Foundations of FinTech

Decentralized Finance (DeFi)

Eshwar Venugopal

UCF

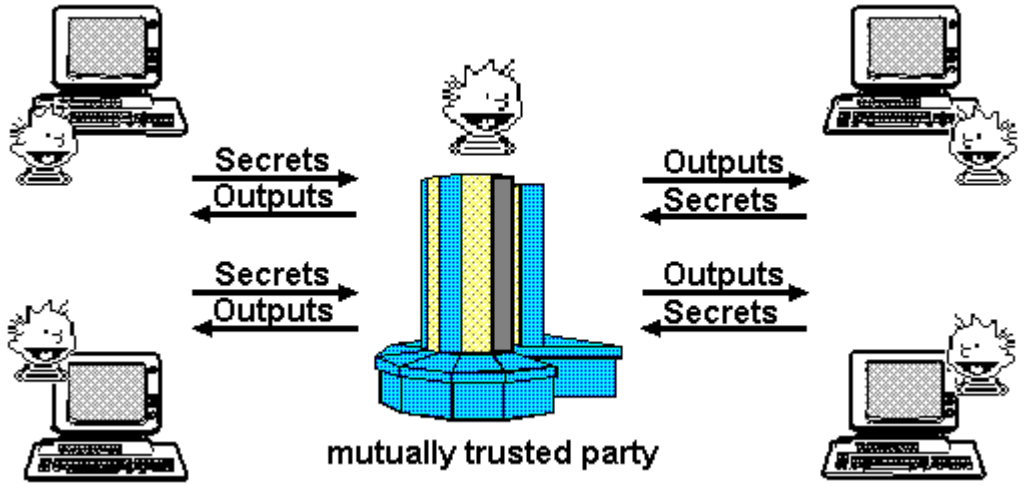
Origins

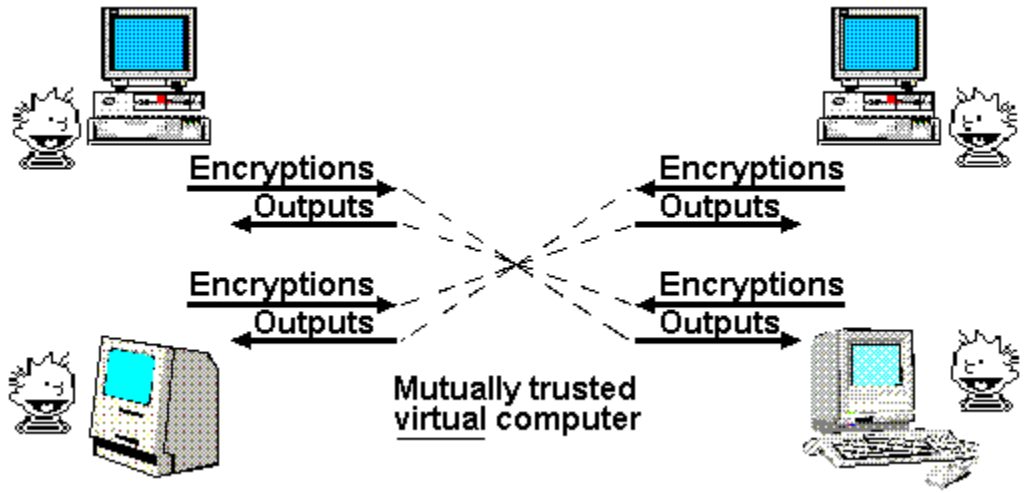
- To understand Decentralized Finance (DeFi) we need to understand the origins of ‘smart contracts and Ethereum’s role.

The God Protocols, by Nick Szabo (1997)

“Imagine the ideal protocol. It would have the most trustworthy third party imaginable – a diety who is on everybody's side. All the parties would send their inputs to God. God would reliably determine the results and return the outputs…, no party would learn anything more about the other parties' inputs than they could learn from their own inputs and the output.

Alas, in the our temporal world,…, too often we are forced to treat people in a nearly theological manner, because our infrastructure lacks the security needed to protect ourselves.”





Source: https://nakamotoinstitute.org/the-god-protocols/

Origins: Smart Contract

"A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs"

-- Nick Szabo, 1994.

Origins: Smart Contract

- Bitcoin solved the long-standing centralization and double spending issue to create an electronic token that can proxy money be tracked.
- Ethereum added the possibility of wrapping token with code – smart contracts that can transact when triggered.
  - Like “if this, then that” type of code
- A *smart contract* is a piece of code that automates/executes a signed contract between two parties without the need for a third-party supervision.
  - E.g., Escrow, lawyers in real estate transaction, etc.
- Allows for quick verification of on-chain contract terms execution.
- Disallows contract modification (modifications must be made via a new contract!)
- Note: Smart contracts CANNOT physically enforce contracts. They only give you the paper trail.
  - E.g., Confirmation that a house has been sold. It cannot make the current occupants leave.

Origins: Smart Contract

Steps involved

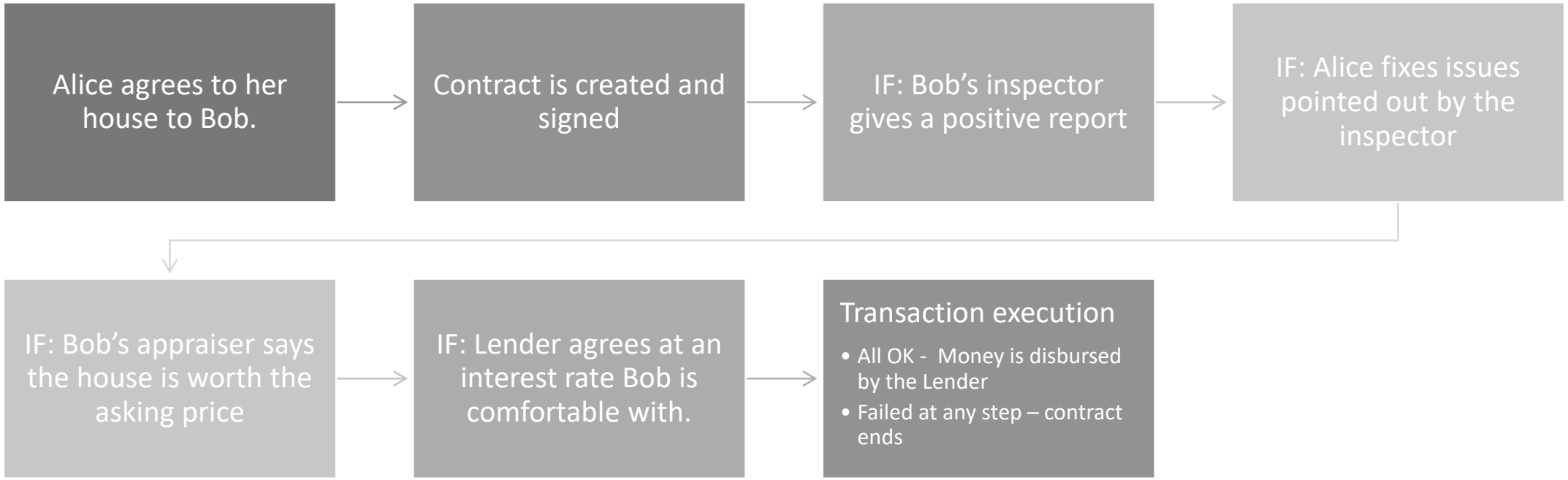
- Negotiation & agreement
- Coding up the contract
- Compile and store it on the blockchain
- Execution & record events when triggered

Currently, majority of the smart contracts are written using Solidity and executed on Ethereum.

- Solidity interacts with Ethereum Virtual Machine (EVM) program to store and execute contracts

Smart Contract: Thought exercise

Think about the steps below and steps when time/money can be saved in a fully digital world.



Smart Contract: Thought exercise

- Which steps could be automated or made less expense?
  - Title verification
  - Back & forth emails about the inspection
  - Escrow & lawyer fees
  - …

Smart Contract: Use cases

- Smart contracts are useful in many industries that currently need a trusted third party to facilitate transactions
  - Identity verification
  - Insurance
  - Real estate
  - Supply chain
  - Any contracting situation…

Smart Contract: Issues

- Contracts are incomplete!
  - No contract is perfect – there are always uncovered scenarios or loopholes
- Digital contracts are vulnerable to hacks
- Lack of regulatory clarity: off-chain and sometime on-chain as well
  - In 2016, a vulnerability in Ethereum DOA's smart contract was used to drain funds from a project
- Technical skills are required to write basic contracts
- Becomes complicated if the contract requires off-chain information (Oracle integration is required)
- Scalability is an issue (inherent to all Blockchain based applications)
- Gas fees were an issue even after merge (Layer-2s help but not enough)
  - Expected to go down after the Surge in 2023

Smart Contract: Demonstration

Solidity & Remix – Codes on Webcourses

Decentralized Finance (DeFi)

Decentralized Finance (DeFi)

2008
- Great recession
- Loss of trust across multiple intermediaries

2009
- Introduction of Bitcoin
- Blockchain as the immutable record keeping device

2014
- Ethereum
- Smart contracts
- Decentralized Applications (DApps)

2016
- Launch of Maker (announced in 2014)
- Decentralized Autonomous Corporation/Company (DAO)

2016+
- Concept of DeFi was born soon after MakerDAO's launch
- Got a boost in 2020

Decentralized Applications (Dapps)

An application can be classified as a Dapp if:

- The application must be completely open-source, it must operate autonomously, and with no entity controlling the majority of its tokens. The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by consensus of its users.
- The application's data and records of operation must be cryptographically stored in a public, decentralized blockchain in order to avoid any central points of failure.
- The application must use a cryptographic token (bitcoin or a token native to its system) which is necessary for access to the application and any contribution of value from (miners/farmers) should be rewarded in the application's tokens.
- The application must generate tokens according to a standard crytptographic algorithm acting as a proof of the value nodes are contributing to the.

--- The General Theory of Dapp, Johnston et al. (2015),
https://github.com/DavidJohnstonCEO/DecentralizedApplications

Decentralized Applications (Dapps): Types

- Type I decentralized applications have their own block chain.
  - Bitcoin is the most famous example of a type I decentralized application but Litecoin and other “alt-coins” are of the same type.
- Type II decentralized applications use the block chain of a type I decentralized application. Type II decentralized applications are protocols and have tokens that are necessary for their function.
  - The Omni Protocol is an example of a type II decentralized application.
  - Ethereum can be considered as a combination of Type I and II (ETH and ERC-20)
- Type III decentralized applications use the protocol of a type II decentralized application. Type III decentralized applications are protocols and have tokens that are necessary for their function.
  - For example, the SAFE Network that uses the Omni Protocol to issue ‘safecoins’ that can be used to acquire distributed file storage is an example of a type III decentralized application.
  - Smart contract on Ethereum is a Type III

Decentralized Autonomous Organization (DAO)

DAO is an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do.

--- Vitalik Buterin (2014), https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide

- A DAO is supposed to be fully autonomous (Level 5 automation)
  - We are not there yet
- DApp has some level of automation but is considered to be a primitive – pre-coded logi (Level 1 automation)
- The gap between DApps and DAO is filled by iDApp or Intelligent DApp
  - iDApps are supposed to use machine learning techniques to make decisions on the fly.

Decentralized Finance (DeFi)

- Our traditional financial system is centralized (CeFi)
- DeFi aims to decentralize the financial system – do away with need for trusted central third parties.
  - Distribute power
  - Distribute risk
- Does NOT mean there will be no power players – just that there will be more than one.

- Tagline: *An open, trustless, permissionless, and interoperable protocol-backed financial market*
  - Caution: We are not there yet! But getting there, especially with the hype surrounding crypto dying.

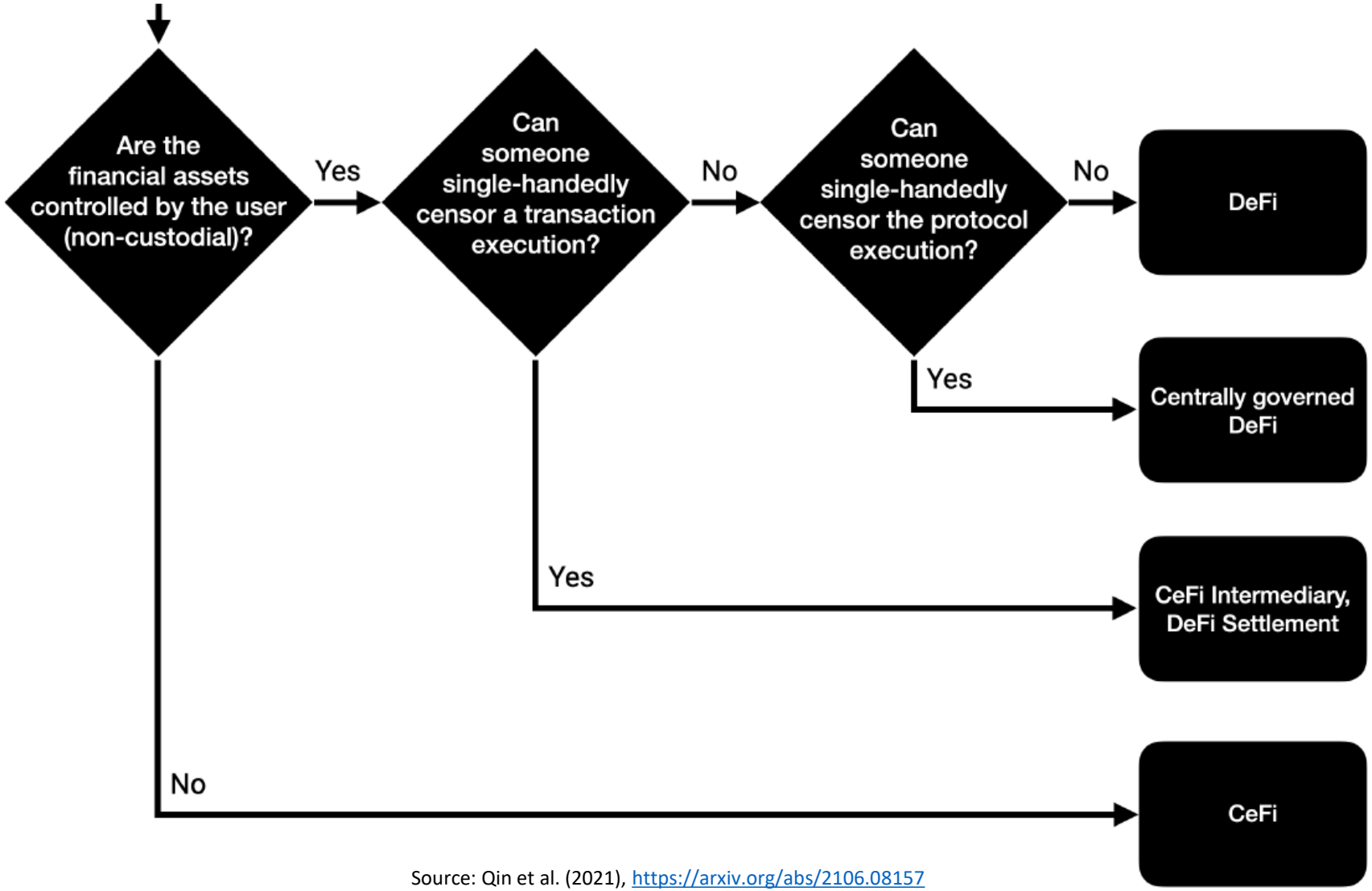
- At the moment, *DeFi can be seen as a nexus of smart contracts that are attempting to replace intermediaries.*
  - It

CeFi vs DeFi

Centralized Finance (CeFi)	Decentralized Finance (DeFi)
Closed system backed by centralized databases and protected firewalls – single point of failure	Open-source code backed by permissionless blockchains. Code and security native to the system
Only authorized users can access the system or improve it	No need for third-party approval in public DeFi systems (this depends on the implementation)
Assets are held by centralized third-parties/custodians	Assets are meant to be held by end-user
Decisions are made by the company or entity that controls the system. End user typically has no say in governance.	No single entity can control the system. Majority rule. Governance is decentralized via token. Transparent
Single entity can censor transactions and freeze accounts	Censorship possible but distributed
Physical identity is revealed to the central third party	Pseudonymous. Wallet address is available to the network's users
Need to adhere to KYC, AML laws	Wallet address and necessary gas fees
Fees are collected by central party	Fees may be distributed to the network/service providers
Data is siloed and opaque	With appropriate permission, data is fully visible

Source: Based on Song (2021) notes

CeFi vs DeFi



Source: Qin et al. (2021), https://arxiv.org/abs/2106.08157

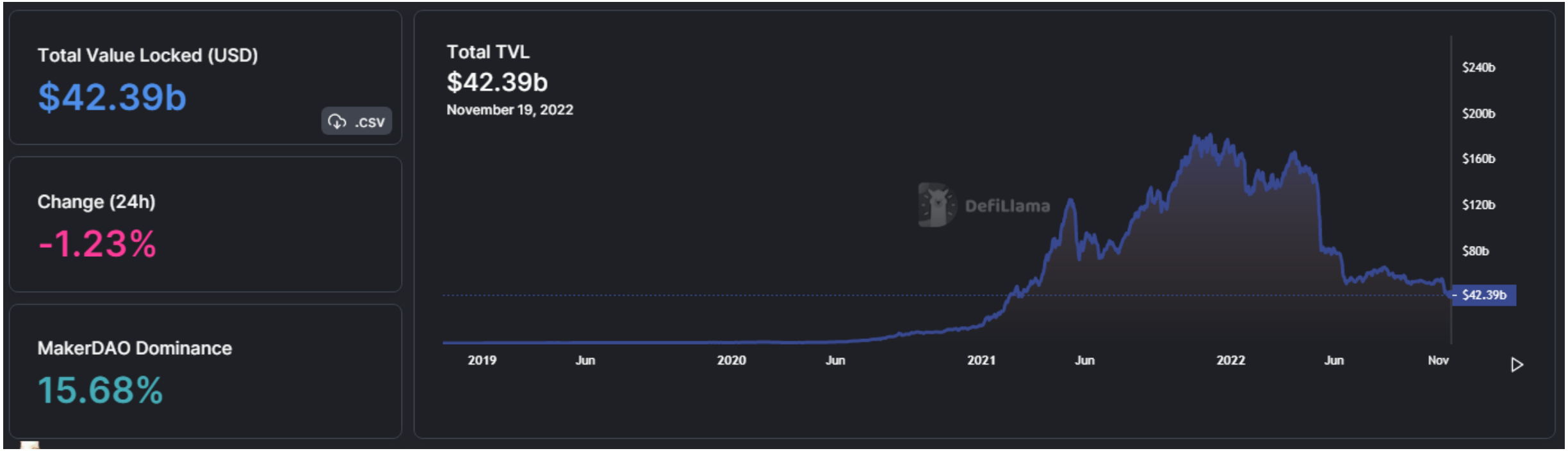
DeFi advantages

- Less reliant on central third party and potential for lower fees
- Potential for financial inclusion (although digital inclusion must precede)
- Transparent governance and data
- Public/network verifiability
- Censorship resistant
- Personal custody of assets (could become a disadvantage if not properly stored)
- Increase in competition due to lower barriers to entry
- Allows for experimentation at a wider scale (but at the risk of no regulations!)
- Non-stop market hours
- Atomicity: A blockchain transaction supports sequential actions, which can combine multiple financial operations. This combination can be enforced to be atomic — which means that either the transaction executes in its entirety with all its actions, or fails collectively.

DeFi disadvantages

- Steep learning curve
- Security
- Rug pull risks: New protocols can run away with investors' locked funds without notice, and with low chance of ever being retraced

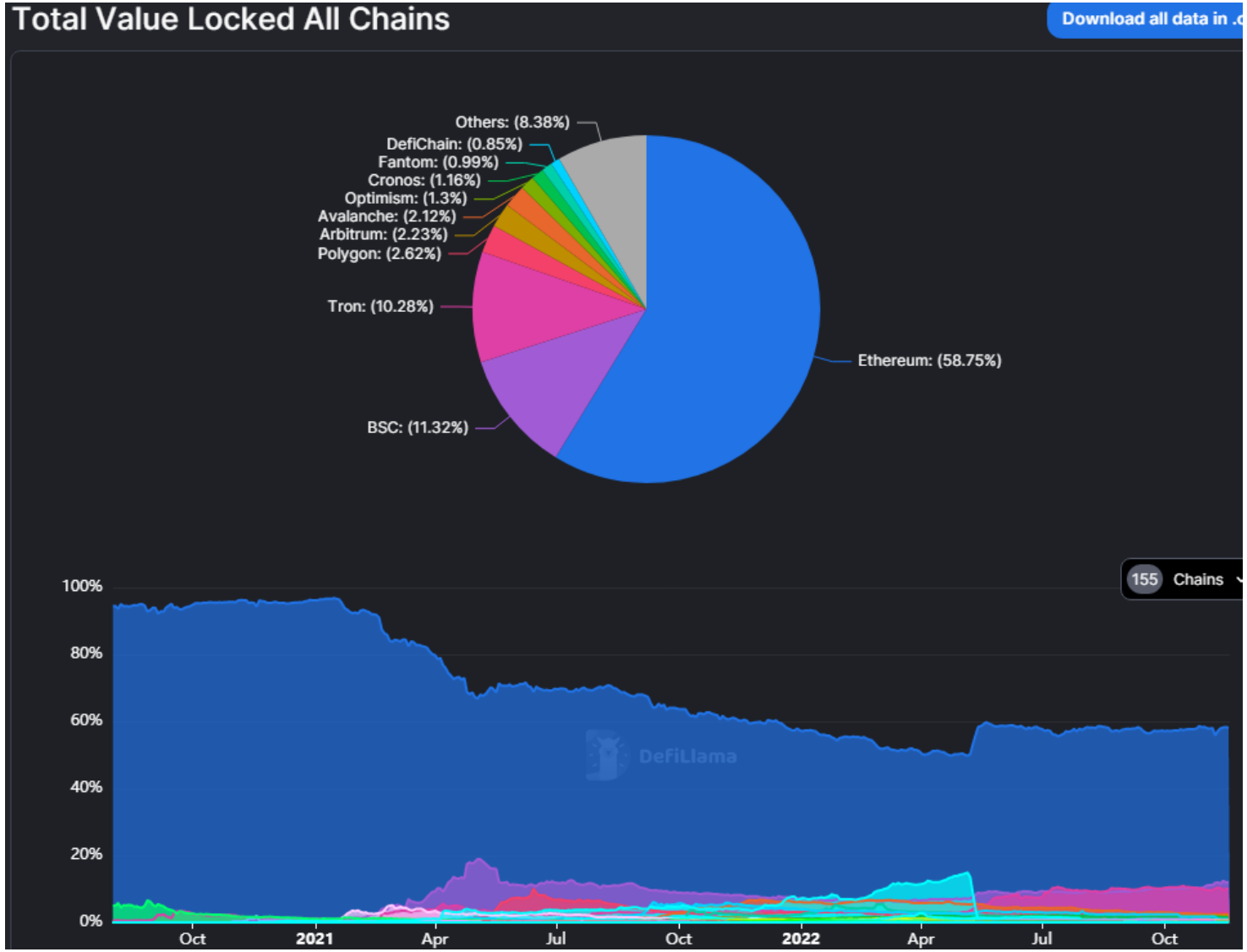
DeFi current state



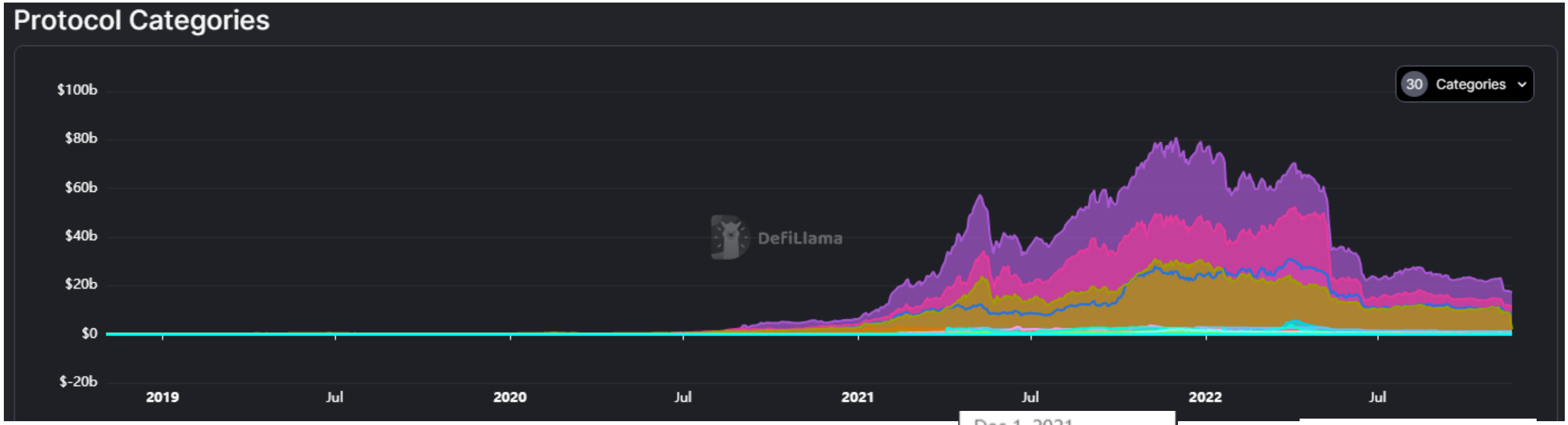
Source: https://defillama.com/

- Total Value Locked (TVL) – a measure of value of projects based on the demand and inner working of each project
- TVL was at $180 billion in December 2021 but fell dramatically during the crypto winter.

DeFi current state



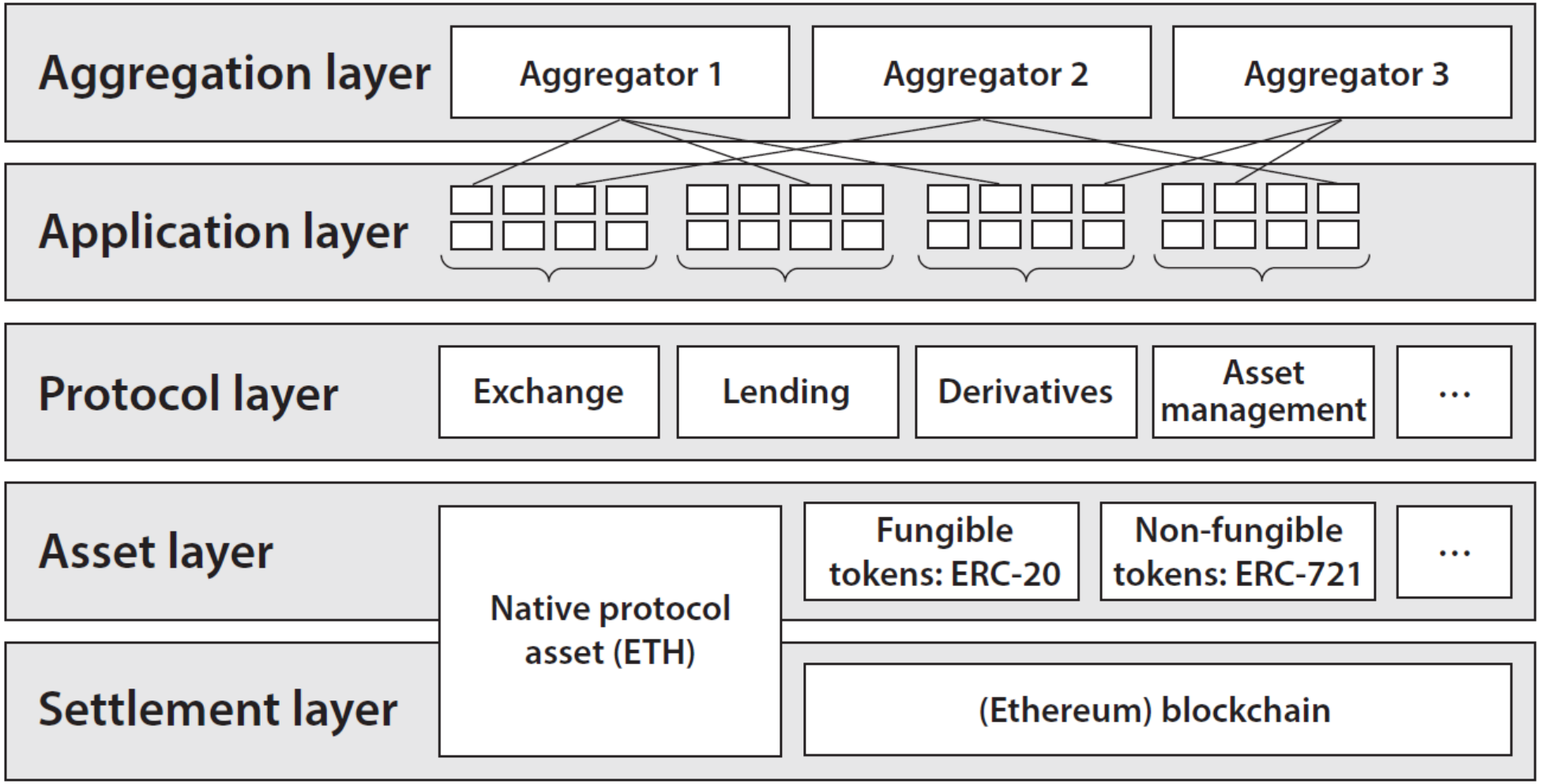
DeFi current state



Dec 1, 2021
- Bridge $25.87b
- Dexes $81.01b
- Lending $48.85b
- Synthetics $2.74b
- CDP $30.7b
- Services $277.51m
- Insurance $1.67b
- Cross Chain $1.95b
- Options $436.09m
- Derivatives $2.6b
- Others $10.45b

Nov 19, 2022
- Bridge $8.85b
- Dexes $17.25b
- Lending $11.64b
- Synthetics $418.48m
- CDP $2.09b
- Services $427.29m
- Insurance $234m
- Cross Chain $721.53m
- Options $134.58m
- Derivatives $1.22b
- Others $1.8b

DeFi Stack

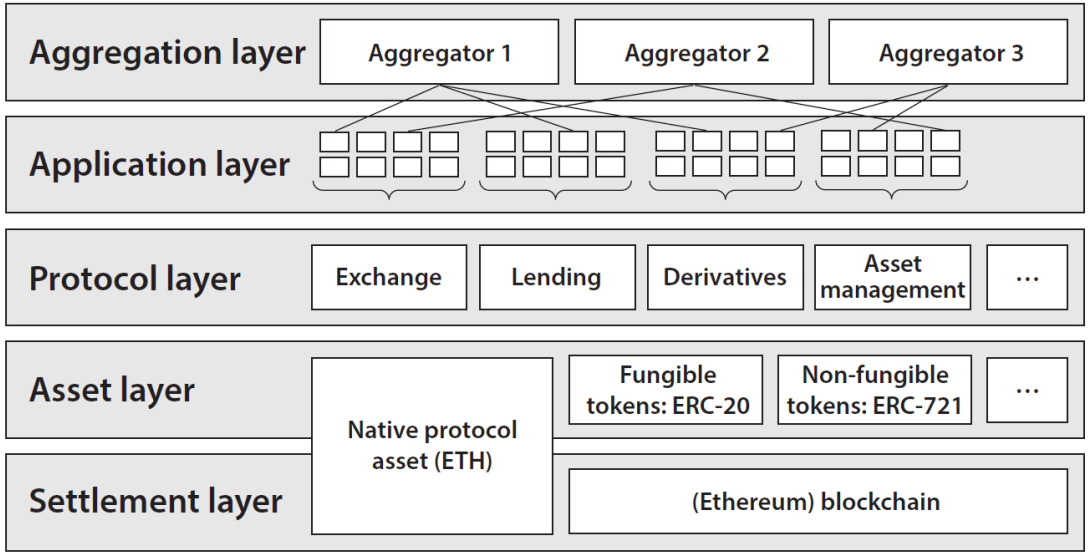


Source: Schar (2021), Federal Reserve Bank of St. Louis, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3843844

DeFi Stack

Settlement layer: “Layer-1” chains like Ethereum, Solana, etc.

- Transactions are validated through consensus mechanisms. E.g., Proof of Work (PoW) and Proof of Stake (PoS).

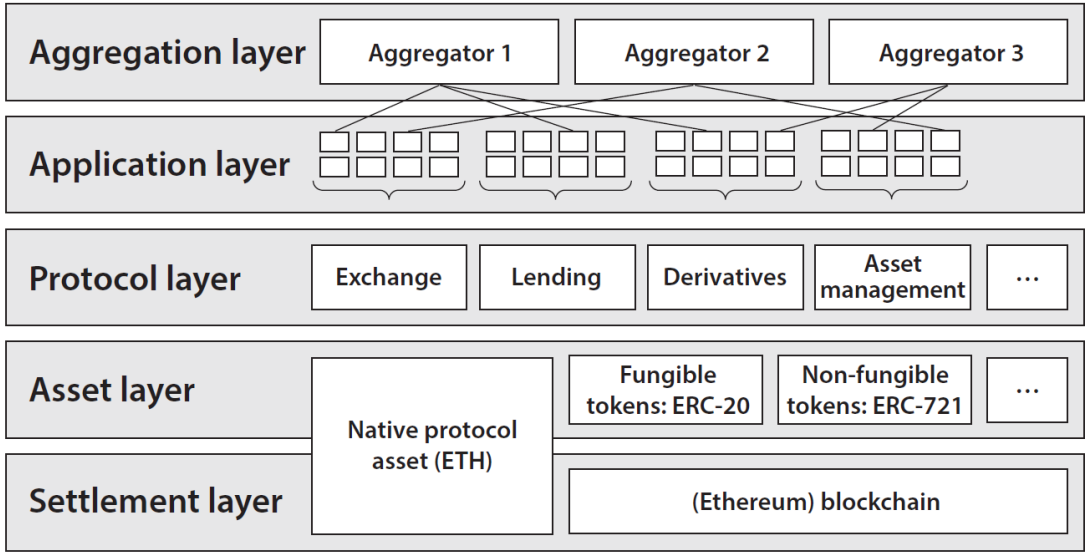


Source: Schar (2021) & WWVentures

DeFi Stack

Asset Layer: comprises both a chain's native coin (ex: $ETH, $SOL, etc.) and assets adhering to token standards (ERC-20, ERC-721, SPL, etc.).

- Native coins all have unique configurations, which is why exchanges need more time to connect and list them.
- Token standards were introduced to lower the barriers to entry, making anyone able to create their own cryptocurrency overnight. A token standard is a template containing a defined set of variables. For example, the variables for an ERC-20 token (contract) are the following:
  - balanceOf
  - totalSupply
  - transfer
  - transferFrom
  - approve
  - allowance
  - Token name (optional)
  - Symbol (optional)
  - Number of decimal places with which the token can be measured (optional)
- Introduction of token standards facilitated innovation as founders could now spend more time on building actual use cases for their tokens
  - Makes it easier for bad actors as well

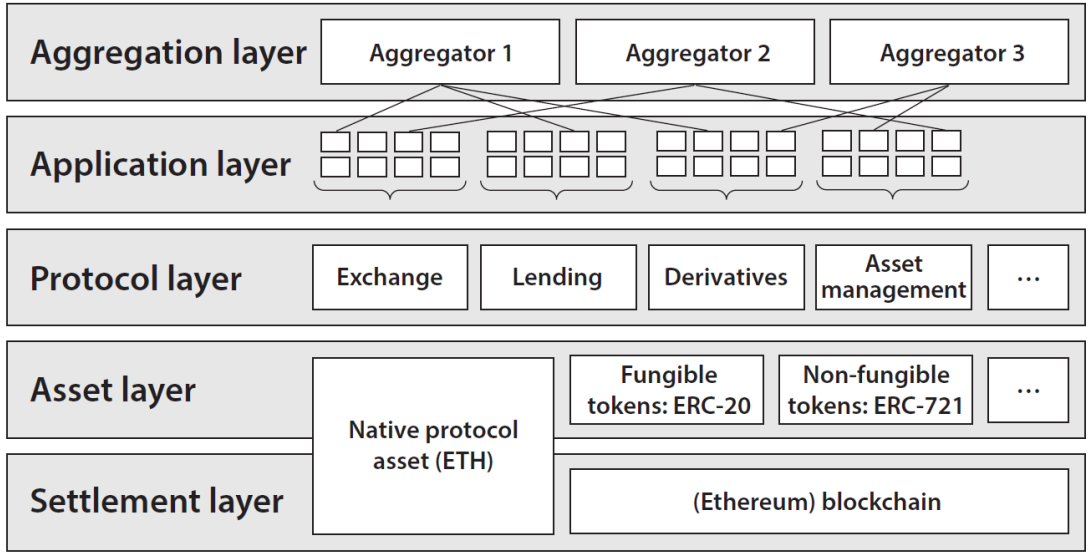


Source: Schar (2021) & WWVentures

DeFi Stack

Protocol Layer: A wide variety of Decentralized Applications (DApps) compose the Protocol Layer.

- Each DApp consists of a set of smart contracts interlinked together.
- A DApp is typically started on a single chain, but recent advancements in interoperability (notably through bridges and new code libraries) have led to the talk of multi-chain DApps (think of softwares running on both Windows and MacOS, leading to great adoption).

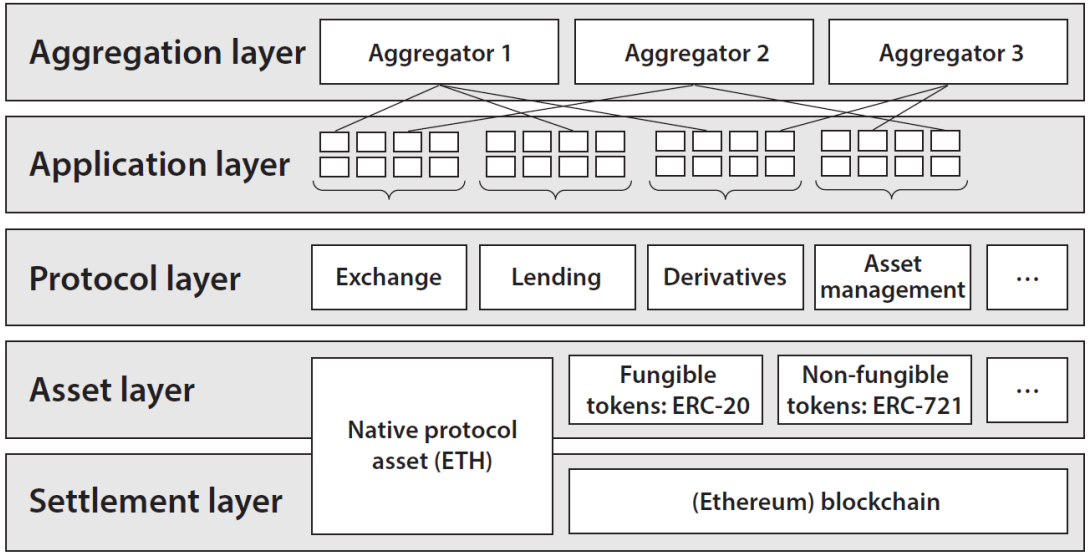


Source: Schar (2021) & WWVentures

DeFi Stack

Application Layer: Application Layer is the front-end.

- Consists of User Interfaces (UIs) that allow any DeFi user to interact with the Protocol Layer, regardless of their technical skills.
- The Application Layer is a no-code environment most often taking the form of web clients (device-agnostic websites that can be accessed through any browser).

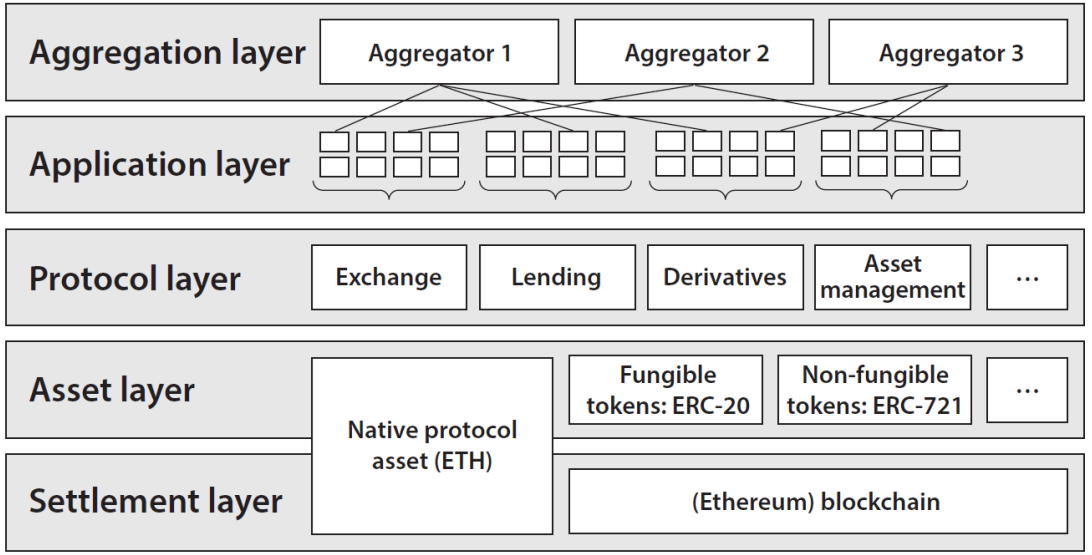


Source: Schar (2021) & WWVentures

DeFi Stack

Aggregation Layer: Aggregators have appeared as a direct result of DeFi's adoption growth: As more and more DApps emerged, users started spending more time managing their positions across all of them, as well as searching for the best options/products to use.

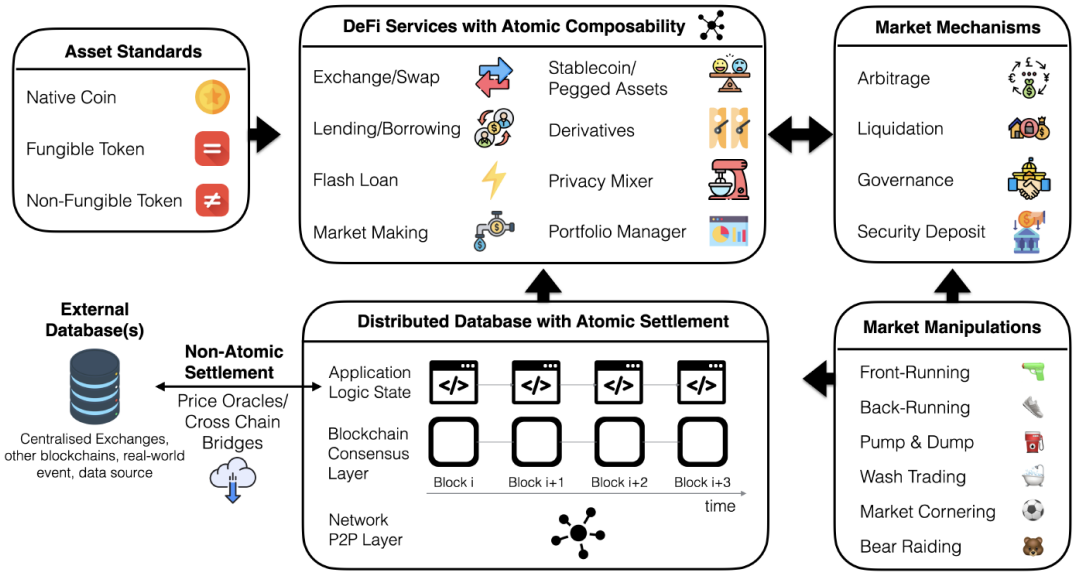
- The Aggregation Layer is considered an extension of the Application Layer in that it is also user-focused.
- Aggregation allows DeFi users to maximize their returns while reducing the efforts required to do so.



Source: Schar (2021) & WWVentures

DeFi Stack

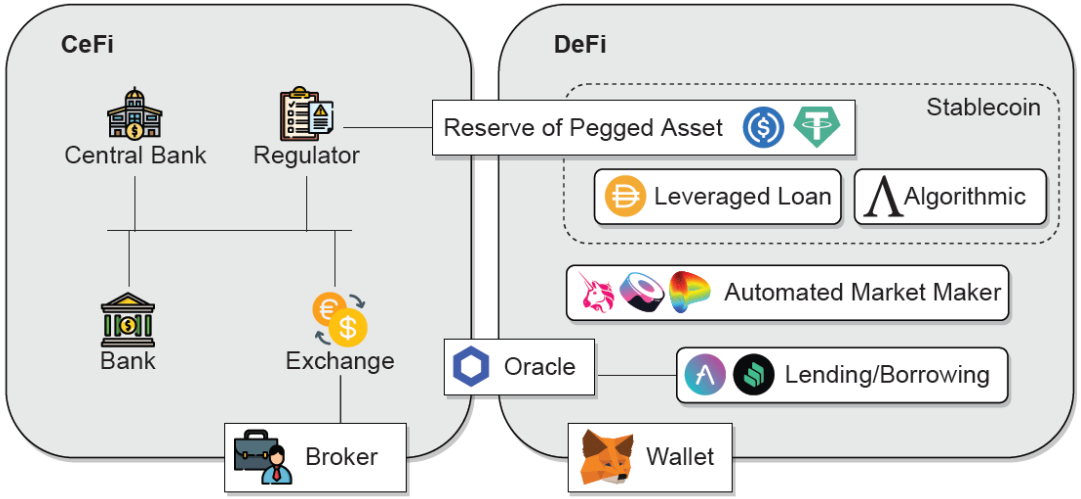
- **Oracle**: Allows for external data collection. E.g., price of an asset, news, etc.
- **Bridge**: protocols that connects tokens/blockchains from different networks.
- **Keeper**: Triggers events that execute smart contracts for a market incentive



Source: Qin et al. (2021), https://arxiv.org/abs/2106.08157

CeFi and DeFi working together

- DeFi is currently in its early stages. DeFi relies significantly on the long-standing financial system.
- Notably, the value of crypto-assets on DeFi is still primarily determined and recognized in fiat currency. Stablecoins are among the most extensively used crypto-assets since their value is tied to fiat currency.
- CeFi lending platforms act as a link between the traditional monetary system and the crypto-asset market. Those services allow users to borrow fiat money directly (rather than fiat-pegged stablecoins) and use their crypto holdings as collateral.
- DeFi and CeFi have the same goal: to provide high-quality financial goods and services to customers while also powering the economy.



Source: Schar (2021) & WWVentures

DeFi Use cases

- Decentralized Exchanges
- Lending
- Insurance
- Derivatives/Synthetics
- Non-Fungible Tokens

FinTech and DeFi

- FinTech is essentially a set of emerging technologies that aim to transform financial institutions and deliver value.
- This are is primarily driven by startups that fall into:
  - Data capture (ex: sensors, IOT, smart products)
  - Data storage (ex: cloud computing, blockchain)
  - Data analysis (ex: data visualization, artificial intelligence)
- Decentralization is part of this transformation.
- API that are critical to open banking also fall under the push for decentralization.