

Blockchain Advanced Topics

Tecnologie Internet
a.a. 2022/2023

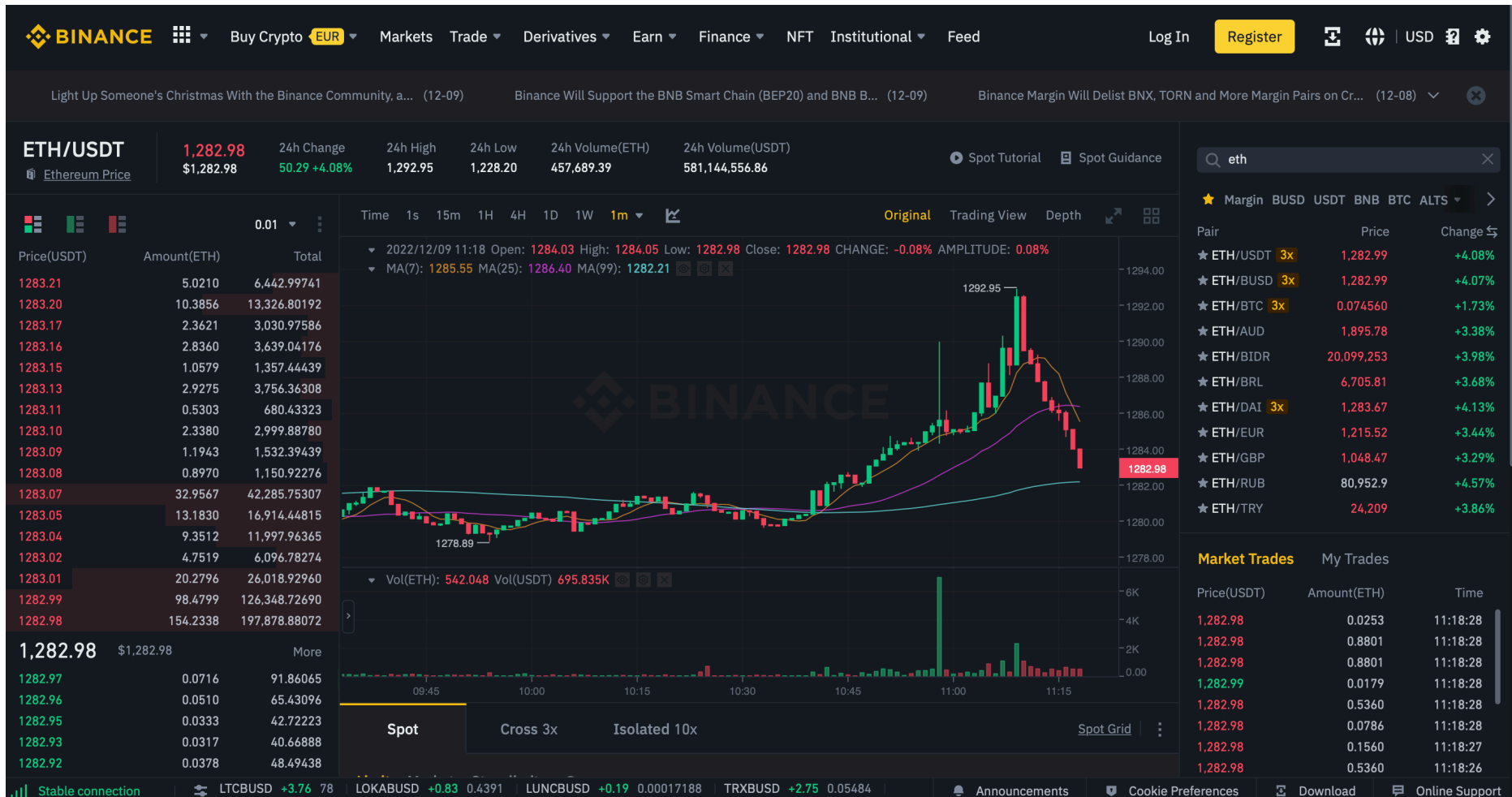
Decentralized Finance (DeFi)

- is an emerging financial technology based on **secure distributed ledgers** similar to those used by cryptocurrencies
- it offers financial instruments **without relying on intermediaries** such as brokerages, exchanges, or banks by using smart contracts on a blockchain

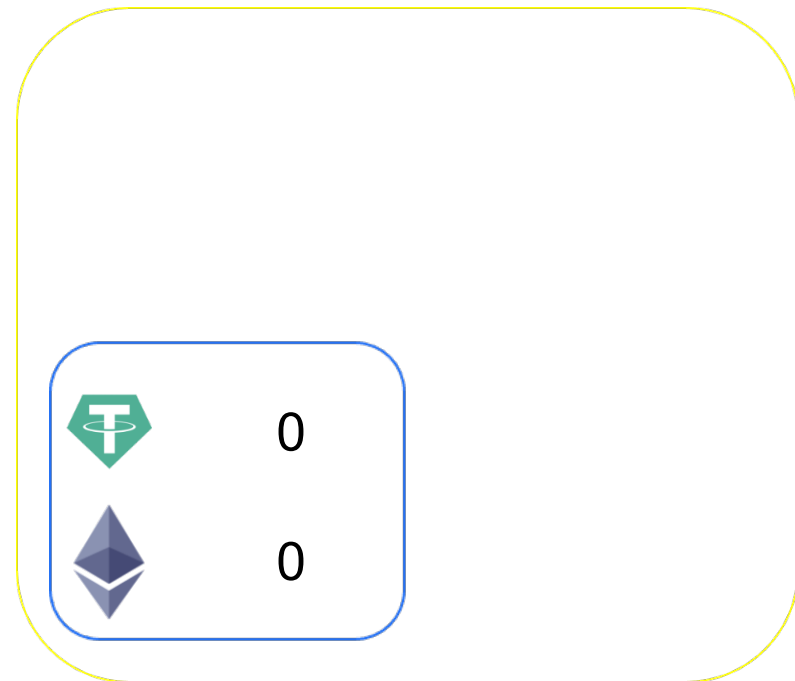
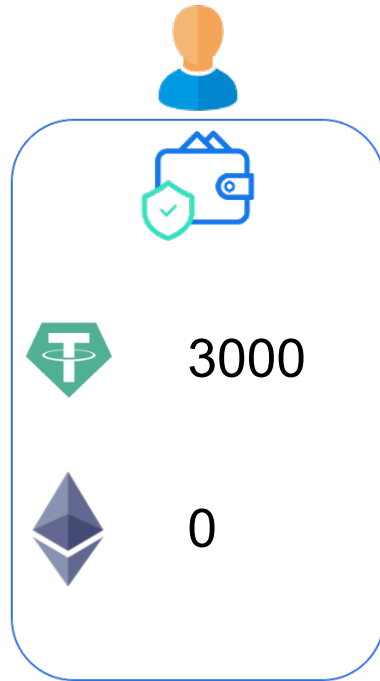
Decentralized Finance (DeFi)

- **decentralized exchanges** connect users directly (they can buy and sell tokens) without trusting an intermediary
- **lending platforms** use smart contracts to replace intermediaries such as bank that manage lending in the middle. Users deposit collateral to borrow other assets without having to sell them directly
- ***wrapped* concept**: wrapped token allow unsupported assets (non-erc20 tokens) like bitcoin to be traded, lent and borrowed on DeFi platforms (i.e. WBTC)
- **identity free**: no need for AML, KYC. DeFi is open to everyone

Centralized Exchanges (CEXs)

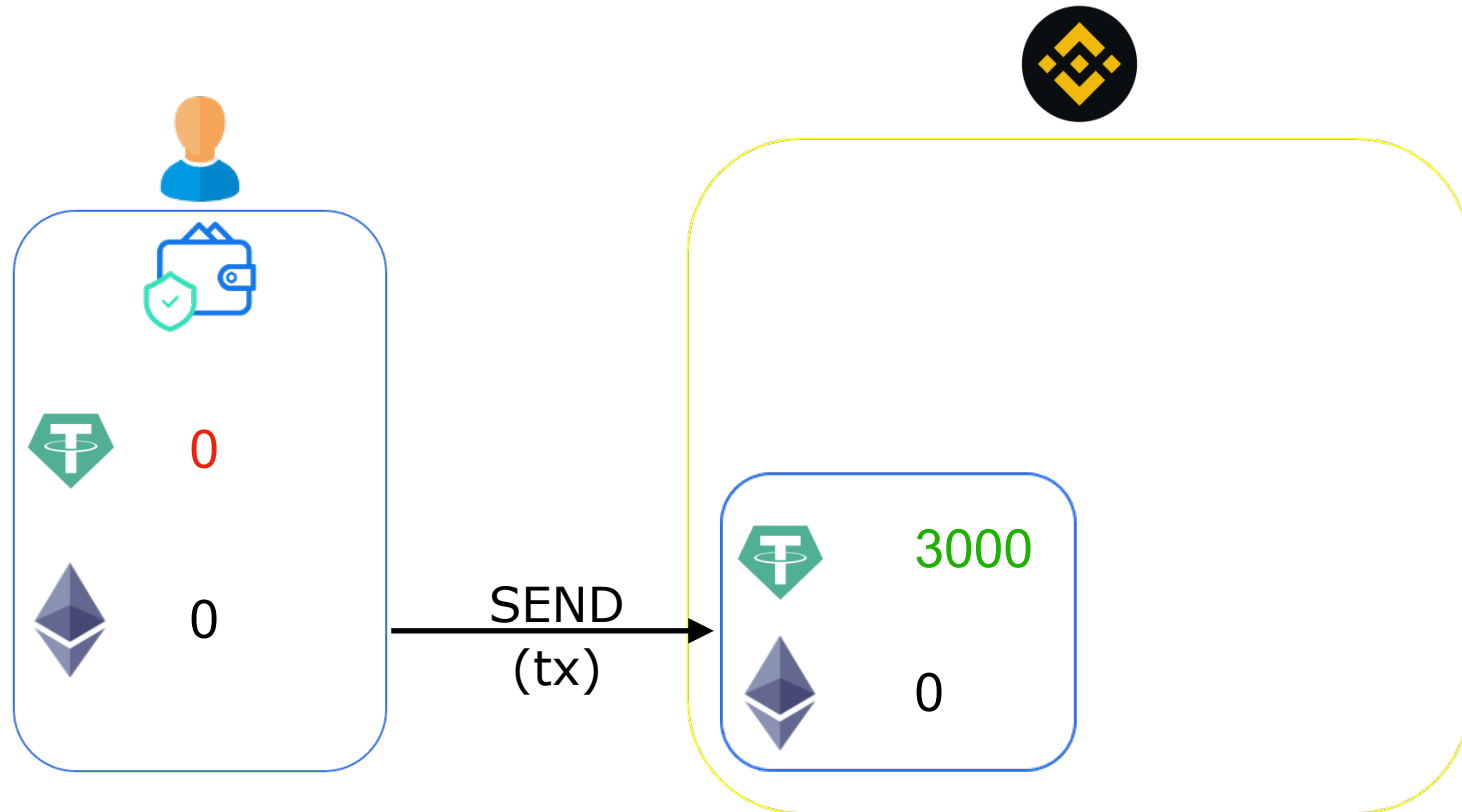


Centralized Exchanges (CEXs)



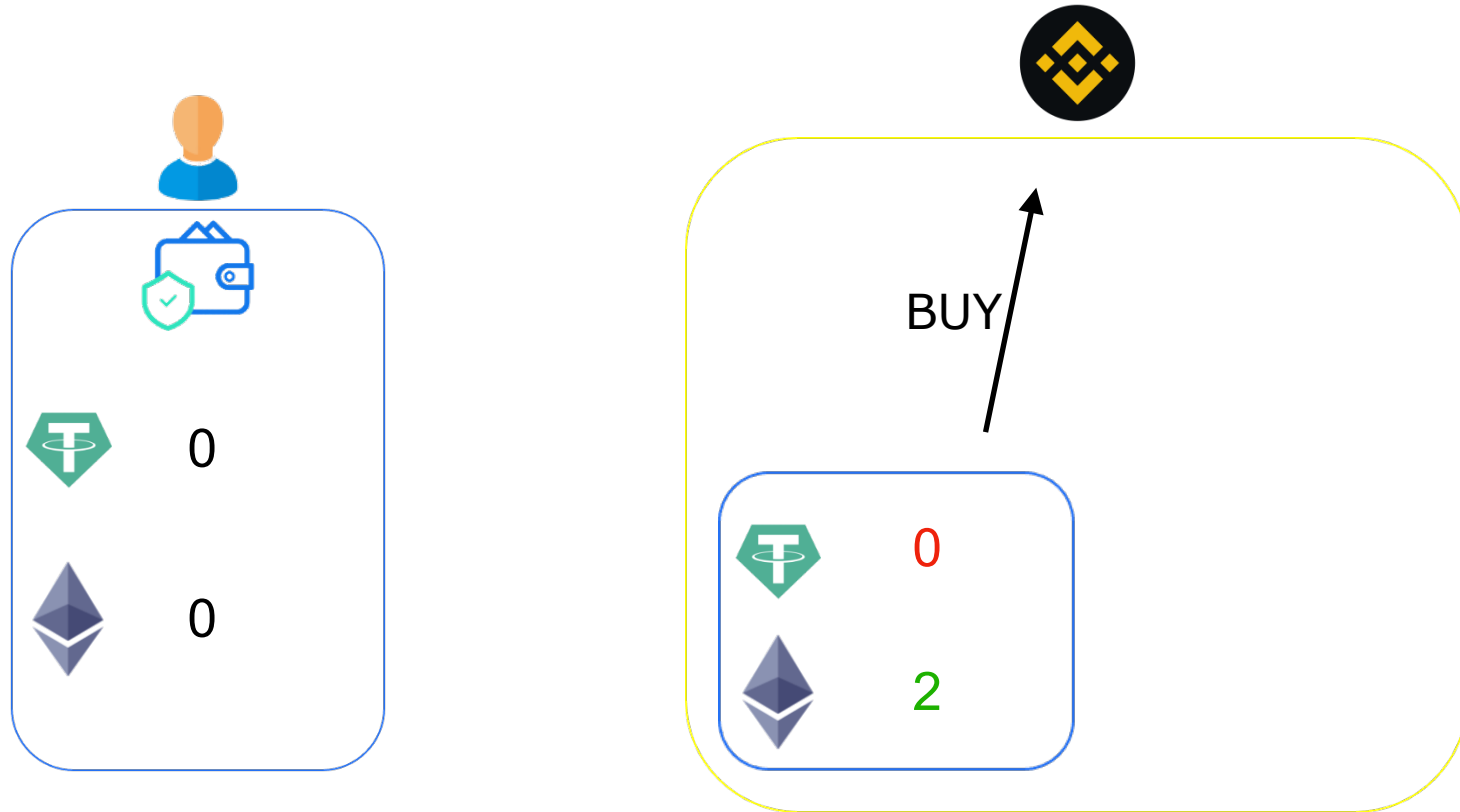
1 ETH = 1500 USDT

Centralized Exchanges (CEXs)



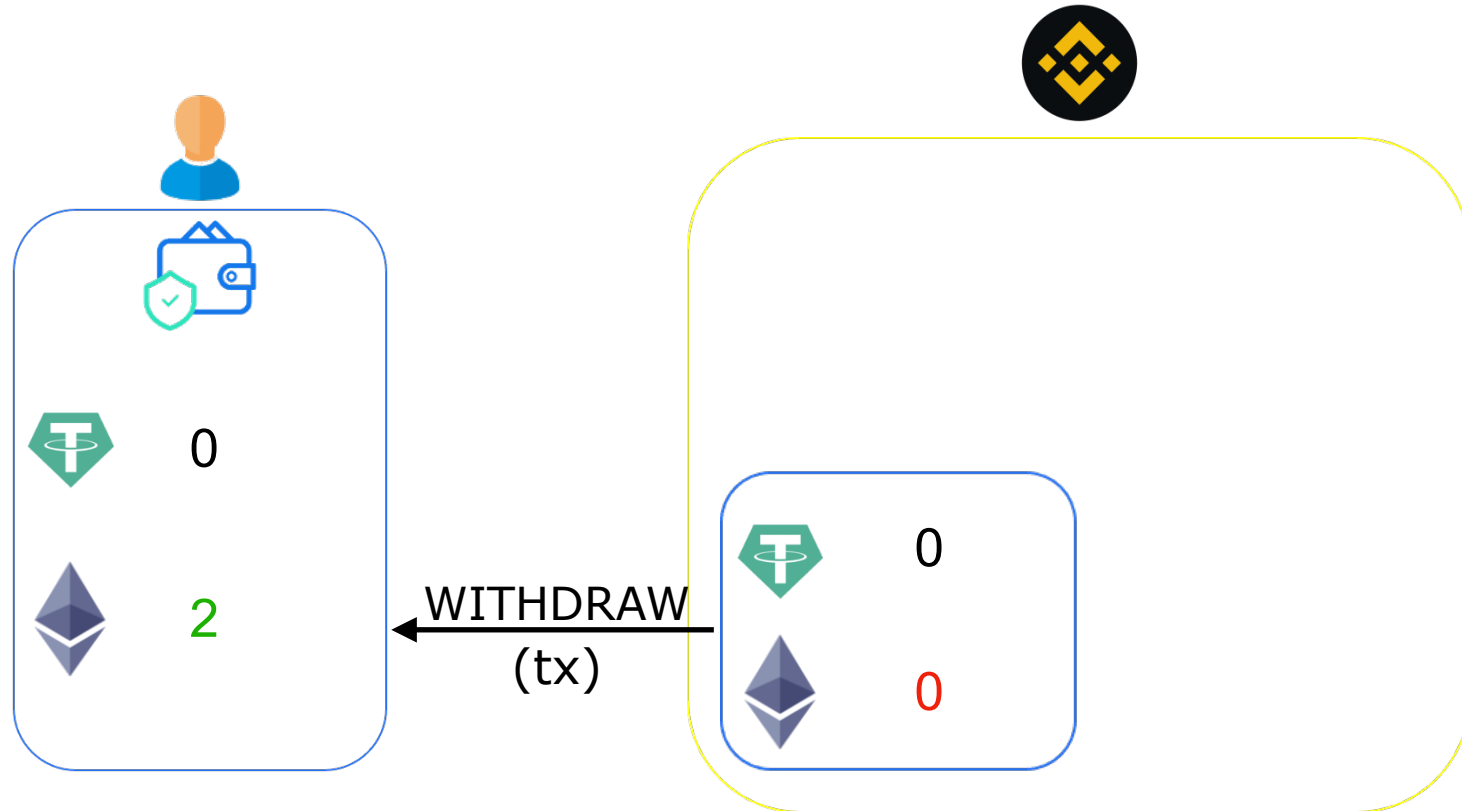
1 ETH = 1500 USDT

Centralized Exchanges (CEXs)



1 ETH = 1500 USDT

Centralized Exchanges (CEXs)



1 ETH = 1500 USDT

Centralized Exchanges (CEXs) - FTX

TECH

Cryptocurrency exchange FTX hits \$32 billion valuation despite bear market fears

PUBLISHED MON, JAN 31 2022•8:00 AM EST | UPDATED MON, JAN 31 2022•7:44 PM EST

KEY POINTS

- Bahamas-based crypto exchange FTX says it has raised \$400 million in a new round of funding.
- The deal values the company at an eye-watering \$32 billion, up from \$25 billion in October 2021.
- FTX has built up a war chest of funds at a time when crypto prices have sunk considerably.

Centralized Exchanges (CEXs) - FTX

FTX's token plunges 80% on liquidity concerns, wiping out over \$2 billion in value

Crypto exchange FTX saw \$6 bln in withdrawals in 72 hours

FTX-owned Liquid exchange pauses all trading after withdrawal halt

Bitcoin plunges to a 2-year low as FTX collapse contaminates industry

Centralized Exchanges (CEXs) - FTX

Global Cryptocurrency Charts

Total Cryptocurrency Market Cap



Global Cryptocurrency Charts

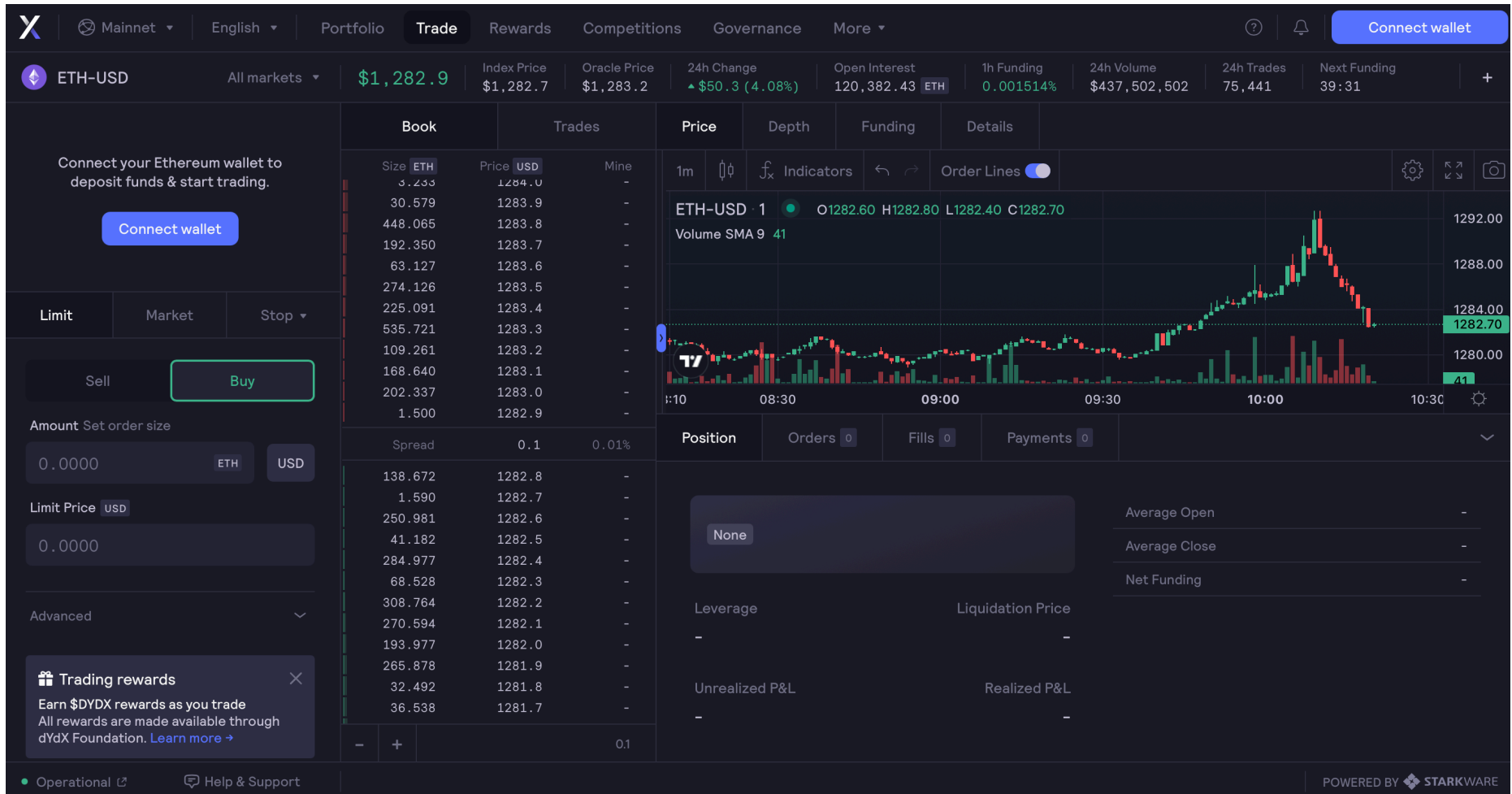
Total Cryptocurrency Market Cap



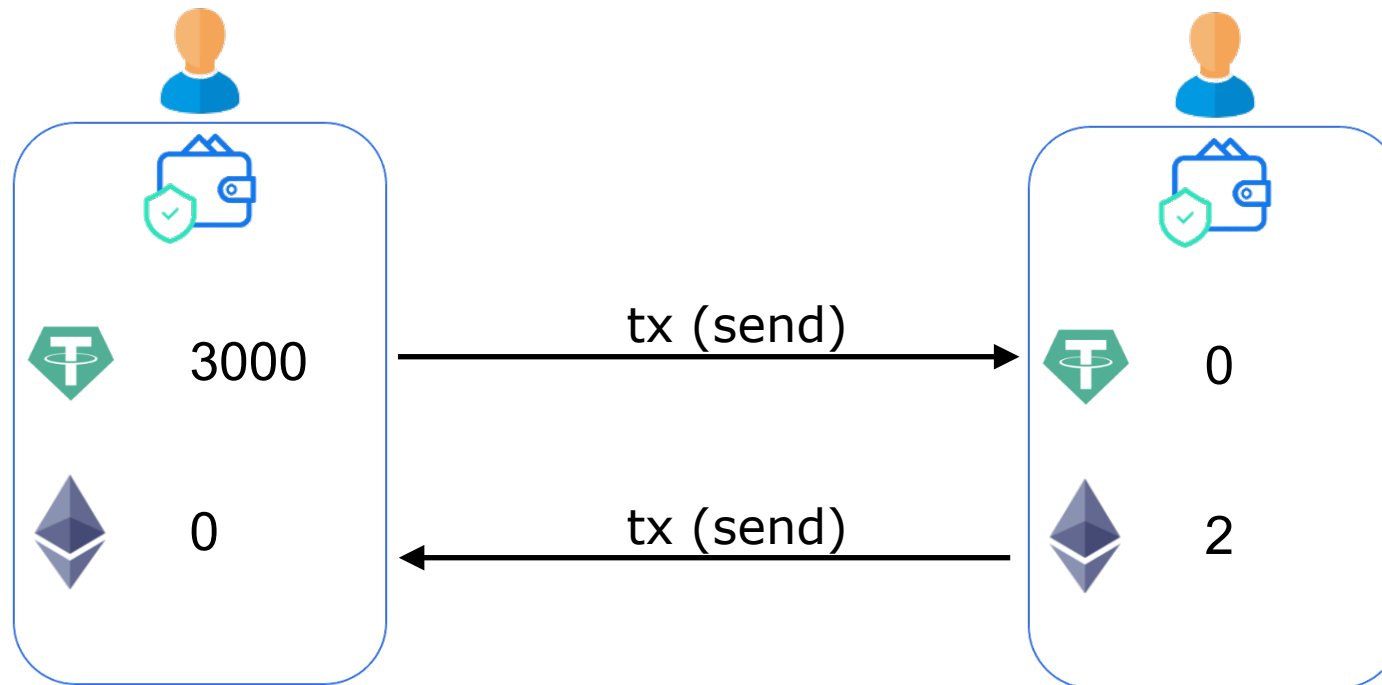
Centralized Exchanges (CEXs) - Security

- **Mt Gox** - \$8.75M in 2011
- **Mt Gox** - \$350M in 2014
- **KuCoin** - \$281M in 2020 (\$204M recovered)
- **Upbit**- \$49M in 2019 ([tx link](#))
- **Binance** - \$40M in 2019
- **Bitfinex** - \$60M in 2016
- **Cryptopia** - \$15.5M in 2019
- **Zaif** - \$60M in 2018

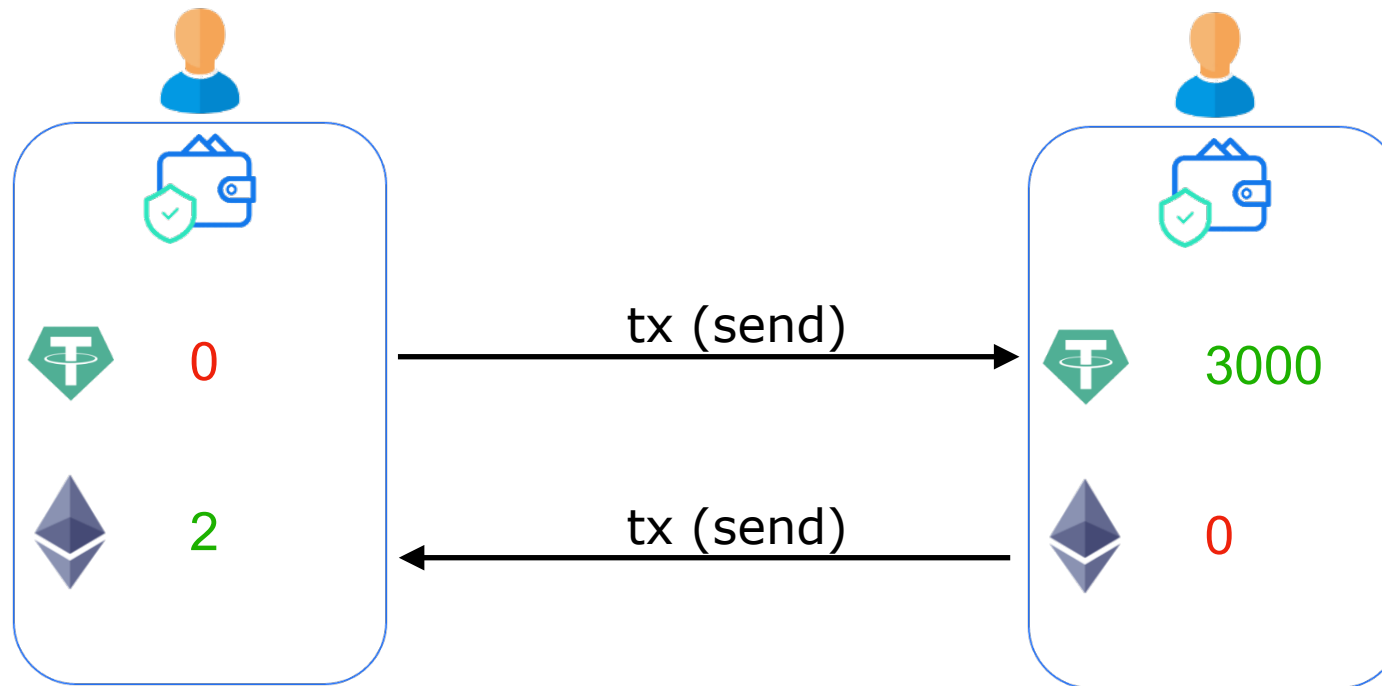
Decentralized Exchanges (DEXs)



Decentralized Exchanges (DEXs)



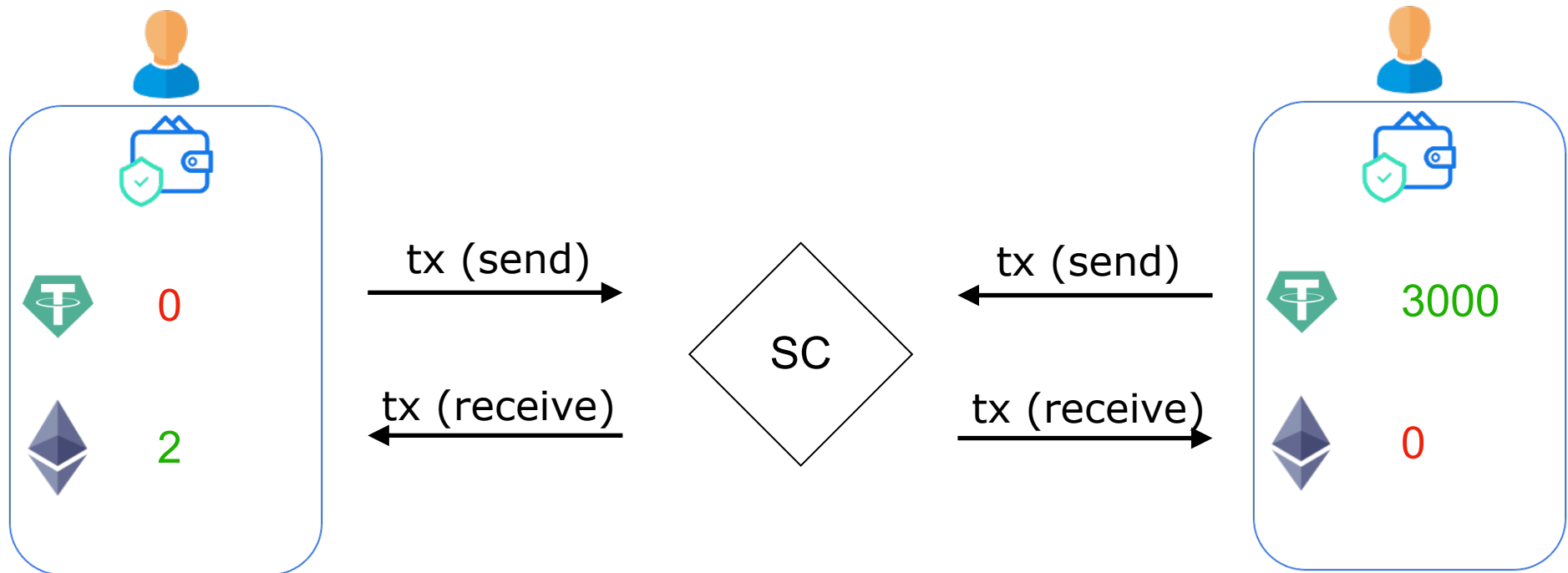
Decentralized Exchanges (DEXs)



Decentralized Exchanges (DEXs)

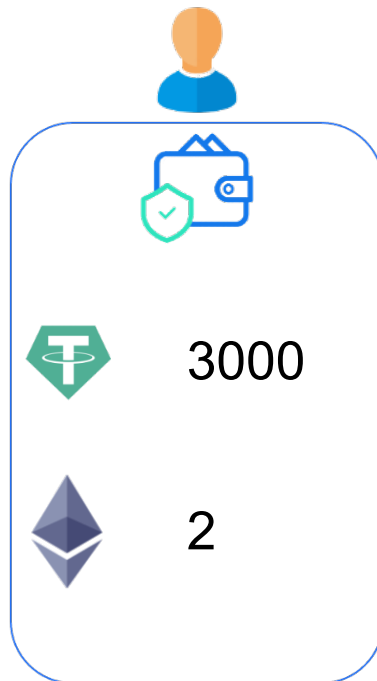
- also known as DEXs, are **peer-to-peer marketplaces** where cryptocurrency traders make transactions directly without handing over management of their funds to an intermediary or custodian
- self-custody allows one to *simply* manage his funds by using the private key to sign transactions
- users can create trading pools by providing initial liquidity since the selection of tokens is not limited to the agenda of a central entity
- Decentralized Autonomous Organizations (DAOs) ensure the project will be maintained and schedule future works and developments

Decentralized Exchanges (DEXs)



Decentralized Exchanges (DEXs)

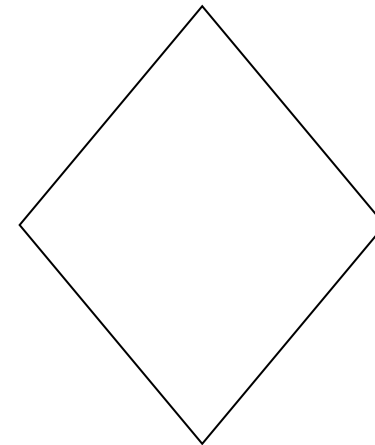
Liquidity Provider



Add Liquidity

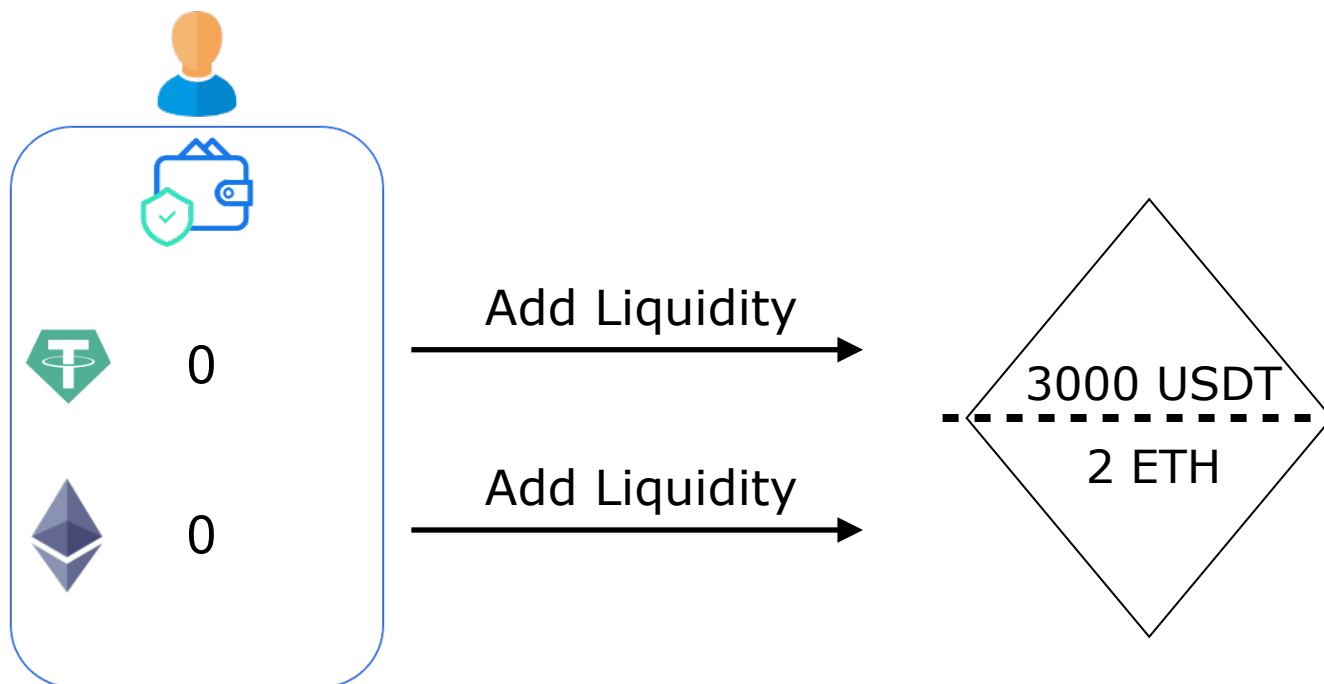


Add Liquidity



Decentralized Exchanges (DEXs)

Liquidity Provider

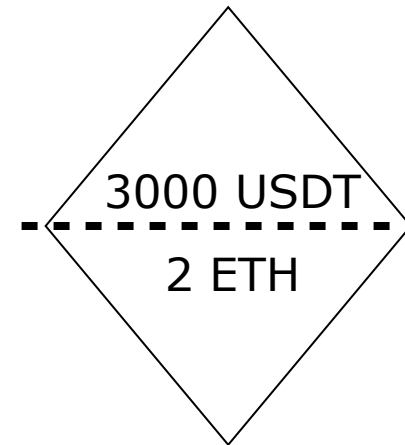
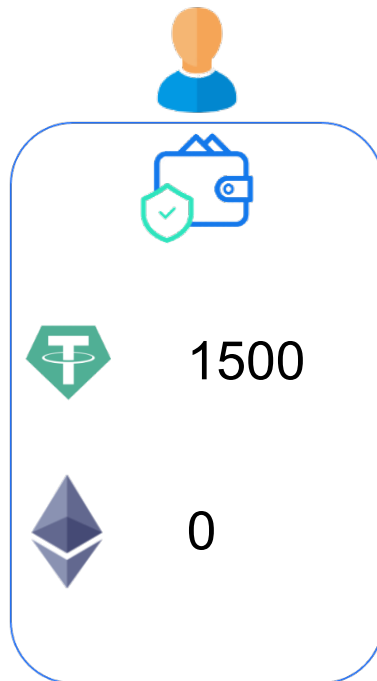


$$1 \text{ ETH} = 3000 / 2 = 1500 \text{ USDT}$$

$$1 \text{ USDT} = 2 / 3000 = 0.00067 \text{ ETH}$$

Decentralized Exchanges (DEXs)

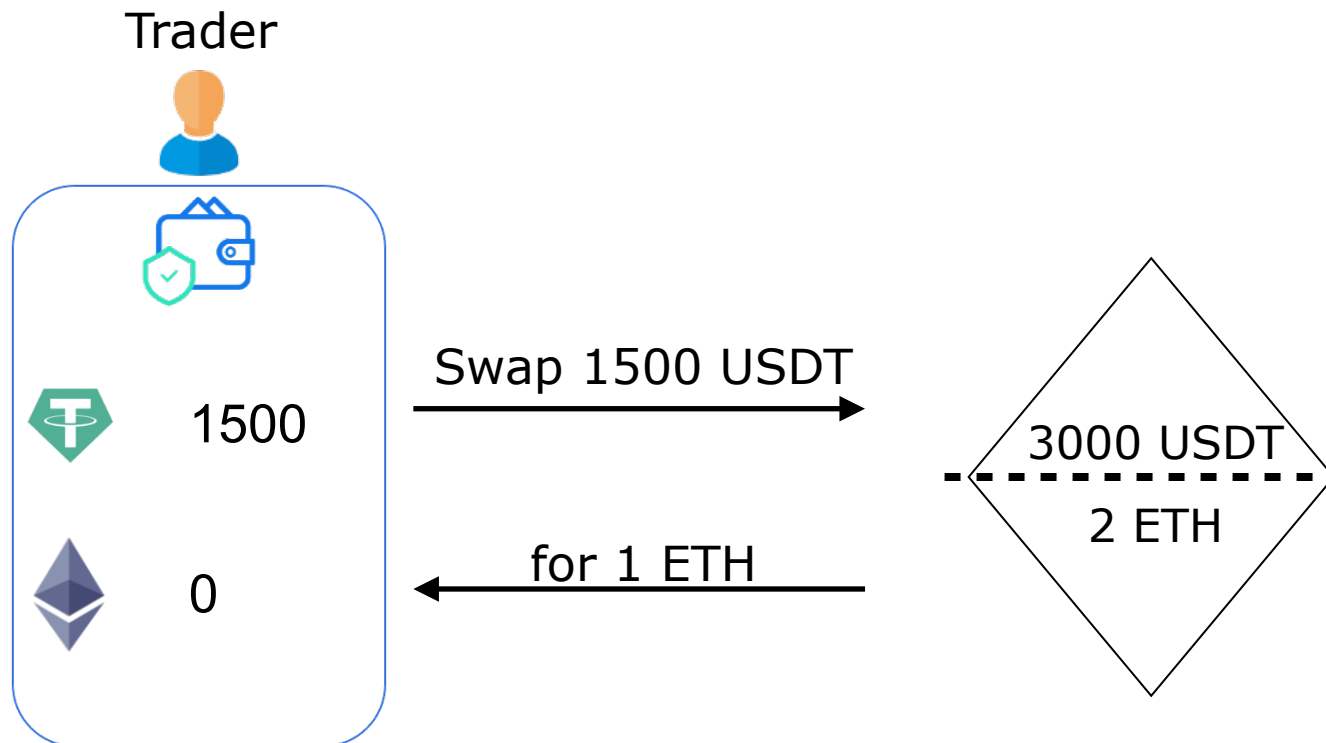
Trader



$$1 \text{ ETH} = 3000 / 2 = 1500 \text{ USDT}$$

$$1 \text{ USDT} = 2 / 3000 = 0.00067 \text{ ETH}$$

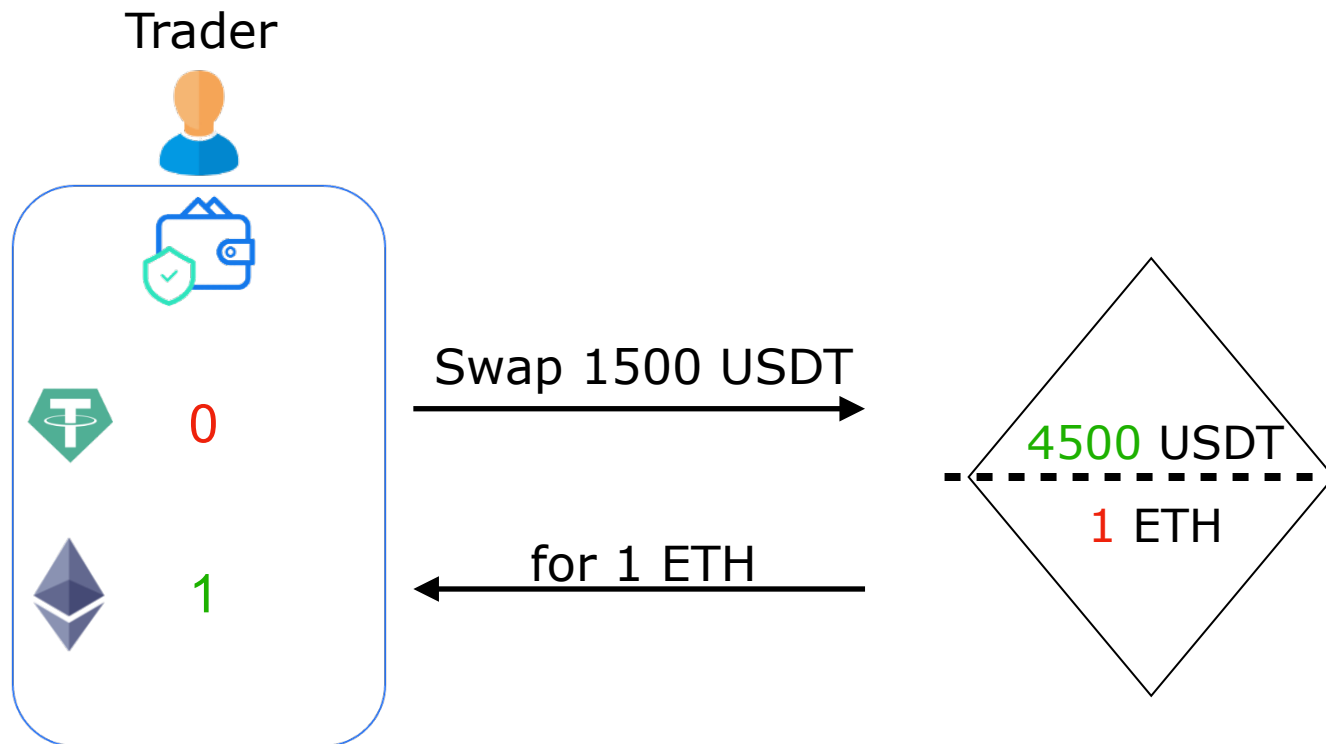
Decentralized Exchanges (DEXs)



$$1 \text{ ETH} = 3000 / 2 = 1500 \text{ USDT}$$

$$1 \text{ USDT} = 2 / 3000 = 0.00067 \text{ ETH}$$

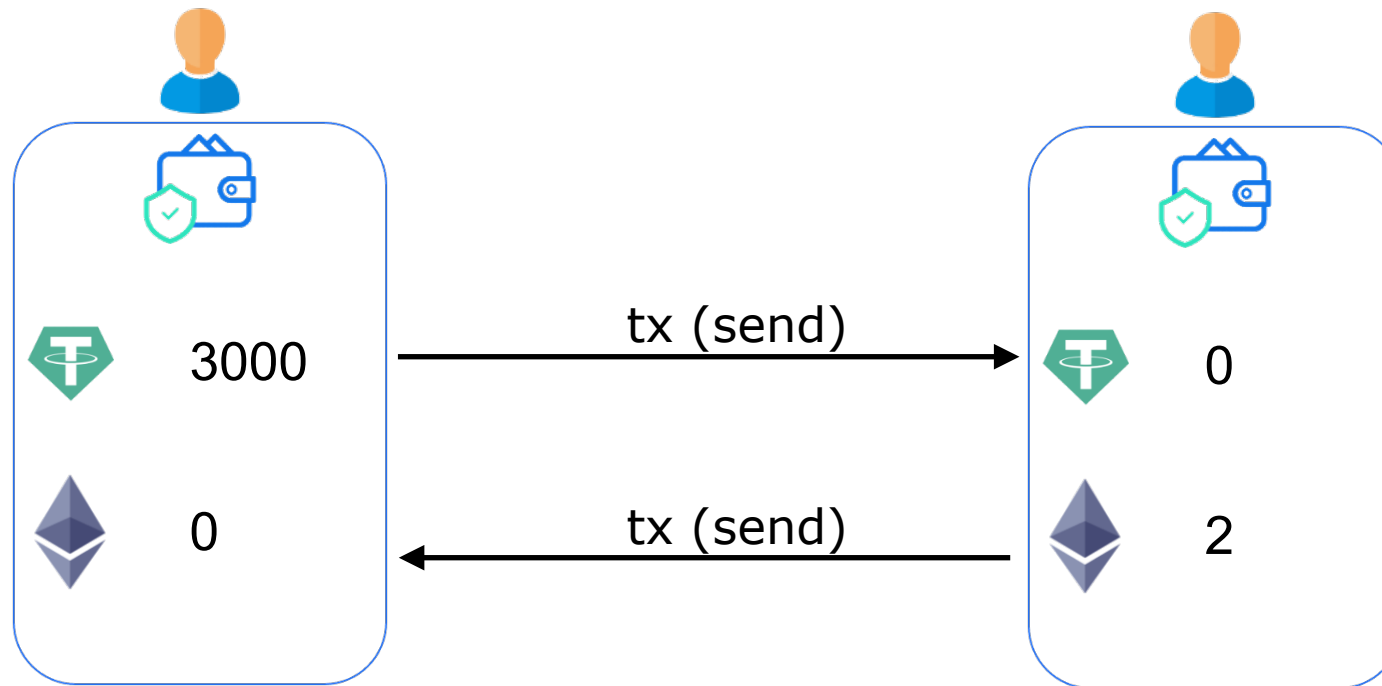
Decentralized Exchanges (DEXs)



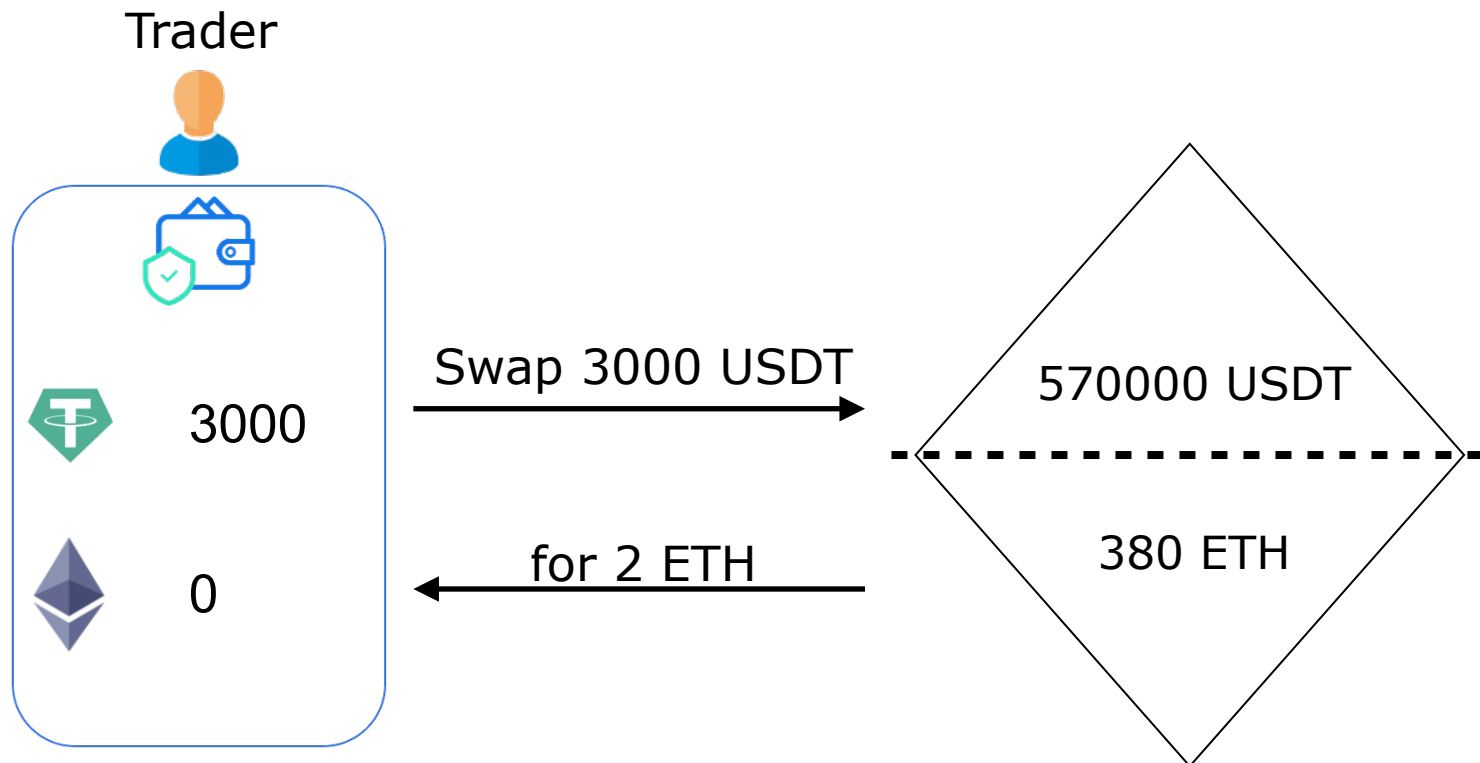
$$\cancel{1 \text{ ETH}} = 3000 / 2 = \text{1500 USDT}$$

$$\text{1 USDT} = 2 / 3000 = \cancel{0.00067 \text{ ETH}}$$

Decentralized Exchanges (DEXs)

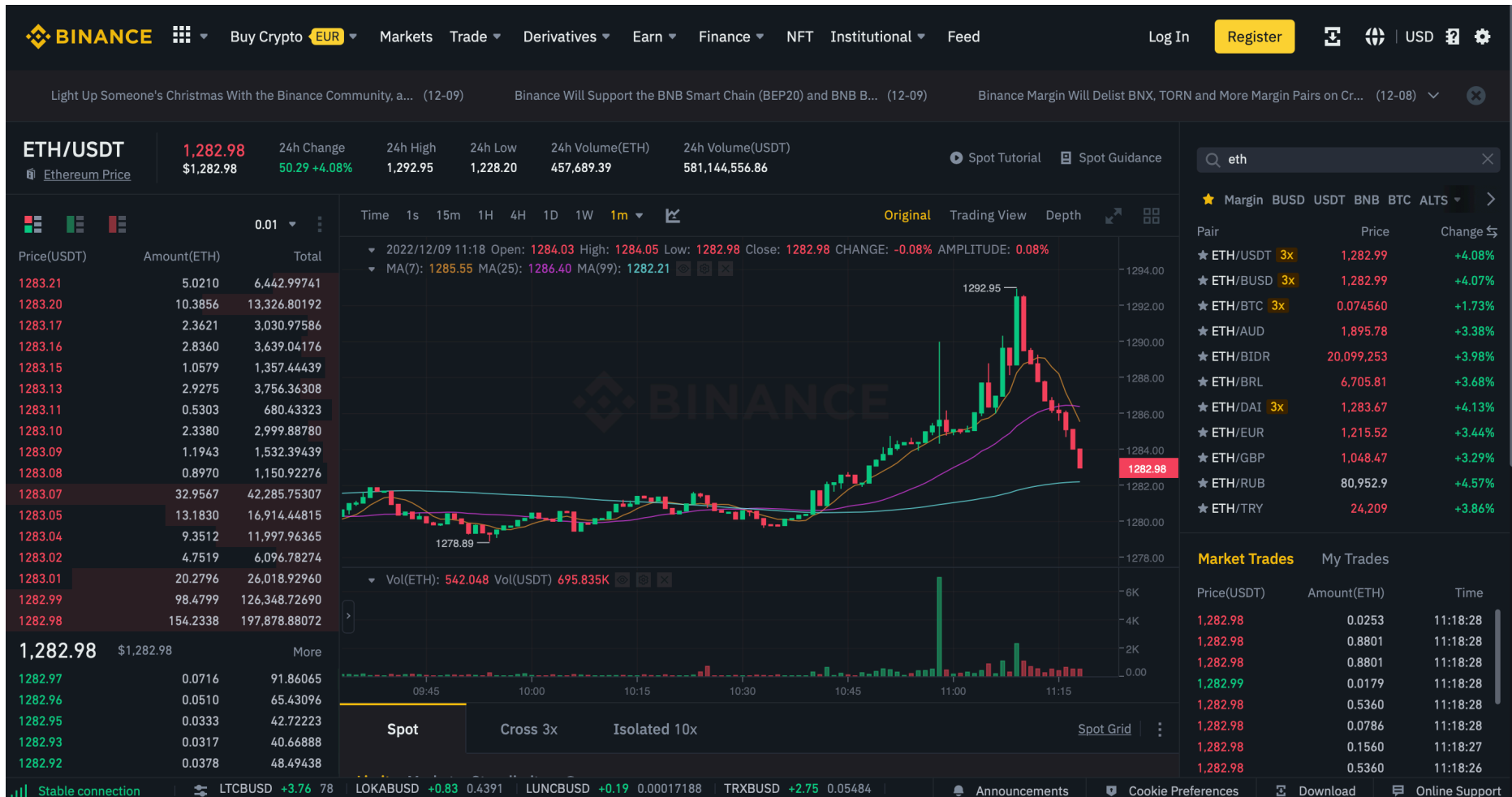


Decentralized Exchanges (DEXs)

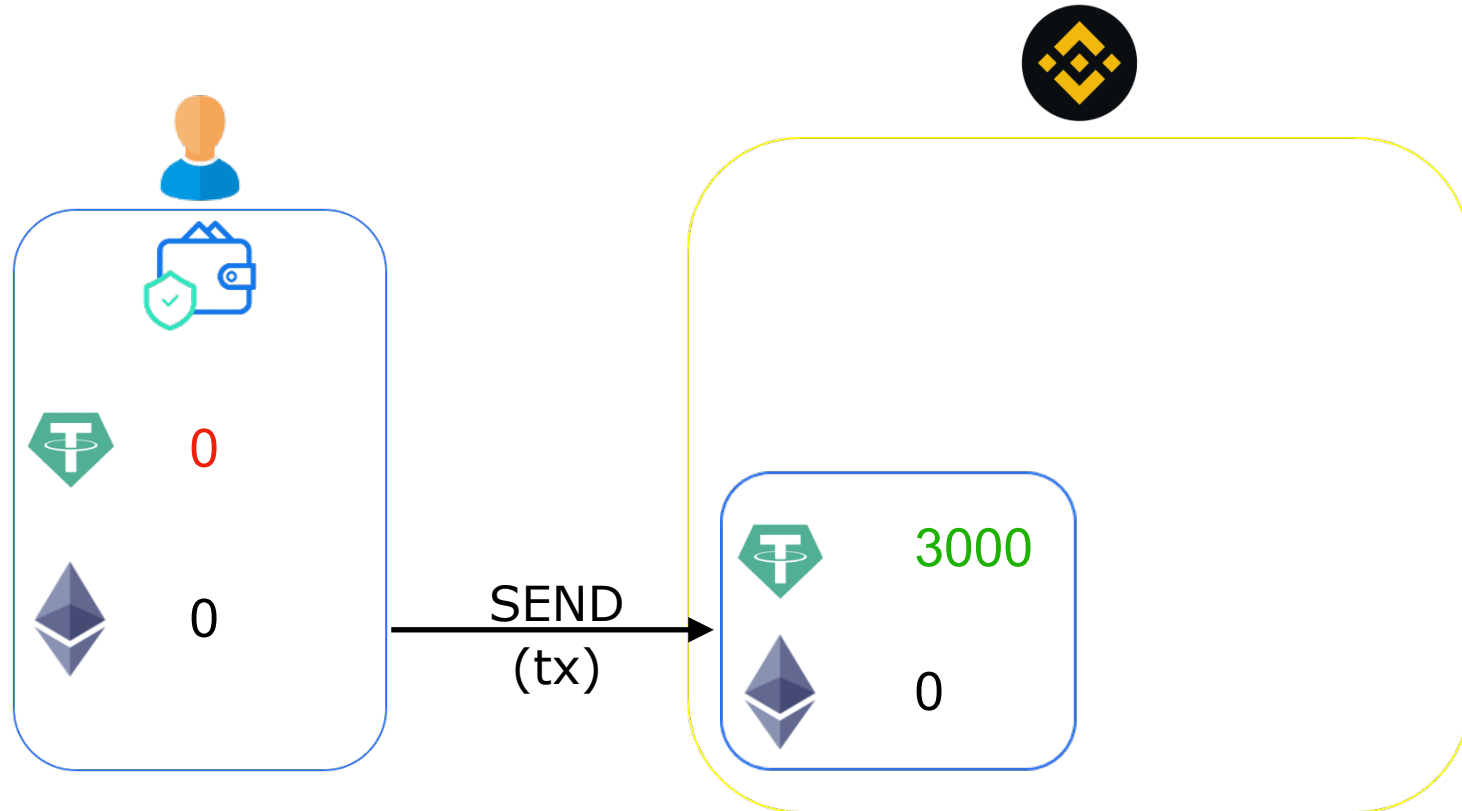


$$1 \text{ ETH} = 570000 / 380 = 1500 \text{ USDT}$$

Centralized Exchanges (CEXs)

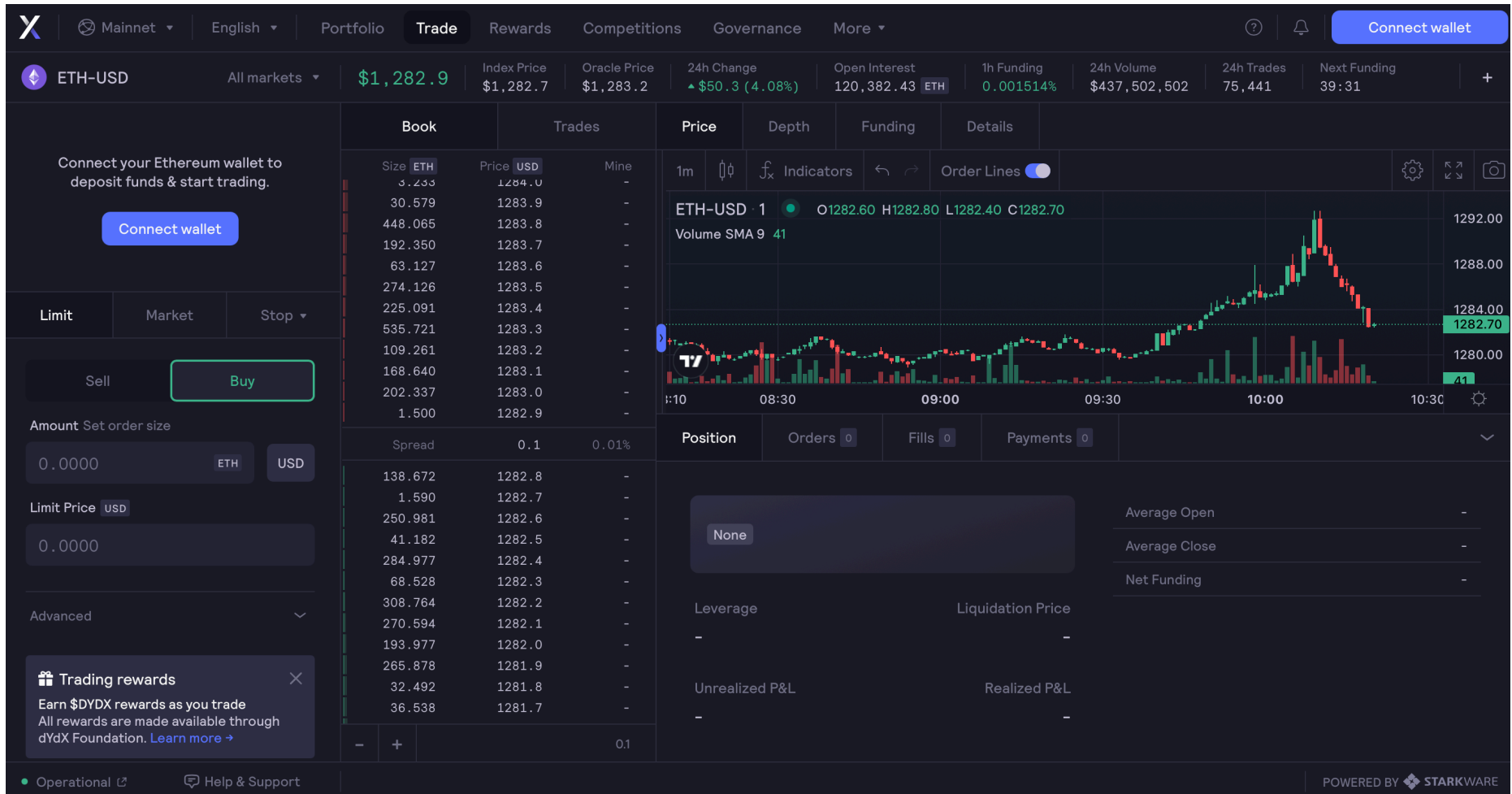


Centralized Exchanges (CEXs)

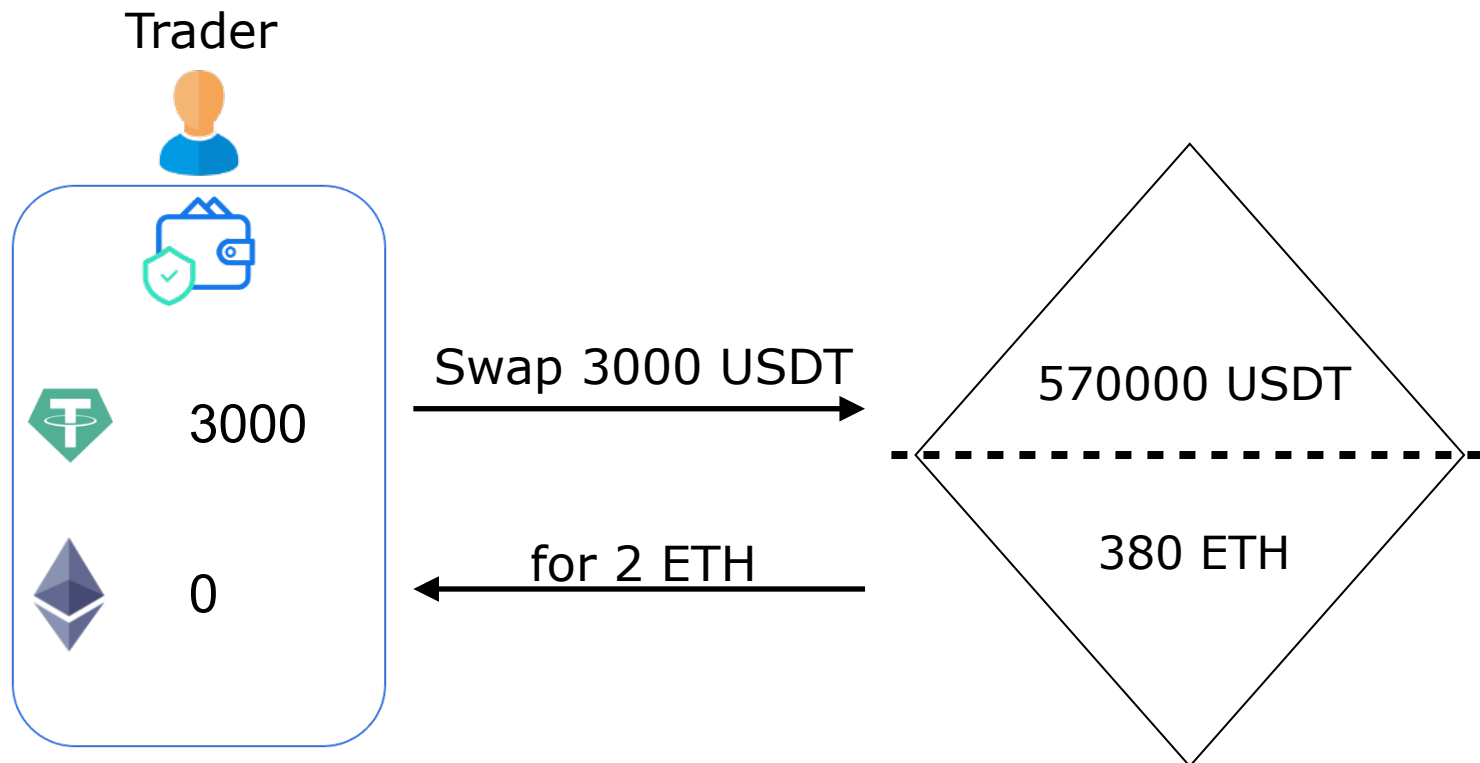


1 ETH = 1500 USDT

Decentralized Exchanges (DEXs)



Decentralized Exchanges (DEXs)



$$1 \text{ ETH} = 570000 / 380 = 1500 \text{ USDT}$$

Decentralized Finance (DeFi) - Security












- **Ronin Network**- \$620M in 2022
- **Wormhole Bridge**- \$320M in 2022
- **Nomad Bridge** - \$190M in 2022
- **Beanstalk Farm**- \$182M in 2022
- **Wintermute** - \$160M in 2022
- **Elrond** - \$113M in 2022
- **Horizon Bridge** - \$100M in 2022
- **Qubit Finance** - \$80M in 2022

Decentralized Finance (DeFi)

- **Total Value Locked (TVL)** measures the total value of all assets locked into DeFi protocols



<https://defillama.com>

Name	Category	Chains	1d Change	7d Change	1m Change	TVL	Mcap/TVL
1  MakerDAO	CDP		-1.14%	+2.09%	-16.79%	\$6.7b	0.09
2  Lido	Liquid Staking	    	-0.13%	+7.99%	-17.95%	⌚ \$6.25b	0.14
> 3  AAVE		      	+0.10%	+6.13%	-27.87%	\$3.9b	
4  Curve	Dexes	      +5	-0.48%	+5.60%	-38.11%	\$3.69b	0.12
> 5  Uniswap		    	+0.33%	-1.15%	-17.25%	\$3.5b	1.16
6  Convex Finance	Yield	 	-0.38%	+2.70%	-21.51%	⌚ \$3.05b	0.1
7  JustLend	Lending		+0.17%	+3.54%	-10.84%	\$2.84b	0.07
8  PancakeSwap	Dexes	  	+13.64%	-0.82%	-13.24%	\$2.84b	0.21
> 9  Compound Finance			+0.85%	+3.72%	-24.02%	\$1.74b	
10  Instadapp	Services		+0.45%	+6.93%	-20.07%	⌚ \$1.71b	0.01
11  Balancer	Dexes	  	+0.42%	+4.94%	-17.99%	\$1.52b	0.15
> 12  Frax Finance		      +2	-0.28%	+3.12%	+1.46%	⌚ \$1.23b	
13  Coinbase Wrapped S...	Liquid Staking		-0.20%	+9.63%	-10.19%	⌚ \$1.17b	

<https://defillama.com>

Decentralized Finance (DeFi)



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price
					380	570k	1500 USDT
Alice	2	50k					
Bob	2	50k					
Eve	2	50k					

Decentralized Finance (DeFi)



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price
					380	570k	1500 USDT
Alice	2	50k	15k USDT	10 ETH	370	585k	1581 USDT
Bob	2	50k					
Eve	2	50k					

Decentralized Finance (DeFi)



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price
					380	570k	1500 USDT
Alice	12	35k	15k USDT	10 ETH	370	585k	1581 USDT
Bob	2	50k					
Eve	2	50k					

Decentralized Finance (DeFi)



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price
					380	570k	1500 USDT
Alice	12	35k	15k USDT	10 ETH	370	585k	1581 USDT
Bob	2	50k	15k USDT	9.48 ETH	360.5	600k	1664 USDT
Eve	2	50k					

Decentralized Finance (DeFi)



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price
					380	570k	1500 USDT
Alice	12	35k	15k USDT	10 ETH	370	585k	1581 USDT
Bob	11.48	35k	15k USDT	9.48 ETH	360.5	600k	1664 USDT
Eve	2	50k					

Decentralized Finance (DeFi)



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price
					380	570k	1500 USDT
Alice	12	35k	15k USDT	10 ETH	370	585k	1581 USDT
Bob	11.48	35k	15k USDT	9.48 ETH	360.5	600k	1664 USDT
Eve	2	50k	15k USDT	9.01 ETH	351.49	615k	1749 USDT

Decentralized Finance (DeFi)



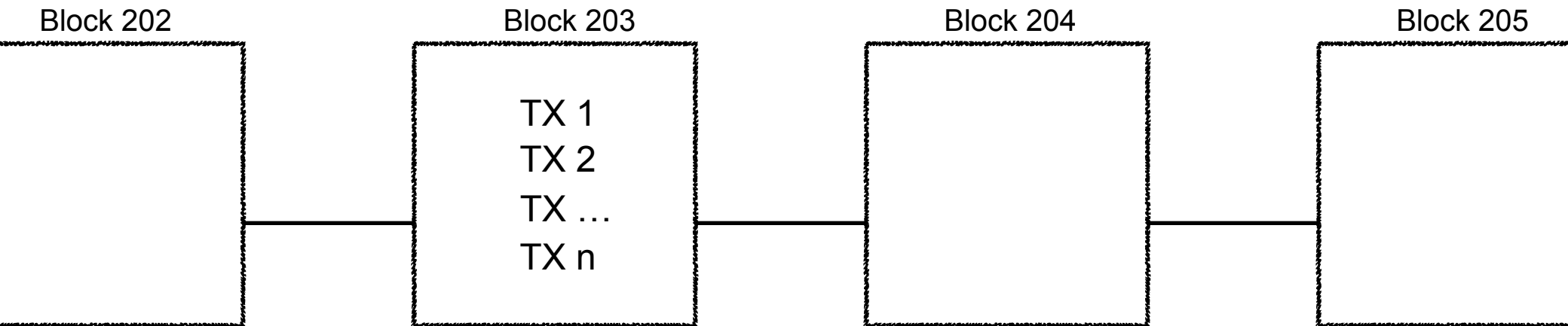
User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price
					380	570k	1500 USDT
Alice	12	35k	15k USDT	10 ETH	370	585k	1581 USDT
Bob	11.48	35k	15k USDT	9.48 ETH	360.5	600k	1664 USDT
Eve	11.01	35k	15k USDT	9.01 ETH	351.49	615k	1749 USDT

Decentralized Finance (DeFi)



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price
					380	570k	1500 USDT
Alice	12	35k	15k USDT	10 ETH	370	585k	1581 USDT
Bob	11.48	35k	15k USDT	9.48 ETH	360.5	600k	1664 USDT
Eve	11.01	35k	15k USDT	9.01 ETH	351.49	615k	1749 USDT

Ethereum transactions execution order



Ethereum **V**irtual **M**achine (EVM) always processes transactions **sequentially**

Decentralized Finance (DeFi)



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Alice	12	35k	15k USDT	10 ETH	370	585k	1581 USDT	15 GWEI
Bob	11.48	35k	15k USDT	9.48 ETH	360.5	600k	1664 USDT	11 GWEI
Eve	11.01	35k	15k USDT	9.01 ETH	351.49	615k	1749 USDT	3 GWEI

Ethereum transactions execution order

- including transactions: a user provides **higher fees** than others and his transaction will jump to the first position in order to be executed as soon as possible
- excluding transactions: as a *validator*, one may exclude transactions from being propagated to the p2p network, by **replacing** them with new self-made transactions (i.e. they where profitable)
- reordering transactions: order matters. Transactions change state of pools, protocols, balances and open up to **new profitable opportunities**

Maximal Extractable Value (MEV)

- maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding and changing the order of the transactions in a block
- MEV techniques: front-running, back-running, sandwich attacks

Maximal Extractable Value (MEV)

<https://txstreet.com/v/eth-btc>

Maximal Extractable Value (MEV) - Front-running attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Alice	2	50k						
Bob	2	50k						

Maximal Extractable Value (MEV) - Front-running attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Alice	2	50k	45k USDT	30 ETH	350	615k	1757 USDT	5 GWEI
Bob	2	50k						

Maximal Extractable Value (MEV) - Front-running attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Alice	2	50k	45k USDT	30 ETH	350	615k	1757 USDT	5 GWEI
Bob	2	50k	3000k USDT					6 GWEI

Maximal Extractable Value (MEV) - Front-running attack



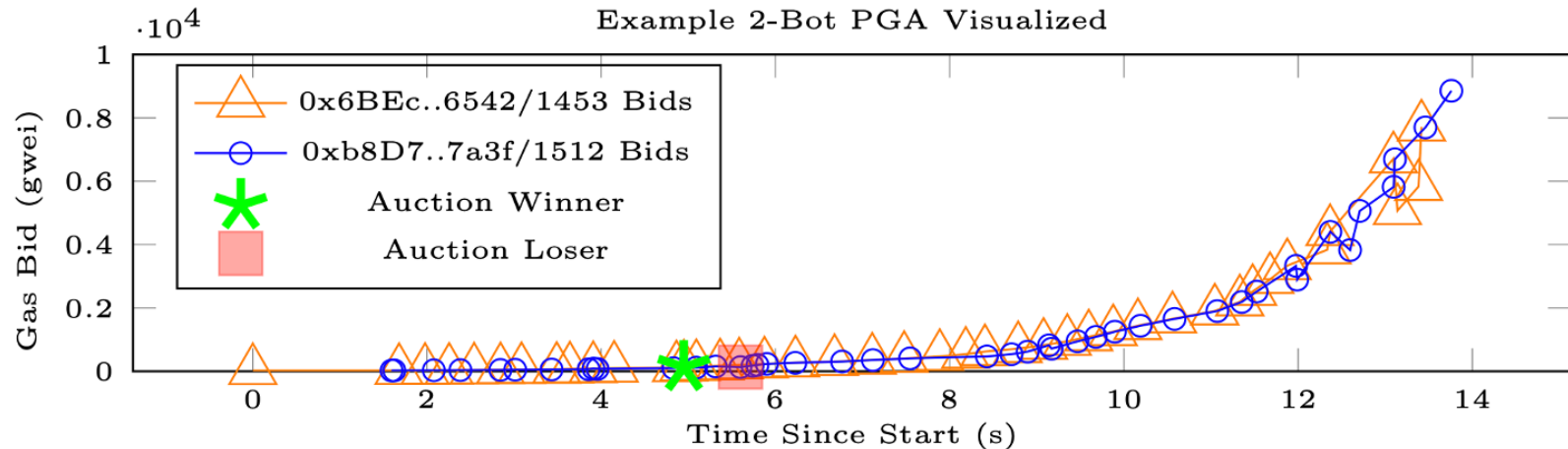
User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Bob	2	50k	3000k USDT	2 ETH	352	573k	1627 USDT	6 GWEI
Alice	2	50k	45k USDT	30 ETH	350	615k	1757 USDT	5 GWEI

Maximal Extractable Value (MEV) - Front-running attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Bob	2	50k	3000k USDT	2 ETH	352	573k	1627 USDT	6 GWEI
Alice	2	50k	45k USDT	27 ETH	325	618k	1901 USDT	5 GWEI

Maximal Extractable Value (MEV) - Front-running attack



Seconds Elapsed	Quantity @ Price Bid	Ethereum Transaction Origin (Public Key Hash)	Nonce	Transaction Hash
0.000	192085 @ 25.10	0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542	1453	0xd32653ca9694a6d1299335f3c04f74cc159bee48c1d32d3a421db08c638ffc78
1.593	231520 @ 25.00	0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f	1512	0xb901e6dc2c229fd9105448fcc23eabdedb476c21b6c6e7ddf82df4e838d2c7
1.624	231520 @ 28.75	0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f	1512	0x9f592504eb71a7452b7a395a7f5ecd34eaa5d090da1162e74221562af54c8f67
1.679	227534 @ 28.81	0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542	1453	0x83e2a6774654a9540c3fad8837afcc88b4c932ab2374819254f887305c3a4b22
...
4.949	227534 @ 134.02	0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542	1453	0xc889bd13594f75e4dd824f04f0c2ad03896cb7ec6518df02455e9560367bb9c4
5.599	231520 @ 133.76	0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f	1512	0xaa86d782328c0c9c422e3f2a3170ff41ae21a27ad395c48db76b0080898f85db
...
13.383	227534 @ 5834.77	0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542	1453	0xb0dc97140394c5f65332ebc459d5e66f89099dbb4d335c866b32280270102858
13.416	227534 @ 7716.48	0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542	1453	0x1825be6951577e72a1dafc8de564ce1ccfe5d284173e11e77b2e7f6b1b44571c
13.462	231520 @ 7701.08	0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f	1512	0xa9823358c99149f0e6343c604c35988468d01d02868437d8251b3cee282dc92b
m13.759	231520 @ 8856.24	0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f	1512	0x366c30a534b5f3d8a6d251f97d401997624d1fe8d3af07ede4d19105dc970942

Fig. 2. One example PGA that was observed over the Ethereum peer-to-peer network, resulting from the profit opportunity in Figure 1. The top graph shows the gas bids of two observed bots over time, while the bottom table details the first and last two bids placed by each bot and the two mined bids (center).

Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges

Maximal Extractable Value (MEV) - Back-running attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Alice	2	50k						
Bob	2	50k						

Maximal Extractable Value (MEV) - Back-running attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Alice	2	50k	45k USDT	30 ETH	350	615k	1757 USDT	5 GWEI
Bob	2	50k						

Maximal Extractable Value (MEV) - Back-running attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Alice	2	50k	45k USDT	30 ETH	350	615k	1757 USDT	5 GWEI
Bob	2	50k	2 ETH					

Maximal Extractable Value (MEV) - Back-running attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Alice	2	50k	45k USDT	30 ETH	350	615k	1757 USDT	5 GWEI
Bob	2	50k	2 ETH	3514 USDT				

Maximal Extractable Value (MEV) - Back-running attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Alice	2	50k	45k USDT	30 ETH	350	615k	1757 USDT	5 GWEI
Bob	2	50k	2 ETH	3514 USDT	-	-	-	4 GWEI

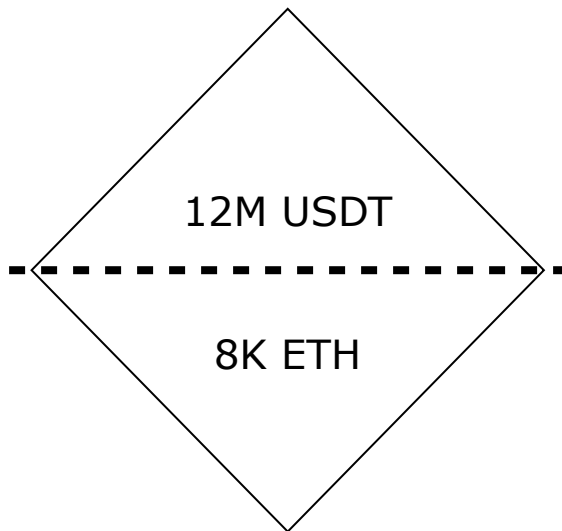
Maximal Extractable Value (MEV) - Sandwich attack



User	Balance ETH	Balance USDT	Amount In	Amount Out	Balance ETH	Balance USDT	ETH Price	Fees
					380	570k	1500 USDT	
Bob	2	50k	3000k USDT	2 ETH	352	573k	1627 USDT	6 GWEI
Alice	2	50k	45k USDT	27 ETH	325	618k	1901 USDT	5 GWEI
Bob	2	50k	2 ETH	3802 USDT	327	614k	1878 USDT	4 GWEI

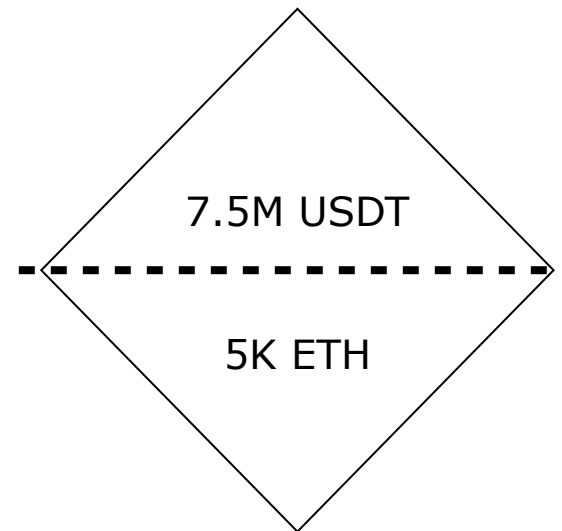
Maximal Extractable Value (MEV) - Arbitrages

Pool A



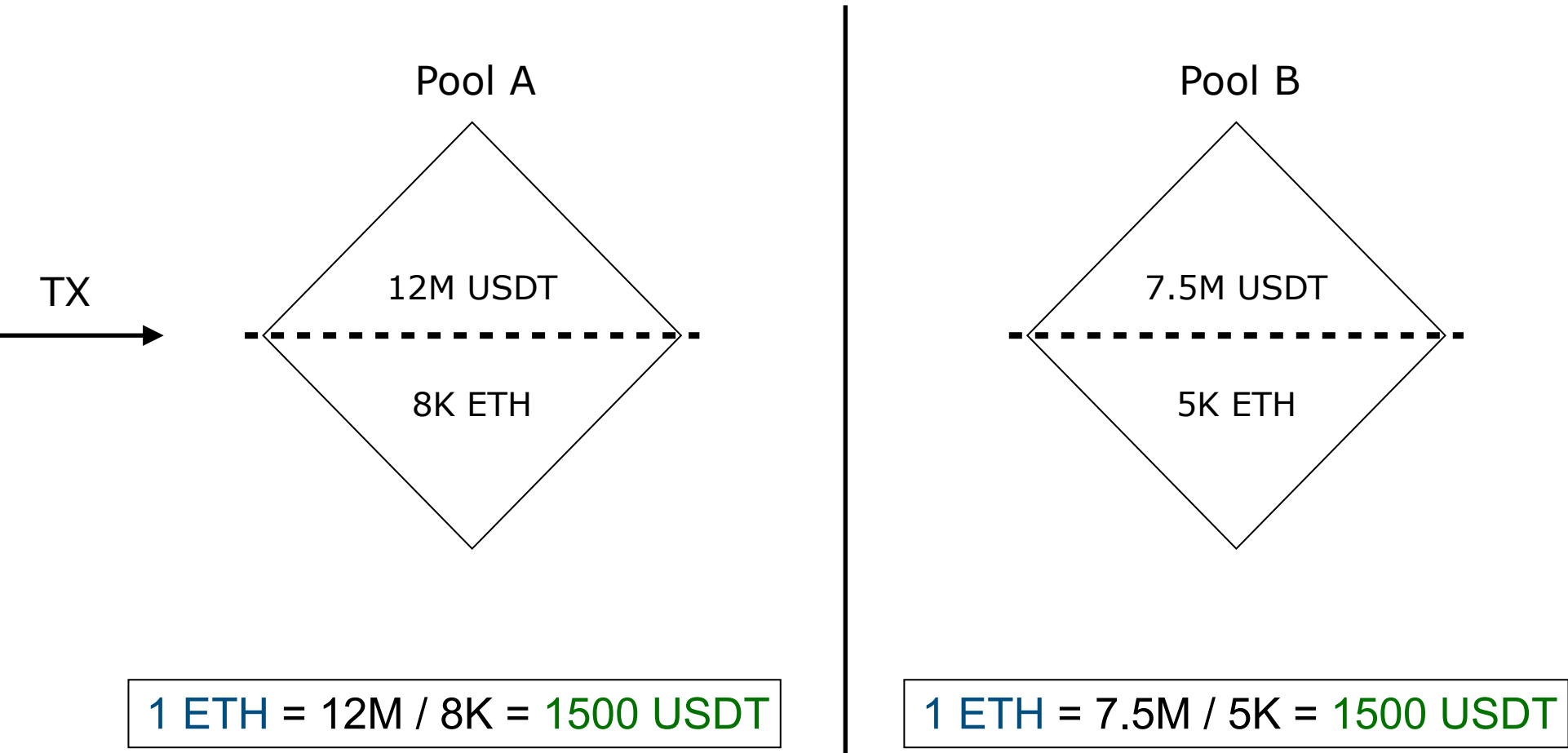
$$1 \text{ ETH} = 12\text{M} / 8\text{K} = 1500 \text{ USDT}$$

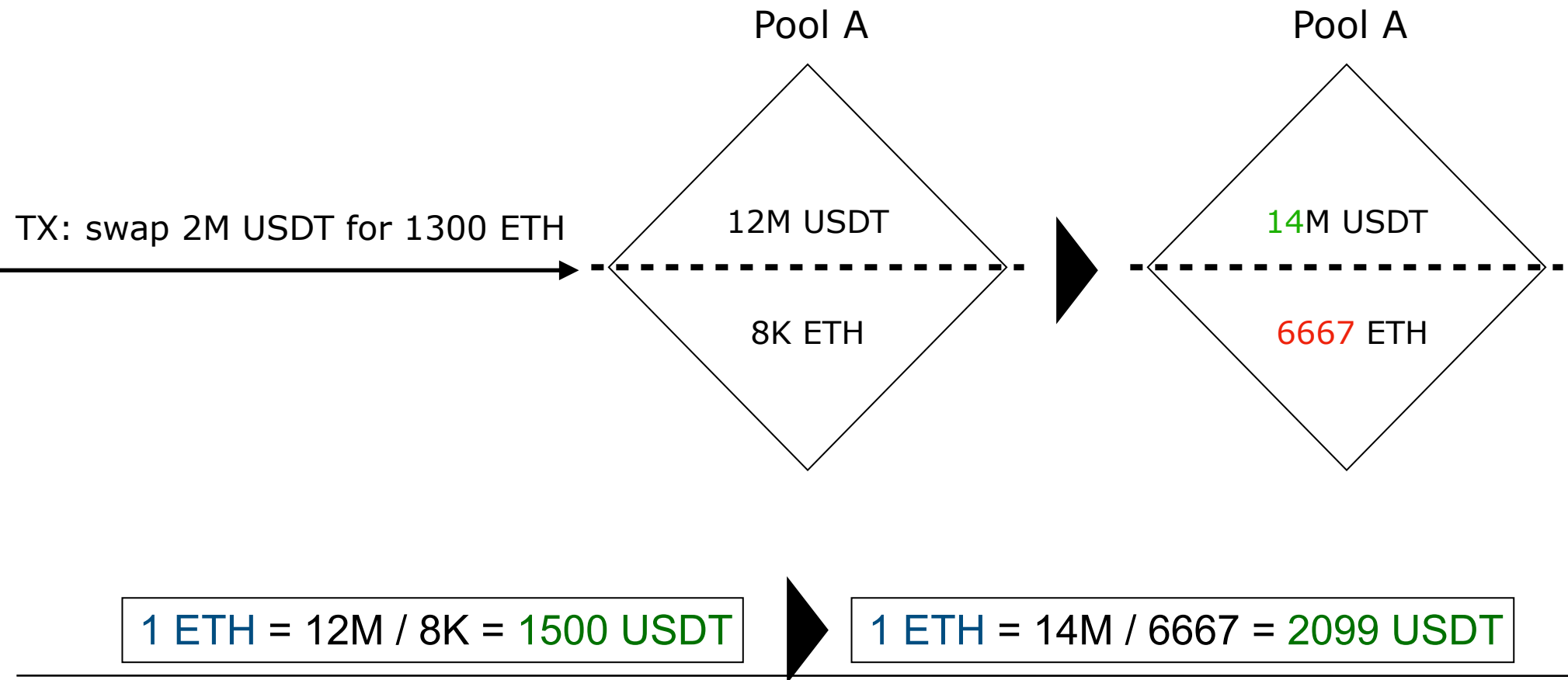
Pool B



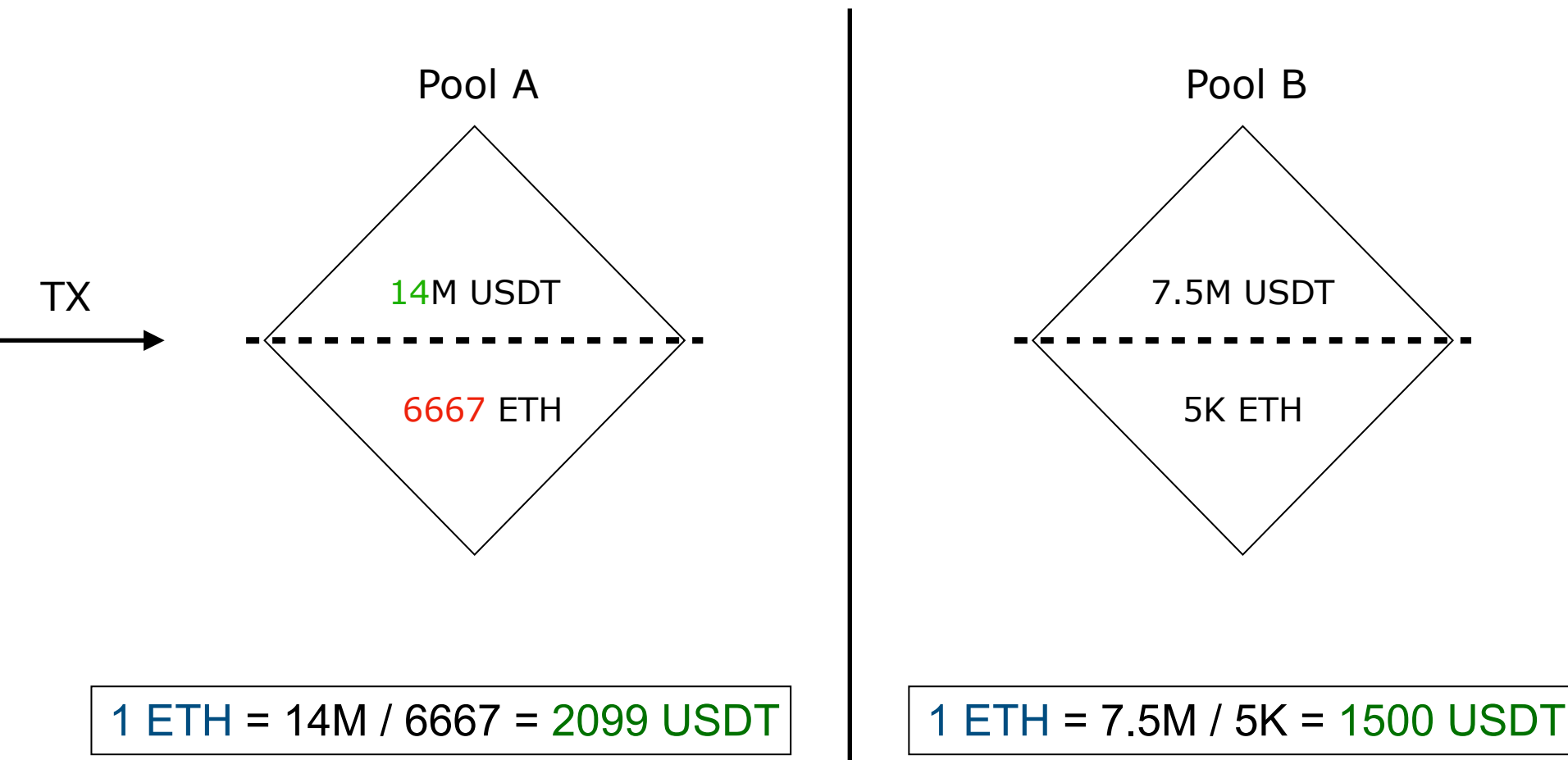
$$1 \text{ ETH} = 7.5\text{M} / 5\text{K} = 1500 \text{ USDT}$$

Maximal Extractable Value (MEV) - Arbitrages





Maximal Extractable Value (MEV) - Arbitrages



Maximal Extractable Value (MEV) - Arbitrages

Alice TX: swap 2M USDT for 1300 ETH (pool A)



Bob TX: swap 1500 USDT for 1 ETH (pool A)



Bob TX: swap 1 ETH for 2099 USDT (pool B)

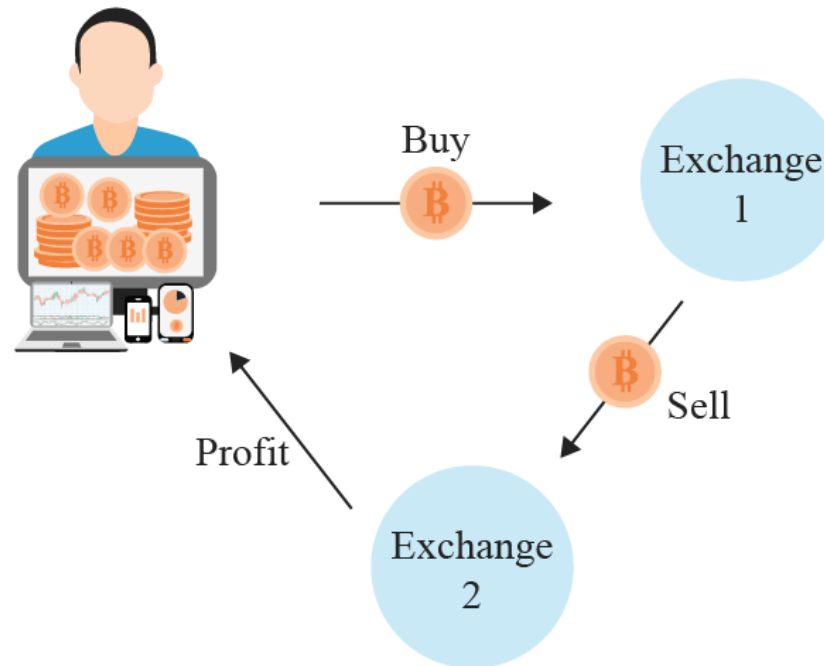


Profit: $2099 - 1500 = 599$ USDT

Maximal Extractable Value (MEV) - Arbitrages

- arbitrage is the simultaneous purchase and sale of the same or similar asset in different markets in order to profit from tiny differences in the asset's listed price
- they exist as a result of market inefficiencies and they both exploit those inefficiencies and resolve them

Maximal Extractable Value (MEV) - Arbitrages



Mitigate negative externalities posed by MEV: Flashbots



- Flashbots is research and development organization working on **mitigating the negative externalities** of current MEV extraction techniques and avoiding the **existential risks MEV could** cause to state-rich blockchains like Ethereum
- it falls under three goals: Democratizing Access to MEV Revenue, Bringing Transparency to MEV Activity, and Redistributing MEV Revenue
- Flashbots auction with the Flashbots relay, Flashbots protect RPC, MEV-inspect, MEV-explore, MEV-boost

<https://docs.flashbots.net>

<https://explore.flashbots.net>

<https://flashbots-explorer.marto.lol>



\$686,445,988

Total Extracted MEV

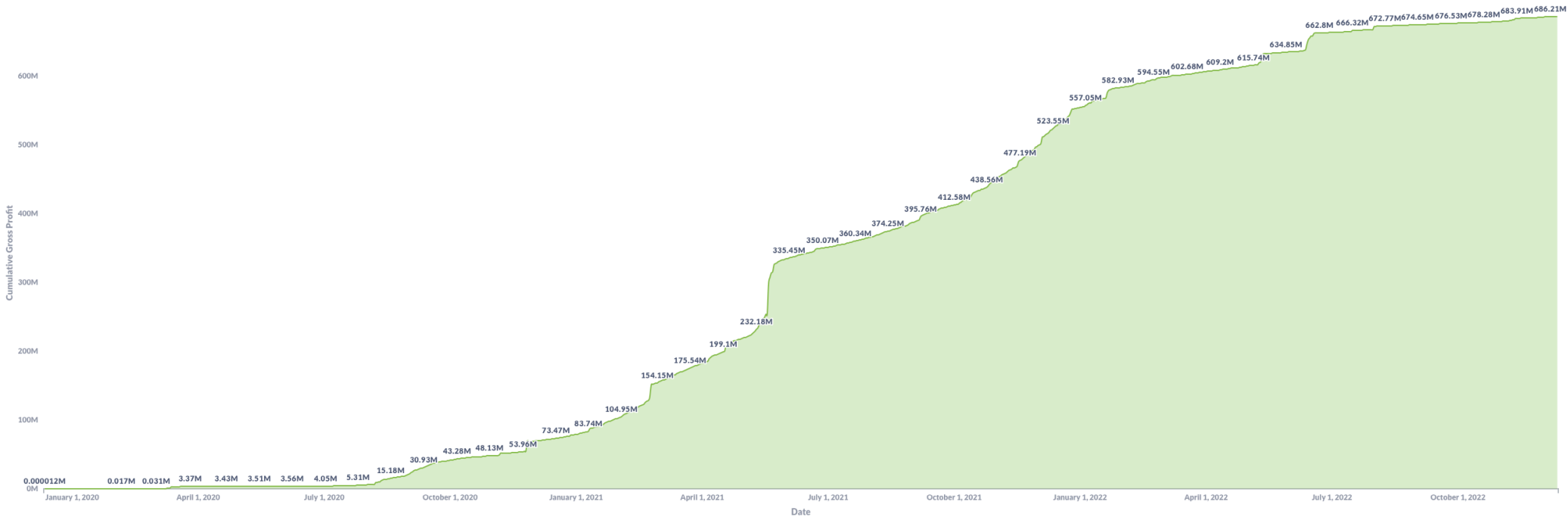
\$2,534,648

Last 30 days Extracted MEV

k

Last 24h Extracted MEV

Cumulative Extracted MEV - Gross Profit ⓘ



Daily Extracted MEV - Gross Profit

<https://explore.flashbots.net>

Single Unifying Auctions for Value Expression (SUAVE)

- each publishing node requests a wait time from a secure **hardware time source** within their computer system
- the secure hardware time source will generate a **random wait time**
- publishing nodes take the random time they are given and become **idle** for that duration
- once a publishing node wakes up from the idle state, it creates and publishes a block to the blockchain network
- any publishing node that is still idle will stop waiting, and the entire process starts over
- requires a permissioned and trusted execution environment

Resources

- Ethereum is a dark forest
- Escaping the dark forest
- Flashbots: running the MEV crisis
- Quantifying MEV
- EigenPhi

Resources

- Remix (solidity)
- Brownie (python)
- Ganache
- Truffle.js (Javascript)

Working in Python or Javascript is fine for testing purposes,
while ***golang*** is the best choice for production code