UNIVERSITY of NICOSIA

Session 12

Decentralized Finance

DFIN 511: Introduction to Digital Currencies

Session objectives

- The objective of this session is to provide an introductory coverage of **Decentralized Finance (DeFi)**.
- We will explore the history of DeFi, how it evolved over the years and what aspects of the traditional financial/banking sector it may disrupt in the future.
- Then, we will dive deeper into the DeFi ecosystem and discuss its foundations, as well as constituent elements.
- Finally, we will explain how the different ingredients/pillars of DeFi are connected and interdependent.
- The objective is to develop an understanding of DeFi, its advantages, but also the risks associated with it.

Session outline

1. DeFi History
2. Foundations of the DeFi Ecosystem
3. Lending & Borrowing
4. Decentralized Exchanges (DEXs)
5. Stablecoins
6. Oracles
7. Wallets
8. Non-fungible tokens (NFTs)
9. Conclusions
10. Further reading

Session 12: Decentralized Finance

1. DeFi History

DeFi History

The origins of DeFi

- There is not a particular date on which Decentralized Finance was born, but there are some important events that played an important role on its evolution and the form that it has today.
- DeFi is part of the broader ecosystem of cryptocurrencies:
  - Bitcoin redefined payments and the concept of store of value.
  - However, Bitcoin did not directly impact the main functions of the traditional financial services industry, like exchange, borrowing and lending, insurance, prediction markets, etc.
  - The birth of smart contracts by Ethereum set the foundations for such areas to be disrupted by blockchain.
- The precursors to DeFi were projects like **TheDAO** and **Etherdelta** (2016-2018).
  - While both projects were hacked and finally failed, they paved the way for many subsequent DeFi applications.
  - TheDAO has already been discussed in previous sessions of the course.

DeFi History

The origins of DeFi

- Etherdelta, was one of the first decentralized exchanges (DEX). It was based on order books, like centralized exchanges, which is an inefficient model for a DEX, in terms of costs for market making. Further to that important design limitation, the exchange was hacked for around $800K and soon after its founder was charged by the SEC for "operating an unregistered national securities exchange".

○ You can find a brief timeline of the DeFi history until early 2021 here.

DeFi History

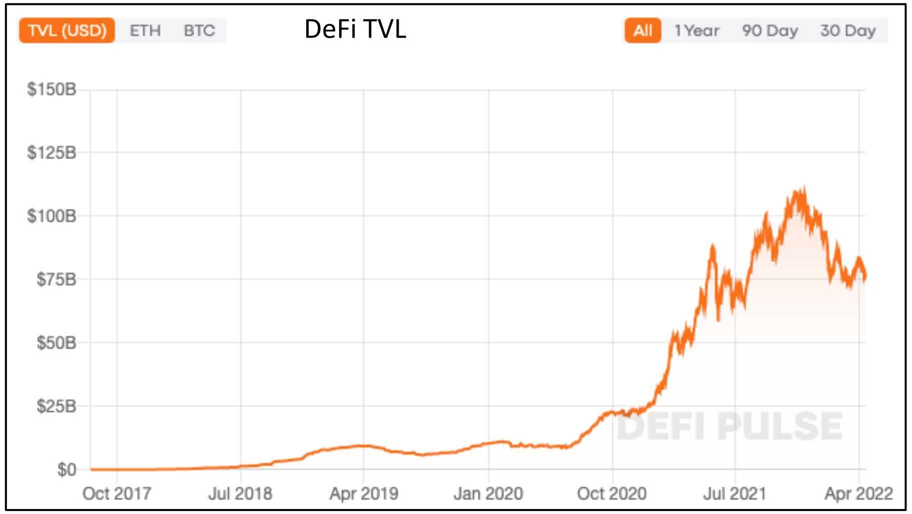
Early DeFi projects

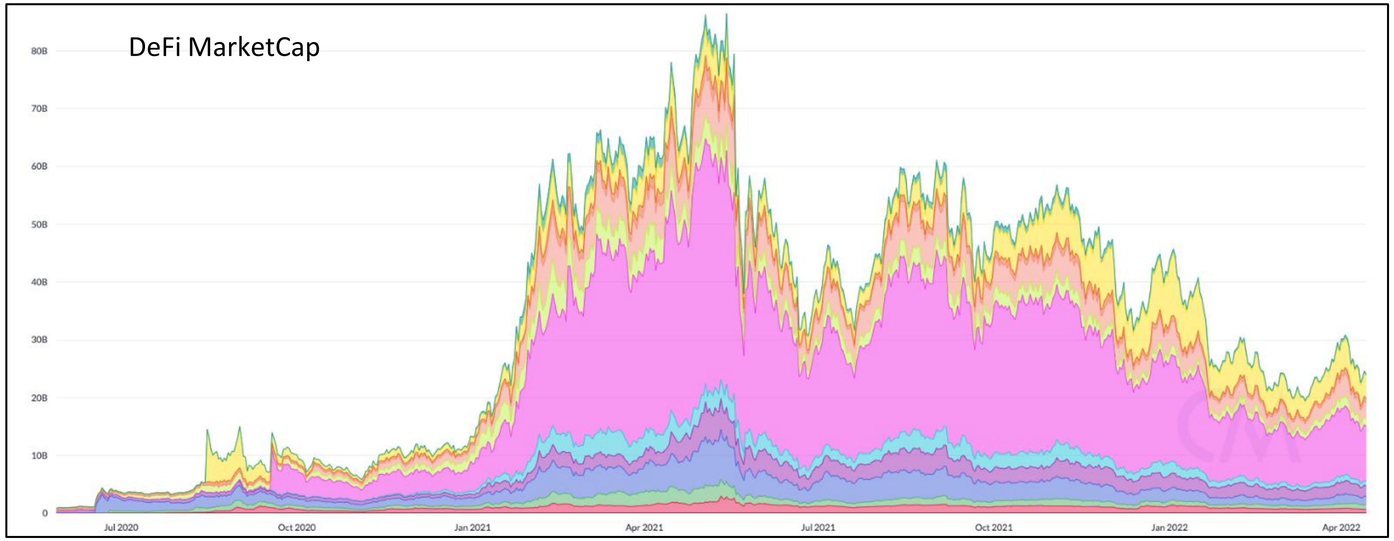
- **Maker** is considered by many as the "father" of DeFi. The idea was conceived in 2014, but it was not implemented until 2017.
  - Maker is deployed on Ethereum as a smart contract that allows anyone to put a crypto asset as collateral and borrow a percentage of its value through a stablecoin called **DAI**.
- A bit later (2018-2019), many projects that played an important role in the early DeFi ecosystem were born. Among them **Aave** (previously ETHLend), **0x** and **Synthetix**.
  - Despite these early pioneers, DeFi was not identified/named as a separate crypto sector back then.
- Important breakthroughs in 2019-2020 created the sector as we know it today and popularized the DeFi term.
  - The most important innovation was probably the shift from a user-to-user to a **user-to-contract interaction model**, initially by Compound & Aave.
  - Other important developments in that era, were the introduction of **liquidity pools** and **Automated Market Makers (AMM)** by Bancor & Uniswap and the **liquidity incentive program** launched by Compound & Synthetix.

DeFi History

The state of DeFi today

- The main catalysts for the explosive growth of DeFi in the summer of 2020 was the creation of the notion of **yield farming**.
- As a result, **Total Value Locked (TVL)** and the total market capitalization of the DeFi ecosystem have skyrocketed.
  - **TVL** is the total amount of assets that are supplied to (locked in) DeFi protocols. There is a common misunderstanding that TVL represents the amount of outstanding loans in the DeFi ecosystem, when it actually represents the total amount of underlying supply being secured by a specific decentralized application and/or by DeFi as a whole.


DeFi TVL


DeFi MarketCap

Session 12: Decentralized Finance

2. Foundations of the DeFi ecosystem

The DeFi ecosystem

Creating "Money Legos"

- **DeFi** implements in the world of crypto, services typically provided by the traditional financial system (**TradFi**), in a way that is (aimed to be) more efficient in terms of capital allocation, execution time, participation, transparency, security, decision making, and decentralization.
- We use the term **DeFi ecosystem** to refer to the entirety of such services.
  - That is because DeFi can be thought of as a living organism, whose different organic systems are connected and dependent on each other to function normally.
  - Similarly, you may conceptualize DeFi as an interconnected ecosystem, with several intertwined pillars, connected in what is sometimes referred to as **money legos**, in which the same building blocks can be reconfigured to create wholly new types of services. That is because in contrast to TradFi, DeFi protocols are open-ended, and permissionless.
  - Of course, there is competition inside the same pillars of the ecosystem to attract users and assets, but among the different pillars there is a (mostly) symbiotic relationship.
- As a matter of fact, it was exactly when DeFi projects realized that the success of one is dependent on the success of others and started to cooperate to unlock further possibilities and increase their efficiency, that the DeFi space exploded in innovation and popularity.

The DeFi ecosystem

DeFi VS TradFi

Characteristic	DeFi	TradFi
Accessibility	Open to anyone	Must apply and be verified
Custody of funds	Mostly self-custody	Mostly by third-parties
Control of funds	User and smart contracts	Institutions and their partners
Speed	Final settlement happens in minutes and is irrevocable	Final settlement can take weeks and can be revoked
Availability	Markets are open 24/7/365, and cannot be shut down	Markets operate in business hours, and can be shut down
Transparency	Mostly transparent - anyone can verify the financial activity of open source protocols on the blockchain	Mostly not transparent – besides financial statements, you can't ask banks for their loan history or assets under management
Protection	Auditing, self-verification, or no protection	Guarantees by the central bank and regulation
Services available	Limited but growing - poorly integrated with TradFi	All services – Poorly integrated with DeFi

The DeFi ecosystem

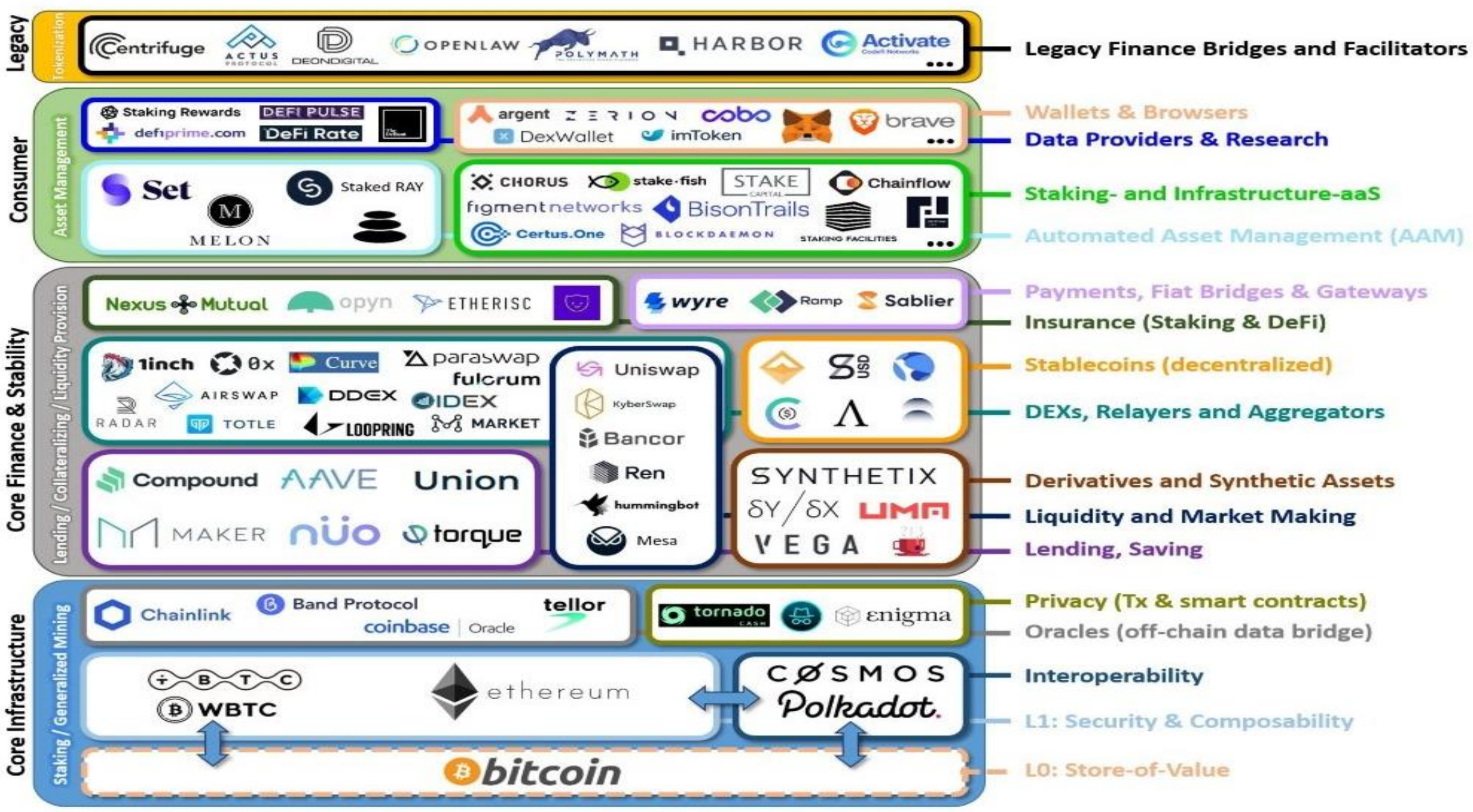
Main Pillars

- There is no universally accepted categorization of the different pillars of the DeFi ecosystem.
    - Moreover, innovation in the space is moving fast, so any such strict categorization would be short-lived.
- DeFi projects are basically **dApps (decentralized applications)**, based on an underlying blockchain, which is called **Layer 1 (L1)**, as it is the first underlying layer of the DeFi stack.
    - Typical L1 blockchains include **Ethereum, Binance Smart Chain, Polkadot, Solana** and others (in previous sessions we referred to such L1's as platform coins)
    - DeFi-enabling L1's need to support smart contracts, of course. So, Bitcoin wouldn't be a natural choice for L1.
    - L1's provide the first and more important line of **security** of the DeFi ecosystem, responsible for providing the necessary tools that allow DeFi projects to discover and implement application-layer innovations.

The DeFi ecosystem

Main Pillars

Decentralized Finance (DeFi) Stack: Product & Application View

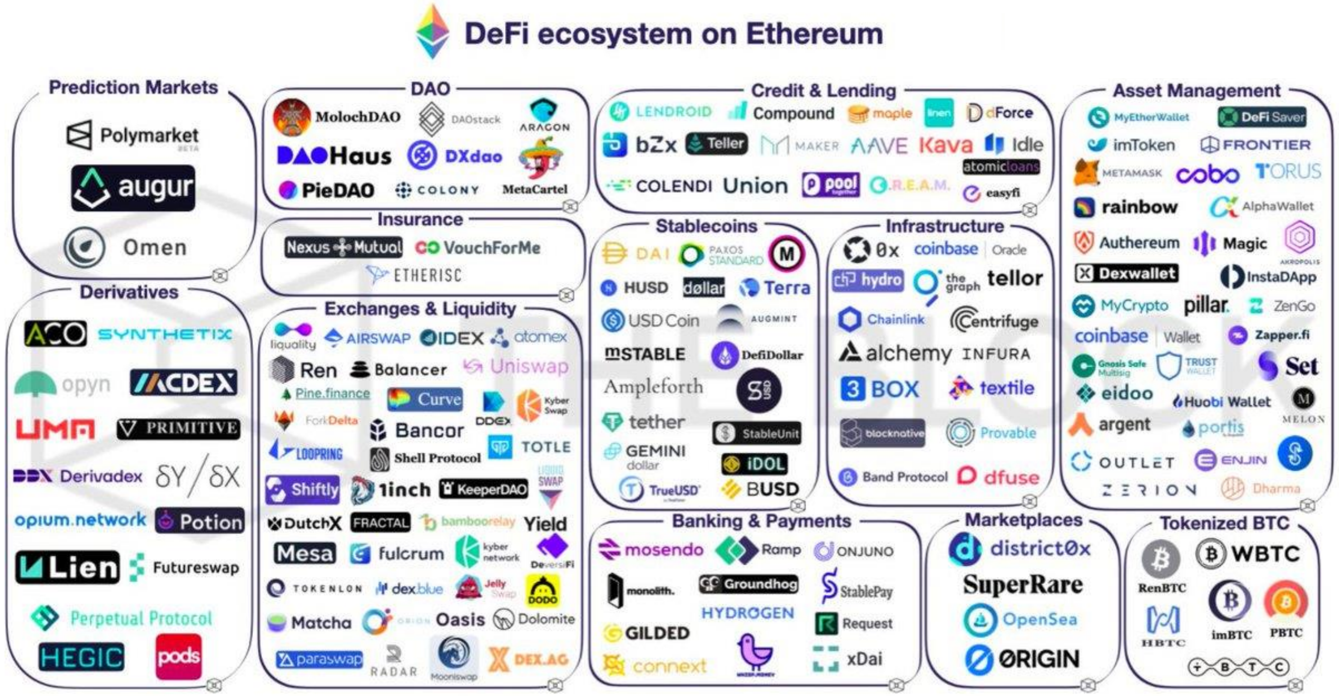


Source: StakingRewards

The DeFi ecosystem

Layer 1 – Ethereum

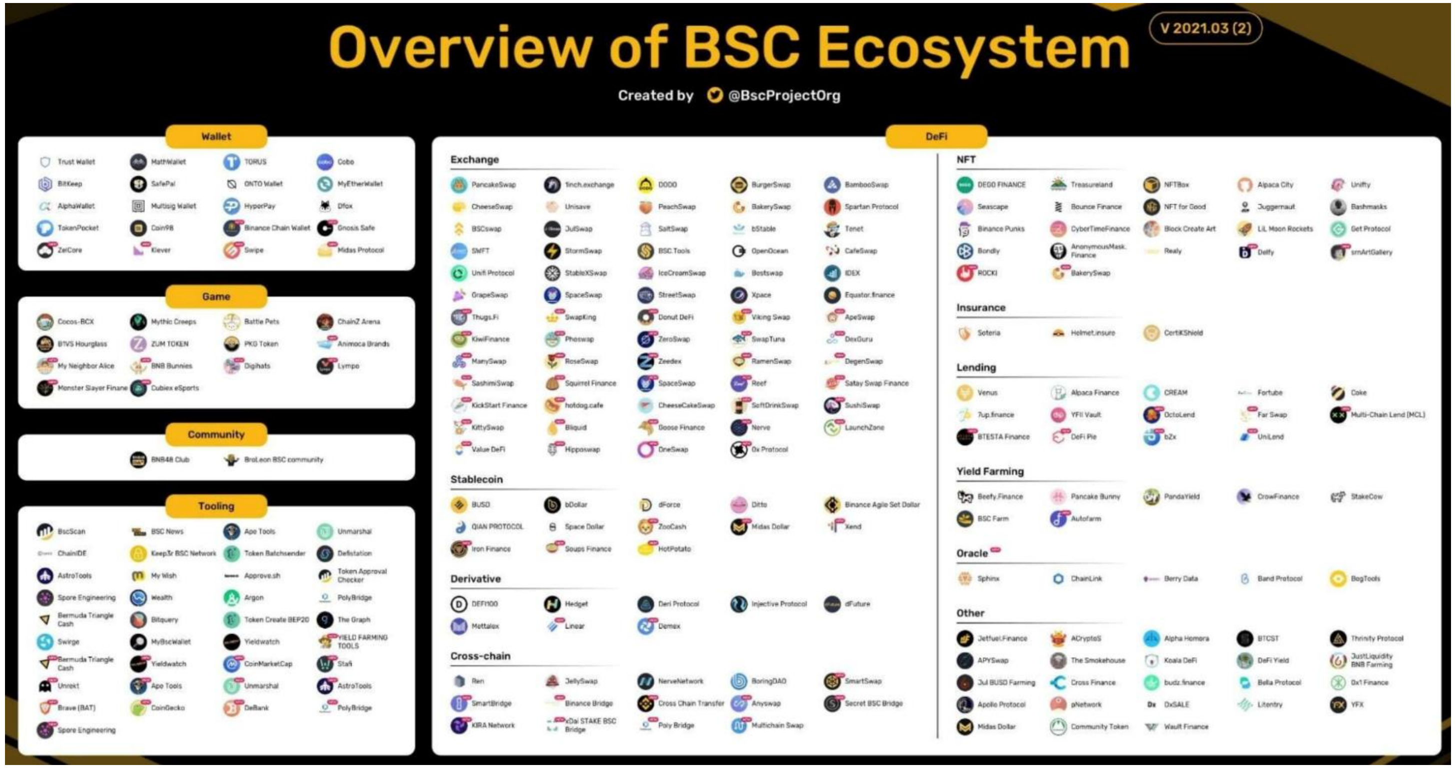
- Ethereum is, to date, by far the L1 solution with the largest DeFi ecosystem.
  - Ethereum was the first platform to focus on smart contracts, which later became the building block of DeFi. That gave Ethereum the first mover’s advantage, creating network effects and scales of economy. However, the idea of smart contracts was not new, as they were proposed in 1994 by computer scientist Nick Szabo.



The DeFi ecosystem

Layer 1 – Binance Smart Chain

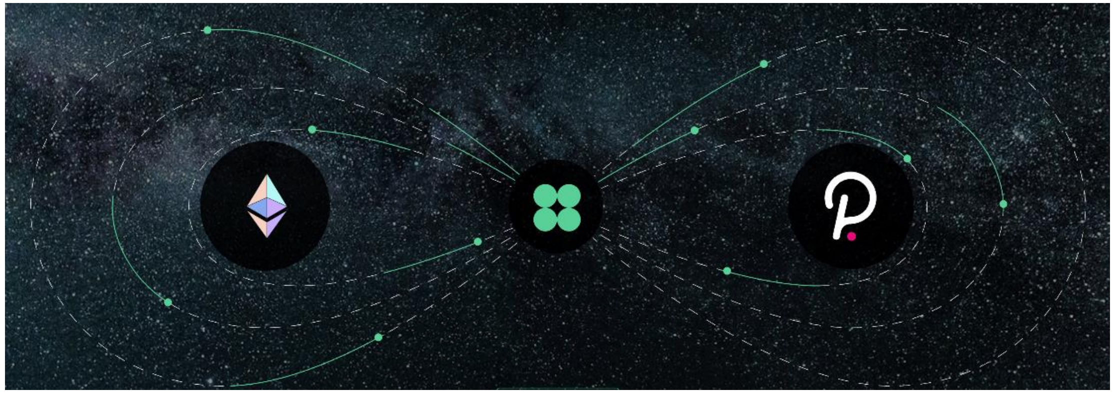
- **Binance Smart Chain (BSC)** has recently emerged as a popular L1 alternative, especially as transaction fees skyrocketed in Ethereum due to the popularity and increased used of DeFi applications there.



The DeFi ecosystem

Layer 1 – Interoperability

- Until today, L1 blockchains are, by and large, not interoperable.
    - Hence, different L1’s provide the basis for different DeFi ecosystems, which do not communicate with each other.
    - A lot of research is being focused currently on the field of **L1 interoperability** and creating **bridges** between different protocols.
    - **Polkadot** and **Cosmos** are two frameworks focused on blockchain interoperability.
    - An example of cross-chain interoperability implementation between Ethereum and Polkadot is **Clover**



The DeFi ecosystem

Beyond L1: outline of the presentation

- For many, the most important and disruptive part of DeFi ecosystem, is **decentralized lending and borrowing**. We will examine how the sector evolved and what kind of services are offered in the next section.
- Then, we will look at **decentralized exchanges (DEXs)**, which have recently become very popular, attracting volumes similar to the biggest centralized exchanges (CEXs).
- We will then move to discuss another revolutionary component of DeFi ecosystem, namely **decentralized autonomous organizations (DAOs)**, focusing particularly on their role as autonomous asset management protocols in DeFi.
- Another important pillar DeFi ecosystem are **stable-coins**. We will focus on their usage in the DeFi ecosystem, especially for **crypto-backed** & **algorithmic stable-coins**.
- Next, we will see how **oracles** are used for connecting real-time data with blockchains to allow DeFi applications to algorithmically communicate with the outside (to the blockchain) world.
- Then we will briefly re-discuss **wallets** and their importance for connecting the whole ecosystem together.

Session 12: Decentralized Finance

3. Lending & Borrowing

Decentralized Lending/Borrowing

Disintermediating commercial banking

- Lending & Borrowing were the first DeFi applications that gained popularity.
- Decentralized lending and borrowing platforms are simply **smart contracts that let you lend or borrow crypto assets at a fixed or variable interest rate**.
  - In other words, they offer exactly what commercial banks offer through deposits and loans.
  - What differs here is that **there is no central authority** to decide who participates and mediate the whole lifecycle of lending and borrowing.
  - There is no need for credit history or other financial records.
  - Anyone can lend their assets and earn interest or deposit some collateral and borrow a percentage of its value.
- Removing the intermediaries is aimed at enhancing the efficiency of capital allocation, cutting costs, eliminating exclusion and increasing economic privacy and freedom.

Decentralized Lending/Borrowing

DeFi vs TradFi

Feature	DeFi	TradFi
Creditor	Anyone including smart contracts	Banks or appointed institutions
Debtor	Anyone including smart contracts	Vetted individuals or businesses
Interest rate	Set algorithmically by the protocol	Set by central bank, financial institutions, and lenders
Collateral	Overcollateralized	Undercollateralized or unsecured debt
Maturity	Fixed or Undefined	Fixed
Risk to lender	Platform risk, protocol risk, volatility, governance risk, rug pulls	Based on the credit rating of the borrower (default risk)
Risk to borrower	Liquidation/loss of collateral	Bankruptcy, loss of financial flexibility

Decentralized Lending/Borrowing

Over-collateralized loans

- DeFi loans are typically **over-collateralized**, meaning that practically a user can borrow less money than the value of the collateral they deposit.
  - This decreases the likelihood of insolvency that would result in **forced liquidation** of a user's position by the smart contract managing the loan.
- One might naturally ask: why would someone want to borrow money (and pay interest), when the value of the loan is less than the collateral they already possess and lock?
  - The answer is that borrowers post as collateral assets whose value varies.
  - If someone possesses an asset, the value of which they believe would appreciate in the future, but, at the same time, need liquidity, there is a rational incentive to deposit the asset as collateral and borrow part of its value.
  - In this way, if the prediction is correct, the user receives liquidity, while continuing to capture the increase of the locked asset's value. They can even use that liquidity to buy more of the provided asset for multiplicative returns.
  - However, if the prediction is incorrect and the value of the collateral decreases, the DeFi lending protocol will start liquidating part of the collateral, as it approaches the value of the loan, in order to repay it or maintain an acceptable loan-to-collateral ratio.

Decentralized Lending/Borrowing

Using DeFi for leverage

- To demonstrate why someone may be willing to borrow even if their collateral is worth more than the loan, consider the following scenario (assuming no interest, transaction costs, or slippage):
  - Suppose that I deposit my 1 ETH ($1,500) as loan collateral to platform X, with a collateral to loan ratio of 150%.
  - I will be able to borrow up to $1,000 worth of DAI (stablecoin).
  - I then proceed to swap my $1,000 DAI for 0.666 ETH at current prices ($1,500).
  - I now own 1,666 ETH ($2,500), of which 1 ETH is loan collateral and 0.666 in my wallet.
  - If the price of ETH were to increase by 10% the total value of my holdings would be 1.666 ETH = $2,750.
  - **My profit is $250, meaning $100 more than if I simply held my 1 ETH**
  - If the price of ETH decreased by 10%, I would lose $250, instead if $100 (In reality, my losses would be higher since my collateral would be liquidated due to the price change)
- I have effectively used **leverage to multiply my potential profits (and losses)**
  - Leverage is the use of debt to amplify returns (and losses) from an investment.
  - I can even redeposit my ETH, to borrow more DAI and swap it for ETH to increase my leverage and profit (losses).
  - The money Lego nature of DeFi even allows other dApps that do this automatically for me.

Decentralized Lending/Borrowing

Other reasons for DeFi Lending/Borrowing

- You can calculate the potential profit or loss with the following equation

$$Total\ Potential\ Profit/Loss\ = \left\{\left[Collateral\,Value + \left(\frac{Collateral\ Value}{Collateral\ to\ Loan\ Ratio}\right)\right] \times \%Change\ of\ Collateral\,Value\right\} - fees + interest$$

- In the above, note that if the value drops below what is allowed by the collateral to loan ratio, the position is liquidated.
- Besides leverage there are other reasons for lending/borrowing in DeFi
  - Lenders and borrowers maintain exposure to the funds they lend or use as collateral
  - Lenders receive interest on the funds they lend according to the supply APY
  - Lenders and borrowers receive additional rewards in the form of governance tokens that can be sold in the market
  - Depending on the jurisdiction, through lending/borrowing users might avoid or delay paying capital gains taxes

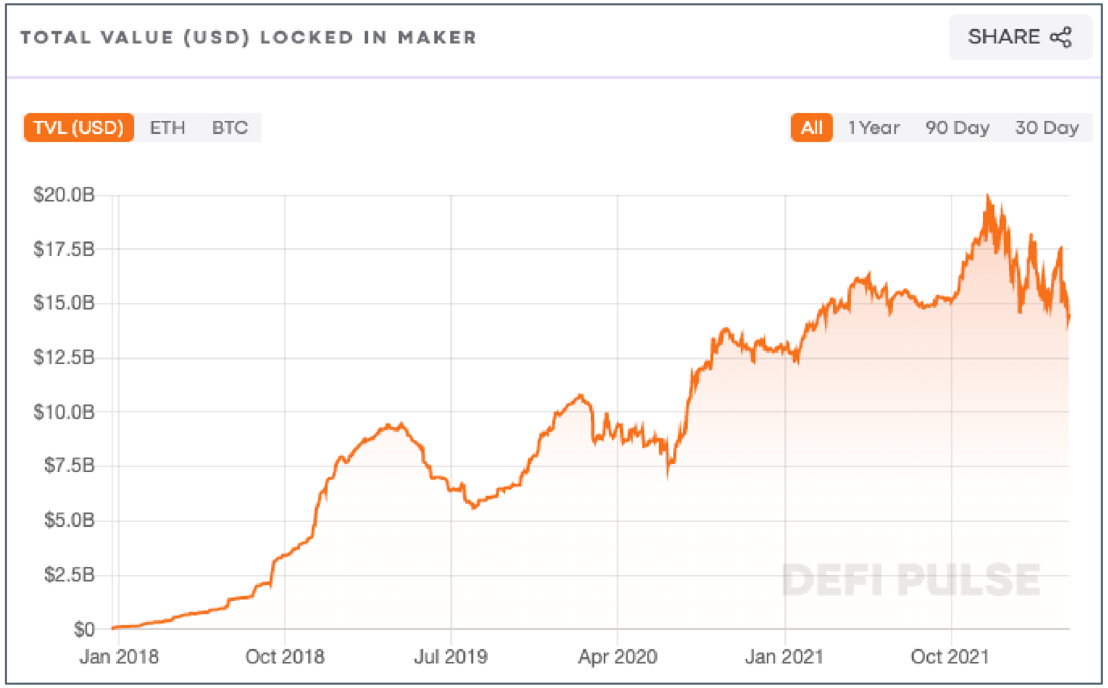
Decentralized Lending/Borrowing

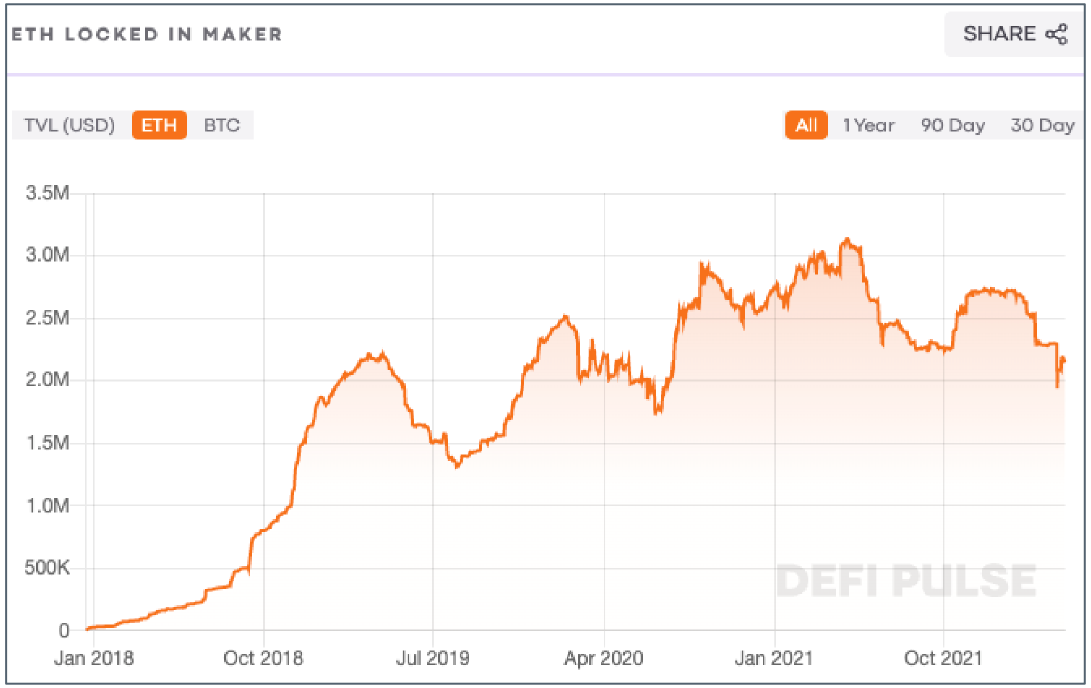
Main platforms: Maker

- The first DeFi lending/borrowing platform in the market was **Maker**, a protocol that initially allowed users to deposit ETH and receive 50% of its value as loan denominated in an algorithmic stablecoin called **DAI**, which was issued accordingly after a user deposited the ETH collateral.
  - DAI's circulating supply is algorithmically regulated based on the overall value of locked collaterals, the demand for loans and their repayment.
  - Nowadays, Maker has evolved to offer a variety of assets to deposit as collateral, beyond ETH.
  - It is also governed in a decentralized way (see DAOs section).
  - Its TVL in July 2021 is around $6 bn.

Decentralized Lending/Borrowing

Maker TVL





Decentralized Lending/Borrowing

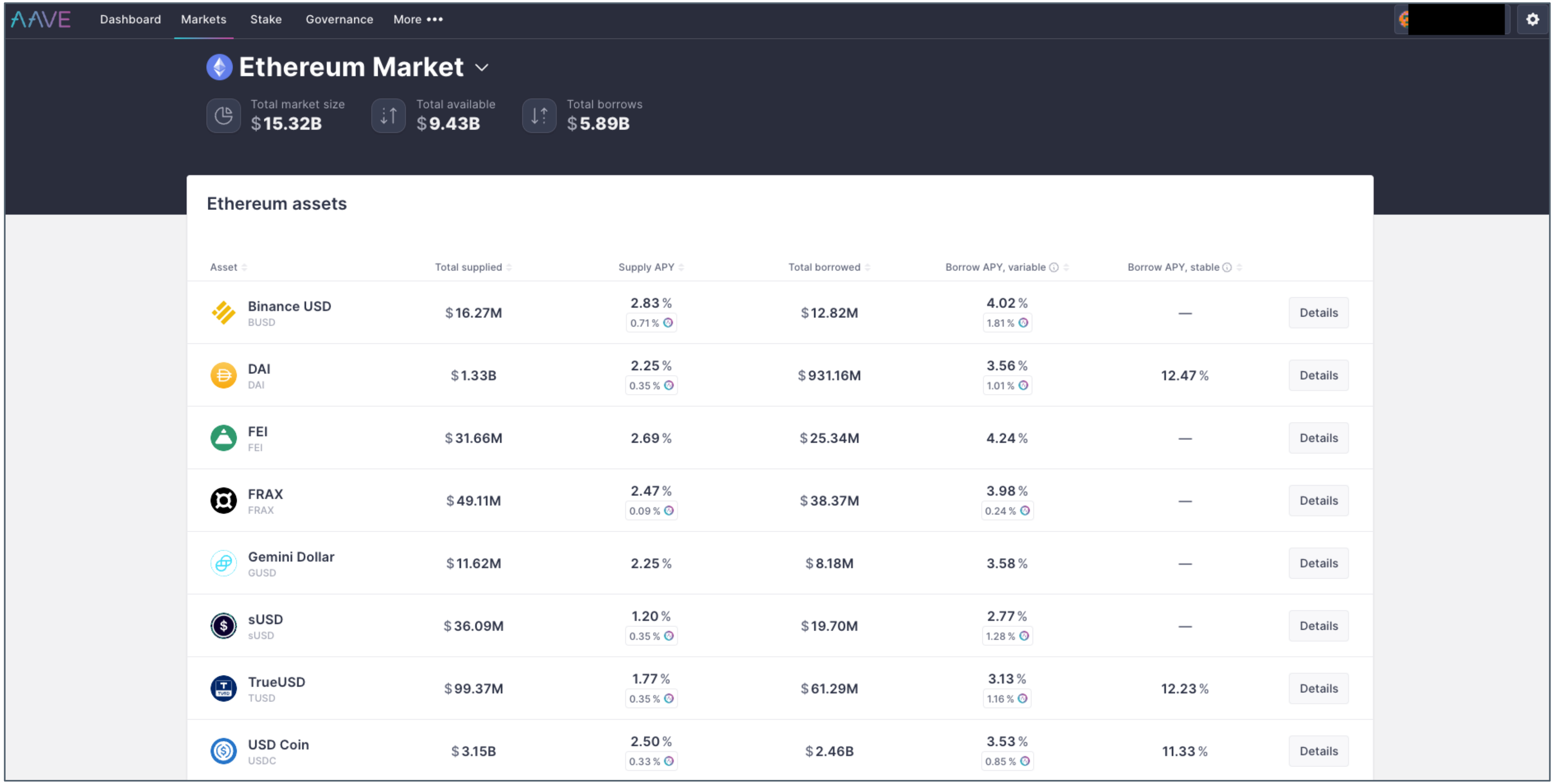
Main platforms: Aave

○ **Aave**, the other important project of the space, begun as **EthLend** during the ICO era in 2017.

- AAVE started as a peer-to-peer platform, meaning that a user who wanted a loan had to find another user to take the other side of the loan and mutually agree on the specific terms.
- That was an inefficient model, and the resulting use of the platform was limited.
- Success came after the shift to a model of a **pool of funds**. Users then were interacting with a smart contract and not with other users directly. Funds from lenders were gathered into a common pool, which had specific and predetermined rules. Borrowers under this model had immediate access to loans, provided that the pool had enough liquidity.
- AAVE also were the first to introduce the revolutionary idea of **flash loans**, were someone can borrow funds with zero collateral, under specific circumstances and for a limited amount of time.
- AAVE was originally deployed on Ethereum but has recently also launched on **Polygon** as well.
- Its TVL in April 2021 is around $9 bn.

Decentralized Lending/Borrowing

Aave front-end



[redacted]

Ethereum Market

Total market size $15.32B

Total available $9.43B

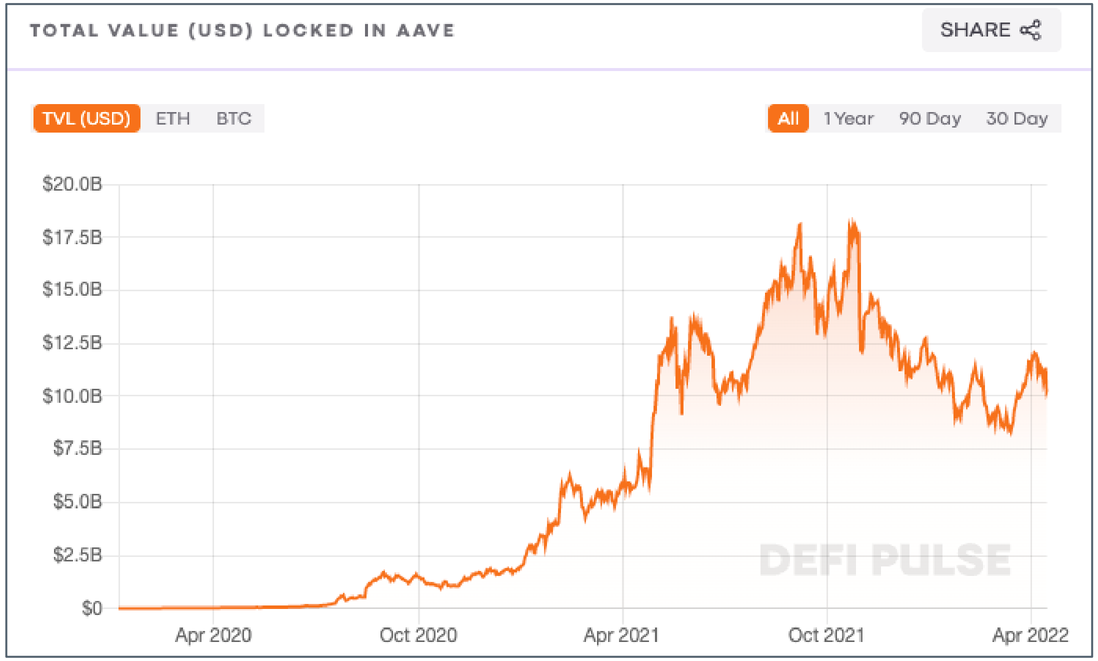
Total borrows $5.89B

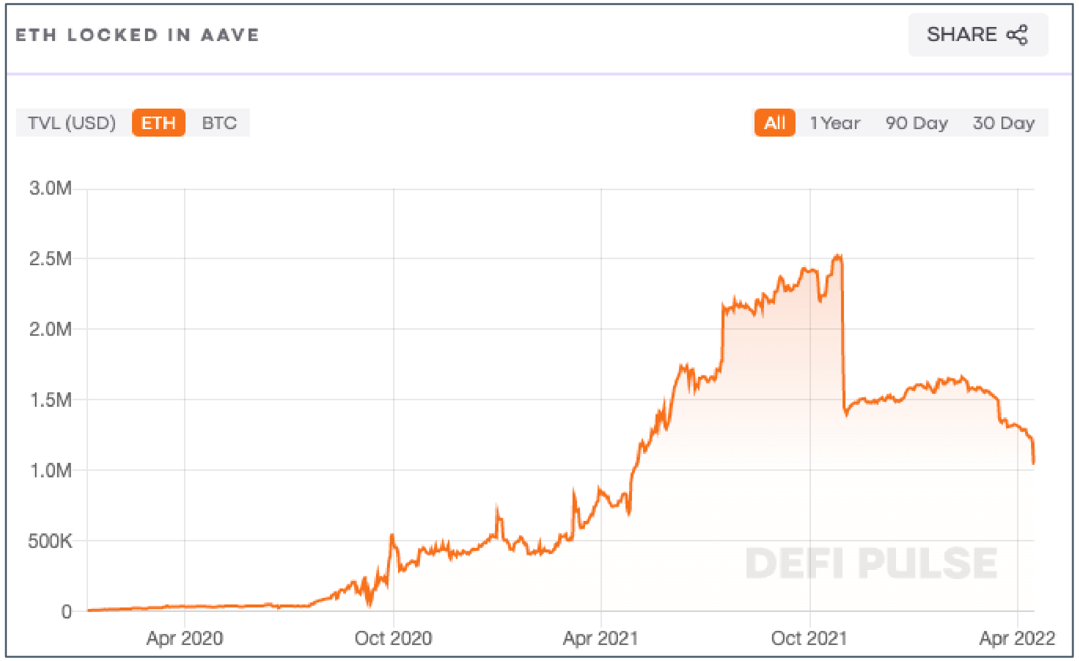
Ethereum assets

Asset	Total supplied	Supply APY	Total borrowed	Borrow APY, variable	Borrow APY, stable	
Binance USD BUSD	$16.27M	2.83 % 0.71 %	$12.82M	4.02 % 1.81 %	—	Details
DAI DAI	$1.33B	2.25 % 0.35 %	$931.16M	3.56 % 1.01 %	12.47 %	Details
FEI FEI	$31.66M	2.69 %	$25.34M	4.24 %	—	Details
FRAX FRAX	$49.11M	2.47 % 0.09 %	$38.37M	3.98 % 0.24 %	—	Details
Gemini Dollar GUSD	$11.62M	2.25 %	$8.18M	3.58 %	—	Details
sUSD sUSD	$36.09M	1.20 % 0.35 %	$19.70M	2.77 % 1.28 %	—	Details
TrueUSD TUSD	$99.37M	1.77 % 0.35 %	$61.29M	3.13 % 1.16 %	12.23 %	Details
USD Coin USDC	$3.15B	2.50 % 0.33 %	$2.46B	3.53 % 0.85 %	11.33 %	Details

Decentralized Lending/Borrowing

Aave TVL





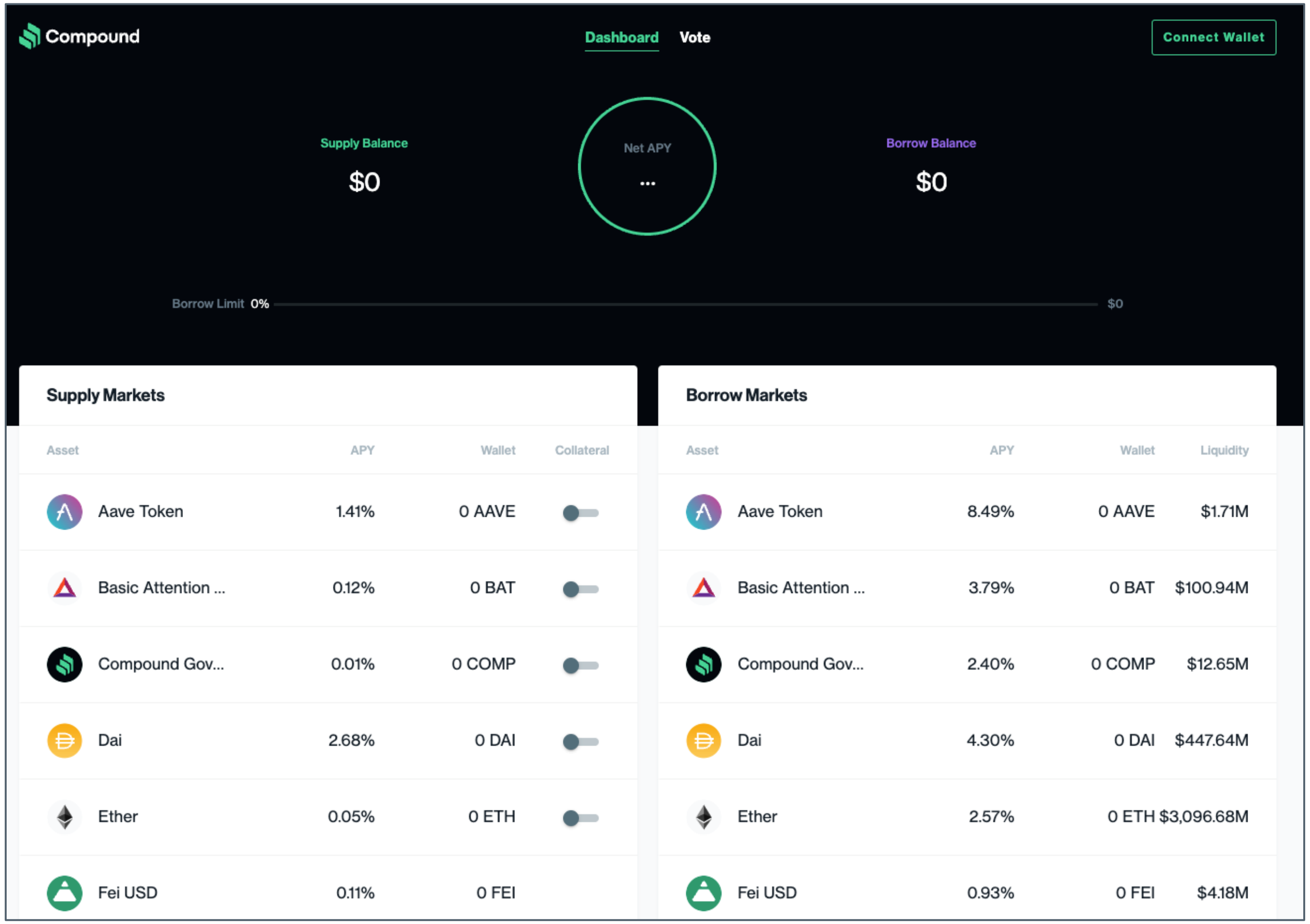
Decentralized Lending/Borrowing

Main platforms: Compound

- **Compound** is another large lending/borrowing project that has also introduced some innovative concepts, which helped the whole DeFi lending space to evolve.
  - The **liquidity mining** mechanism that Compound implemented is a mechanism that was later copied and extended by many other projects and attracted many users to DeFi lending.
  - The mechanism introduced extra incentives to lenders and borrowers to use their platform, in the form of distributing the platform’s native **COMP token** to the users.
  - That led to the creation of the notion of **yield farming**, which describes the situation of users being incentivized to switch back and forth between lending and borrowing, among different tokens, in order to achieve the best yield possible.
  - Compound has today the largest TVL among DeFi lending protocols, above $10 bn.

Decentralized Lending/Borrowing

Compound front-end



Compound

Dashboard Vote

Connect Wallet

Supply Balance

$0

Net APY

...

Borrow Balance

$0

Borrow Limit 0% $0

Supply Markets

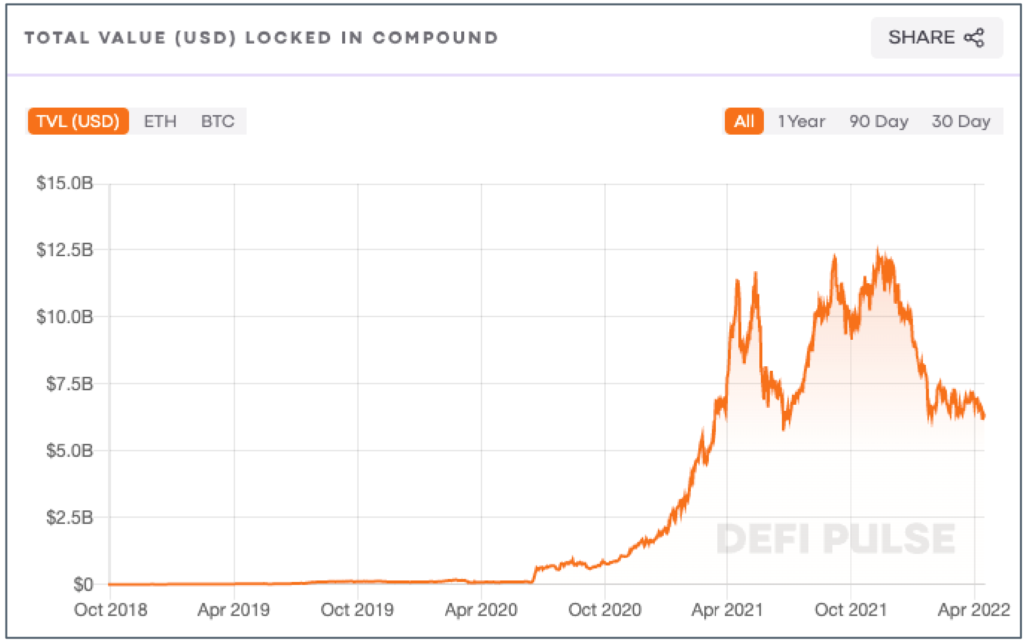
Asset	APY	Wallet	Collateral
Aave Token	1.41%	0 AAVE	○
Basic Attention ...	0.12%	0 BAT	○
Compound Gov...	0.01%	0 COMP	○
Dai	2.68%	0 DAI	○
Ether	0.05%	0 ETH	○
Fei USD	0.11%	0 FEI	

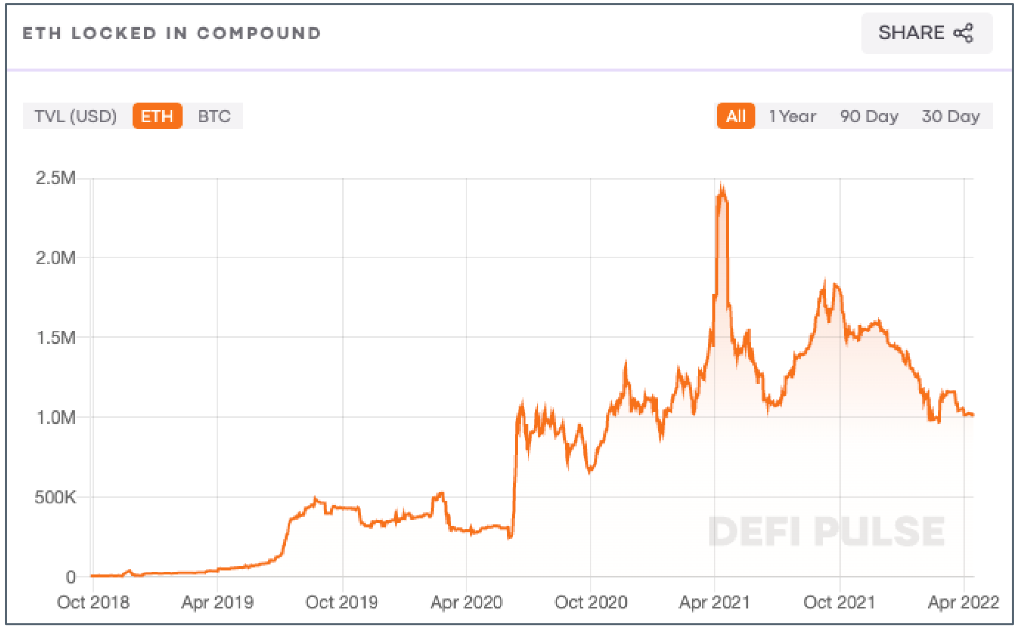
Borrow Markets

Asset	APY	Wallet	Liquidity
Aave Token	8.49%	0 AAVE	$1.71M
Basic Attention ...	3.79%	0 BAT	$100.94M
Compound Gov...	2.40%	0 COMP	$12.65M
Dai	4.30%	0 DAI	$447.64M
Ether	2.57%	0 ETH	$3,096.68M
Fei USD	0.93%	0 FEI	$4.18M

Decentralized Lending/Borrowing

Compound TVL





Session 12: Decentralized Finance

4. Decentralized Exchanges (DEXs)

Decentralized Exchanges

Definitions: DEXs and AMMs

What is a Decentralized Exchange?

- A **Decentralized Exchange (DEX)** is a decentralized application, based on smart contracts, enabling its users to perform peer-to-peer token swaps without the intervention of a third party.
- The main innovation and difference of DEXs compared to CEXs (like Coinbase or Binance*) is allowing users to trade directly from their wallets, without having to trust an exchange for the custody of their funds ("your keys, your money").
    - In other words, users have full control of their funds and privacy in their transactions (no KYC is required).

What is an Automated Market Maker?

- An **Automated Market Maker (AMM)** is a special type of DEX: AMMs are algorithmic agents that provide liquidity in markets, through holding reserves of a token pair.
    - In contrast with the order book model typically used in CEXs, in an AMM model, funds are reserved in **Liquidity Pools (LP)** and the exchange rate between tokens is determined algorithmically.
    - Most DeFi DEXs today follow the AMM model.

* Although Binance have launched a DEX too

Decentralized Exchanges

Definitions: Liquidity pools

What are Liquidity Pools (LPs)?

- LPs are one of the most foundational mechanisms in the current DeFi ecosystem.
  - They are an essential part of AMMs, lending/borrowing platforms, yield farming, synthetic assets, on-chain insurance, etc.
- A liquidity pool is simply **a collection of funds which are locked in a smart contract**.
  - They are used to facilitate decentralized trading, lending, and many more functions in the DeFi ecosystem.
- **Bancor** was the first protocol that utilized the mechanism of LPs, but the concept became really popular when it was introduced by **Uniswap**.
  - Today, the vast majority of DEXs function under the LP model, with very few using the order book model.
  - Other popular DEXs (AMMs) that use LPs are **Sushiswap**, **Pancakeswap**, **Curve** and **Balancer**.

Decentralized Exchanges

Definitions: Aggregators

What is a DEX Aggregator?

- Aggregators are ‘friendly’ **protocols build on top of DEXs to provide users with deeper liquidity**.
- Aggregators, as their name suggest, search liquidity pools across different DEXs to provide a user with the best possible price for a particular trading pair.
- Aggregators retain all the advantages that DEXs offer to users, such as privacy and full control of funds, and they typically also offer better execution prices for a token swap.
- However, due to the fact that through an aggregator you may transact with more than one DEXs, transaction fees can be higher.
  - That is why aggregators are typically used for big trades, which may result to a large **price slippage**.

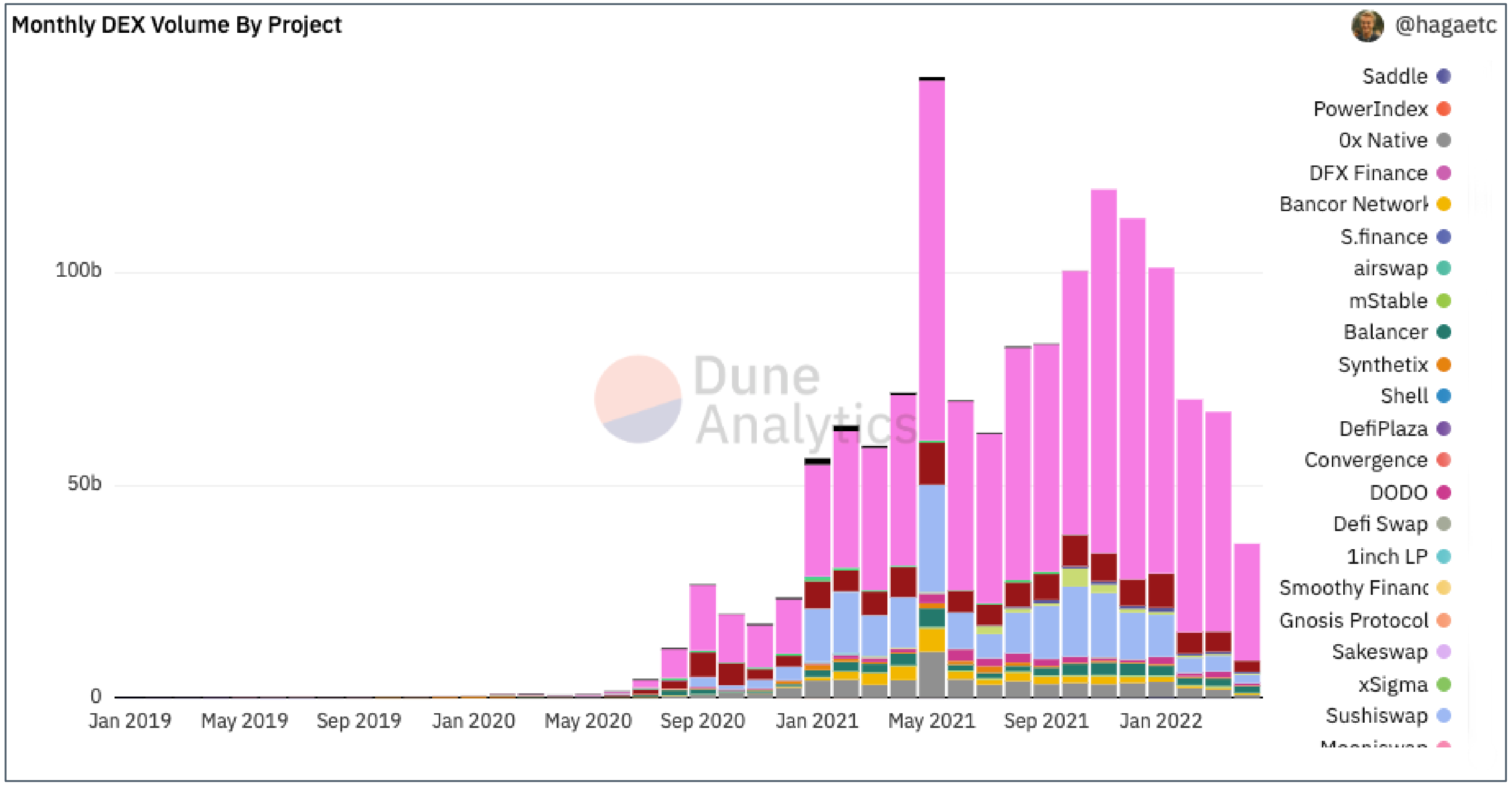
Decentralized Exchanges

Why LPs and AMMs

- DEXs did not really became popular until **Uniswap** implemented the mechanism of LPs and AMMs.
- Until then, DEX trading was similar to centralized ones, i.e with bid/ask order books.
- However, this presented a big problem:
  - Exchanges that use order books are heavily dependent on **Market Makers (MMs)** for liquidity provision.
  - In theory, MMs provide liquidity without affecting the direction of the price. To do so, they may engage in many trades.
  - In CEXs, MMs will typically not pay trading fees for the service they provide. Indeed, they may get paid by the exchange!
  - However, **in DEXs all trades are on-chain**, i.e. using and recorded on the blockchain the DEX is build on (e.g. Ethereum). Users connect their wallets to the smart contract and there is no exchange to regulate fees.
  - So, DEX MMs would have to pay their trading costs (fees), like all market participants.
  - On top of that they would have to wait for the block confirmation time
  - That is **expensive**, **comparatively slow** and created a huge liquidity problem for DEXs **(bad user experience)**.
- This is the problem that LPs solved:
  - Anyone can provide liquidity on a pair traded on a DEX, thus becoming a MM and being rewarded for that.
  - The introduction of LPs led to an explosive adoption of DEXs (see next slide).

Decentralized Exchanges

DEX growth



Decentralized Exchanges

Using a DEX

- To use a DEX, a user must connect a compatible wallet (like **Metamask**) to it.
  - Connecting a wallet to a DEX basically means allowing the DEX smart contract to view the wallet contents (balances) and, depending on the approvals provided by the user, transacting on specific tokens up to specific amounts or without limit.
- DEX interfaces are typically very simple and user-friendly:
  - Users simply choose their trading pair (e.g., ETH/DAI) and set an amount for the token to sell.
  - The DEX will offer an estimated amount for the token to buy, as well as inform the user about the price impact of the trade (next slide).
  - Should the user accept the terms offered (both on the DEX user interface and the wallet), the transaction is submitted to the L1 blockchain. The trade is executed when the transaction is confirmed on-chain.
  - Users can also set their own desirable values regarding price slippage and transaction fees (or simply let the values of the DEX's default settings).
- High transactions fees constitute, at the moment, the biggest disadvantage of DEXs, especially those using Ethereum as their underlying L1 protocol.

Decentralized Exchanges

How DEXes (AMMs) work (assuming no fees, slippage, etc.)

- Most DEXes use various formulas to determine prices. The most popular is the **constant product formula:**

$$\boxed{\begin{array}{c} k = x \times y \\ where\ k = constant,\ and\ x,\ y\ the\ amount\ of\ supplied\ tokens \end{array}}$$

  - The first Liquidity Provider (LP) sets the initial exchange rate of assets in the Liquidity Pool.
  - LPs are incentivized to provide an equal value of tokens (otherwise they will lose money by arbitrageurs).
  - Suppose that the LP provides 10 Ethereum, with market value of $1,500 and 15,000 DAI:

$$\boxed{k = 10 \times 15,000 = 150,000\ (constant)}$$

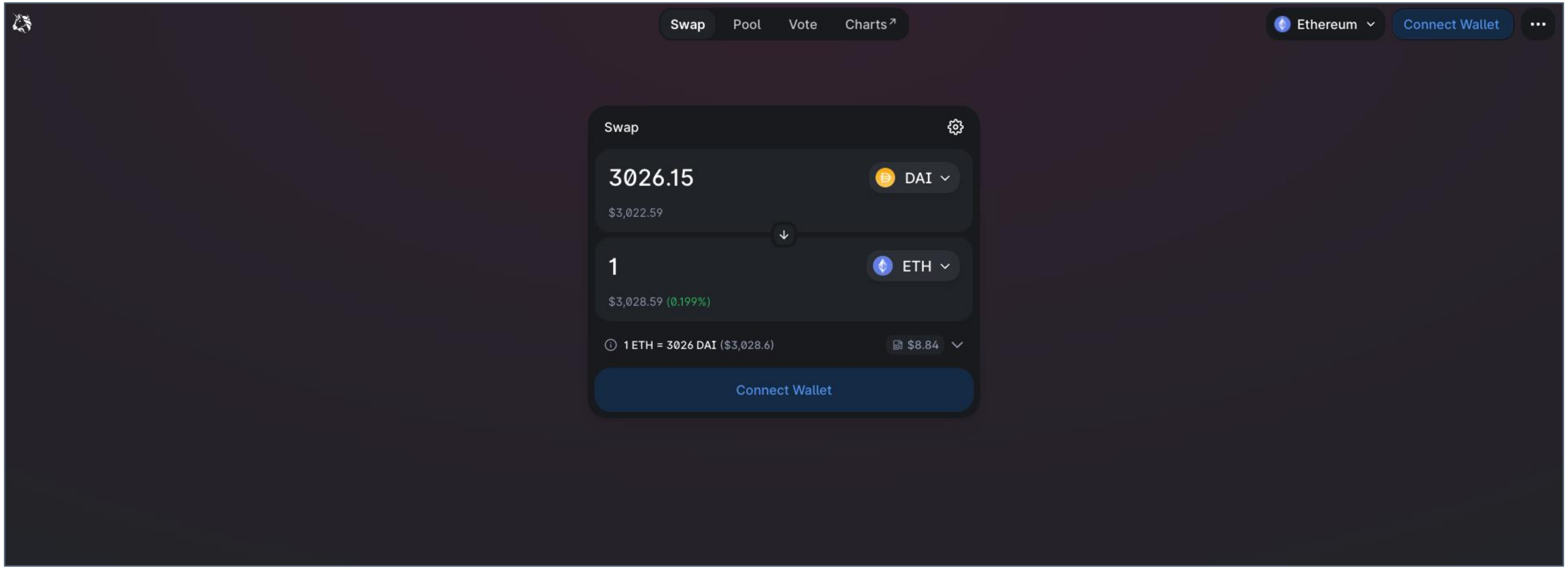
- Now imagine that you wanted to trade DAI for 2 ETH. How much DAI would you have to pay?
  - You would take away 2 ETH from the pool and have to provide a proportionate amount of DAI

$$\boxed{(10-2) \times (15,000 + z) = 150,000 \Rightarrow 15,000 + z = \frac{150,000}{8} \Rightarrow 15,000 + z = 18,750 \Rightarrow z = 3,750}$$

  - You would have to pay 3,750 DAI for 2 ETH, or **on average** 1,875 DAI per ETH (in reality, the first ETH is cheaper and the second more expensive)
  - Arbitrageurs would then lower the price again by providing ETH to the pool to benefit from the difference

Decentralized Exchanges

Example: token swap (DAI to ETH) in Uniswap



3026.15 DAI

$3,022.59

1 ETH

$3,028.59 (0.199%)

1 ETH = 3026 DAI ($3,028.6)

$8.84

Decentralized Exchanges

Impermanent loss

- Impermanent loss is a **temporary loss** caused to a LP due to the **price volatility** of the tokens they provide
  - As AMMs lack order books and centralized parties, they rely on market forces for price discovery.
  - This means that price changes (e.g., on centralized exchanges) are not immediately reflected on AMMs.
  - As a result, there are often price discrepancies between their price on CEXes and AMMs.
  - **Arbitrageurs** discover those discrepancies and execute favorable trades (e.g., by buying low and selling high)
  - LPs suffer **impermanent losses** by being at the receiving end of the arbitrage
  - **Impermanent loss is essentially the difference between providing tokens versus holding them.**
  - The more volatile the tokens, the higher the exposure to impermanent loss.
- Why is the loss temporary, or impermanent?
  - If the price of the staked tokens returns to the original price, the impermanent loss is neutralized
  - If the LP chooses to withdraw their funds, the impermanent loss is realized and becomes permanent.
- Impermanent loss can be mitigated to an extend by supplying less volatile tokens, same-pegged stablecoins, opting for one-sided liquidity pools, and by participating in uneven pools

Decentralized Exchanges

Impermanent loss example

- Consider the example of a previous slide where a LP has provided 10 ETH and 15,000 DAI to a Pool

Token	Amount	Price/Unit	Total Value
ETH	10	$1,500	$30,000
DAI	15,000	$1	

  - Suppose that the price of ETH **increases** from $1,500 to $1,600 per unit. This would incentivize arbitrageurs to buy the “cheaper” ETH in the pool until it there is no price discrepancy.
  - They will be able to buy ~ 0.32 ETH in exchange for ~496 DAI before the price of ETH in the pool reaches $1,600 and is at equilibrium with the market. (we calculate this by using the constant product formula k=x*y)

- The LP would still realize profits but not as much as if they simply held the tokens:

If supplied to pool

Token	Amount	Price/Unit	Total Value
ETH	9.68	$1,600	$30,984
DAI	15,496	$1	

If held

Token	Amount	Price/Unit	Total Value
ETH	10	$1,600	$31,000
DAI	15,000	$1	

Decentralized Exchanges

Impermanent loss continued

- If impermanent loss makes supplying assets to a liquidity pool is less profitable that holding, then one might wonder: why even become a LP?
  - The answers is that AMMs compensate LPs in various ways for the services they provide.
  - AMMs charge a (small) swapping fee for their services. Uniswap's swapping fee is 0.3%, applicable to all trades.
  - They then use those fees to reward LPs
  - Once a LP withdraws their provided funds, they receive an amount of fees proportional to their share of the liquidity pool and to the time that they provided liquidity.
- In addition to fees, AMMs reward their LPs in other ways too:
  - Some AMMs reward their LPs with governance tokens.
  - Governance tokens are used for voting on proposals that determine the future of the AMM.
  - Governance tokens can also be sold in the market.
  - Some LPs might even provide those tokens as liquidity for additional rewards from fees.
  - Finally, LPs are usually targeted with Airdrops from competing dApps.

Session 12: Decentralized Finance

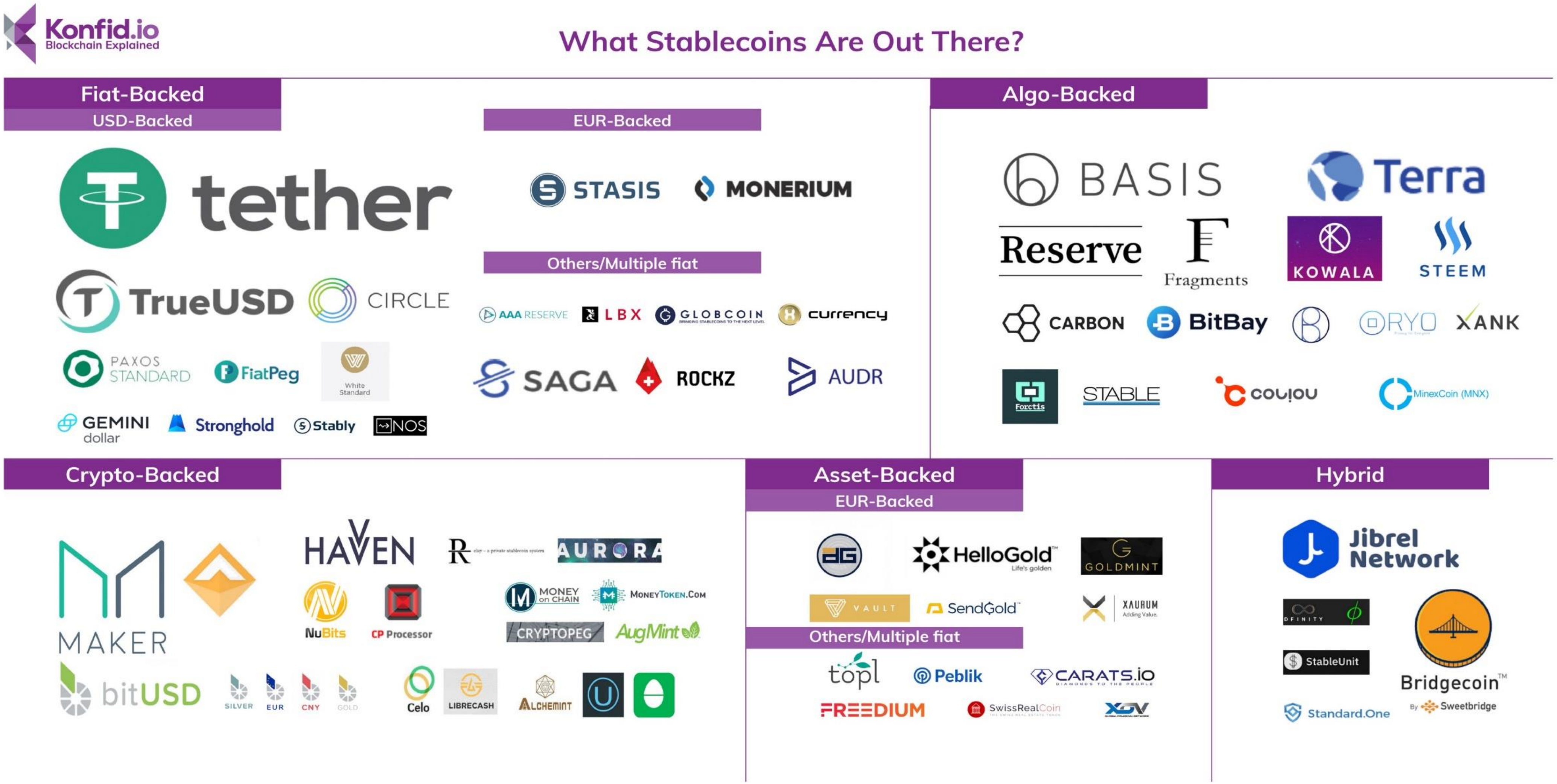
5. Stablecoins

Stablecoins

Types of stablecoins

- We have discussed stablecoins in general in previous sessions.
  - Remember that stablecoins are cryptocurrency tokens that are meant to hold a stable value against (being pegged to) another asset, like the US dollar.
  - Stablecoins are an important pillar for the whole crypto space and, of course, for the DeFi Ecosystem.
- There are many different types of stable-coins, based on the way they maintain their value stable to its peg:
  - **Fiat-backed** stablecoins are collateralized by fiat currencies (e.g. USDT). For every newly minted stablecoin, there should be the corresponding amount of fiat currency in safe custody.
  - **Crypto-backed** stablecoins (e.g. DAI) are collateralized by a cryptocurrency or a basket of cryptocurrencies.
  - **Asset-backed** stablecoins are collateralized by a single or multiple real-world assets, other than fiat currencies, e.g. gold.
  - **Algorithmic** stablecoins use algorithmic strategies to achieve price stability; they are generally not fully backed by any asset.

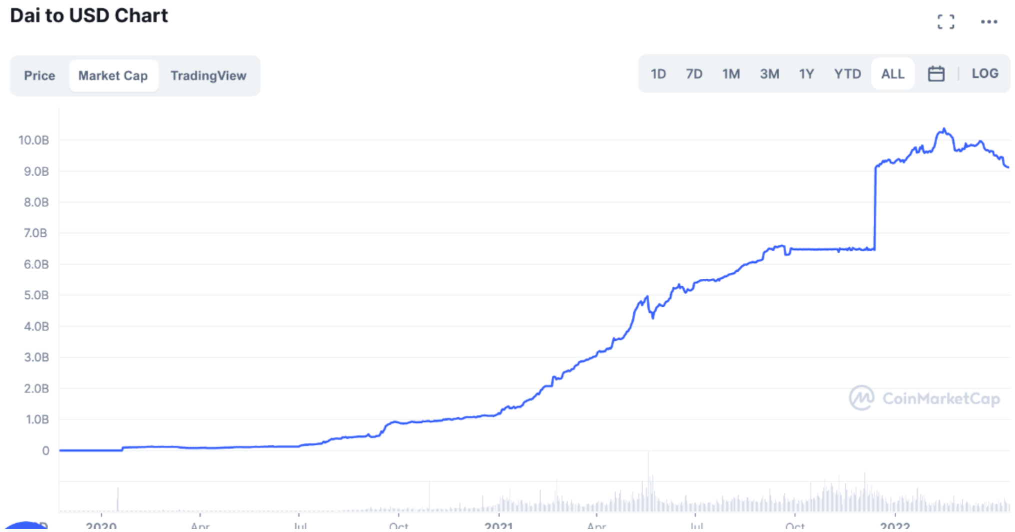
The stablecoin universe



Stablecoins

Stablecoins for DeFi

- Stablecoins are used for many purposes in the DeFi ecosystem: store of value, trading, loans.
    - Interestingly, **the vast majority of DeFi loans are taken in stablecoins**.
    - A characteristic example is DAI, the stablecoin of the MAKER ecosystem, the market cap of which represents the value of outstanding loans in the MAKER's ecosystem.
    - DAI is a crypto-backed stablecoin, that is minted every time someone deposits a crypto asset as a collateral to take a loan. When the loan is repaid, the corresponding DAI are burned.



Stablecoins

Algorithmic stablecoins

- Algorithmic stablecoins (otherwise known as **non-collateralized stablecoins**) are the newest category of stablecoins.
    - They are generally not backed by an asset, at least not fully.
    - Instead, they depend on algorithms and smart contracts to control the supply of issued token.
- Their financial power does not rely on a central entity or unaudited back-up but on a formula balancing demand and supply to maintain a stable price for the token.
    - An algorithmic stablecoin will reduce the token supply if its price remains under the price of the fiat currency it represents (for example, USD).
    - Conversely, if its price exceeds the fiat one, additional tokens will be issued until price decreases to be equal to the fiat's price.
- Philosophically, the monetary policy of such stablecoins resembles the mechanism of how central banks (should) control their national currencies.

Session 12: Decentralized Finance

6. Oracles

Oracles

Connecting smart contracts to the outside world

- There are many cases, where a smart contract needs data from the real world to function properly.
  - For instance, in decentralized prediction markets, in order for a market to be settled and the winners to be paid, the outcome of the relevant real world event needs to be determined.
- The problem is that blockchains and smart contracts cannot (directly) access data outside of the network in a trusted way.
- **Oracles act as intermediates between blockchains and the real world**, by feeding real world data, relevant to a contractual agreement, into a smart contract.
  - This information triggers state changes on the blockchain and smart contracts are able to function properly.
- The main challenge blockchains face with oracles is that they need to trust the outside sources of information.
  - Such information comes from centralized parties like websites, sensors, etc.
  - Oracles usually take feed from multiple external resources to minimize risks and avoid a central point of failure.

Oracles

Types of oracles

There are two main types of blockchain oracles, depending on the way that they allow blockchains to interact with the real world:

- **Inbound oracles** provide data from the external world to blockchains and smart contracts.
- **Outbound oracles** provide smart contracts with the ability to send data to the outside world.

Depending on their implementation, we can distinguish oracles into:

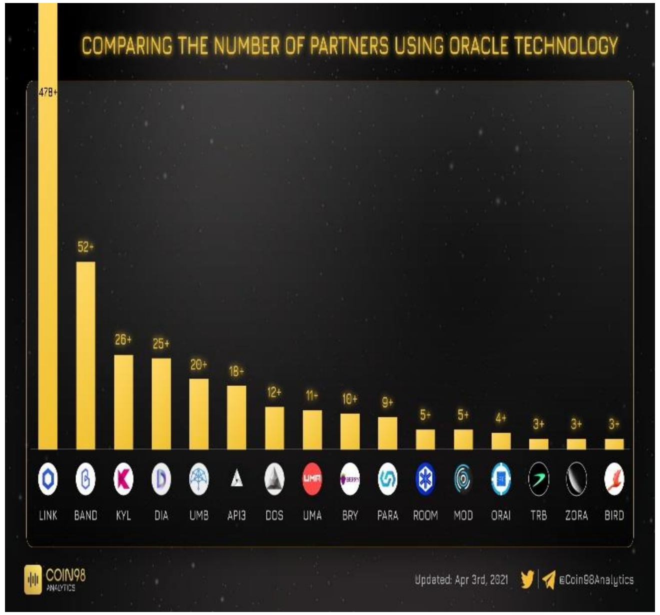
- **Software oracles** that handle information data coming from the Internet (e.g. asset prices from websites).
- **Hardware oracles** used when smart contracts need information directly from the physical world, e.g. IoT sensors.
- **Consensus-based oracles** that get their data from human consensus. For example, to avoid market manipulation, prediction markets implement a rating system where different users vote on the outcome in question and their weighted-by-rating average is transmitting to the enquiring smart contract.

Oracles

Example: Chainlink

The most widely used blockchain oracle in the DeFi ecosystem is **Chainlink**.

- As it can seen from the chart below (on the left), it has by far the largest number of blockchain partners using it (example DeFi projects using it on the right).



AAVE

SYNTHETIX

celsius

kyber network

yearn.finance

δY/δX

Ampleforth

Nexus Mutual

ARBOL

crypto.com

Session 12: Decentralized Finance

7. Wallets

Wallets

Crypto wallets for DeFi

- DeFi wallets can be used as regular wallets, but also allowing us to interact with the DeFi ecosystem.
  - That being said, DeFi wallets are a crucial part of the whole DeFi ecosystem because, without them, it would be impossible for users to interact with the DeFi ecosystem.
  - They act as the gateways for interacting securely with DeFi applications and, at the same time, they are **non-custodial**, which means that users can store their assets without having to depend on third-parties.
- DeFi wallets have to be compatible with the token standards set by the L1 blockchain of a DeFi ecosystem and should be able to support a wide range tokens, e.g. be compatible with ERC-20 standard in Ethereum's network.
  - In practice, many DeFi wallets will support more standards (e.g. ERC20 and ERC721 for non-fungible tokens) or even multiple L1's (e.g. Ethereum and Binance Smart Chain).
  - Many wallets have also evolved to have their own built-in exchanges (**Trust Wallet**) or act as DEX aggregators (**Metamask**).
- Most of them are desktop & mobile wallets or just browser extensions, but hardware wallets can also be used/connected to DeFi applications.

Wallets

DeFi wallet characteristics

Core characteristics good DeFi wallets should have include:

- **Non-Custodial**: No third party should have any kind of access/control on user funds, except for explicitly provided functions.
- **Multi-asset**: Anyone should be able to access DeFi wallets and they should be able to handle a suit of assets.
  - For instance, DeFi wallets compatible with Ethereum's blockchain should handle at least ETH, ERC20 and ERC721 tokens.
- **Compatible**: They should be compatible with any kind of DeFi application, so that the same wallet can be used across applications.

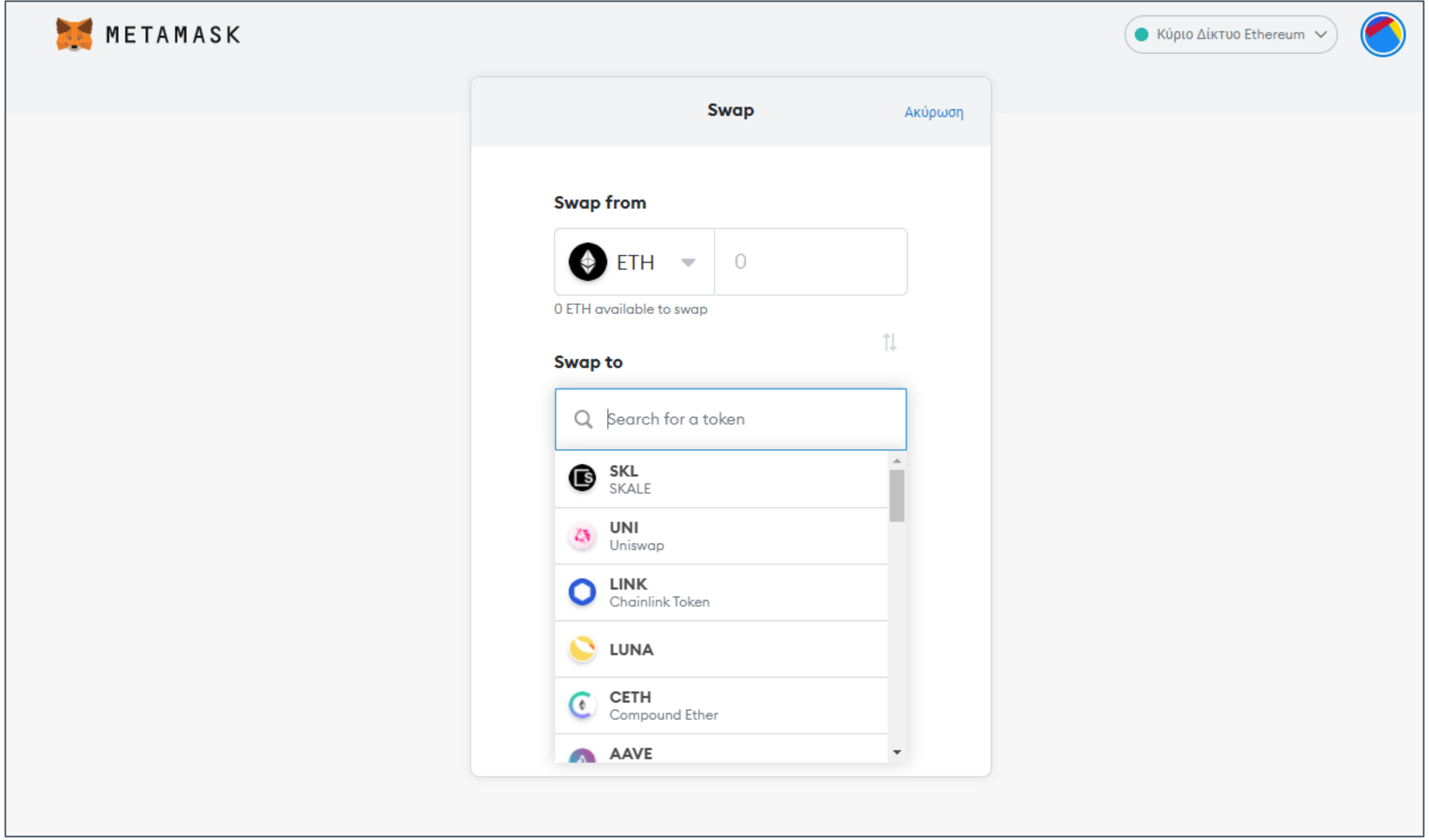
Wallets

Example: Metamask

- The most widely used wallet in the DeFi ecosystem today is the MetaMask browser extension.
  - It is compatible with both Ethereum's network and Binance Smart Chain, the two largest DeFi ecosystems at the moment.
- Metamask uses a 12-world passphrase, which can be used to access the wallet from any device (or restore it, in case it is lost).
- While it is very easy to use, we should note that it has not been designed with security as its prime concern (as for all web wallets).
- Metamask can be used to access the DeFi ecosystem directly, from swapping between tokens with a simple click to accessing farming, staking, prediction markets and loans.
  - Connecting with all these activities is again really simple. Every time you access a site/platform/DApp that offers some kind of DeFi activity, a window will pop out asking you to connect your wallet. With two clicks, your Metamask wallet will be connected and ready to interact with the DeFi application of your choice.
  - Remember when you want to interact with a different DeFi ecosystem,s e.g. if you want to switch from Ethereum's network to BSC, you must change the settings on the wallet, otherwise you run the risk of losing funds.

Metamask

Example: Direct swap from wallet



METAMASK

Κύριο Δίκτυο Ethereum

Swap

Ακύρωση

Swap from

ETH 0

0 ETH available to swap

Swap to

Search for a token

SKL
SKALE

UNI
Uniswap

LINK
Chainlink Token

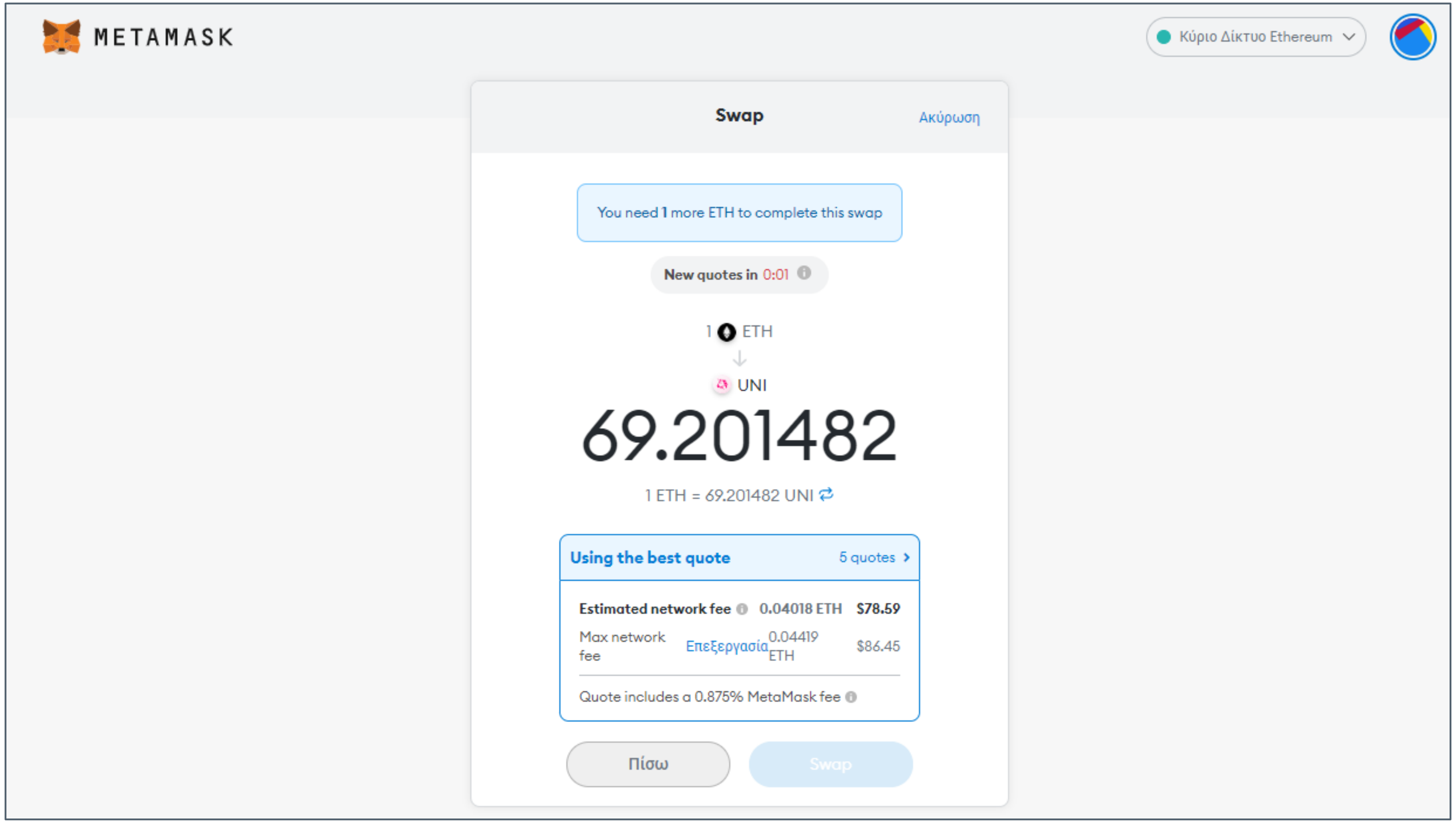
LUNA

CETH
Compound Ether

AAVE

Metamask

Example: Direct swap from wallet (DEX aggregator function)



Swap

You need 1 more ETH to complete this swap

New quotes in 0:01

1 ETH

UNI

69.201482

1 ETH = 69.201482 UNI

Using the best quote

Estimated network fee		0.04018 ETH	$78.59
Max network fee	Επεξεργασία	0.04419 ETH	$86.45

Quote includes a 0.875% MetaMask fee

Session 12: Decentralized Finance

8. Non-fungible tokens (NFTs)

Non-fungible Tokens (NFTs) Introduction

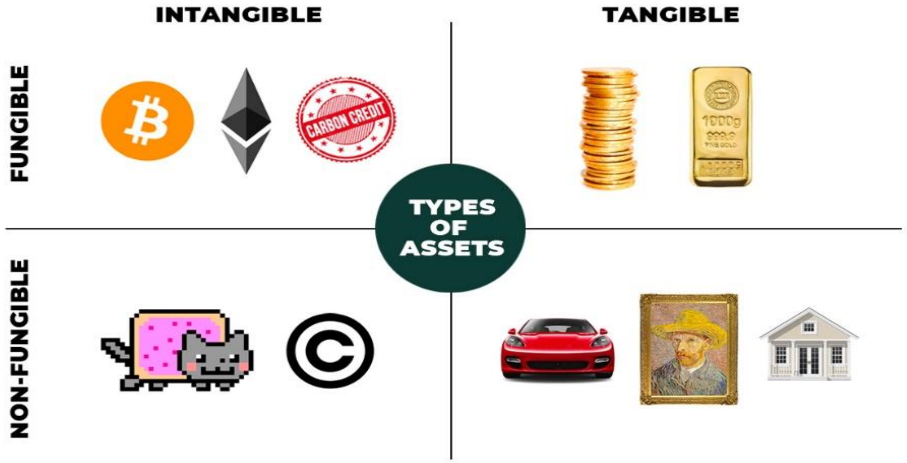
The art of Digitization

- The potential of blockchain technology is not limited to cryptocurrencies
- As we demonstrated in the previous weeks, with tokenization and wrapped tokens, almost everything could be digitized (e.g., art, music, educational certificates, collectibles, event tickets etc.)
  - Jack Dorsey's Genesis Tweet, Grimes' artwork[1]
  - Digital blockchain-verifiable certificates are available (see Block.co)
- Cryptocurrencies work fine as fungible tokens – they are interchangeable (e.g., 1 bitcoin could be exchanged for another 1 bitcoin

Non-fungible Tokens (NFTs): Think of that: Almost everything in the world is unique - they are NOT interchangeable

- Your phone, personal suitcase, house, car, dog …. all are unique
- Non-fungible Tokens (NFTs) are another blockchain-based token type that enable the exchange of ownership of unique digital items - Introduced a new way for proof of ownership

NFTs are presenting the non-fungibility of the world in a programmable way



Source: 1.Cointelegraph, 2. jingculturecommerce.com

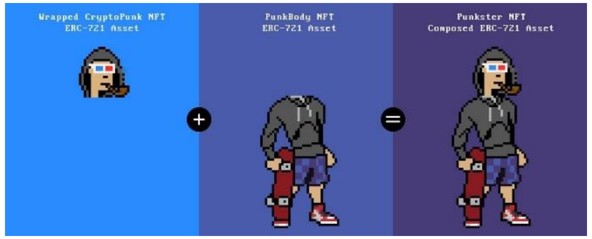
Non-fungible Tokens (NFTs) Introduction (continued)

- NFTs unique attributes:
  - **Indivisibility:** NFTs cannot be split into smaller denominations. E.g., you cannot purchase 10% of a plane ticket
  - **Composability:** Ability of a token to combine different NFTs to represent a combination of digital assets
  - **Scarcity:** NFT creator could generate as many assets as he/she likes and thus to drive their value. E.g., CryptoPunks are 10,000 uniquely generated characters
  - **Uniqueness:** They are not interchangeable. No two NFTs are the same
  - **Ownership:** Creators control the private key of their NFT creations able to transfer them to any account
  - **Transparency:** Records of token issuance, transfer and activity can be publicly verified
  - **Interoperability:** Could be traded, purchased or sold across different DLTs

Scarcity – 10,000 unique CryptoPunks

Source: Larvalabs.com

Composability – Combination of diffent NFTs



Source: metaversal.banklesshq.com

Growth of the NFT market

The NFT Hype

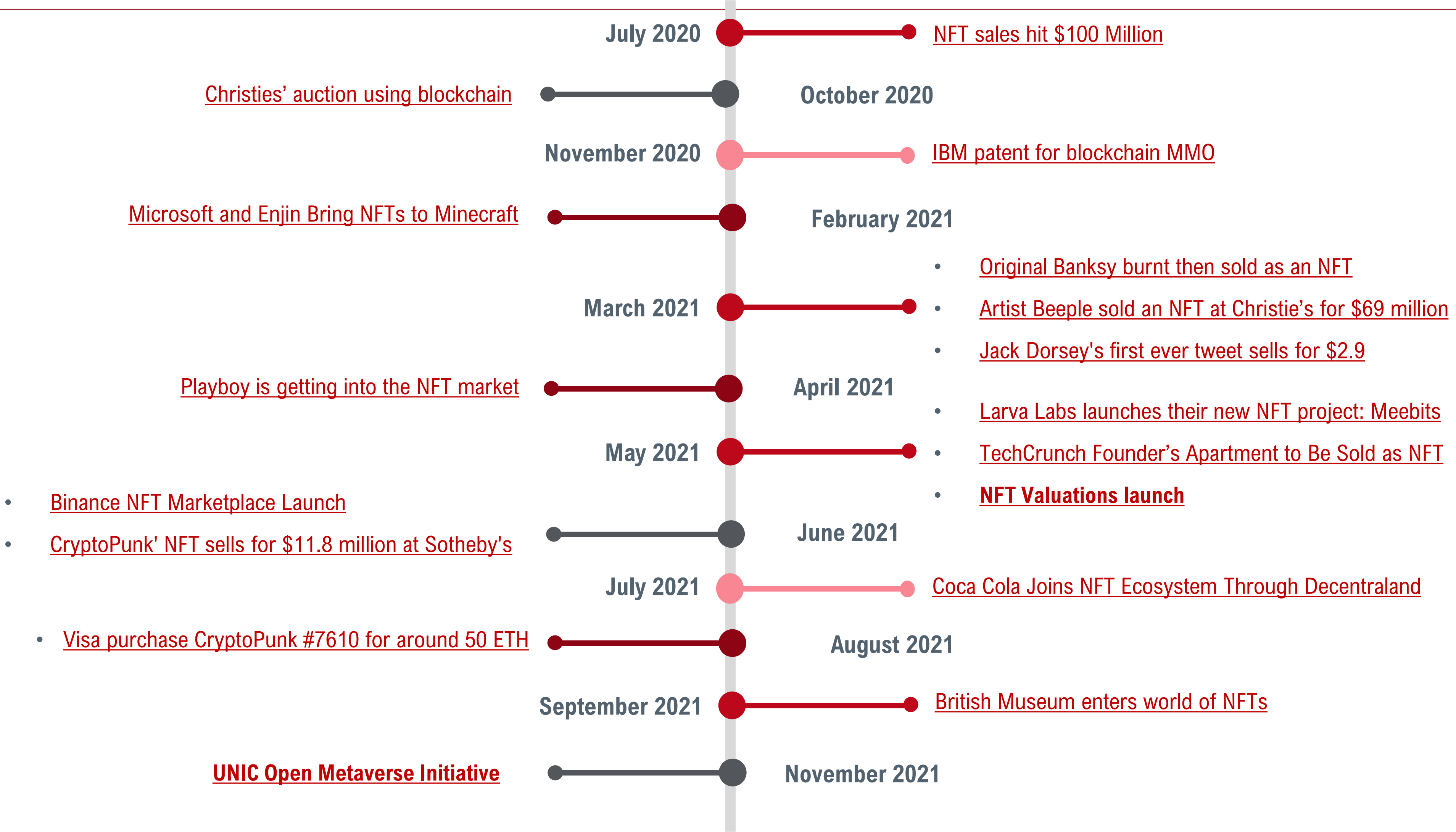
- The NFT market has experienced explosive growth over the past months
- Last year (2020) NFT market traded about $250M, while currently (Q3 of 2021) NFT market trades increased more than **2000%** to $5B
- NFTs are a paradigm of horizontal technology that has the potential to disrupt a number of areas:
  - Art, Tickets, Coupons, Real Estate, Supply Chain

Total volume traded in NFT per year

	2018	2019	2020	2021 (Q3)
USD Traded[1]	$159 142 527	$62 862 687	$250 846 205	$5 915 337 738

Sources: 1. Data collected from nonfungible.com Yearly, Quarterly reports and reuters.com report

The NFT timeline



July 2020 – NFT sales hit $100 Million

October 2020 – Christies' auction using blockchain

November 2020 – IBM patent for blockchain MMO

February 2021 – Microsoft and Enjin Bring NFTs to Minecraft

March 2021
- Original Banksy burnt then sold as an NFT
- Artist Beeple sold an NFT at Christie's for $69 million
- Jack Dorsey's first ever tweet sells for $2.9

April 2021 – Playboy is getting into the NFT market

May 2021
- Larva Labs launches their new NFT project: Meebits
- TechCrunch Founder's Apartment to Be Sold as NFT
- **NFT Valuations launch**

June 2021
- Binance NFT Marketplace Launch
- CryptoPunk' NFT sells for $11.8 million at Sotheby's

July 2021 – Coca Cola Joins NFT Ecosystem Through Decentraland

August 2021
- Visa purchase CryptoPunk #7610 for around 50 ETH

September 2021 – British Museum enters world of NFTs

November 2021 – **UNIC Open Metaverse Initiative**

NFT-related Standards

- Overview of standards from major blockchain networks
  - From ERC-20 to ERC-721 and ERC-1155 Standards
    - ERC-20 introduced fungible tokens (a class of identical tokens) in Ethereum blockchain
    - ERC-721 introduced non-fungible tokens (a class of unique tokens) in Ethereum and the whole blockchain ecosystem:
      - Free
      - Open standard
    - ERC-721 defines a minimum interface (a smart contract) must implement to allow unique tokens to be managed, owned and traded in Ethereum blockchain
    - ERC-1155 enables the management of multiple token types (e.g., fungible and non-fungible) in a single deployed contract attempting to decrease redundant bytecode on the Ethereum blockchain
  - Other non-Ethereum blockchains that support NFTs:
    - Near
    - Hedera Hashgraph
    - Flow
    - Efinity
    - Polygon
    - Binance Smart Chain

NFTs: Marketplaces

- Current status of NFT marketplaces:
  - Opensea – World's largest digital marketplace ~$ 240M*
  - SuperRare – Create sell and collect rare digital art on Ethereum ~$12M*
  - Foundation – Reclaiming the idea of the stock market to benefit creators and collectors ~$9M*
  - Rarible - Create and sell digital collectibles secured with blockchain
- Types of NFT Marketplaces
  - Focused on digital art – OpenSea, SuperRare, Rarible, Nifty Gateway, Foundation
  - In-game items – Axie Infinity, Sorare, Decentraland, OpenSea, The Sandbox, Enjinx
- Characteristics of Marketplaces
  - Buy NFT
  - Sell NFT
  - Trade NFT
  - Minting an NFT

*30d NFT Trading Volume

From NFTs to the Metaverse

Origins of the Metaverse

- What is “metaverse”
  - From words “beyond” and “universe”
  - Imagine Ready Player One film in real life
  - In a metaverse people could:
    - Participate in virtual shows, conferences, digital galleries, meet-ups with friends
    - Own digital plots, arts, clothes, items
    - Build digital houses, businesses
    - Do almost everything as in real life and beyond
- Overview of existing blockchain-based metaverses
  - Decentraland – Decentralized Virtual World
  - Axie Infinity – Decentralized Gaming Ecosystem
  - The Sandbox - Decentralized Gaming Ecosystem
- How NFTs contributed to the explosion of the metaverse
  - Constitute a building block for the metaverse
  - A place where NFTs could be hosted

UNIC and the metaverse

The first university **in the metaverse**

- Launching a free MOOC on NFTs & the metaverse in June 2022 – to be held **inside** the Metaverse!
- Begun development of an MSc in Metaverse Systems
- Launching a new research center (The Center for an Open Metaverse)
- Incubating startups & supporting creators
- Rolling out NFTs on-campus

Session 12: Decentralized Finance

9. Conclusions

Conclusions

In this session:

- We explored the origins of DeFi and its history. We saw that most of the pieces of DeFi ecosystem pre-existed 2020, but it was **the summer of 2020 when DeFi became widely popular**.
- Projects like **Maker**, **Aave**, **Compound** & **Synthetix** and innovative mechanisms like **AMMs**, **LPs**, **liquidity mining** and **yield farming**, have played a crucial role on the adoption of DeFi.
- The whole DeFi space today (April 2021) has a market valuation of **over $100 billion and TVL around $60 billion**.
- We saw that the whole DeFi stack is constituted by many different pieces, which are constantly evolving and growing, with new pieces continuously being added. In a big part, all these projects are interconnected and interdependent.
- The main pillars of the DeFi ecosystem are **lending** & **borrowing platforms**, **DEXs**, **stablecoins**, **oracles**, **wallets** and others not covered in this session (e.g. DAOs, synthetic assets).

Conclusions

- **Lending & borrowing** platforms allow users to lend and borrow assets, operating without a central authority, need for credit history or other financial records.
  - Projects like Aave, Compound and Maker have locked in their protocols assets of over $25 billion in value and lead the space.
- In **DEXs**, like Uniswap, PancakeSwap and SushiSwap, mass adoption came with the introduction of **AMMs** and **LPs**.
  - Volume have exploded to levels equal to the most successful CEXs.
  - In DEXs users have full control of their funds, privacy (no KYC), no central authority / point of failure and anyone can freely list their project.
- **Wallets**, **stablecoins** and **oracles** are the tools that support the whole ecosystem and make it functional.
  - Wallets enable users to interact with DeFi projects in a simple way.
  - Stable-coins are extensively used in lending & borrowing platforms.
  - Oracles are feeding real world data, otherwise inaccessible, to blockchains and smart contracts.

Session 12: Decentralized Finance

10. Further reading

Further Reading

General

DeFi - The Decentralized Finance Leaderboard at DeFi Pulse

DeFi - Decentralized Finance Projects

Defi Analysis Tools

A Brief History of Decentralized Finance (DeFi)

Binance Smart Chain 2021 Overview

Blockchain for Decentralized Finance | Consensys

Further Reading

DEXs, Liquidity Pools, Market Makers and Aggregators

2key Blog | DeFi, DEXes, DEX Aggregators, AMMs, and Built-In DEX Marketplaces, Which is Which and Which is Best?

What Are Liquidity Pools in DeFi and How Do They Work? | Binance Academy

Impermanent Loss Explained | Binance Academy

Understanding DeFi: flash loans explained | by Monolith | Monolith | Medium

What Is Yield Farming? | CoinMarketCap

Uniswap — A Unique Exchange. Uniswap is one of the most interesting… | by Cyrus Younessi | Scalar Capital | Medium

A Comparison of Decentralized Exchange Designs | by Richard Chen | The Control

How to interpret Total Value Locked (TVL) in DeFi | Messari

Stablecoins

INTO THE WORLD OF ALGORITHM STABLECOIN | by Greg 丁丁 | Dinsight | Medium

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**
Course Support: **digitalcurrency@unic.ac.cy**
IT & Live Session Support: **dl.it@unic.ac.cy**