

PLASMA

Johann Barbie



parseclabs.org

Agenda

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







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?



Plasma
Operator

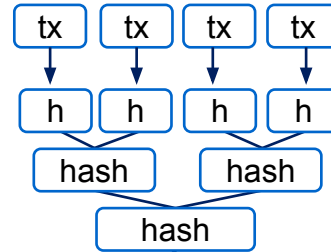
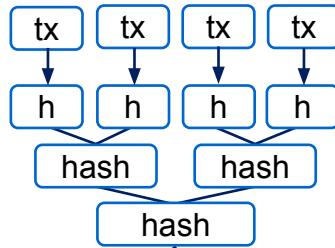


Alice

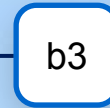
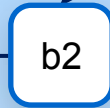
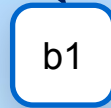
many transactions



Bob



compaction in
merkle tree



Ethereum
Miner

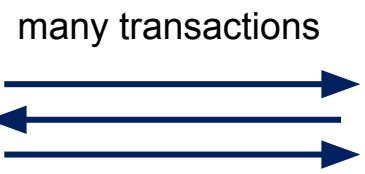




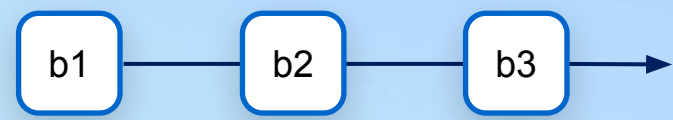
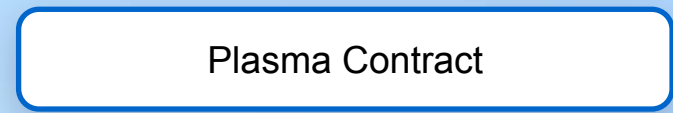
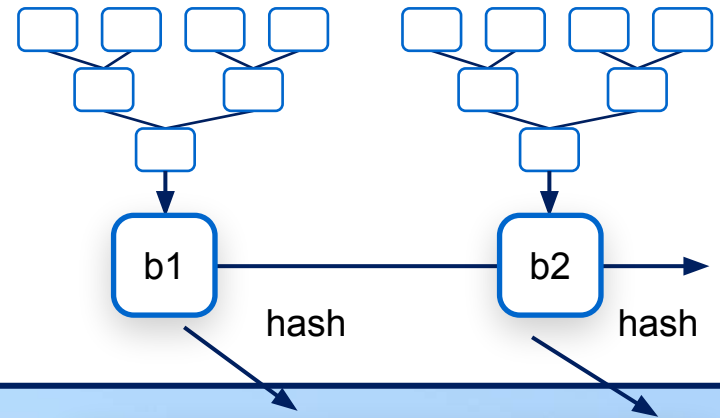
**Plasma
Operator**



Alice



Bob



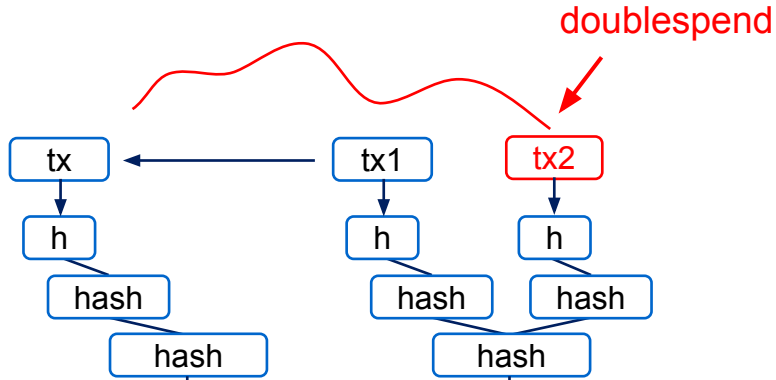
**Ethereum
Miner**



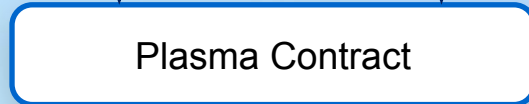
Restricted Authority



Plasma
Operator



Ethereum
Miner



challenge(tx1, tx2, proof1, proof2)

=> revert



Alice

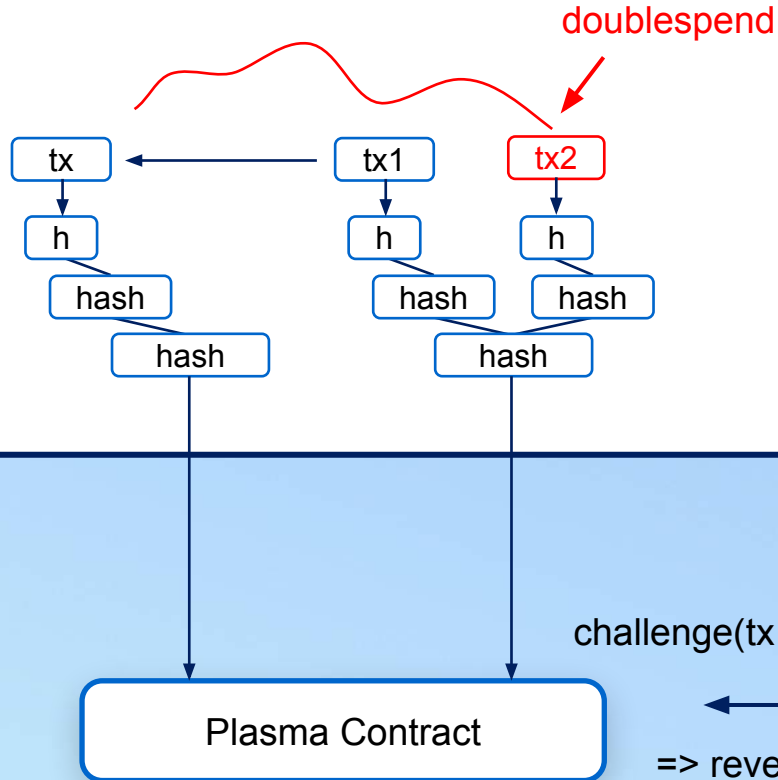
Restricted Authority



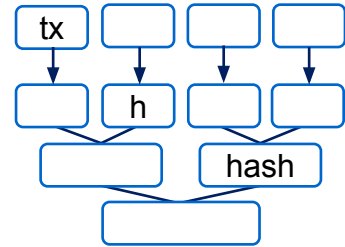
Plasma
Operator



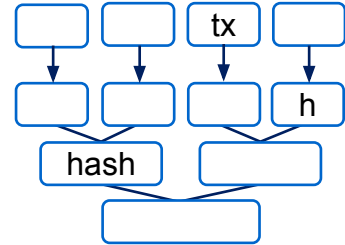
Ethereum
Miner



merkle proof 1:



merkle proof 2:



Alice

Plasma Deposit



Plasma
Operator

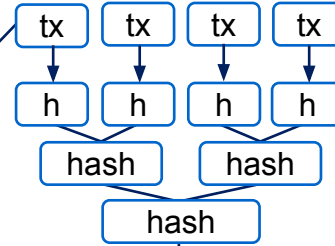


Ethereum
Miner



Alice

PETH



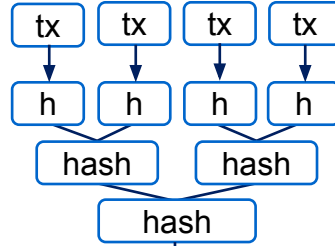
ETH

Plasma Contract

Plasma Exit

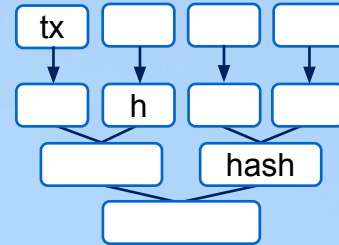


Ethereum
Miner



Plasma Contract

merkle
proof



ETH



Alice

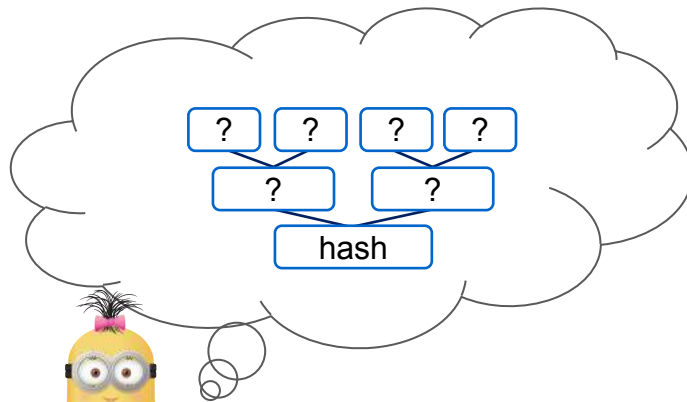
Data Withholding



Plasma
Operator



hash



Alice



Ethereum
Miner

Plasma Contract

bogus
proof

ETH



Operator

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



PLASMA CASH

A Layer-2 Scaling Solution ++

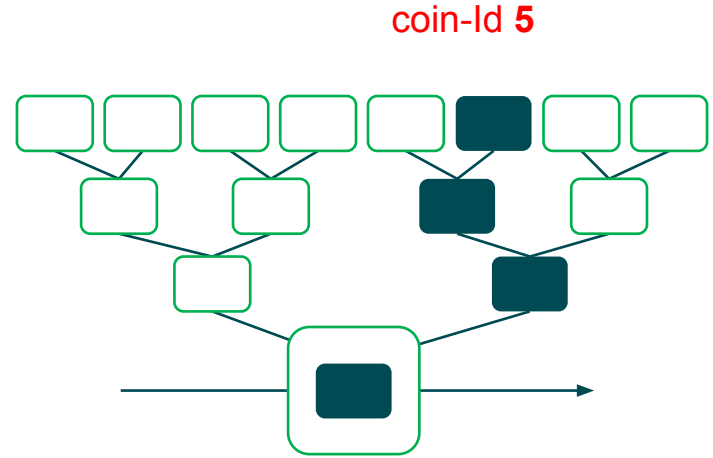
Johann Barbie



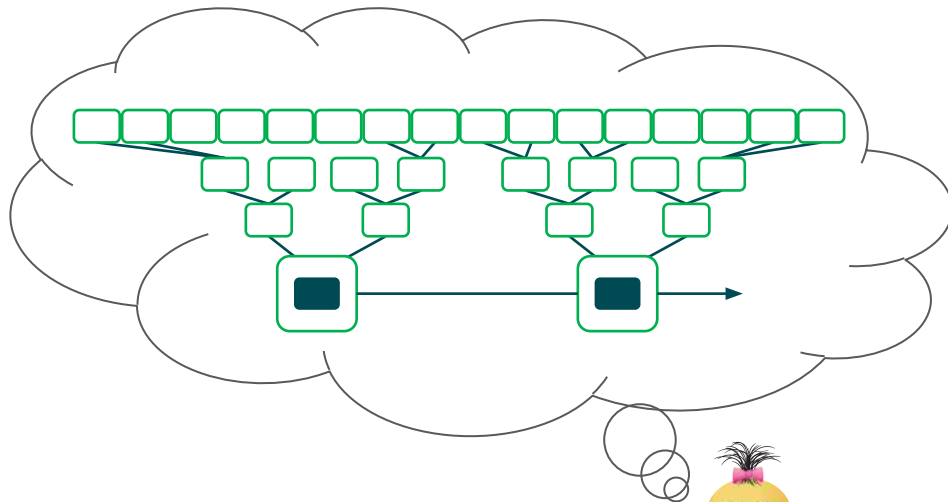
parseclabs.org

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



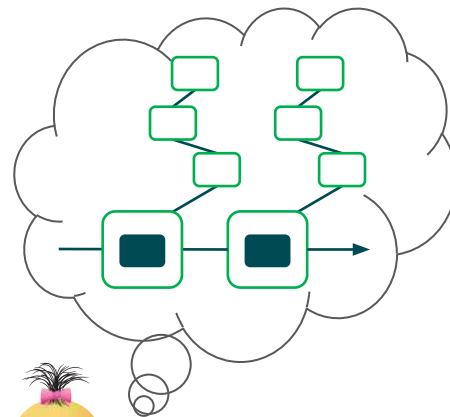
What is Plasma Cash?



Data required: $N * t$



Plasma Classic



Data required: $\sim C * t * \log(n/c)$



Plasma Cash

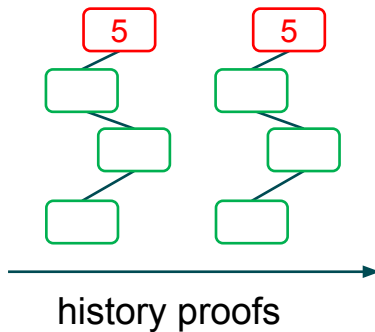
Plasma Cash Transfers



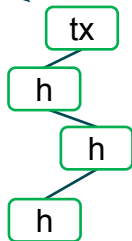
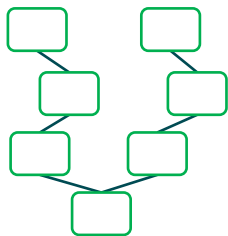
Plasma
Operator



Alice



Bob



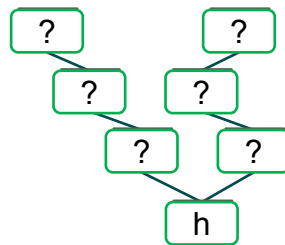
Plasma Contract

Ethereum
Miner



Data Withholding

Operator

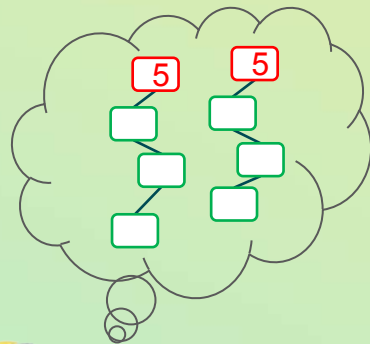


exit(coinId 5)



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



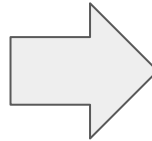
security by economic incentives

=> new chains have low cost of attack

Plasma vs. Sidechains

MUCH WOW !!

SO PLASMA!!



Fraud Proof Challenge

1. review blocks - bit.ly/2vdHM6U
2. submit 3 different fraud proofs
3. mine next block

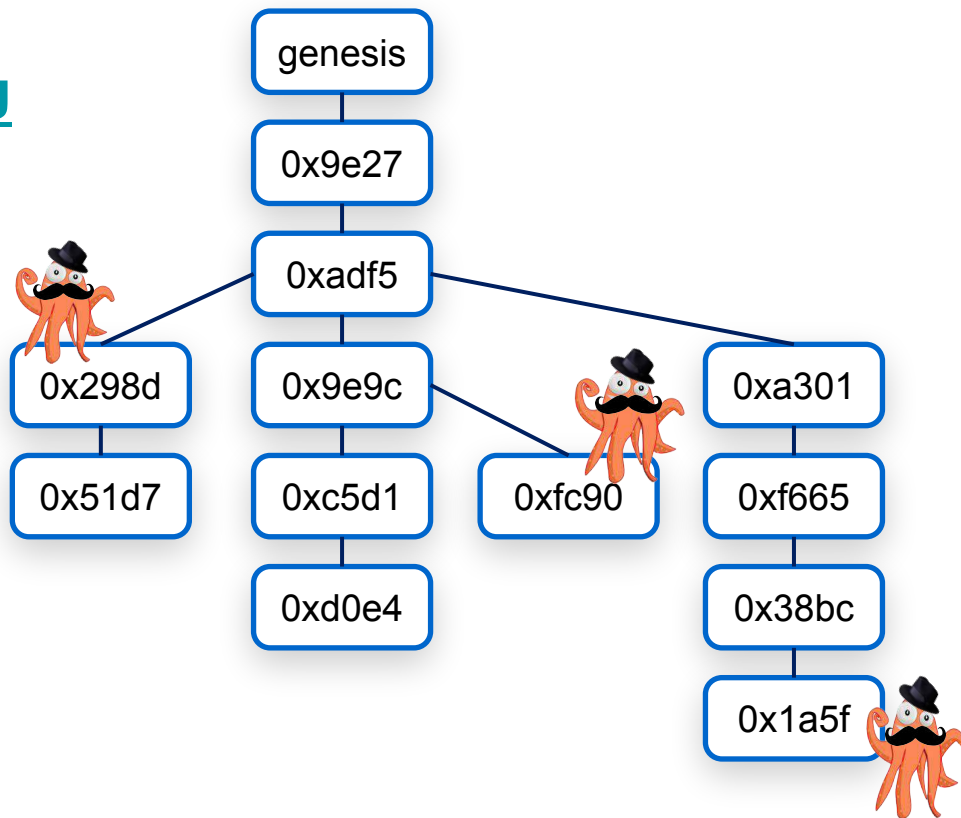
Hints:

0x298d - invalid deposit

0xfc90 - double spend

0x1a5f - light tip

0xd0e4 - heavy tip



Rewards:



[Instructions:](#)



PARSECLABS

Where can I use Plasma?



parseclabs.org



t.me/parseclabs



contact@parseclabs.org



twitter.com/Parsec_Labs



PARSEC LABS

omisego




Voltaire Labs



BANKEX

Backup

How can I contribute to Plasma Development?



Plasma

620 subscribers

HOMEVIDEOSPLAYLISTSCHANNELSDISCUSSION

Uploads PLAY ALL



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