PLASMA

Johann Barbie

parseclabs.org

Agenda

1. Plasma Classic
2. CAS
3. Code Challenge
4. Distribute Rewards ==>

Mauveover ChainCat

Chestnut | Skyblue

Kitty #65222

Calicool Snagglepuss

Paris

ethCC 2018

Vitalik

Karl

The Scalability Problem

To enforce correctness every participant has to validate the chain themselves.

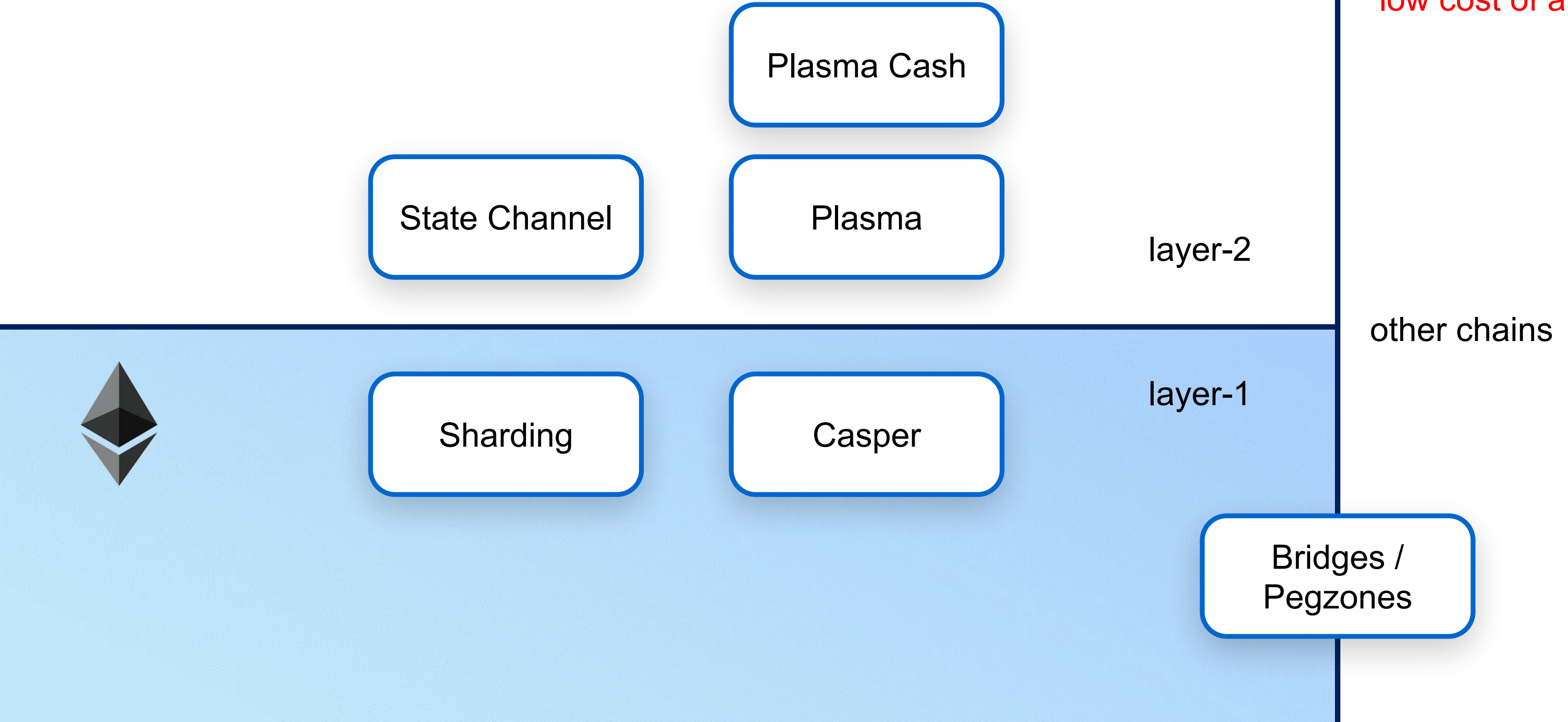
=> Block size limited to stay decentralized.

=> limited transaction throughput
=> limited execution complexity

Scalability Solutions Map

security by economic incentives

=> new chains have low cost of attack



Plasma Cash

State Channel

Plasma

layer-2

other chains

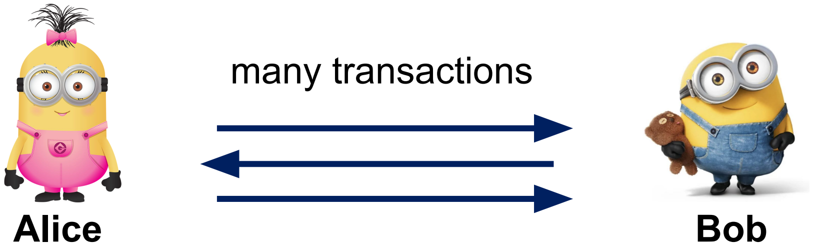
Sharding

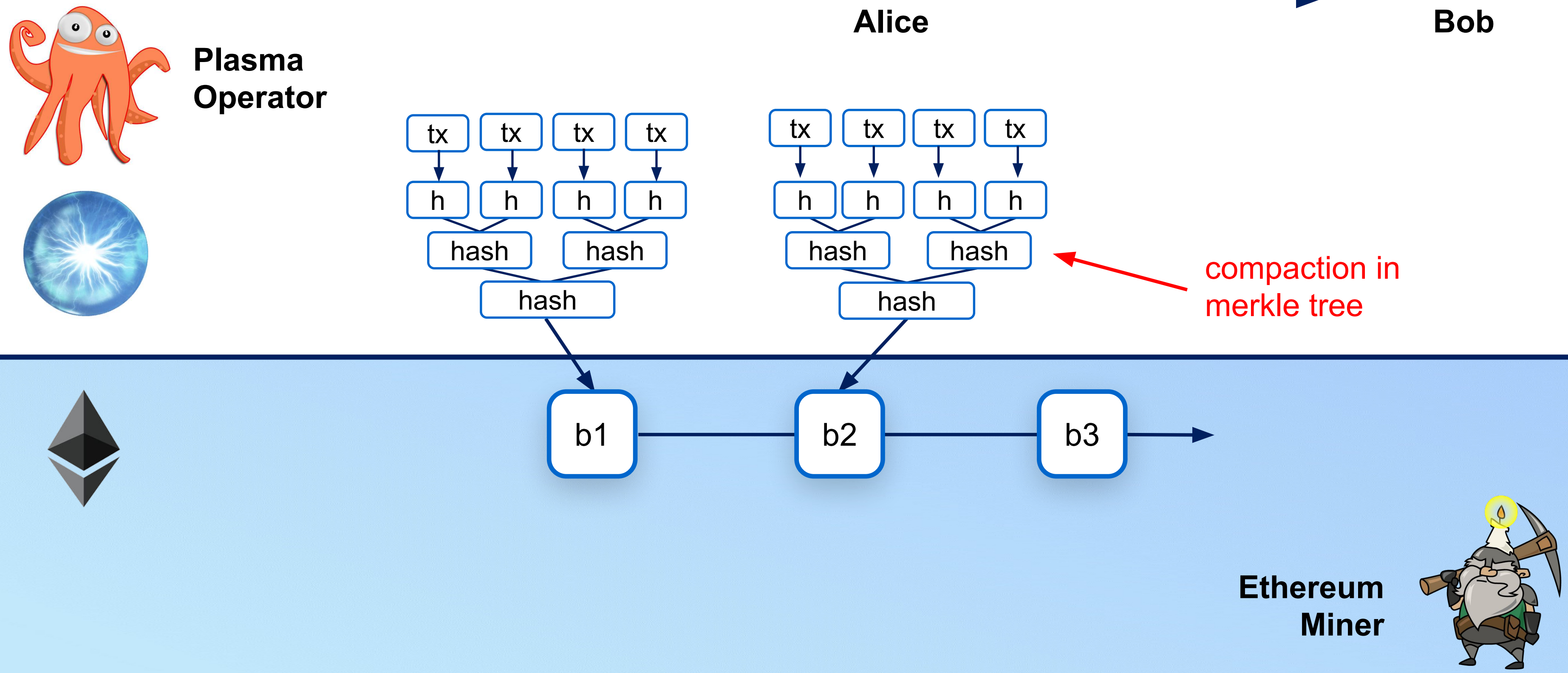
Casper

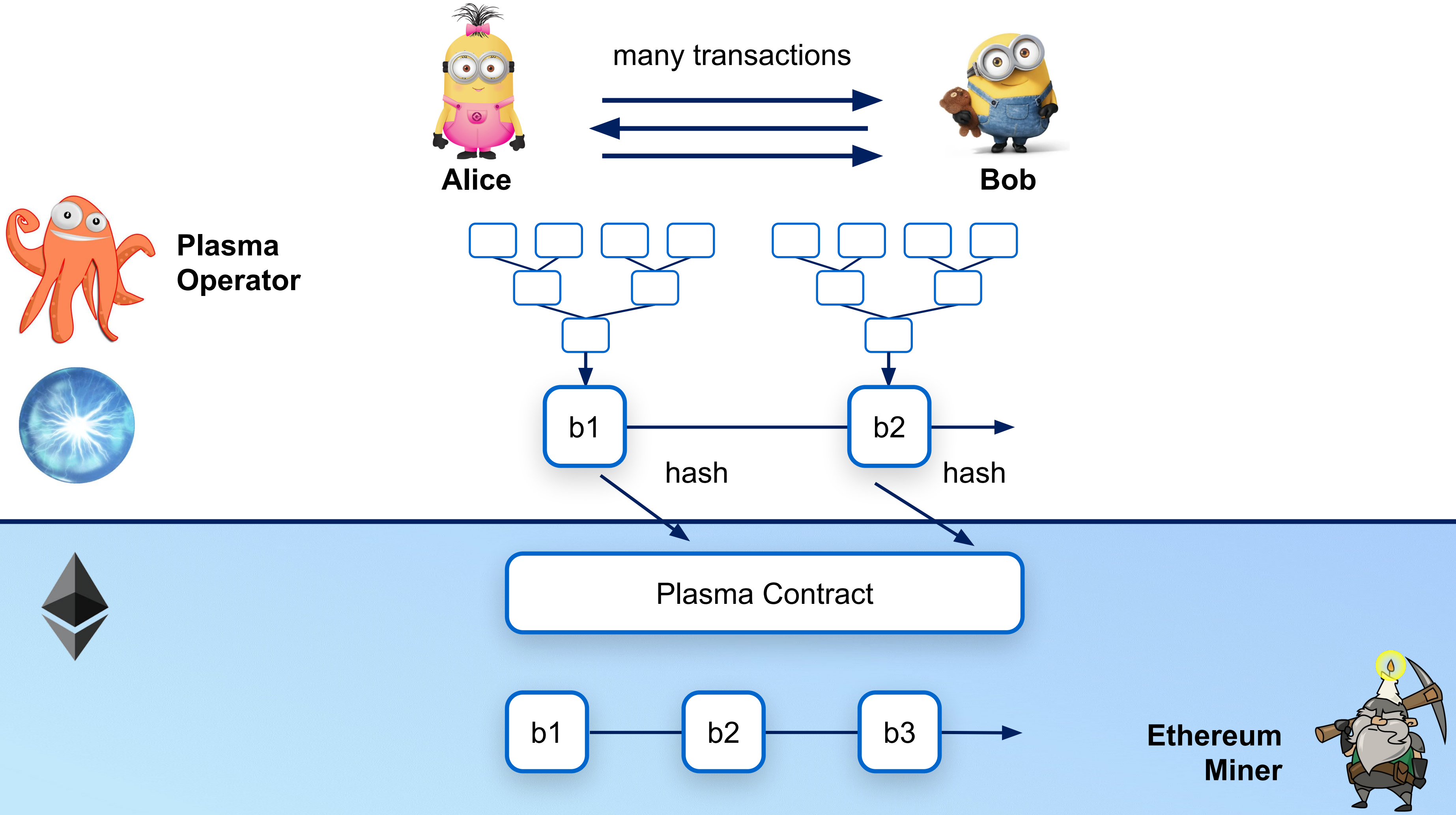
layer-1

Bridges / Pegzones

What is Plasma?







many transactions

Alice

Bob

Plasma
Operator

b1

b2

hash

hash

Plasma Contract

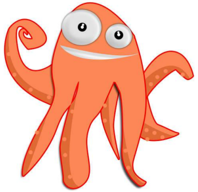
b1

b2

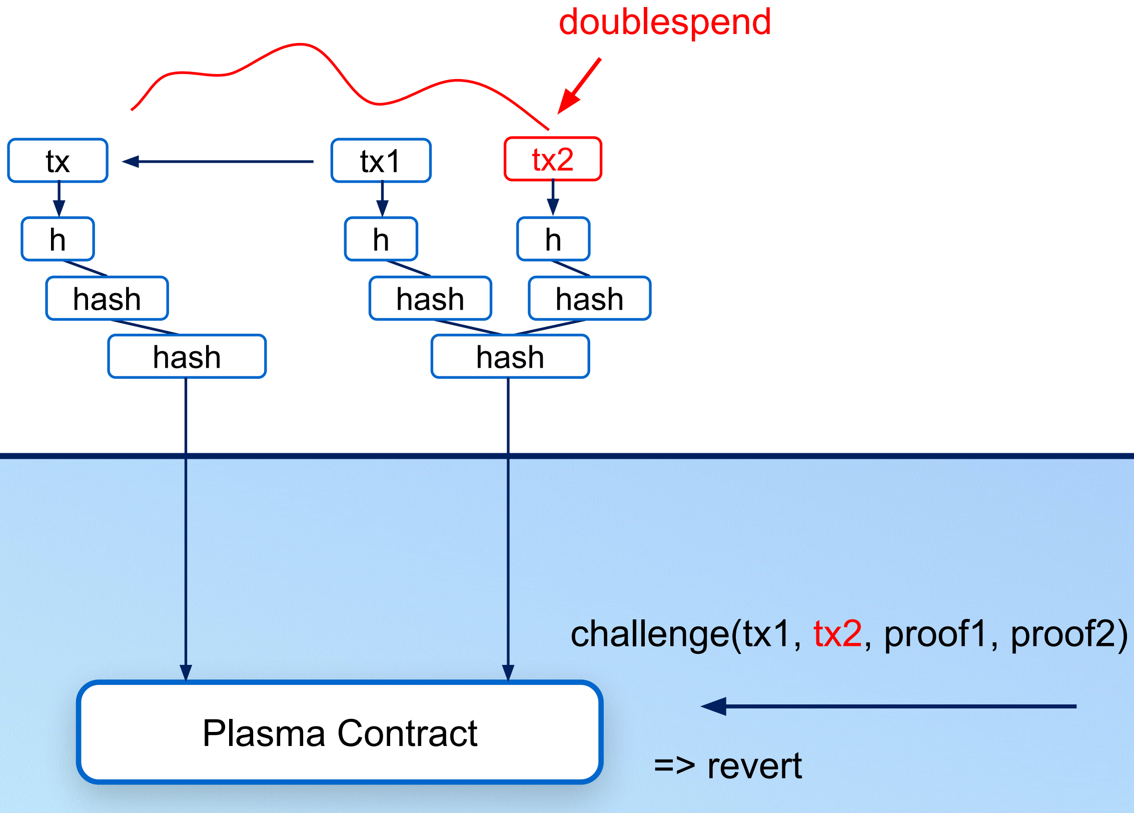
b3

Ethereum
Miner

Restricted Authority



Plasma Operator



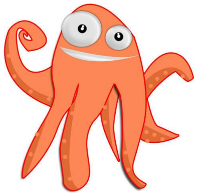
challenge(tx1, tx2, proof1, proof2)

=> revert

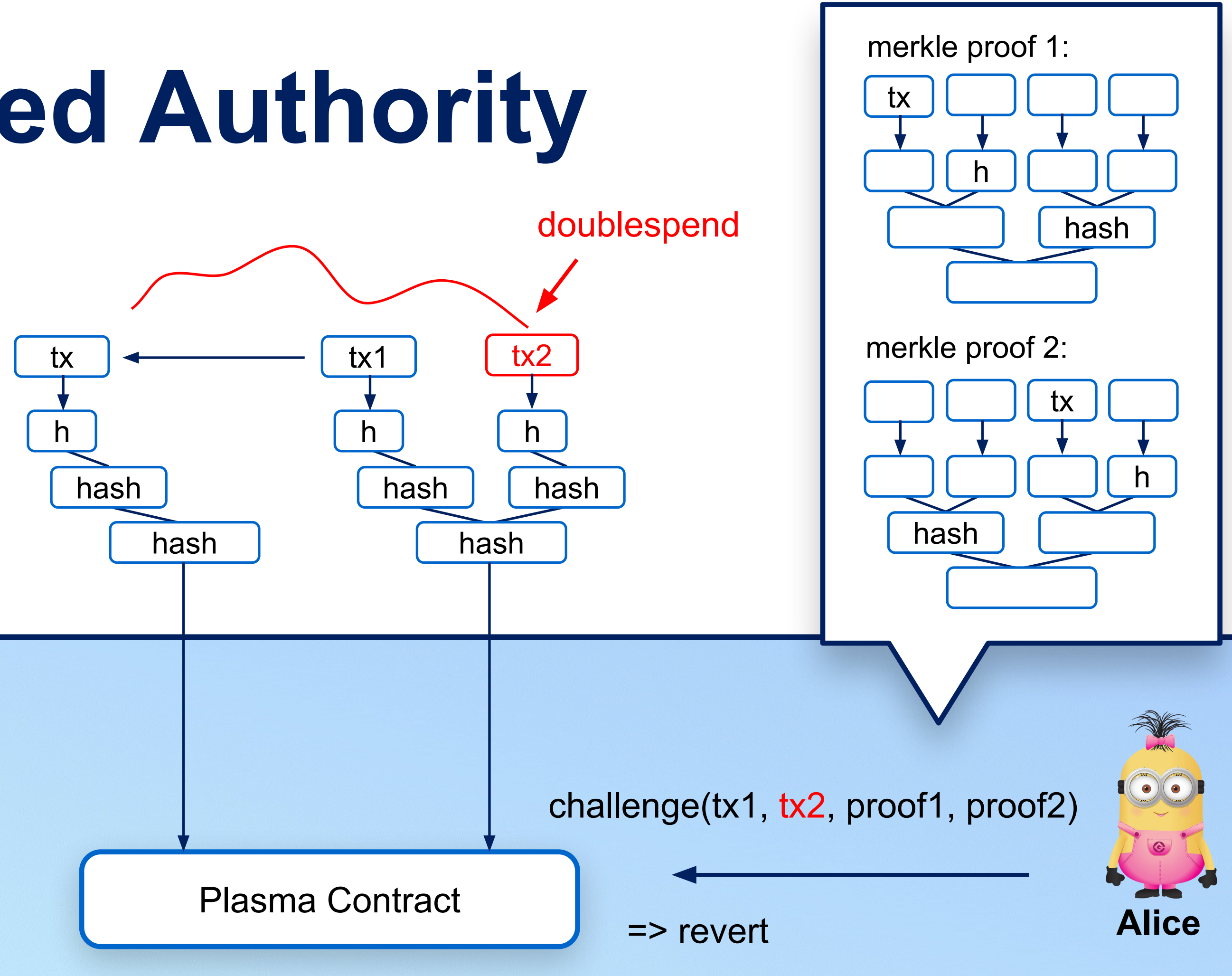
Ethereum Miner

Alice

Restricted Authority



Plasma Operator



doublespend

tx

tx1

tx2

h

h

h

hash

hash

hash

hash

hash

merkle proof 1:

tx

h

hash

merkle proof 2:

tx

h

hash

challenge(tx1, tx2, proof1, proof2)

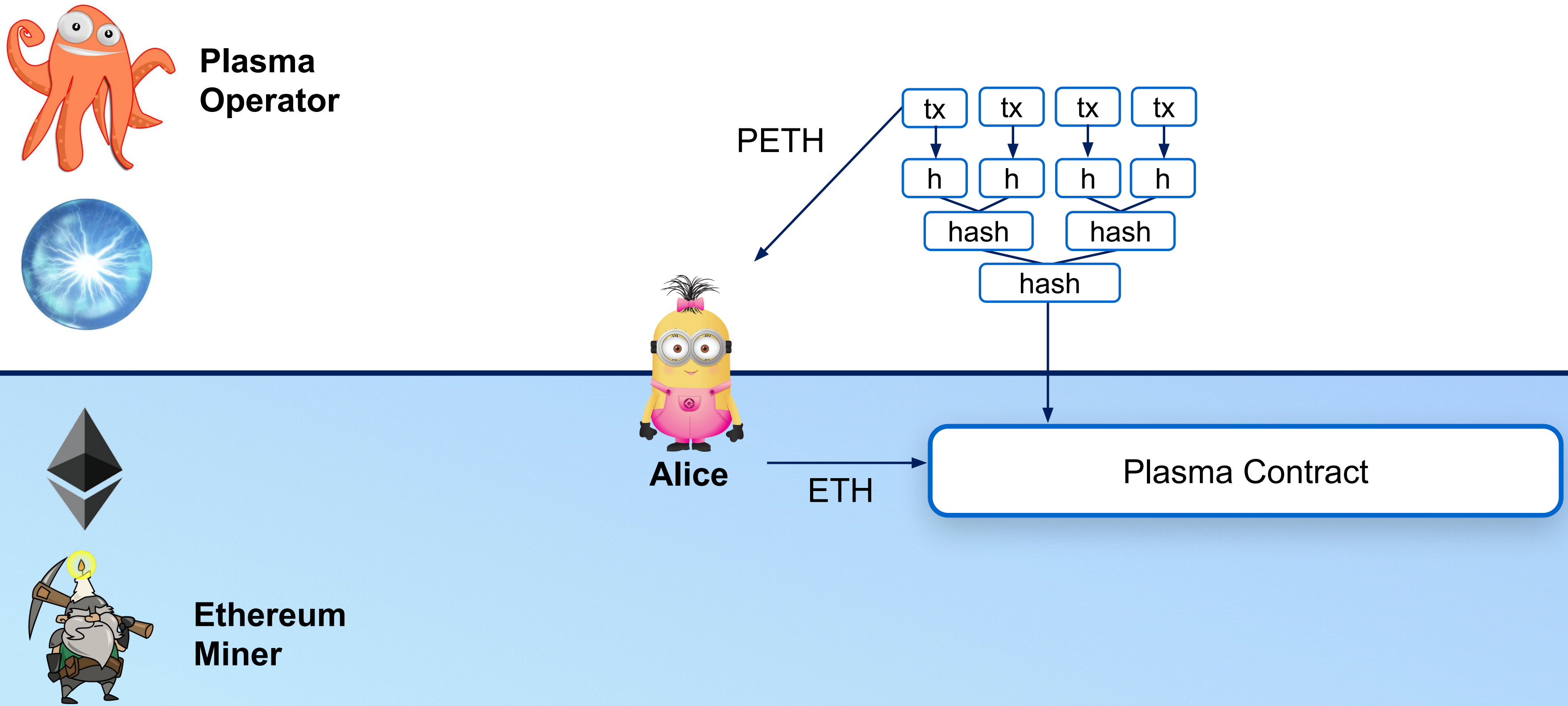
Plasma Contract

=> revert

Alice

Ethereum Miner

Plasma Deposit



Plasma Operator

PETH

tx tx tx tx

h h h h

hash hash

hash

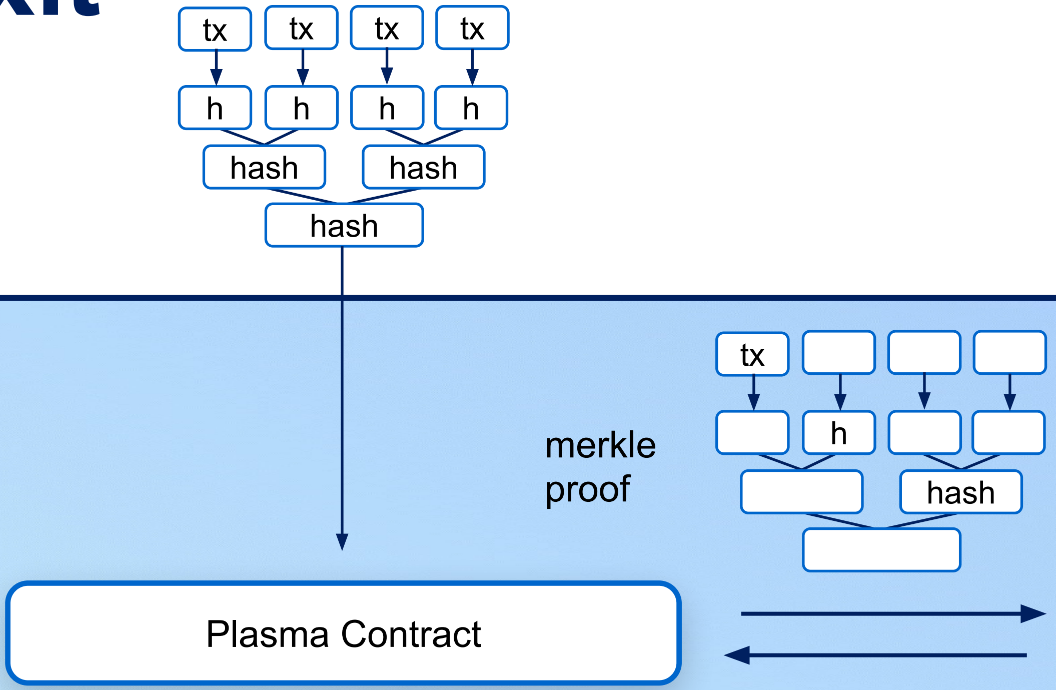
Alice

ETH

Plasma Contract

Ethereum Miner

Plasma Exit



tx tx tx tx

h h h h

hash hash

hash

merkle proof

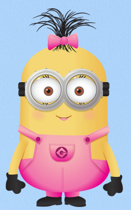
tx

h

hash

Plasma Contract

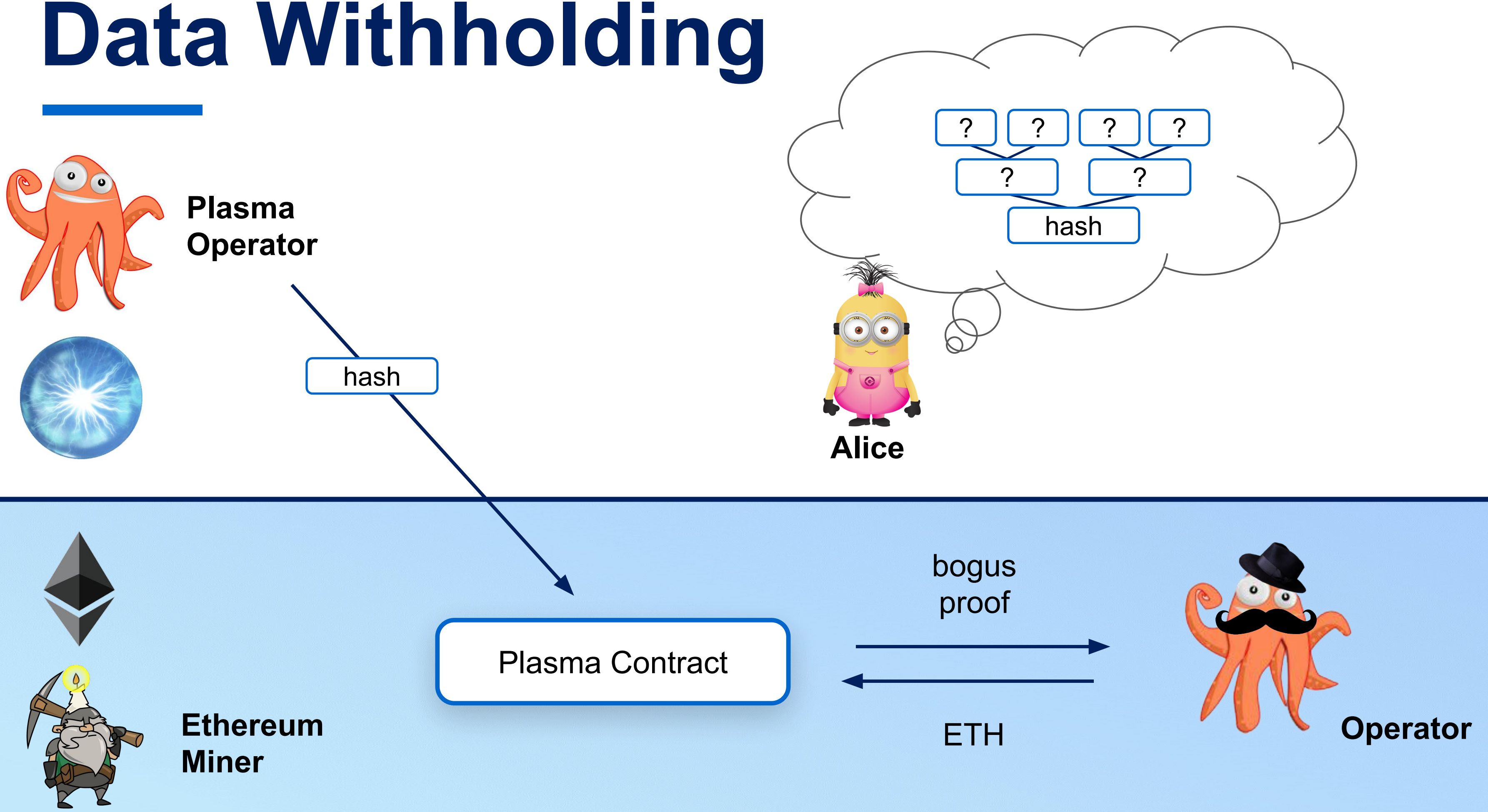
ETH



Alice

Ethereum Miner

Data Withholding



Plasma Operator

hash

? ? ? ?

? ?

hash

Alice

Plasma Contract

bogus proof

ETH

Operator

Ethereum Miner

Drawbacks of Plasma Classic

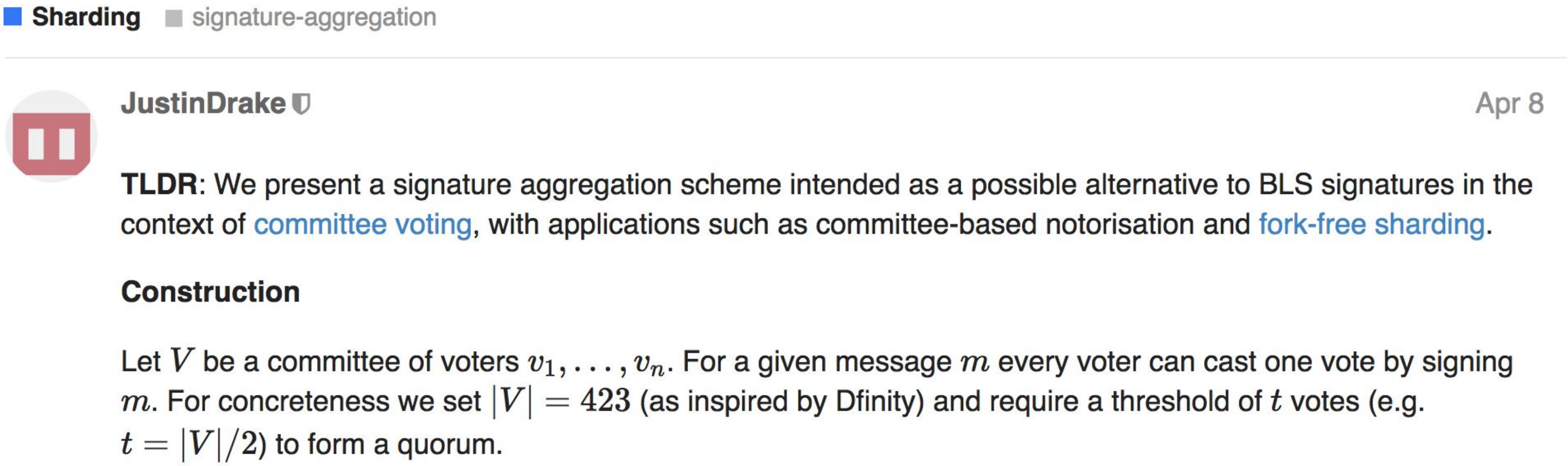
data availability problems

  => risk for fractional reserve

    => If operator becomes byzantine, everyone needs to exit

=> limited scalability: everyone needs to validate whole plasma chain

Cryptoeconomic Aggregate Signatures



■ **Sharding** ■ signature-aggregation

JustinDrake Apr 8

TLDR: We present a signature aggregation scheme intended as a possible alternative to BLS signatures in the context of committee voting, with applications such as committee-based notorisation and fork-free sharding.

Construction

Let V be a committee of voters $v_1, \dots, v_n$. For a given message m every voter can cast one vote by signing m. For concreteness we set $|V| = 423$ (as inspired by Dfinity) and require a threshold of t votes (e.g. $t = |V|/2$) to form a quorum.

https://ethresear.ch/t/cryptoeconomic-signature-aggregation/1659

Fraud Proof Challenge

1. review blocks - bit.ly/2uKHAJ6
2. submit 3 different fraud proofs
3. submit next block

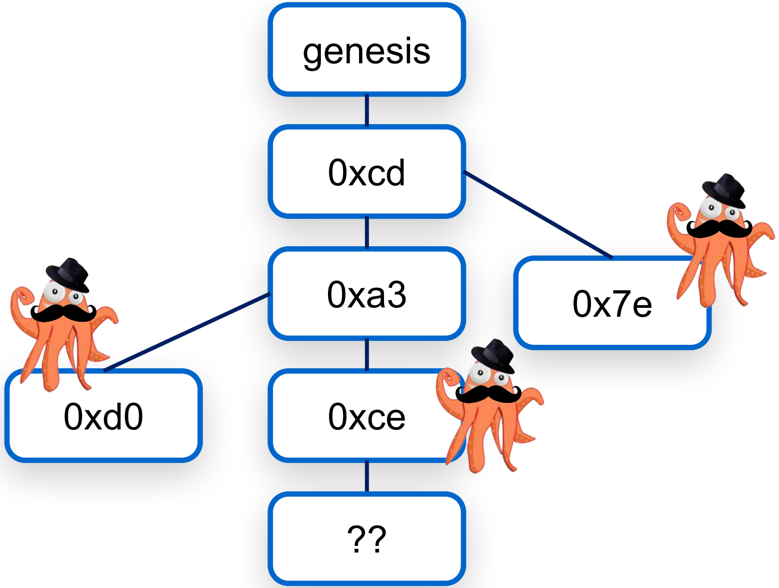
Hints:

0xe7 - double spend

0xd0 - signed 2 blocks at same height

0xce - double spend exit UTXO

?? - mine a block here



Rewards:

Mauveover ChainCat

Chestnut | Skyblue

Kitty #65222

Calicool Snagglepuss

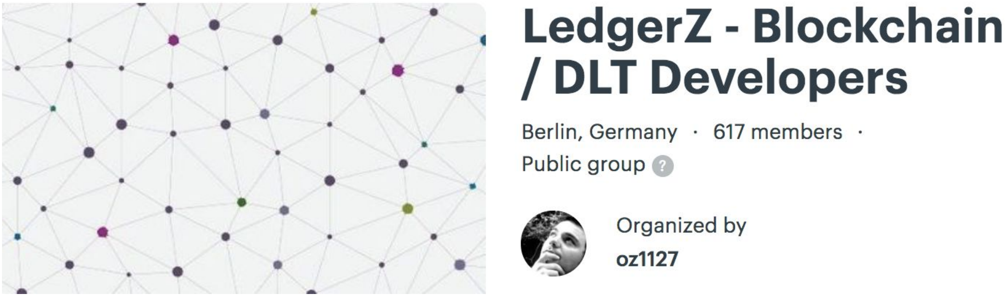
Instructions:

PARSEC LABS

Where can I use Plasma?

meetup

https://www.meetup.com/ledgerz/



LedgerZ - Blockchain / DLT Developers

Berlin, Germany · 617 members ·

Public group ?

Organized by

oz1127

PARSEC LABS

omisego

MATIC Matic Network

BANKEX

Thank You :)

parseclabs.org

parseclabs.org/blog/

t.me/parseclabs

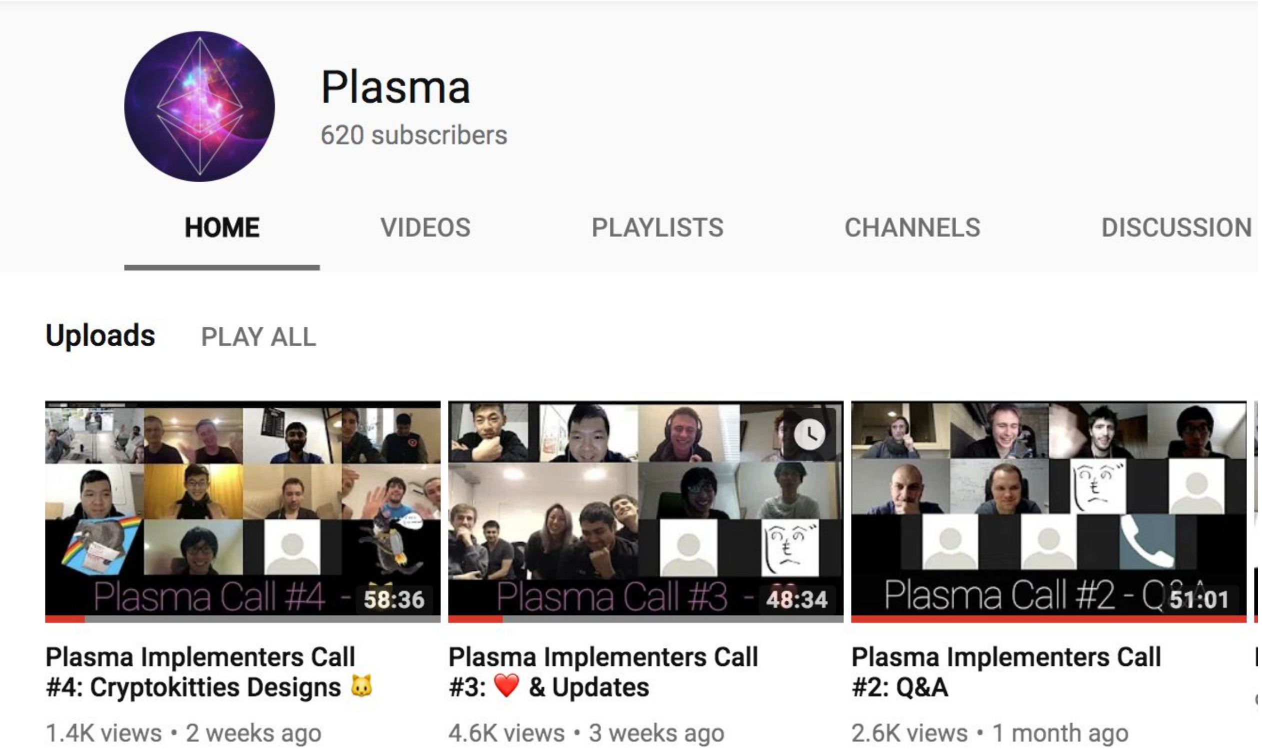
facebook.com/parsecIabs/

twitter.com/parsec_labs

github.com/parsec-labs

Backup

How can I contribute to Plasma Development?



Plasma

620 subscribers

Uploads

Plasma Implementers Call #4: Cryptokitties Designs 🐱

1.4K views • 2 weeks ago

Plasma Implementers Call #3: ❤️ & Updates

4.6K views • 3 weeks ago

Plasma Implementers Call #2: Q&A

2.6K views • 1 month ago

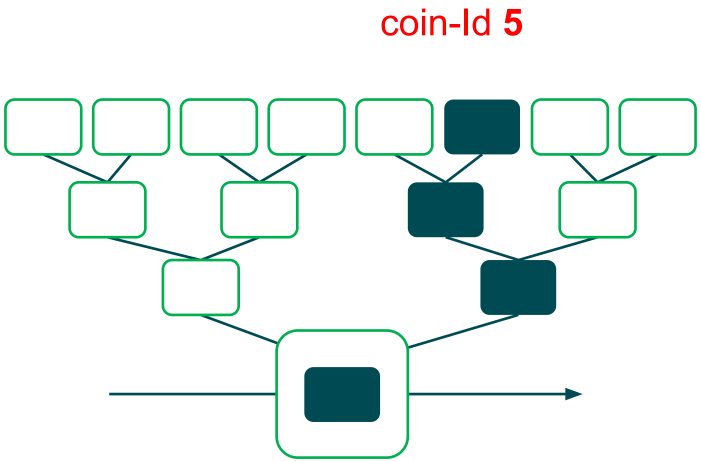
PLASMA CASH

A Layer-2 Scaling Solution ++

Johann Barbie

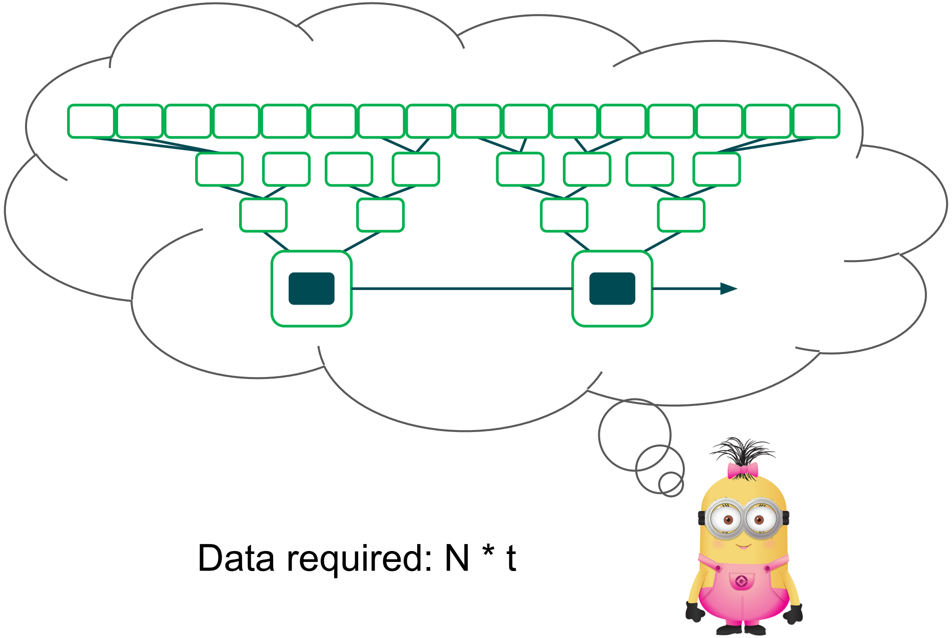
parseclabs.org

What is Plasma Cash?



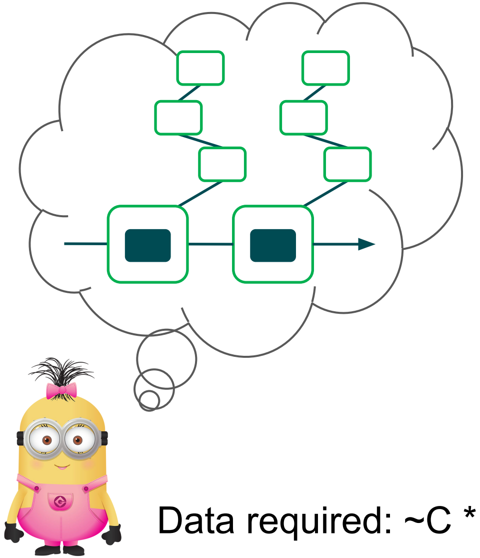
- plasma Cash is Plasma, but even more scalable
- each deposit creates a “coin” with Id
- coins can not be split and can not be merged
- Transactions spending coin must be included at position in merkle tree corresponding to Id.
- Only coins that have been deposited can be withdrawn

What is Plasma Cash?



Data required: N * t

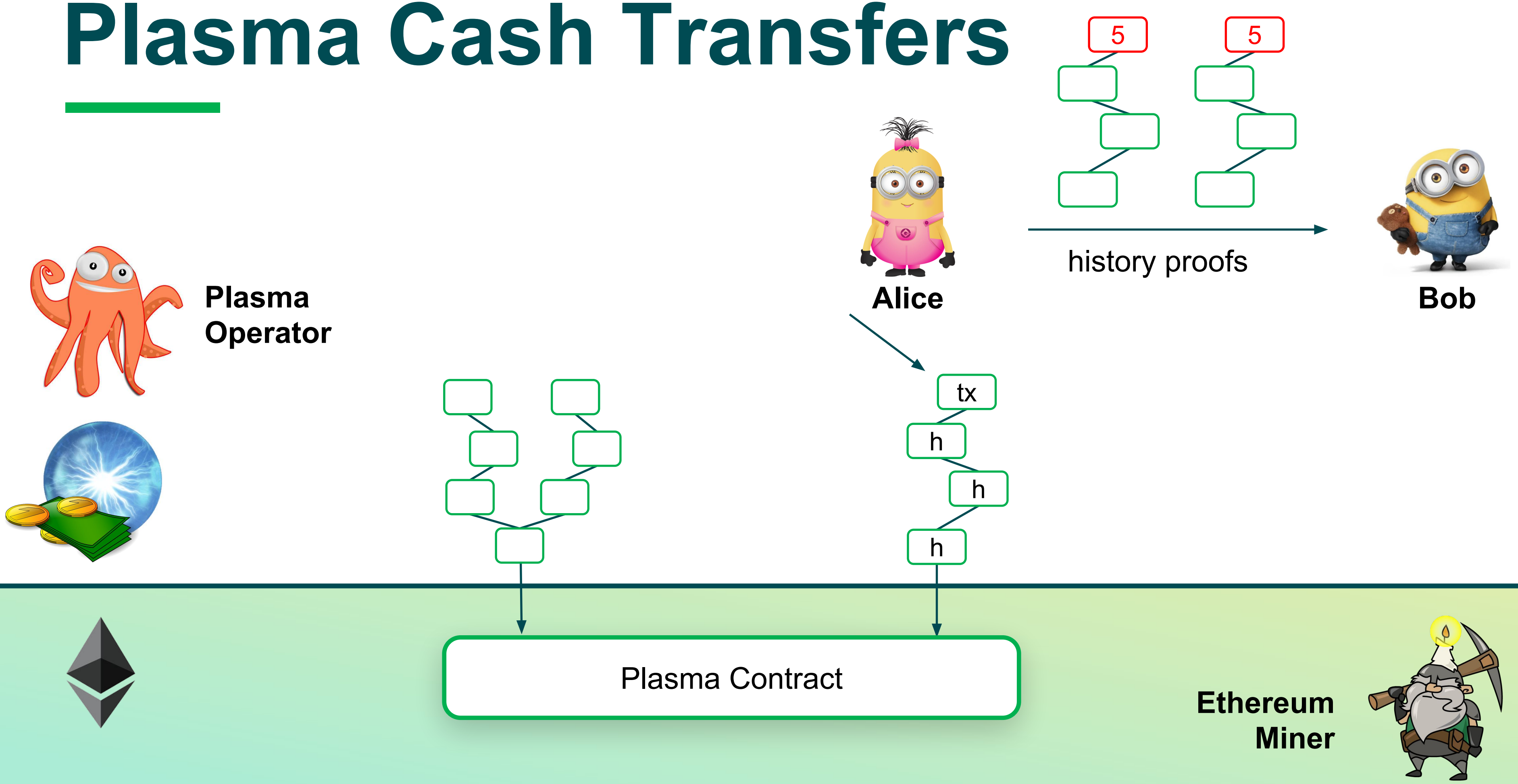
Plasma Classic



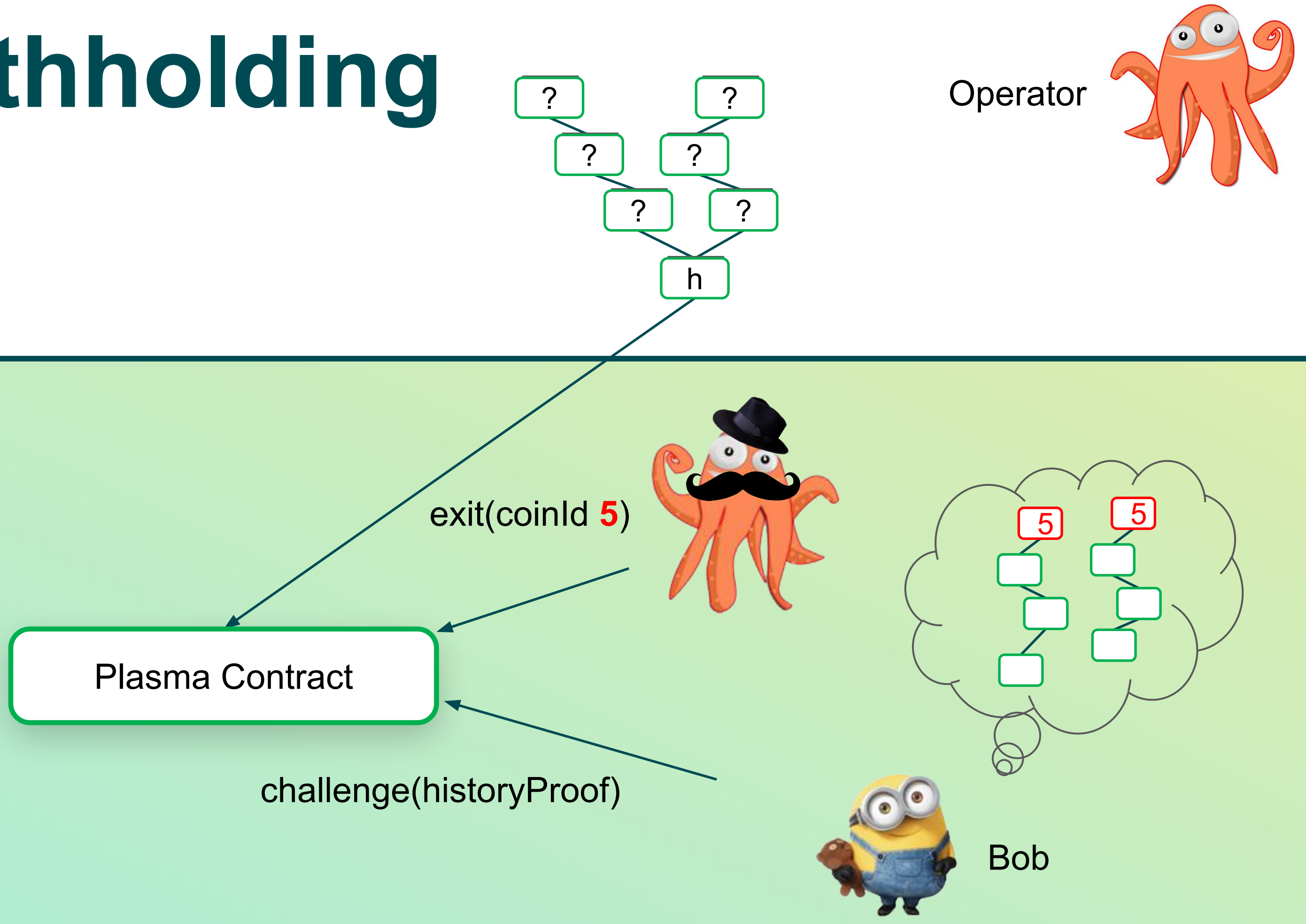
Data required: ~C * t * log(n/c)

Plasma Cash

Plasma Cash Transfers



Data Withholding



Operator

exit(coinId **5**)

Plasma Contract

challenge(historyProof)

Bob

Plasma Cash

- only coin Ids that have been deposited can be withdrawn
- any attempt to steal a coin has a specific victim
- operator can’t inflate and steal from “everyone”

  => fractional reserve impossible

=> more hack resistant

=> exponentially scalable

Plasma Cash

- only coin Ids that have been deposited can be withdrawn
- any attempt to steal a coin has a specific victim
- operator can’t inflate and steal from “everyone”

  => fractional reserve impossible

=> more hack resistant

=> exponentially scalable

Sidechain Security

security by economic incentives

=> new chains have low cost of attack

Plasma vs. Sidechains

MUCH WOW !!

SO PLASMA!!