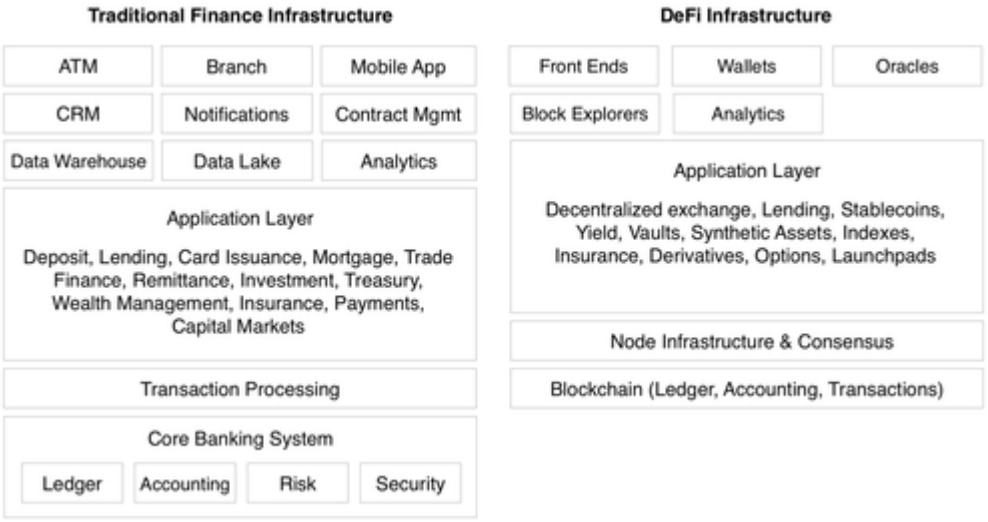
With DeFi applications, all you need is a wallet address to interact with these systems. DeFi apps don't ask for income verification, they don't need credit checks, and in most cases they don't even need to know who you are outside of the wallet address you are using.

This is commonly referred to as DeFi apps being permissionless. If you have the funds inside your wallet for the transaction you want to do, you can do it. There are no institutions or intermediaries to stop or deny service to you. It doesn't matter what your background is or what country you come from, DeFi apps do not discriminate.

This is one of the most under-appreciated aspects of DeFi products.

Traditional Fintech Architectures vs. DeFi Architecture

Here is a more architectural diagram on the main technical differences between a traditional fintech app and DeFi app (simplified for brevity's sake):



Here is a more direct comparison chart on some of the key differences between centralized and decentralized financial applications:

	Traditional Finance	DeFi
Custody	Held by institution or custody provider	Held directly by users in non-custodial accounts or via smart contract
Unit of Account	Fiat Currency	Denominated in digital asset or stable coin
Execution	Facilitated via intermediaries	Facilitated via smart contract
Settlement	~3-5 business days depending on transaction, during M-F business hours.	Seconds to minutes depending on blockchain, 24/7 operating times.
Clearing	Facilitated via clearinghouses	Facilitated via blockchain transaction
Governance	Specified by exchanges & regulators	Governed by the protocol developers & users
Auditability	Authorized third-party audits	Open source code & public ledger, can be audited by anyone
Collateral	Transactions may involve no collateral, intermediates take on risk	Over-collateral generally required.
Risks	Vulnerable to hacks and data breaches	Vulnerable to hacks and data breaches of smart contracts

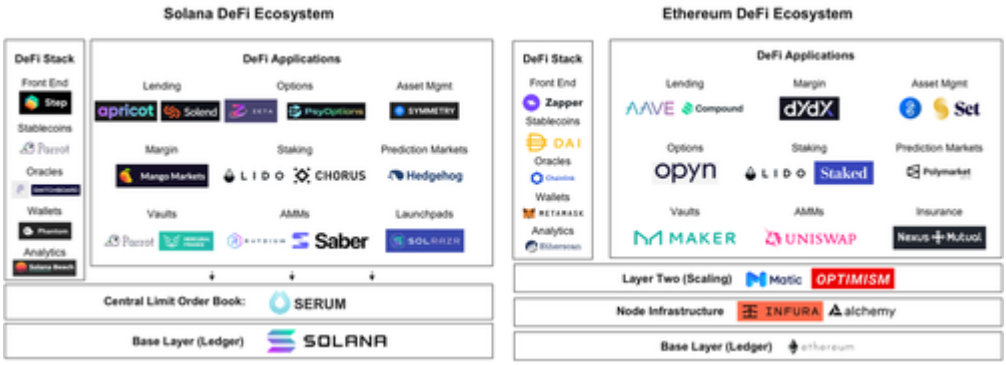
DeFi Infrastructure — Market Map

Below is a market map of two different DeFi ecosystems, one built on the Solana ecosystem and the other built on the Ethereum ecosystem.

The reason why I am picking these two ecosystems to focus on is to show the breadth of DeFi apps being built across two different underlying protocols. I also believe Solana is the most interesting new layer one protocol because of its high transaction throughput (50K+ transactions per second), sub second latency & transaction confirmation times, and fast growing ecosystem of developers building

DeFi apps on top of the Solana protocol.

While similar in structure, each underlying protocol has its own ecosystem built on top which is largely independent of the other. Below are some of the further explanations of each layer and the tradeoffs between them.



Base Layer (Layer One)

The base layer is the blockchain in which the core ledger itself sits. Ethereum is the most dominant layer one today, and Solana is the most promising new entrant with faster transaction speeds, more throughput, and cheaper transactions.

Node Infrastructure

A never ending amount of data needs to be queried about the underlying ledger (retrieving blocks, finding transactions, syncing data, writing transactions, etc). In the Ethereum ecosystem, a whole industry sprung up to solve this need (Infura, Alchemy, etc.).

Contrast this with Solana where the underlying ledger is fast enough and in sync enough that teams can just query Solana's RPC nodes directly (*this might not last forever though*).

Layer Two

On Ethereum, there are various layer two solutions primarily used for scaling since Etheruem itself cannot handle all of the transactions on itself. Two of the promising scaling solutions include Matic, Optimism, among others.

On Solana, since there is only one layer to build upon (no layer 2 scaling solution needed) there are no specialized integrations needed and no mismatches with the underlying ledger which is processing settlement.

Order Book Aggregation

Unique to Solana, there is an additional layer occupied by a DeFi project named Serum which provides a CLOB (Central limit order book) that is used by all of the DeFi projects built on top.

When new DeFi projects are built on top of Solana (DEX, AMM, Options, etc.), they can pull orders from Serum and push orders back into Serum, greatly reducing the cold start challenge most new financial applications face.

The best way to think about it is to think of it as "networked liquidity" and an "order management" system which is used by the majority of projects within the Solana ecosystem.

One of the more innovative examples of combining a CLOB (Serum) and an AMM is Raydium (very similar to Uniswap v3). The combining of these systems allows for passive LPs with active market making using Serum.

DeFi Toolset

There are a set of common tools needed to operate most of these DeFi apps, either from the perspective of developers or end users. These services don't have direct traditional finance analogies but they include:

- *Wallets* — The main interface people use to store assets & interface with DeFi apps.
- *Oracles* — On-chain data feeds DeFi apps use to reference prices and execute transactions against (example: liquidations).
- *Block Explorers & Analytics* — Tools like Block Explorers were created to allow people to query the blockchain ledger itself directly. These are used most often when verifying transactions.
- *Stablecoins* — The two main assets used in DeFi ecosystems include the underlying native protocol token (ETH or SOL) and ideally on-chain stablecoins (USDC, Dai, or Pai).
- *Front-Ends* — A new emerging layer which creates easy to use front-end applications to interact with multiple DeFi projects at once, or to simplify transactions. This includes both Zapper.fi within the Ethereum Ecosystem or Step Finance within the Solana ecosystem.

DeFi Apps

The DeFi apps themselves are composed of all of the core financial applications which can be used directly, or embedded into other various apps within the crypto ecosystem.

DeFi App Category	Ethereum Examples	Solana Examples
DEX/AMM (Automated Market Makers)	Uniswap, 0x, Balancer, Curve	Raydium, Saber, DexLab, Orca, Luna Network
Lending	Aave and Compound	Apricot Finance, Solend, Everlend, Oxygen, Jet
Margin Trading	dYdX	Mango Markets
Options & Derivatives	Opyn, Hegic, Finnexus	Zeta Markets, PsyOptions, HXRO, Synthetify
Staking (Liquid Staking)	Lido, Staked (Eth2)	Lido, Staking Facilities
Prediction Markets	Polymarket, Augur	Hedgehog
Insurance	Nexus Mutual	*(Doesn't exist yet)*
Vaults	Maker	Mercurial, Parrot
Units of Value (Protocol tokens & Stablecoins)	ETH, DAI, USDC, USDT	SOL, PAI, USDC, USDT
Asset Management	Set Protocol, Yearn, Melon	Symmetry, Laguna Finance, SolRaise
Oracles	Chainlink, API3, Band	Pyth, Switchboard

Potential Missing Pieces of DeFi Infrastructure

When comparing and contrasting DeFi infrastructure with traditional financial infrastructure, there were a few pieces that don't exist yet in the decentralized world that could be interesting to explore.

A few to highlight below:

- **Consumer Applications** — In the traditional financial world, consumers typically act with consumer apps (ex. Robinhood, Chime, Transferwise) not the underlying protocols themselves. The front-ends of the DeFi space could be greatly improved and intermediate much more of the total consumer experience. In general, the UI/UX of most DeFi apps are still very difficult to use from a consumer perspective.
- **CRM** — The DeFi space doesn't really have a concept of customer relationship management nor typically collects any amount of consumer data. While great from a privacy perspective, there is great value in understanding the customer better.
- **Notifications** — Notifications or alerts don't really exist at all in the DeFi space at all. On a more broader level there aren't any great methods to communicate with users either.
- **Product Analytics** — There are tools to measure blockchain activity, but not to measure engagement within DeFi applications.
- **Security —** DeFi products do typically conduct security audits; however, none of the security audits guarantee the most common protections consumers are accustomed to in the traditional financial world. On top of this, the demand for security auditors outstrips the supply, so it's a big bottleneck.
- **Transaction Rollbacks** — In traditional finance, if you make a mistake, a financial institution can

initiate a rollback of the transaction. This does not yet exist in DeFi.

- **Custody** — Right now, most DeFi projects need to be interacted with from an individual wallet perspective. None of the custodians allow you to interact with DeFi apps.
- **Developer Platforms** — Most of the developers in the crypto space are building right on top of the layer one protocol itself. There are no concepts of developer platforms or middleware just yet.
- **Embeddable Wallets** — Wallets are seen as these external services, there aren't any offerings of white-label wallets to embed these directly into the DeFi apps themselves. There are several initiatives such as Torus, but these are still in its infancy.
- **Identity** — One of the biggest complaints from the traditional finance world about DeFi is the pseudonymity of users. Ideally there needs to be a way to keep out the bad actors while persevering consumer privacy.

Future of Financial Applications

After meeting hundreds of founders and seeing progress teams are making, one thing is very clear — the pace of innovation in DeFi is 10x faster vs. that of traditional fintech apps.

In traditional finance:

- The underlying ledgers are not open source nor developer friendly.
- There are a whole host of "banking as a service" applications just to wrap underlying partner banks in developer friendly platforms.
- Fintech apps are very challenging regulatory wise and typically take years of development before releasing a single product.

Contrast that to DeFi where:

- Everything is open source including the ledger itself.
- All of the transactions are public.
- Everything is built from the perspective of developers building applications on top of protocols.
- New DeFi apps are built and released in weeks, not years.

We at Race Capital believe that **DeFi developers will forever change how the finance world works.** We are incredibly bullish about the DeFi infrastructure stack and community.

* * *

If you are building the horizontal infrastructure layers of the new open source financial stack including: trading, lending, borrowing, and/or any horizontal tools all new DeFi projects will rely upon in the future, we want to chat with you. Send me a message > chris@race.capital

by Chris McCann

Date Created
07/01/2021