



**OST**

Eastern Switzerland  
University of Applied Sciences

# Blockchain (BlCh)

DeFi

Thomas Bocek (\*slides partially based on Christian Killer's slides)

07.10.2024

# Traditional / Centralized Finance (TradFi/CeFi)

- Traditional / Centralized finance (TradFi/CeFi) originally from ancient **Mesopotamia**
- However, in this lecture, with CeFi, I refer to trading using blockchain with centralized entities, when talking about the regular banking, I refer to TradFi.
- Since then, wide range of goods and assets as currency [[link](#)].
  - Cattle, cacao and coffee beans, or cowrie shells, salt, precious metals
    - Gold has enjoyed near universal global acceptance as a store of value
    - **Fiat** currencies (USD, CHF).
      - **fiat** („Es sei getan! Es geschehe! Es werde!“)
- “Clay tokens, described by some scholars as the world's first money, found in Susa, Iran have been dated to 3300 B.C.” [[history](#)]













Image Source: <https://factsanddetails.com/world/cat56/sub363/item1514.html>

# CeFi vs. DeFi - Key Features










- Currency either carries intrinsic value (e.g., land, shares) or created by a centralized entity (**reserve bank**) (fiat currency) [**SNB**]
  - Government is backing the financial value of a currency (regulated, trusted)
- Blockchain's (BC) key innovations is the transfer and trade of financial assets without trusted intermediaries.
  - Decentralized Finance (DeFi) specializes in advancing financial technologies and services on top of smart contract enabled ledgers.
- CeFi vs. DeFi – 3 distinct features
  - 1) Transparency
    - Public rules and protocols [**sushiswap**]
    - Avoid private agreements, back-deals and centralization
  - 2) Control
    - DeFi gives control to its users. No-one should censor, move or destroy the users' assets
  - 3) Accessibility [**unbanked**] [**but...**]
    - Anyone with a computer, internet connection and know-how can use or create DeFi products

# High Risk, High Reward?

- Financial gain in DeFi also presents a significant contrast to TradFi.
  - In the years 2020 and 2021, DeFi offered higher annual percentage yields (APY) than TradFi
  - TradFi interest rates
  - DeFi interest rates
  - Today: TradFi vs DeFi - closing the gap
- DeFi enables “similar” traditional financial products
  - DeFi also enables novel financial primitives, such as flash loans [hack, what happened]

 <b>BUSD</b> 1 bBUSD = 1.0708 BUSD	Lending APR: 10.35% Staking APR : 1.38% Total APR: 11.73% Total APY 	206.17M BUSD	131.73M BUSD	63.89%
 <b>USDT</b> 1 bUSDT = 1.0266 USDT	Lending APR: 9.81% Staking APR : 1.76% Total APR: 11.56% Total APY 	117.95M USDT	71.4M USDT	60.53%
 <b>TUSD</b> 1 bTUSD = 1.0057 TUSD	Lending APR: 0.921% Staking APR : 1.98% Total APR: 2.9% Total APY 	59.56M TUSD	11M TUSD	18.47%
 <b>BTCB</b> 1 bBTCB = 1.0043 BTCB	Lending APR: 0.377% Staking APR : 1.16% Total APR: 1.54% Total APY 	2.75k BTCB	325.09 BTCB	11.82%
 <b>ETH</b> 1 bETH = 1.0121 ETH	Lending APR: 0.830% Staking APR : 0.632% Total APR: 1.46% Total APY 	55.81k ETH	9.79k ETH	17.53%

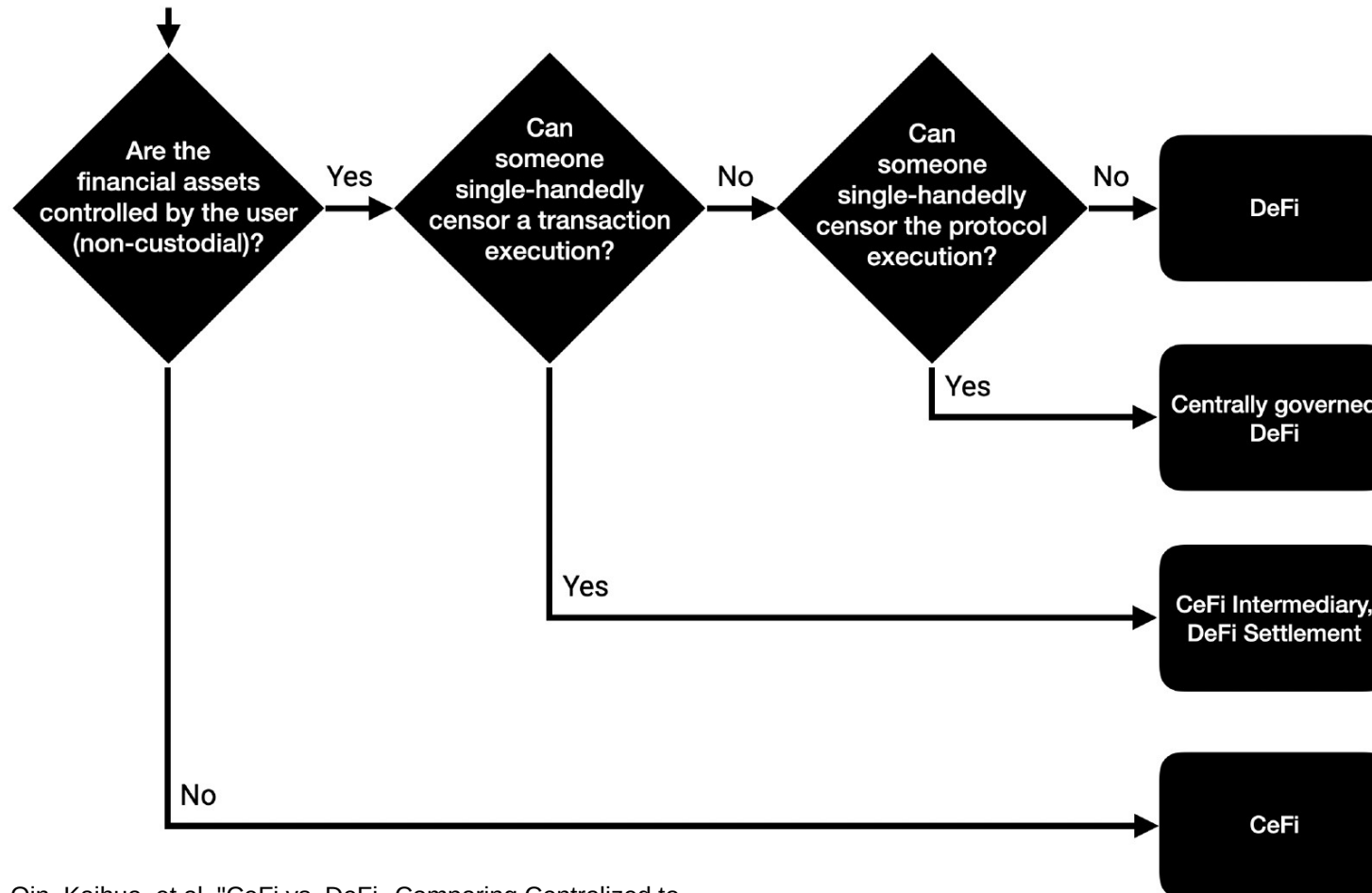
2021: <https://app.alpacafinance.org/lend>

Asset	Total supplied	Supply APY	Total borrowed	Borrow APY, variable
 <b>USD Coin</b> USDC	1.50B \$1.50B	4.22 %	1.31B \$1.31B	5.38 %
 <b>Tether</b> USDT	1.69B \$1.69B	4.02 %	1.44B \$1.44B	5.25 %
 <b>Dai Stablecoin</b> DAI	119.89M \$119.86M	3.83 %	109.79M \$109.76M	5.63 %
 <b>Rocket Pool Protocol</b> RPL	570.99K \$5.86M	3.82 %	378.99K \$3.89M	7.31 %
 <b>Curve.Fi USD Stablecoin</b> crvUSD	700.70K \$699.83K	3.54 %	525.33K \$524.68K	5.29 %
 <b>PayPal USD</b> PYUSD	11.03M \$11.02M	3.49 %	8.71M \$8.71M	5.58 %
 <b>LUSD Stablecoin</b> LUSD	3.96M \$3.96M	3.45 %	3.11M \$3.11M	5.55 %
 <b>Frax</b> FRAX 	798.25K \$795.95K	2.80 %	599.88K \$598.15K	4.70 %

2024: [https://app.aave.com/markets/?marketName=proto\\_mainnet\\_v3](https://app.aave.com/markets/?marketName=proto_mainnet_v3)

# DeFi Decision Tree

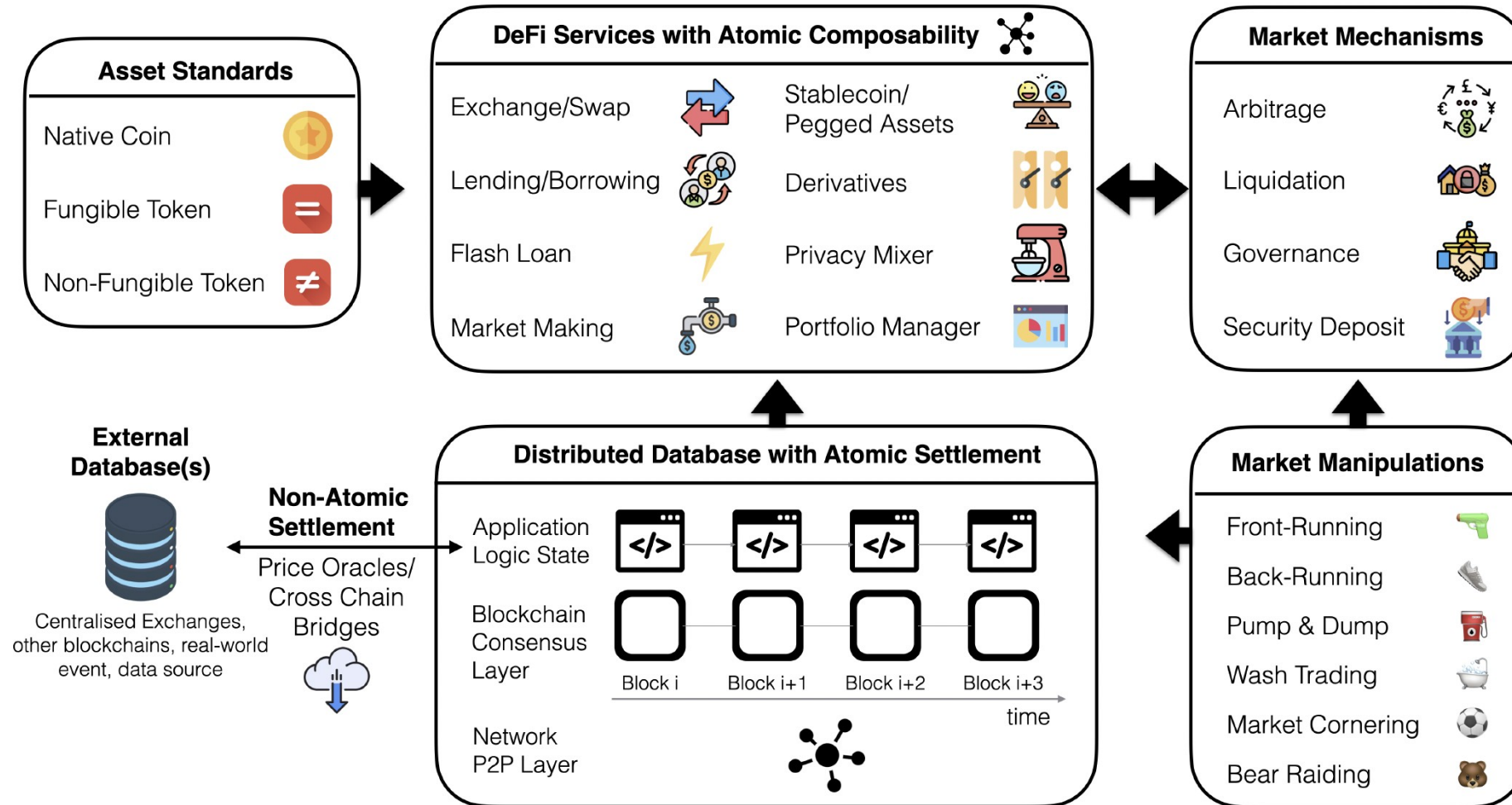
- The boundaries of DeFi and CeFi not clear cut





Bear raid  
 Cornering the market

# High-Level Systematization of DeFi



# Key DeFi Properties

## 1) Public Verifiability

- While the DeFi app may not be fully open-sourced, the execution and bytecode must be publicly verifiable on a BC
  - **Verify and Publish Source Code**

## 2) Custody

- DeFi allows its users to control their assets at any time (no need to wait for the bank to open). Technical risks are with the user, with CeFi, is mostly with the bank (USP)

## 3) Privacy: DeFi is present on non-privacy preserving smart contract blockchains (e.g., not on **Monero**).

- BCs offer pseudoanonymity, but no real anonymity
  - **deanonymization / clustering of transaction data**
- Centralized exchanges with KYC/AML practices are often the only viable route to convert between fiat and cryptocurrency assets
  - Can be queried by law enforcement

# Key DeFi Properties

4) Atomicity: A BC transaction supports sequential actions, which can combine multiple financial operations.

- Flash loan example
- This combination can be enforced to be atomic
- While this programmable atomicity property mostly absent from CeFi, (likely costly and slow) legal agreements could enforce atomicity in CeFi as well.

5) Execution Order Malleability: Users on permissionless blockchains typically share publicly the transactions

- No centralized entity ordering transaction execution, peers can perform transaction fee bidding contests to steer the transaction execution order. [frontrunning]
  - Such order malleability was shown to result in various market manipulation strategies, which are widely used on BCs nowadays [generalized-frontrunning]
- In CeFi: regulatory bodies impose strict rules on financial institutions and services as in how transaction ordering must be enforced



# Key DeFi Properties

6) Transaction Costs: Transaction fees in DeFi and blockchains in general are essential for the prevention of spam

- In CeFi, financial institutions can opt to offer transaction services at **no cost** (or are mandated by governments to offer certain services for free) because of the ability to rely on KYC/AML verifications of their clients

7) Anonymous Development and Deployment: Many DeFi projects are developed and maintained by anonymous teams

8) Non-stop Market Hours: It is rare for TradFi markets to operate without downtime.

- New York Stock Exchange & Nasdaq Stock Exchange business hours are Monday to Friday from 9:30 a.m. to 4 p.m. Eastern Time.
  - Many DeFi markets are open 24/7 (unless hacked or in maintenance mode)
- DeFi has no pre- or post-market trading
- System outages at TradFi stock happened (e.g., **GameStop** short squeeze event)

# Regulations

- Regulatory uncertainty (e.g., does a software programmer hold liability to do KYC/AML for an application or code he/she provides to the public?)

## A) Censoring (Temporarily) Transactions

- Miners can decide to temporarily censor transactions
- Nodes in lightning may simply refuse a transaction (forcing the user to fall-back to on-chain payment channels)

## B) Blacklists, Fungibility and Destruction of Assets

- Once a service provider is KYC/AML regulated, the freezing and confiscation of financial assets may be requested

- **USDT** and **USDC** have blacklists

- USDT: 1820 accounts **blacklisted** so far, 1.27B USDT are banned

```
1 function transfer(address _to, uint _value) public
  whenNotPaused {
2   require(!isBlackListed[msg.sender]);
3   if (deprecated) {
4     return UpgradedStandardToken(upgradedAddress).
      transferByLegacy(msg.sender, _to, _value);
5   } else {
6     return super.transfer(_to, _value);
7   }
8 }
9 function addBlackList (address _evilUser) public
  onlyOwner {
10  isBlackListed[_evilUser] = true;
11  AddedBlackList(_evilUser);
12 }
13 function destroyBlackFunds (address _blackListedUser)
  public onlyOwner {
14  require(isBlackListed[_blackListedUser]);
15  uint dirtyFunds = balanceOf(_blackListedUser);
16  balances[_blackListedUser] = 0;
17  _totalSupply -= dirtyFunds;
18  DestroyedBlackFunds(_blackListedUser, dirtyFunds);
19 }
```

Listing 1: USDT **code** blacklist functionality.

# Future? (opinion)

- Will DeFi replace CeFi?
  - Financial system still requires trust
    - Fully decentralized mortgage ~difficult
  - DeFi will change traditional banking
- DeFi could become the underlying infrastructure of future banks, whereas traditional finance / custody adapt

[https://en.wikipedia.org/wiki/File:Paradeplatz\\_2015.jpg](https://en.wikipedia.org/wiki/File:Paradeplatz_2015.jpg)



# CEX: Exchange Rate

- **Centralized (CEX):** ask/bid, sell/buy, the last trade, e.g., 200 DAI for 1 ETH → price (order book)
  - Workflow: create order, publish on exchange, wait to get filled. Browse orders, start fill order.
  - Price changes if trade happens, ask was same or lower than bid. Ask/bid submitted by users – add/remove orders
  - **Slippage:** you see a price, submit, and until its executed, price can change.
    - Set limits, order may stay in the orderbook
- **Decentralized (DEX):** ratio of pairs (**automatic market making**)
  - Workflow: exchange pairs
  - Example amount in pool: DAI 200, ETH 1 → price 200DAI/1ETH
- Both: large swap can change price → price impact

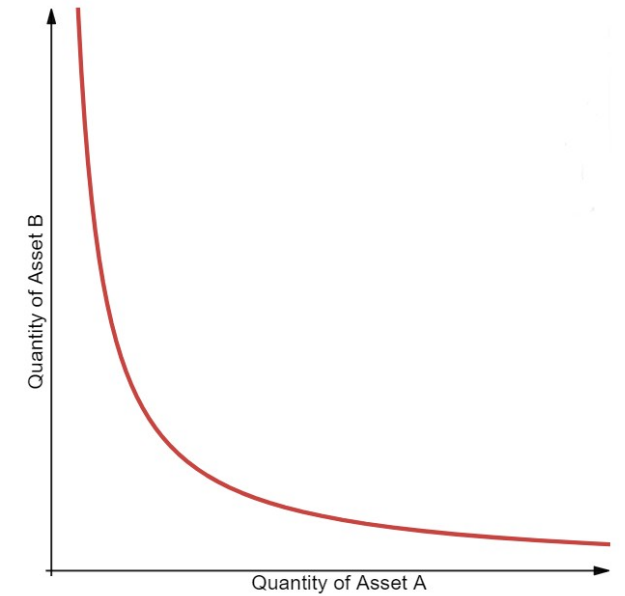
Price(USDT)	Amount(BTC)	Total
63239.97	0.44255	27,986.84872
63239.96	0.36276	22,940.92789
63238.74	0.07300	4,616.42802
63238.65	0.10230	6,469.31390
63237.52	0.07800	4,932.52656
63237.00	0.01493	944.12841
63236.98	0.06168	3,900.45693
63235.57	0.10038	6,347.58652
63233.64	0.04732	2,992.21584
63232.60	0.01429	903.59385
63232.40	0.10459	6,613.47672
63232.39	0.06168	3,900.17382
63231.49	0.01791	1,132.47599
63231.48	0.16768	10,602.65457
63231.47	0.15867	10,032.93734
63227.71	0.16472	10,414.86839
63227.70	0.69732	44,089.93976
<b>63,227.69 ↓ \$63,227.69</b> <span style="float:right">More</span>		
63227.69	0.09446	5,972.48760
63227.68	0.07903	4,996.88355
63225.08	0.00367	232.03604
63223.01	0.06710	4,242.26397
63222.59	0.02300	1,454.11957
63222.20	0.11855	7,494.99181
63222.00	0.02000	1,264.44000
63221.00	0.11908	7,528.35668
63220.88	0.00074	46.78345
63220.65	1.56572	98,985.83612
63220.15	0.00237	149.83176
63220.00	3.92240	247,974.12800
63219.84	0.00032	20.23035
63218.21	0.04054	2,562.86623
63217.98	0.10230	6,467.19935
63216.80	0.00032	20.22938
63216.60	0.08410	5,316.51606



# DEX: Exchange Rate / Decentralized Swaps

- DEX uses  $X * Y = k$ , where  $k$  is constant,  $X$  and  $Y$  are asset values (if you take out  $X$  you need to provide  $Y$ )
  - DAI = 200, ETH = 1,  $k = 200$
- Constant function market makers (CFMM)
  - “We are still very early in the evolution of constant function market makers...” [ref]
- Exchange price calculation ( $X * Y = k$ ) →  $X * Y = (X + x) * (Y - y)$ 
  - Swap for 0.5 ETH, if you send 0.5 ETH to pool
    - $200 * 0.5 / (1+0.5) = 66$
    - $66/0.5 \rightarrow 133$  DAI → **~133 DAI for 1 ETH**
  - Deduct 66 DAI from pool, add 0.5 ETH →  $133/1.5 \rightarrow$  **~ 88 DAI for 1 ETH**
    - $K = 133.333 * 1.5 = 200$
    - Never draining the pool
    - Trade with better price than resulting pool (huge price impact)

$$y = \frac{Yx}{X + x}$$



$x$  is input asset amount (ETH)  
 $X$  is input asset balance (ETH)  
 $y$  is output asset amount (DAI)  
 $Y$  is output asset balance (DAI)



# Exchange Rate / Decentralized Swaps

- Reverse of 133/1.5 → I want to buy ETH with 66 DAI

- $1.5 \cdot 66 / (133 + 66) = 0.5$       $x = \frac{Xy}{Y+y}$

- Swap at price 133.333 → new price 200DAI/ETH → reversible

- If swap price == the final pool price

- $\frac{Y-y}{X+x} = \frac{y}{x}$       $y = \frac{Yx}{X+2x}$

- Example  $200 \cdot 0.5 / (1 + 2 \cdot 0.5) = 50$

- $150 / 1.5 = 50 / 0.5$  (swap and final price the same)

- However, not reversible with same numbers. To get the same price (200), need to swap 75 DAI for 0.375ETH → 225/1.125ETH

- THORChain

$$y = \frac{xYX}{(x+X)^2}$$

x is input asset amount (ETH)  
X is input asset balance (ETH)  
y is output asset amount (DAI)  
Y is output asset balance (DAI)

# Decentralized Swap

- Many AMM variations
  - THORChain – punish large swaps [[how its calculated](#)]
  - Example:  $0.5 * 200 * 1 / (0.5 + 1)^2 = 44.4$  (price 88DAI/1ETH)
  - Resulting pool: 155.555/1.5 → price 103.7DAI/1ETH
    - Large trades gives you a worse rate than the resulting pool price. Small values, e.g., 0.1 ETH → 16.5DAI / 165DAI/ETH, pool: 166.8DAI/ETH
- More [AMMs, here](#)
- Attacks: Exploit slippage tolerance: [sandwich attack](#) (front-running) [[seen in practice](#)]

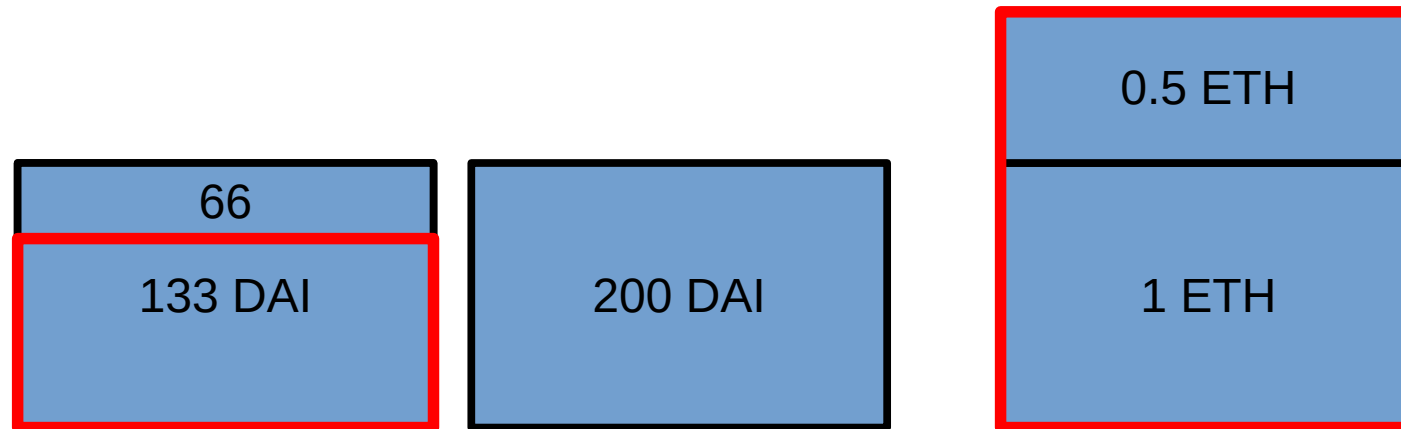
x is input asset amount (ETH)  
X is input asset balance (ETH)  
y is output asset amount (DAI)  
Y is output asset balance (DAI)

$$y = \frac{xYX}{(x + X)^2}$$

# Decentralized Swap

- Swap 0.5 ETH for DAI, how much DAI? (price 200DAI/ETH)
- (price 133DAI/ETH), but DAI funds not decreased yet
- Pool: 133 DAI, 1.5 ETH, price (88DAI/ETH)

$$y = \frac{Yx}{X+x}$$



# DeFi Fundamentals

- Swaps (just covered)
- Arbitrage bots
  - Swapping in multiple pools or CEX, if a bot sees e.g., a trading opportunity,
    - Example: Pool 1: 250 DAI for 1 ETH, pool 2: 200 DAI for 1 ETH
    - Arbitrage bot has 1 ETH (not considering price impact in this example)
      - Buy for 1 ETH 250 DAI in pool 1
      - Sell 250 DAI for 1.25 ETH in pool 2, profit = 0.25 ETH
  - Keep the same price across exchanges
- Flash loans
  - Same chain: arbitrage bots can use flash loans
  - Get loan and pay it back in the same transaction
    - No risk for lender, either he gets the tokens back or transaction is invalid
- **Example** with Aave: from 1000 to 1045, including payback of 1000.9
  - SushiSwap, Uniswap, DAI, wETH
- Without arbitrage bots, DEX does not work!
  - Essential part of the ecosystem

# DeFi Fundamentals






- Swaps (just covered)
- Arbitrage bots (just covered)
- Liquidity providers (LP)
  - Someone should provide liquidity - filling the pools
  - General rules for AMM-based DEX
    - Providing / removing liquidity - **no change of price**
    - LP provide 50/50 ratio of assets, example with a 200DAI/1ETH pool
    - LP can provide 100DAI/0.5ETH, or 400DAI/2ETH
    - LP<sub>a</sub> gets liquidity units (LP token), with 100/0.5 (new pool: 300/1.5), LP<sub>a</sub> owns 1/3 of the pool
- Why should a LP provide liquidity?



# Liquidity Providing

- LP token → % of the liquidity provided in the pool
  - Earn fees for providing liquidity
  - For each swap, user has to pay fees
    - Fees are distributed proportionally to the amount of LP tokens
    - Eg., fees collected are 2ETH, LP gets 10%, 0.2ETH
  - More liquidity provided by others, the 10% will be decreased → less earnings

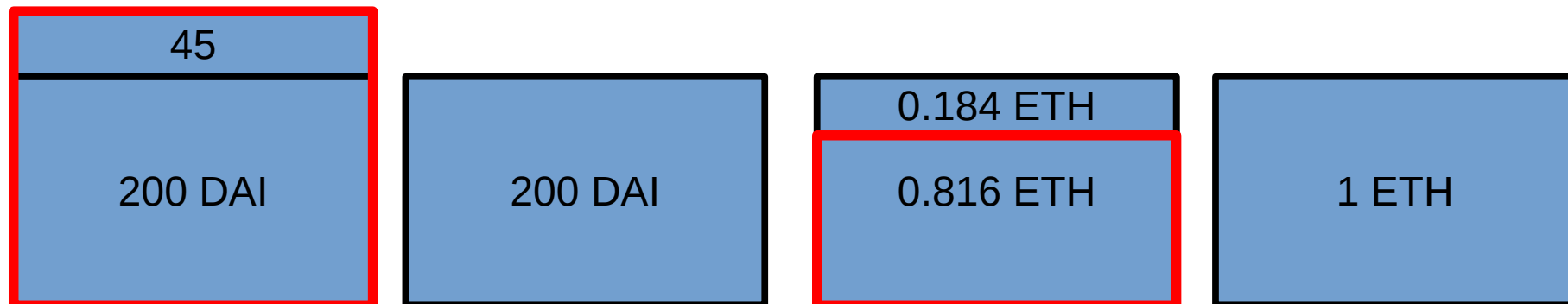
- Why is not everyone providing liquidity?
  - Free money?

	<b>BUSD</b> 1 ibBUSD = 1.0708 BUSD	Lending APR: 10.35% Staking APR : 1.38% Total APR: 11.73% Total APY ☺: 12.44%	206.17M BUSD	131.73M BUSD	63.89%
	<b>USDT</b> 1 ibUSDT = 1.0266 USDT	Lending APR: 9.81% Staking APR : 1.76% Total APR: 11.56% Total APY ☺: 12.26%	117.95M USDT	71.4M USDT	60.53%
	<b>TUSD</b> 1 ibTUSD = 1.0057 TUSD	Lending APR: 0.921% Staking APR : 1.98% Total APR: 2.9% Total APY ☺: 2.94%	59.56M TUSD	11M TUSD	18.47%
	<b>BTCB</b> 1 ibBTCB = 1.0043 BTCB	Lending APR: 0.377% Staking APR : 1.16% Total APR: 1.54% Total APY ☺: 1.55%	2.75k BTCB	325.09 BTCB	11.82%
	<b>ETH</b> 1 ibETH = 1.0121 ETH	Lending APR: 0.830% Staking APR : 0.632% Total APR: 1.46% Total APY ☺: 1.47%	55.81k ETH	9.79k ETH	17.53%

# Liquidity Providing

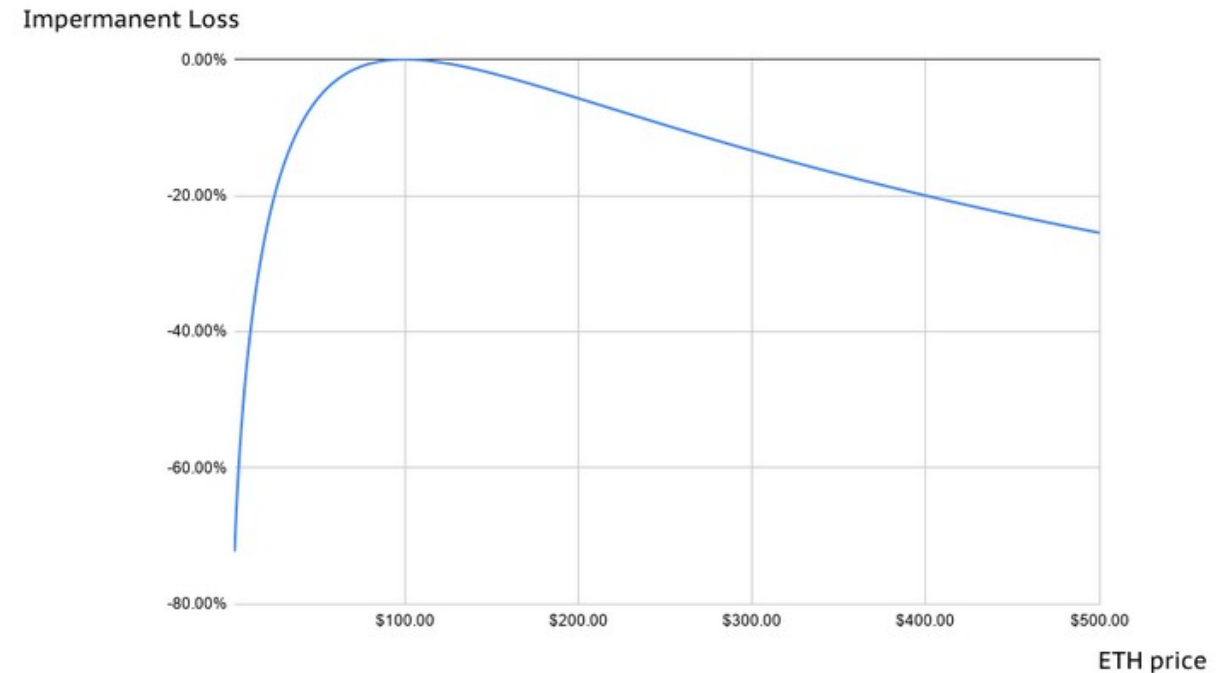
- Impermanent Loss (its mostly permanent, better name: price shift loss)
  - “Users who provide liquidity to AMMs can see their staked tokens lose value compared to simply holding the tokens on their own.”
  - Example: I own 10% of the pool: 200 DAI (price 1\$), 1 ETH (price 200\$)
    - 20 DAI, 0.1 ETH (\$20) → \$40
  - ETH price goes up 300\$, hodler:
    - 20 DAI, 0.1 ETH (\$30) → \$50
  - Pool is at 200/1, other pools are at 300/1 → arbitration

$$y = \frac{Yx}{X+x}$$



# Liquidity Providing

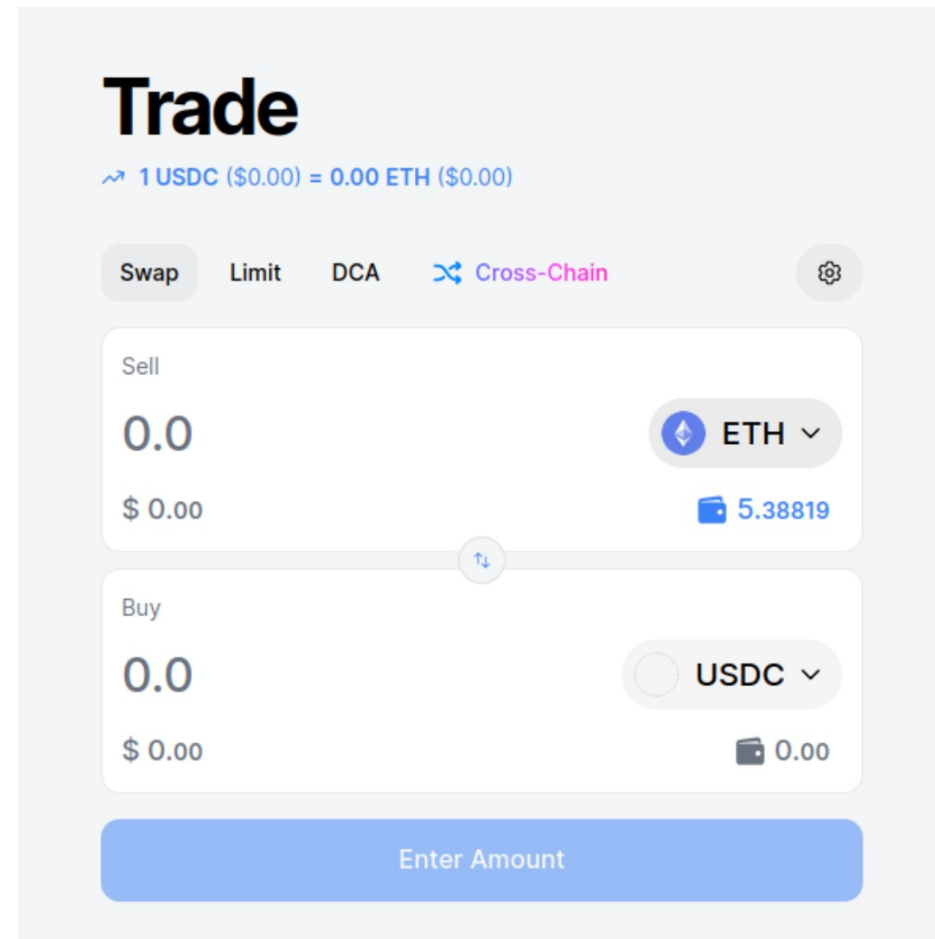
- Uniswap formula:  $\sim 245\text{DAI}/0.8166$ 
  - 10% of 245 DAI  $\rightarrow$  \$24.5
  - 10% of 0.8166 ETH  $\rightarrow$  0.08166 ETH (\$24.5)
- \$49 vs \$50 - 1\$ loss instead hodling
  - The more volatile the market is the higher the impermanent loss
- LP Token: fees + impermanent loss
  - Other incentive staking: if you place your token in a staking or yield farming contract



# Lets use a DEX

- SushiSwap
  - ClassicAMM → v3 introduces concentrated liquidity, which makes the impermanent loss situation better, but introduces complexity
- [UniswapV2Router02.sol](#)
- [UniswapV2Factory.sol](#)
- Sepolia, [V2Factory](#)
- Sepolia, [V2Router02](#)

- <https://www.sushi.com/swap?chainId=11155111>



The screenshot displays the 'Trade' interface on the SushiSwap website. At the top, it shows a trade preview: '1 USDC (\$0.00) = 0.00 ETH (\$0.00)'. Below this, there are tabs for 'Swap', 'Limit', 'DCA', and 'Cross-Chain', with a settings gear icon on the right. The 'Swap' tab is selected. The interface is divided into two sections: 'Sell' and 'Buy'. In the 'Sell' section, the amount '0.0' is entered, and the currency is set to 'ETH'. Below the amount, the value '\$ 0.00' is shown. In the 'Buy' section, the amount '0.0' is entered, and the currency is set to 'USDC'. Below the amount, the value '\$ 0.00' is shown. A blue button at the bottom is labeled 'Enter Amount'. A double-headed arrow icon is positioned between the 'Sell' and 'Buy' sections.