

# PLASMA

Johann Barbie



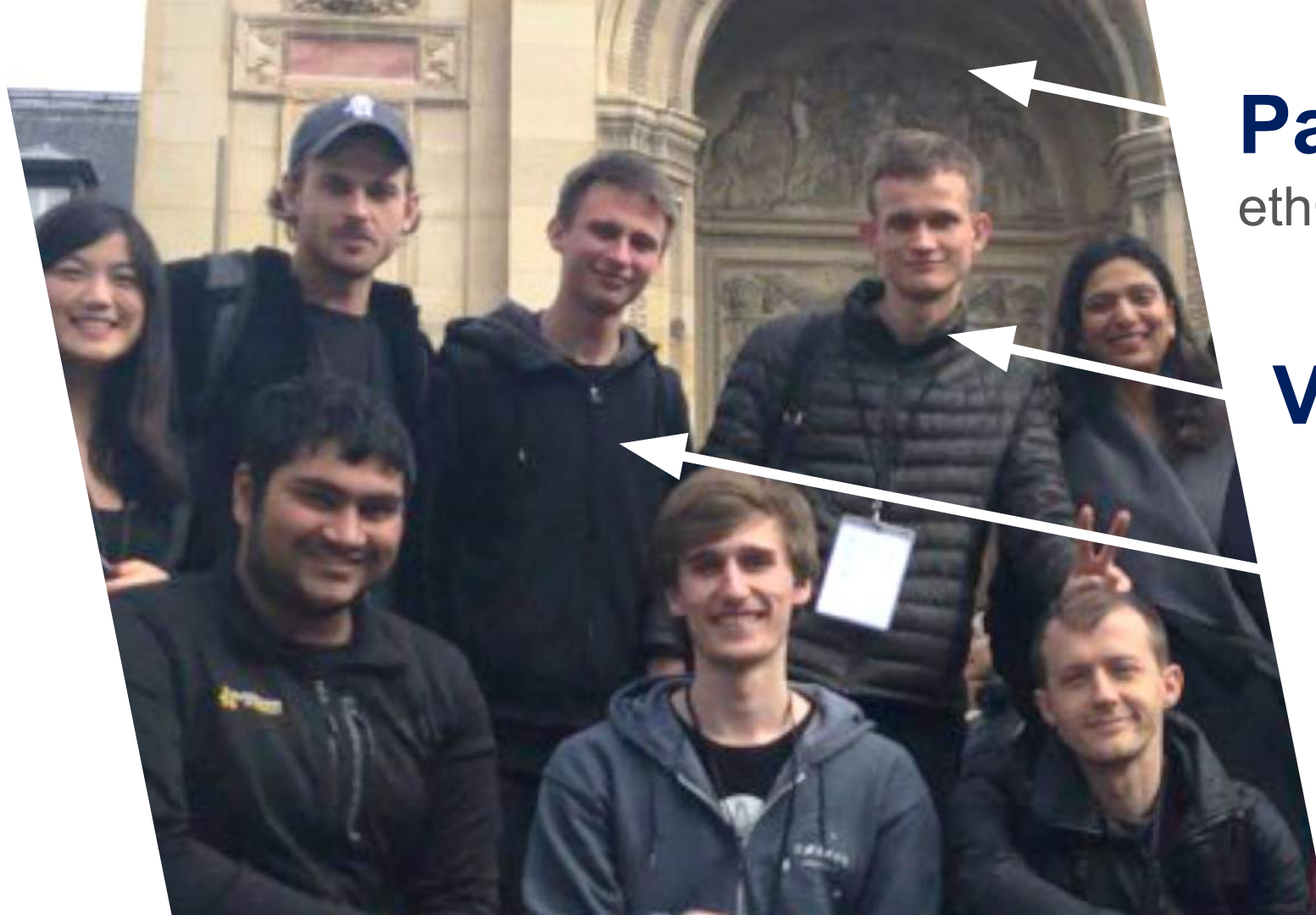
[parseclabs.org](https://parseclabs.org)

# Agenda

1. Plasma Classic
2. CAS
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

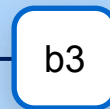
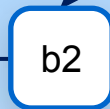
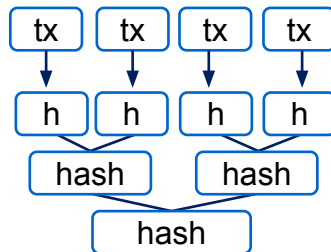
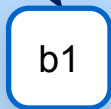
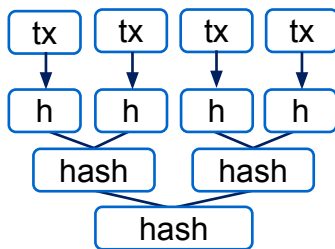


Alice

many transactions



Bob



compaction in  
merkle tree



Ethereum  
Miner

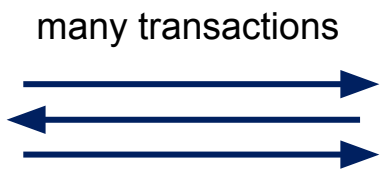




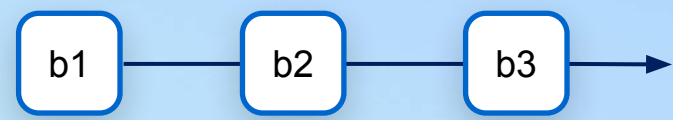
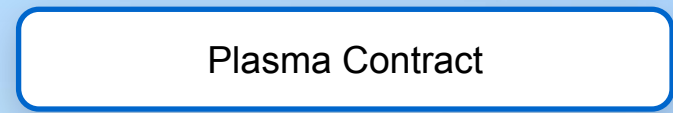
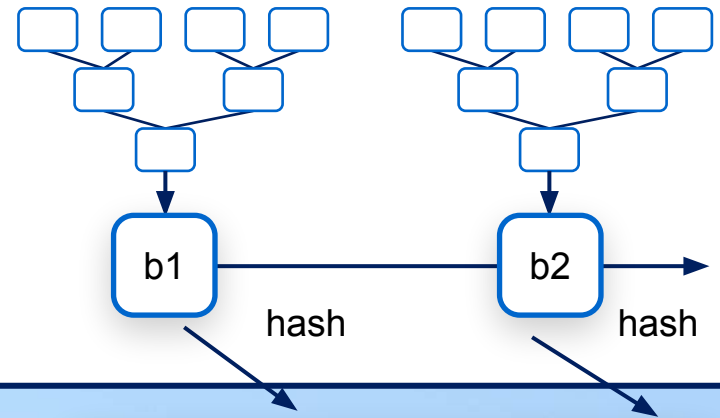
**Plasma Operator**



**Alice**



**Bob**



**Ethereum Miner**

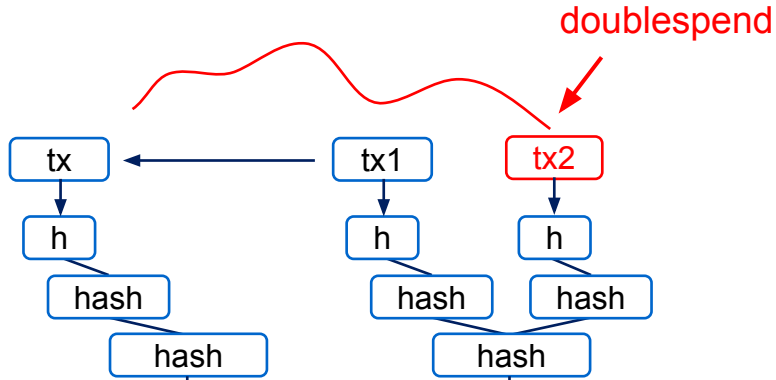




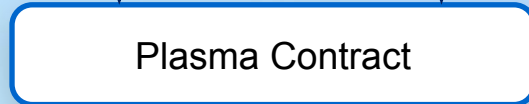
# Restricted Authority



Plasma  
Operator



Ethereum  
Miner



challenge(tx1, tx2, proof1, proof2)

=> revert



Alice

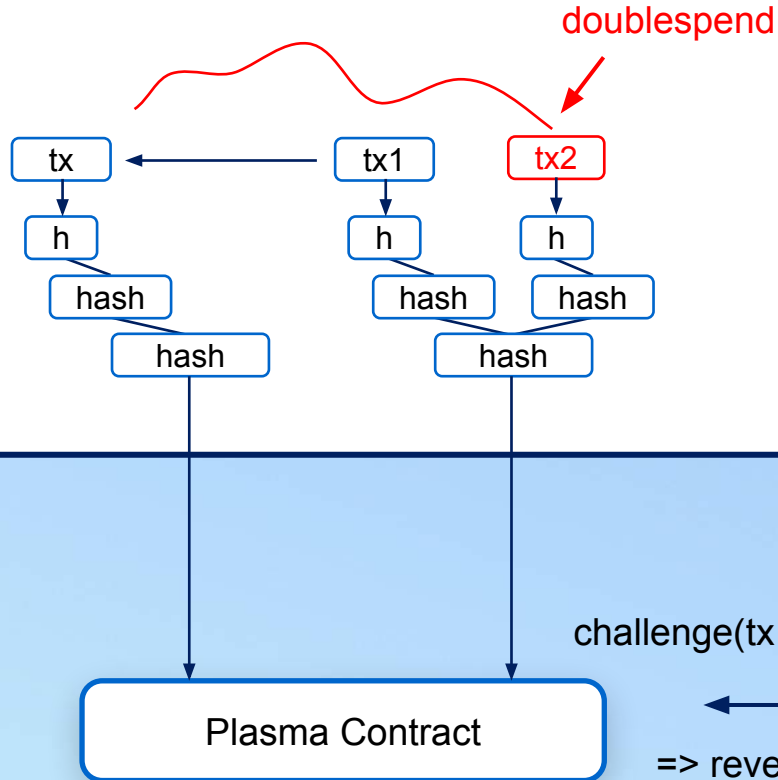
# Restricted Authority



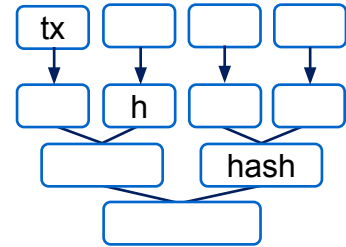
Plasma  
Operator



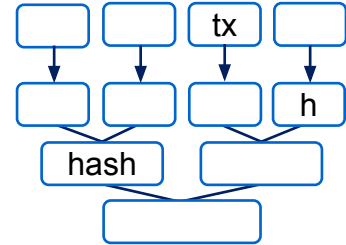
Ethereum  
Miner



merkle proof 1:



merkle proof 2:



Alice

# Plasma Deposit



Plasma  
Operator

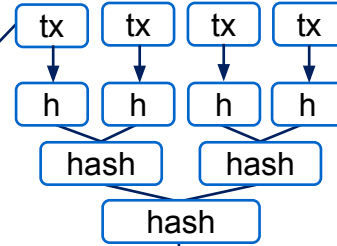


Ethereum  
Miner



Alice

PETH



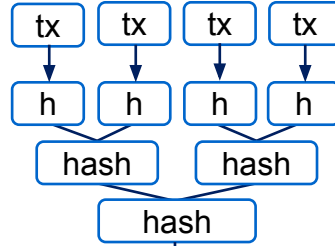
ETH

Plasma Contract

# Plasma Exit

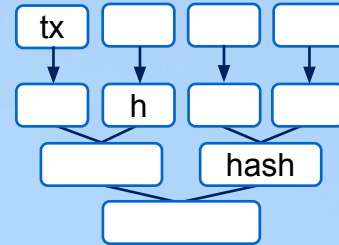


Ethereum  
Miner



Plasma Contract

merkle  
proof



ETH



Alice

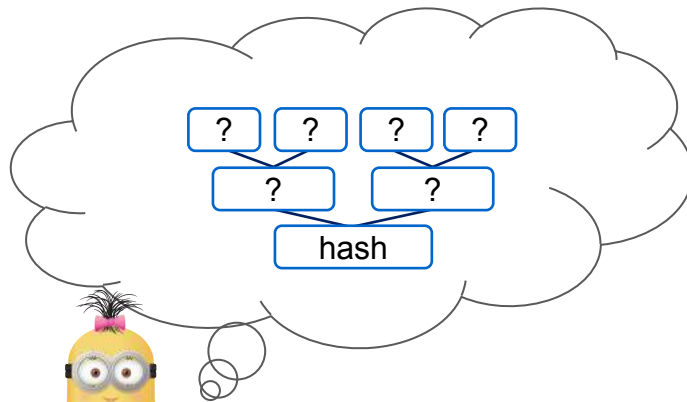
# Data Withholding



**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



# Fraud Proof Challenge

---

1. review blocks - [bit.ly/2MwsDIE](https://bit.ly/2MwsDIE)
2. submit 3 different fraud proofs
3. submit next block

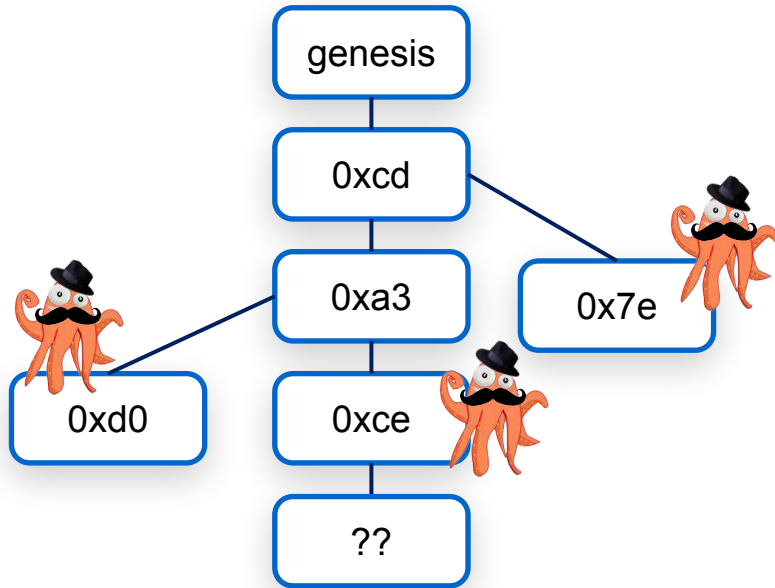
Hints:

**0xe7** - double spend

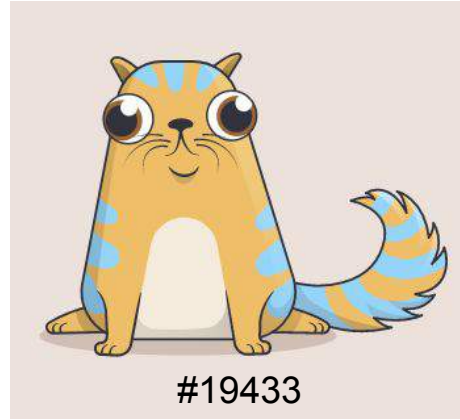
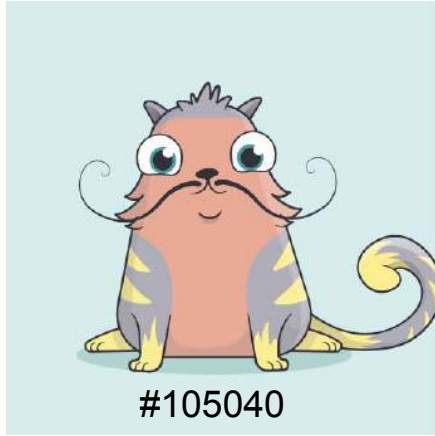
**0xce** - double spend exit UTXO

**0xd0** - signed 2 blocks at same height

**??** - mine a block here



# Rewards:



[bit.ly/2MwsDIE](https://bit.ly/2MwsDIE) :



**PARSECLABS**

# 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](#).

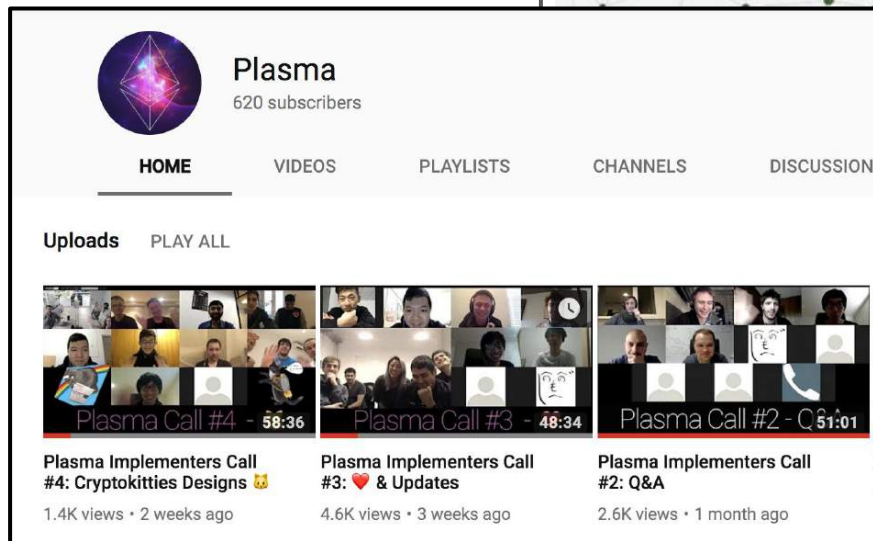
## Construction

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.

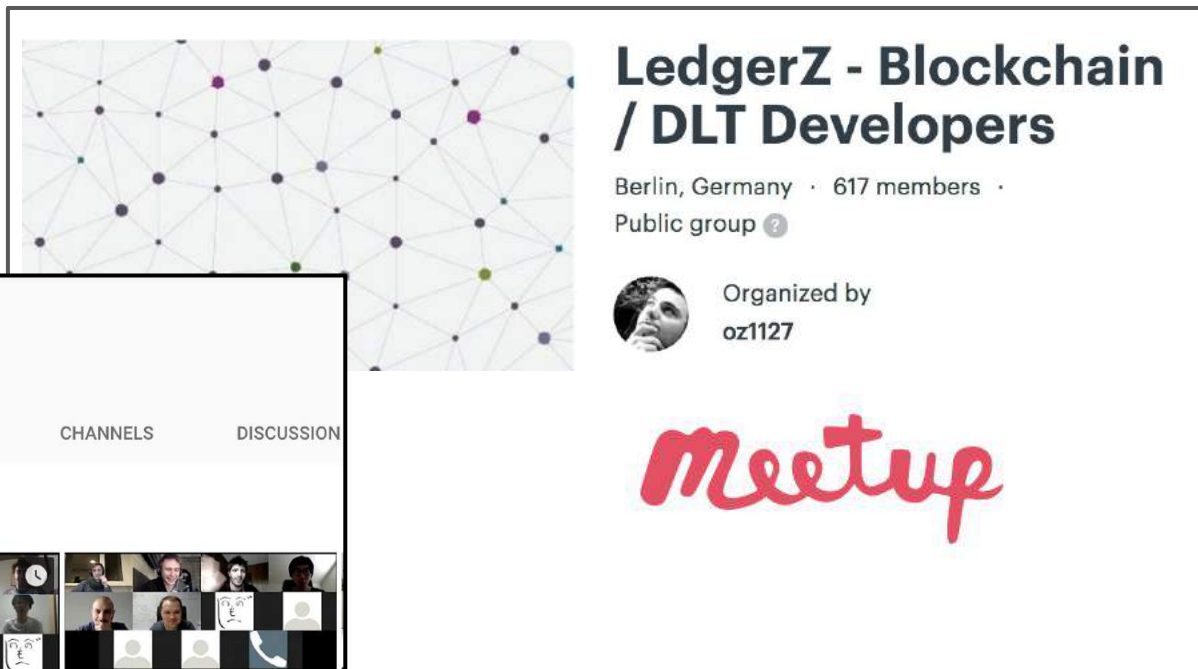
<https://ethresear.ch/t/cryptoeconomic-signature-aggregation/1659>

# Where can I learn about Plasma?

[y2u.be/w45PXH0DJa0](https://y2u.be/w45PXH0DJa0)



The image shows a YouTube channel page for 'Plasma'. At the top is the channel's profile picture, a purple and blue geometric shape, and the name 'Plasma' with '620 subscribers'. Below this are navigation tabs: 'HOME' (selected), 'VIDEOS', 'PLAYLISTS', 'CHANNELS', and 'DISCUSSION'. Under the 'Uploads' section, there are three video thumbnails. Each thumbnail shows a grid of people in a video call. The first video is 'Plasma Call #4 - 58:36' with the title 'Plasma Implementers Call #4: Cryptokitties Designs' and '1.4K views • 2 weeks ago'. The second video is 'Plasma Call #3 - 48:34' with the title 'Plasma Implementers Call #3: ❤️ & Updates' and '4.6K views • 3 weeks ago'. The third video is 'Plasma Call #2 - 05:01' with the title 'Plasma Implementers Call #2: Q&A' and '2.6K views • 1 month ago'.



The image shows a Meetup page for 'LedgerZ - Blockchain / DLT Developers'. The header features a background image of a network graph. The title 'LedgerZ - Blockchain / DLT Developers' is in large, bold, black text. Below the title, it says 'Berlin, Germany · 617 members · Public group'. To the right, it says 'Organized by oz1127' next to a small profile picture. At the bottom of the page is the red 'Meetup' logo.

[www.meetup.com/ledgerz/](https://www.meetup.com/ledgerz/)

# Where can I use Plasma?

[alice.parseclabs.org](https://alice.parseclabs.org)



**PARSEC** LABS



**Matic Network**

**omise**go



**BANKEX**

# Thank You :)



[parseclabs.org](https://parseclabs.org)



[parseclabs.org/blog/](https://parseclabs.org/blog/)



[t.me/parseclabs](https://t.me/parseclabs)



[facebook.com/parseclabs/](https://facebook.com/parseclabs/)



[twitter.com/parseclabs](https://twitter.com/parseclabs)



[github.com/parseclabs](https://github.com/parseclabs)






# Backup

# How can I contribute to Plasma Development?

---




## Plasma

620 subscribers

HOMEVIDEOSPLAYLISTSCHANNELSDISCUSSION

Uploads


PLAY ALL



Plasma Call #4 - 58:36

Plasma Implementers Call #4: Cryptokitties Designs 🐱


1.4K views • 2 weeks ago



Plasma Call #3 - 48:34

Plasma Implementers Call #3: ❤️ & Updates

4.6K views • 3 weeks ago



Plasma Call #2 - Q&A 51:01

Plasma Implementers Call #2: Q&A

2.6K views • 1 month ago



# PLASMA CASH

A Layer-2 Scaling Solution ++

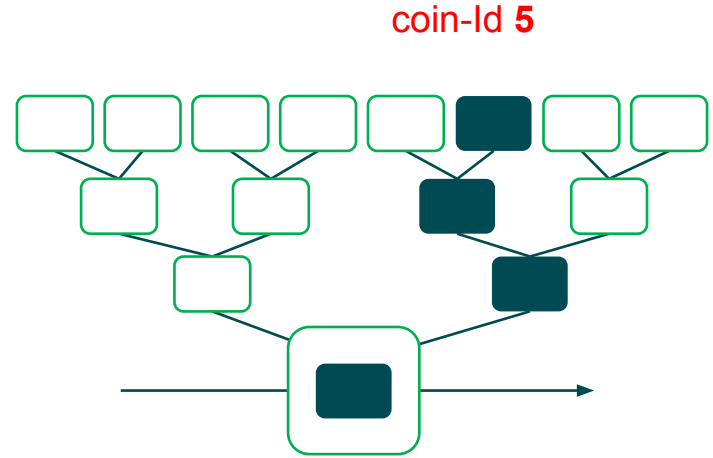
Johann Barbie



[parseclabs.org](https://parseclabs.org)

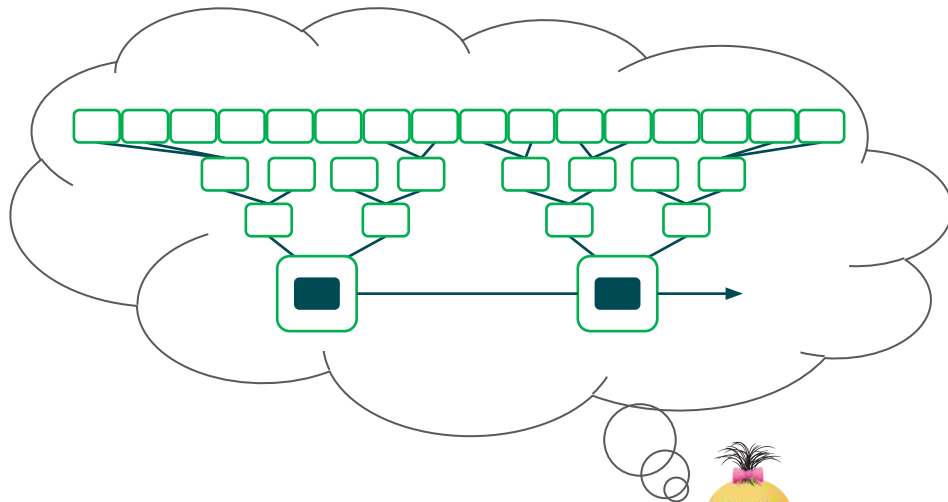
# What is Plasma Cash?

- 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



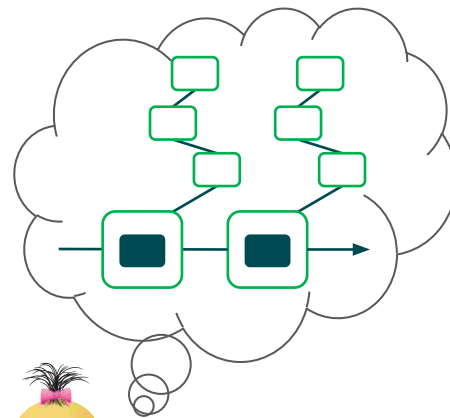
# What is Plasma Cash?

---



Data required:  $N * t$

**Plasma Classic**



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

**Plasma Cash**

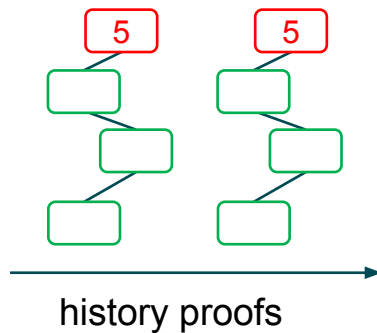
# Plasma Cash Transfers



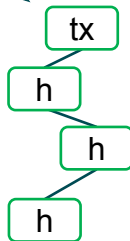
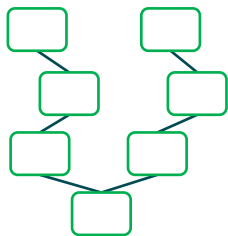
Plasma  
Operator



Alice



Bob



Plasma Contract

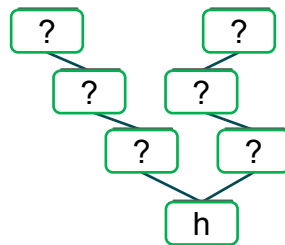
Ethereum  
Miner





# Data Withholding

Operator

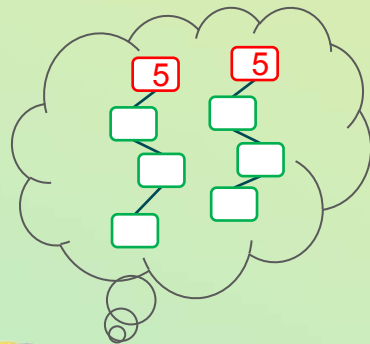


exit(coinId 5)



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!!

