

DeFi 2020

The bank-less revolution

Andrea Di Nenno - May 2021

Virtues of DeFi

Equal and open access - An internet connection is the only requirement to use DeFi Markets runs 24/7 and can't be shut down

Non-custodial design - Users have full control of their capital and how it's spent

Transparency - Data and applications can't be tampered with and anyone can inspect how a particular service works. Every transaction is recorded in an immutable ledger that is inspectable by anyone at any point in the future

Composability - DeFi protocols are interoperable by default and can be used as *money legos* to build more complex use cases. Potential cross-chain interoperability

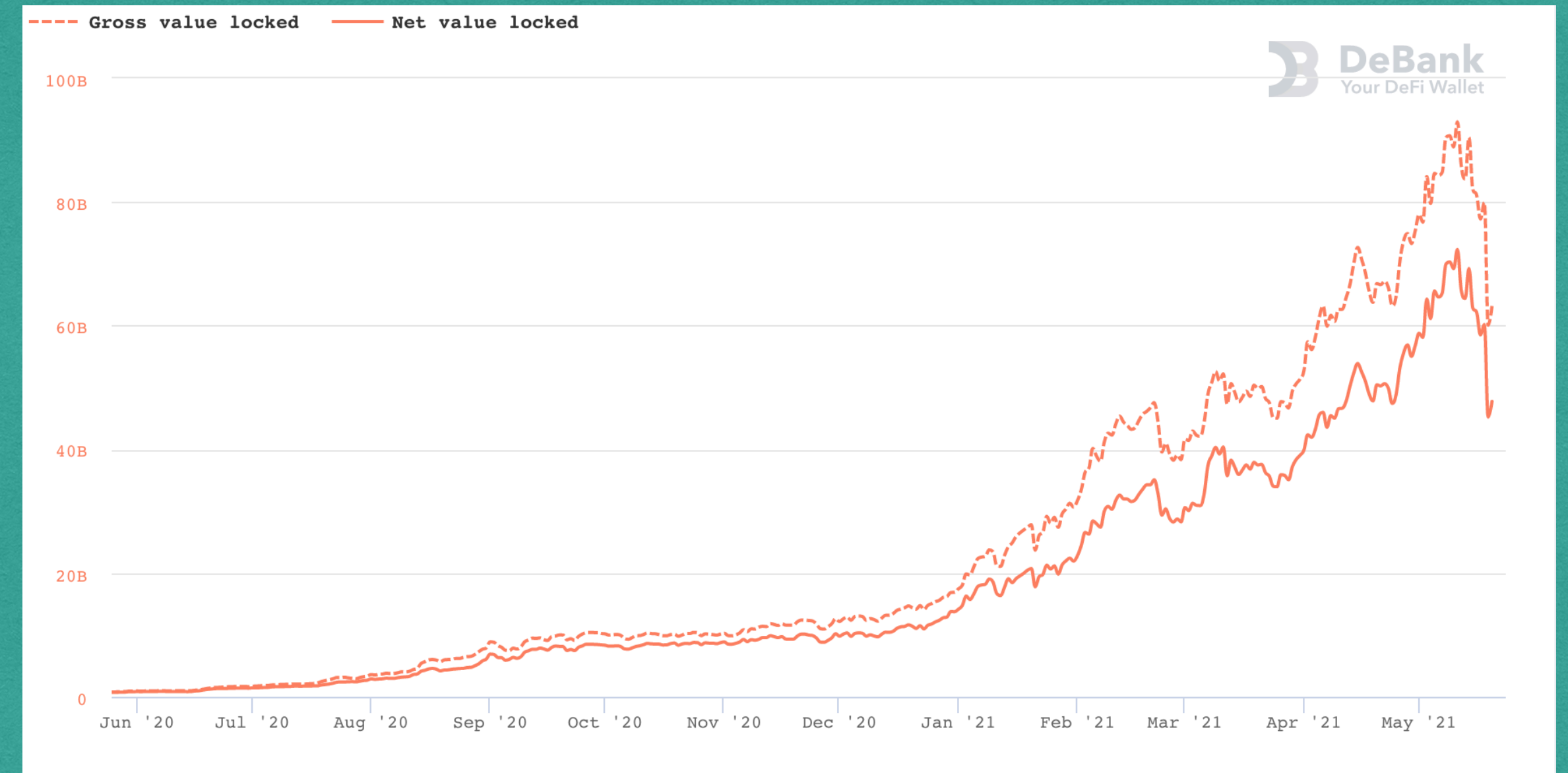
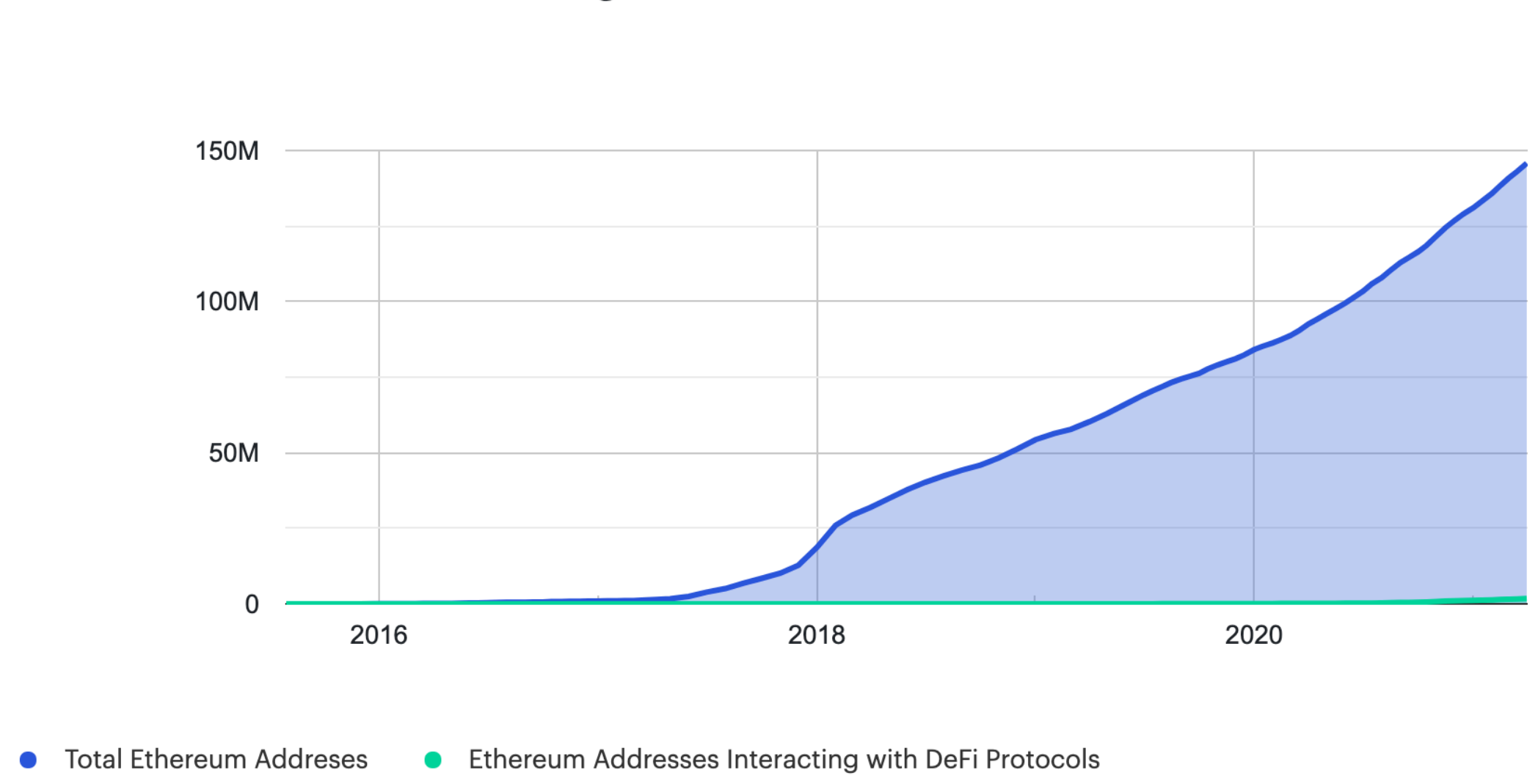
Efficiency - Transferring value becomes as cheap as transferring information over the internet (post Proof of Stake transition)

Explosive growth on Ethereum

1.75 Million DeFi addresses (1% of Ethereum active addresses)

Total Value Locked into Ethereum DeFi protocols

Ethereum Addresses Interacting with Defi Protocols



<https://consensys.net/reports/defi-report-q1-2021/>

https://debank.com/ranking/locked_value?chain=eth&chart_date=1Y

Key Innovations

Data Oracles

Stable coins

Decentralised Exchanges

Money Markets

Decentralised Governance Systems

The Oracle Problem

Blockchains are isolated networks, akin to a computer with no internet connection, preventing smart contracts to communicate with external systems.

However, for smart contracts to realise most of their potential they must be connected to the outside world (market information, IoT, web APIs)

An additional piece of infrastructure is required to bridge the blockchain to the outside world, known as an **oracle**

How do we ensure that blockchain security is kept by introducing an additional component?

What do Blockchain Oracles Do?

Listen: monitor the blockchain network to check for any incoming user or smart contract requests for off-chain data

Request: fetch data from one or multiple external systems

Format & Validate: encode data in blockchain format and create a cryptographic proof to attest the performance of the oracle

Compute: perform some type of computation on the data, like aggregating data from multiple oracles

Broadcast: sign and broadcast a transaction on the blockchain to send data and its corresponding proof for the smart contract's use

Chainlink - Decentralised Oracle Network

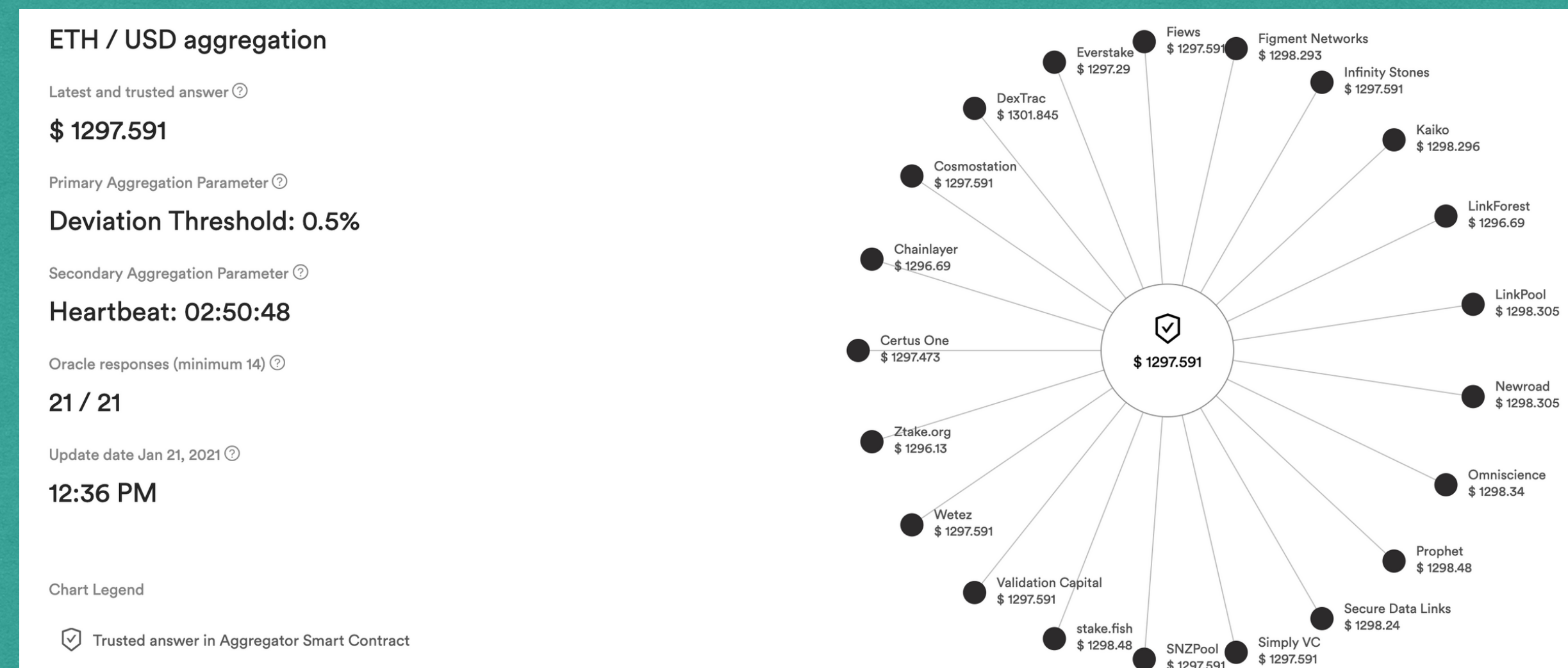
Decentralised network of independent entities (oracles) that retrieve data from multiple sources, aggregate it, and deliver a validated, single data point

Price feed and market data needed to issue, settle, and secure DeFi applications

Verifiable Random Function to provide a cryptographically secure and provably fair source of on-chain randomness

Reputation System oracles' historical performance is publicly available on-chain with metrics such as average response time, completion ratio and more

Blockchain agnostic



Key Innovations

Data Oracles

Stable coins

Decentralised Exchanges

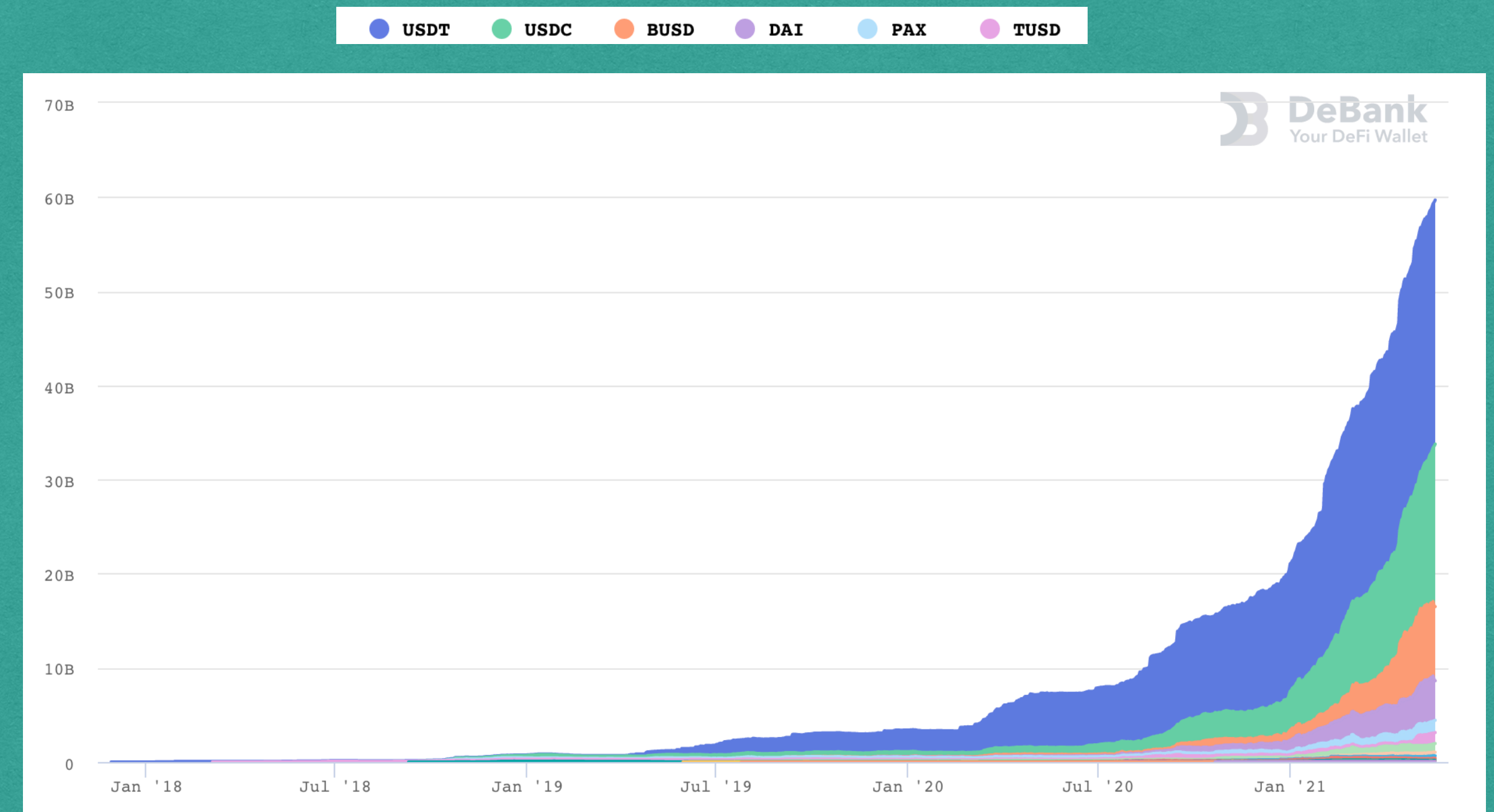
Money Markets

Decentralised Governance Systems

Stable coins

- Smart contracts that mimics a cryptocurrency without the volatility, keep their price stable in different ways
- Crucial to achieve more complex financial protocols than simple payments
- Demand for stable coins is high in lending markets, yielding high interests fully to lenders
- Many people in Latin America have used stable coins as a way of protecting their savings in a time of great uncertainty with their government-issued currencies

Stablecoins issued on Ethereum



https://debank.com/ranking/stablecoin?chain=eth&chart_date=MAX

How do stable coins maintain stability?

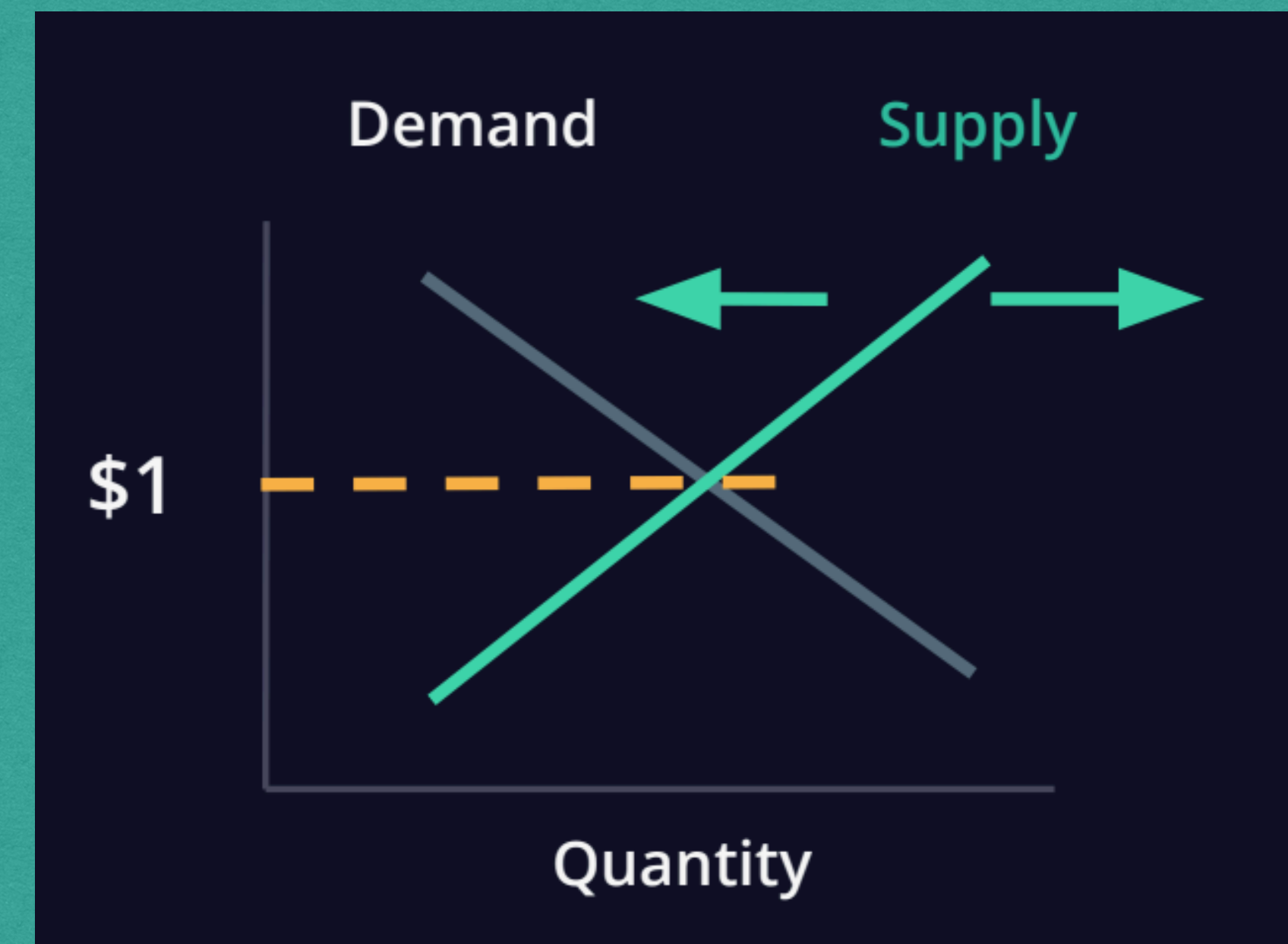
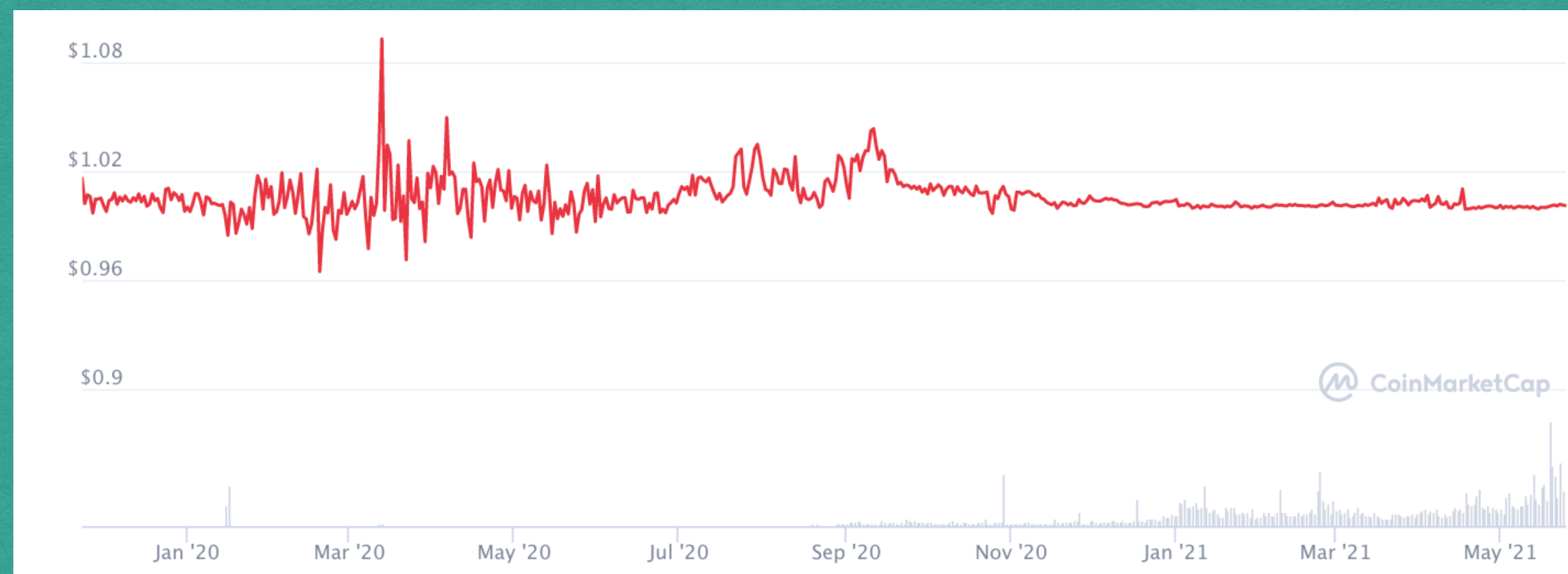
Type	Description	Example
Fiat-Backed	Centralised Each token issued on-chain is backed by the corresponding fiat currency in a treasury	USDC USDT
Crypto collateralized	Decentralised Issued when collateralised by other digital assets like ETH	Dai
Algorithmic	Decentralised Supply is increased and decreased algorithmically based on demand	AMPL FRAX

Dai

Dai is a digital currency on Ethereum whose value consistently tracks the US Dollar

A system of incentives allows users to shift the supply curve of Dai through a Maker Vault, by either issuing or burning Dai, to ensure the price stays as close as possible to \$1

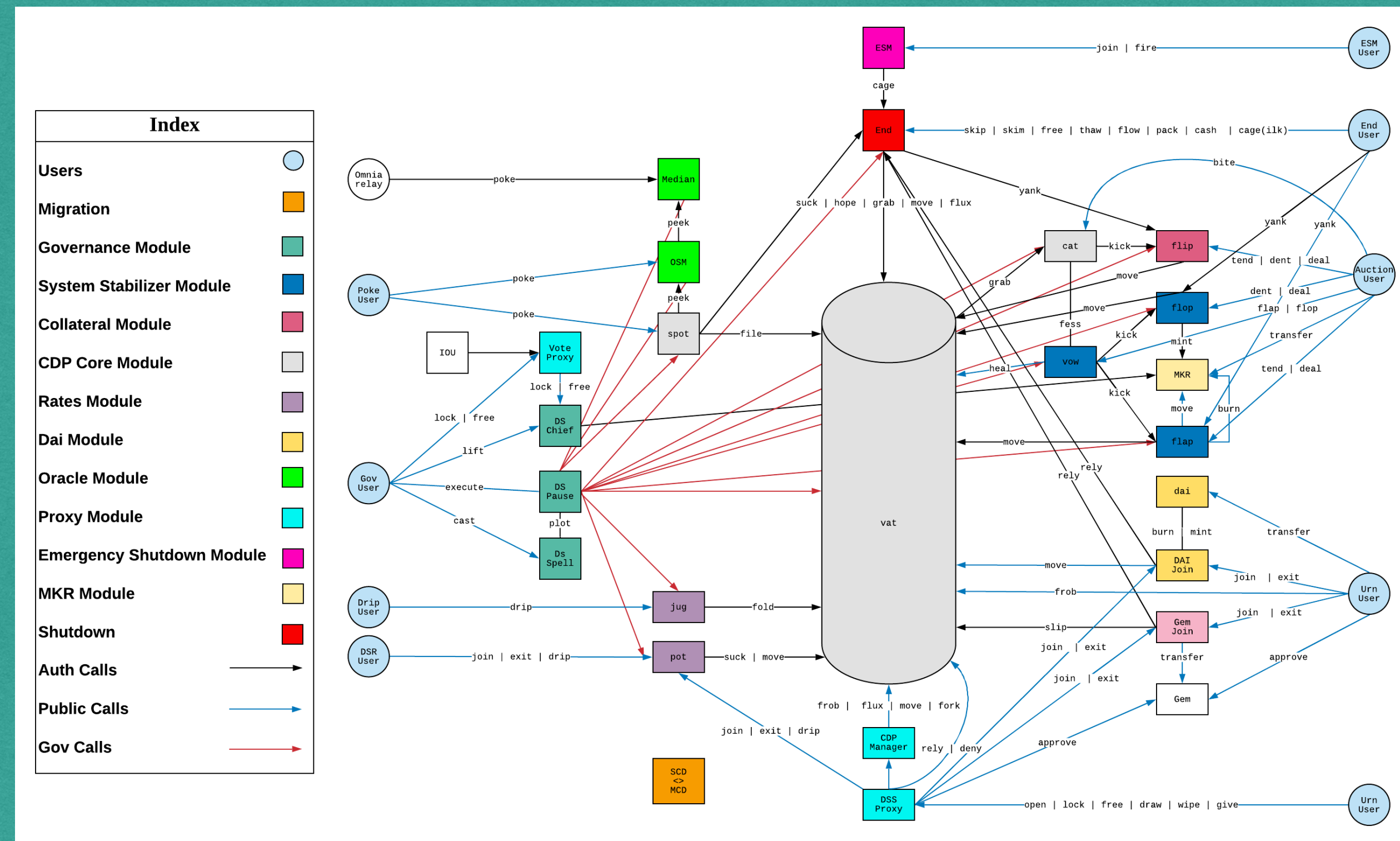
Supply of Dai in circulation is around \$5bln, fully overcollateralised



Maker Protocol

Collateralised Debt Positions - users can issue new **Dai** by locking up collateral (crypto assets) in the protocol with a 150% collateralisation ratio
Can anytime retrieve collateral by repaying Dai + interests accrued

Liquidations If the collateral value (in USD) falls below the 150% threshold, position is liquidated and collateral is taken by the protocol to cover the **Dai** loan



Key Innovations

Data Oracles

Stable coins

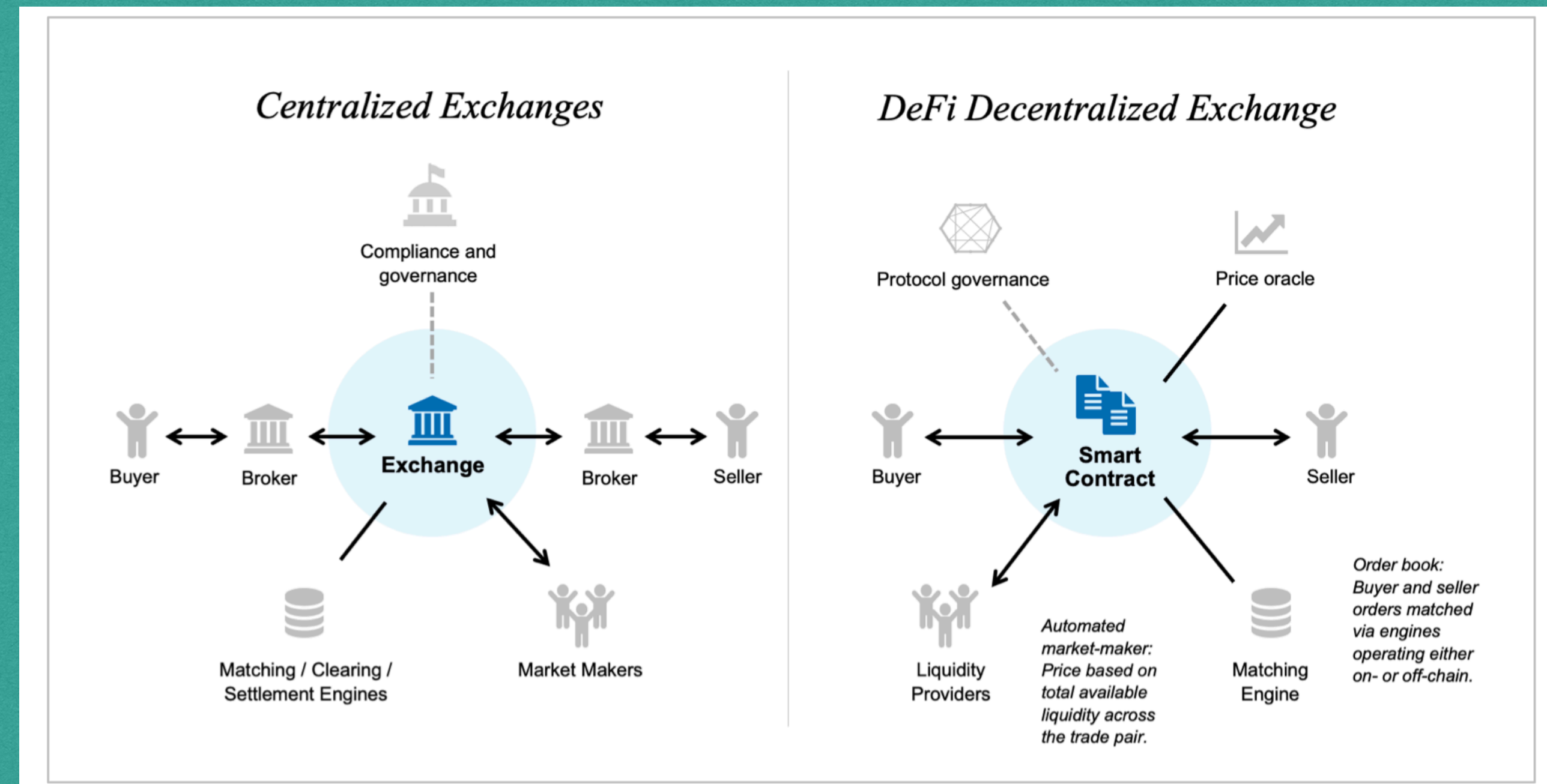
Decentralised Exchanges

Money Markets

Decentralised Governance Systems

Decentralised Exchanges

- Decentralise key functions of traditional exchanges such as **price discovery, trades matching and settlement.**
- They don't require custody of assets and so trust in the intermediary
- **Automated Market Makers (AMM)**: replaces the buy and sell orders in an order book market with a liquidity pool of two assets. Price of any trade is determined algorithmically based on the available liquidity
- **Liquidity Providers** deposit their assets in liquidity pools used for trades, earning fees paid by traders. Can withdraw their funds anytime
- **Traders** interact with Smart Contracts to trade without ever losing control of their assets

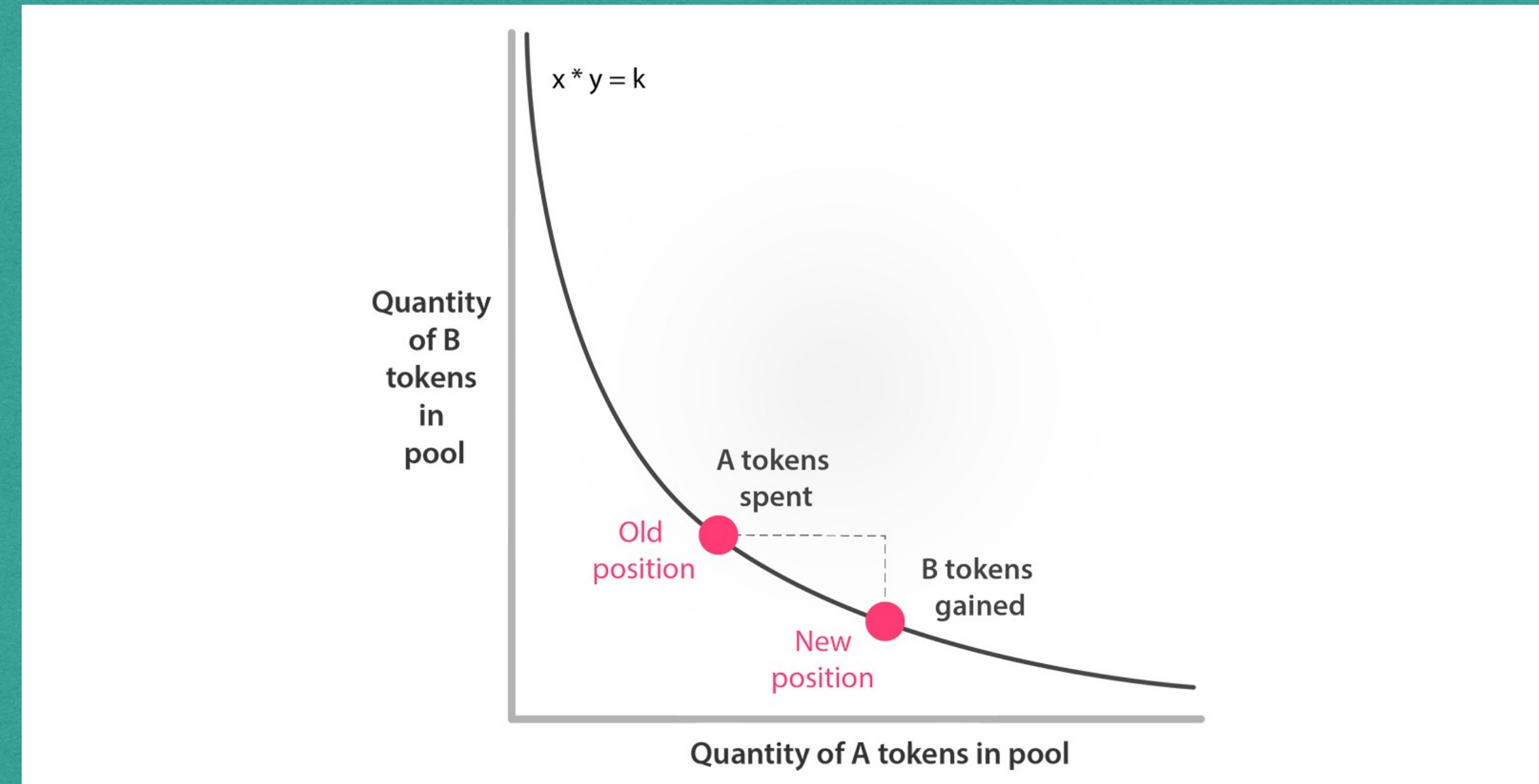


Uniswap

The **Uniswap protocol** is an AMM designed for exchanging ERC-20 tokens on the Ethereum blockchain. Ideated by Hayden Adams, at the time mechanical engineer, in 2017

Constant Product AMM: the product of quantities of assets in the pools is **constant**. Price is determined by the ratio between the two quantities

Uniswap V3 to increase capital efficiency by a factor of 4000x



PERFORMANCES

2018-2020

Over \$100bln trading volumes - 1.5mln users - \$8bln liquidity - 20k markets

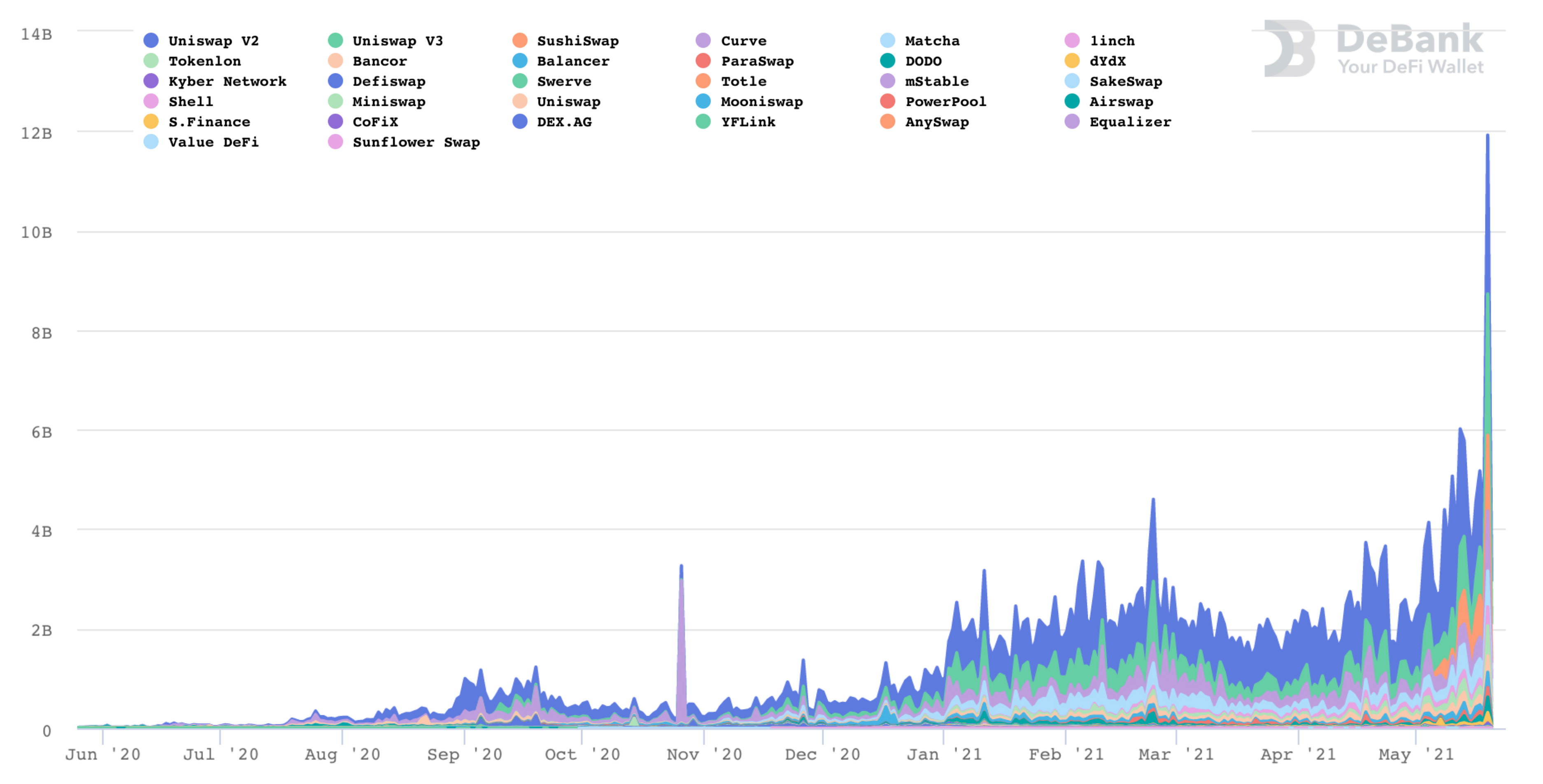
Q1 2021

\$30bln monthly volume with **\$5mln avg daily fees** for LPs

Name	▼ 1 Day Fees	7 Day Avg. Fees
🔱 Ethereum	\$16,691,146.20	\$32,053,524.84 ▼
🦄 Uniswap V3	\$4,589,020.55	\$4,696,228.46 ▼
🦄 Uniswap V2	\$3,829,918.55	\$5,434,145.03 ▼
🟠 Bitcoin	\$3,793,787.44	\$4,030,967.66 ▼

<https://cryptofees.info/>

Decentralised Exchanges Volume



https://debank.com/ranking/dex?chain=eth&chart_date=1Y

Key Innovations

Data Oracles

Stable coins

Decentralised Exchanges

Money Markets

Decentralised Governance Systems

Money Markets

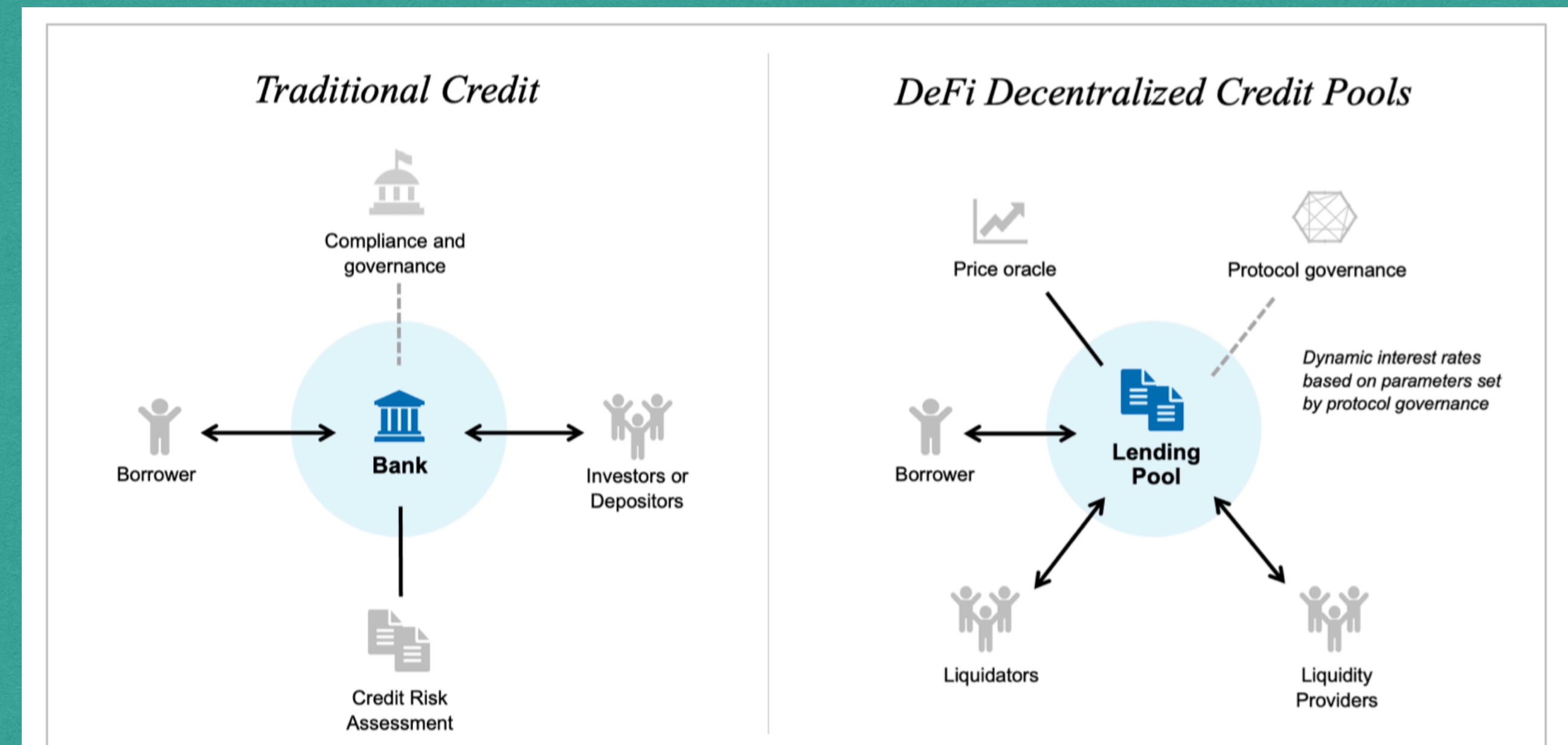
Money markets fill the gap between people with surplus assets they can't use, and people without assets that would make them productive.

Decentralised Money Markets: non custodial pools of assets with **algorithmically derived interest rates for lending and borrowing**, based merely on supply and demand and thus dynamic

Lenders provide liquidity to the market to earn a **passive income**, accrued and available at each new block. Can remove their liquidity anytime

Borrowers are able to borrow with no regulatory requirements against their crypto-asset collateral, interest determined by overall liquidity demand.

Loans are subject to liquidation in case of low margin



DeFi Money Markets

COMPOUND Protocol

- +**350k** users since mid 2020
- +**\$40bln** Total Borrow Volume
- +**\$130bln** Total Supply Volume
- +**\$20bln** liquidity (deposits and loans)

AAVE

- +**50k** users since mid 2020
- +**\$18bln** liquidity (deposits and loans)

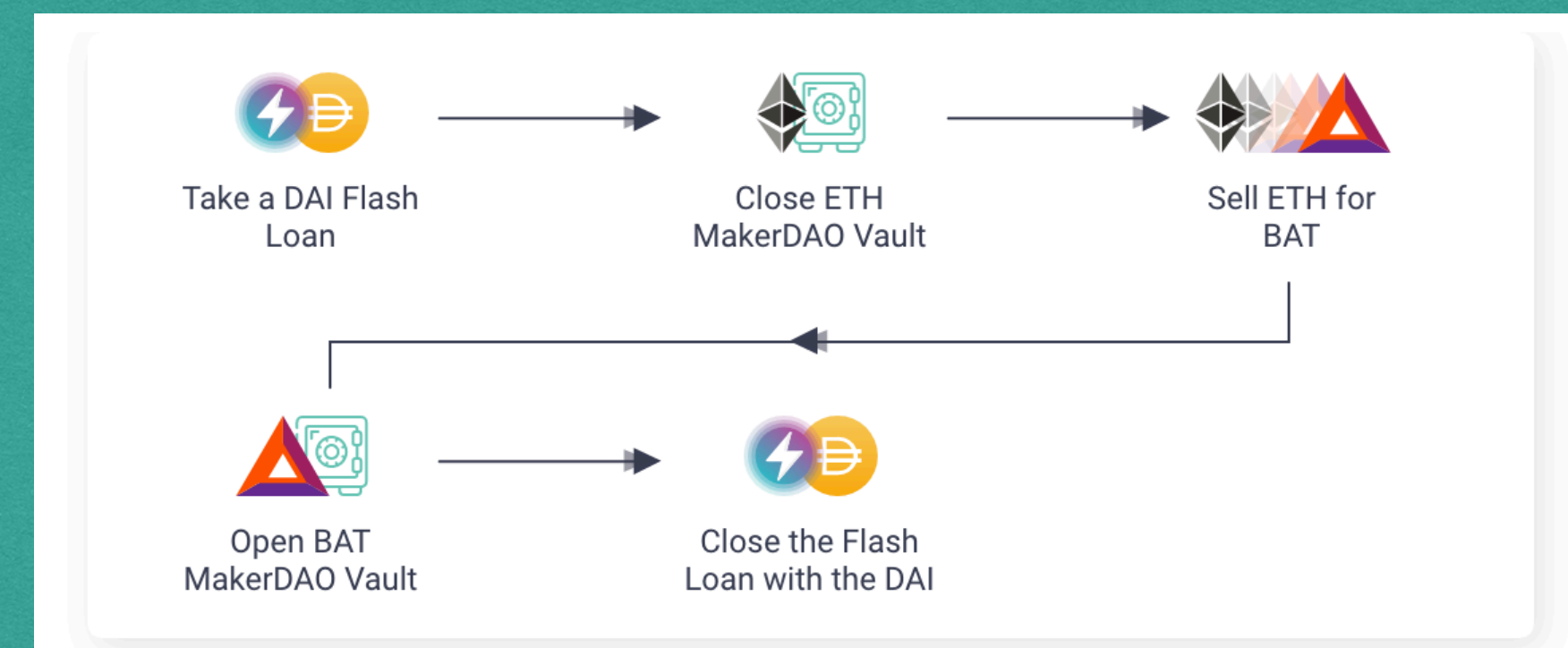
<https://duneanalytics.com>

Flash Loans

Zero-collateral loans that must repaid within the same transaction, which can be made up of multiple operations

The whole transaction is reverted to effectively undo the actions executed until that point **if loan is not fully repaid**

Use-cases include **arbitrage, collateral swapping and protocol exploits**



Collateral swapping through a Flash Loan

Key Innovations

Data Oracles

Stable coins

Decentralised Exchanges

Money Markets

Decentralised Governance Systems

Decentralised Protocol Governance

Crucial decisions about protocol issues, incentives, parameters, enhancements and more are given to protocol users and stakeholders, through **Governance Tokens** (ie ERC-20)

Discussions around issues and changes on protocols forum

Improvement proposals are coded into smart contracts and put on community votes that happens on-chain where **1 token equal 1 vote**

If quorum is reached and proposal is accepted, code is implemented and deployed to the network

Governance tokens are distributed to platform users as a reward for using the protocol, typically proportional to liquidity provided

No private pre-sales of the token and no tokens set aside for the protocol's creators attracts communities to organically grow and enhance the protocol without concentrated power

Liquidity Mining firstly launched by **Compound Protocol** in July 2020 to bootstrap liquidity, followed by most of other DeFi protocols

Uniswap airdropped **400 UNI** (15% of total supply, now worth over \$10k) to each user (also one-time users)

DeFi Ecosystem just keeps growing

Insurance Protocols - Nexus Mutual

Derivatives Markets - Synthetix Protocol, UMA Protocol

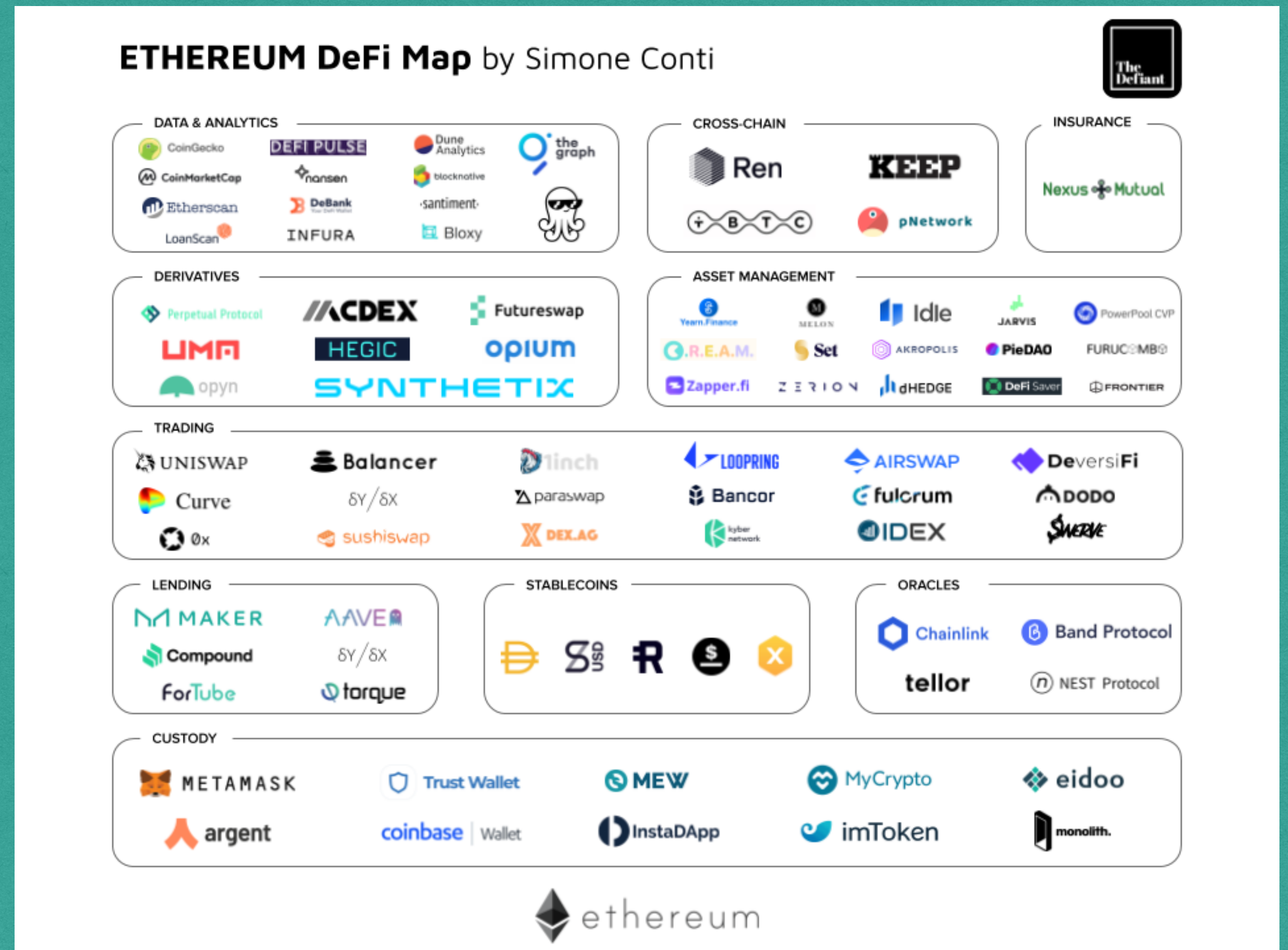
Asset Management - Yearn Finance, Set Protocol

Prediction Markets - Augur

Options markets - Hegic, Opyn

Liquidity Aggregators - 1Inch, Paraswap

No-loss lotteries - PoolTogether



DeFi 2020

The bank-less revolution

Andrea Di Nenno - May 2021