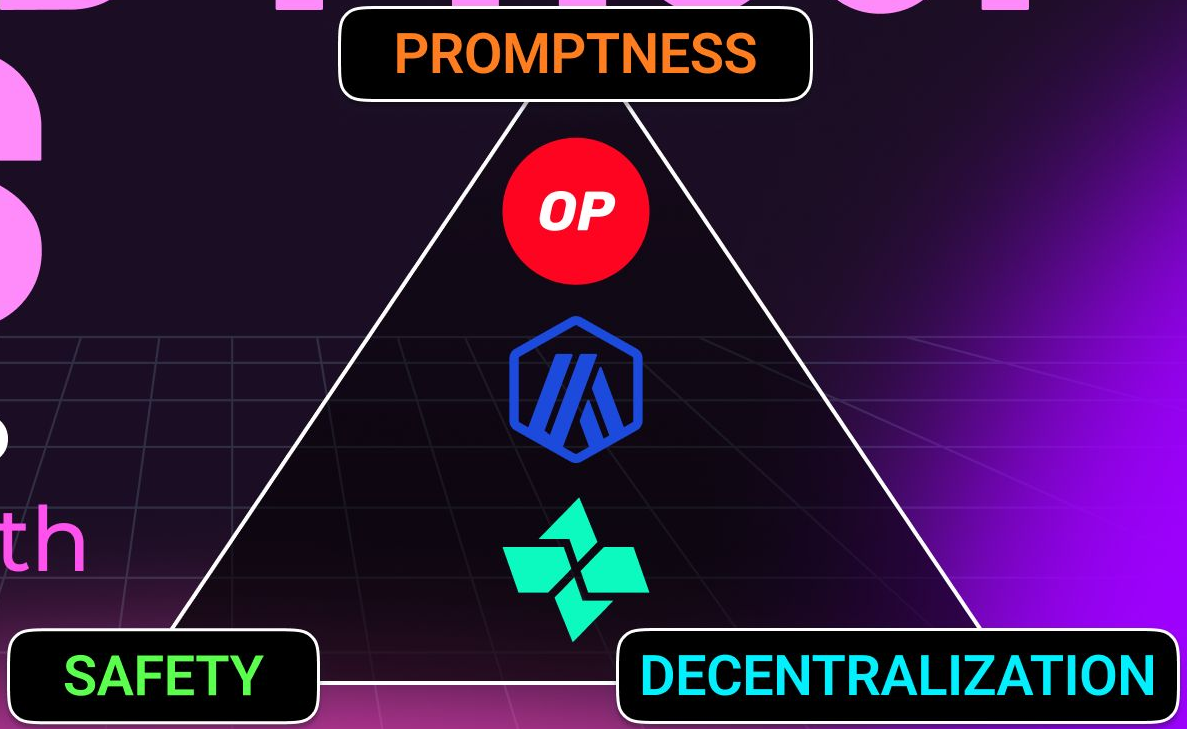
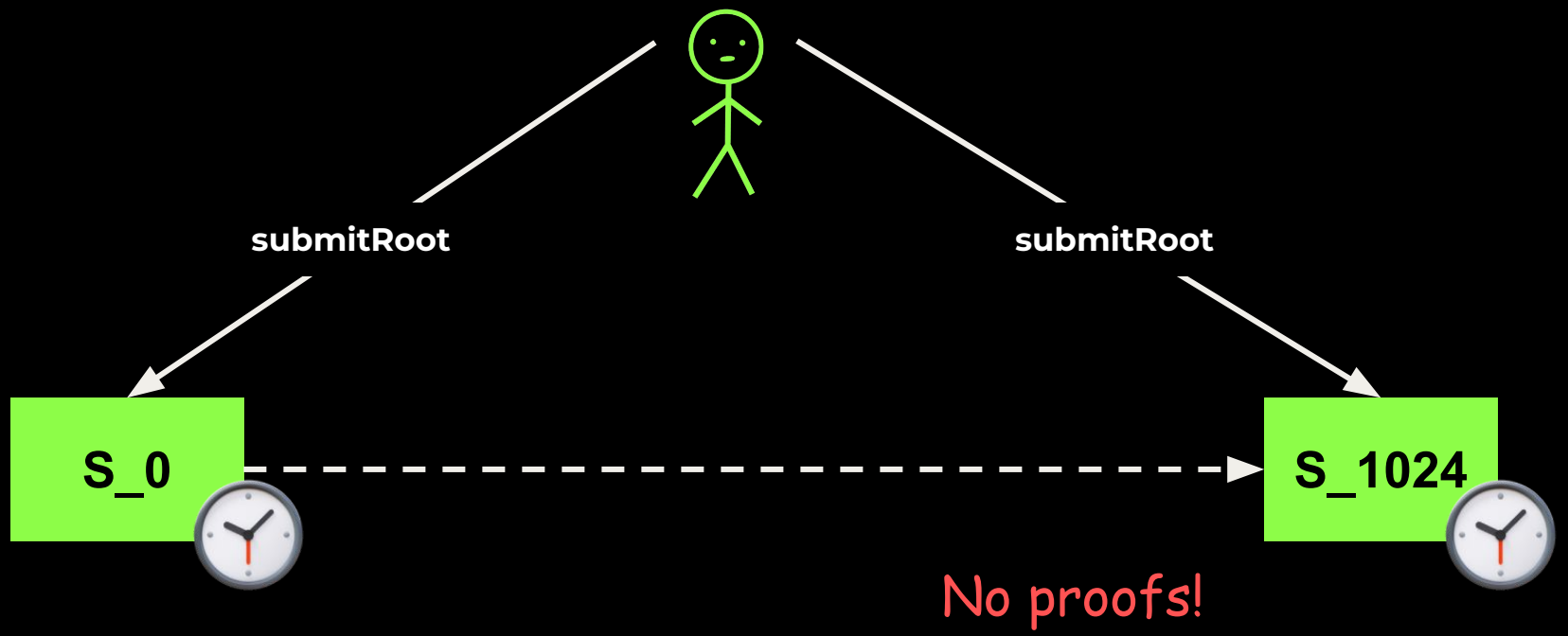
FRAUD PROOF WARS

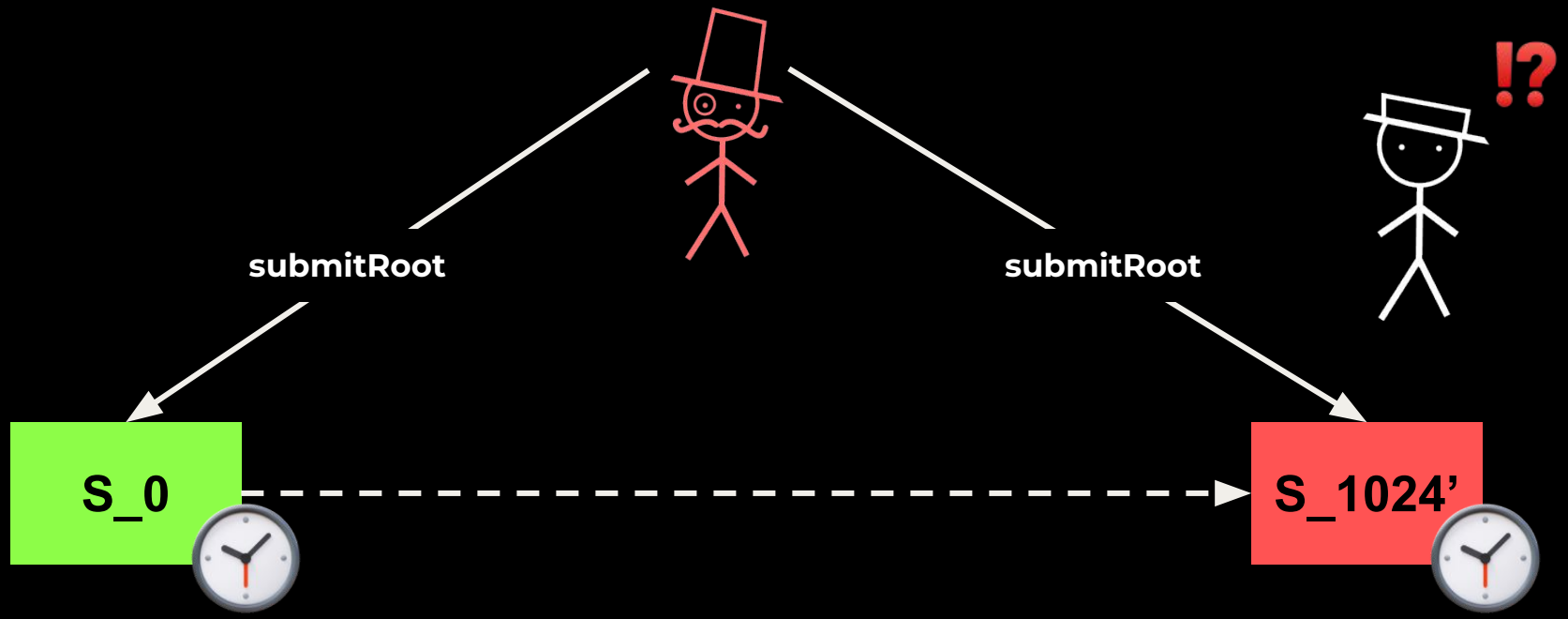
by Luca Donno
@donnoh_eth



Optimistic rollups: **Happy case**



Optimistic rollups: Not so happy case



THE ORIGINAL VISION:

Any single honest challenger can protect an optimistic rollup with a fixed challenge period

HE ORIGINAL VISION:

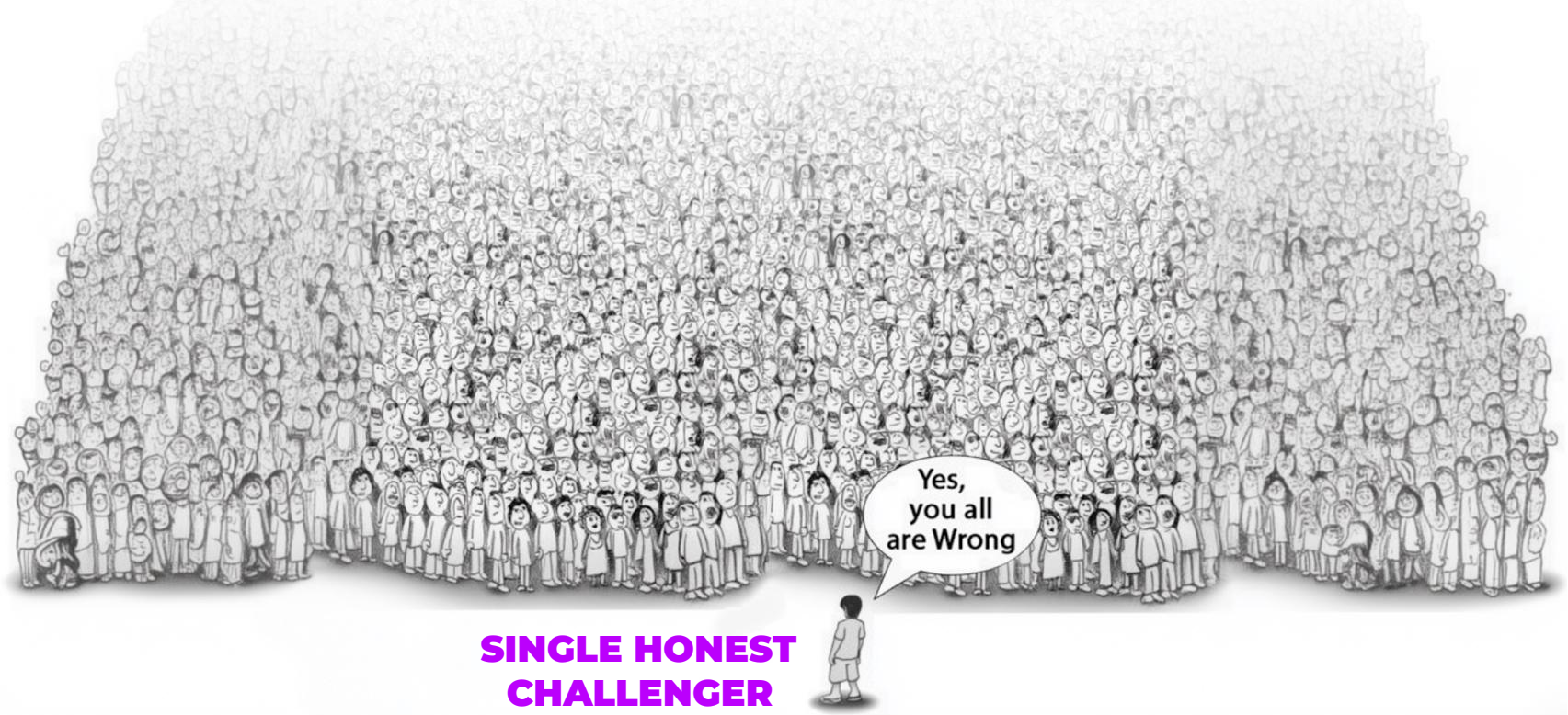
Any st challenger

can protec rollup

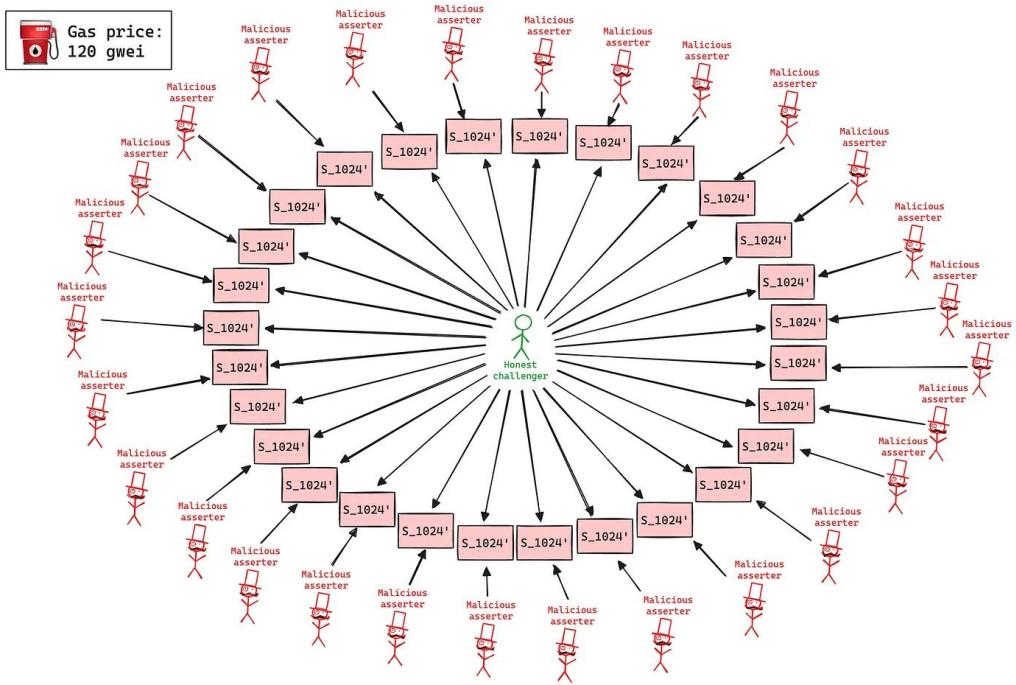
with a fixed chal

NOT POSSIBLE

Sybil attack on optimistic rollups



Option 1: Full concurrency



CHALLENGE PERIOD:
7d (global)

COST OF ONE CHALLENGE:
1 ETH (symmetrical)

FUNDS IN THE BRIDGE:
1000 ETH

ATTACKER FUNDS:
800 ETH

HONEST CHALLENGER FUNDS:
500 ETH

ATTACKER WINS

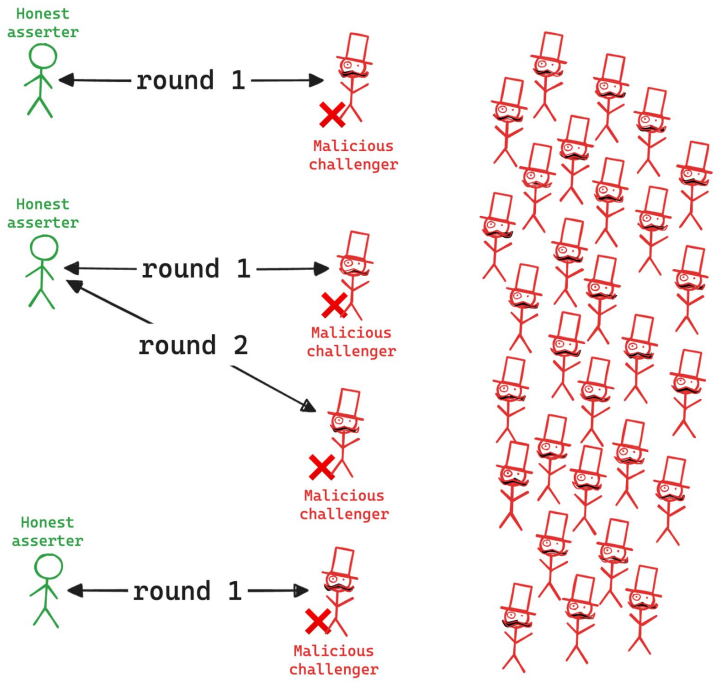
~~Any single honest challenger~~
can protect an optimistic rollup
with a fixed challenge period

CHALLENGERS WITH MORE FUNDS THAN THE ATTACKERS

challenger

can protect an optimistic rollup with a fixed challenge period

Option 2: Partial concurrency



CHALLENGE PERIOD:
7d (per challenge)

COST OF ONE CHALLENGE:
1 ETH (symmetrical)

FUNDS IN THE BRIDGE:
1000 ETH

ATTACKER FUNDS:
800 ETH

HONEST CHALLENGER FUNDS:
2 ETH

TOTAL DELAY: 800 WEEKS (>15 YEARS)

Any single honest challenger can protect an optimistic rollup with a ~~fixed challenge period~~

Any single honest challenger can protect an optimistic rollup with a ~~fixed challenge period~~

NON-FIXED CHALLENGE PERIOD

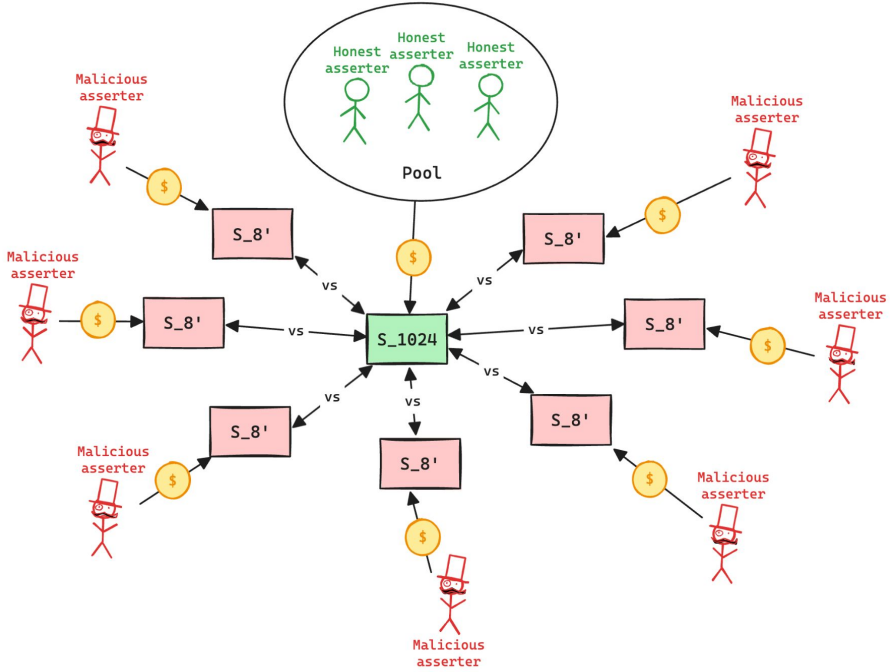
Full concurrency vs Partial concurrency

Resource exhaustion attacks
(full concurrency)

TRADE-OFF

Delay attacks
(partial concurrency)

Full concurrency optimizations



CHALLENGE PERIOD:
7d (global)

BONDS:
10 ETH

COST OF ONE CHALLENGE:
1 ETH (symmetrical)

FUNDS IN THE BRIDGE:
1000 ETH

ATTACKER FUNDS:
800 ETH

HONEST CHALLENGERS FUNDS:
500 ETH

DEFENDERS WIN

Execution history commitments

PROBLEM:

This improvement is **not possible** if correct state roots can lose via invalid bisections.

SOLUTION:

Enforce correct bisection via an "execution history commitment" over all steps.

Ex history commitments

PR

Th

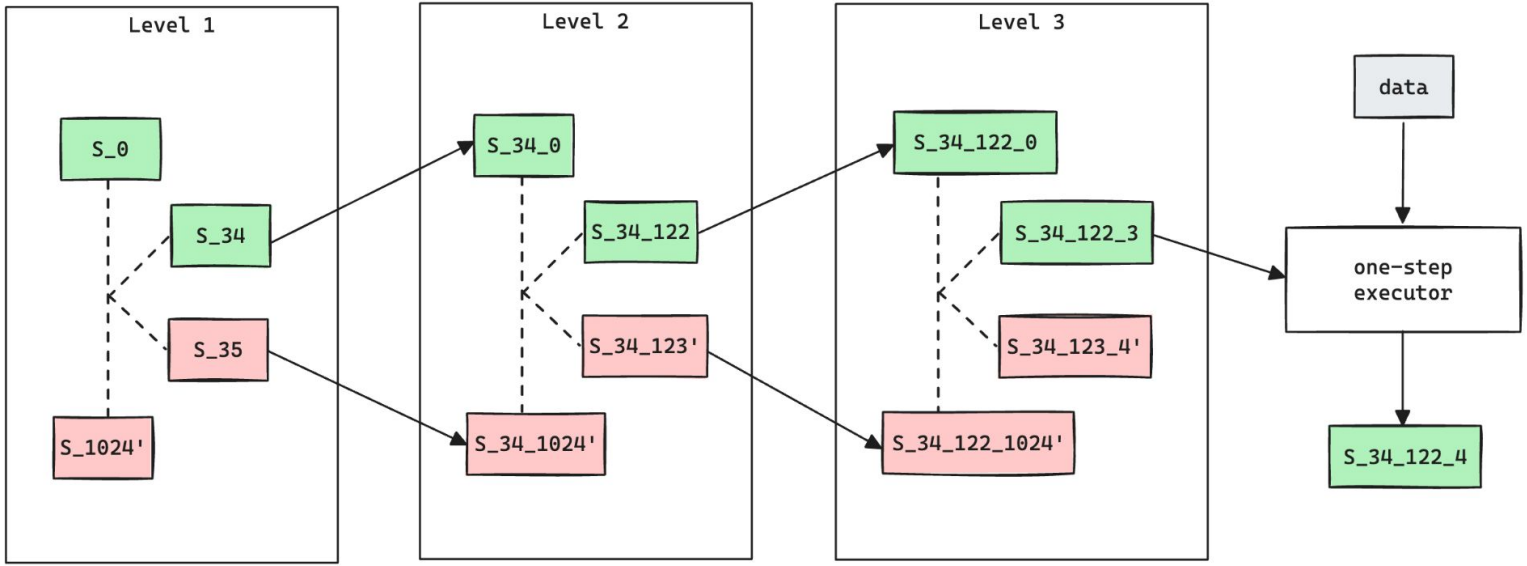
ro

S

Enforce

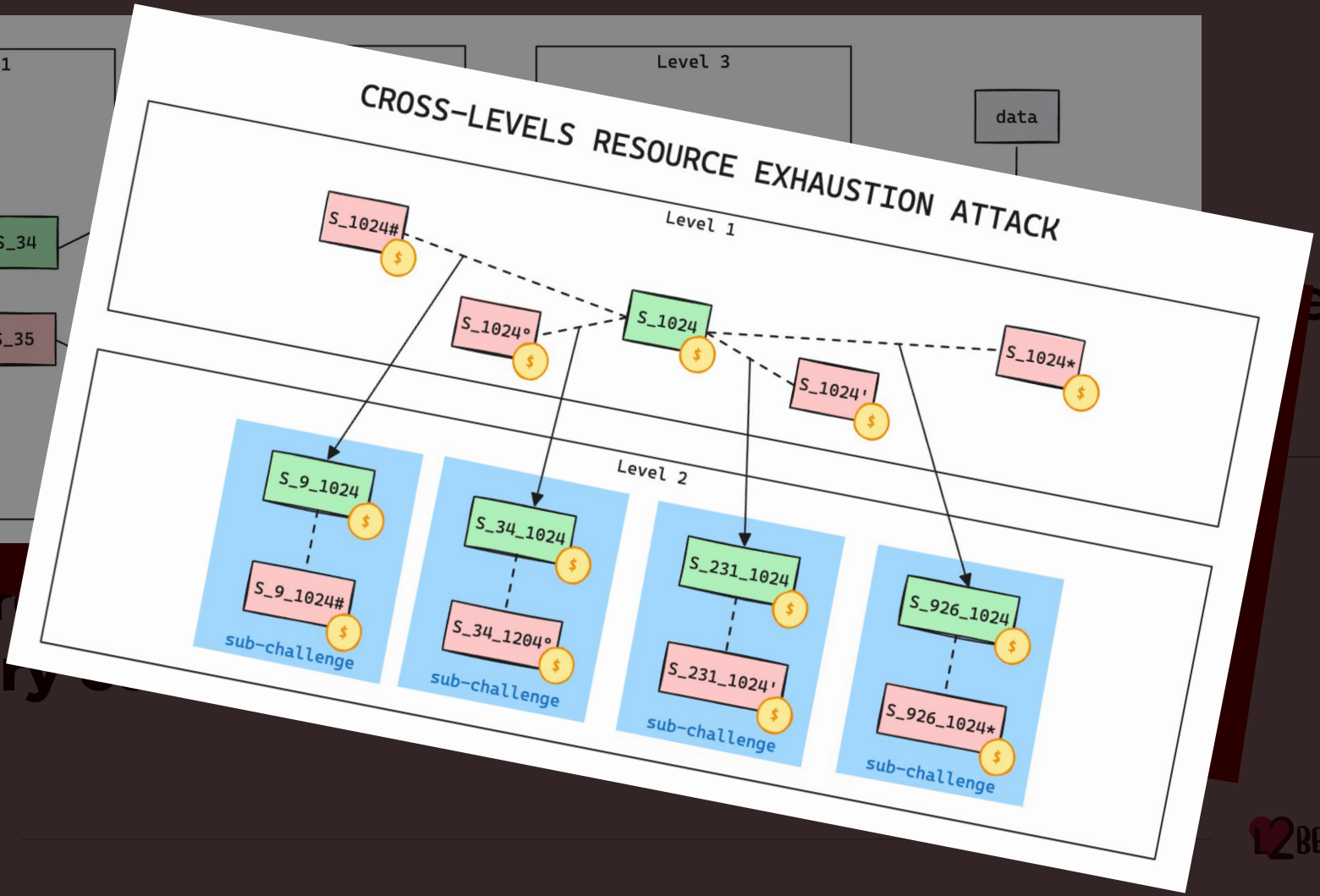
history commitment

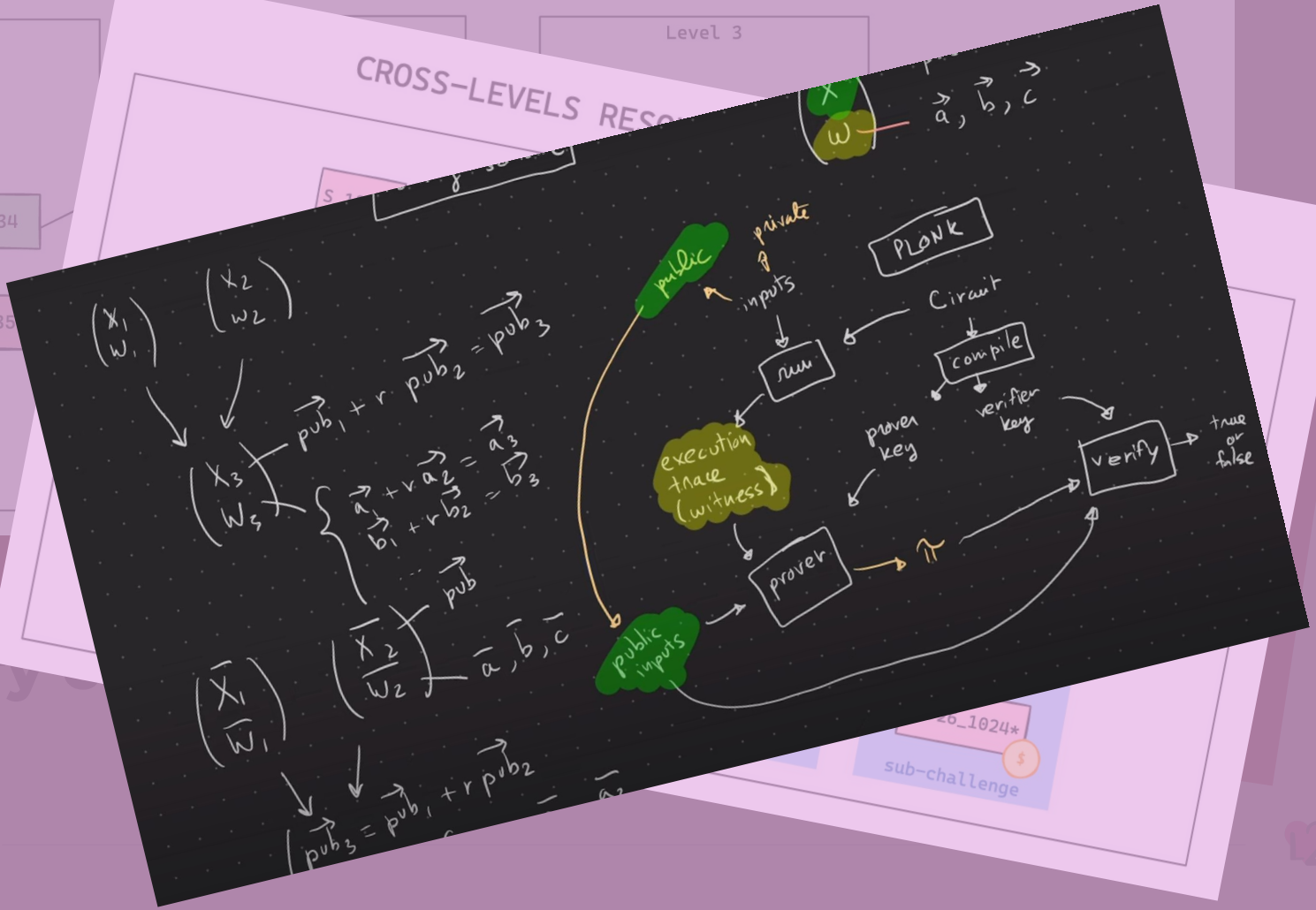
MUCH MORE COMPLICATED THAN IT SEEMS



THAN IT SEEMS

Enforce
history commitment


CROSS-LEVELS RESOURCE EXHAUSTION ATTACK
Level 1
S_1024#
S_1024°
S_1024
S_1024'
S_1024*
Level 2
S_9_1024
S_9_1024#
S_34_1024
S_34_1204°
S_231_1024
S_231_1024'
S_926_1024
S_926_1024*
sub-challenge
sub-challenge
sub-challenge
sub-challenge


PLONK
Circuit
compile
run
inputs
private
public
execution trace (witness)
prover key
verifier key
prover
verify
true or false
public inputs

Full concurrency in practice

	Execution history commitments	Resource ratio	Initial bond size
Arbitrum (BoLD)	✅	15%	3600 ETH
OP Mainnet	❌	109%	0.08 ETH

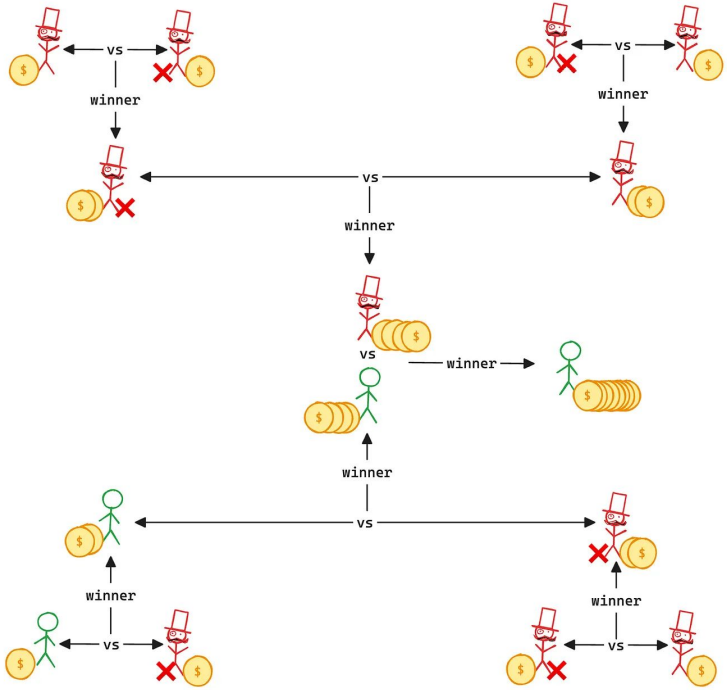
Full concurrency

Resource ratio
(safety)

FULL CONCURRENCY
TRADE-OFF

Initial bond size
(decentralization)

Partial concurrency optimizations



CHALLENGE PERIOD:
7d (per challenge)

COST OF ONE CHALLENGE:
1 ETH (symmetrical)

FUNDS IN THE BRIDGE:
1000 ETH

ATTACKER FUNDS:
800 ETH

HONEST CHALLENGER FUNDS:
2 ETH

TOTAL DELAY:
2 MONTHS AND 1 WEEK

Partial concurrency in practice: 3 million ETH attack ($9.5B)

	Tournament	Initial bond size	Settlement delay
Arbitrum (Classic)	❌	3 ETH	4.5 months
Cartesi (Dave)	✅	3 ETH	5 weeks

Partial concurrency

Delay attacks
(promptness)

PARTIAL CONCURRENCY
TRADE-OFF

Initial bond size
(decentralization)

The fraud proofs trilemma