Gabriel Coutinho de Paula
Twitter: @GCdePaula_
Github: @GCdePaula

link to paper

Dave fraud proof

triumphing over Sybils
with *a laptop* and a *small collateral*


cartesi

why not *ZK*?

There are no silver bullets!

fraud proofs can prove 10,000× *larger computations*
with *less costs*

(I love ZK btw)

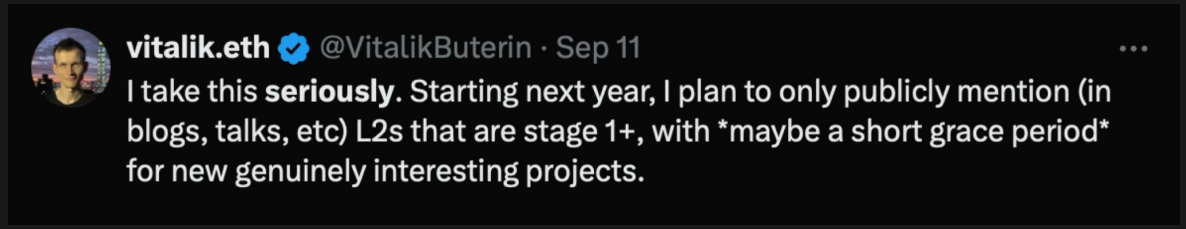
TL;DR

- Fraud proofs are hard.
- Previous attempts are either unsafe, centralized, or slow.
- dave goes brrrrr

Dave paper

Motivation

fraud proofs are in a pickle



#	NAME	RISKS	TYPE	STAGE	TOTAL VALUE LOCKED
1	Arbitrum One		Optimistic Rollup	STAGE 1	$13.72B ▼2.48%
2	Base		Optimistic Rollup OP	STAGE 0	$8.07B ▲4.35%
3	OP Mainnet		Optimistic Rollup OP	STAGE 1	$6.13B ▼3.10%
4	Mantle		Optimium OP	N/A	$1.38B ▼2.95%
5	Blast		Optimistic Rollup OP	STAGE 0	$1.37B ▼3.03%

What is holding fraud proofs back?

It is hard to get them right.

1. *you* can be a *validator*

even if you're broke and your computer is a toaster

+

2. *you* can defeat *anyone*

even if they're a nation-state

=

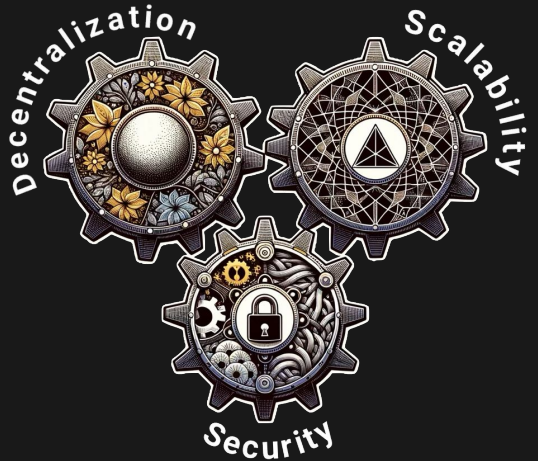
inherit L1 security ✨

3. without delays

even if you’re George R. R. Martin

Design goals

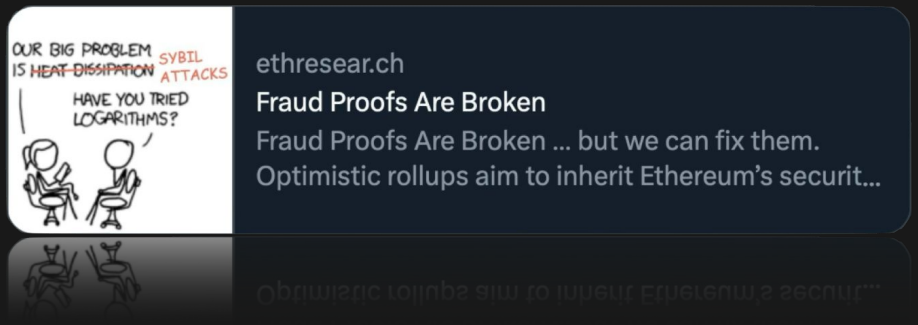
1. **Decentralization:** no supercomputer, no huge bonds
2. **Security:** can’t steal TVL
3. **Liveness:** no large delays



Sybil attacks

1. Resource exhaustion attacks that steal TVL (*no security*)
2. Delay attacks (*no liveness*)

Mitigation restricts participation (*no decentralization*)



Current solutions

1. **Optimism:** Optimism fault proof system (OP)
2. **Arbitrum:** Bounded Liquidity Delay (BoLD)
3. **Cartesi:** Permissionless Refereed Tournaments (PRT)

Comparison sneak peek

1 million ether Sybil attack

	bond	expenses*	delay
OP	0.08 ETH	1 000 000 ETH	2 weeks
BoLD	3600 ETH	150 000 ETH	2 weeks
PRT-1L	1 ETH	1 ETH	20 weeks
Dave	3 ETH	7 ETH	4 weeks

* Expenses are reimbursed to honest parties after the dispute is over.

Concepts

Sybil is a wolf to Sybil

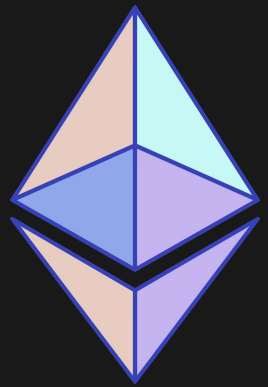
Threat model

1. L1 works, but:
    a. adversary can censor for 1 week;
    b. adversary can control tx order.
2. One honest validator (Willie).
    a. Willie has a laptop and few ether.

Pairwise refutation game

- **Goal:** prove the result of a program to the blockchain.
- **Setup:** blockchain, player one and player two.

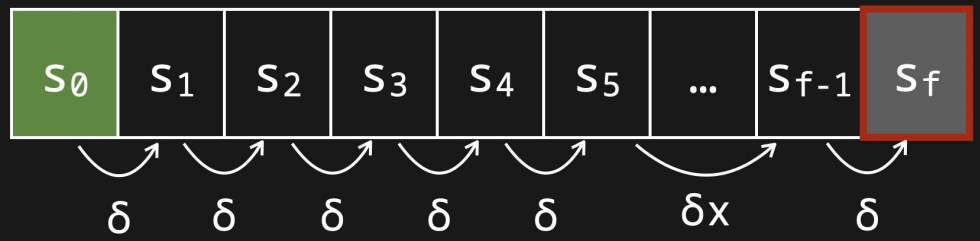
Players fight to prove the other player is *incorrect*.



Intuition for pairwise refutation game

Computation Model

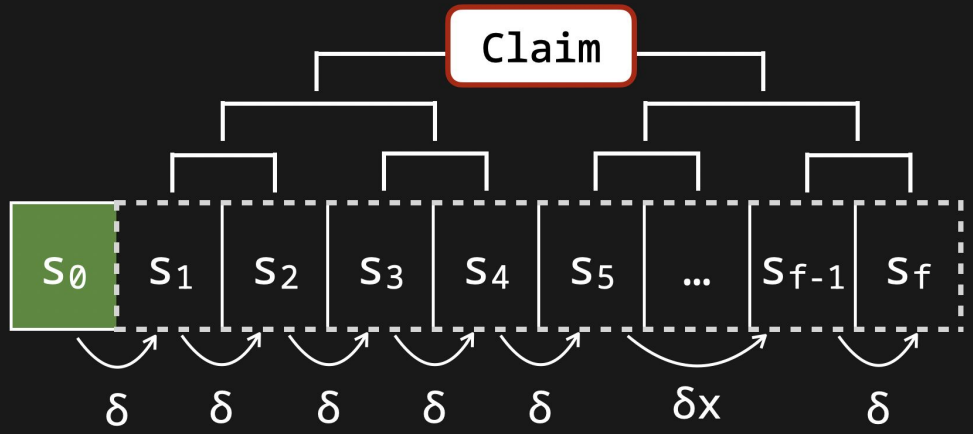
- An *initial state* s_0, agreed by everyone.
- A *state-transition function* δ, agreed by everyone.



1. Binary search to find first divergence
2. Verify divergence (single δ) onchain

Computation hash

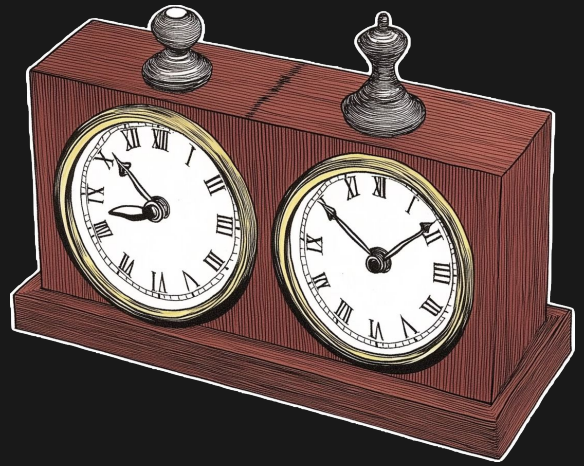
Validators commit to the computation history (i.e. *computation hash*)



(Merkleized!)

Improvement: validators can't lie during bisection

Chess clock



- Players act in turns for binary search.
- Matches can end by timeout.

Problem: 1 week censorship 🥵
...otherwise interaction would take minutes 🤔

Chess clocks amortize censorship over many interactions.

$$(7d + 5m) \times i$$

$$7d + 5m \times i$$

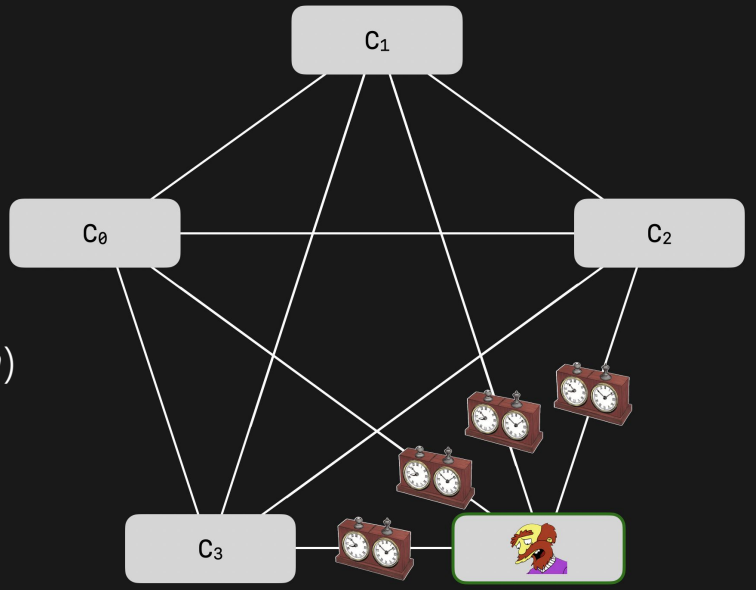
Multiparty refutation game — parallel (BoLD)

- Finishes fast!
- ...but might *overwhelm* Willie and steal TVL.

I don't want Willie to personally fight everyone.

Mitigation: high bond price

However, restricts participation (*no decentralization*)



... but with 1M Sybils

Multiparty refutation game — brackets (PRT)

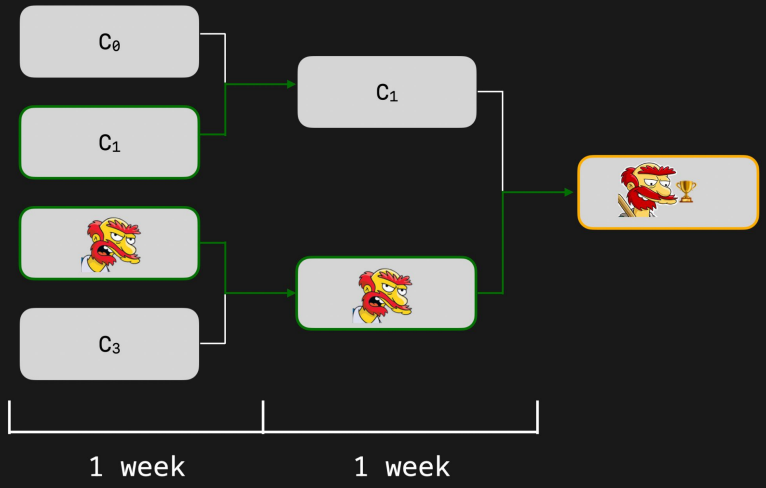
Sybil eliminates Sybil:

- Expenses grow logarithmically ✨
- Delay grows logarithmically ✨

Exponential resource and delay advantage

Problem: 1 week censorship 🥵

...otherwise matches would take only ~2h 🤔



... but with 20 rounds

The goal of Dave

PRT pays censorship time *every round*:

$$(7d + 2h) \times \log2(Sybils)$$

$$7d >> 2h$$

Dave *amortizes* censorship time over entire dispute:

$$7h + 2h \times \log2(Sybils)$$

link to paper

Dave

Triumphing over Sybils

Repechage setup

Make matches not eliminatory!

let censorship = 7d; match = 1d

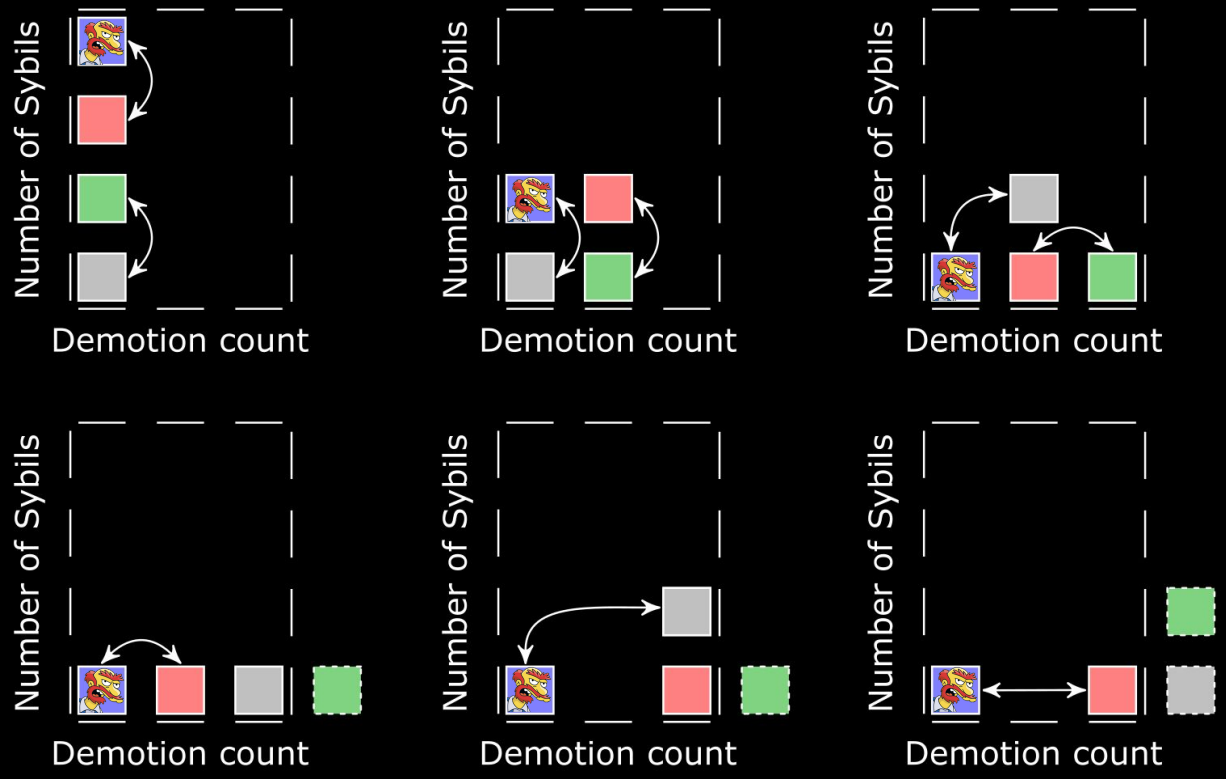
- Surviving claims are *rematched* pairwise every 1 day.
- Willie can only lose a match due to censorship.
- Willie plays many matches, but *never loses more than 7 matches.*

Claims start dispute with 8hp

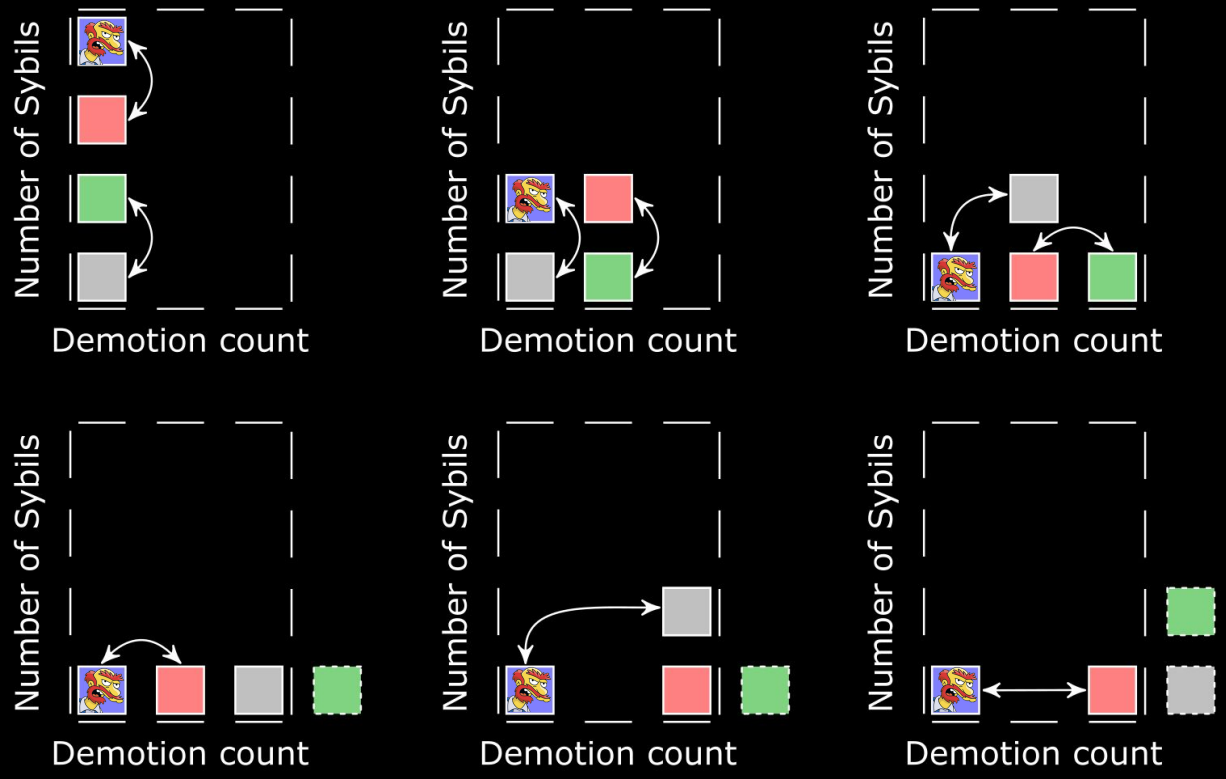
but adversary has only 7 bullets

hp: ❤️❤️❤️❤️❤️❤️❤️❤️

Repechage with three hp {❤️❤️❤️}



Matchmaking with three hp {❤️❤️❤️}



Dave matchmaking

Rematching adversarially

$\propto 7d \times \log_2(\text{Sybils})$

Rematching with *similar hp*

$\propto 7d + 1d \times \log_2(\text{Sybils})$

see paper for proof

you can be Wille ✅

requires a laptop and a 3 ether collateral

+

you can defeat *anyone* ✅

exponential resource advantage

=

L1 security inherited 🦇📢

< 4 weeks

even if you're Willie

Thus Dave triumphed over the Sybils with a laptop and a small collateral.
Dave had no supercomputer on his hands.

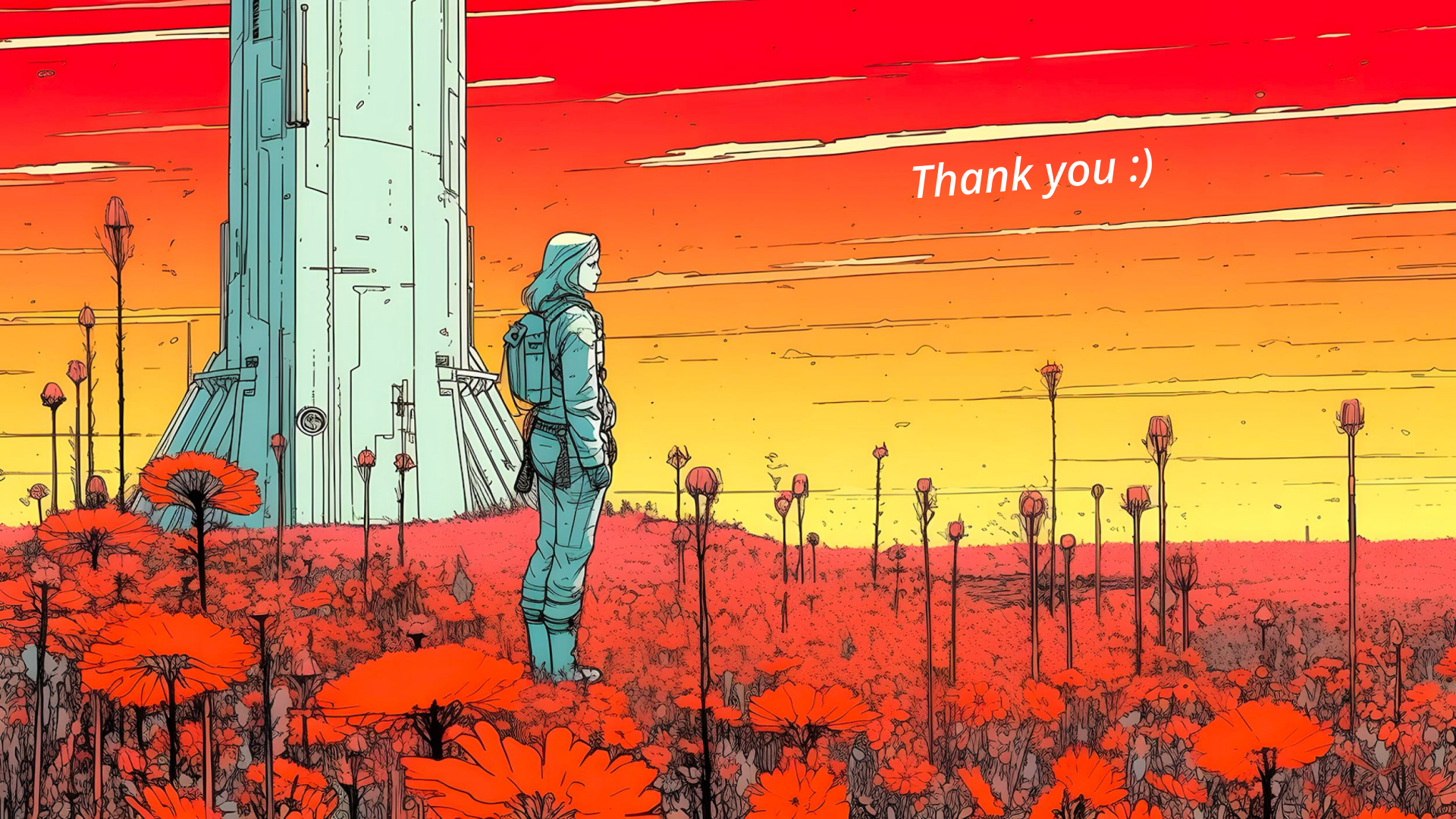
1 Samuel 17:50

Comparison

1 million ether Sybil attack

	bond	expenses*	delay
OP	0.08 ETH	1 000 000 ETH	2 weeks
BoLD	3600 ETH	150 000 ETH	2 weeks
PRT-1L	1 ETH	1 ETH	20 weeks
Dave	3 ETH	7 ETH	4 weeks

* Expenses are reimbursed to honest parties after the dispute is over.


Thank you :)

Dave paper

Gabriel Coutinho de Paula
Twitter: @GCdePaula_
Github: @GCdePaula