Transparent Dishonesty: Front-running Attacks on Blockchain

Jeremy Clark

MADIBA
security research group

UNIVERSITÉ Concordia UNIVERSITY

GINA CODY
SCHOOL OF ENGINEERING
AND COMPUTER SCIENCE

FUNDING & PARTNERS:

NSERC
CRSNG

Raymond Chabot
Grant Thornton

catallaxy

AUTORITÉ
DES MARCHÉS
FINANCIERS

Fonds de recherche
Nature et
technologies
Québec

Office of the
Privacy Commissioner
of Canada

SHAYAN ESKANDARI, CONCORDIA / CONSENSYS DILIGENCE

MAHSA MOOSAVI, CONCORDIA / OFFCHAIN LABS

JEREMY CLARK, CONCORDIA

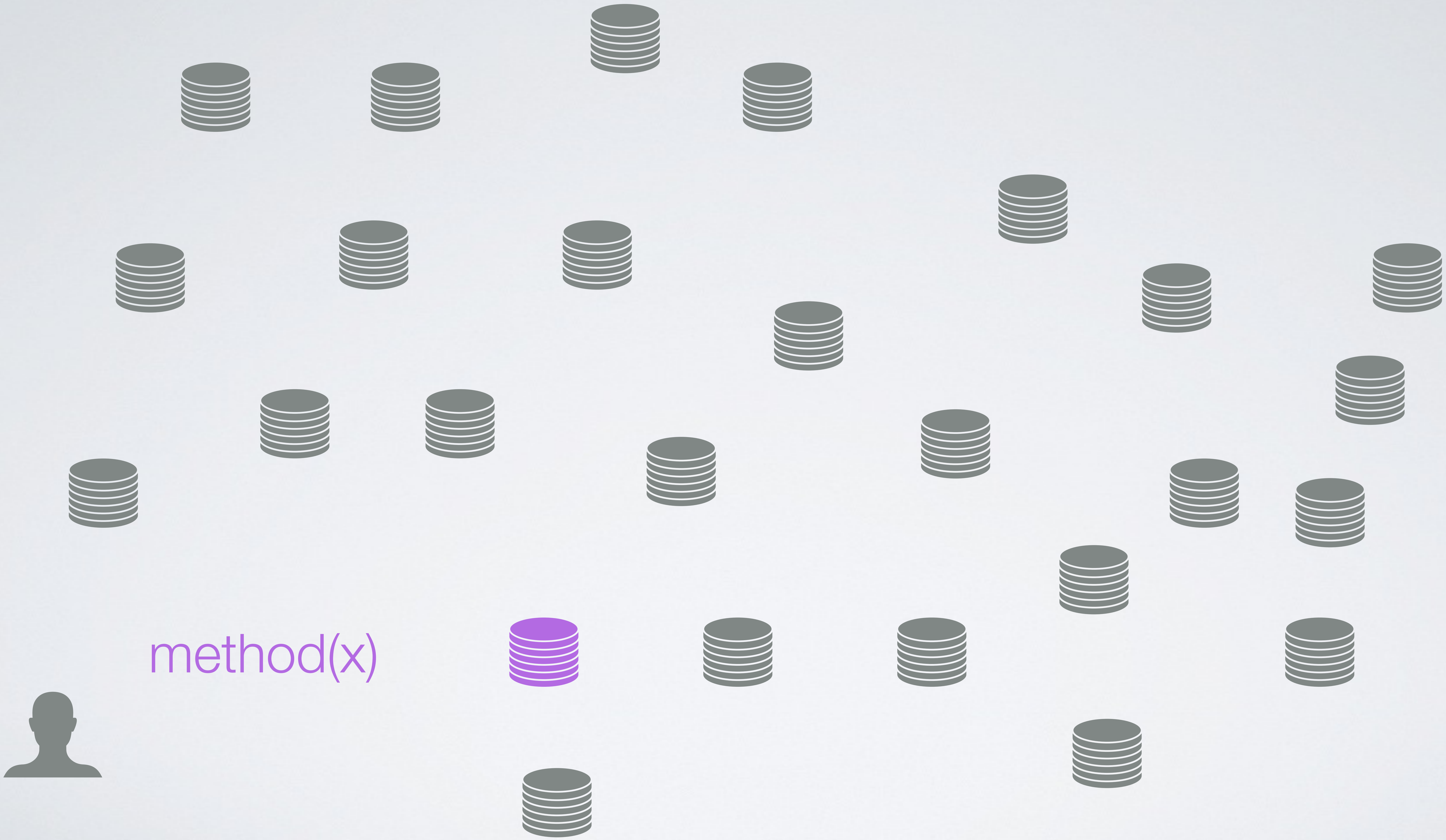
UNIVERSITÉ
Concordia
UNIVERSITY

CONSENSYS
Diligence

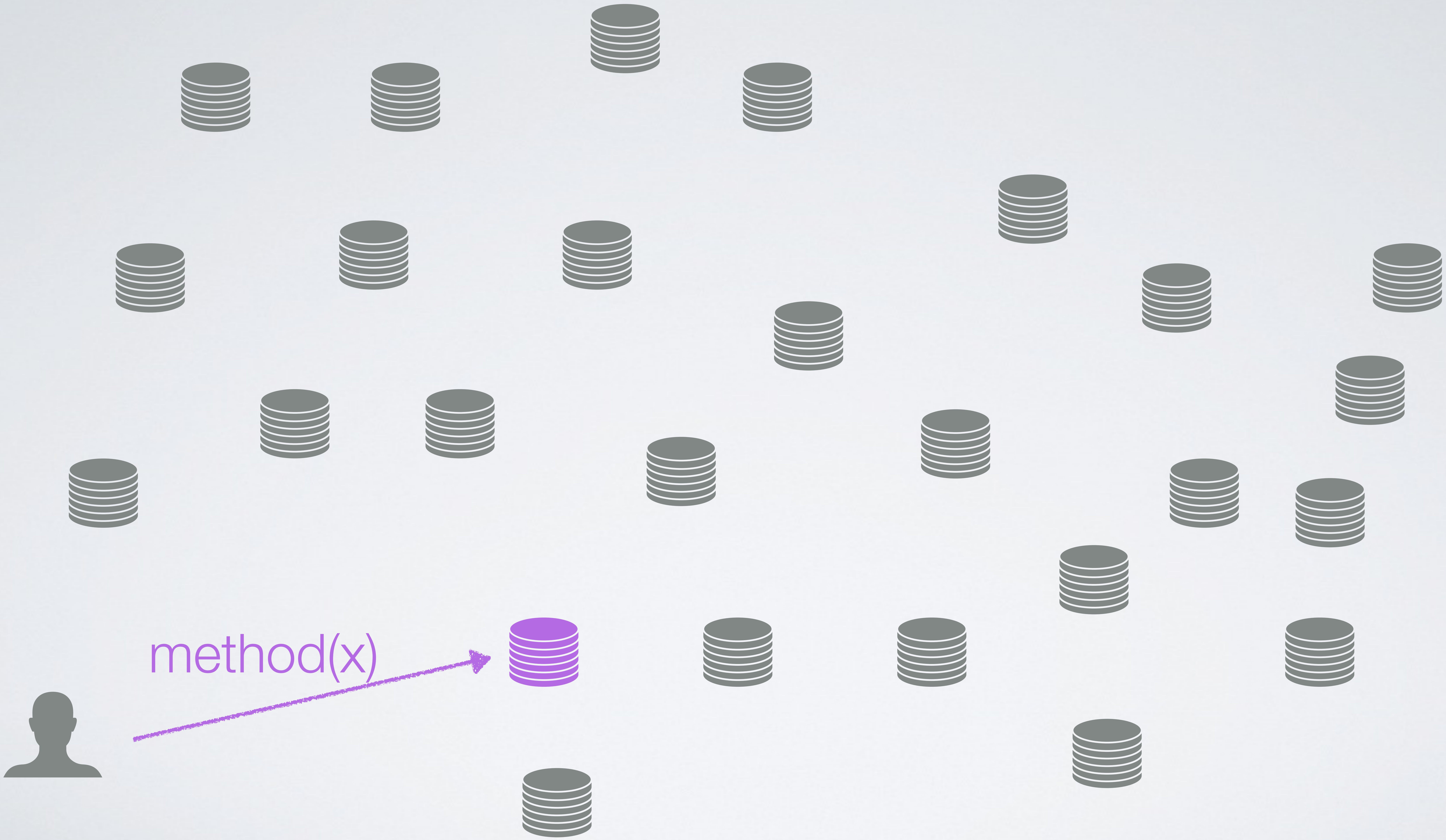
OFFCHAIN
LABS

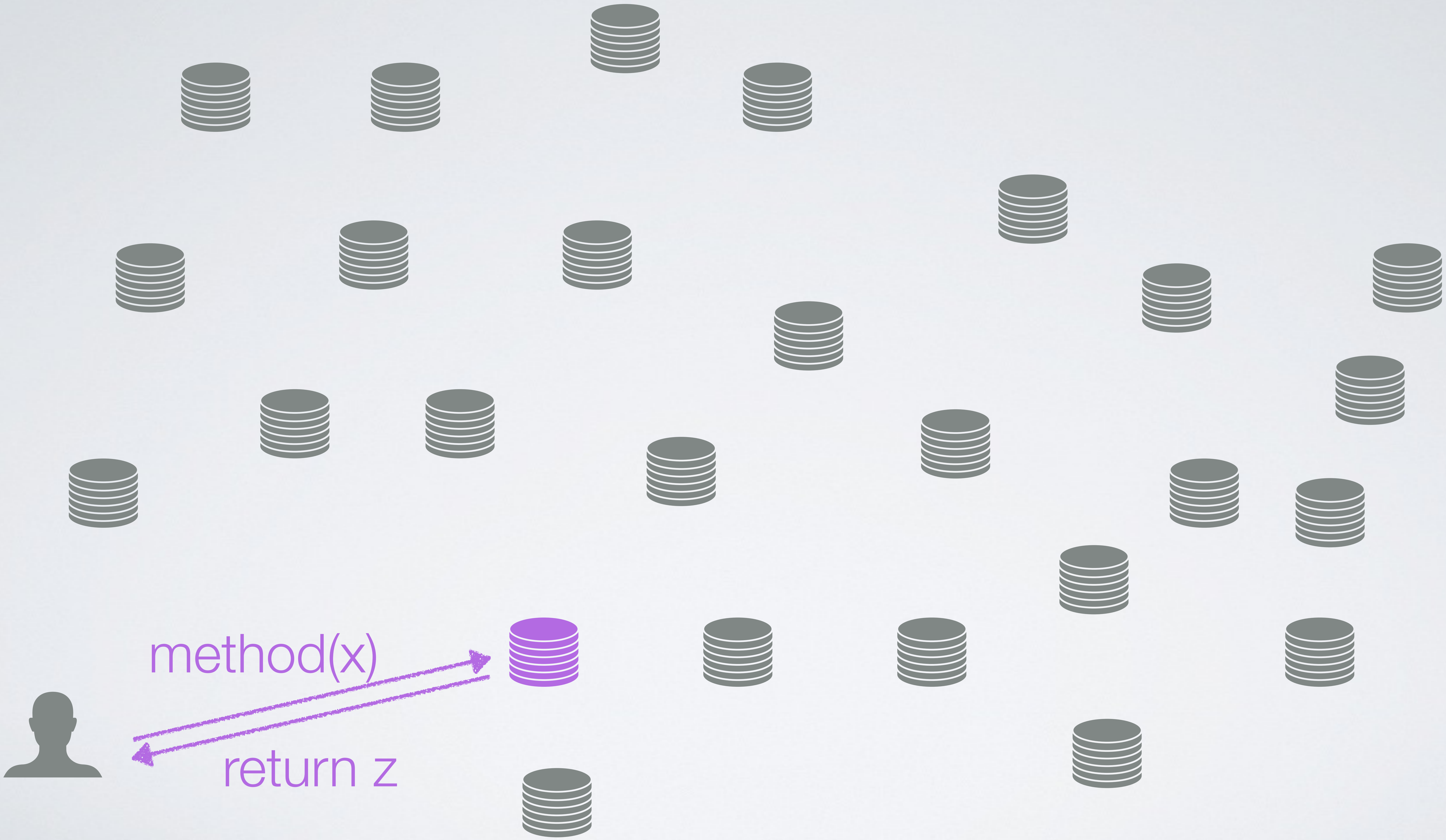
Cloud

method(x)

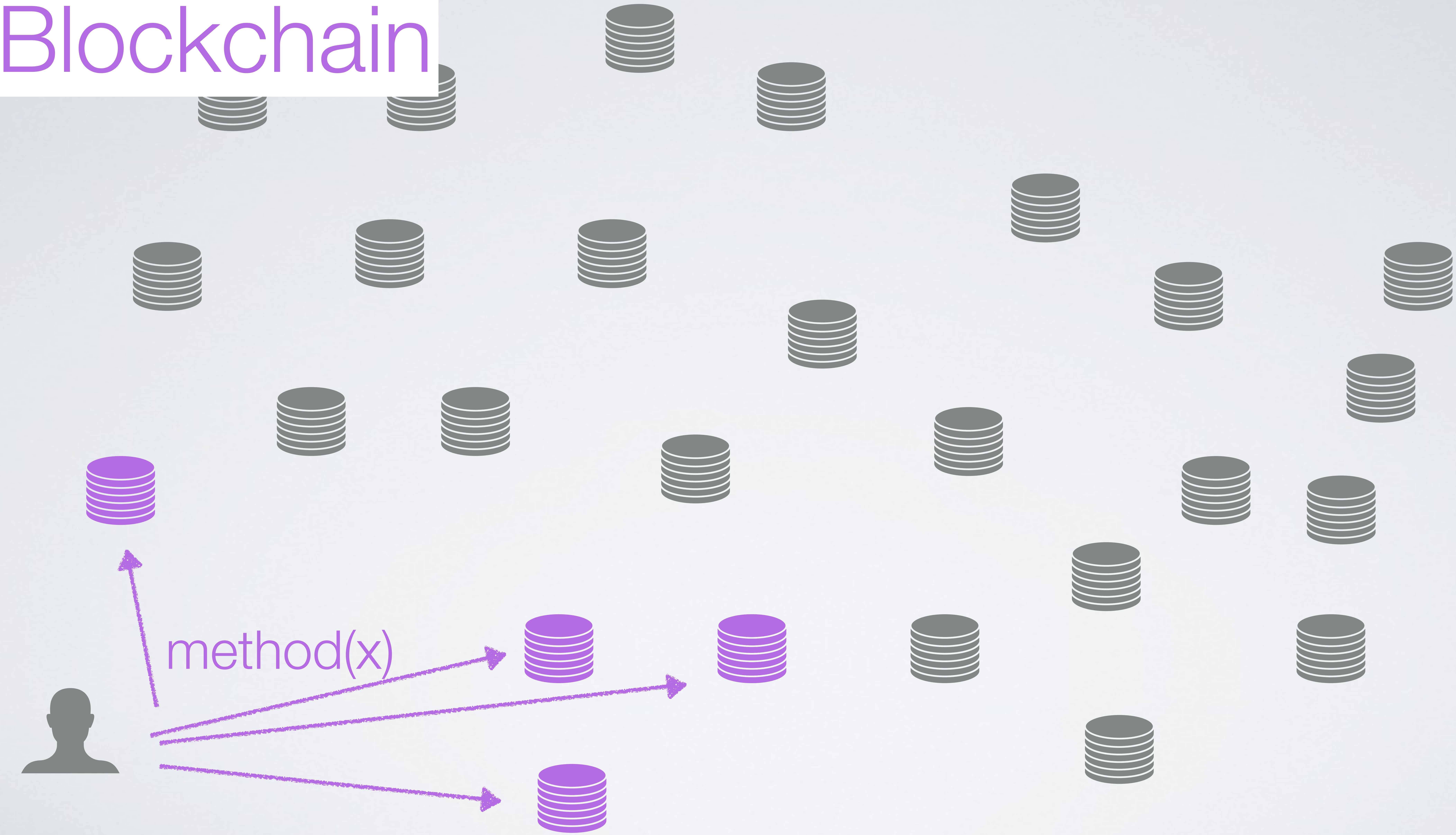


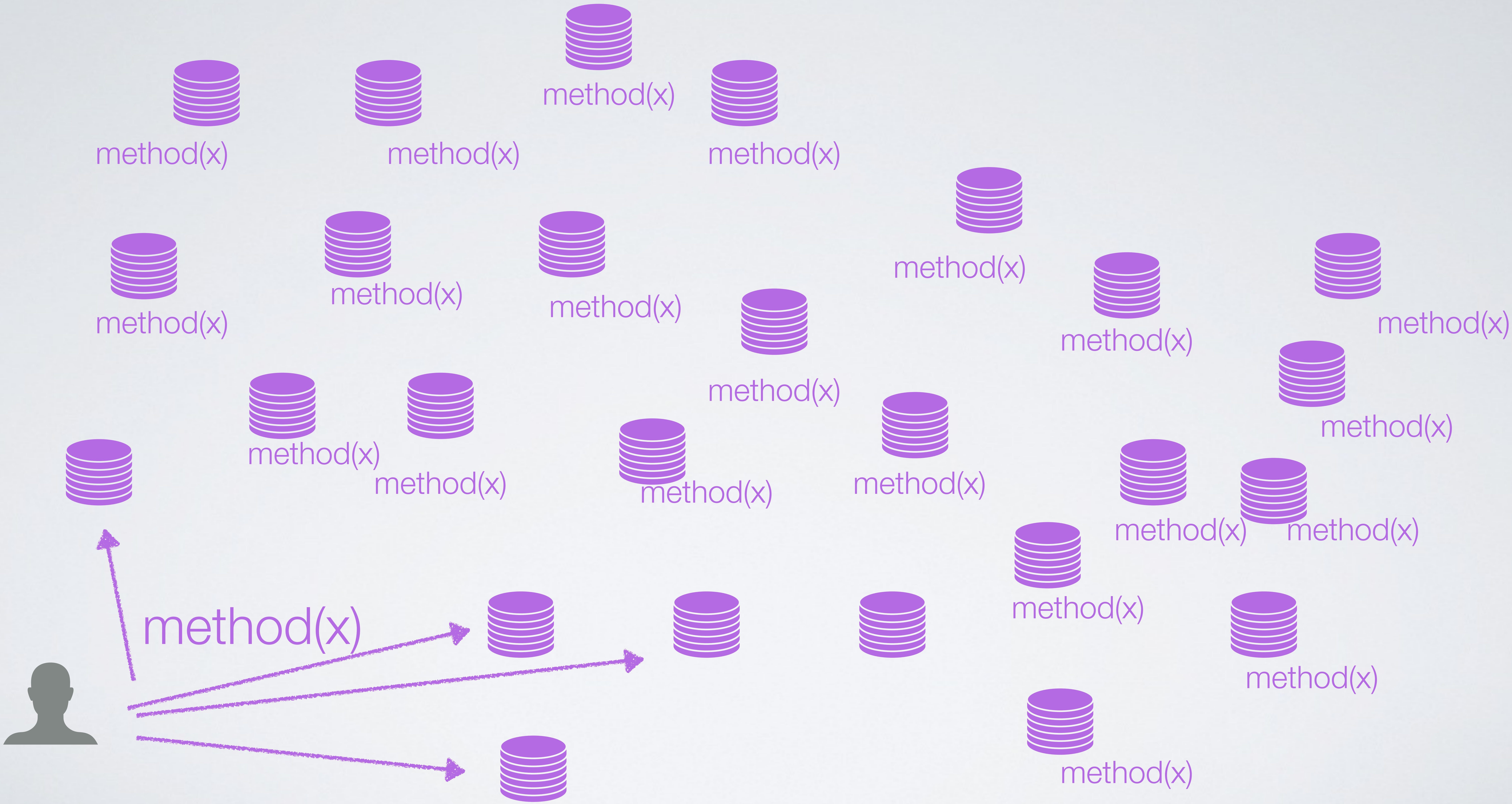
method(x)

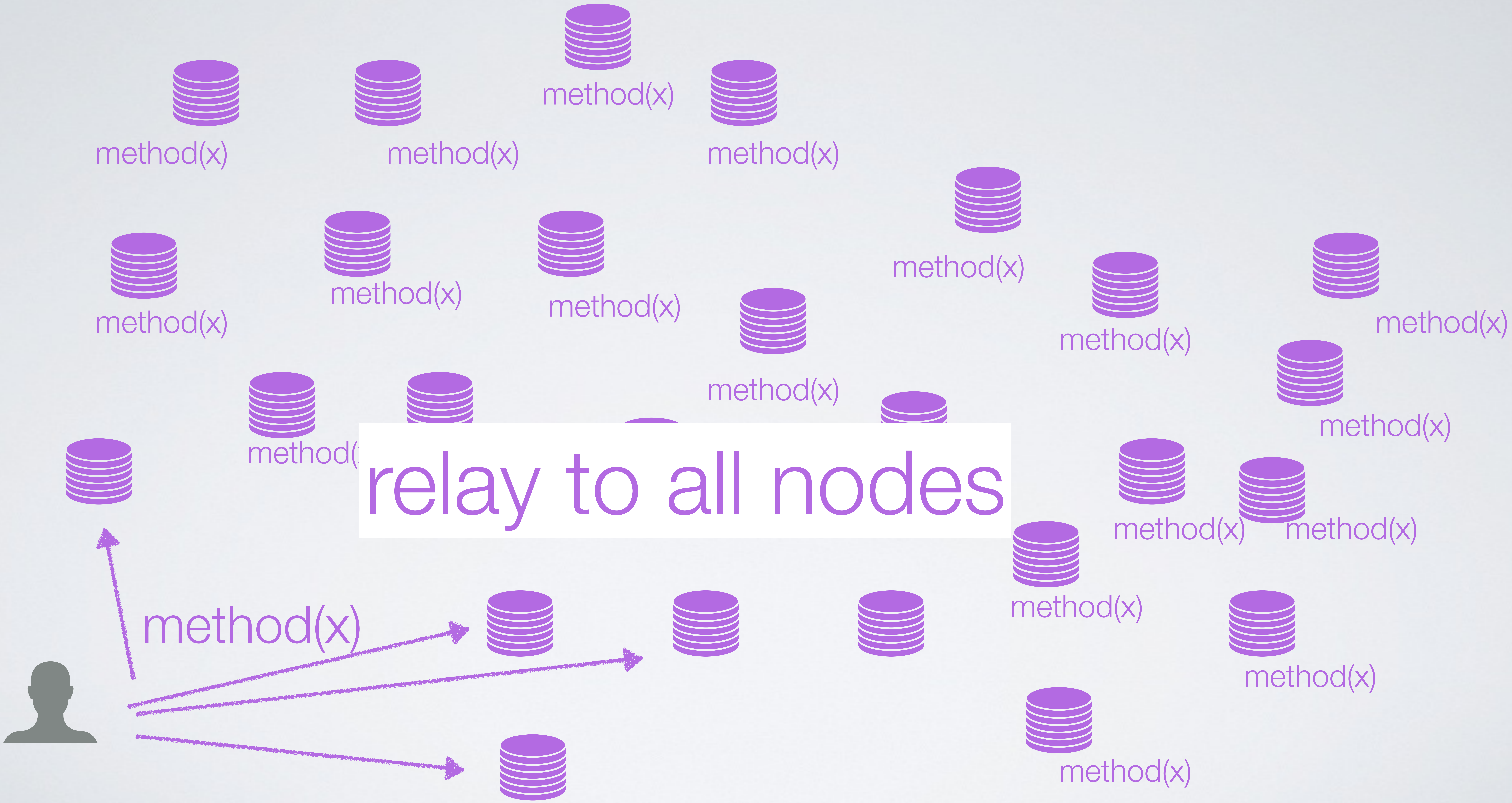

method(x)


method(x)
return z

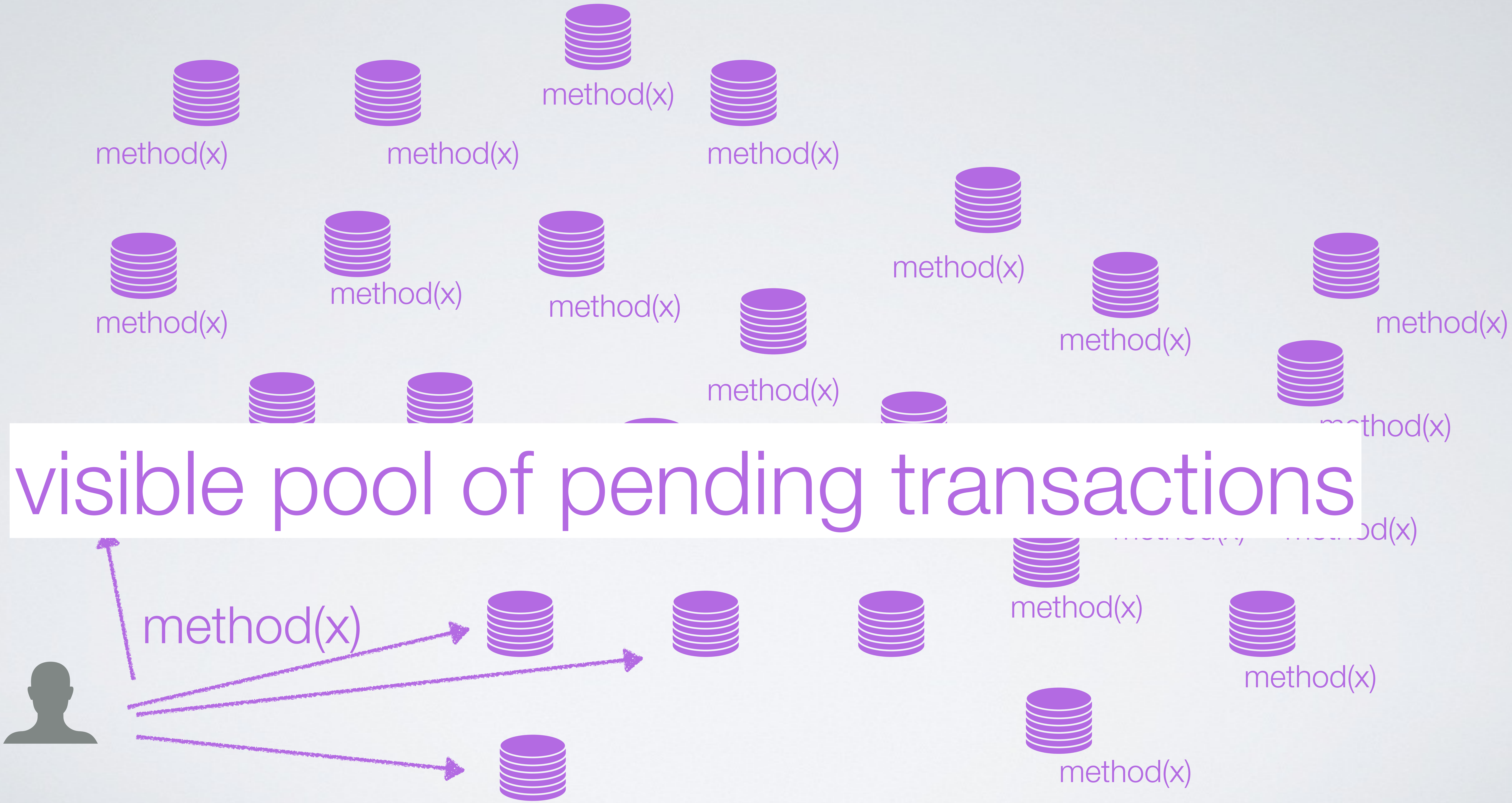
Blockchain



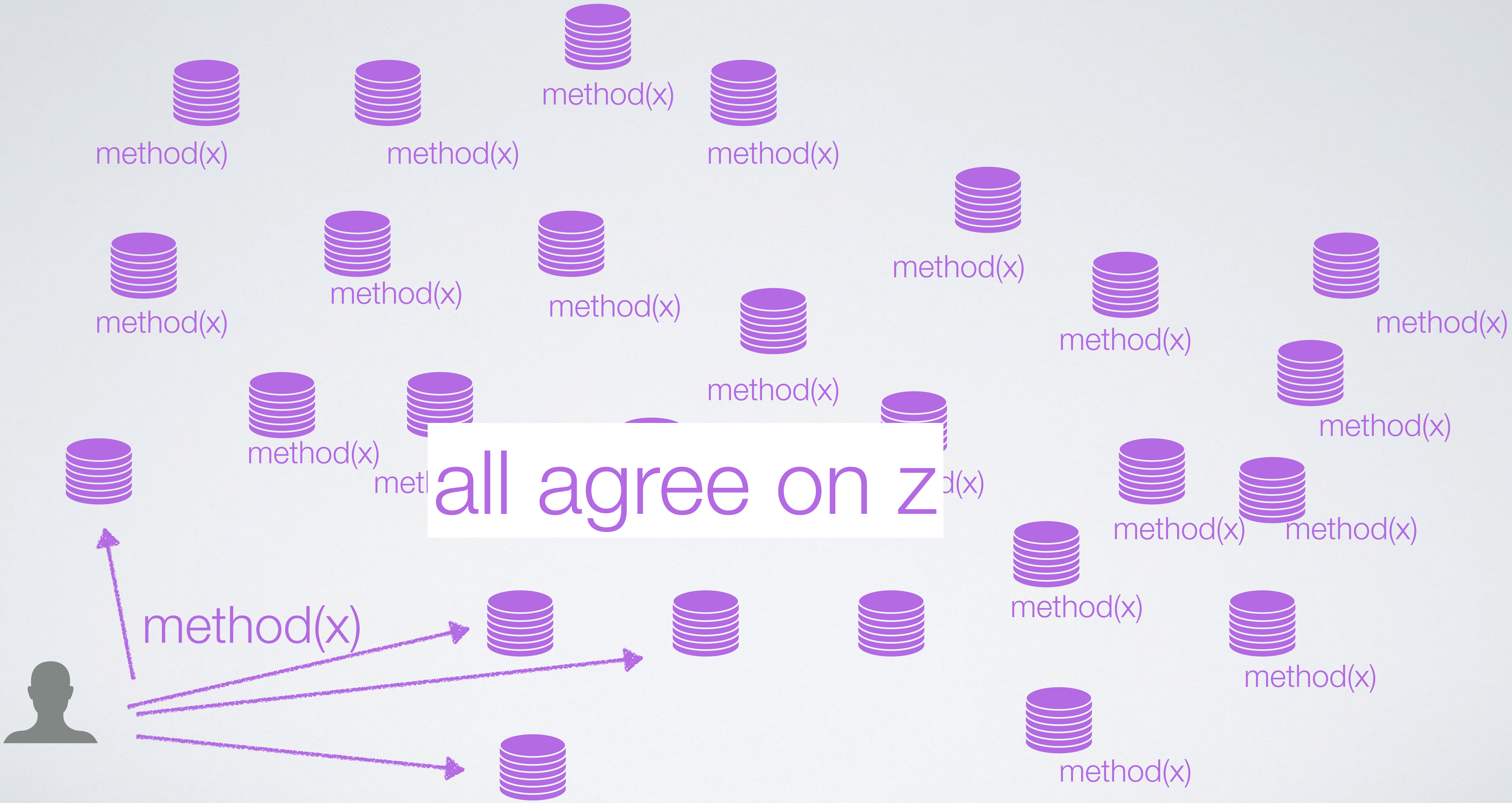

method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)
method(x)



relay to all nodes

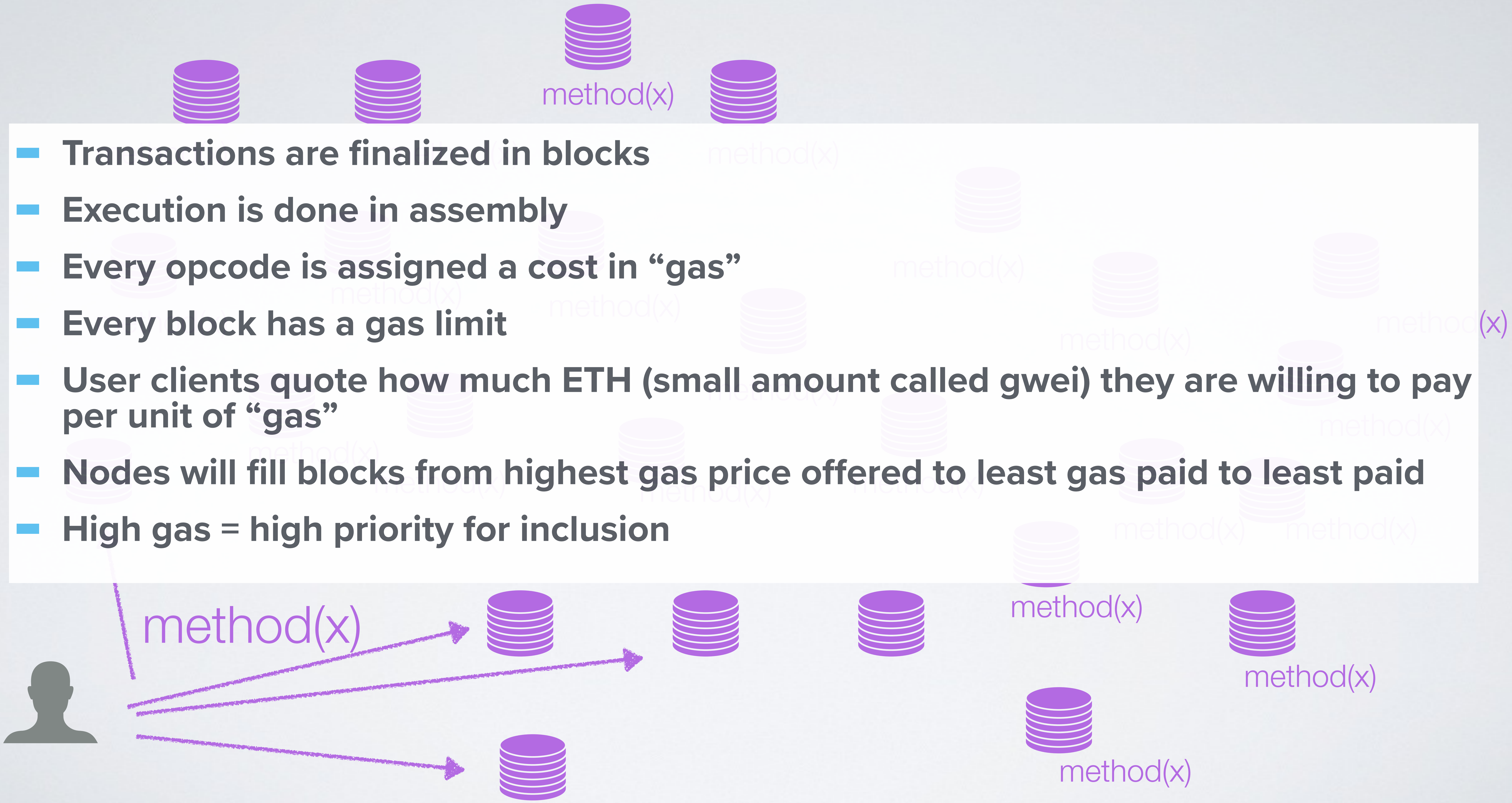


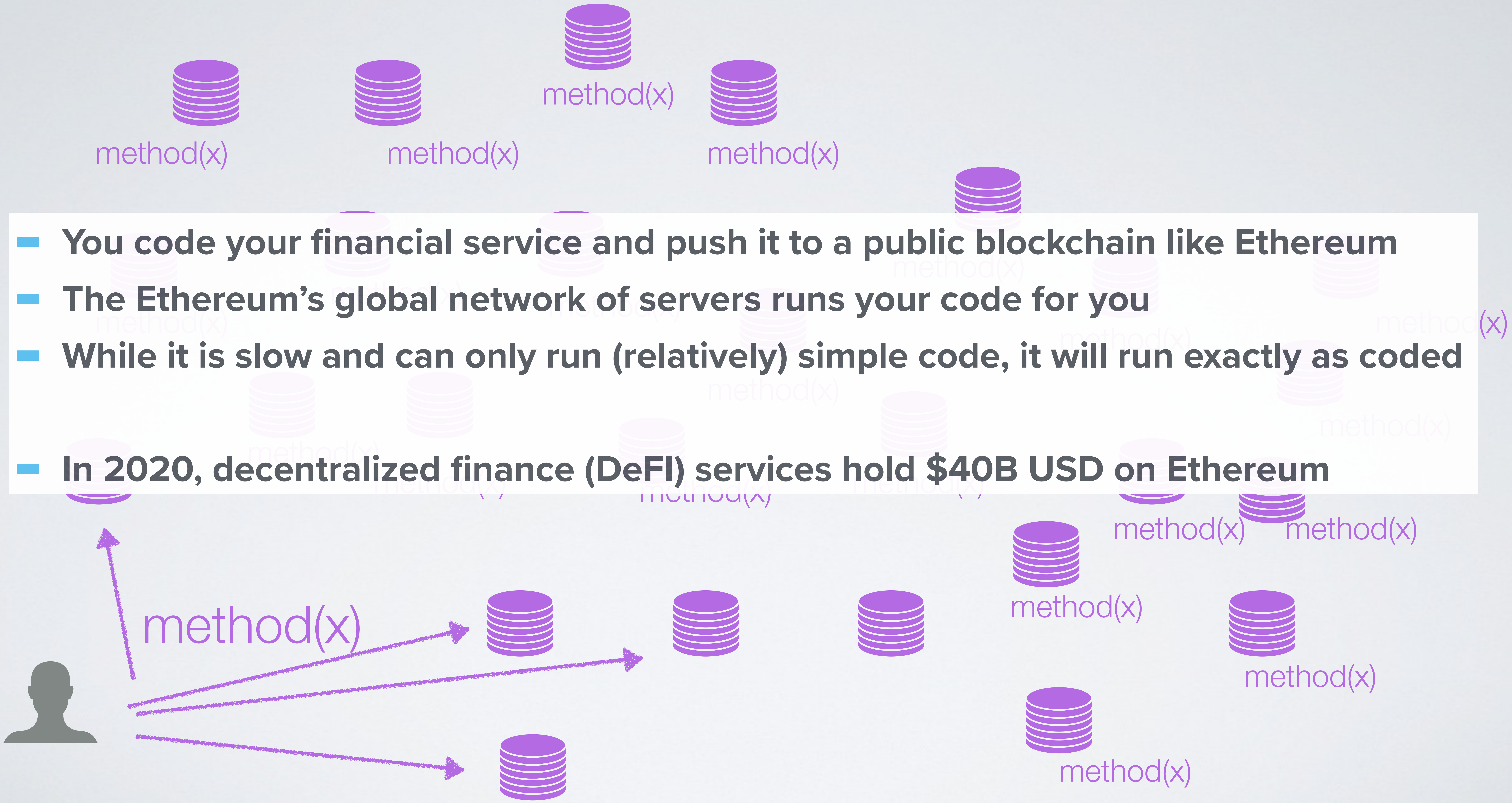
visible pool of pending transactions



all agree on z

- Transactions are finalized in blocks
- Execution is done in assembly
- Every opcode is assigned a cost in “gas”
- Every block has a gas limit
- User clients quote how much ETH (small amount called gwei) they are willing to pay per unit of “gas”
- Nodes will fill blocks from highest gas price offered to least gas paid to least paid
- High gas = high priority for inclusion





- You code your financial service and push it to a public blockchain like Ethereum
- The Ethereum's global network of servers runs your code for you
- While it is slow and can only run (relatively) simple code, it will run exactly as coded

- In 2020, decentralized finance (DeFI) services hold $40B USD on Ethereum

Story #1

ICO hype circa 2017

Brand Promise
Dropil offers both reliability and safety in a volatile market. Utilizing smart learning bot trading, diversification, tested indicator algo-trading, and auto portfolio management Dex is able to offer the best returns possible to you stress free.

User Portal
-Multiple insight tabs
-Secure personal wallets
-Planning and tracking tools

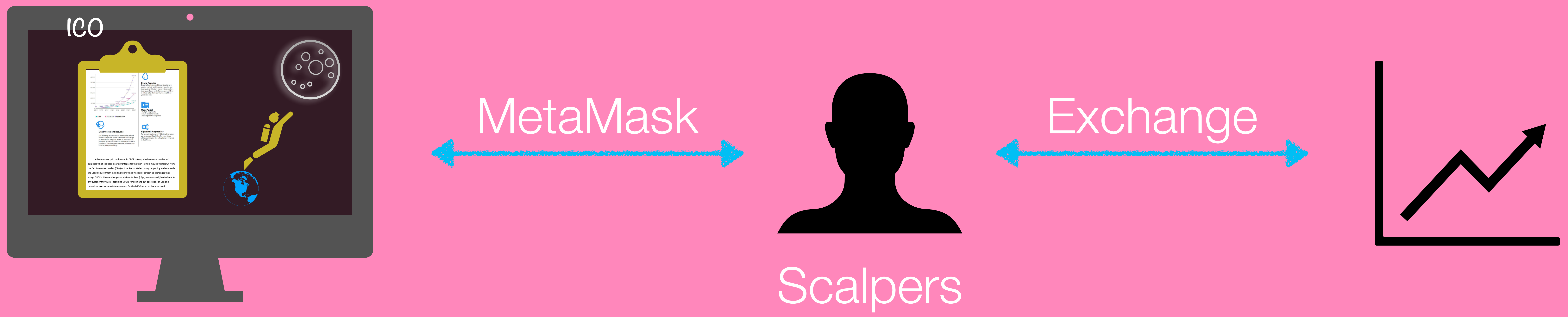
Dex Investment Returns

The following returns are the estimated standard for each respective mode: Safe mode will average an annual time weighted return of 24-45% of the principal, Moderate moves the returns estimate to 39-63% and finally Aggressive Mode will return 57-83% the principal funding.

High Limit Augmenter
For users investing over $100k into Dex return percentages will be higher for every Mode while retaining the risk safety factors inherent in that Mode.

All returns are paid to the user in DROP tokens, which serves a number of purposes which includes clear advantages for the user. DROPs may be withdrawn from the Dex Investment Wallet (DIW) or User Portal Wallet to any supporting wallet outside the Dropil environment including user owned wallets or directly to exchanges that accept DROPs. From exchanges or via Peer to Peer (p2p), users may sell/trade drops for any currency they wish. Requiring DROPs for all in and out operations of Dex and related services ensures future demand for the DROP token so that users and

ICO hype circa 2017



MetaMask

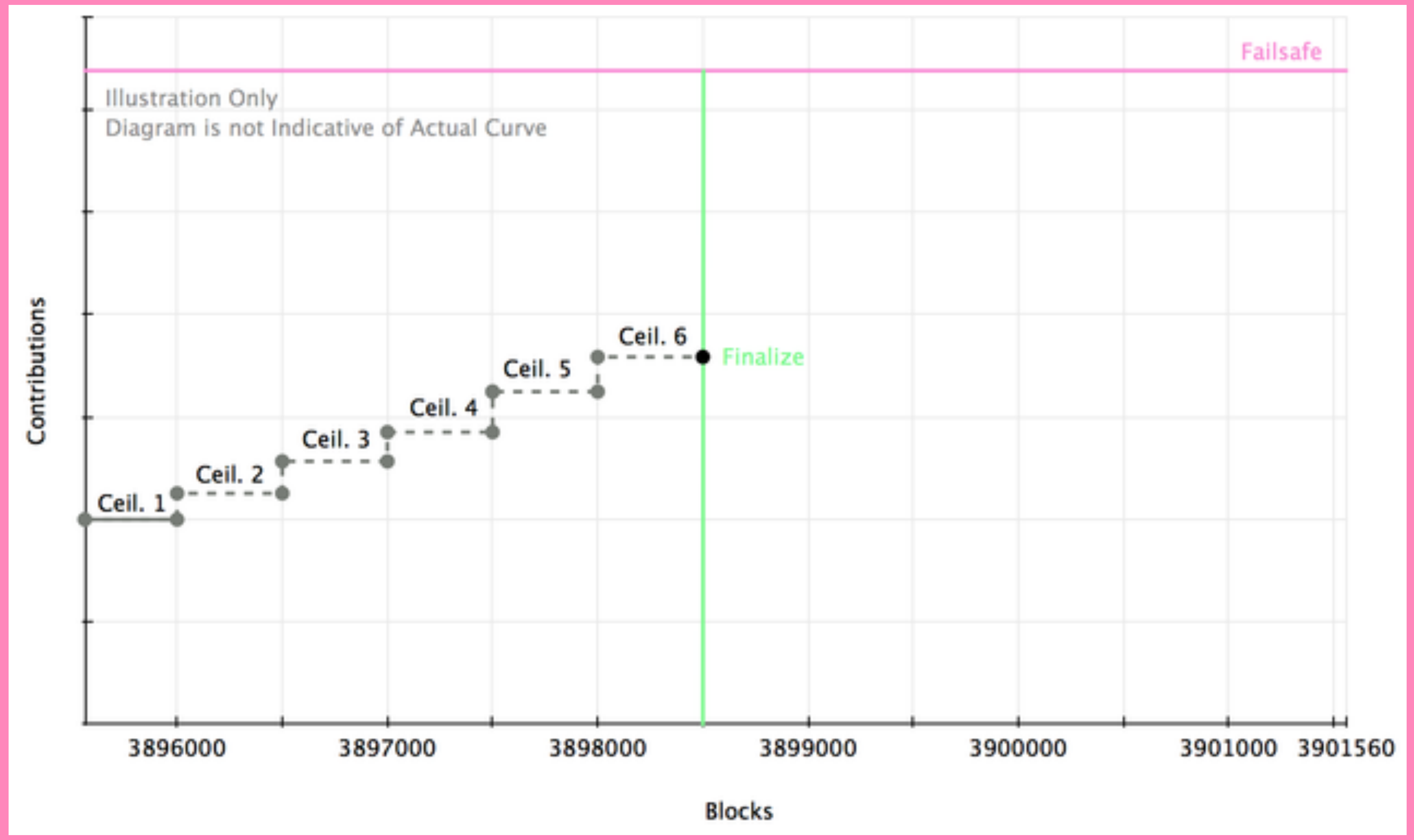
Exchange

Scalpers

Status: Fair ICO

Status: Fair ICO

- Dynamic Cap/Ceiling // Maximum deposit amount per ceiling
-



Status: Fair ICO

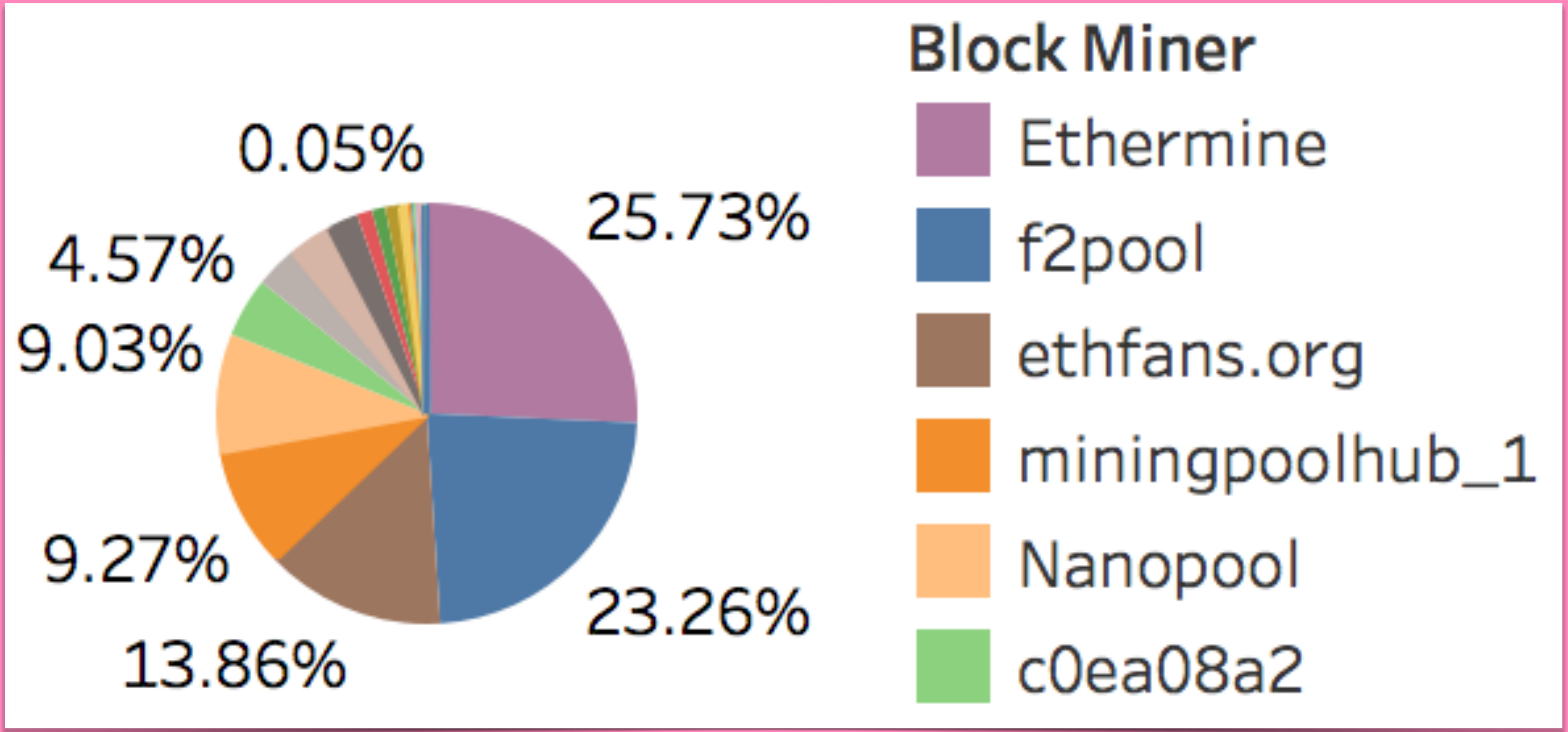
- Dynamic Cap/Ceiling // Maximum deposit amount per ceiling
- Limit GasPrice // require(gasPrice < 50 gwei)

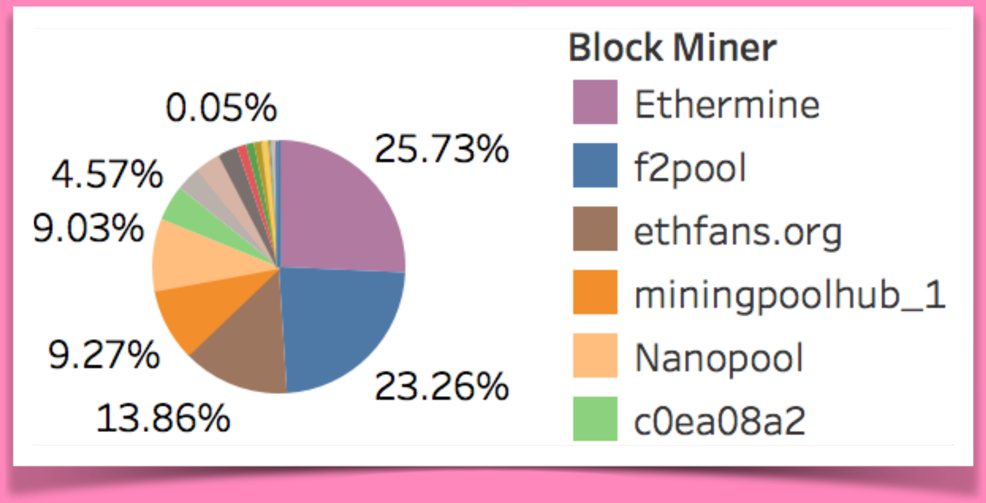
Status: Fair ICO

- June 2017
- Raised: ~300,000 ETH (~$90M USD) in 16 hours
- Refunded 111,161 attempts
  - Total of: 347,154 ETH

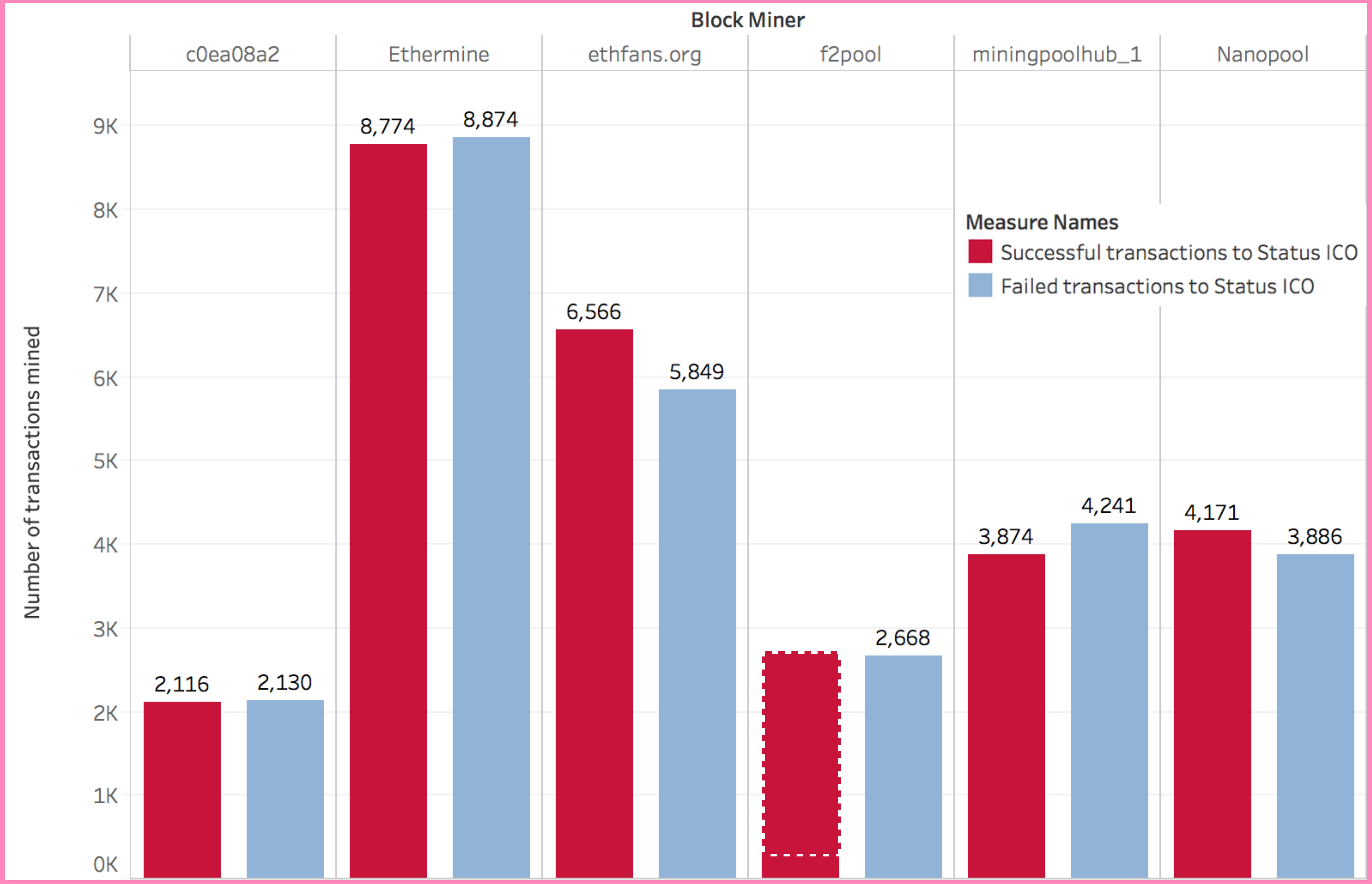
- We define:
  - ***Successful transaction***: resulted in token purchase
  - ***Failed transaction***: failed to purchase any tokens (high gasPrice, over cap, etc)
    - Result of buyers treating Status like a generic ICO

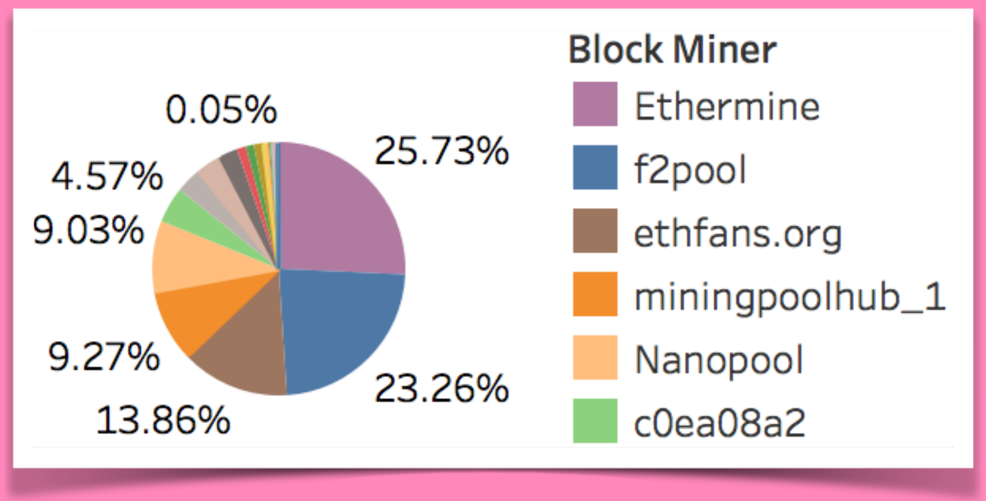
Status: Fair ICO



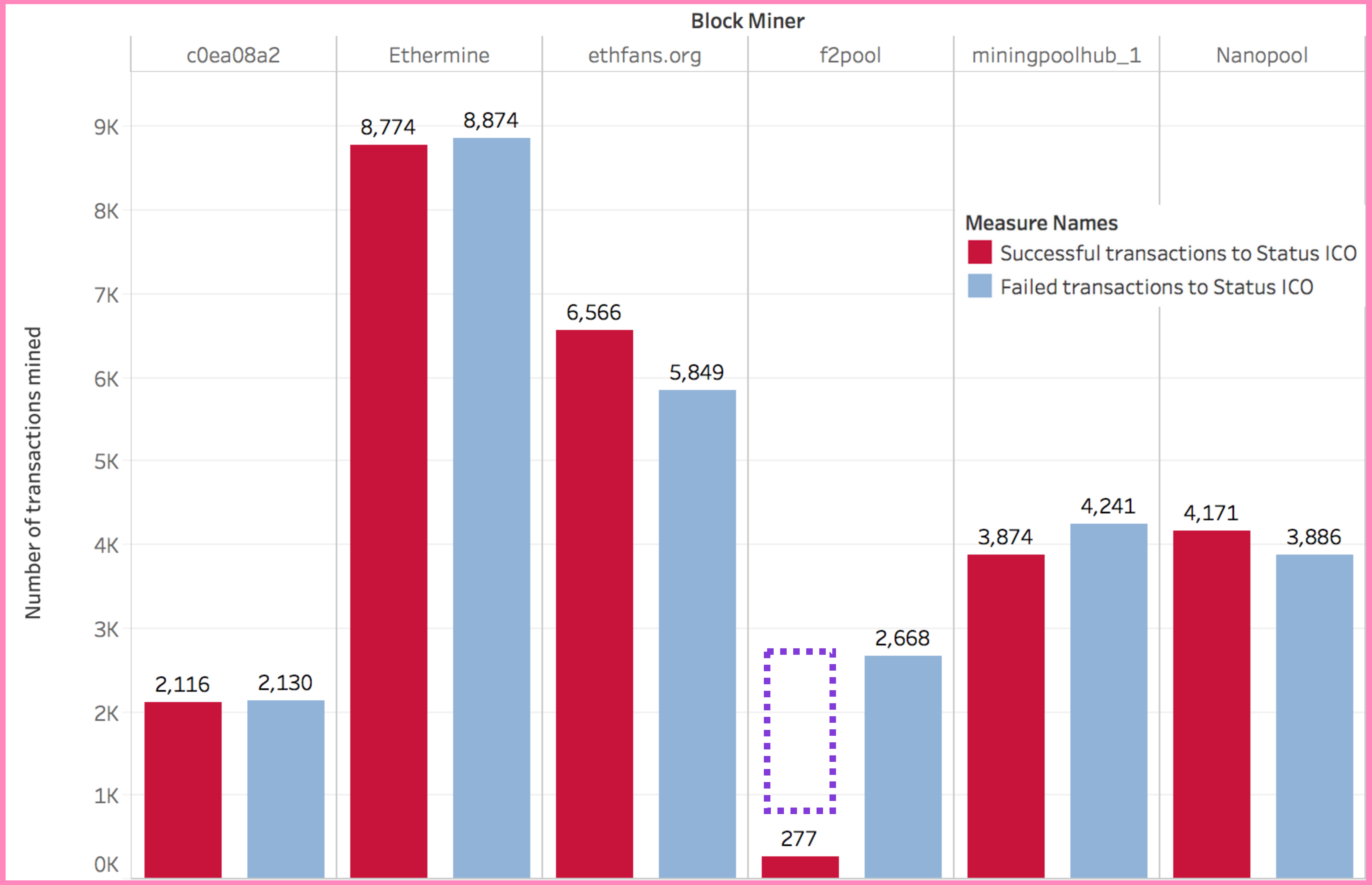


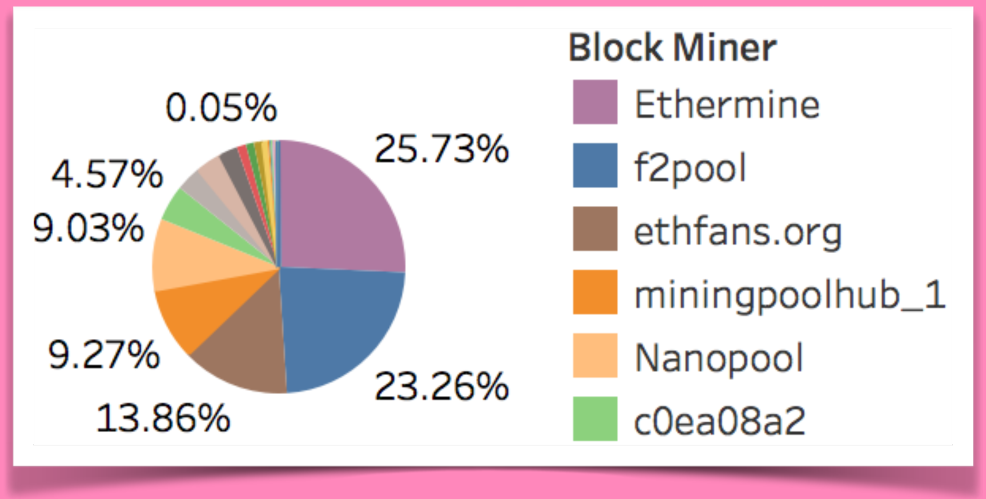
Status: Fair ICO



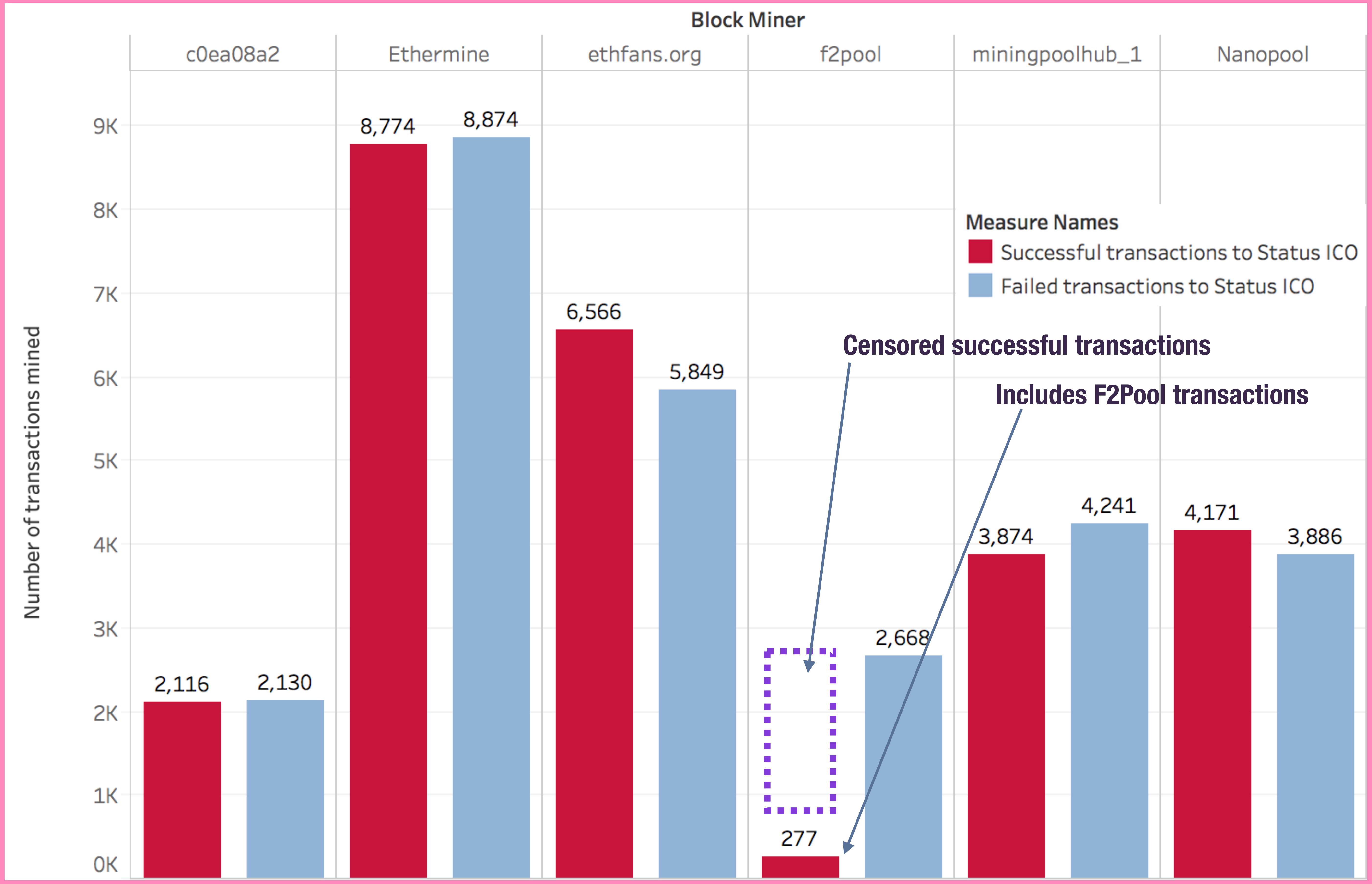


Status: Fair ICO





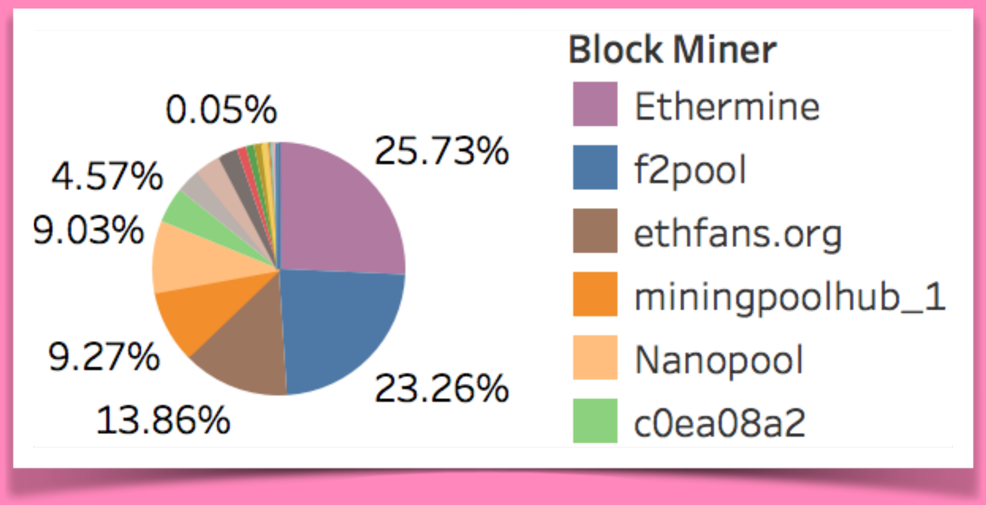
Status: Fair ICO

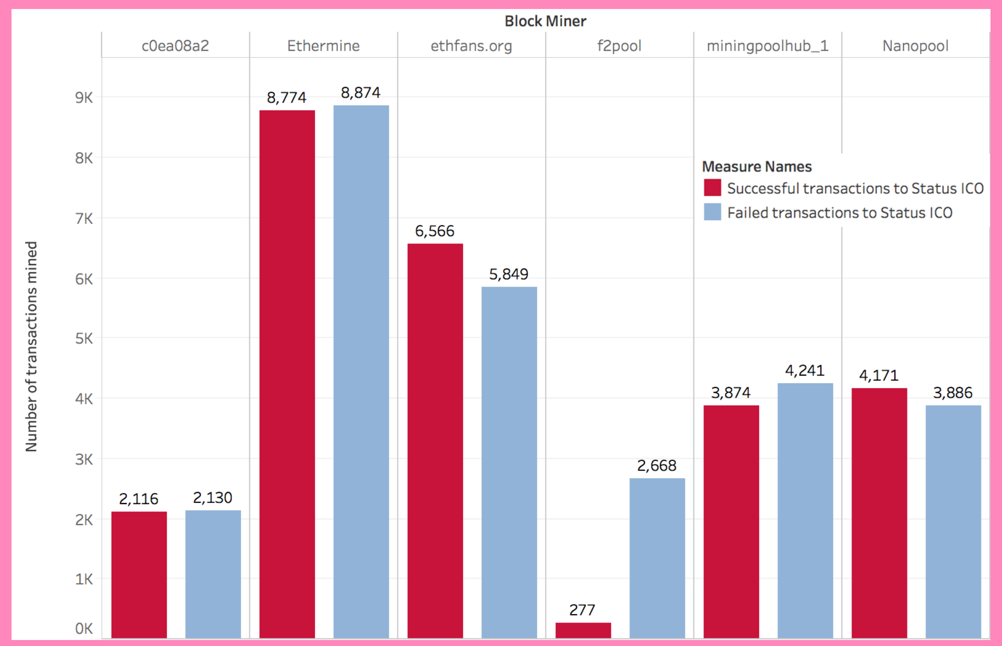


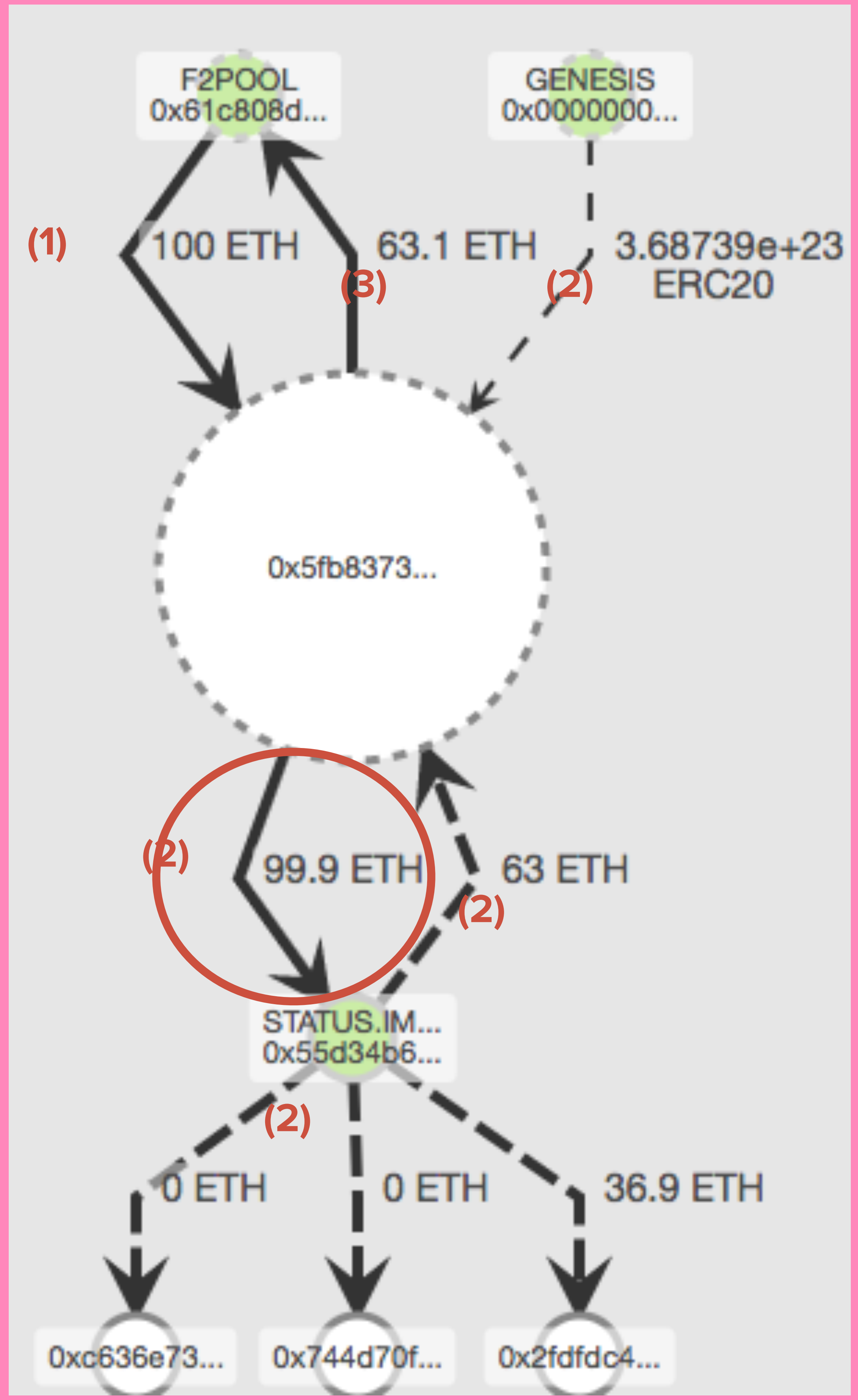
Censored successful transactions

Includes F2Pool transactions

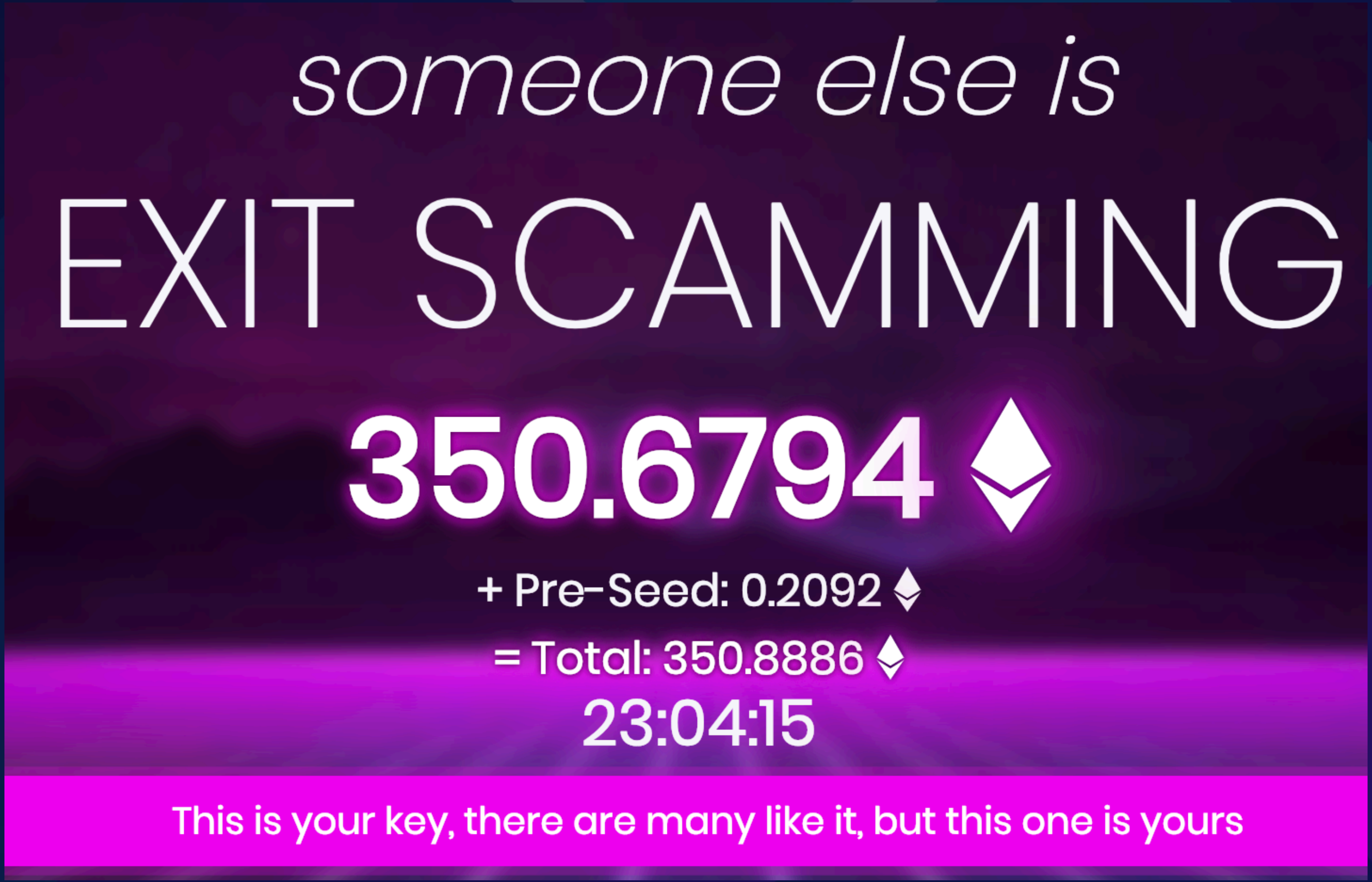
Status: Fair ICO







Story #2



someone else is

EXIT SCAMMING

350.6794 ♦

+ Pre-Seed: 0.2092 ♦

= Total: 350.8886 ♦

23:04:15

This is your key, there are many like it, but this one is yours

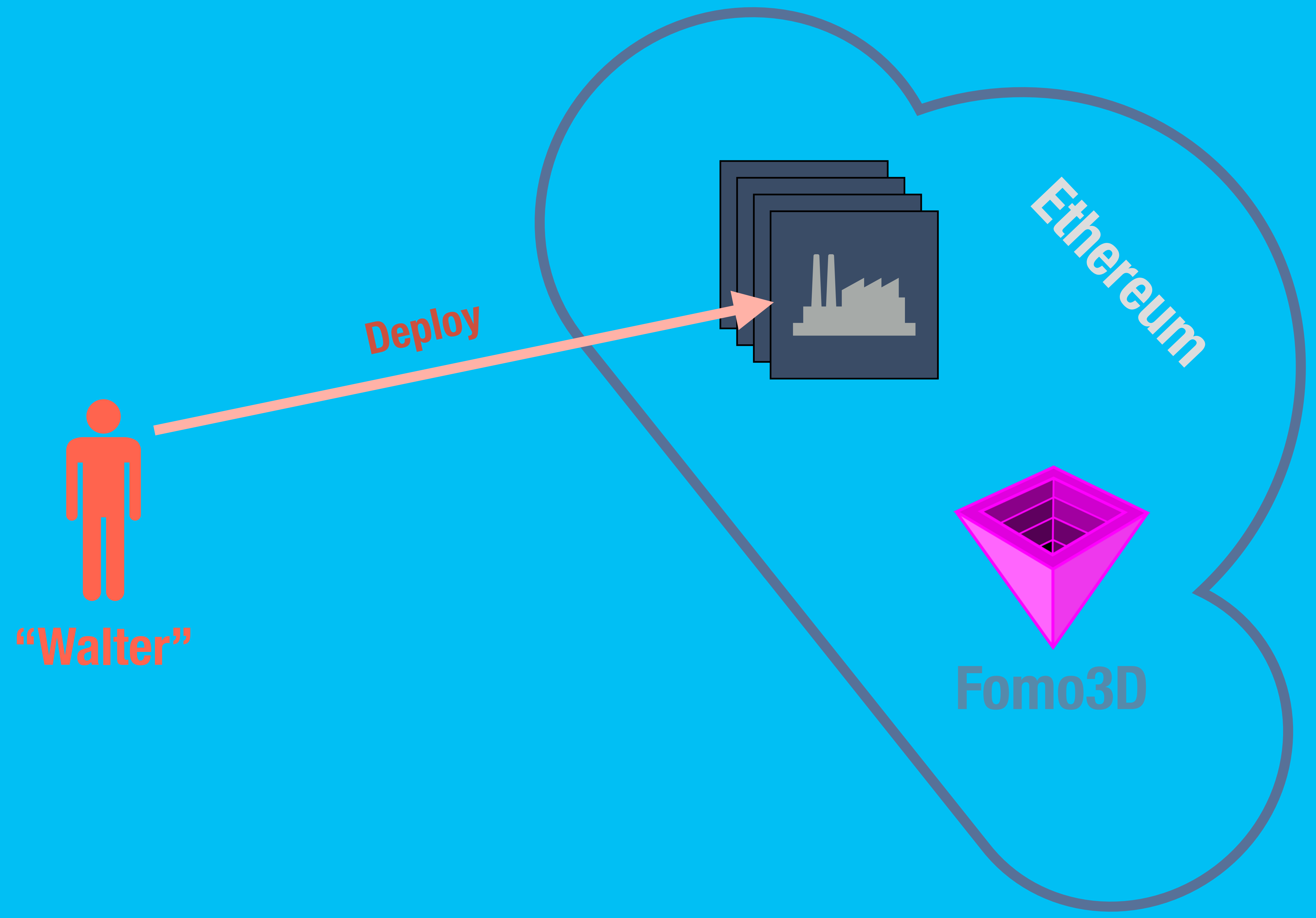
FOMO3D

FOMO3D

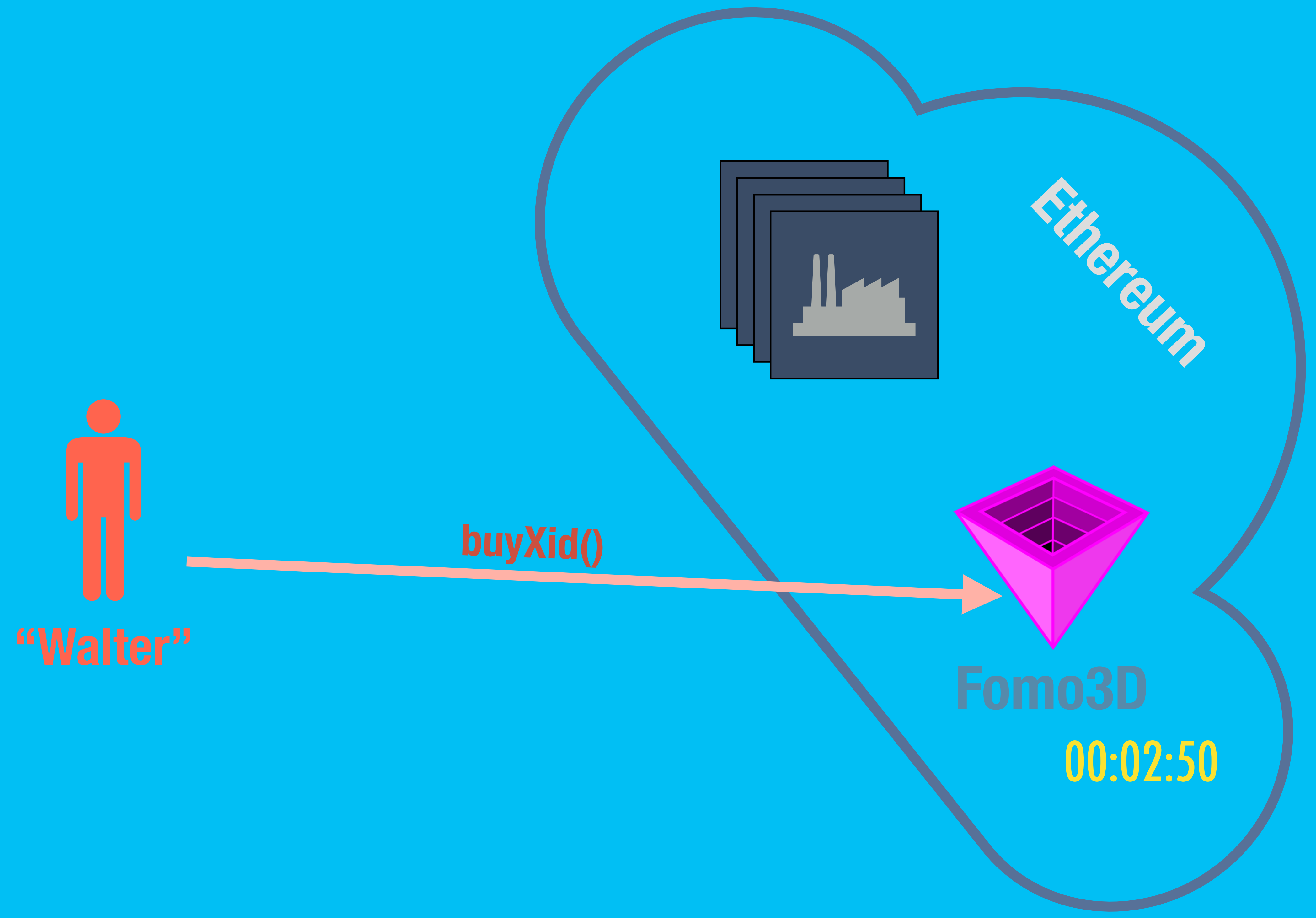
- A countdown timer
- Every ticket purchase increases the timer by 30 seconds
- The last ticket when the timer reaches 00:00:00 wins the pot

FOMO3D

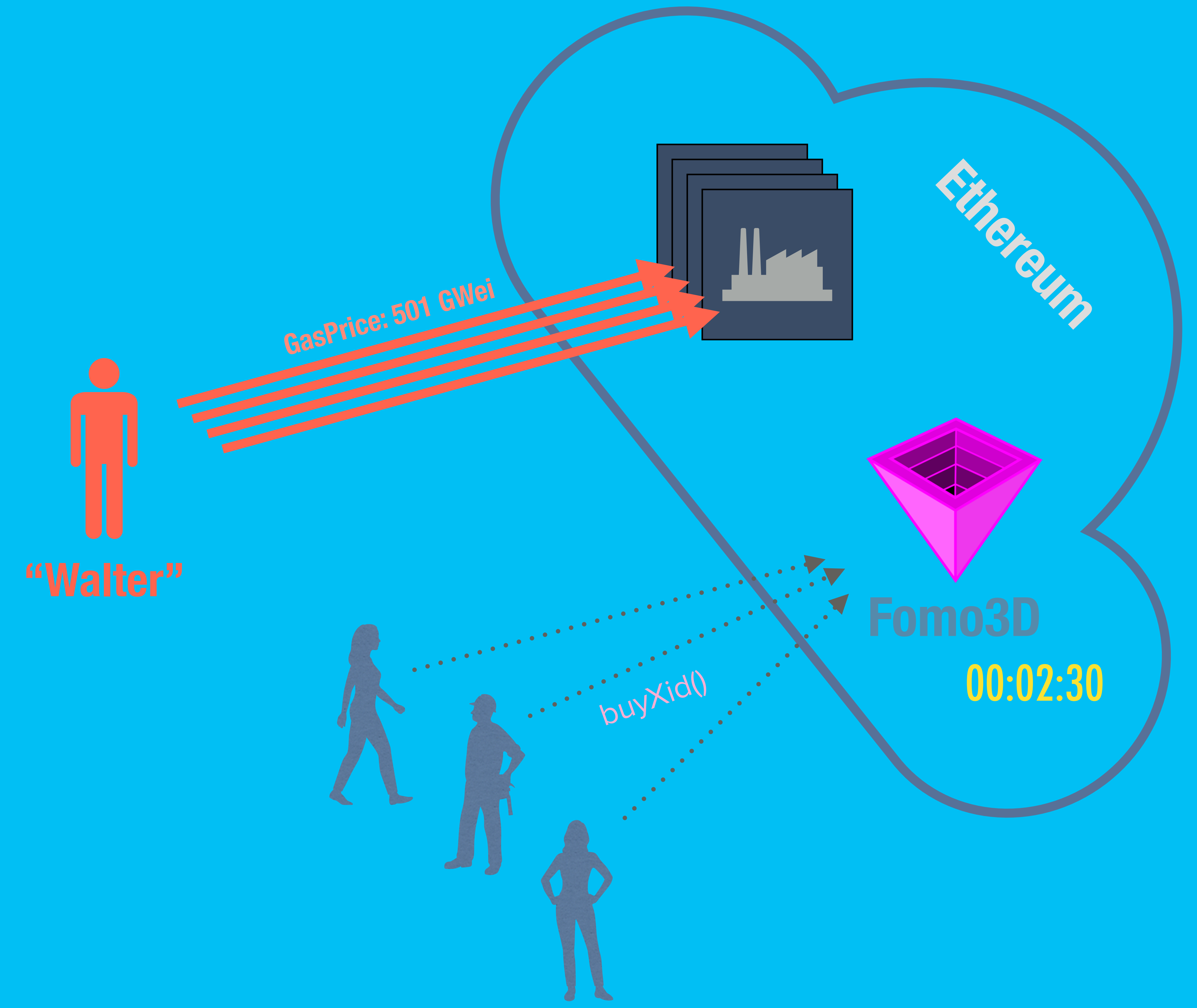
- “Walter” deploys contracts that has high gas consumption



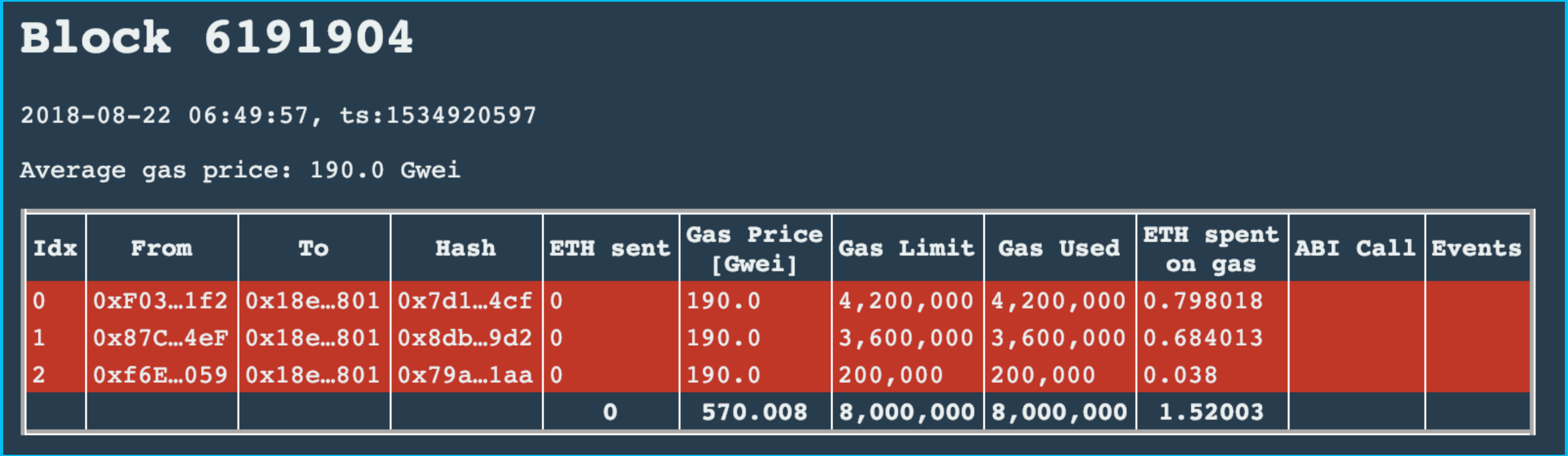
FOMO3D



FOMO3D



FOMO3D



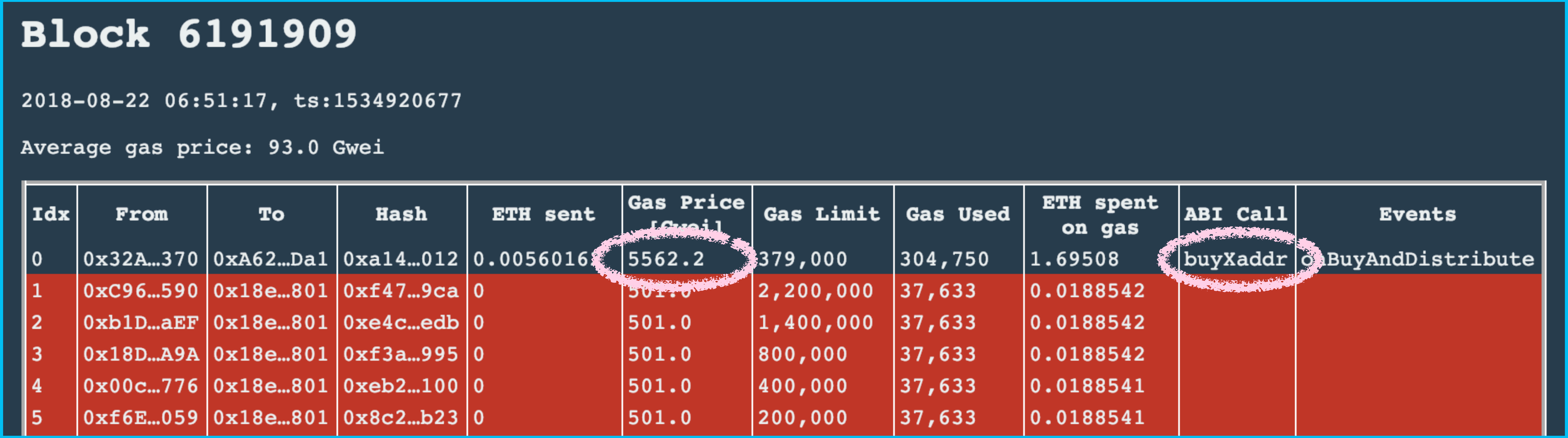
Block 6191904

2018-08-22 06:49:57, ts:1534920597

Average gas price: 190.0 Gwei

Idx	From	To	Hash	ETH sent	Gas Price [Gwei]	Gas Limit	Gas Used	ETH spent on gas	ABI Call	Events
0	0xF03…1f2	0x18e…801	0x7d1…4cf	0	190.0	4,200,000	4,200,000	0.798018		
1	0x87C…4eF	0x18e…801	0x8db…9d2	0	190.0	3,600,000	3,600,000	0.684013		
2	0xf6E…059	0x18e…801	0x79a…1aa	0	190.0	200,000	200,000	0.038		
				0	570.008	8,000,000	8,000,000	1.52003		

FOMO3D



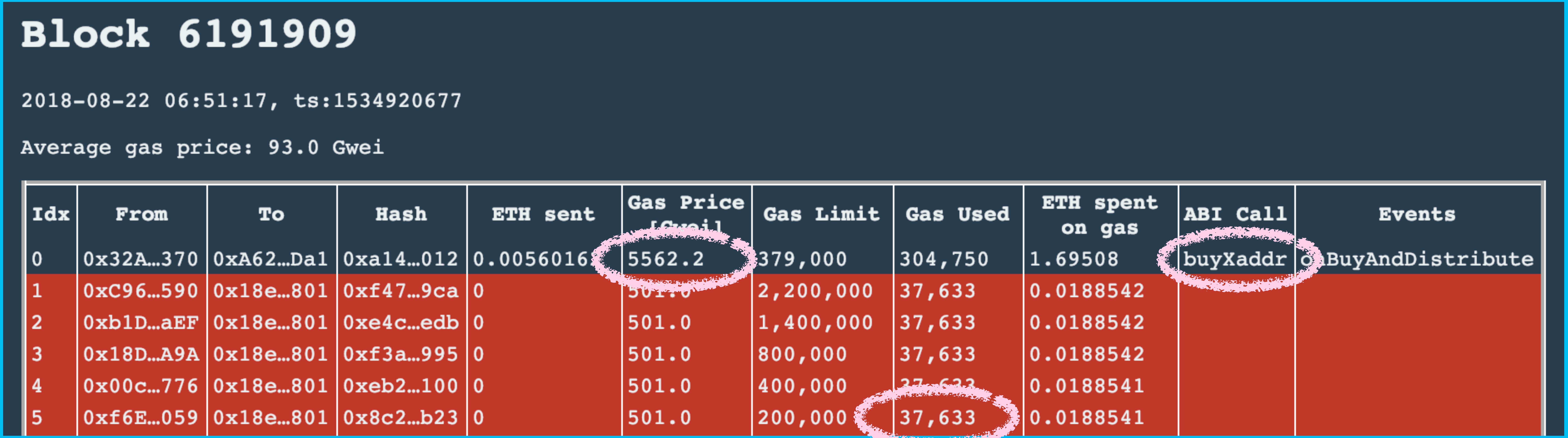
Block 6191909

2018-08-22 06:51:17, ts:1534920677

Average gas price: 93.0 Gwei

Idx	From	To	Hash	ETH sent	Gas Price [Gwei]	Gas Limit	Gas Used	ETH spent on gas	ABI Call	Events
0	0x32A…370	0xA62…Da1	0xa14…012	0.0056016	5562.2	379,000	304,750	1.69508	buyXaddr	onBuyAndDistribute
1	0xC96…590	0x18e…801	0xf47…9ca	0	501.0	2,200,000	37,633	0.0188542		
2	0xb1D…aEF	0x18e…801	0xe4c…edb	0	501.0	1,400,000	37,633	0.0188542		
3	0x18D…A9A	0x18e…801	0xf3a…995	0	501.0	800,000	37,633	0.0188542		
4	0x00c…776	0x18e…801	0xeb2…100	0	501.0	400,000	37,633	0.0188541		
5	0xf6E…059	0x18e…801	0x8c2…b23	0	501.0	200,000	37,633	0.0188541		

FOMO3D



Block 6191909

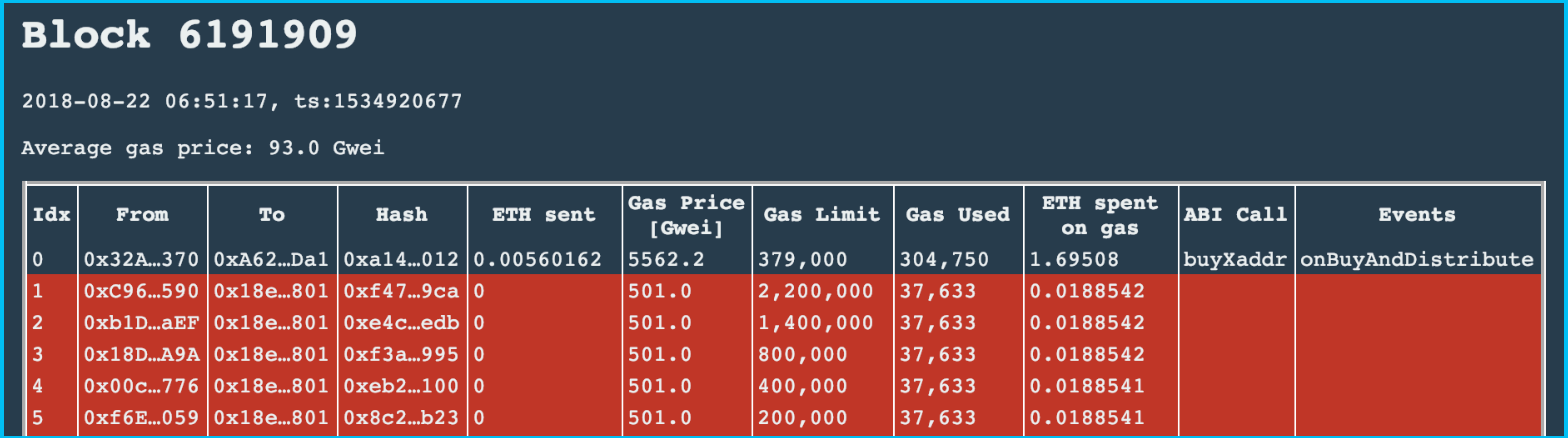
2018-08-22 06:51:17, ts:1534920677

Average gas price: 93.0 Gwei

Idx	From	To	Hash	ETH sent	Gas Price [Gwei]	Gas Limit	Gas Used	ETH spent on gas	ABI Call	Events
0	0x32A…370	0xA62…Da1	0xa14…012	0.0056016	5562.2	379,000	304,750	1.69508	buyXaddr	onBuyAndDistribute
1	0xC96…590	0x18e…801	0xf47…9ca	0	501.0	2,200,000	37,633	0.0188542		
2	0xb1D…aEF	0x18e…801	0xe4c…edb	0	501.0	1,400,000	37,633	0.0188542		
3	0x18D…A9A	0x18e…801	0xf3a…995	0	501.0	800,000	37,633	0.0188542		
4	0x00c…776	0x18e…801	0xeb2…100	0	501.0	400,000	37,633	0.0188541		
5	0xf6E…059	0x18e…801	0x8c2…b23	0	501.0	200,000	37,633	0.0188541		

versus 4,000,000

FOMO3D

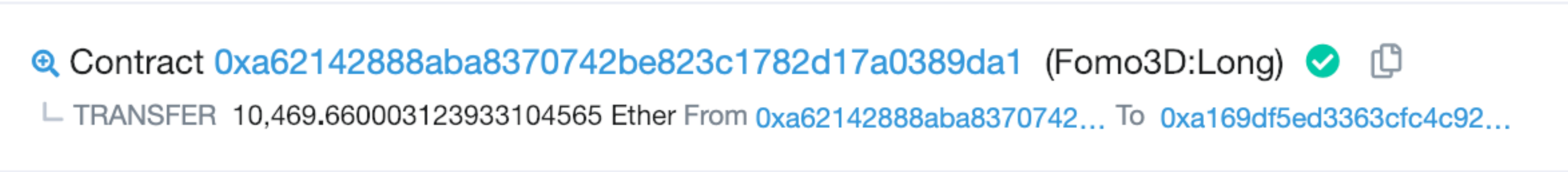


Block 6191909

2018-08-22 06:51:17, ts:1534920677

Average gas price: 93.0 Gwei

Idx	From	To	Hash	ETH sent	Gas Price [Gwei]	Gas Limit	Gas Used	ETH spent on gas	ABI Call	Events
0	0x32A…370	0xA62…Da1	0xa14…012	0.00560162	5562.2	379,000	304,750	1.69508	buyXaddr	onBuyAndDistribute
1	0xC96…590	0x18e…801	0xf47…9ca	0	501.0	2,200,000	37,633	0.0188542		
2	0xb1D…aEF	0x18e…801	0xe4c…edb	0	501.0	1,400,000	37,633	0.0188542		
3	0x18D…A9A	0x18e…801	0xf3a…995	0	501.0	800,000	37,633	0.0188542		
4	0x00c…776	0x18e…801	0xeb2…100	0	501.0	400,000	37,633	0.0188541		
5	0xf6E…059	0x18e…801	0x8c2…b23	0	501.0	200,000	37,633	0.0188541		



Contract 0xa62142888aba8370742be823c1782d17a0389da1 (Fomo3D:Long)

└ TRANSFER 10,469.660003123933104565 Ether From 0xa62142888aba8370742… To 0xa169df5ed3363cfc4c92…

~$3M

What do these stories have in common?

- All (full) nodes in the network have access to “privileged information”
- Gas auction: bribing miners with high fees (GasPrice)
- Miners/Validators/Proposers (nodes that create blocks) have extra power: order transactions in blocks that they create
  - Miner Extractable Value (MEV)

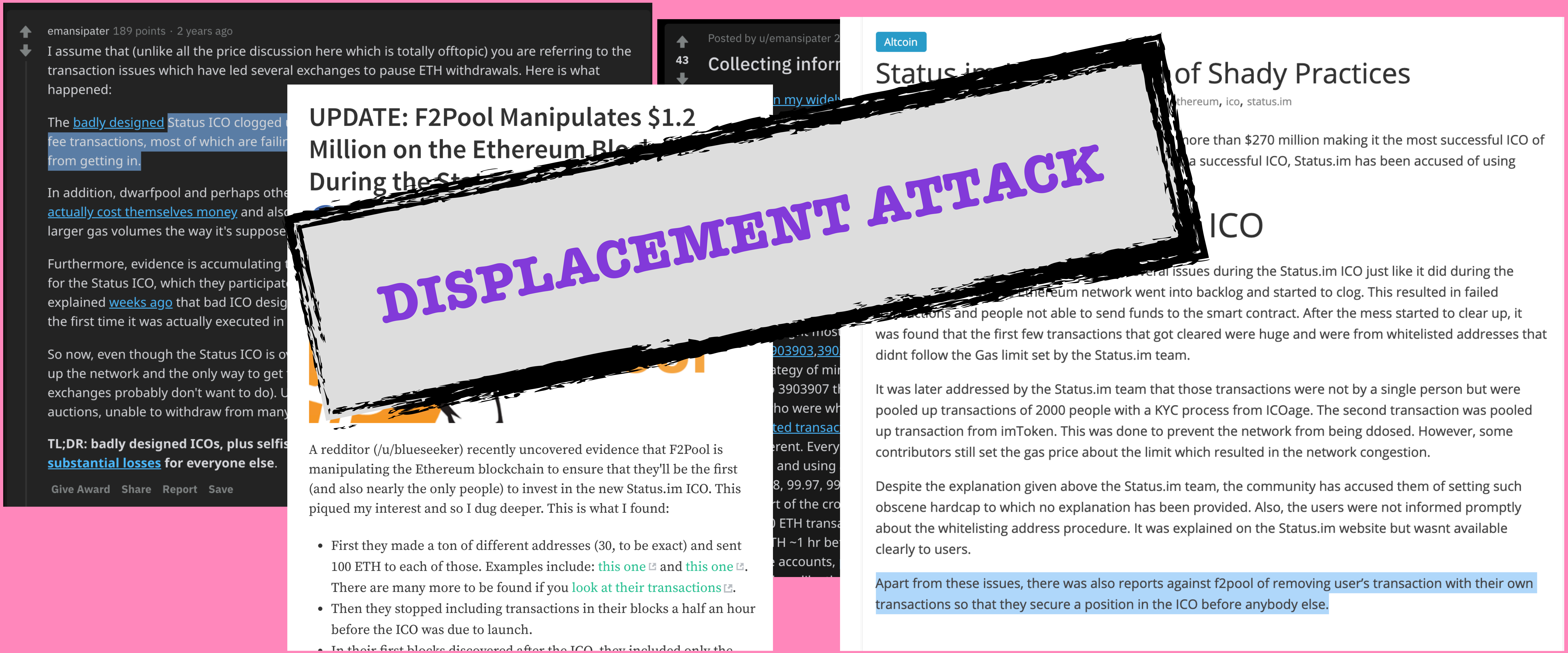
What do these stories have in common?

All examples of “front-running” attacks
But are they all the same attack?

Taxonomy of Front-running attacks

Attack Type	*Description*	*Example*
Displacement	**Not important** to the adversary for original function call **to run after her function.**	Domain Name Registration
Insertion	**Important** to the adversary for original function call to **run after her function.**	Asset Trading
Suppression *(aka block stuffing)*	Run function and **delay original function** call	Auction Sniping

Story 1: Status ICO



DISPLACEMENT ATTACK

emansipater 189 points · 2 years ago

I assume that (unlike all the price discussion here which is totally offtopic) you are referring to the transaction issues which have led several exchanges to pause ETH withdrawals. Here is what happened:

The badly designed Status ICO clogged
fee transactions, most of which are failin
from getting in.

In addition, dwarfpool and perhaps othe
actually cost themselves money and also
larger gas volumes the way it's suppose

Furthermore, evidence is accumulating
for the Status ICO, which they participat
explained weeks ago that bad ICO desig
the first time it was actually executed in

So now, even though the Status ICO is o
up the network and the only way to get
exchanges probably don't want to do). U
auctions, unable to withdraw from many

TL;DR: badly designed ICOs, plus selfis
substantial losses for everyone else.

Give Award Share Report Save

Posted by u/emansipater 2

43

Collecting inforr

n my widel

903903,390

ategy of mi

3903907 t

ho were wh

ted transac

erent. Every

and using

8, 99.97, 99

t of the cro

ETH transa

TH ~1 hr be

accounts,

UPDATE: F2Pool Manipulates $1.2 Million on the Ethereum Bl During the St

A redditor (/u/blueseeker) recently uncovered evidence that F2Pool is manipulating the Ethereum blockchain to ensure that they'll be the first (and also nearly the only people) to invest in the new Status.im ICO. This piqued my interest and so I dug deeper. This is what I found:

- First they made a ton of different addresses (30, to be exact) and sent 100 ETH to each of those. Examples include: this one and this one. There are many more to be found if you look at their transactions.
- Then they stopped including transactions in their blocks a half an hour before the ICO was due to launch.
- In their first blocks discovered after the ICO, they included only the

Altcoin

Status i of Shady Practices

thereum, ico, status.im

ore than $270 million making it the most successful ICO of
a successful ICO, Status.im has been accused of using

ICO

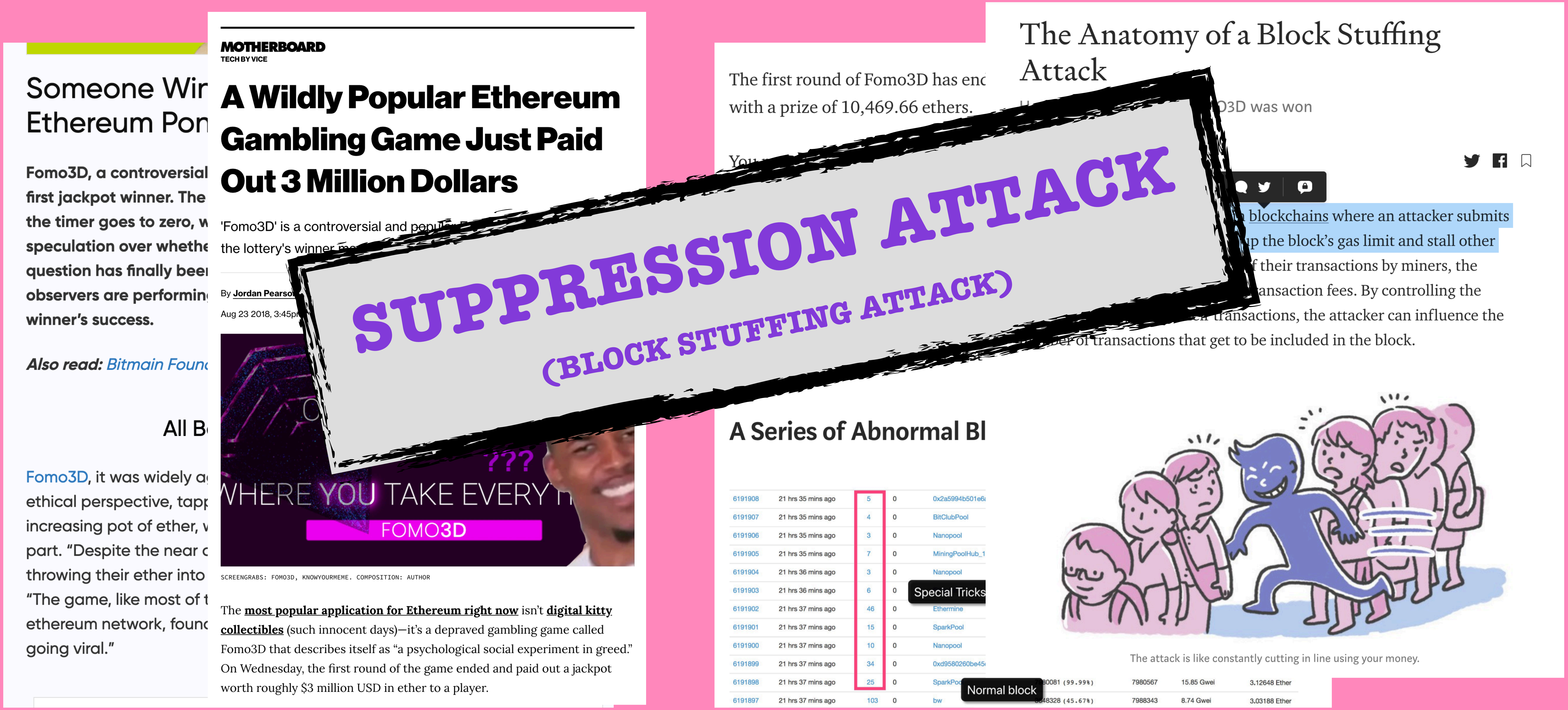
eral issues during the Status.im ICO just like it did during the
Ethereum network went into backlog and started to clog. This resulted in failed
ctions and people not able to send funds to the smart contract. After the mess started to clear up, it was found that the first few transactions that got cleared were huge and were from whitelisted addresses that didnt follow the Gas limit set by the Status.im team.

It was later addressed by the Status.im team that those transactions were not by a single person but were pooled up transactions of 2000 people with a KYC process from ICOage. The second transaction was pooled up transaction from imToken. This was done to prevent the network from being ddosed. However, some contributors still set the gas price about the limit which resulted in the network congestion.

Despite the explanation given above the Status.im team, the community has accused them of setting such obscene hardcap to which no explanation has been provided. Also, the users were not informed promptly about the whitelisting address procedure. It was explained on the Status.im website but wasnt available clearly to users.

Apart from these issues, there was also reports against f2pool of removing user's transaction with their own transactions so that they secure a position in the ICO before anybody else.

Story 2: FOMO3D



Someone Wir
Ethereum Pon

Fomo3D, a controversial
first jackpot winner. The
the timer goes to zero, w
speculation over whethe
question has finally beer
observers are performin
winner's success.

Also read: Bitmain Found

All B

Fomo3D, it was widely a
ethical perspective, tap
increasing pot of ether, w
part. "Despite the near c
throwing their ether into
"The game, like most of t
ethereum network, found
going viral."

MOTHERBOARD
TECH BY VICE

A Wildly Popular Ethereum Gambling Game Just Paid Out 3 Million Dollars

'Fomo3D' is a controversial and popul
the lottery's winner m

By Jordan Pearso
Aug 23 2018, 3:45p

SCREENGRABS: FOMO3D, KNOWYOURMEME. COMPOSITION: AUTHOR

The most popular application for Ethereum right now isn't digital kitty collectibles (such innocent days)—it's a depraved gambling game called Fomo3D that describes itself as "a psychological social experiment in greed." On Wednesday, the first round of the game ended and paid out a jackpot worth roughly $3 million USD in ether to a player.

SUPPRESSION ATTACK
(BLOCK STUFFING ATTACK)

The first round of Fomo3D has enc
with a prize of 10,469.66 ethers.

You

A Series of Abnormal Bl

6191908	21 hrs 35 mins ago	5	0	0x2a5994b501e6				
6191907	21 hrs 35 mins ago	4	0	BitClubPool				
6191906	21 hrs 35 mins ago	3	0	Nanopool				
6191905	21 hrs 35 mins ago	7	0	MiningPoolHub_1				
6191904	21 hrs 36 mins ago	3	0	Nanopool				
6191903	21 hrs 36 mins ago	6	0					
6191902	21 hrs 37 mins ago	46	0	Ethermine				
6191901	21 hrs 37 mins ago	15	0	SparkPool				
6191900	21 hrs 37 mins ago	10	0	Nanopool				
6191899	21 hrs 37 mins ago	34	0	0xd9580260be45				
6191898	21 hrs 37 mins ago	25	0	SparkPoo	80081 (99.99%)	7980567	15.85 Gwei	3.12648 Ether
6191897	21 hrs 37 mins ago	103	0	bw	48328 (45.67%)	7988343	8.74 Gwei	3.03188 Ether

Special Tricks

Normal block

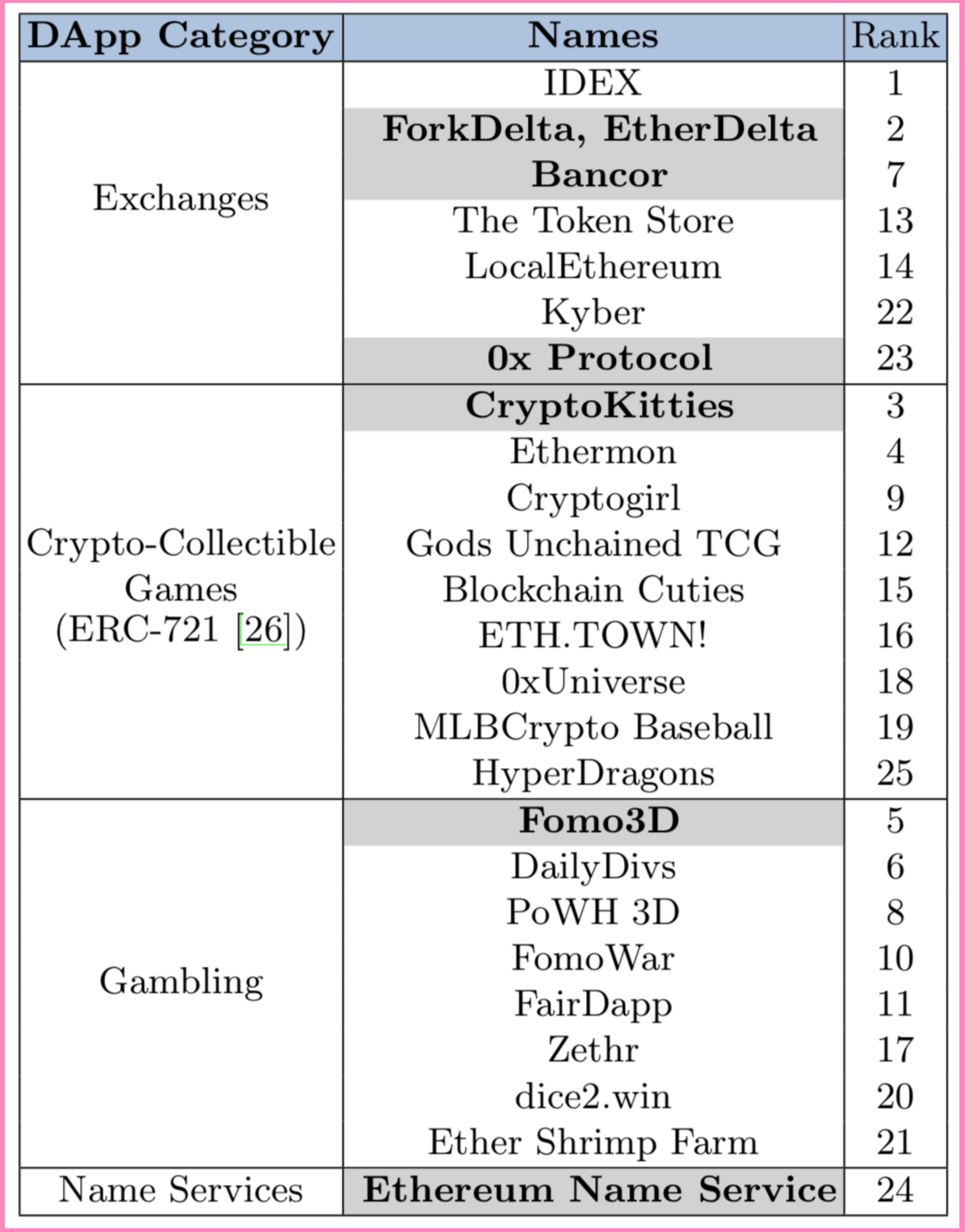
The Anatomy of a Block Stuffing Attack

O3D was won

blockchains where an attacker submits
up the block's gas limit and stall other
f their transactions by miners, the
ansaction fees. By controlling the
transactions, the attacker can influence the
ber of transactions that get to be included in the block.

The attack is like constantly cutting in line using your money.

Case Study



DApp Category	**Names**	Rank
Exchanges	IDEX	1
	ForkDelta, EtherDelta	2
	Bancor	7
	The Token Store	13
	LocalEthereum	14
	Kyber	22
	0x Protocol	23
Crypto-Collectible Games (ERC-721 [26])	**CryptoKitties**	3
	Ethermon	4
	Cryptogirl	9
	Gods Unchained TCG	12
	Blockchain Cuties	15
	ETH.TOWN!	16
	0xUniverse	18
	MLBCrypto Baseball	19
	HyperDragons	25
Gambling	**Fomo3D**	5
	DailyDivs	6
	PoWH 3D	8
	FomoWar	10
	FairDapp	11
	Zethr	17
	dice2.win	20
	Ether Shrimp Farm	21
Name Services	**Ethereum Name Service**	24

- **Top 25 DApps**
  - Based on recent user activity
    - DAppRadar.com
    - September 2018
- Four categories
  - Studied at least one example from each category
  - All had front-running issues
- Added ICOs

- *See the paper for detailed case studies*

Key Mitigations

1. **Transaction Sequencing**
2. **Confidentiality**
3. **Design Practices**
4. **Embrace It**

Transaction Sequencing

- Remove the miner’s ability to arbitrarily order transactions
- Take a consensus on what transactions were seen first (Aequitas)
- Have a third party DApp (“sequencer”) order transactions (Wendy, Chainlink)
- Sort pseudorandomly (e.g. Canonical Transaction Ordering Rule (CTOR) by Bitcoin Cash ABC)

Confidentiality

Limit the visibility of DApps. But what does that mean???

1	**Code** of the DApp
2	Current **state** of the DApp
3	Name of the **function** being invoked
4	**Parameters** supplied to the function
5	**Address** of the contract the function is being invoked on
6	Identity of the **sender**.

Confidentiality

- Commit/Reveal: (3,4)-confidential
- Encryption/Secret Sharing: (3,4)-confidential
- TEEs: (2,3,4)-confidential
- Privacy coins: (6)-confidential

1	**Code of the DApp**
2	**Current state of the DApp**
3	**Name of the function being invoked**
4	**Parameters supplied to the function**
5	**Address of the contract**
6	**Identity of the sender.**

Design Practices

- Assume front-running is unpreventable —> Remove any benefit from it
    - Remove the importance of transaction ordering or time
- **Call market** design instead of a time-sensitive order book
    - See our paper “Trading On-Chain: How Feasible is Regulators’ Worst-Case Scenario?”
- ERC20 allowance functionality, “approve()”, was not designed with front-running in mind
    - See our paper “Resolving the Multiple Withdrawal Attack on ERC20 Tokens"

Embrace It

- Say a transaction nets the user who runs it 1M ETH
- A bot will stage every pending transaction they see, substituting themselves as the originator and measuring if it results in profits (bots are dumb and do not know what they are actually doing)
- A bot will find this transaction and steal it for themself by with higher gas
- Bot #2 will find this transaction and steal it with higher gas… Bot 3, Bot 4, Bot n… This leads to congestion

Embrace It

- Infrastructure exists for bots to “search” for MEV opportunities and “builds” a block of transactions
- The block is given off-chain to a “relay” who compares blocks given to it, looking for the one that will profit the miner (validator / proposer) the most
- The winning block is provided by the relay to the proposer who can use it or not (but generally does because it is more profitable than what they can find individually)

Concluding Remarks

- Front-running is a pervasive issue in Ethereum DApps
- Increase awareness of these type of attacks
- We need usable DApp layer & blockchain-level solutions
    - We highlight this as an important research area.

Q

@PulpSpy