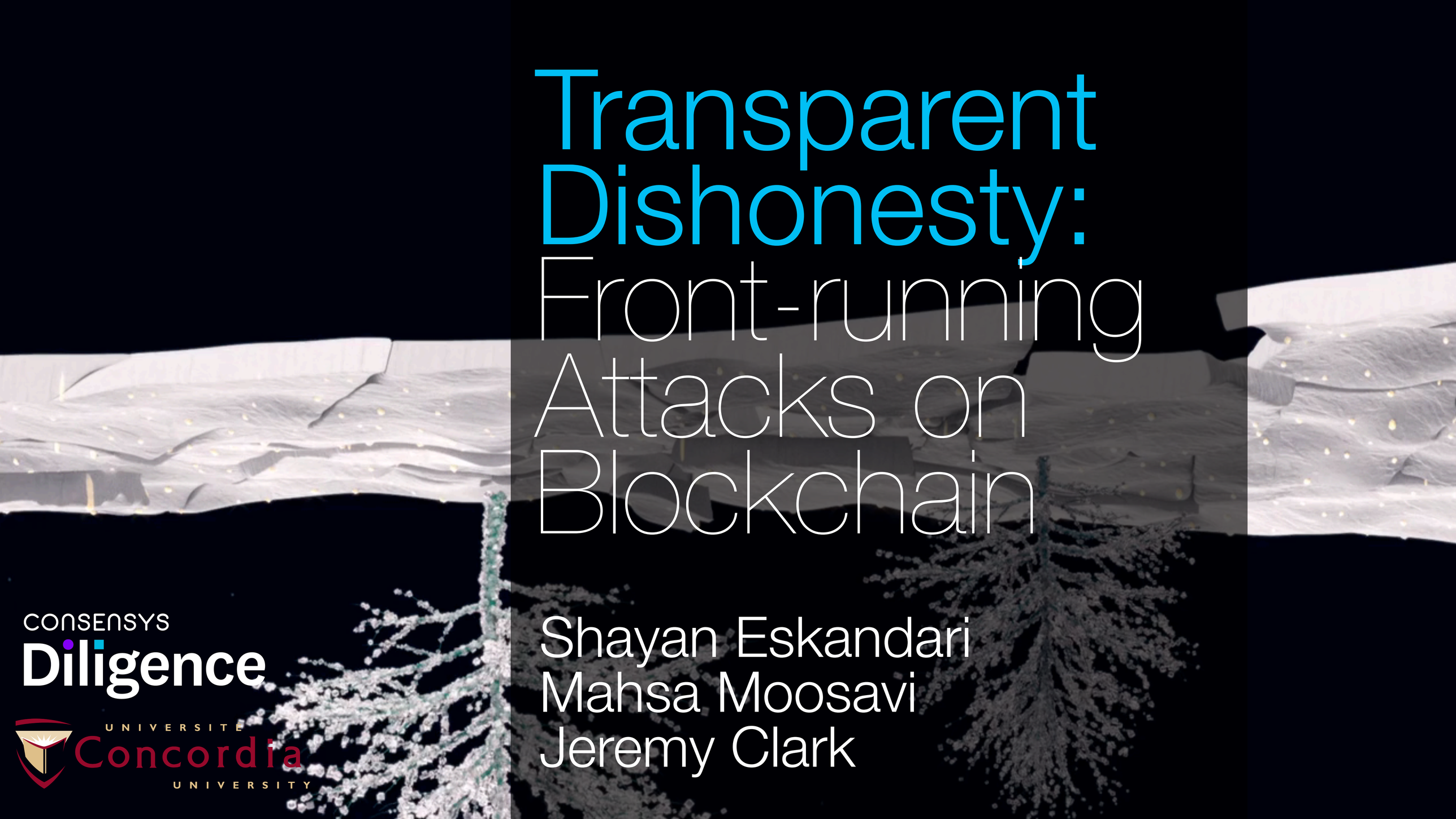


Transparent Dishonesty: Front-running Attacks on Blockchain

Shayan Eskandari
Mahsa Moosavi
Jeremy Clark

CONSENSYS Diligence

Université Concordia University

Jeremy Clark

- Associate Professor at the Concordia Institute for Information Systems Engineering (CIISE) in Montreal
- NSERC / Raymond Chabot Grant Thornton / Catallaxy Industry Research Chair in Blockchain Technologies
- PhD from the University of Waterloo (2009)
- Team of ten graduate students
- Numerous academic papers on Bitcoin/Blockchain
- Contributed to courses (Concordia, Princeton, MIT) & textbook on Bitcoin/blockchain
- Testified to Senate and House committees on Bitcoin/blockchain

MADIBA security research group

UNIVERSITÉ Concordia UNIVERSITY

GINA CODY SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

FUNDING & PARTNERS:

NSERC CRSNG

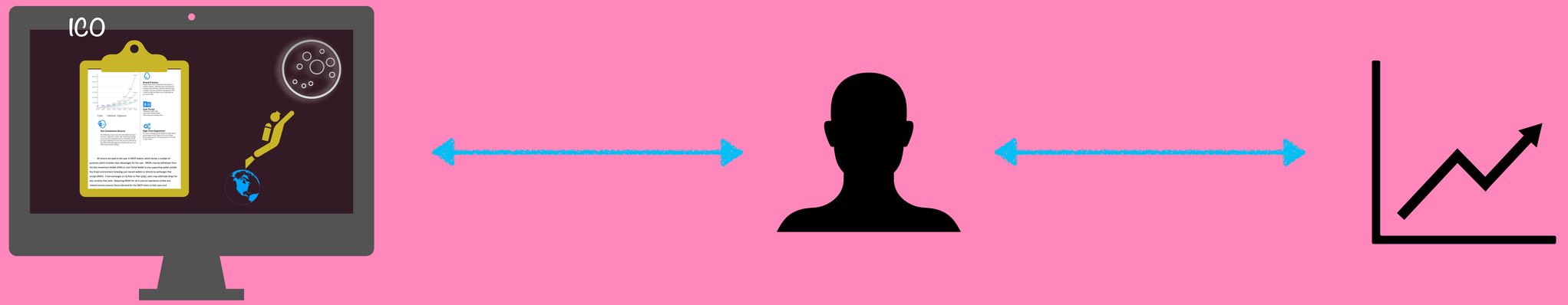
Raymond Chabot Grant Thornton

catallaxy

AUTORITÉ DES MARCHÉS FINANCIERS

Fonds de recherche Nature et technologies Québec

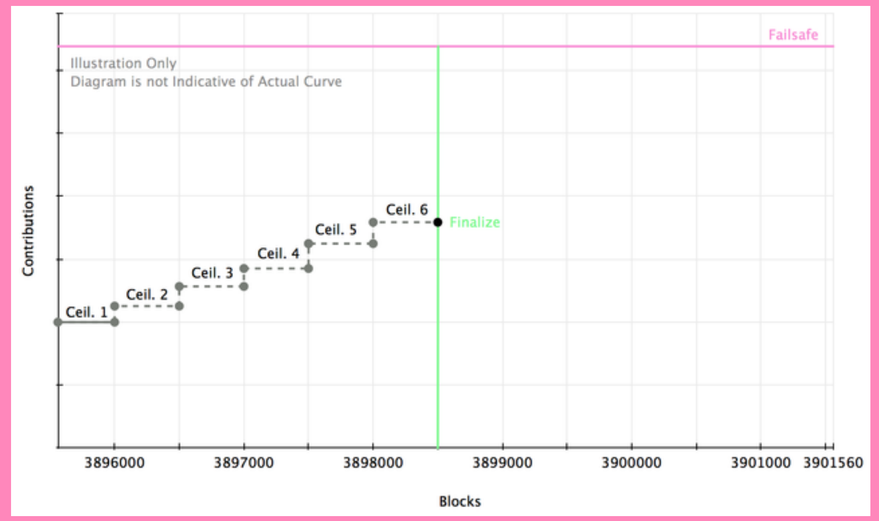
Office of the Privacy Commissioner of Canada


ICO
Brand Promise
Risk Analysis
High Cash Engagement

Status: Fair ICO

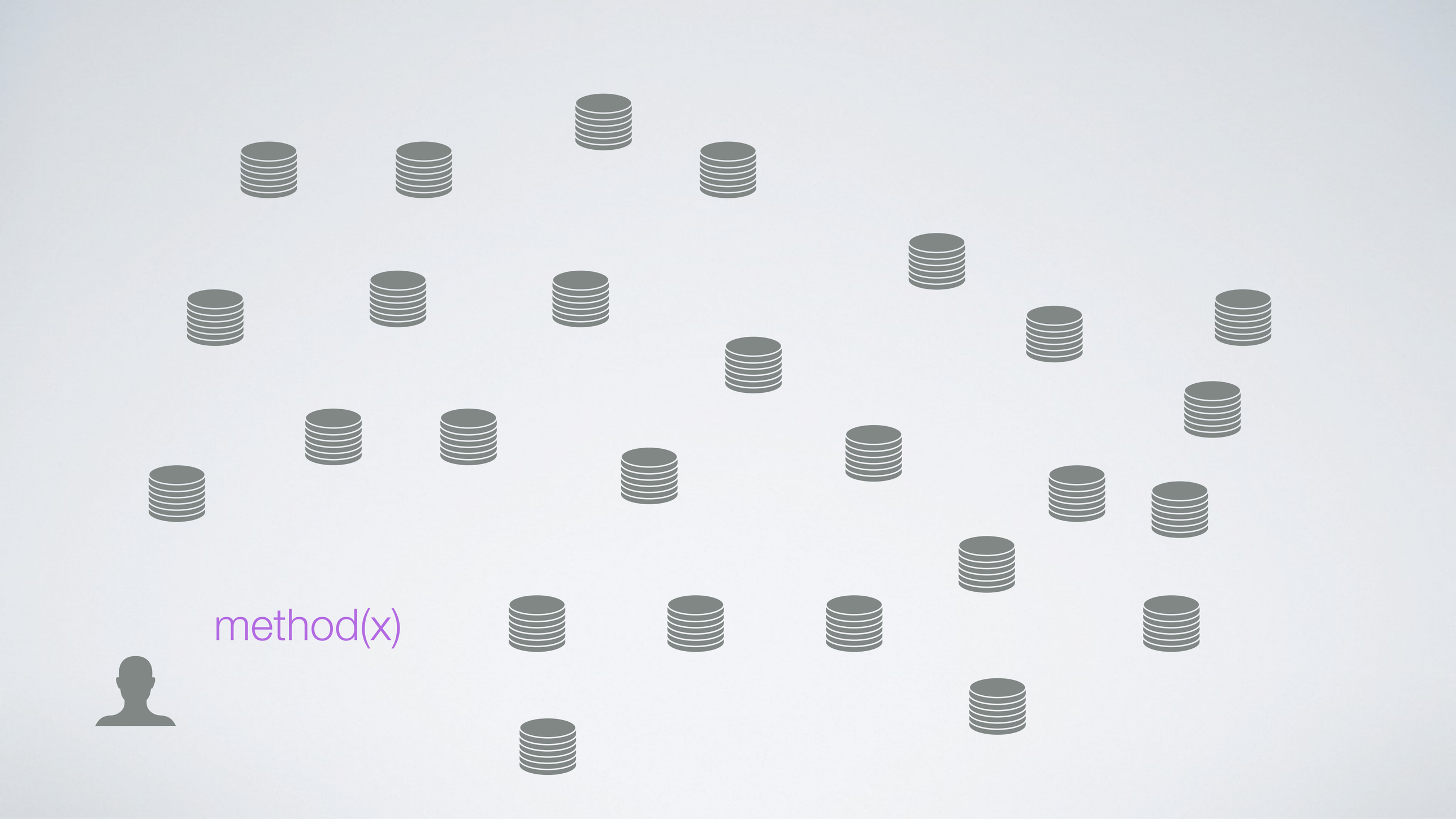
Status: Fair ICO

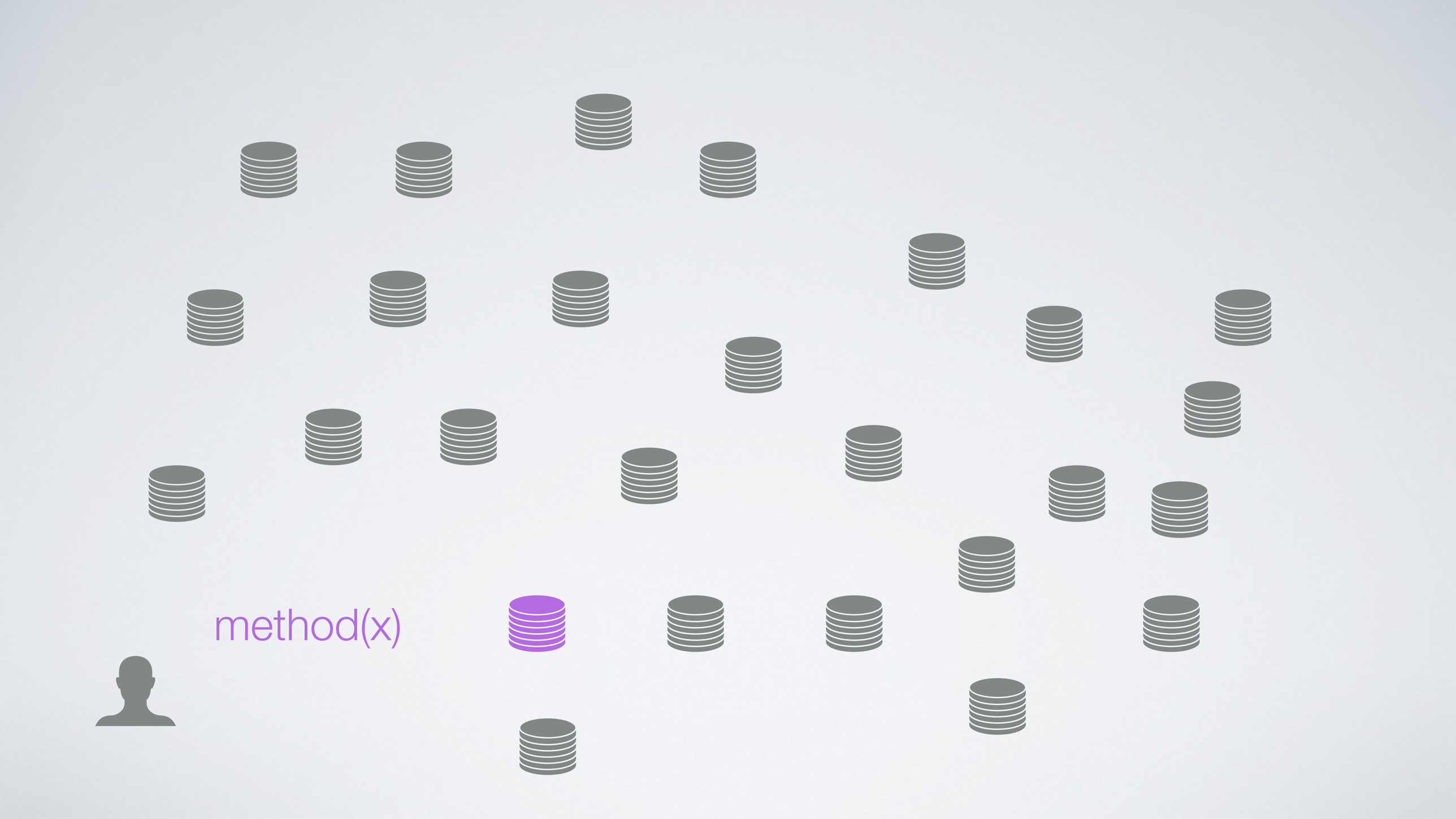
- Dynamic Cap/Ceiling // Maximum deposit amount per ceiling

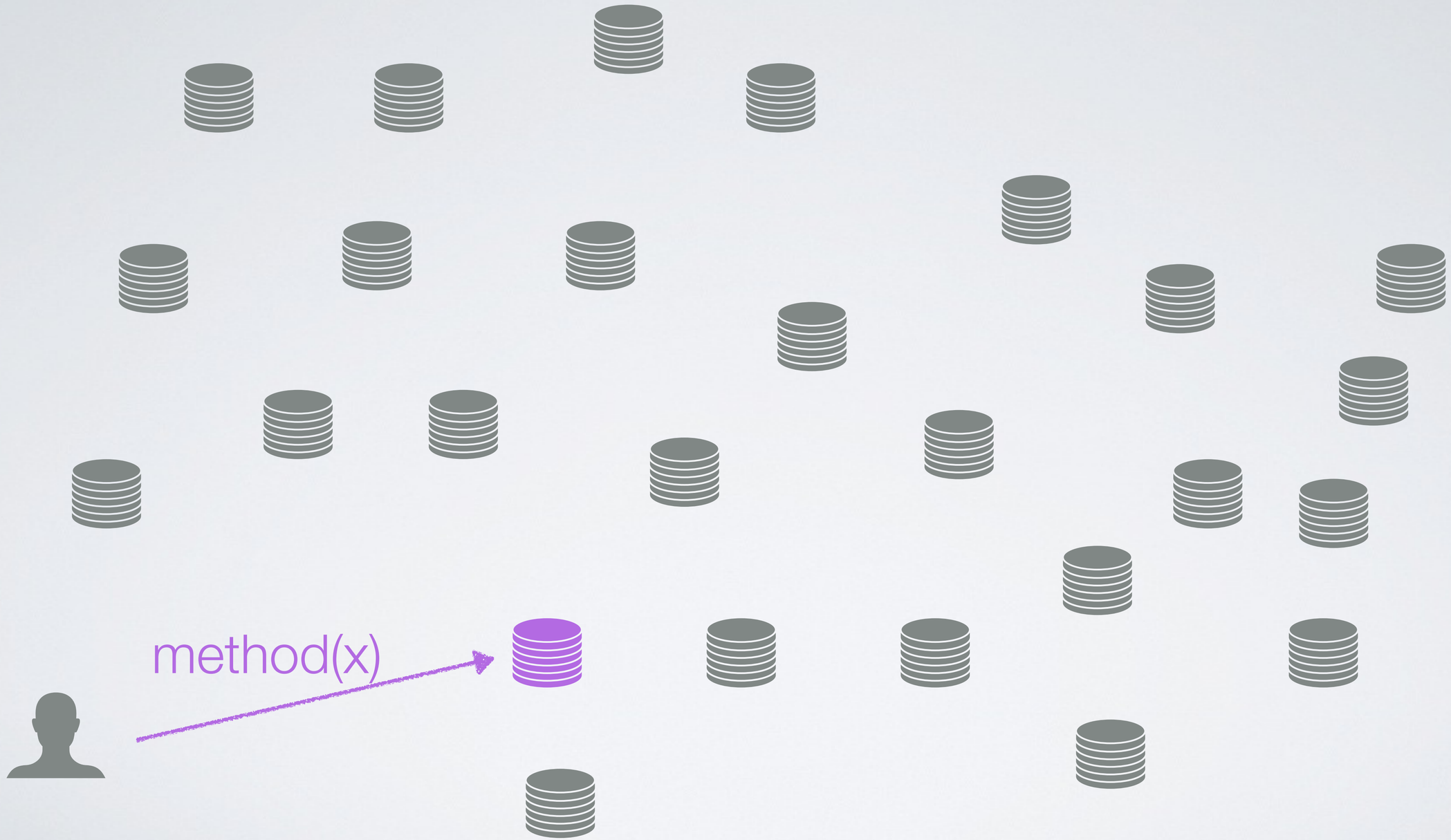


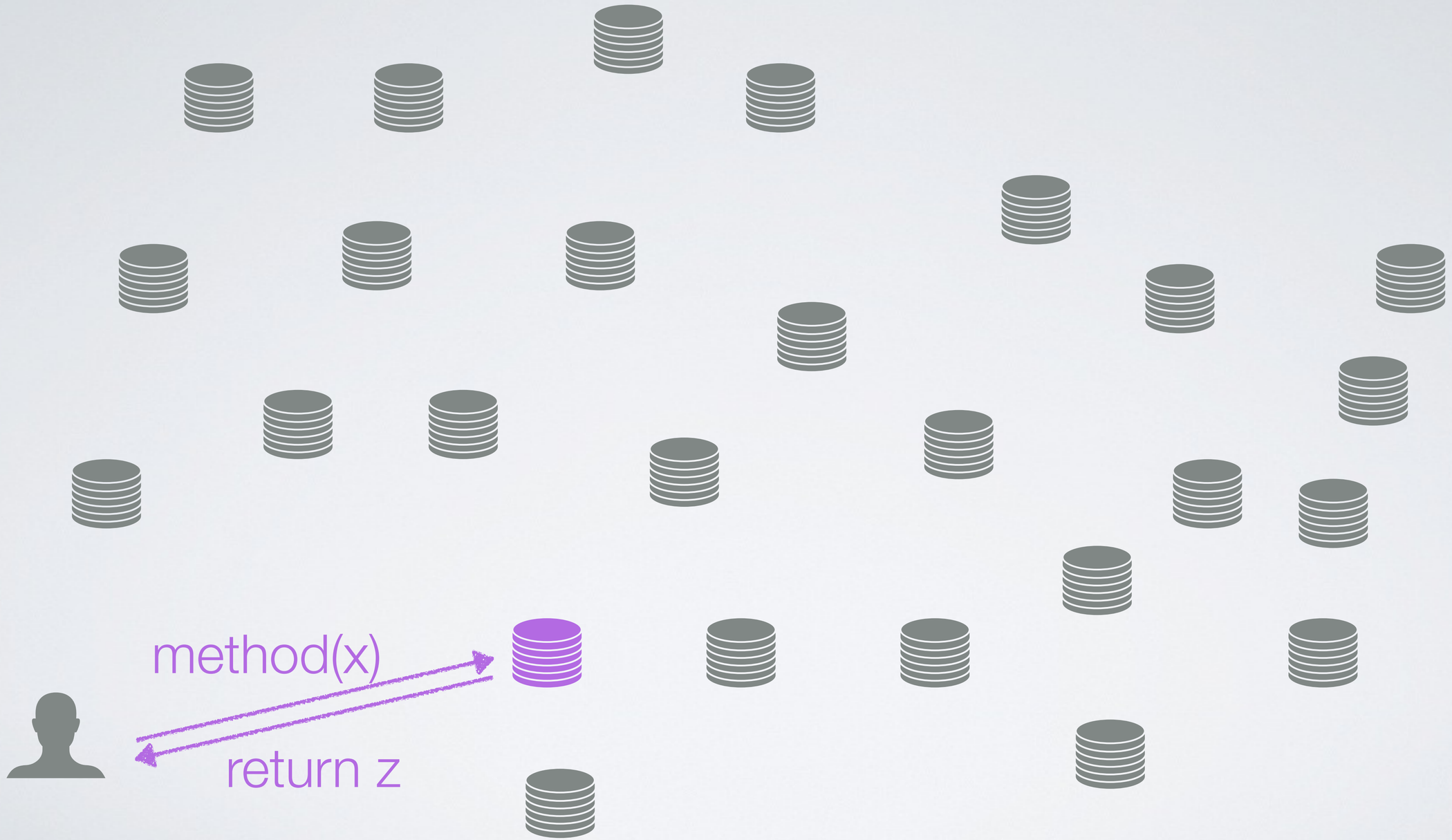
Status: Fair ICO

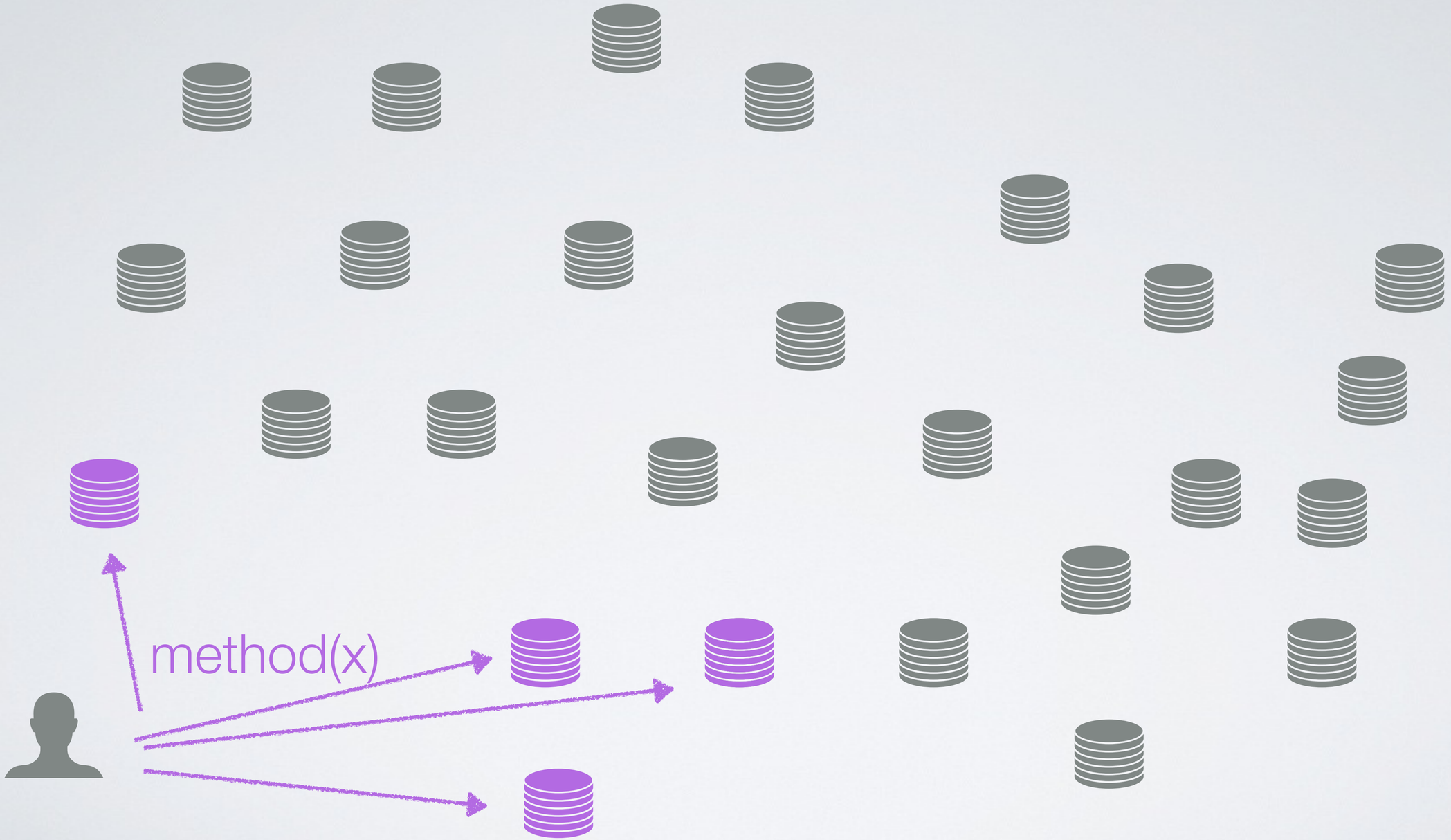
- Dynamic Cap/Ceiling // Maximum deposit amount per ceiling
- Limit GasPrice // require(gasPrice < 50 gwei)

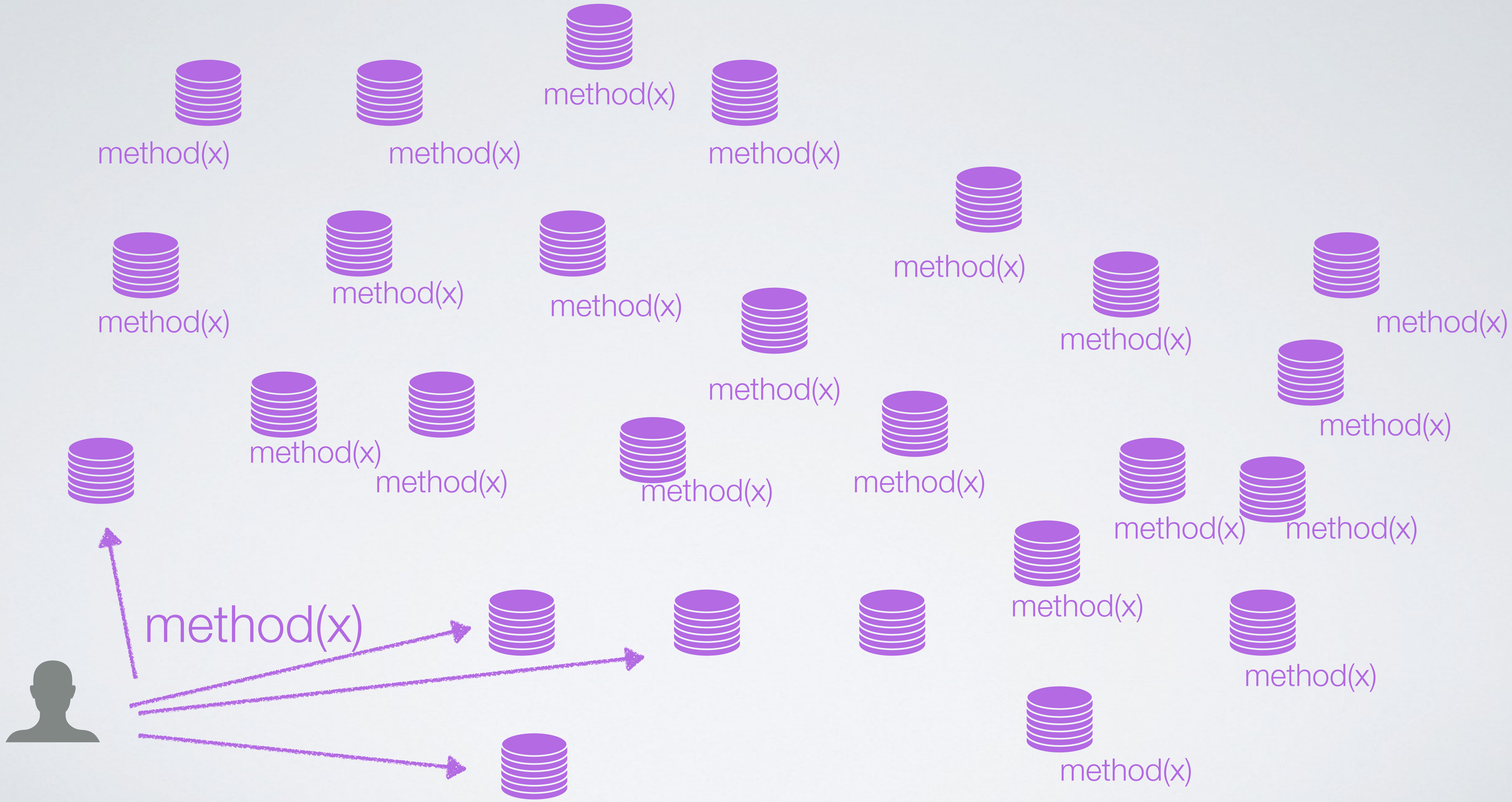

method(x)

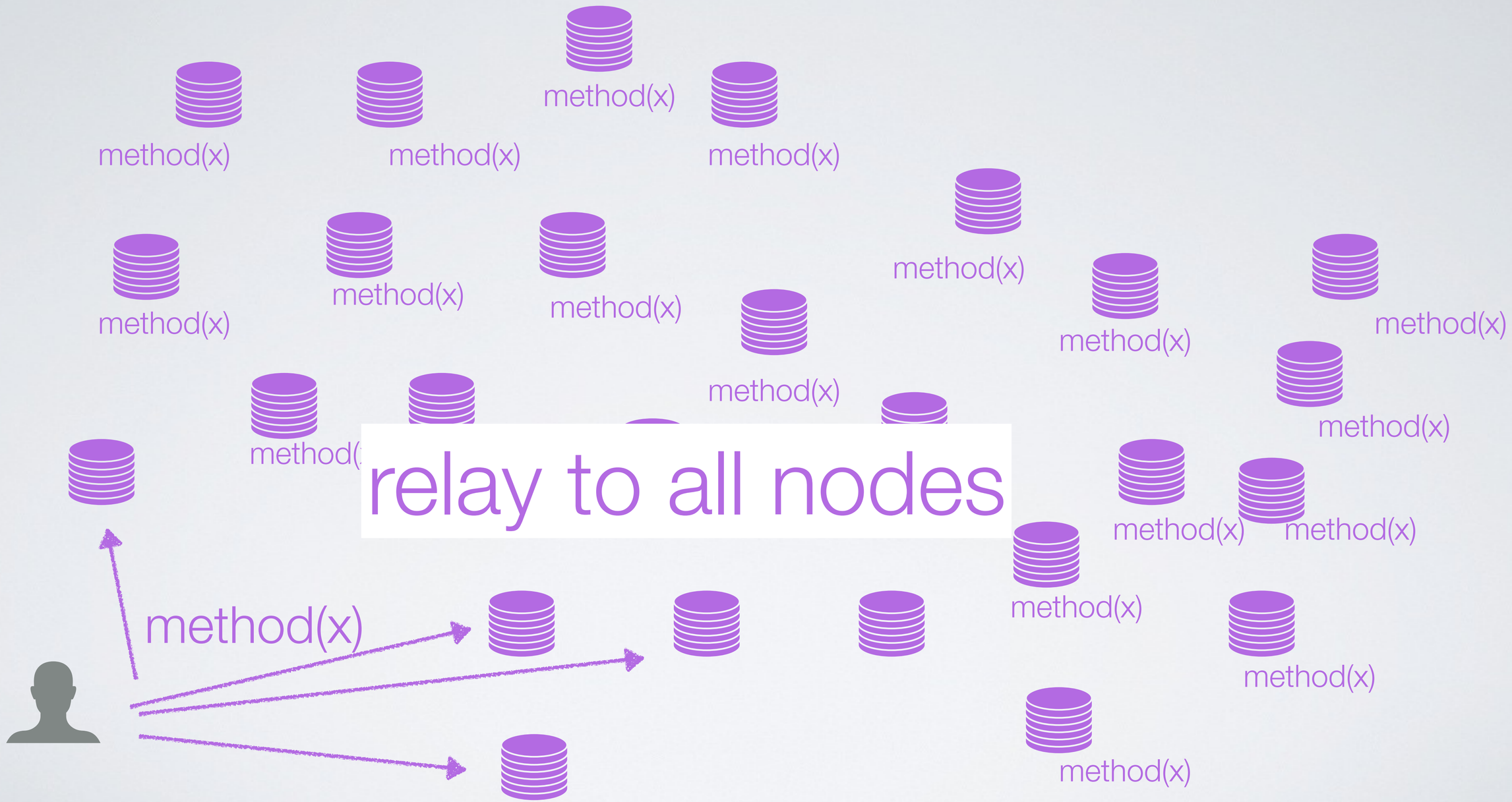

method(x)

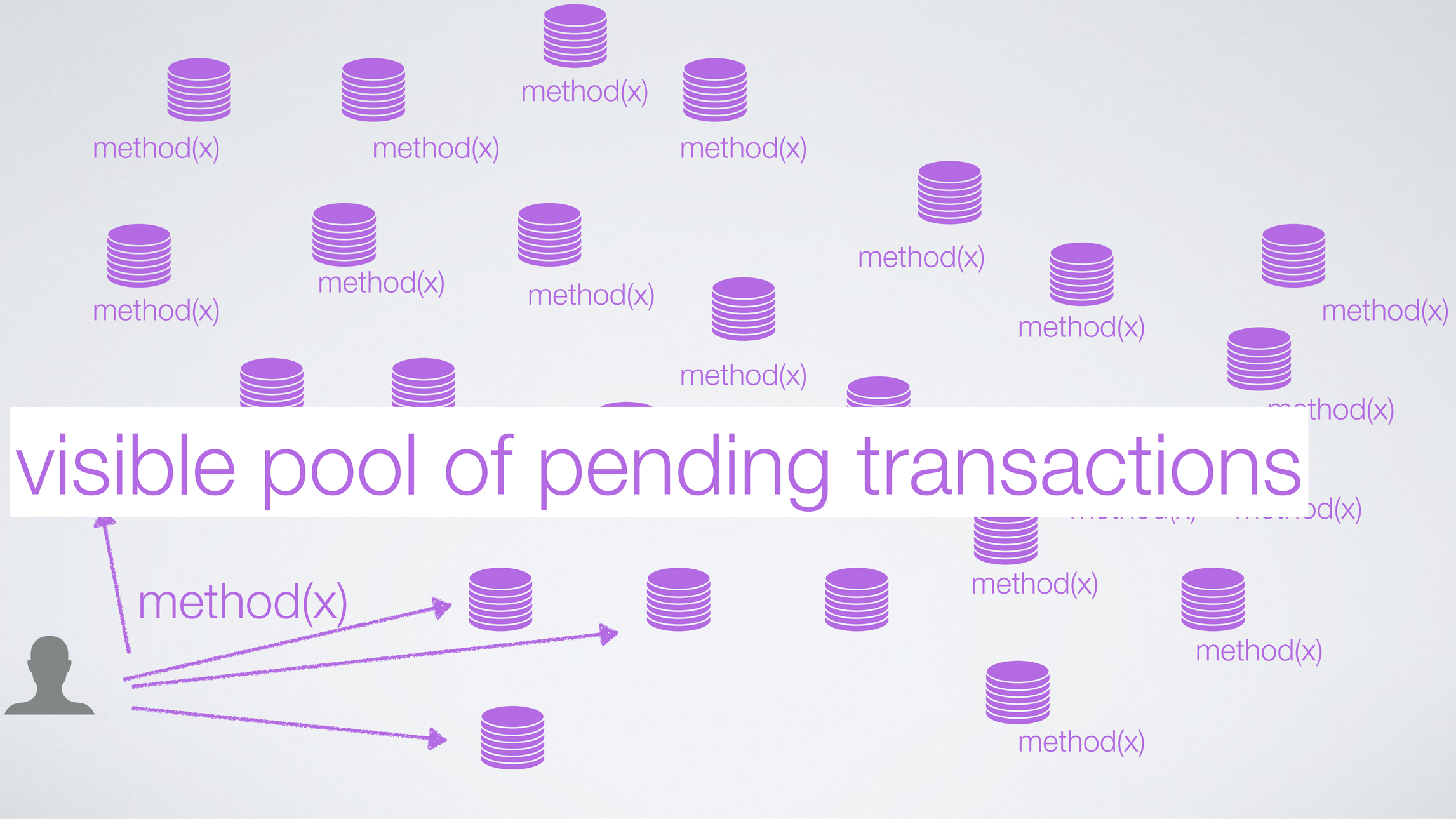

method(x)

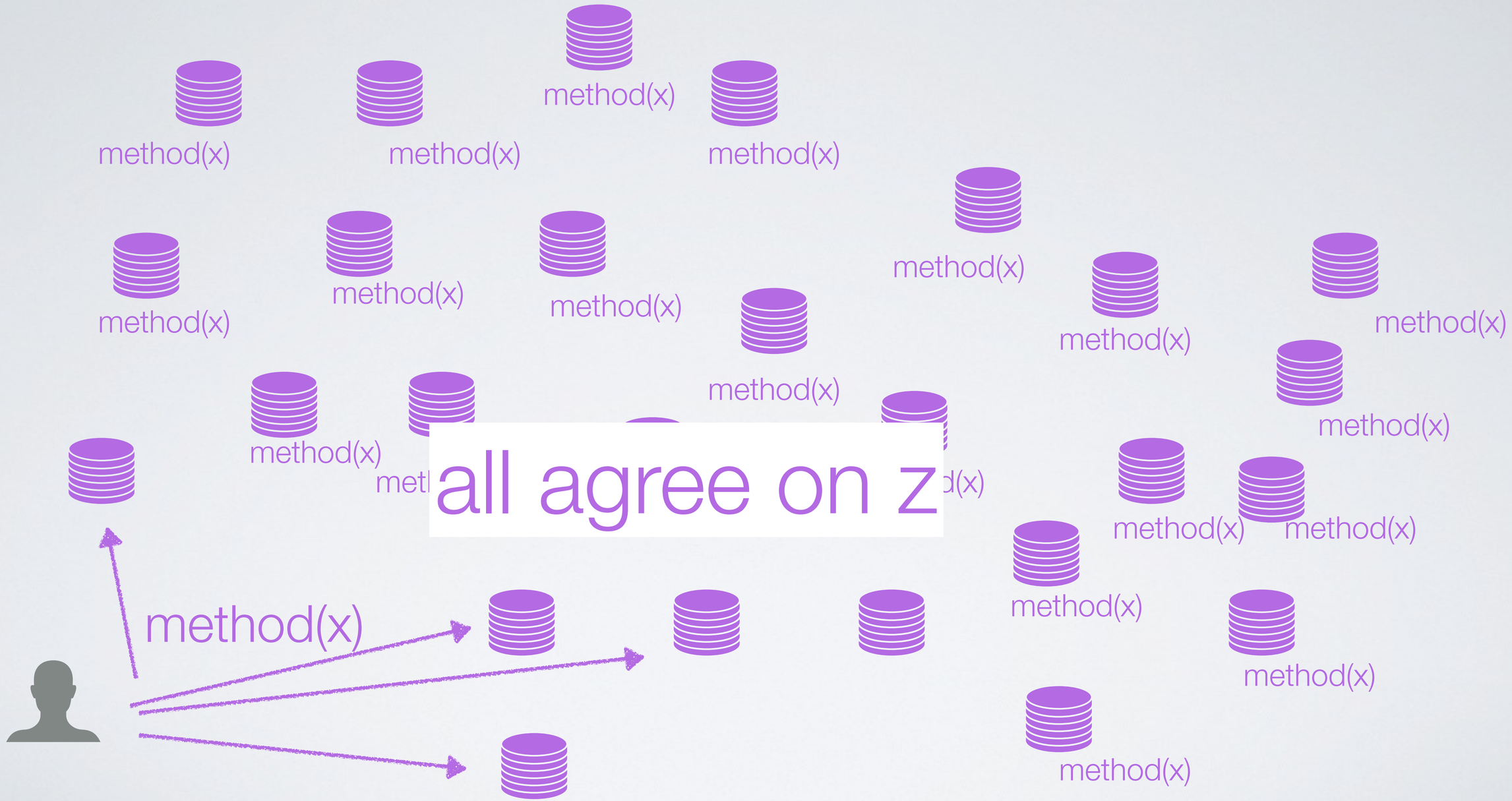

method(x)
return z


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)
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)
method(x)
method(x)
relay to all nodes
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)
visible pool of pending transactions
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)
method(x)
method(x)
all agree on z
method(x)

Status: Fair ICO

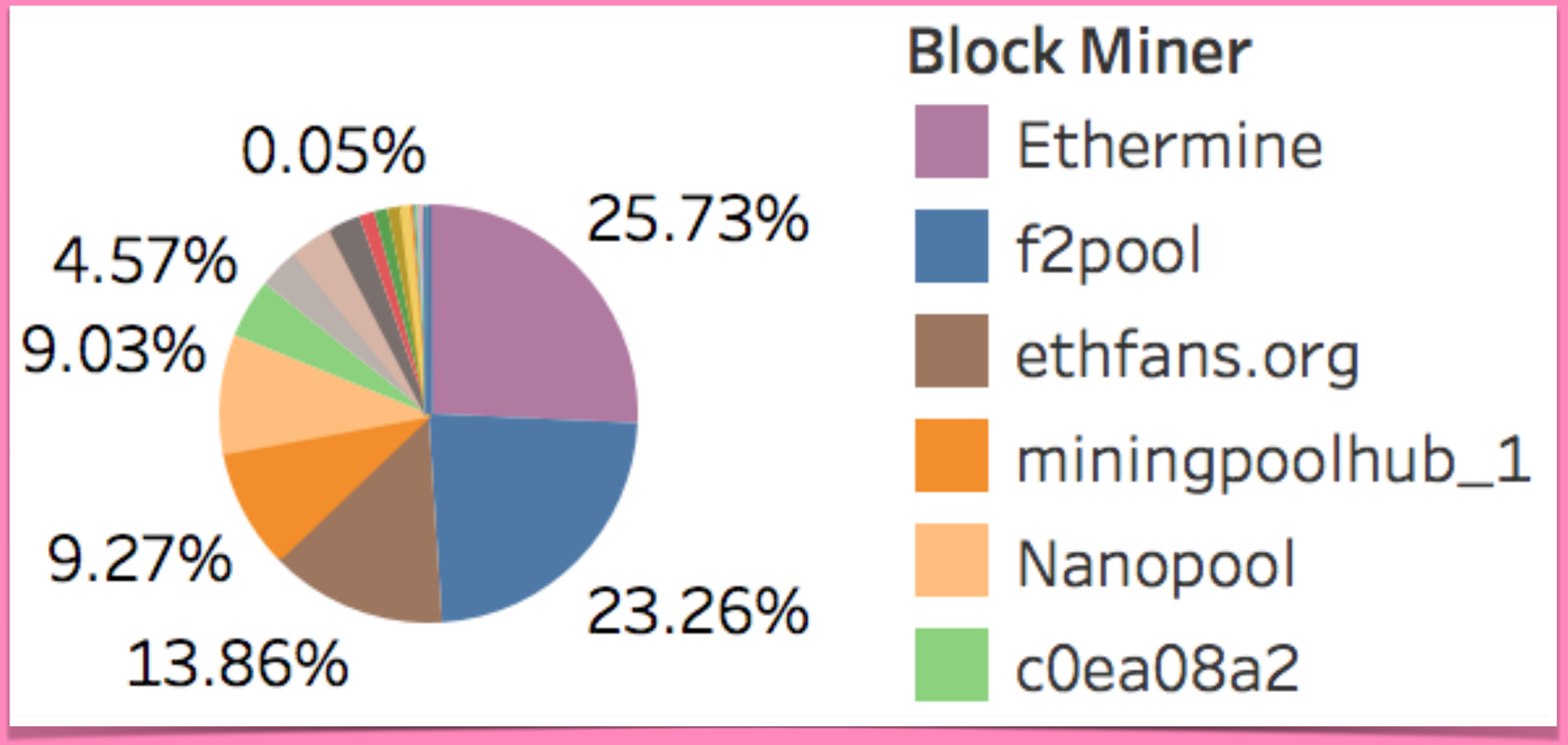
- Dynamic Cap/Ceiling // Maximum deposit amount per ceiling
- Limit GasPrice // require(gasPrice < 50 gwei)

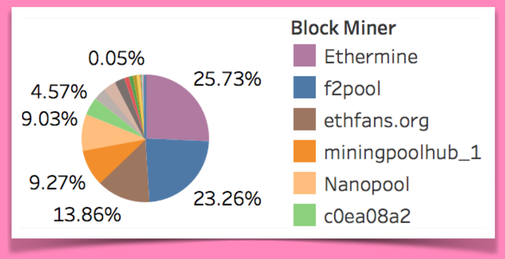
Status: Fair ICO

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

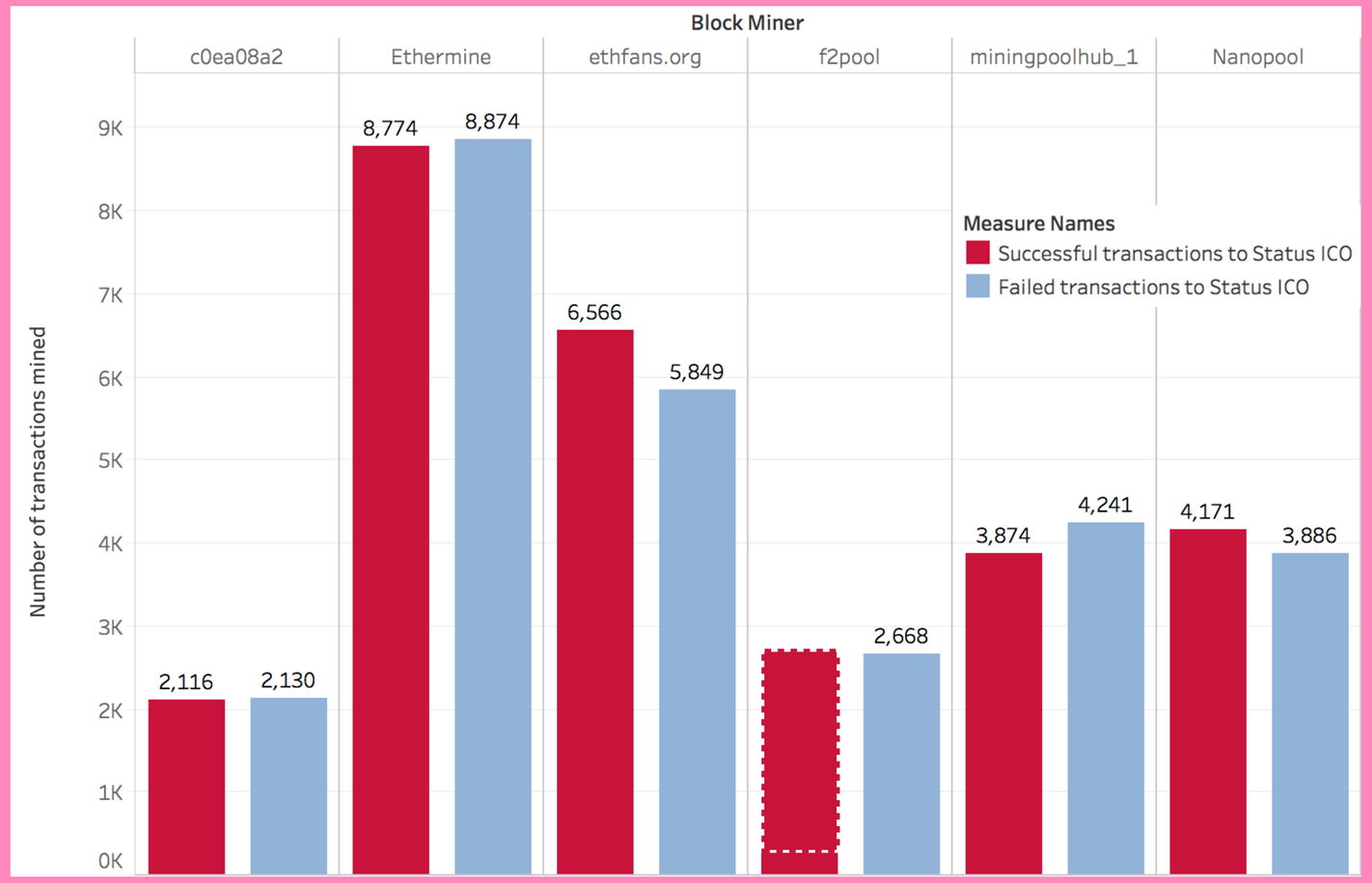
- We define:
  - ***Successful transaction***: resulted in token purchase
  - ***Failed transaction***: failed to purchase any tokens (high gasPrice, over cap, etc)
    - Result of buyers treating Status like a generic ICO

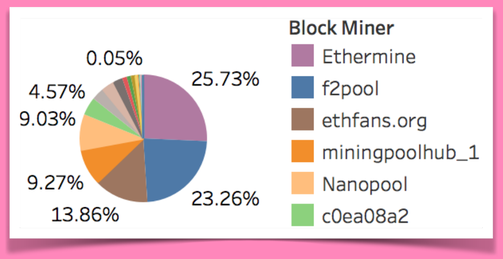
Status: Fair ICO



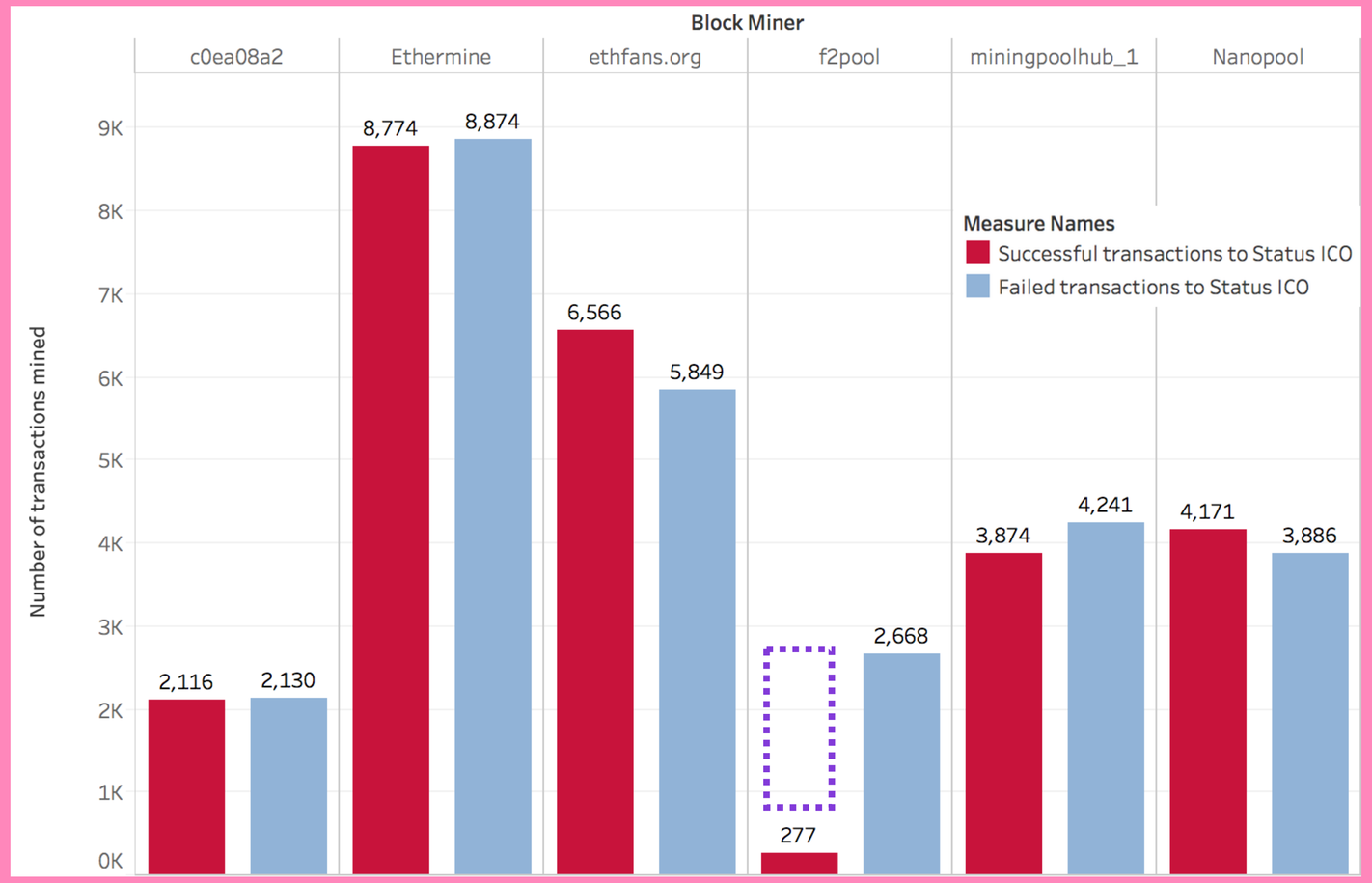


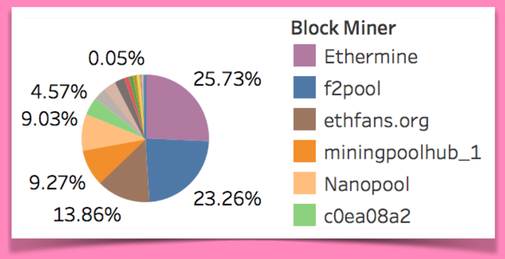
Status: Fair ICO



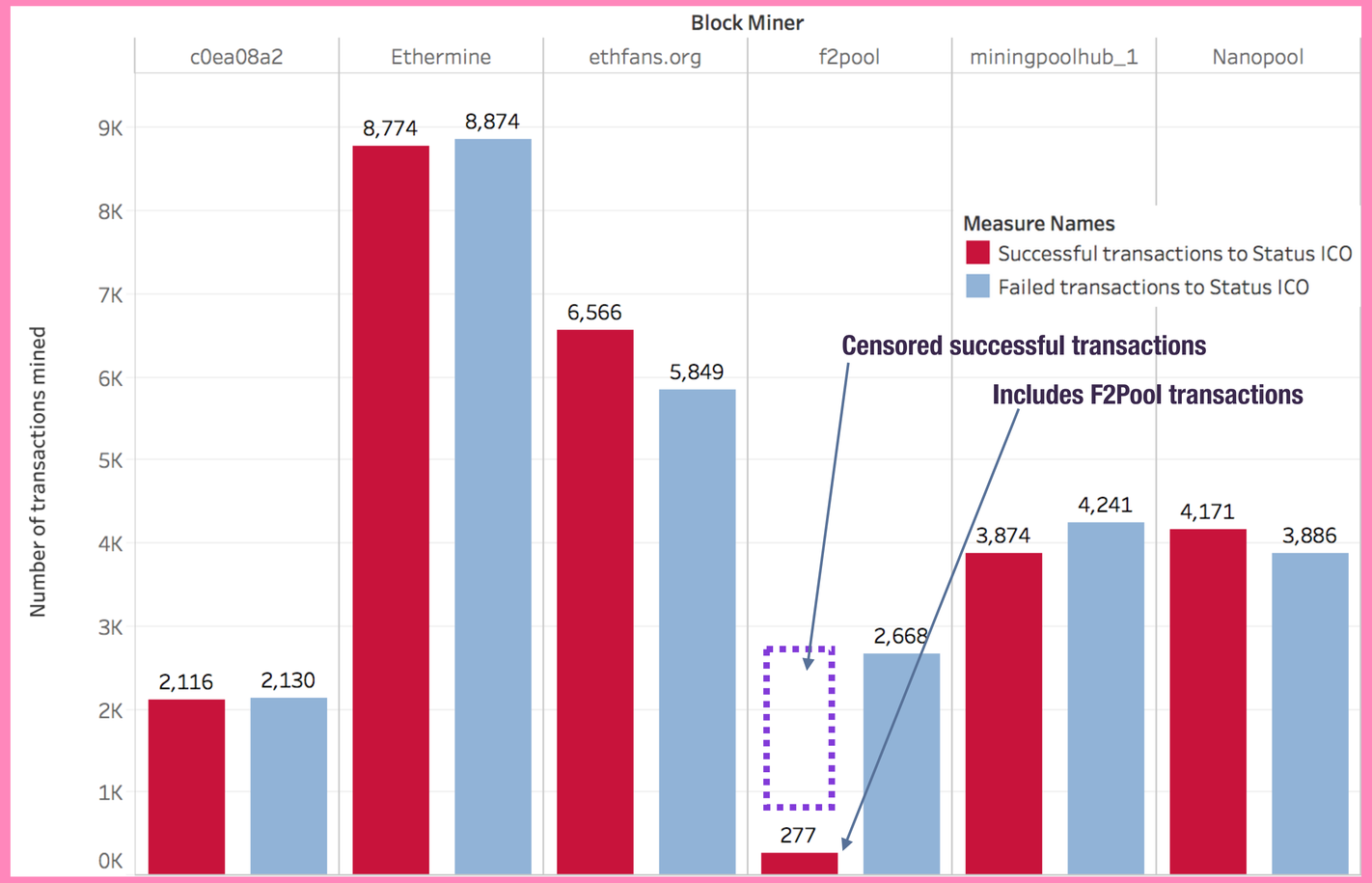


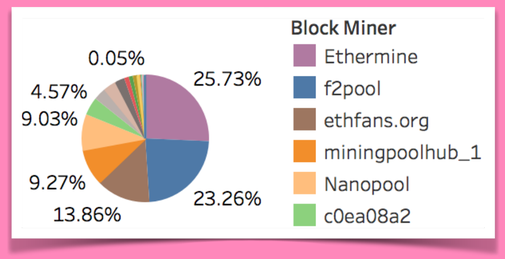
Status: Fair ICO



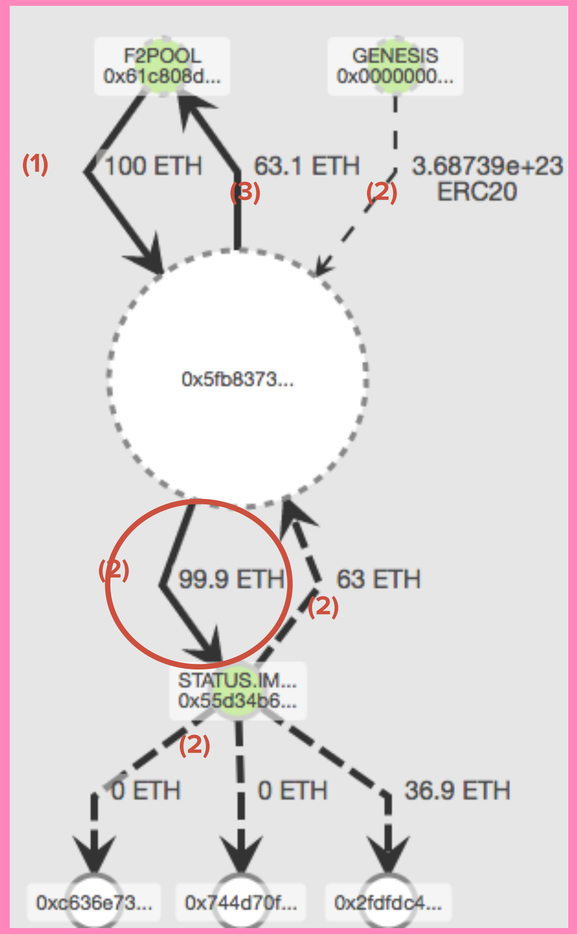


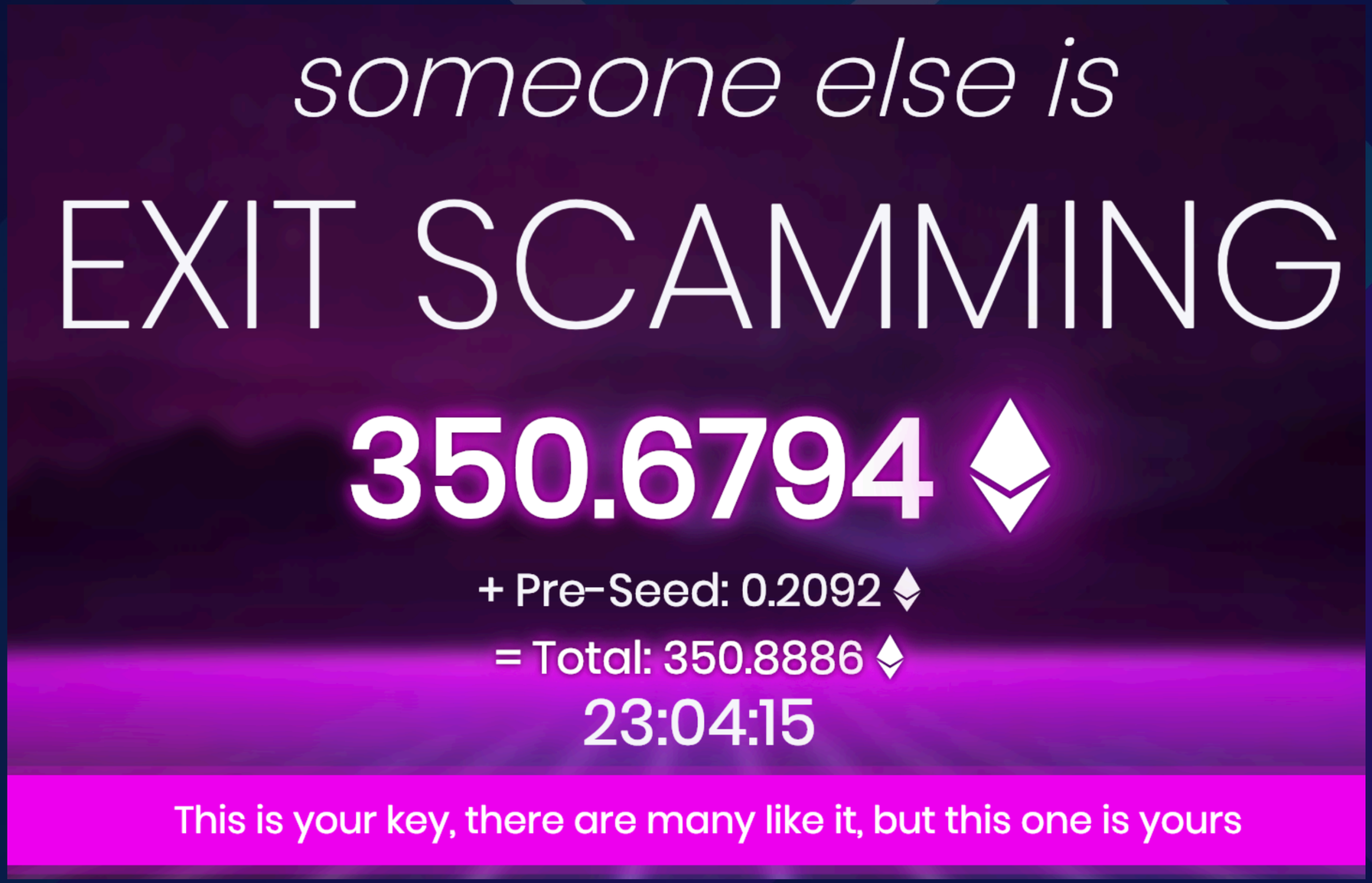
Status: Fair ICO





Status: Fair ICO




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

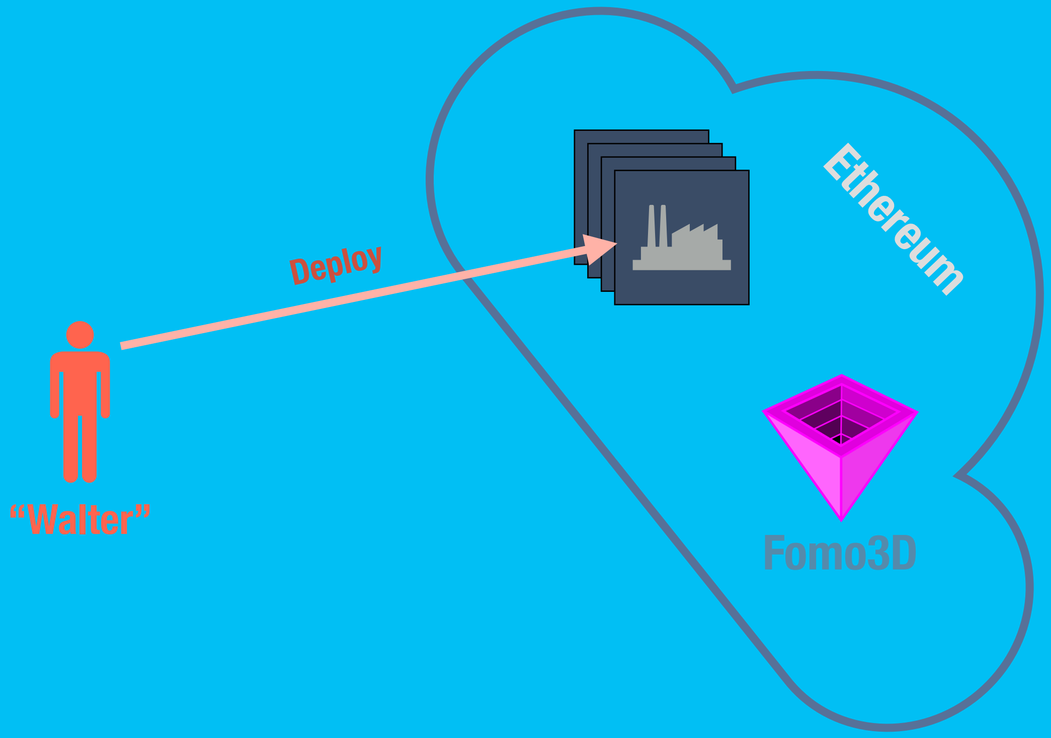
FOMO3D

FOMO3D

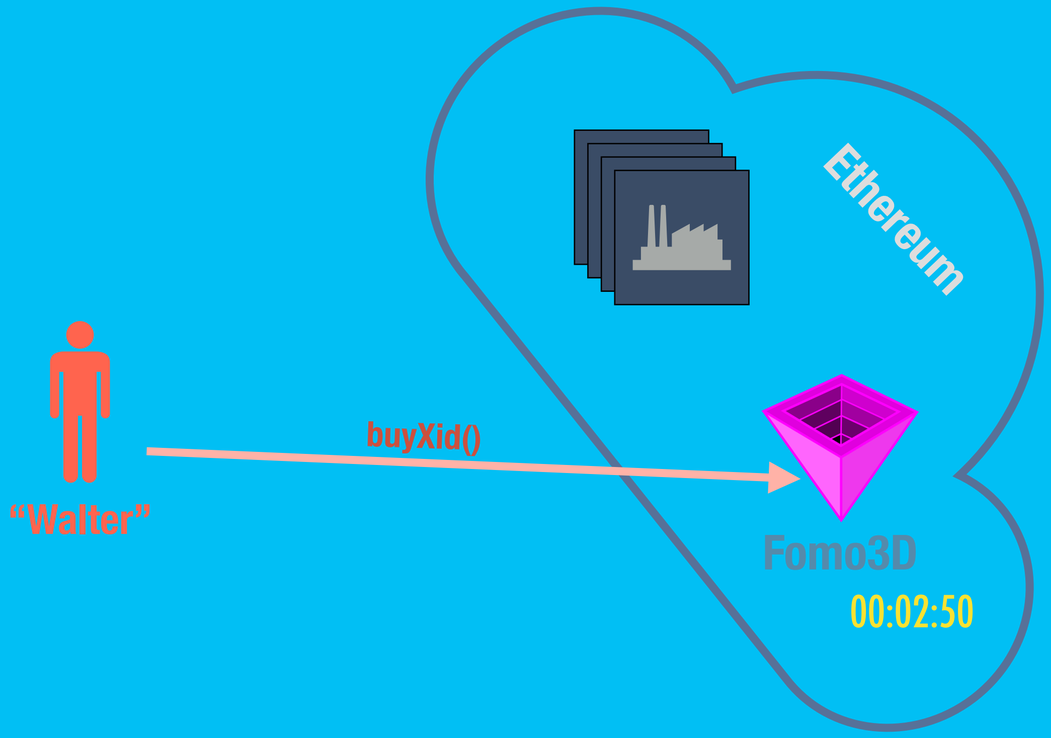
- A countdown timer
- Every ticket purchase increases the timer by 30 seconds
- The last ticket when the timer reaches 00:00:00 wins the pot

FOMO3D

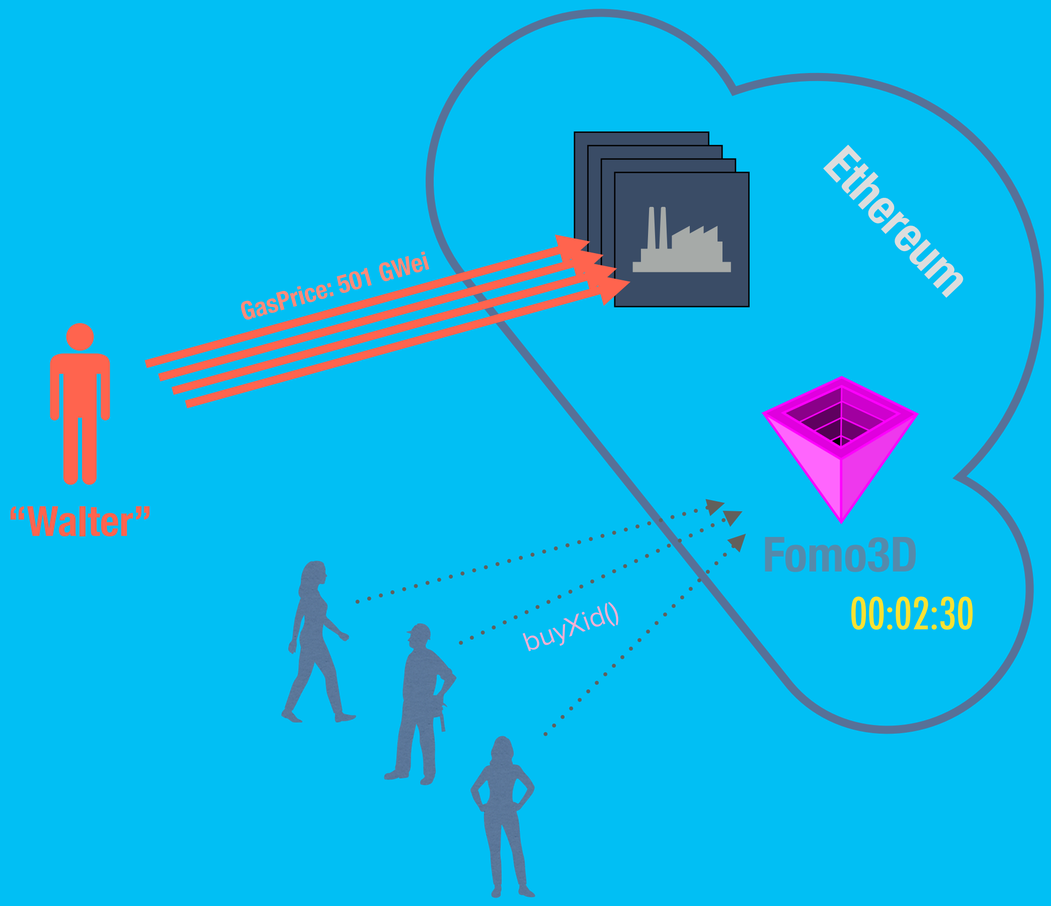
- “Walter” deploys contracts that has high gas consumption



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	BuyAndDistribute
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	BuyAndDistribute
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)

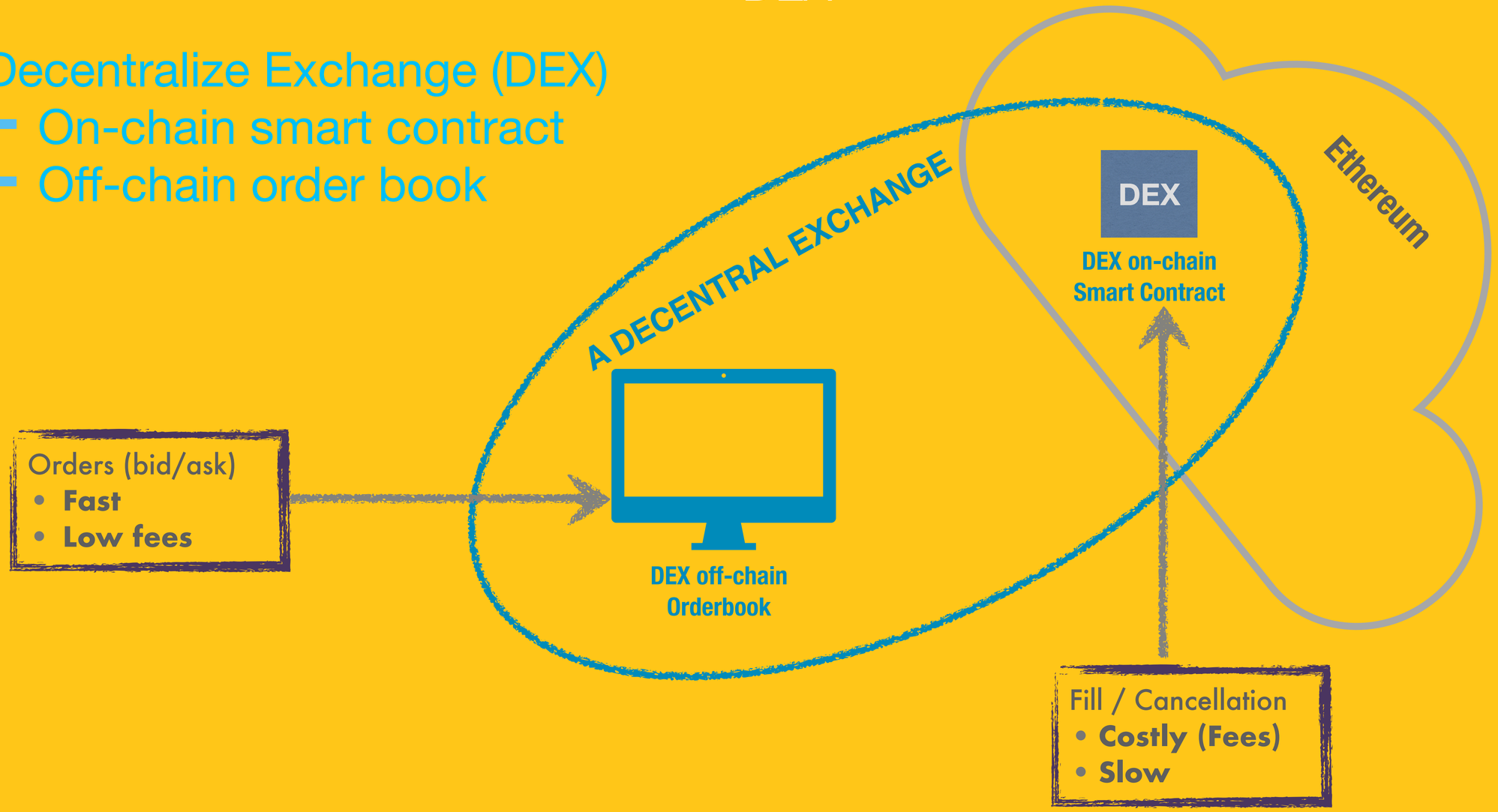
└ TRANSFER 10,469.660003123933104565 Ether From 0xa62142888aba8370742… To 0xa169df5ed3363cfc4c92…

~$3M

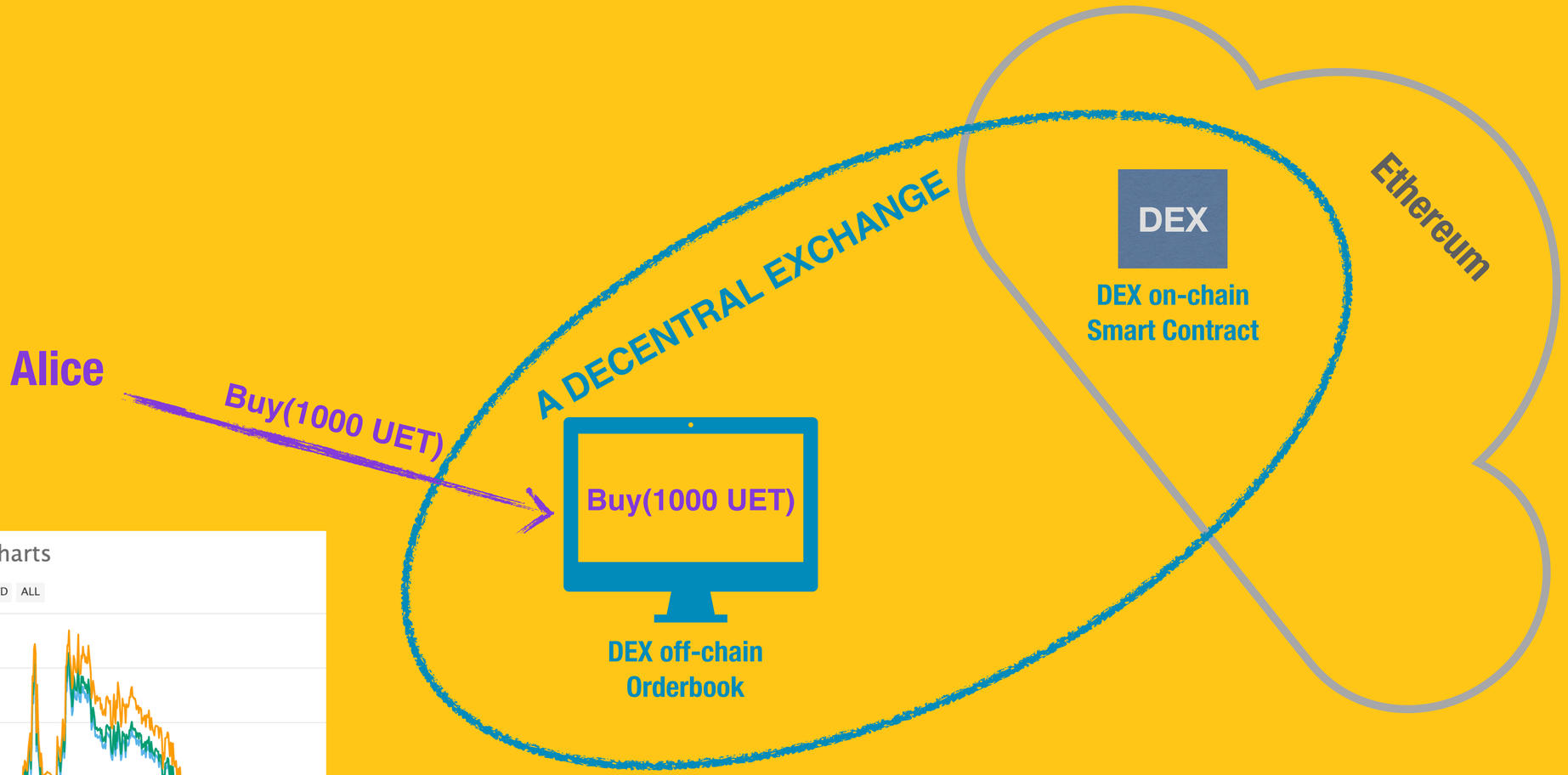
DEX

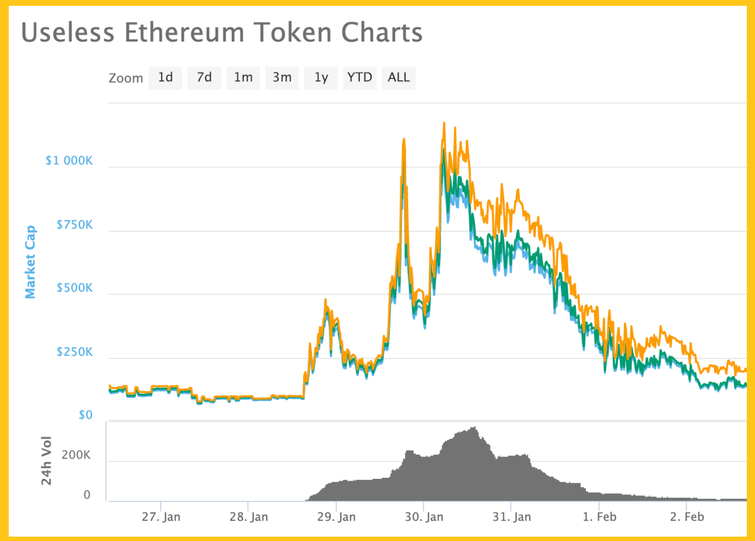
DEX

- Decentralize Exchange (DEX)
  - On-chain smart contract
  - Off-chain order book

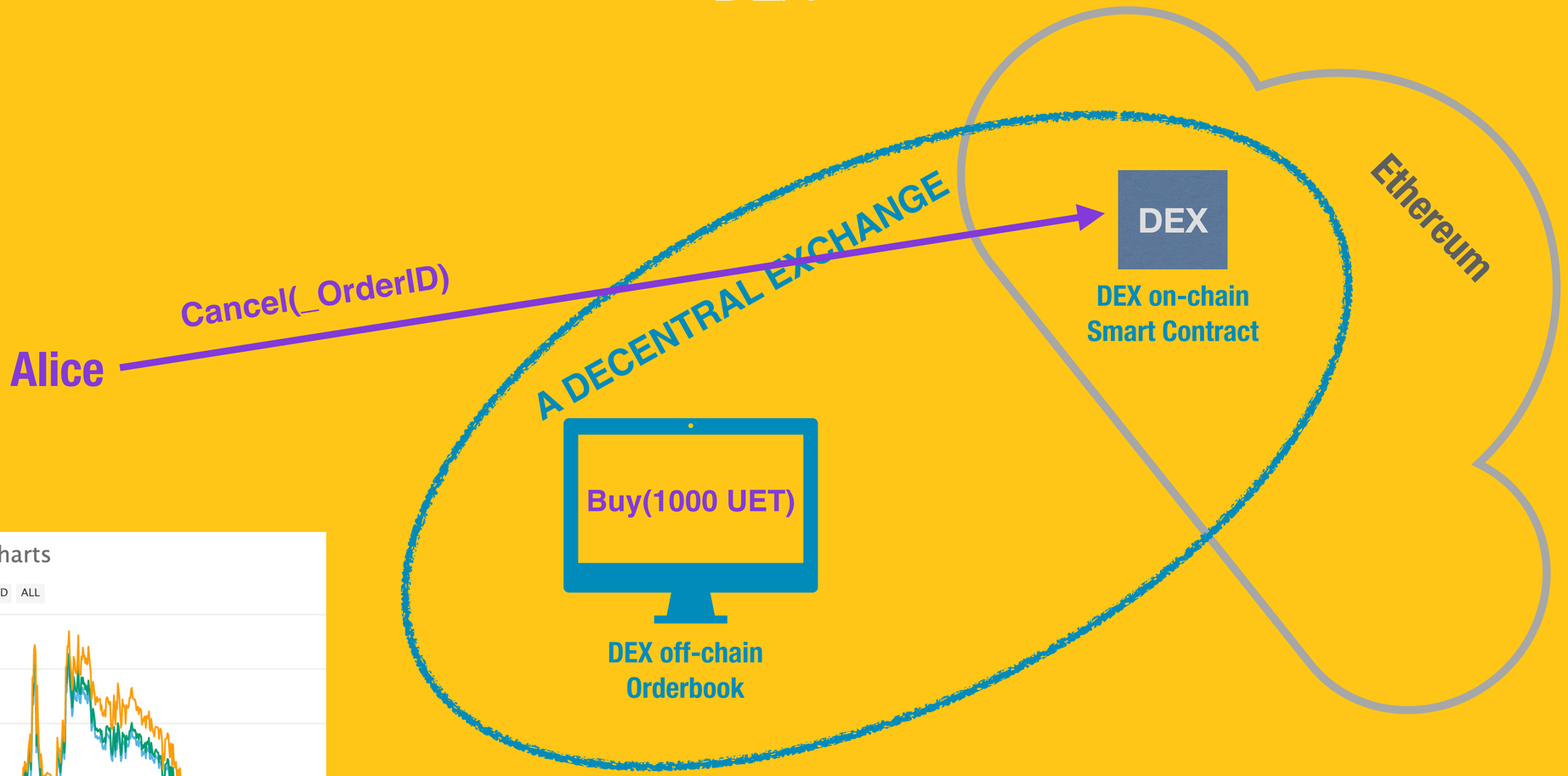


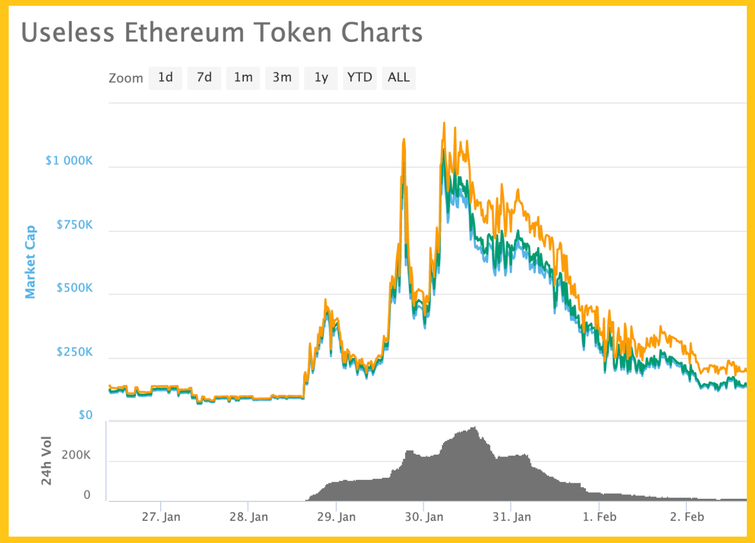
DEX


Alice
Buy(1000 UET)
A DECENTRAL EXCHANGE
Buy(1000 UET)
DEX off-chain
Orderbook
DEX
DEX on-chain
Smart Contract
Ethereum

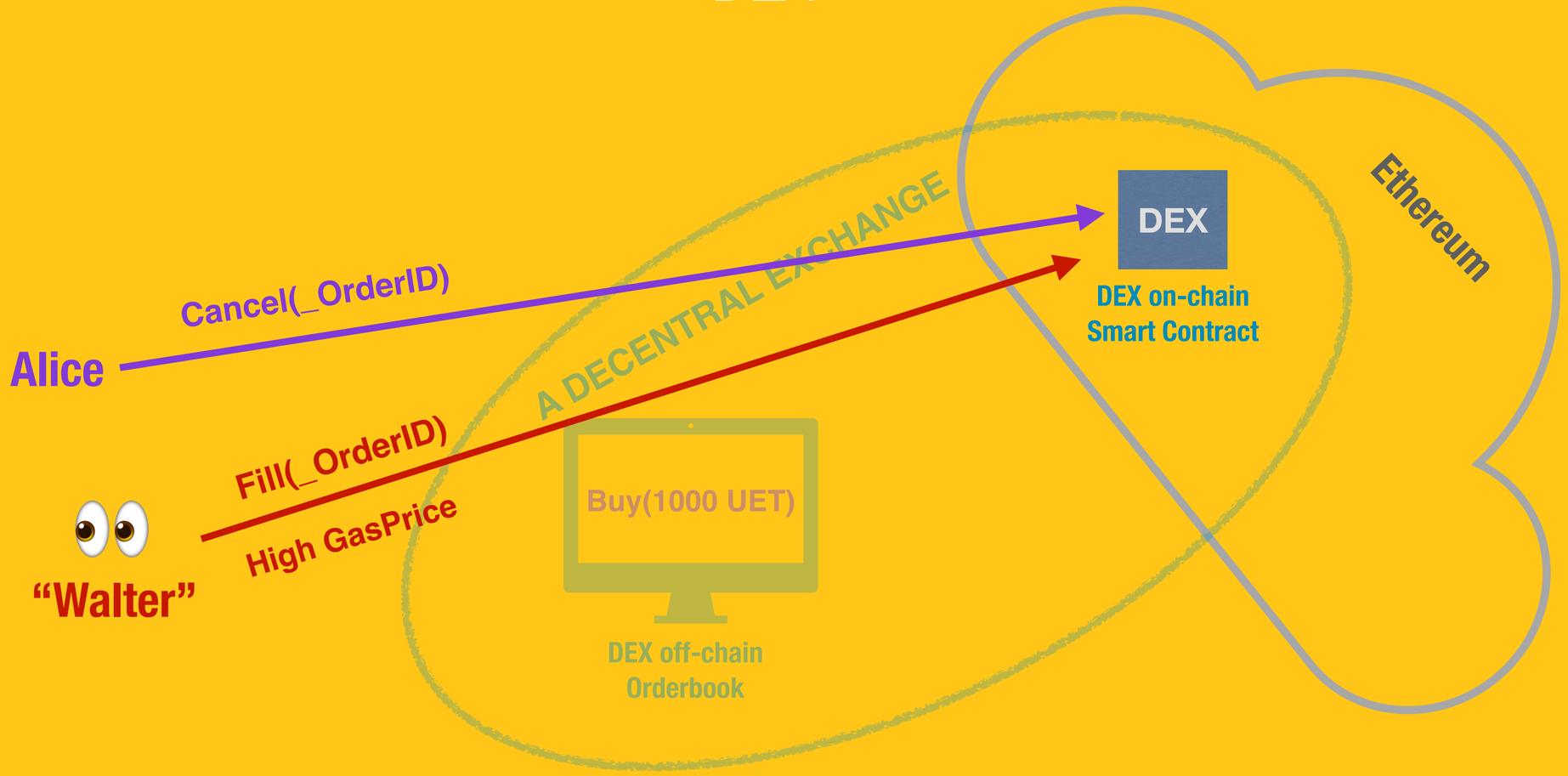

Useless Ethereum Token Charts
Zoom 1d 7d 1m 3m 1y YTD ALL
$1 000K
$750K
$500K
$250K
$0
Market Cap
200K
0
24h Vol
27. Jan
28. Jan
29. Jan
30. Jan
31. Jan
1. Feb
2. Feb

DEX

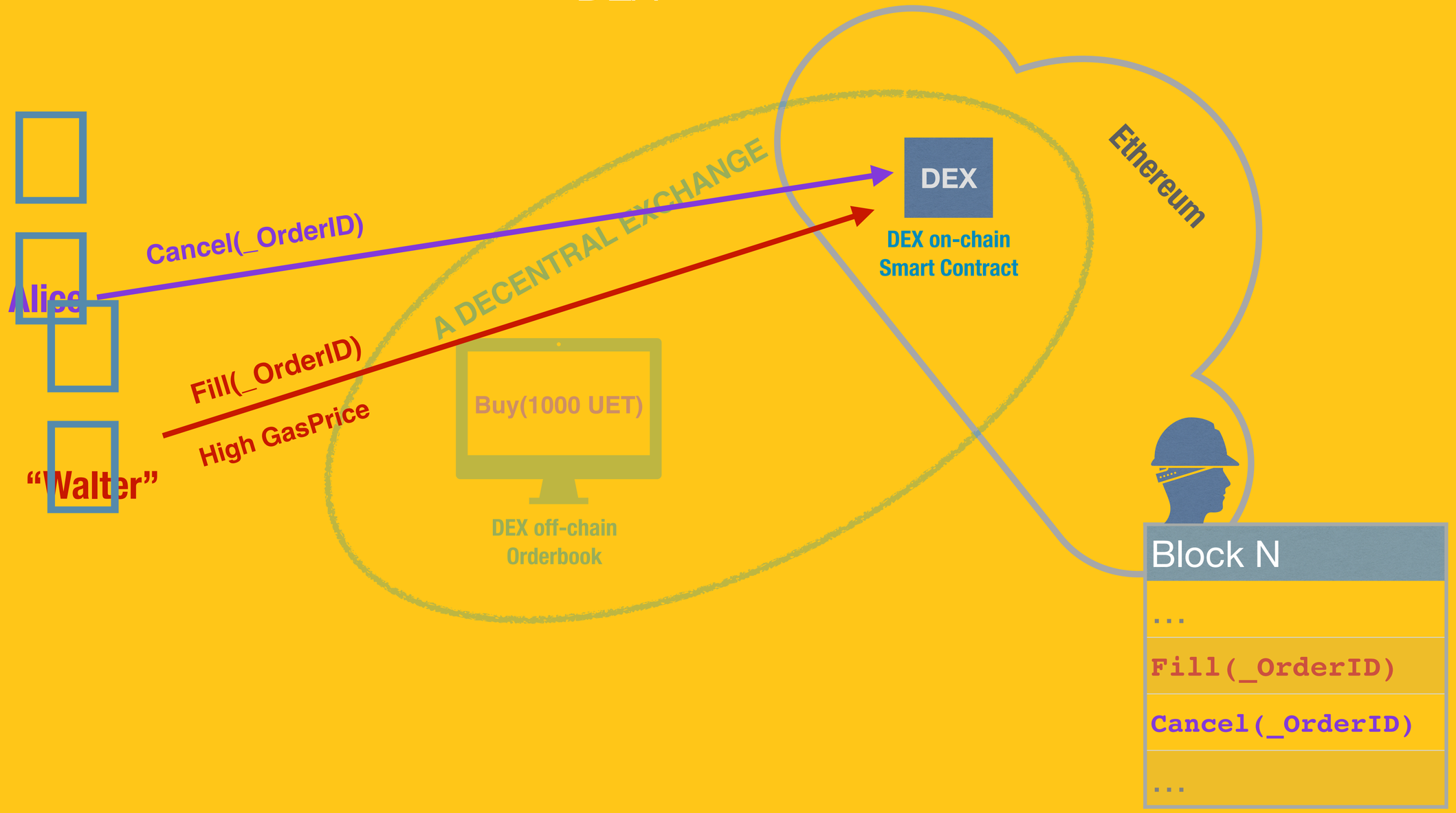

Alice
Cancel(_OrderID)
A DECENTRAL EXCHANGE
DEX
DEX on-chain
Smart Contract
Ethereum
Buy(1000 UET)
DEX off-chain
Orderbook


Useless Ethereum Token Charts
Zoom 1d 7d 1m 3m 1y YTD ALL
$1 000K
$750K
$500K
$250K
$0
Market Cap
200K
0
24h Vol
27. Jan
28. Jan
29. Jan
30. Jan
31. Jan
1. Feb
2. Feb

DEX


Ethereum
DEX
DEX on-chain
Smart Contract
A DECENTRAL EXCHANGE
Cancel(_OrderID)
Alice
Fill(_OrderID)
High GasPrice
"Walter"
Buy(1000 UET)
DEX off-chain
Orderbook

DEX


Alice
"Walter"
Cancel(_OrderID)
Fill(_OrderID)
High GasPrice
A DECENTRAL EXCHANGE
DEX
DEX on-chain
Smart Contract
Ethereum
Buy(1000 UET)
DEX off-chain
Orderbook
Block N
...
Fill(_OrderID)
Cancel(_OrderID)
...

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 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

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, tapp
increasing pot of ether, v
part. "Despite the near c
throwing their ether into
"The game, like most of t
ethereum network, found
going viral."

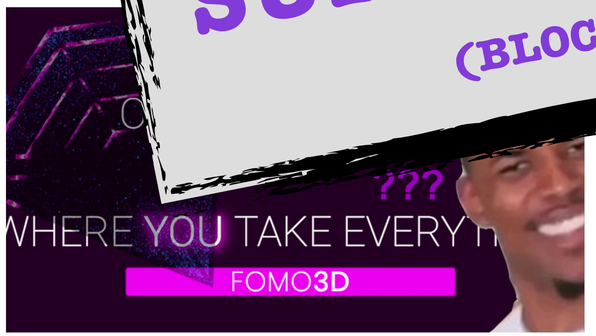
MOTHERBOARD
TECH BY VICE

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, 3:45pm



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.

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

You

SUPPRESSION ATTACK
(BLOCK STUFFING ATTACK)

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	Special Tricks
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	SparkPo
6191897	21 hrs 37 mins ago	103	0	bw

Normal block

30081 (99.99%)	7980567	15.85 Gwei	3.12648 Ether
8048328 (45.67%)	7988343	8.74 Gwei	3.03188 Ether

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**

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???

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

- **Privacy-Preserving Blockchains**
  - (2,3,4)-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.**

Confidentiality

- **Commit and Reveal.**
  - (3,4)- or (4)-confidentiality
  - Namecoin, ENS
  - Collateralized?
    - Leaks information
    - Submarine Commit

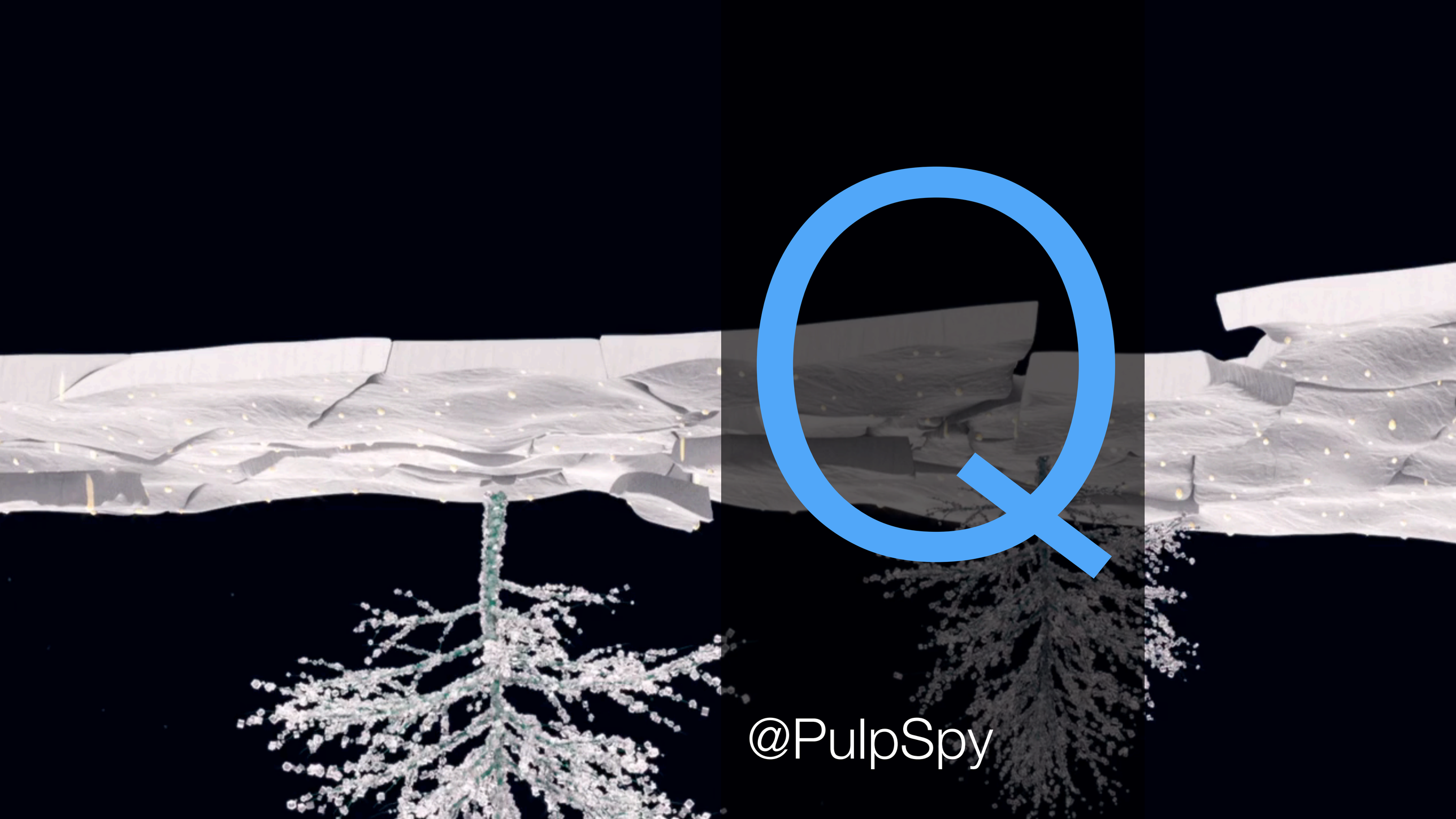
1	**Code of the DApp**
2	**Current state of the DApp**
3	**Name of the function being invoked**
4	**Parameters supplied to the function**
5	**Address of the contract**
6	**Identity of the sender.**

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"

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