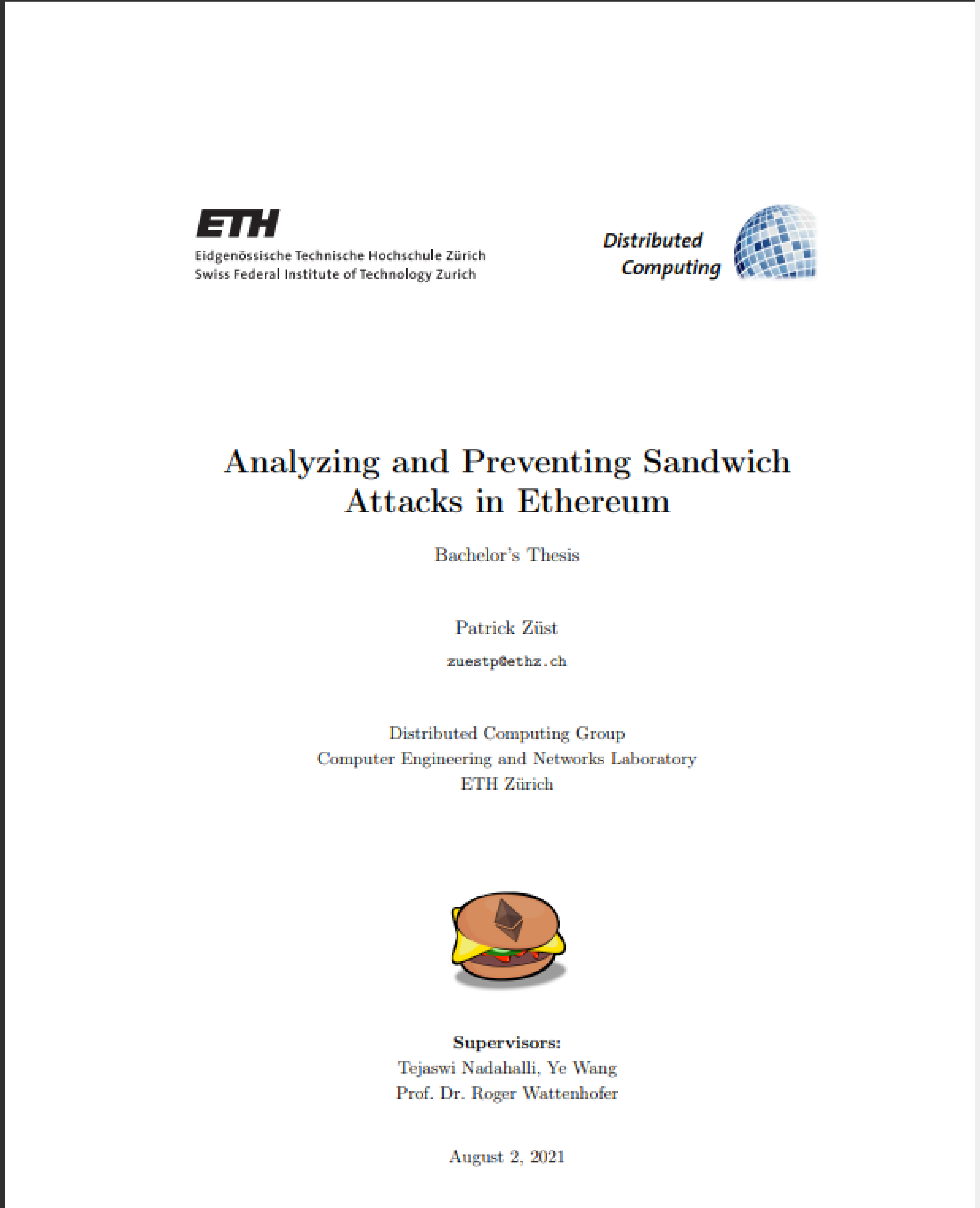


ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Analyzing and Preventing Sandwich Attacks in Ethereum

Bachelor's Thesis

Patrick Züst
zuestp@ethz.ch

Distributed Computing Group
Computer Engineering and Networks Laboratory
ETH Zürich

Supervisors:
Tejaswi Nadahalli, Ye Wang
Prof. Dr. Roger Wattenhofer

August 2, 2021

Analyzing and Preventing Sandwich Attacks in Ethereum

ZÜST, P. (2021). ANALYZING AND PREVENTING SANDWICH ATTACKS IN ETHEREUM.

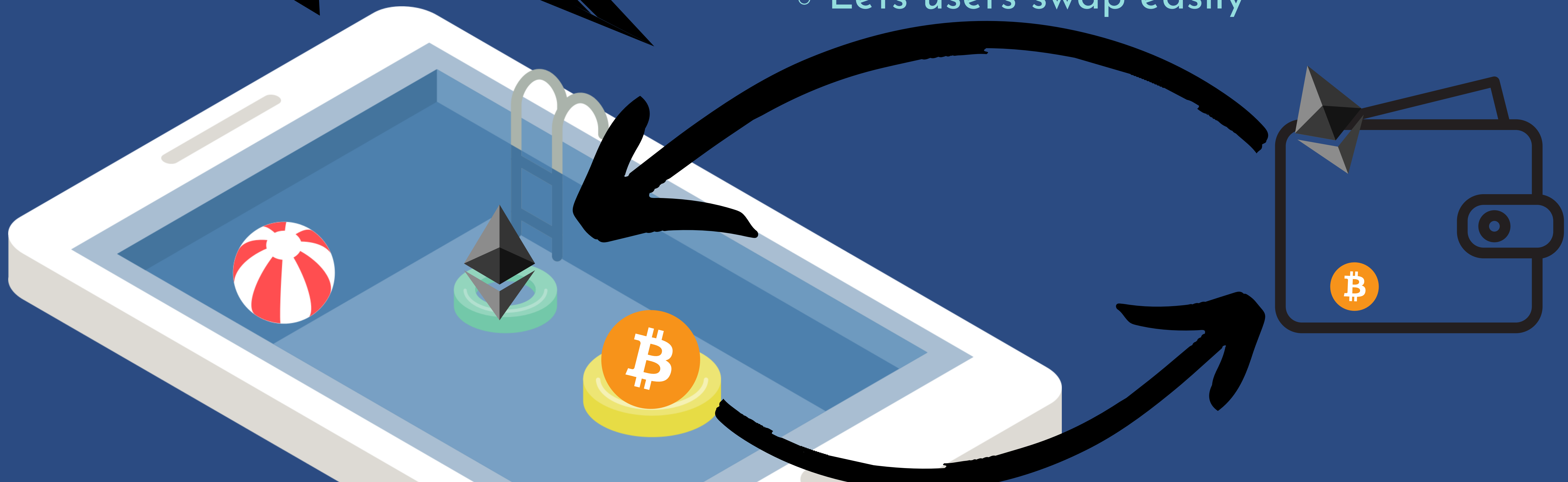
Available at https://pub.tik.ee.ethz.ch/students/2021-FS/BA-2021-07.pdf

Brought to you by
Oscar Mahon - 44782887
Xurong Liang - 45718502
Caleb Wishart - 45856945

Smart Contracts

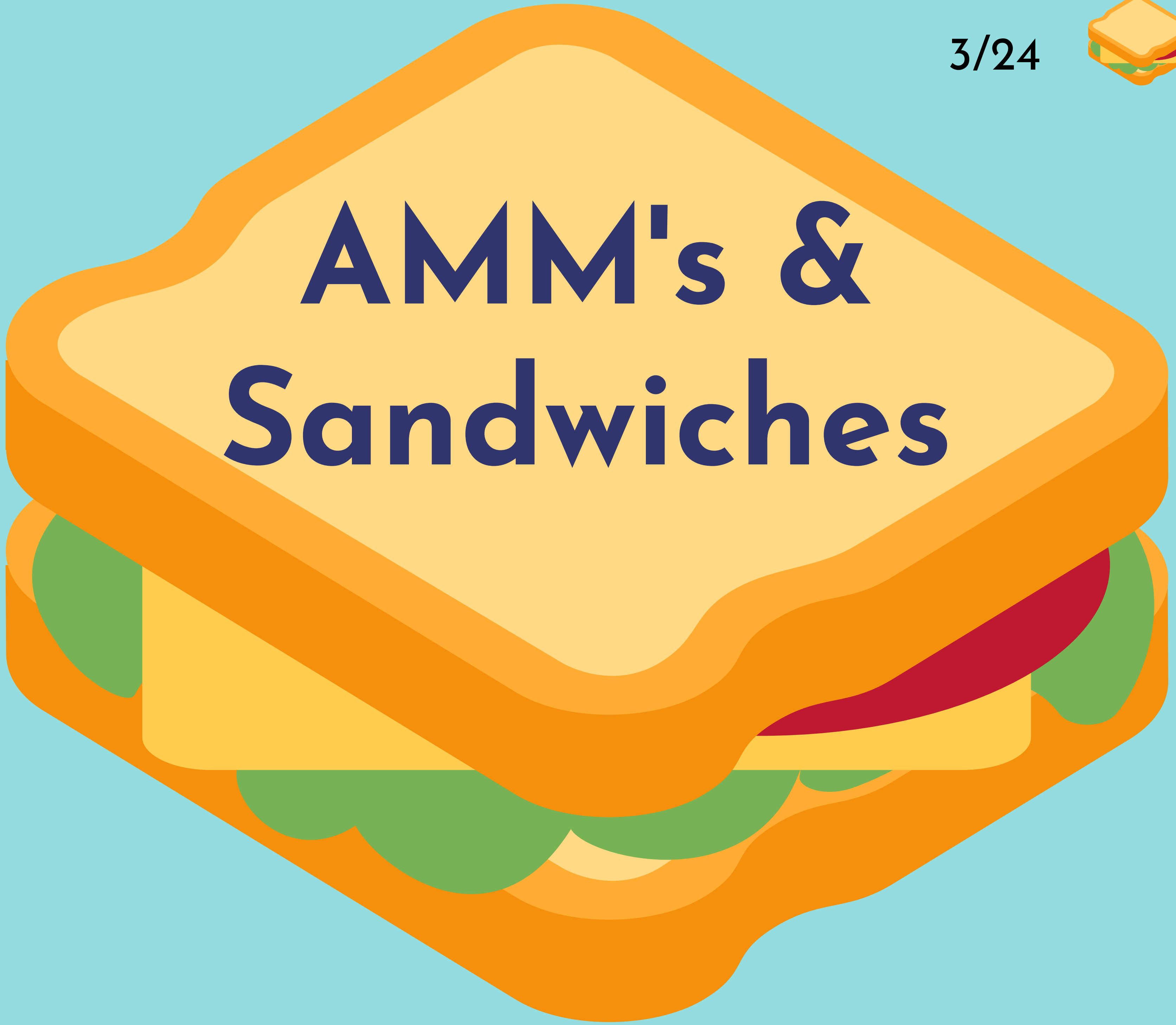
LETS ADD SOME SENSE

- Chains like Eth exploded in popularity
- Downfalls too
  - "Hacks" thru malicious contracts
  - Sandwich attacks
- How do AMM's work?
  - Middle Man
  - LP's help txn's flow
  - Lets users swap easily



UNFORTUNATELY, THEY'RE ALSO PUBLIC

- When you make a swap, the LP gets a request
    - LP takes ~0.3%
- Miners want a slice of bread too - monitor LP contract addresses
        - Once they spot the right addr, slip, txn value, gas fees, take every last cent
- How slippage prevents AMM abuse
    - Not flawless - txns still need to be submitted & processed



Let's run through one!

1

STEP

10 ETH -> 30,000 USDC

2

STEP

Frontrun at low price - miners control your txns

3

STEP

Your TXN for 10 ETH -> 30,000 USDC (Now 30,300 USDC)

4

STEP

Backrun at increased price

5

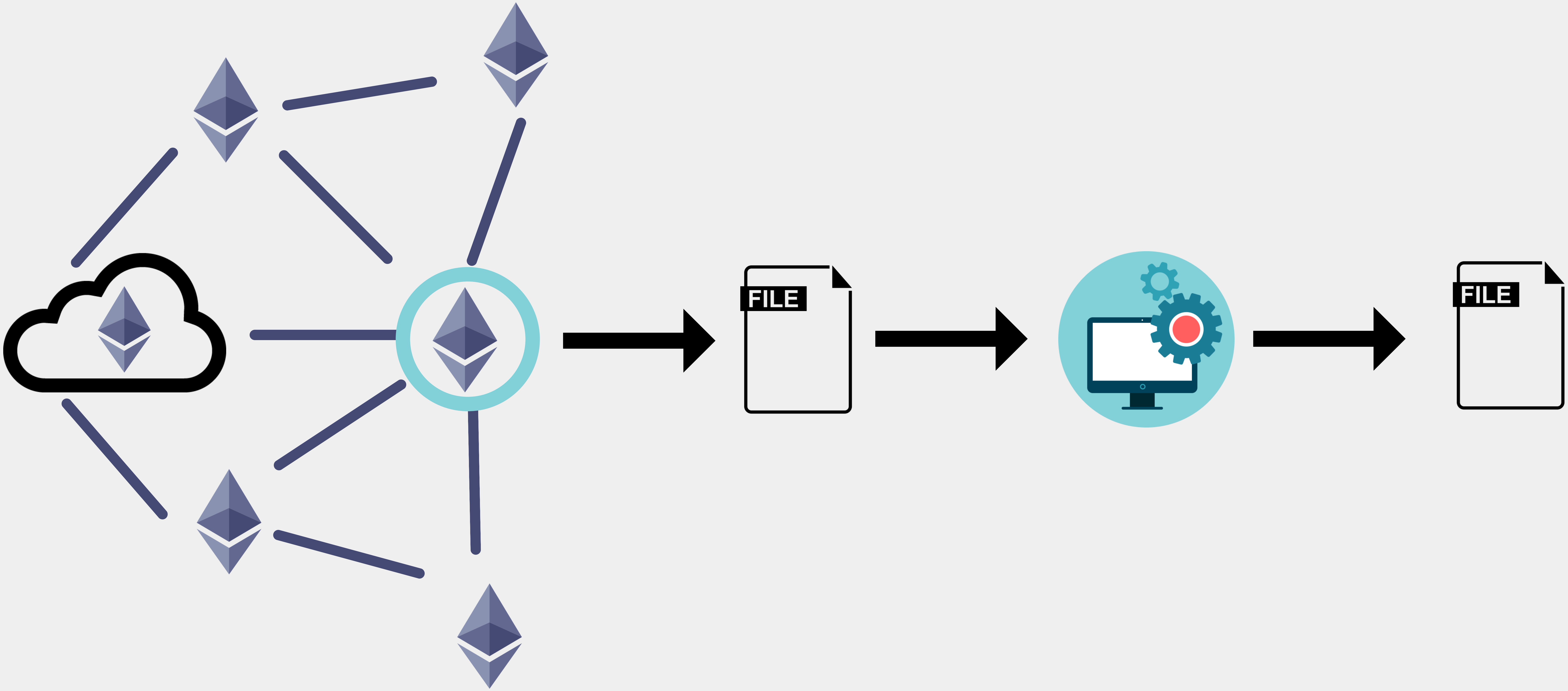
STEP

Easiest 3% profit of my life!

How is this even *legal*?

- Kind of a grey area at the moment
    - Technically not insider trading
        - info generally available
    - Technically *is* insider trading
        - only those with access (computing power)
            - Not generally available, especially today
        - material effects are a factor of insider trading
- Material effects of ~USD190mm (2021)

Analysis - Methodology



Ethereum Network

Processing Programs

Analysis - Heuristics

1. TA1 and TA2 are included in the same block and in this order.

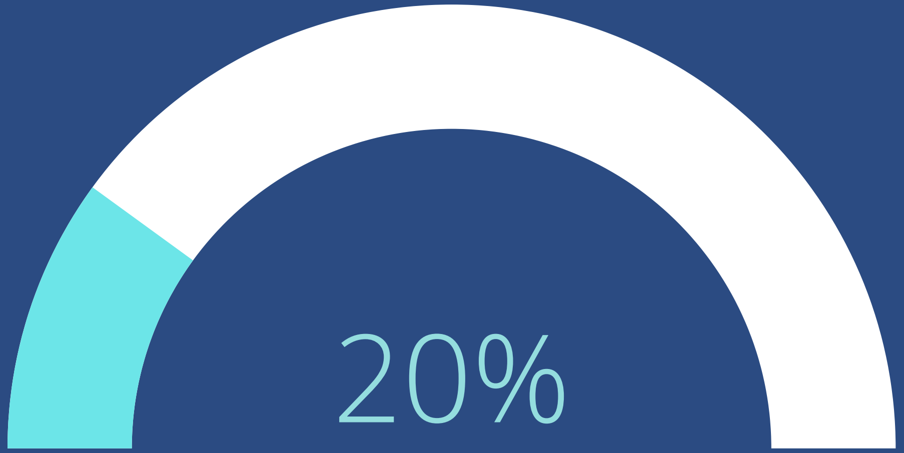
2. TA1 and TA2 have different transaction hashes ($TA1 \neq TA2$)

3.1 TA1 and TA2 swap assets in the same liquidity pool, but in opposite directions.

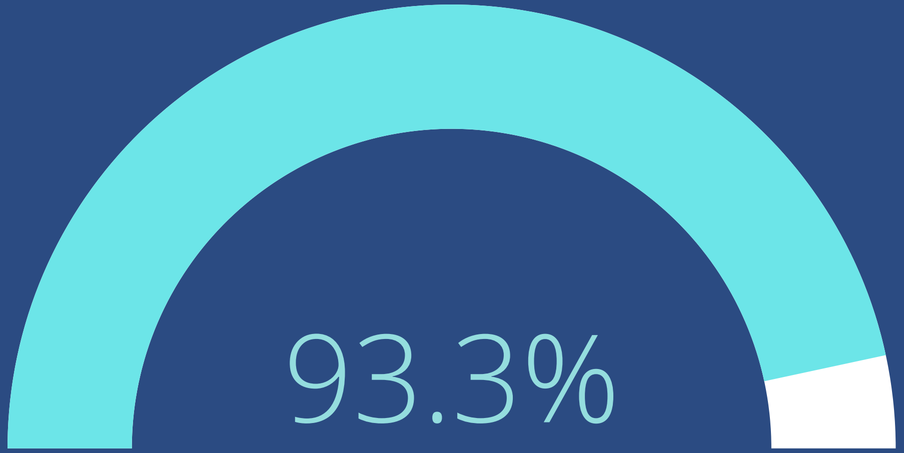
3.2 The input amount for the swap in TA2 is equal to the output amount of the swap in TA1.

4. Every transaction TA2 is mapped to exactly one transaction TA1

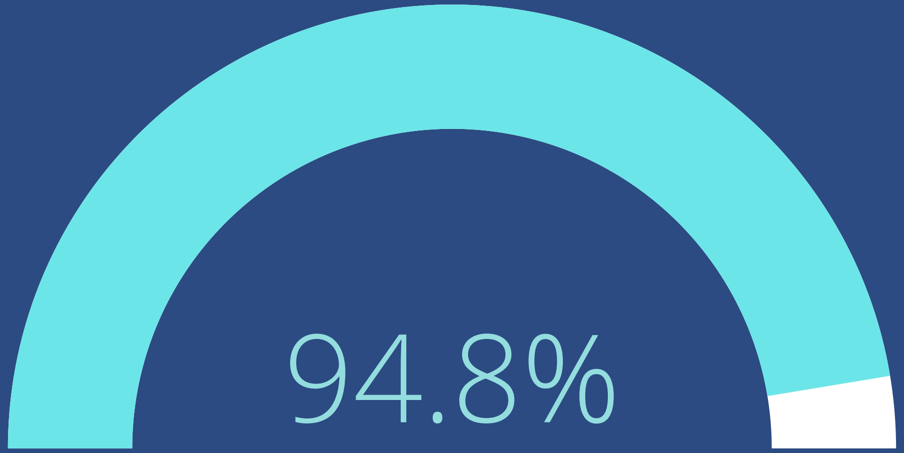
Analysis - Results



Number of blocks attacked
(~2.35 Million blocks total)



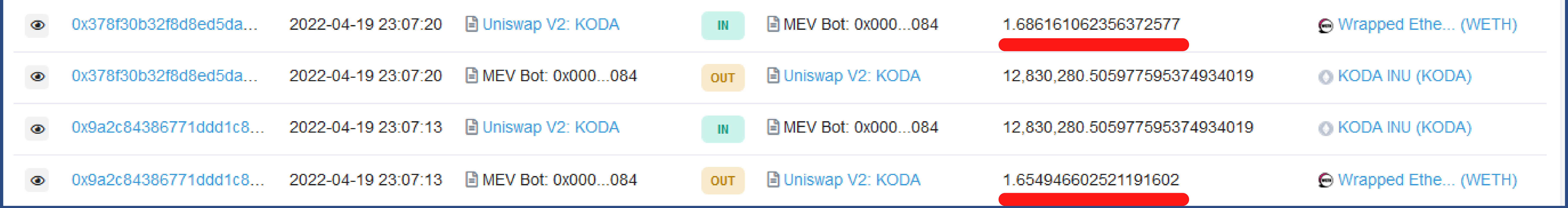
Proxy Contract
(964 unique)



Eth as input coin
(98.32% including 4 well known coins)

Analysis - Proxy Contract

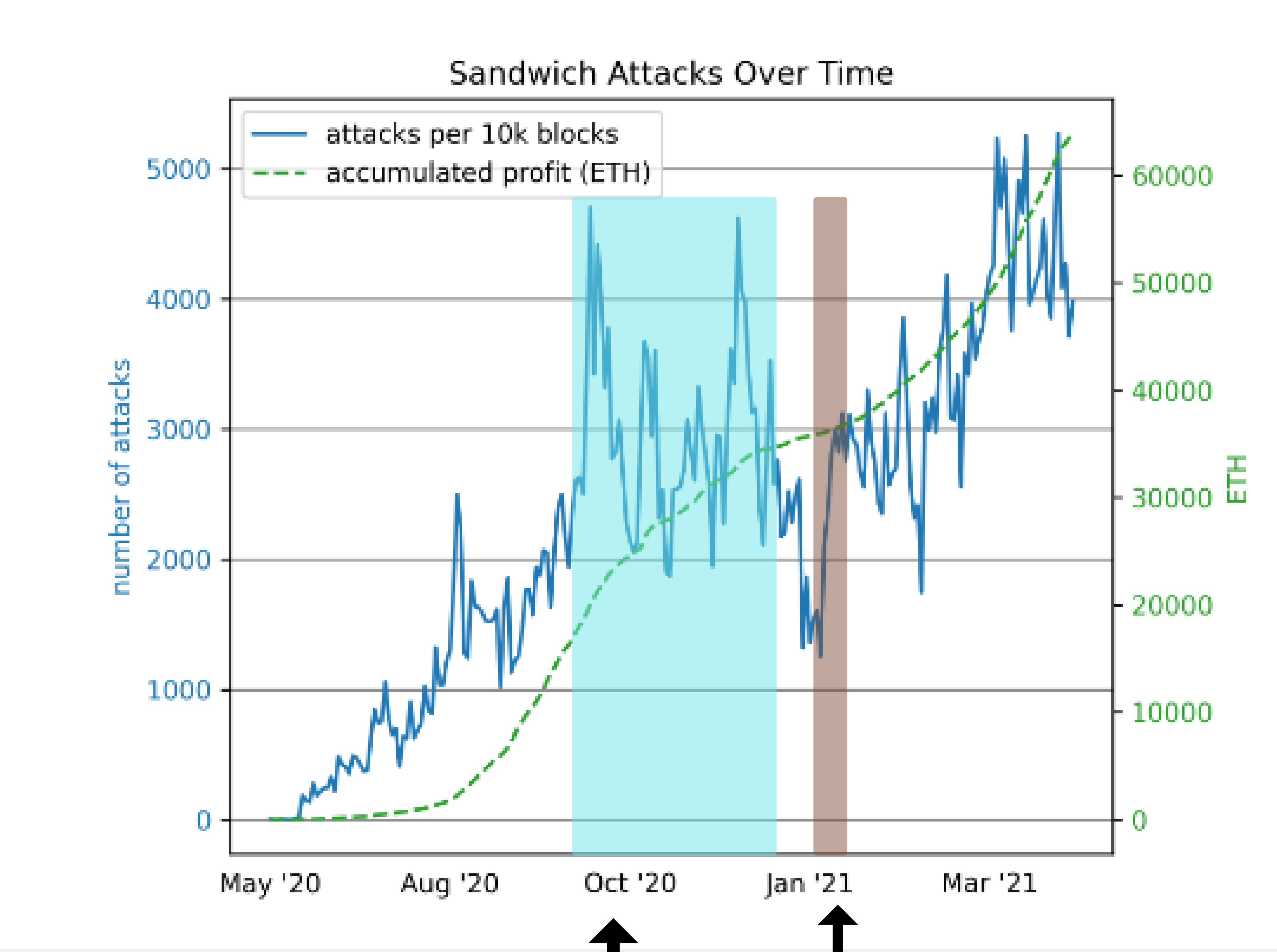
The most active proxy contract (0x0000000000000084e91743124a982076c59f10084) processed 51,475 of the attack transactions discovered (5.36%) and is still active today



👁	0x378f30b32f8d8ed5da...	2022-04-19 23:07:20	Uniswap V2: KODA	IN	MEV Bot: 0x000...084	1.686161062356372577	Wrapped Ethe... (WETH)
👁	0x378f30b32f8d8ed5da...	2022-04-19 23:07:20	MEV Bot: 0x000...084	OUT	Uniswap V2: KODA	12,830,280.505977595374934019	KODA INU (KODA)
👁	0x9a2c84386771ddd1c8...	2022-04-19 23:07:13	Uniswap V2: KODA	IN	MEV Bot: 0x000...084	12,830,280.505977595374934019	KODA INU (KODA)
👁	0x9a2c84386771ddd1c8...	2022-04-19 23:07:13	MEV Bot: 0x000...084	OUT	Uniswap V2: KODA	1.654946602521191602	Wrapped Ethe... (WETH)

*https://etherscan.io/tokentxns?a=0x0000000000000084e91743124a982076c59f10084

Analysis - Profit



Sandwich Attacks increase in popularity

Flashbots released

Noteworthy stats

Profit:

64,217 ETH (189,311,716 USD)

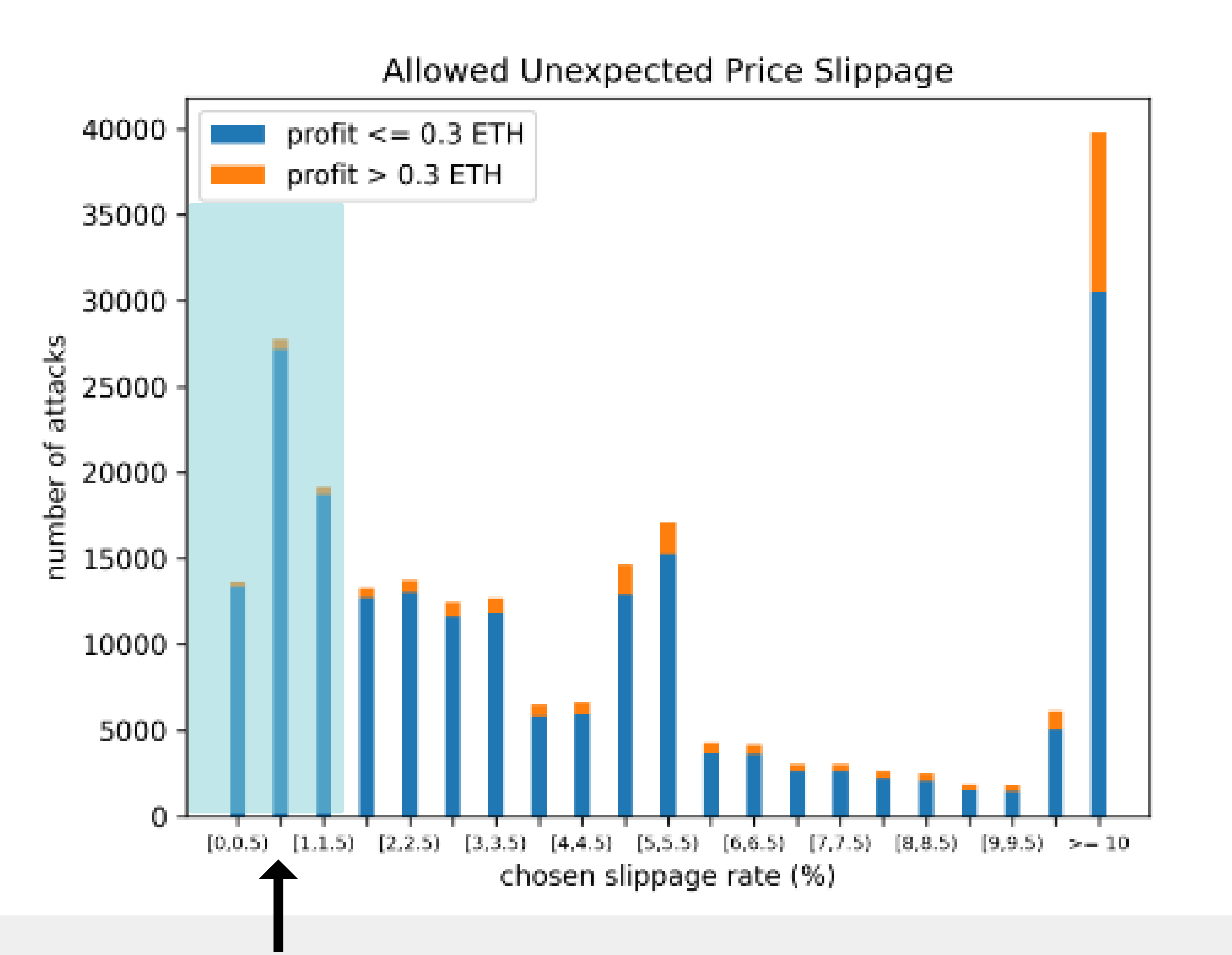
Losses: (18.1% of attacks)

9,120 ETH (26,885,760 USD)

Revenue:

73,337 ETH (216,197,476 USD)

Analysis - Slippage Rate



Recommended rate

Noteworthy stats

Most profitable attack:

13% Slippage rate

Gained 39.17 ETH (100,626 USD)

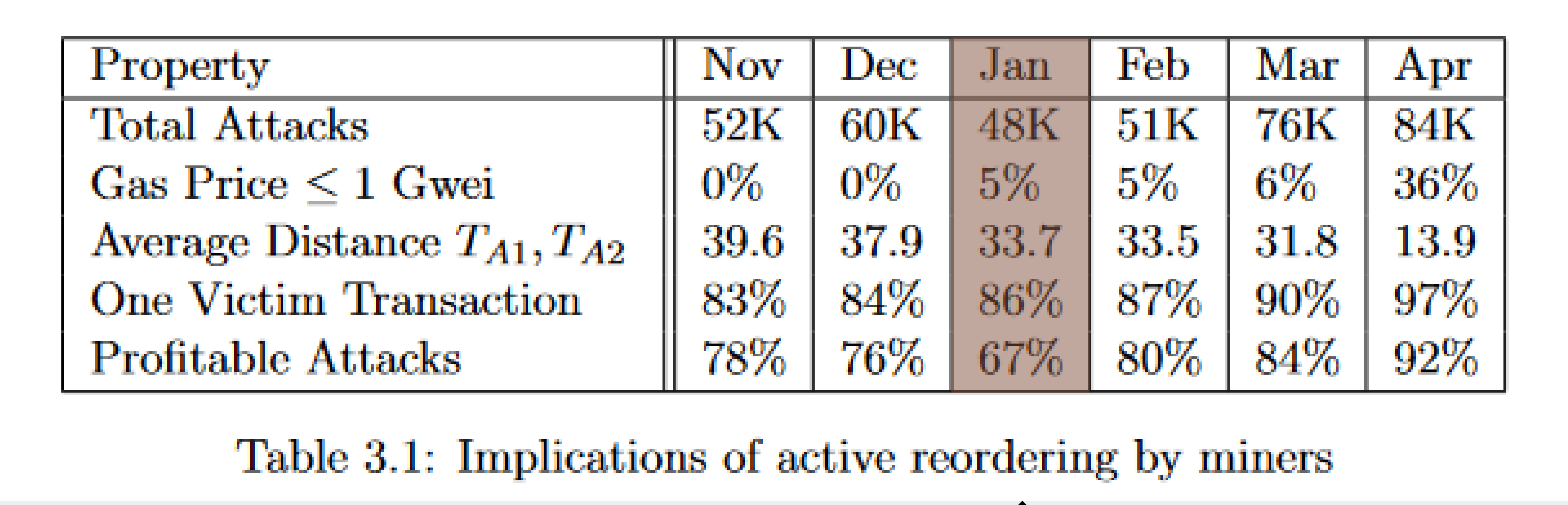
Biggest Loss:

23.67 ETH (69,779 USD)

Swapped wrong token

Victim differs by > 1% on average

Analysis - Miner Control



Property	Nov	Dec	Jan	Feb	Mar	Apr
Total Attacks	52K	60K	48K	51K	76K	84K
Gas Price $\leq$ 1 Gwei	0%	0%	5%	5%	6%	36%
Average Distance T_{A1}, T_{A2}	39.6	37.9	33.7	33.5	31.8	13.9
One Victim Transaction	83%	84%	86%	87%	90%	97%
Profitable Attacks	78%	76%	67%	80%	84%	92%

Table 3.1: Implications of active reordering by miners

Flashbots released

Noteworthy stats

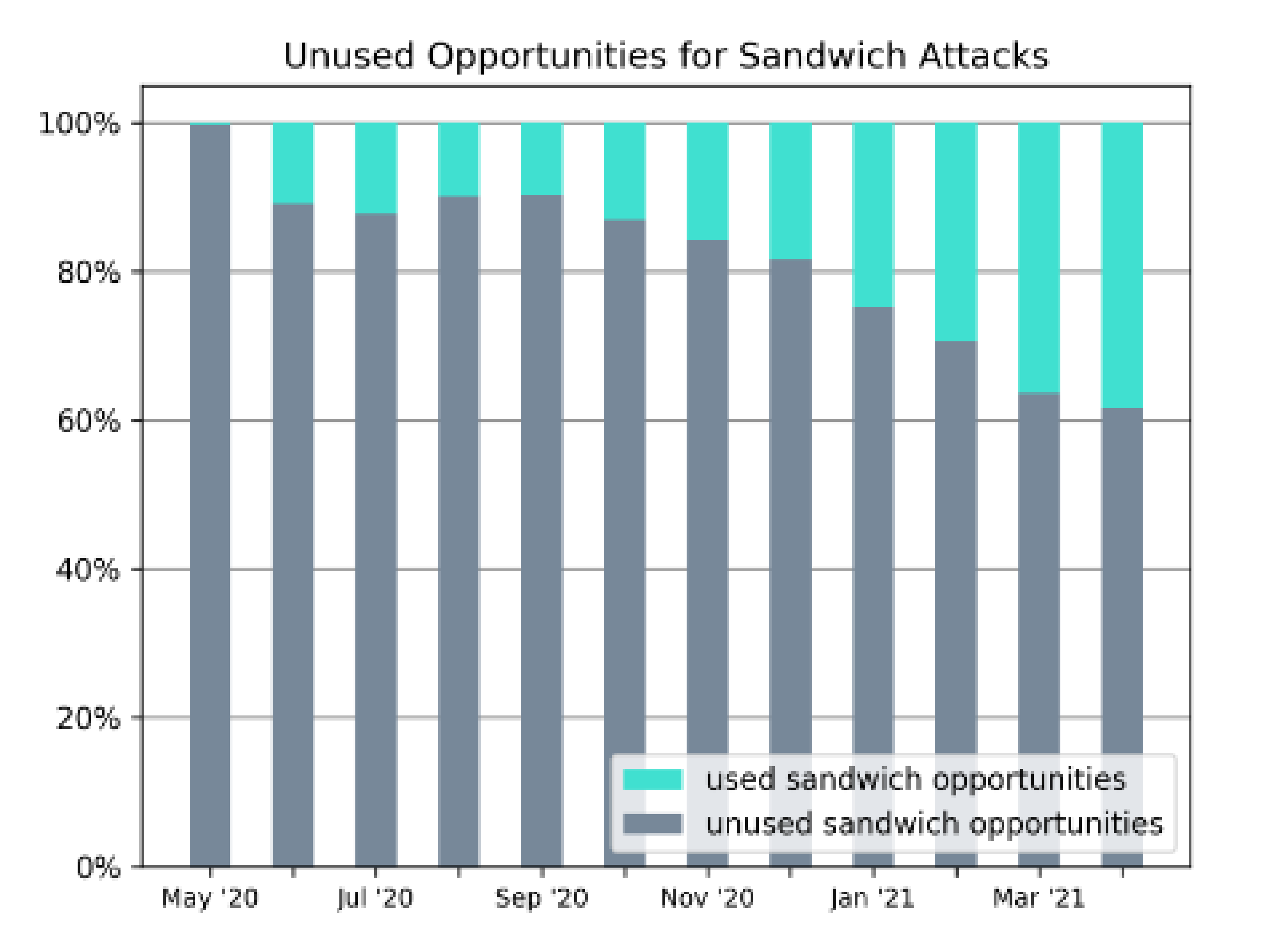
January 2021 showed a drop in total attacks and profitable

March -> April average distance dropped 18 spots

97% of attacks target a specific victim

Attackers are getting better at their craft

Analysis - Missed Opportunity



ETH serves as input token

Noteworthy stats

From 1% to 38% in one year

Biggest missed opportunity:
724 ETH (2,134,352 USD)

52.35% of attackable swaps have a different token as input

Common reasons for a miss:
- Private transaction
- Not enough time in mempool

Mitigation Strategies

Possible Strategies

Single transaction - Lower transaction slipage rate

- Minimize sandwich attack profitability.
- Problem: Low slippage rate on transaction with large swap amount is more likely to fail. (DeGate Team, 2021)

Single transaction - Increase the gas fee

- Increase the cost of attacking a transaction.
- Problem: incur additiomal transaction costs on users. (DeGate Team, 2021)

Multiple transactions - Order Split

- Highlight of this section, introduced by Züst (2021).

Order Split

Assumptions:

- Only transactions of one trader and one attacker are broadcasted
- If a transaction is split into multiple smaller ones, each of which is included in the blockchain before the next one is broadcasted

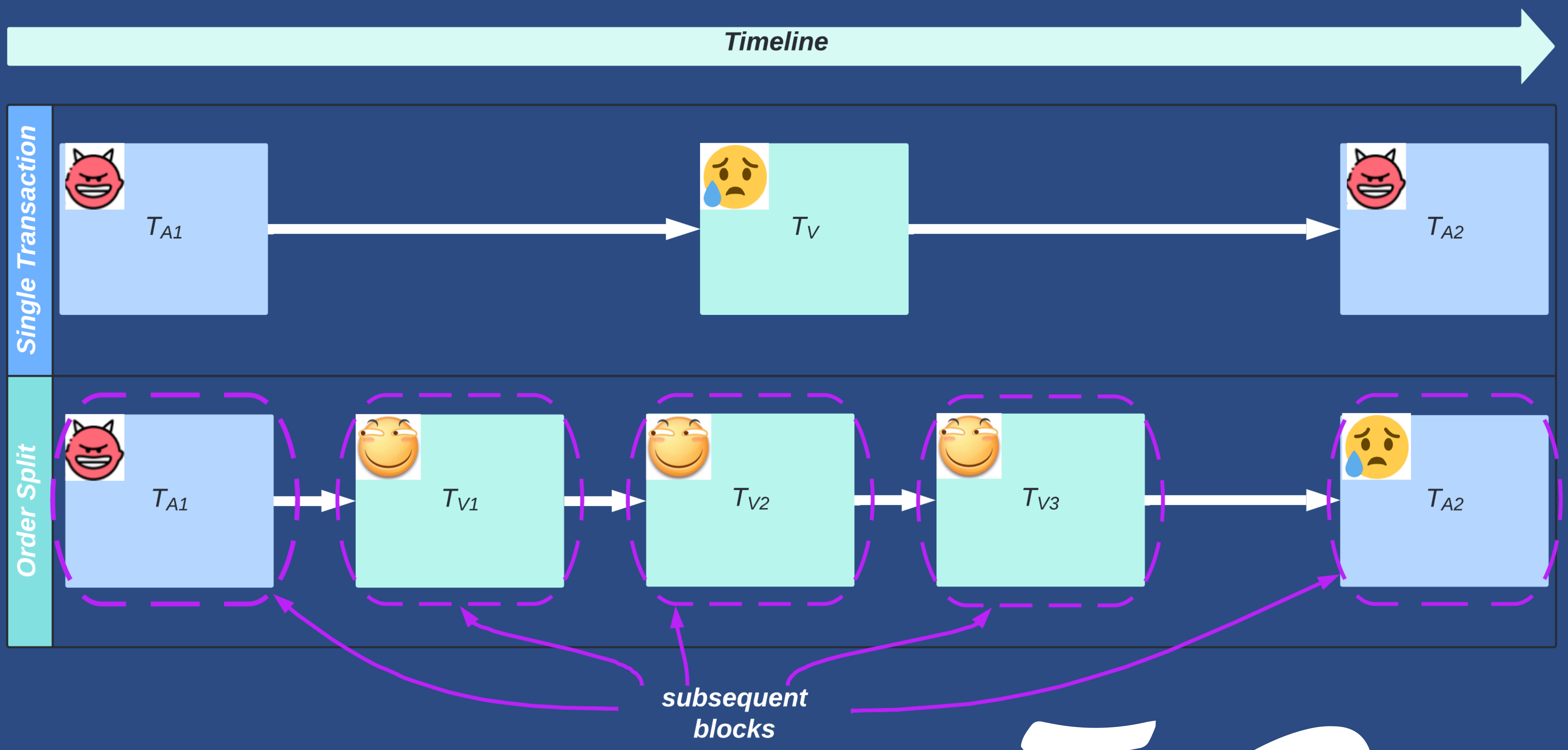
"A sandwich attack is only possible if the difference in market price before and after the swap is large enough to compensate for transaction and exchange fees."

(Züst, 2021)

- Splitting one order with large trading amount into multiple transactions, each of which has relatively smaller trading amount

- Reduce variability in the liquidity pool and hence reduce the room for sandwich attack

Order Split Demo



Premises:

- frontrunning transaction TA1
- backrunning transaction TA2
- victim transaction
  - before split: TV
  - after split: TV1, TV2, TV3

To obtain the same amount of gains as single transaction, attacker needs to ensure exact split ordering acorss sequential blocks as shown, which is HARD!

So order split is a good thing, but how to ensure I make it right?

Solution: do some math to find out!

Solve $output_{A2}(v) - maxInput_{A1}(v) - transactionFees \geq 0$

- maxInput_A1: max input of frontrunning transaction T_A1
- output_A2: output amount of backrunning transaction T_A2
- v: original victim transaction input amount

Input of order splits:

$$v_1 = \max\left(v, v_{max}\right)$$

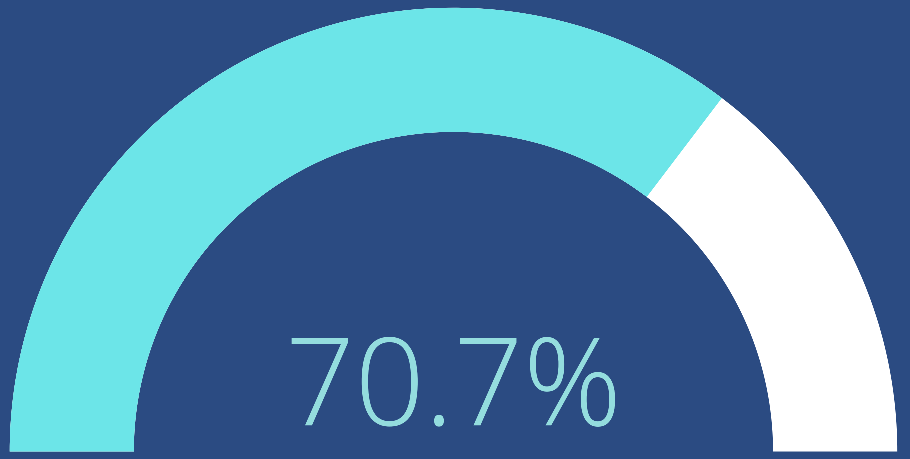
$$v_2 = \max\left(v - v_1, updated\ v_{max}\right)$$

...

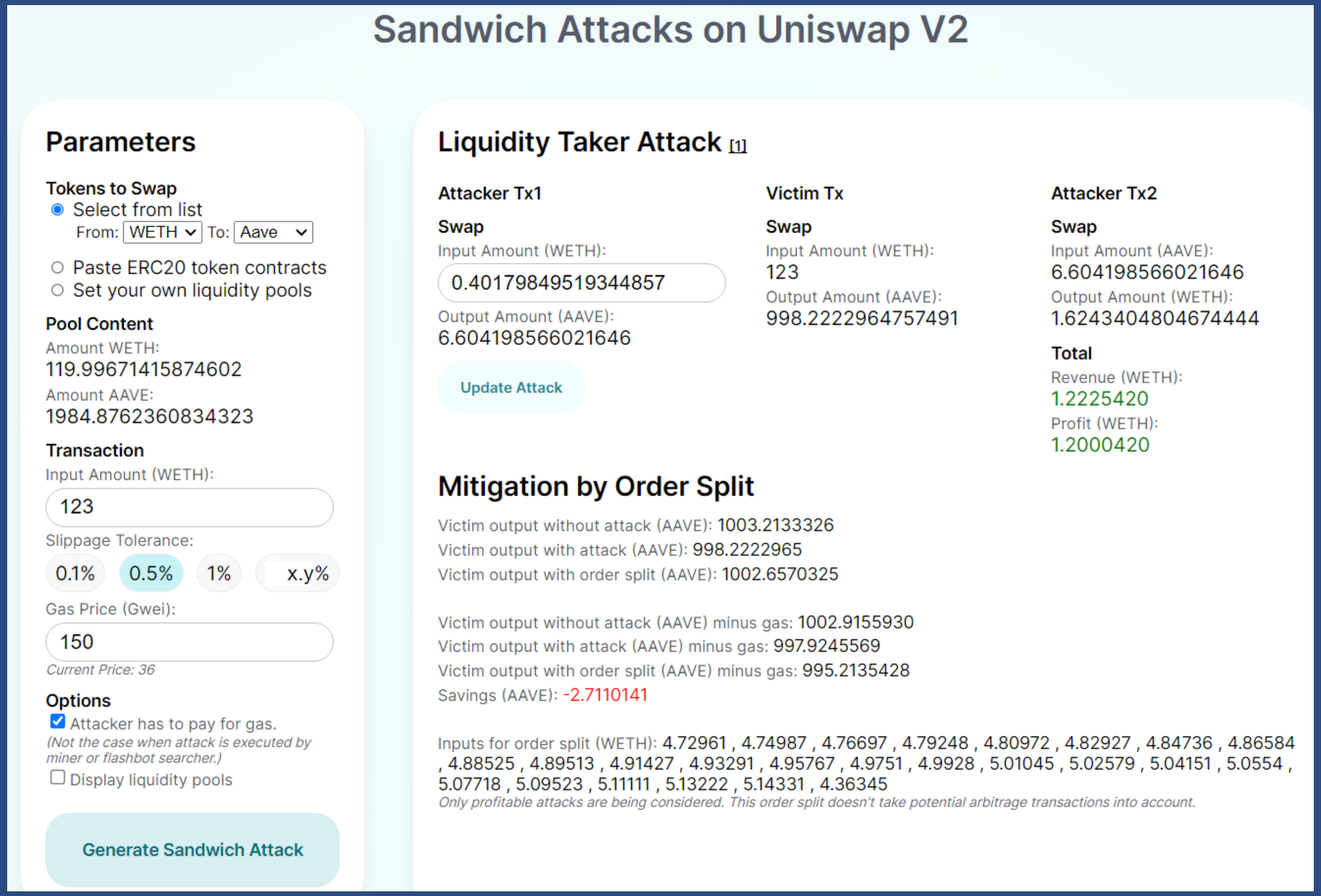
calculate subsequent order splits with updated reserves until sum of orders == v

Order Split Backtesting

- Accumulated trader loss without order split: 42,504 ETH
- Applying order split strategy could have saved 30,525 ETH
- Useful tool for order split deployment: www.DeFi-Sandwi.ch



Percentage of given attacks prevented by implementing order split (~226,895 given attacks in total)



Sandwich Attacks on Uniswap V2

Parameters

Tokens to Swap
● Select from list
From: WETH To: Aave
○ Paste ERC20 token contracts
○ Set your own liquidity pools

Pool Content
Amount WETH:
119.99671415874602
Amount AAVE:
1984.8762360834323

Transaction
Input Amount (WETH):
123
Slippage Tolerance:
0.1% [✓ 0.5%] 1% x.y%
Gas Price (Gwei):
150
Current Price: 36

Options
☑ Attacker has to pay for gas.
(Not the case when attack is executed by miner or flashbot searcher.)
☐ Display liquidity pools

Liquidity Taker Attack [1]

Attacker Tx1
Swap
Input Amount (WETH):
0.40179849519344857
Output Amount (AAVE):
6.604198566021646

Victim Tx
Swap
Input Amount (WETH):
123
Output Amount (AAVE):
998.2222964757491

Attacker Tx2
Swap
Input Amount (AAVE):
6.604198566021646
Output Amount (WETH):
1.6243404804674444

Total
Revenue (WETH):
1.2225420
Profit (WETH):
1.2000420

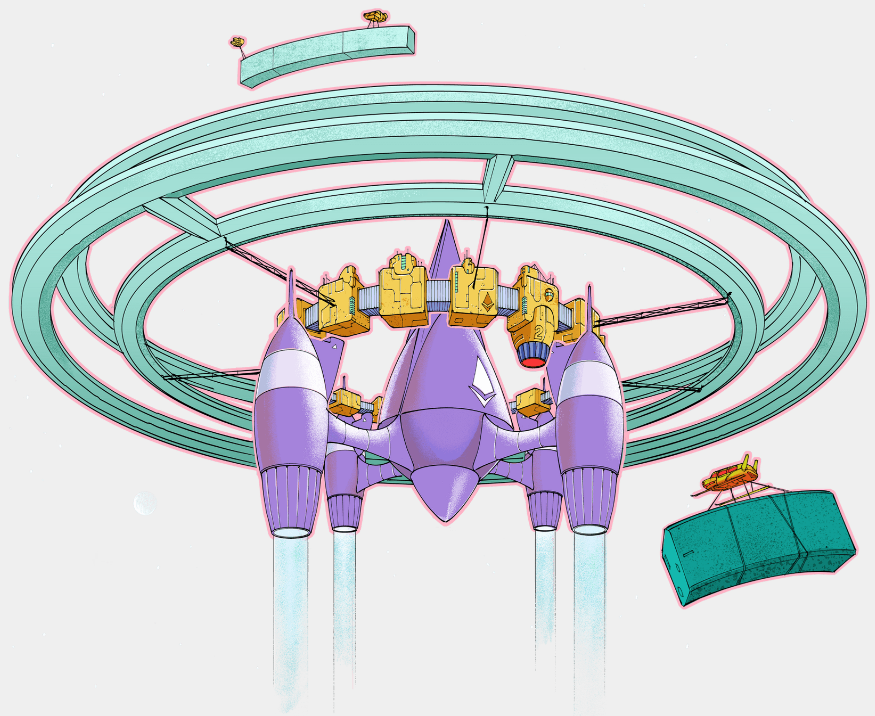
Mitigation by Order Split

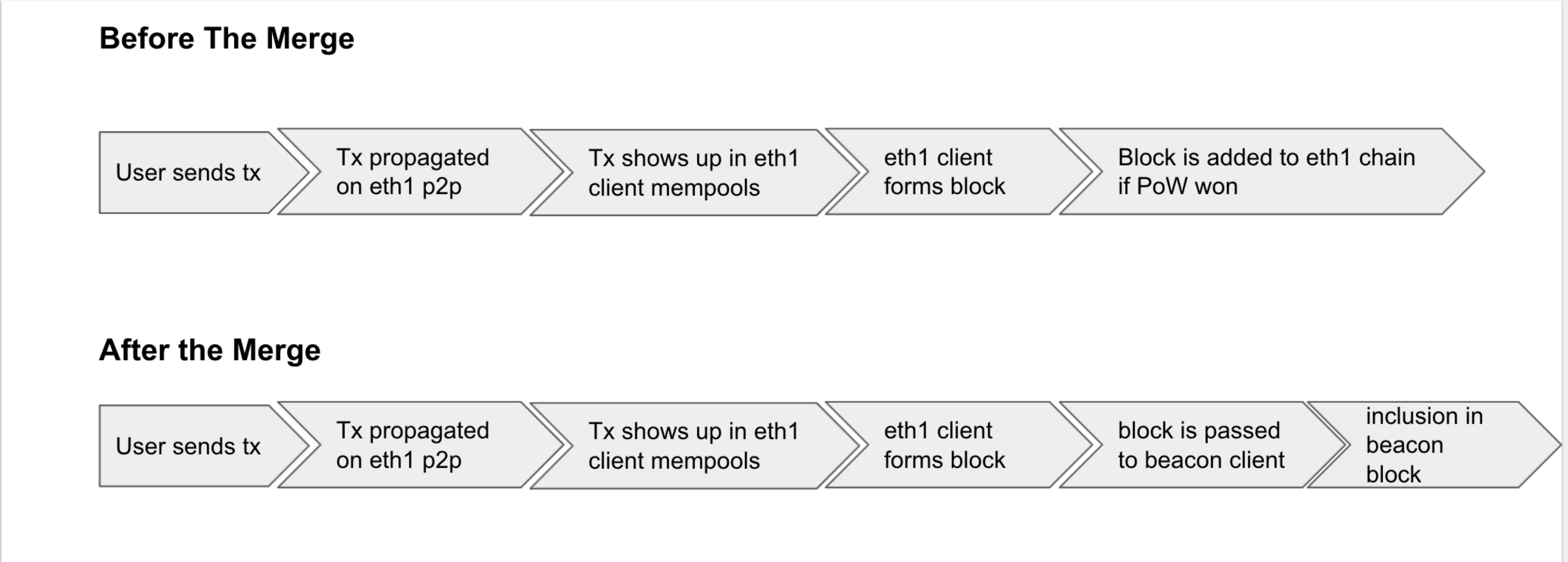
Victim output without attack (AAVE): 1003.2133326
Victim output with attack (AAVE): 998.2222965
Victim output with order split (AAVE): 1002.6570325

Victim output without attack (AAVE) minus gas: 1002.9155930
Victim output with attack (AAVE) minus gas: 997.9245569
Victim output with order split (AAVE) minus gas: 995.2135428
Savings (AAVE): -2.7110141

Inputs for order split (WETH): 4.72961 , 4.74987 , 4.76697 , 4.79248 , 4.80972 , 4.82927 , 4.84736 , 4.86584 , 4.88525 , 4.89513 , 4.91427 , 4.93291 , 4.95767 , 4.9751 , 4.9928 , 5.01045 , 5.02579 , 5.04151 , 5.0554 , 5.07718 , 5.09523 , 5.11111 , 5.13222 , 5.14331 , 4.36345
Only profitable attacks are being considered. This order split doesn't take potential arbitrage transactions into account.

The Future





Before The Merge

User sends tx → Tx propagated on eth1 p2p → Tx shows up in eth1 client mempools → eth1 client forms block → Block is added to eth1 chain if PoW won

After the Merge

User sends tx → Tx propagated on eth1 p2p → Tx shows up in eth1 client mempools → eth1 client forms block → block is passed to beacon client → inclusion in beacon block

The Merge

Transition to Proof-Of-Stake

~Q3/Q4 This year

Likely that in block attacks will decrease but availability for cross block attacks

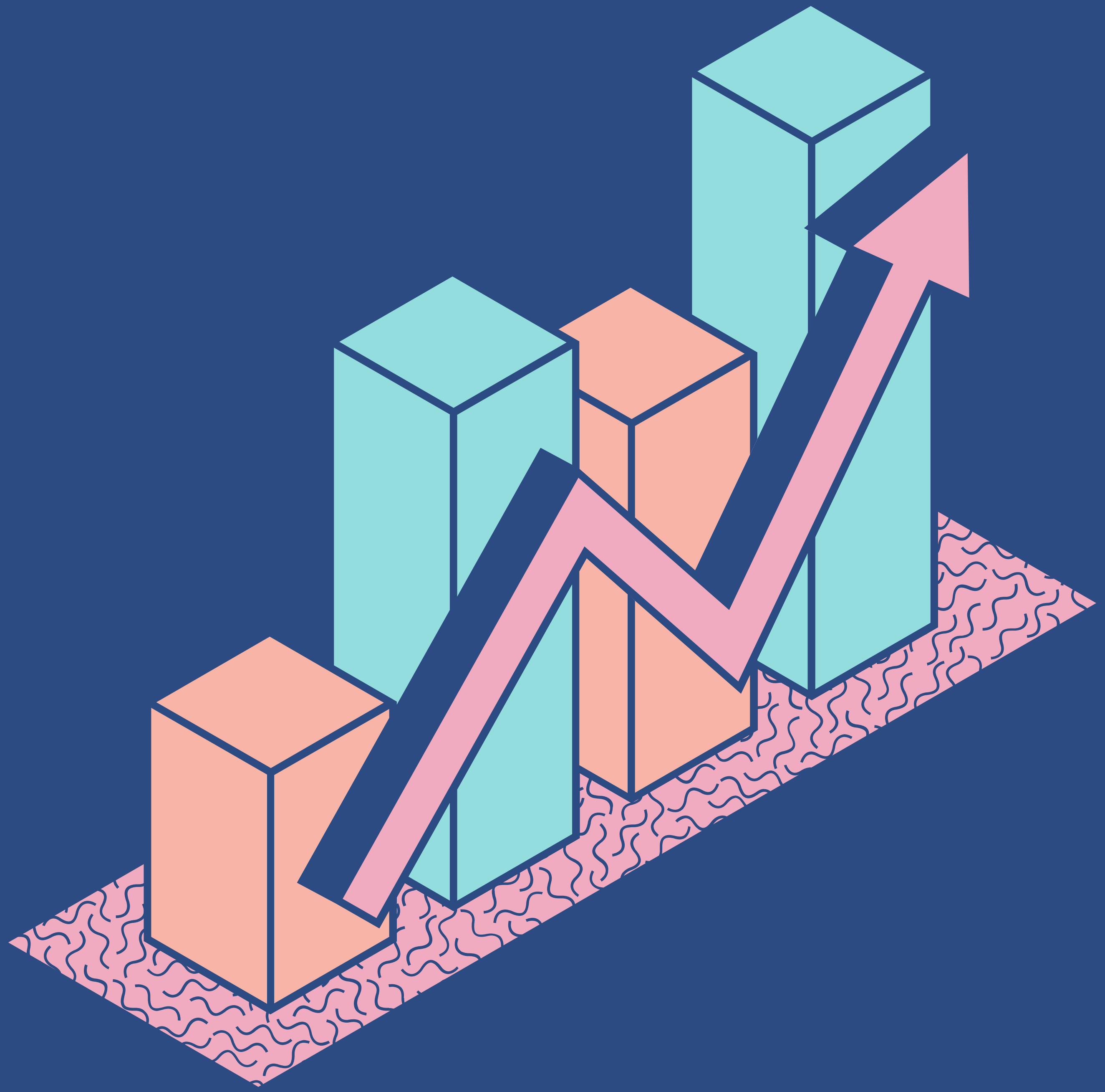
*https://hackmd.io/@flashbots/mev-in-eth2

Conclusion

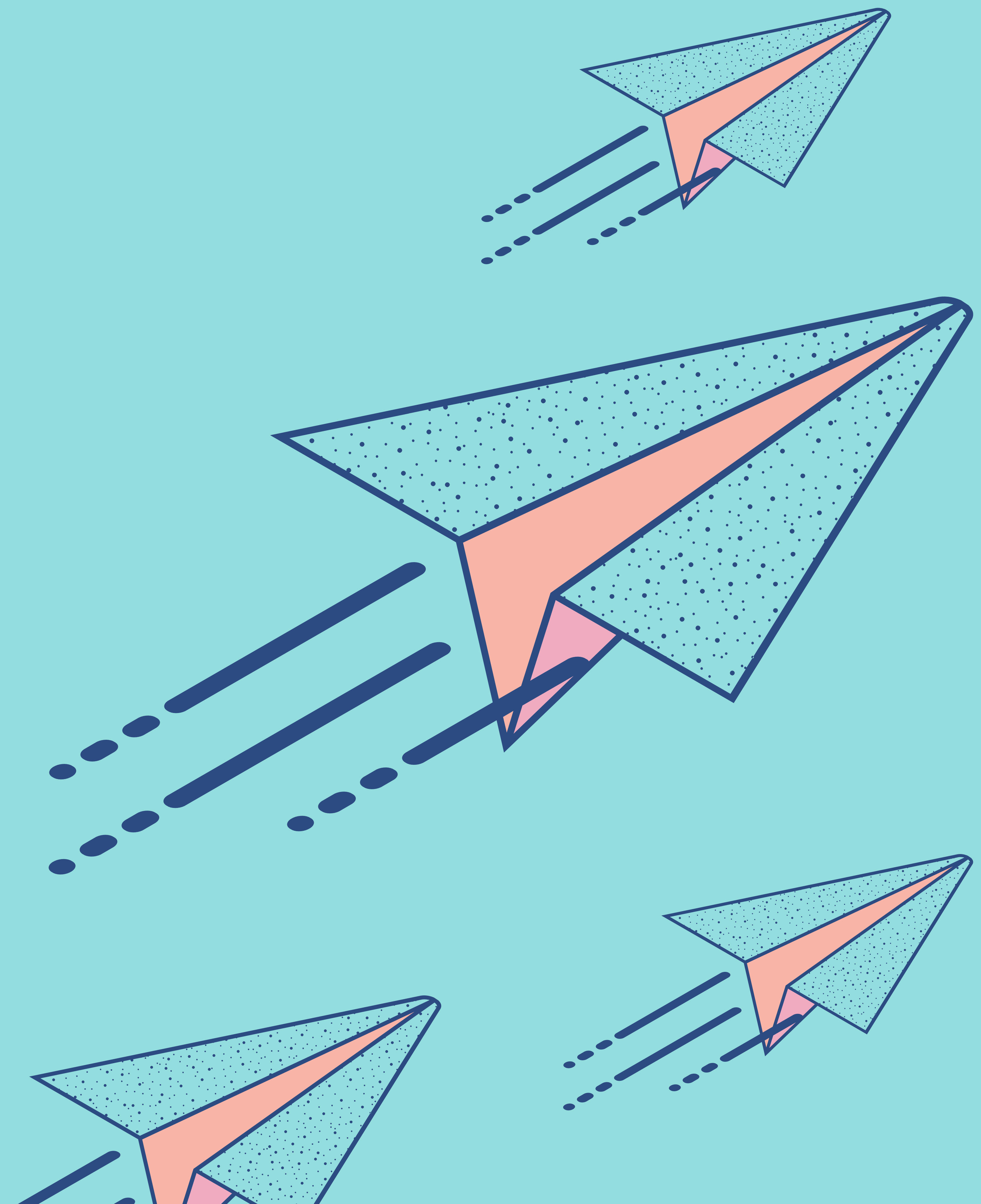
- Basic knowledge about sandwich attacks
- Smart Contracts, AMM's & LP's
- Legality of crypto

- Statistics show that sandwich attacks are common
- Deployment of Flashbots leads to increased activity in the sector

- Single transaction mitigation strategies have side-effects
- Order split mitigation strategy minimizes the chance of being sandwich attacked



Do you have any questions?



References

P. Züst, "Analyzing and Preventing Sandwich Attacks in Ethereum.," 2021.

DeGate Team, "An analysis of Ethereum front-running and its defense solutions," Medium, 4 May 2021. [Online]. Available: https://medium.com/degate/an-analysis-of-ethereum-front-running-and-its-defense-solutions-34ef81ba8456.

Torres, C. F., & Camino, R. (n.d.). Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain.