zeeve

Defi Primitives

Defi Series 2

Ravi Chamria

What will this webinar teach us?

- Primary components of DeFi that make up the DeFi ecosystem.
- Features of these key components of the decentralized financial instruments built on top of the blockchain networks and smart contracts.
- An understanding of the key elements that form the DeFi, how they work, what are their features and how they help in transforming the financial landscape.

- Go through examples of DeFi projects that allow users to lend and borrow.
- Understand the various uses of Stablecoins that facilitate international transactions
- Get an insight into the functioning of the Decentralized exchanges that form the core part of the DeFi ecosystem
- We will focus on the key components of DeFi applications, their key differentiation compared to traditional finance, and longer term implications these DeFi apps are causing.

Quick Recap

What are DEXs or decentralized exchanges?

1. Peer-to-peer markets for crypto traders to conduct transactions without entrusting the administration of their assets
2. No middleman or custodian.
3. Another special feature is smart contracts - self-executing contracts written in computer code, are used to enable these transactions.

Smart contracts
Used by decentralized exchanges to let traders place orders directly with one another.

Comparison between Centralized and decentralized exchanges
centralized exchanges are run by a central institution, like a bank, which is also engaged in the financial services industry and seeks to make a profit.

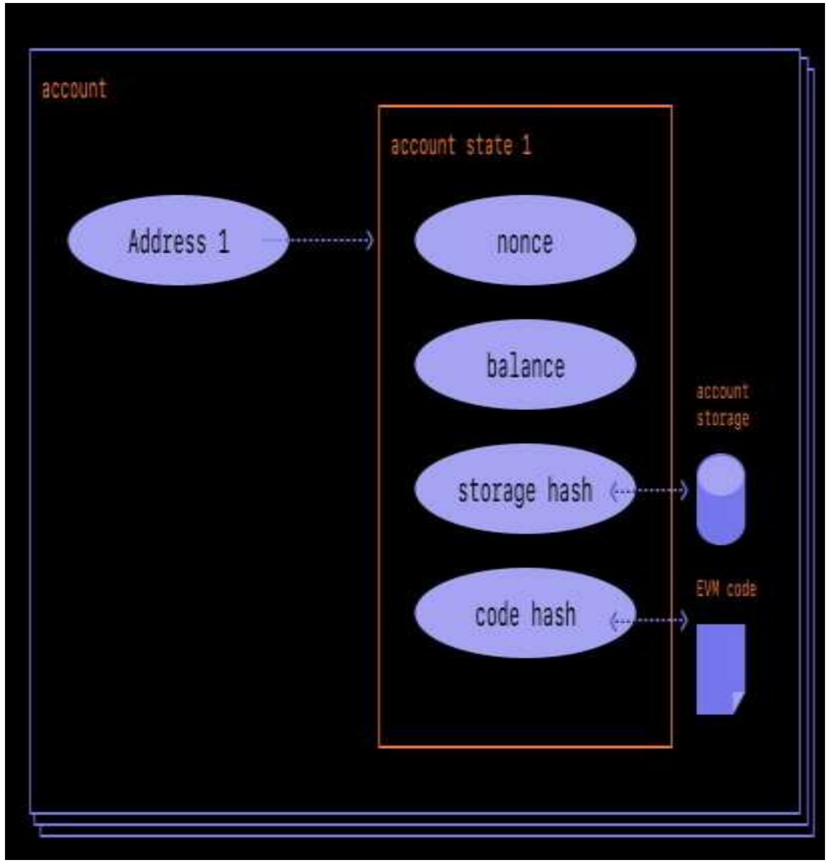
The overwhelming majority of trading activity in the cryptocurrency market is conducted on centralized exchanges since they are usually licensed organizations that guard users' money and provide beginner-friendly interfaces.

zeeve

Understanding the Engine of DeFi: An overview of its core components

Decentralized applications have unlimited potential. Developers can mix and match all sorts of smart contracts and fungible/non-fungible tokens to create transaction flows that are automatic and immune from external influence. Let’s take an expanded look at the toolset that dApp developers possess today.

Transactions



- All Ethereum interactions begin with a transaction. Be it sending data or tokens.

- Ethereum accounts linked with sending/receiving tokens – Externally Owned accounts (EOA)

- Account that interacts with deployed Smart Contracts– Contract Accounts.

- A single transaction initiated by one individual, an EOA, can interact with hundreds of dApps before it is effectively "concluded".

- Transactions have Gas fees that varies with complexity of transactions along with pending transactions in Memepool.

- The visibility of transactions in memepool can allow for advance front-running. Any occurance of direc execution is known as Miner Extractive Value(MEV).

- Hiding such transactions from miners (obfuscation transactions) can mitigate MEV.

Fungible token

- They are Identical & Interchangeable. Like: $100 USD Bill.
- The Ethereum blockchain fungible token standard is ERC-20.
- Implements standard API for tokens within Smart Contracts. And...
- Standards makes things simple. Here's a list of syntaxes used for executing core functions in any ERC-20 token. (Left)
- There are three MAIN types of ERC-20 tokens. Equity Token, Utility Tokens, Governance Tokens.
- Convergence between multiple categories is possible.

Fungible token

Equity Token

- Represents ownership/ equity of an underlying asset/ pool of assets.
- Example: Depositing 1 ETH and getting back 100 'XYZ" tokens on Aave or Compound.
- The exchange rate is variable & depends on supply and demand.
- The Smart contract ensures, it returns a Pro-rata amount of ETH for every 'XYZ' it receives.

Fungible token

Utility Token

- Developed for using inside a specific blockchain ecosystem. They are meant to be used to use the network.

- Do not exist to create value independently.

  Depends on a smart contract system or dApp to fulfil their use case. Examples:

- 1. $DAI, $LINK, $MATIC : Used to pay application specific fees
  2. Synthetix (SNX) : Used as a collateral
  3. ETH in the Ethereum Network for Fee

Fungible token

Governance Token

- Governance tokens are also kind of Equity tokens. But not for assets.
- They represent VOTING RIGHTS for a DeFi protocol or DAOs.
- From implementing Smart contract upgrade to governance proposals- everything done through token holders' vote.
- Eliminates admin controlled functionalities & creates true DeFi.
- Governance token's supply can be:
  Static (MKR token for Maker DAO)
  Inflationary: (COMP token for Compound)
  Deflationary: (MKR token, fees are burned)

Non Fungible Token

- Each unit is unique. Divisible (fractional NFTs) but not interchangeable.
- Hence, can be used as Deeds or Proof-of unique ownership of unitary assets.
- Example: A p2p loan with its own terms & interest rates can be represented as NFTs.
- Technically, NFTs follow ERC-721 & ERC-1155 standards & NOT ERC-20
- While ERC 721 issues only Non-fungible tokens, ERC-1155 can have both fungible + non-fungible ones.
- ERC-1155 also offers batch transfer (saves Gas) & semi-fungibility (serve as Fungible during trading, becomes non-fungible when redeemed).

Custody

A very critical component of DeFi – ability to escrow or custody funds in a smart contract.

Different from Approve of ERC20 Interface.

Facilitates:

- Retaining fees and disbursing incentives
- Token Swaps (ex DEXs)
- Market making of a bonding curve
- Collateralized Loans
- Auctions
- Insurance Funds

The Smart Contract must be programmed to handle the token type – ERC20 or ERC721

- Risk of permanent custody if no mechanism for releasing funds
- Safety checks in token transfer

Supply Adjustment

Token supplies can be adjusted using MINTING & BURNING mechanisms.

Burning -> Intentionally send tokens to an unowned address, or add feature to smart contracts that makes certain number of tokens unusable if matches criterion. **Deflationary and Redemption**
Example: cTokens are burned while exiting a pool in Compound & underlying assets are redeemed. Also burning of AAVE tokens for driving scarcity is another example.

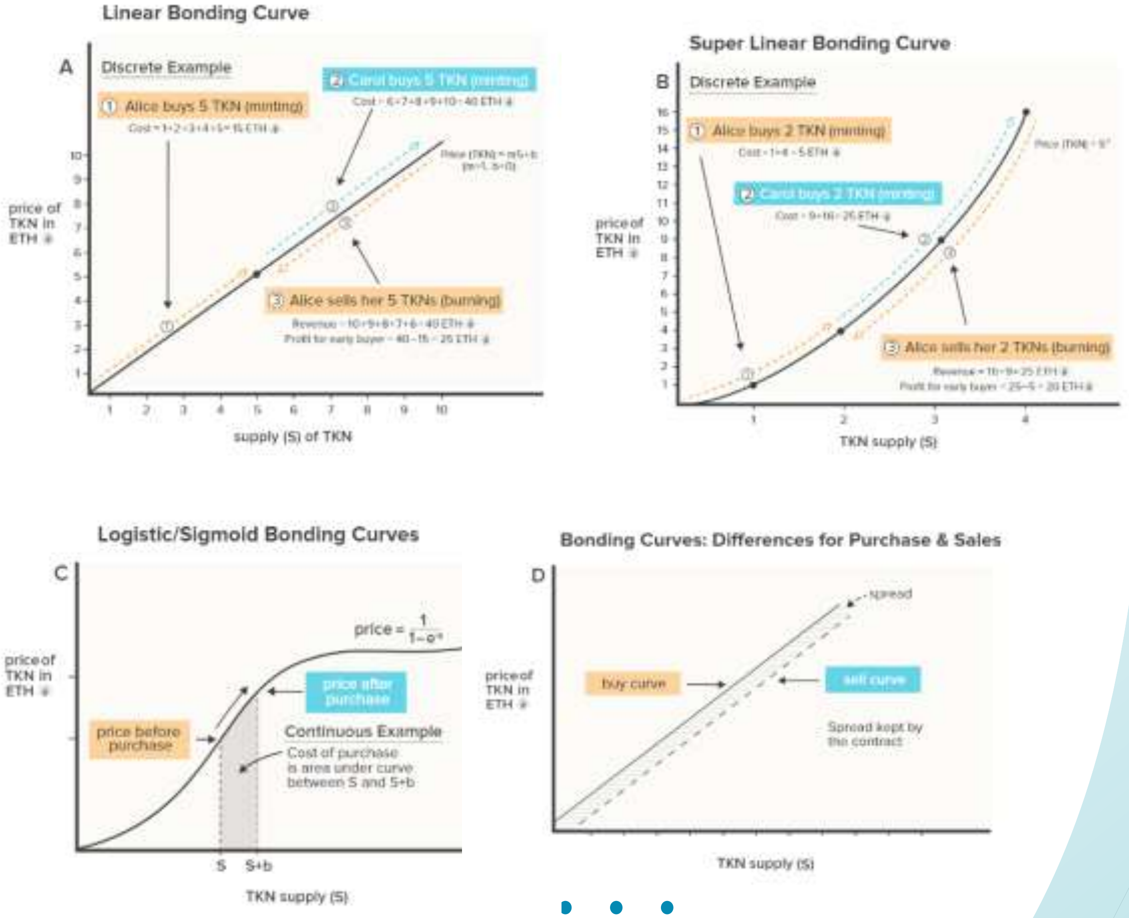
Minting -> can't mint accidentally or manually. Mint mechanics are encoded into Smart contracts. **Inflationary, LP Tokens, Rewards**
Example: Entering a pool and acquiring ownership using cTokens in Compound. Rewarding users for network participations is another example.

Bonding curves -> A dynamic approach to calculate token value taking supply into consideration. Work independent from Crypto exchanges.

- It sells tokens by calculating token prices in Ether and issue them after payment. Also buy them and pay with Ether.

- The growth rate for bonding curve determines users' performances.

Bonding curves



- A linearly increasing bonding curves generously rewards early investors. They can sell back at a higher price point beyond their purchase price.
- A super linear growth can result even more extreme return.
- In practice most projects use a sub-linear growth rate that converges on an upper bounded price.
- The selling curve could have a lower growth rate than buying curve.
- The difference between the two is the value accrued to the Smart Contract and represents a fee for usages.
- Till the contract has sufficient collateral to sell back down the entire sell curve, the contract will continue to fulfil sell demands.

Incentives

Incentives are given or charged to encourage / discourage network participants.

1. Staking rewards is positive incentives given to the stakers on a pro-rata basis or have minimum threshold staked. Kind of direct benefit transfer into the account of users. Compound issues Staking reward in COMP tokens (funded by custodied COMP) on pro-rata basis while Synthetix issues only if the stake matches threshold (based on Inflation). - **Staking Pools, dPoS validators and delegates**

2. Slashing is a kind of staking penalty. It removes complete/ a portion of users staked balances.
It can happen because of under collateralization, malicious behaviours of Nodes or sudden changes in market condition. For example: The fund balance of an user holding Algo Stable coin can be reduced directly by system if it starts losing peg. **DPoS, Collateralized Loans, Algorithmic Stablecoins**

3. Fees are a another typical funding mechanism for a protocol. Though it works as a direct negative incentives for users. The accrued fees has a staked balance associated with it to ensure payments.

4. Direct Rewards and Keepers - But Direct Rewards work as a positive incentive. As Smart contracts can't auto execute, So it will not run until it's triggered by an on-chain transaction. For example: A lending protocol can't liquidate an under collateralized loan until an on-chain transaction calls its liquidation function. Keepers are External Owned Accounts incentivized to perform this action. Keeper Rewards inflate Gas prices due to competition. **Rarible, Aave**

Swap

Swapping is simply exchanging one type of tokens with another. It's Non-custodial and done using a DEX.

There are 2 approaches a DEX gets liquidity.
Order Book Matching
A. Automated Market Makers

For a successful order-book match, all parties must agree on the swap exchange rate. **Kuber Network** has a fully automated order books.

The order-matching approach is expensive and inefficient because each update requires an on-chain transaction.

An AMM replaces order books with Liquidity Pools. Instead of P2P transactions AMM uses P2C (Peer To Contract) mechanism.
Aave, Compound

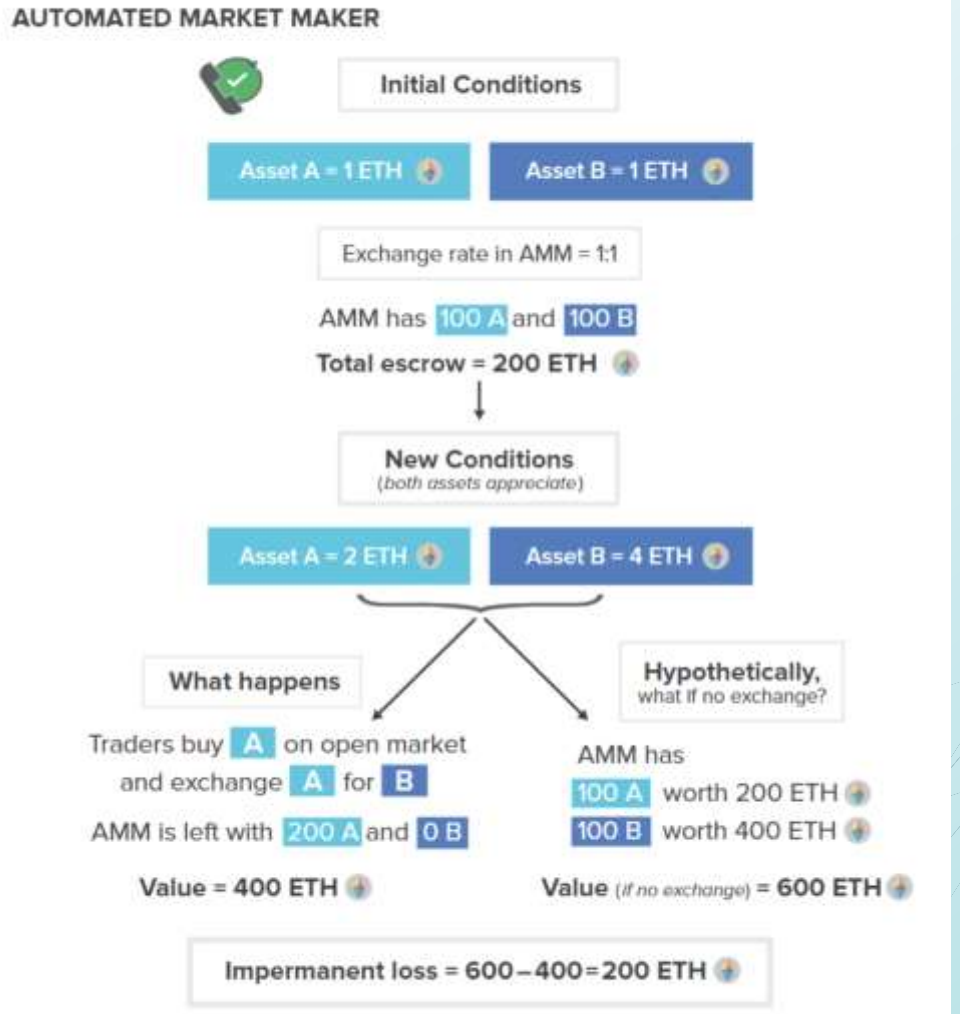
No intermediaries. Price determined by formulae.
Liquidity is provided by Liquidity Providers.

They are reimbursed with Governance Tokens and transactions fees paid by traders.

An additional benefit is composable liquidity. Any exchange contract can plug into the liquidity and exchange rates of any other exchange contract.

Drawback of AMM is impermanent loss. Means: Less dollar value at withdrawal than at the time of deposit.

Impermanent Loss



AUTOMATED MARKET MAKER

Initial Conditions

Asset A = 1 ETH

Asset B = 1 ETH

Exchange rate in AMM = 1:1

AMM has 100 A and 100 B

Total escrow = 200 ETH

New Conditions
(both assets appreciate)

Asset A = 2 ETH

Asset B = 4 ETH

What happens

Traders buy A on open market and exchange A for B

AMM is left with 200 A and 0 B

Value = 400 ETH

Hypothetically,
what if no exchange?

AMM has

100 A worth 200 ETH

100 B worth 400 ETH

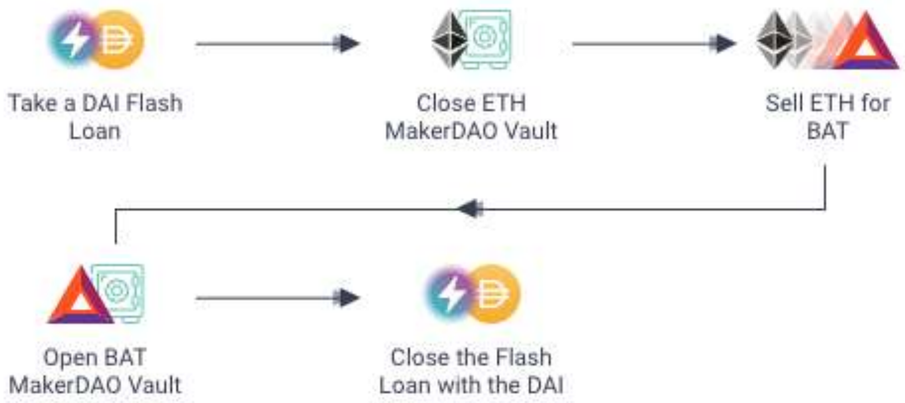
Value *(if no exchange)* = 600 ETH

Impermanent loss = 600–400=200 ETH

Collateralized Loans

- Collateralized loans are backed by an equivalent or excess amount of collateral.
- Here the Collateral can become less valuable than the debt. due to price volatility, leading to unfortunate liquidation.
- To mitigate risk, larger collateralization ratio is required to avoid margin calls.
- For Maker DAO, borrowers are required to keep 150% collateral on loan value. Any drop of ETH value below that will come at a cost of 13% penalty.
- If private key is lost or contract gets hacked, borrowers or lender both will lose their assets.
- Decentralized Insurance protocols (like Nexus Mutual or CDx)can help in such cases.

Flash Uncollateralized Loans



- One of the primary draws of DeFi that aims to exponentially increase access to capital is the flash loan. A flash loan is an instantaneous loan paid back within the same transaction.

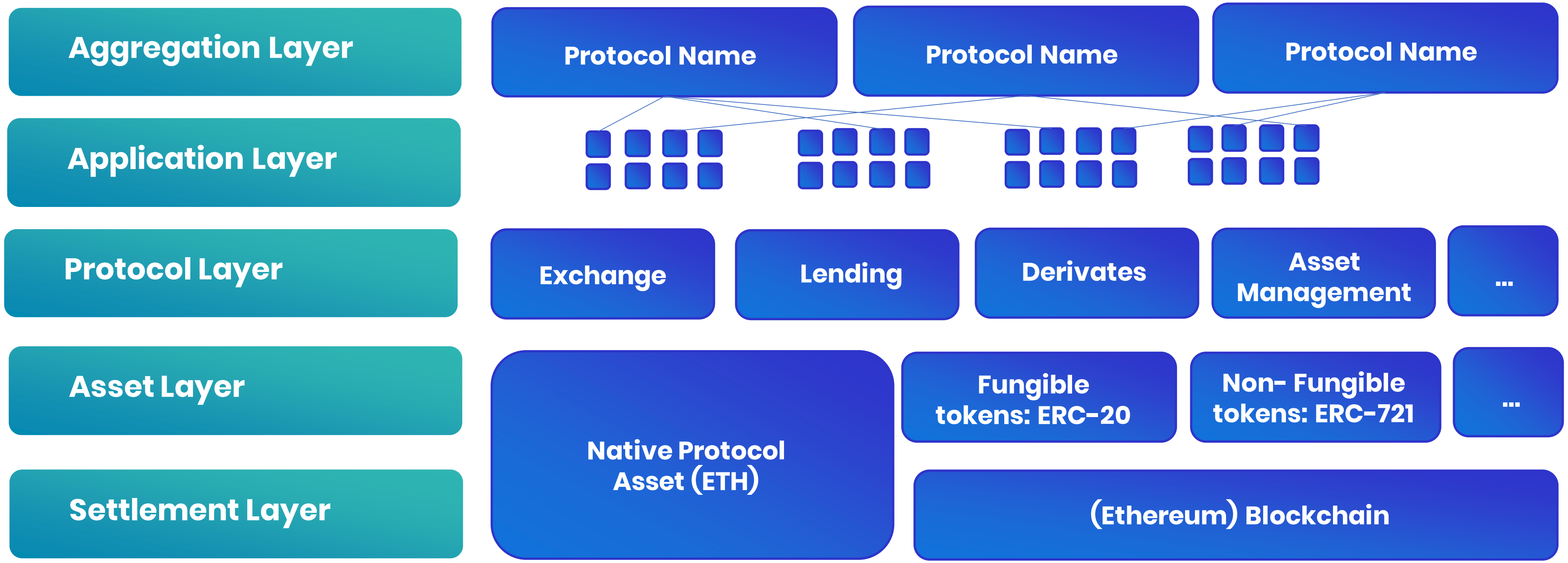
- A flash loan is similar to an overnight loan in the traditional financial ecosystem. However, the main draw here is that repayment is required within the transaction and the same is enforced by the smart contract.

- As a result, the following situations can play out, either the user successfully uses the loan for the desired use case and completely repays it in the course of the transaction; or the transaction fails and everything resets on the blockchain as if the user had not borrowed any money in the first place.

- As a result, a lot of the risk is alleviated. One possible issue may be that of smart contract design, where there may be a logic error in the code or an exploit due to the value of certain economic models in the algorithm that let parties subtly exploit the contract.

Architecture

- DeFi uses a multi-layered architecture.
- Every layer has a distinct purpose.
- The layers build on each other and create an open and highly composable infrastructure that allows everyone to build on, rehash, or use other parts of the stack. It is also crucial to understand that these layers are hierarchical: They are only as secure as the layers below.
- If, for example, the blockchain in the settlement layer is compromised, all subsequent layers would not be secure.
- Similarly, if we were to use a permissioned ledger as the foundation, any decentralization efforts on subsequent layers would be ineffective.



Aggregation Layer

Protocol Name

Protocol Name

Protocol Name

Application Layer

Protocol Layer

Exchange

Lending

Derivates

Asset Management

...

Asset Layer

Native Protocol Asset (ETH)

Fungible tokens: ERC-20

Non- Fungible tokens: ERC-721

...

Settlement Layer

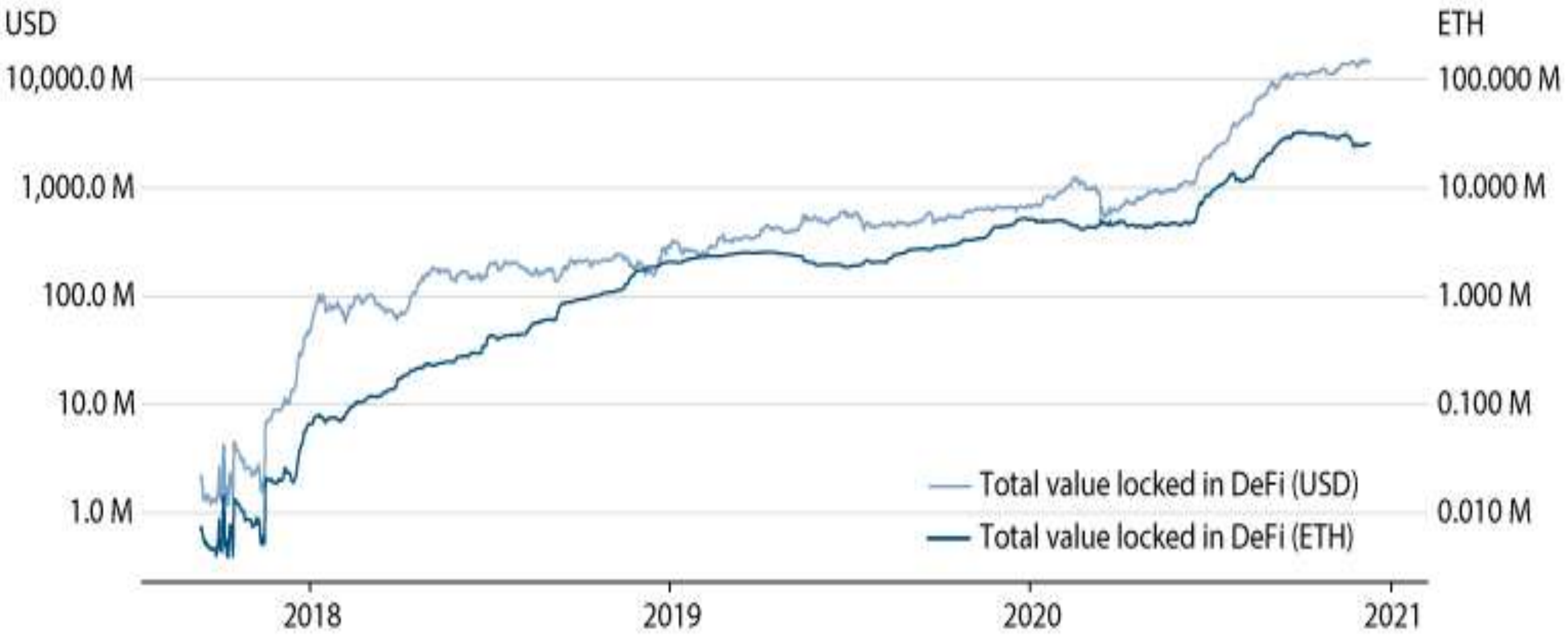
(Ethereum) Blockchain

DeFi grew by 43x over the last 18 months to over $210 billion

Summary

- The total value locked of all assets in DeFi stands at over $210 billion today
- This represents a 4,304% increase from 18 months ago ($4.84B), and a 22,961% increase from two years ago ($924.3M)
- With new DeFi protocols coming online every day and crypto going mainstream, growth is accelerating

Total Value Locked in DeFi Contracts (USD and ETH)



Most Popular Decentralized Exchange Protocols

Protocol Name	Protocol Type	Price discovery
0x	Exchange	Off-chain order books
(Air) Swap	P2P/OTC	P2P negotiation
Bancor	CFMM	Smart Contract
Balancer	CFMM	Smart Contract
Curve	CFMM	Smart Contract
Kyber Network	Reserve aggregator	Proposal by maker
UniSwap	CFMM	Smart Contract

Address

Zeeve Deeptech Pvt Ltd
1283, ATS Greens, Sector-93A
Noida, India 201304

Zeeve Technologies Ltd.
2001, Regal Tower, Business Bay,
Dubai, UAE

Zeeve Inc.
395 Santa Monica Place, Unit 308,
Santa Monica, California - 90405

Contact

- Email: success@zeeve.io
- http://www.zeeve.io

zeeve

USA

Dubai

India