Everything you wanted to know about Plasma but were afraid to ask

Georgios Konstantopoulos
Independent Consultant & Software Engineer
@gakonst / me@gakonst.com

Slides available: gakonst.com/ethereal2019.pdf

<insert motivation for scalable public blockchains>

Layer 1 vs Layer 2

OK, how do we scale?

On-chain, **“Layer 1” (L1)**: Global

- Database tricks (sharding)
- Faster consensus (Casper FFG, Snowball)
- Better VMs (WASM)
- Stateless smart contracts
- Block propagation (FIBER/bloXroute)
- Cryptography instead of onchain components (multisig with threshold sigs)

OK, how do we scale?

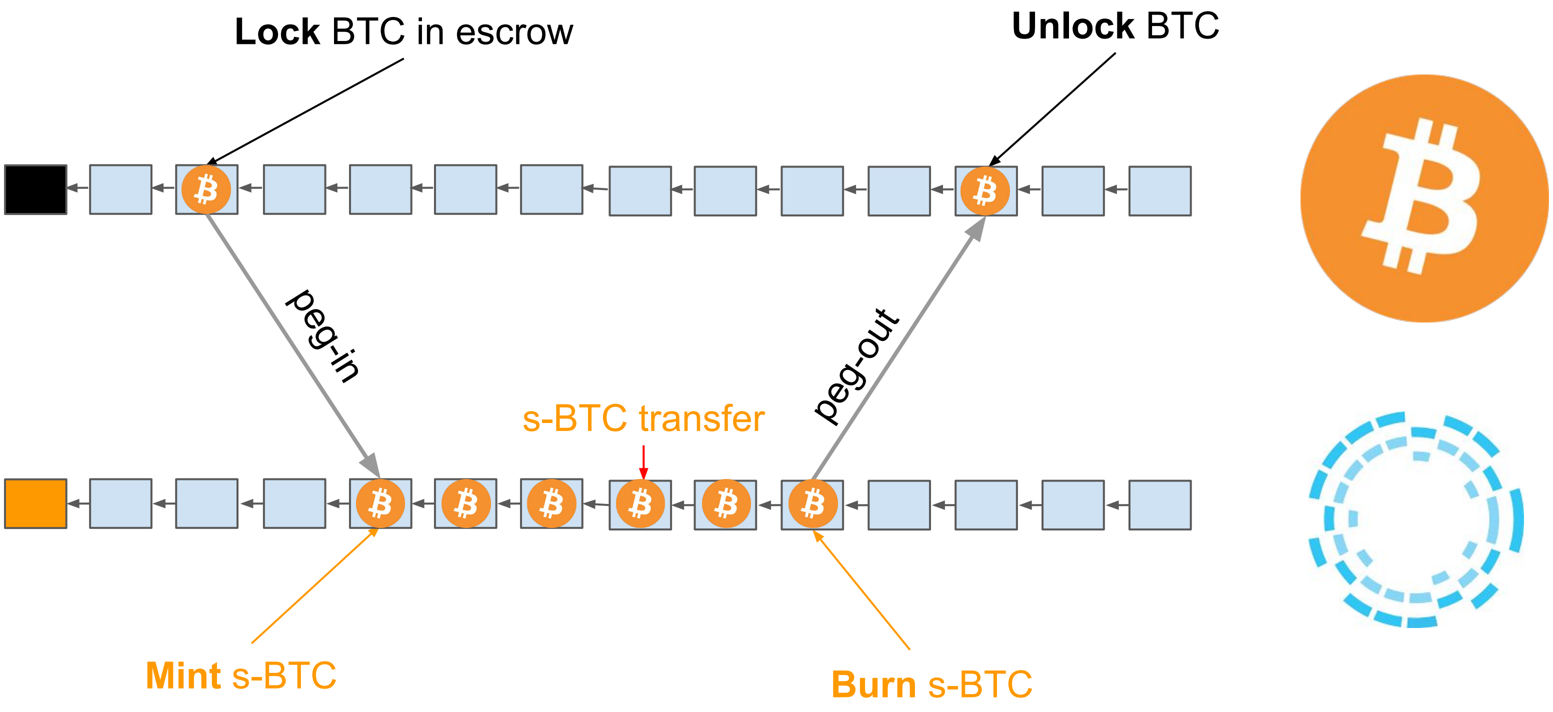
On-chain, **“Layer 1” (L1)**: Global

- Database tricks (sharding)
- Faster consensus (Casper FFG, Snowball)
- Better VMs (WASM)
- Stateless smart contracts
- Block propagation (FIBER/bloXroute)
- Cryptography instead of onchain components (multisig with threshold sigs)

Off-chain, **“Layer 2” (L2)**: Local

- **Plasma**
- Payment/State Channels
- ~~Sidechains (are you sure?)~~

Sidechains considered harmful



Lock BTC in escrow

Unlock BTC

peg-in

peg-out

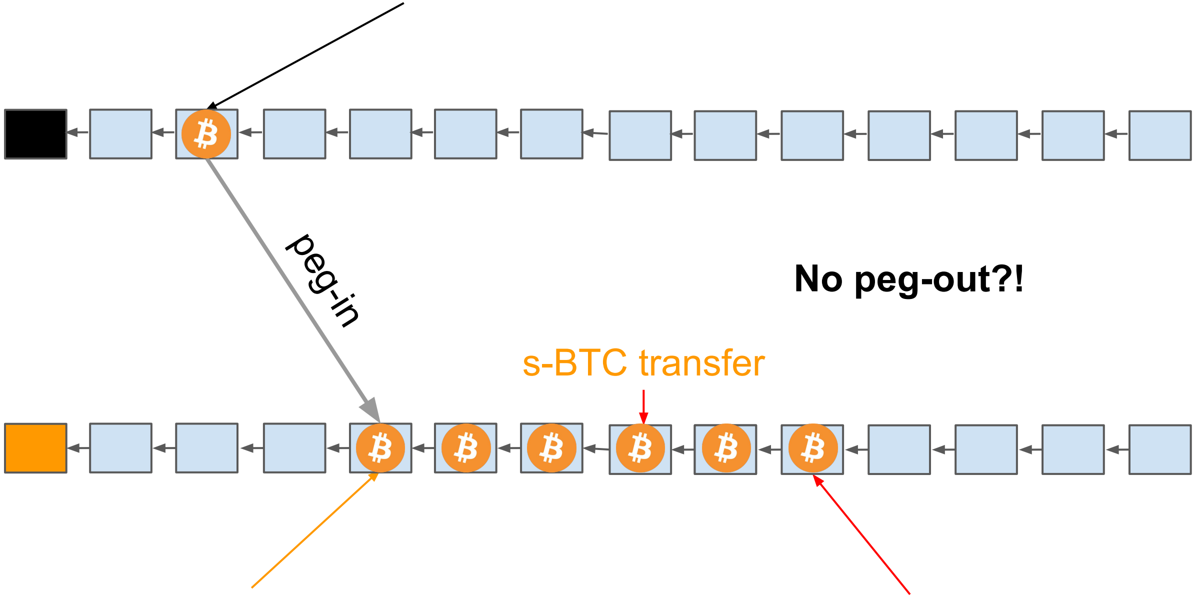
s-BTC transfer

Mint s-BTC

Burn s-BTC

**federated pegs use multisig wallets for peg-in & peg-out*

Sidechains considered harmful



Lock BTC in escrow

peg-in

No peg-out?!

s-BTC transfer

Mint s-BTC

Burn s-BTC transaction gets censored!

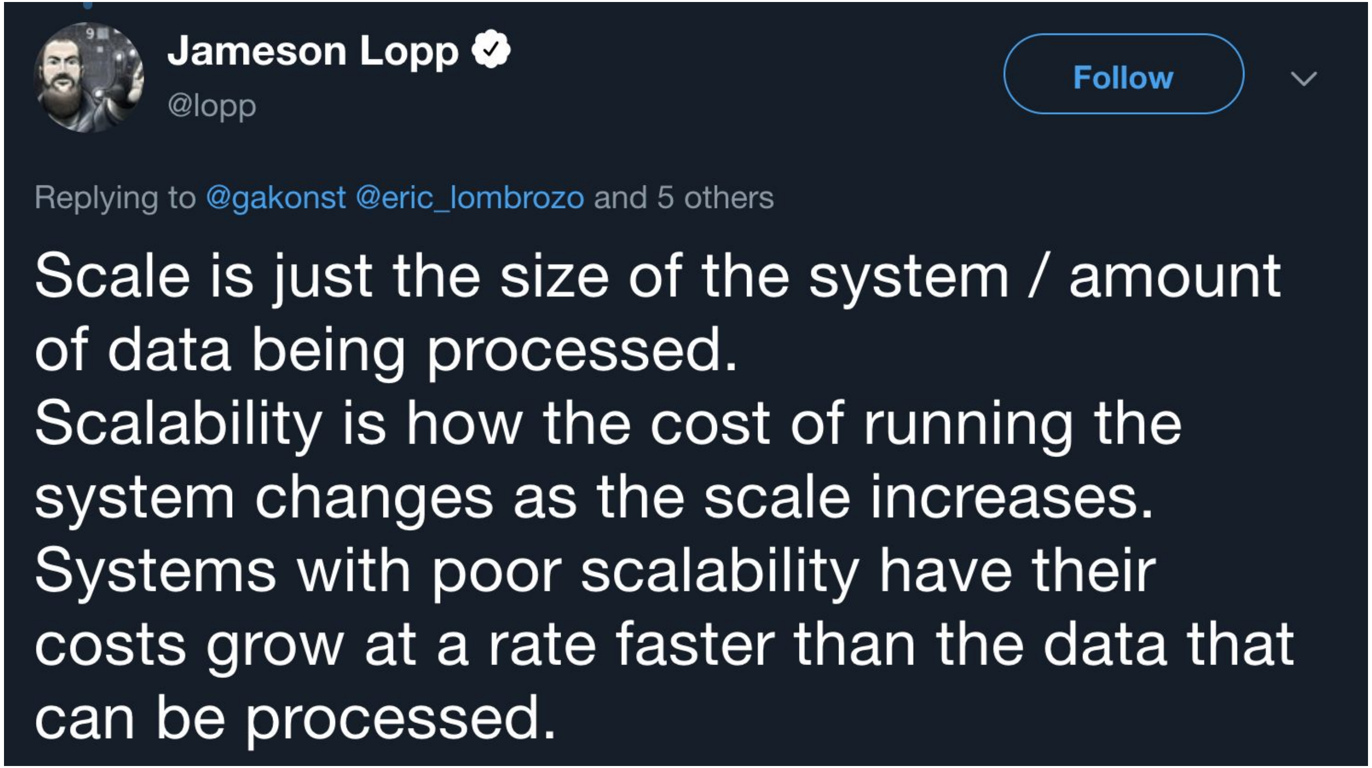
**federated pegs use multisig wallets for peg-in & peg-out*

Sidechains:

- **interoperability** solution
- **NOT** a **scalability** solution
- **independent** security model
- consist of their own **L1 that talks with other L1s**

Layer 2

Layer 2 provides **scalability** while maintaining **Layer 1 security**



Jameson Lopp
@lopp

Replying to @gakonst @eric_lombrozo and 5 others

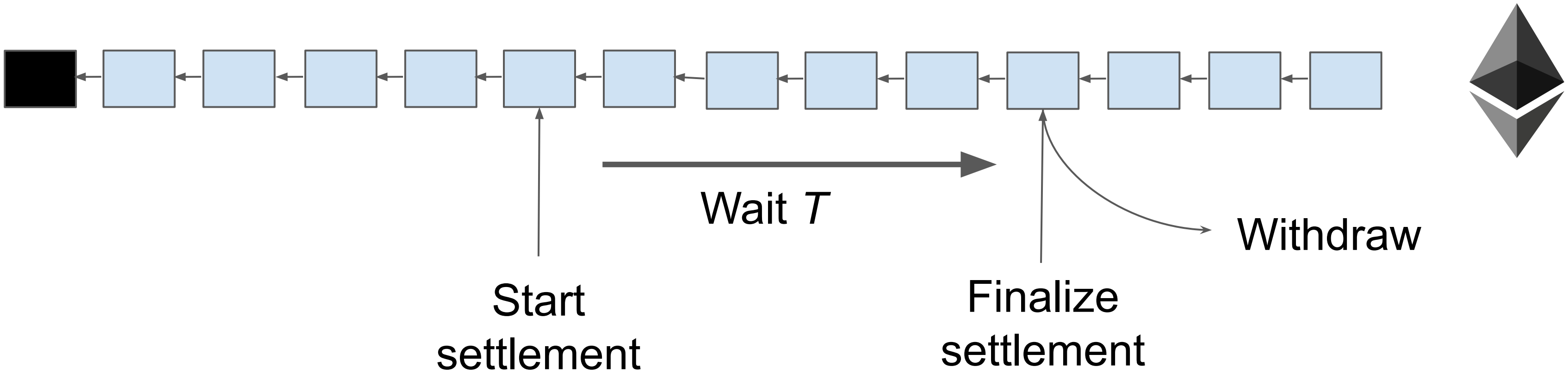
Scale is just the size of the system / amount of data being processed.
Scalability is how the cost of running the system changes as the scale increases.
Systems with poor scalability have their costs grow at a rate faster than the data that can be processed.

Layer 2 provides:
high performance
high security (aka nobody can steal your funds)
lower cost than Layer 1

How?

1. **Lock** funds in **smart contract on L1**
2. Funds are available on L2
3. **Transact** on L2
4. Play a **game** to **withdraw** back to L1

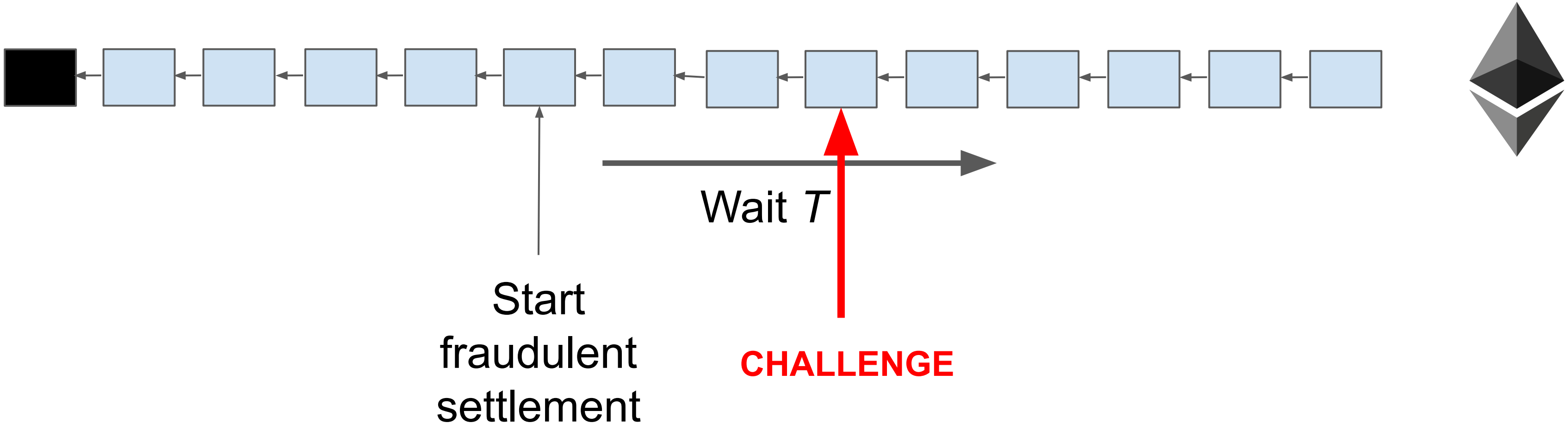
Deferred* Settlement Game



Unlock assets by **proving ownership** on a **smart contract on L1**

*https://medium.com/@nic__carter/transaction-count-is-an-inferior-measure-fba2d5ac97f1

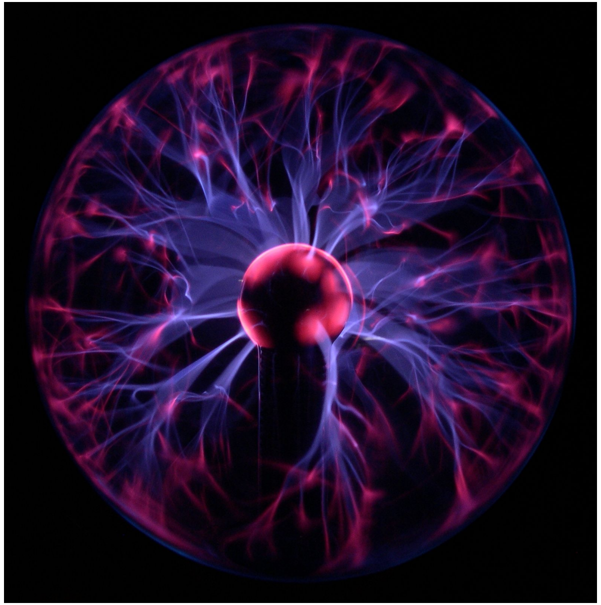
Fraudulent settlement attempts are cancelled



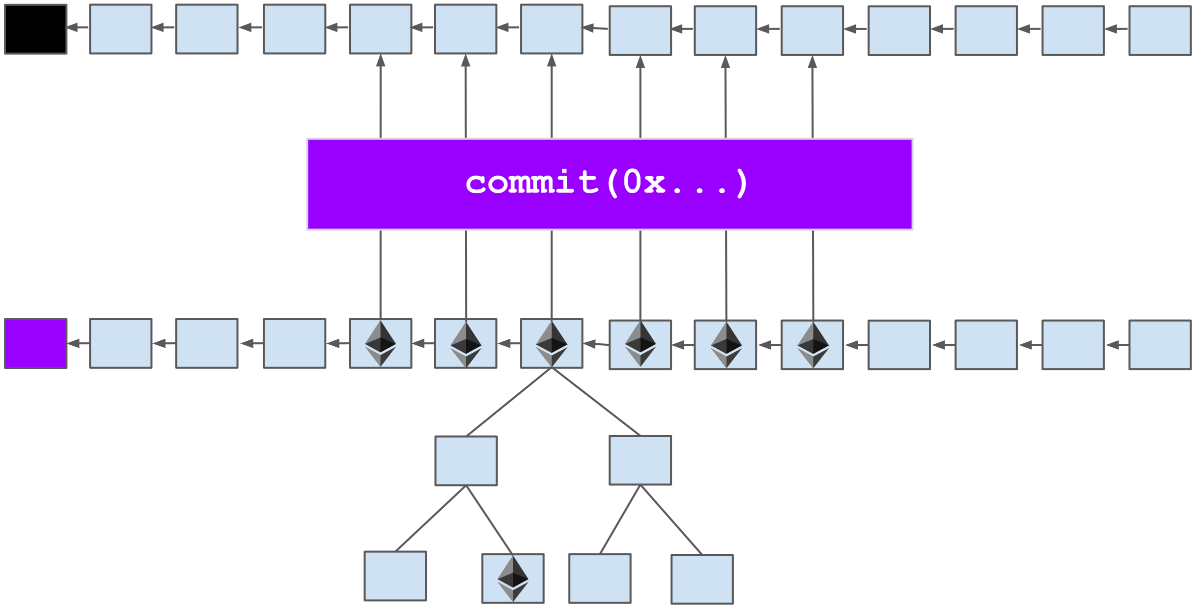
Challenged settlement requests get cancelled.

Plasma

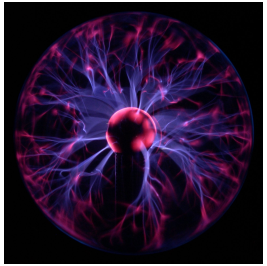
What is Plasma?



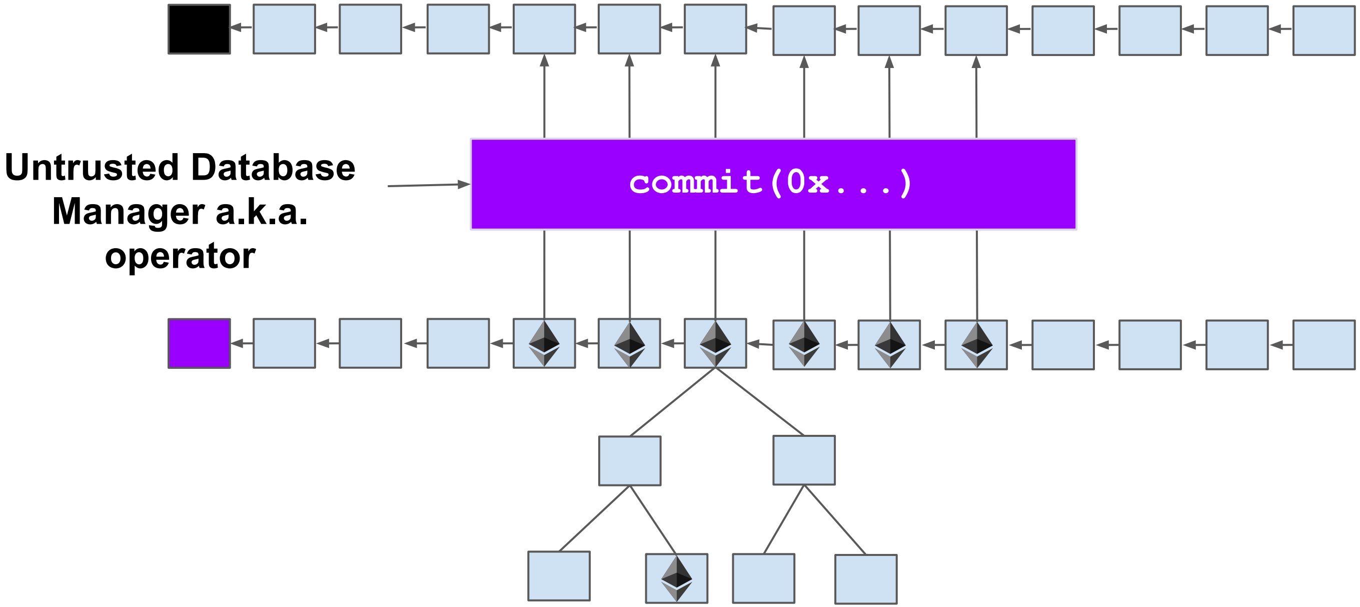
Plasma: commit each block root to “parent chain”



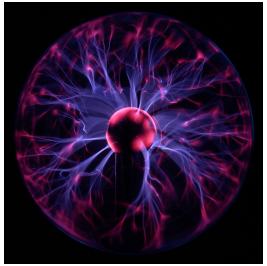
`commit(0x...)`



Plasma: commit each block root to “parent chain”



Untrusted Database Manager a.k.a. operator



Plasma characteristics

Periodic checkpoints on L1

Centralized, not custodial

Data availability problems

Finality = Parent chain finality

No routing requirements

Plasma is “non-custodial”.

Funds are secured by:

- **parent chain consensus**
- **exit game**

Desired properties

Micropayments
(can pay $0.0001)

Light nodes
(can run on a mobile phone)

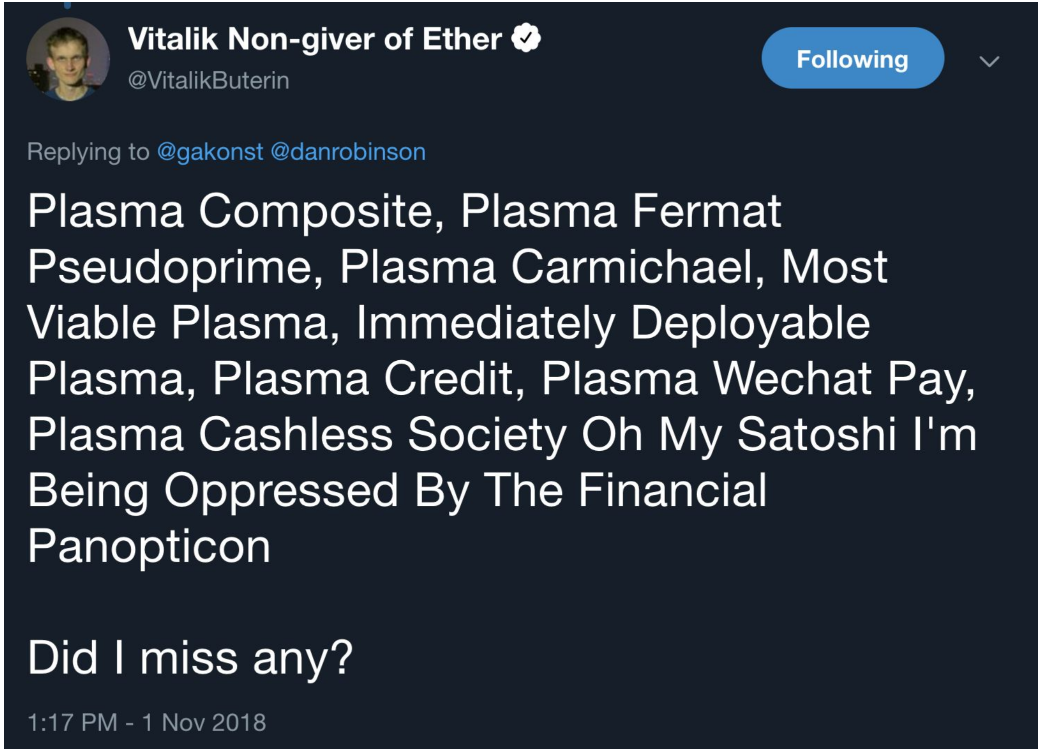
Safety of funds under data unavailability & L1 congestion

Endless Plasma flavors (find the fake ones)

Minimal Viable Plasma,
More Viable Plasma,
Non-Viable Plasma
Plasma Cash,
Plasma Debit,
Plasma Credit,
Gluon Plasma,
Quark-Gluon Plasma

Plasma EVM,
Plasma Leap,
Plasma Snapp,
Lightning Plasma,
Plasma “Classic”,
Plasma Cashflow,
Plasma Prime,
Plasma XT

Endless Plasma flavors (continued...)



Replying to @gakonst @danrobinson

Plasma Composite, Plasma Fermat Pseudoprime, Plasma Carmichael, Most Viable Plasma, Immediately Deployable Plasma, Plasma Credit, Plasma Wechat Pay, Plasma Cashless Society Oh My Satoshi I'm Being Oppressed By The Financial Panopticon

Did I miss any?

1:17 PM - 1 Nov 2018

Only 1 “works”: Plasma Cashflow

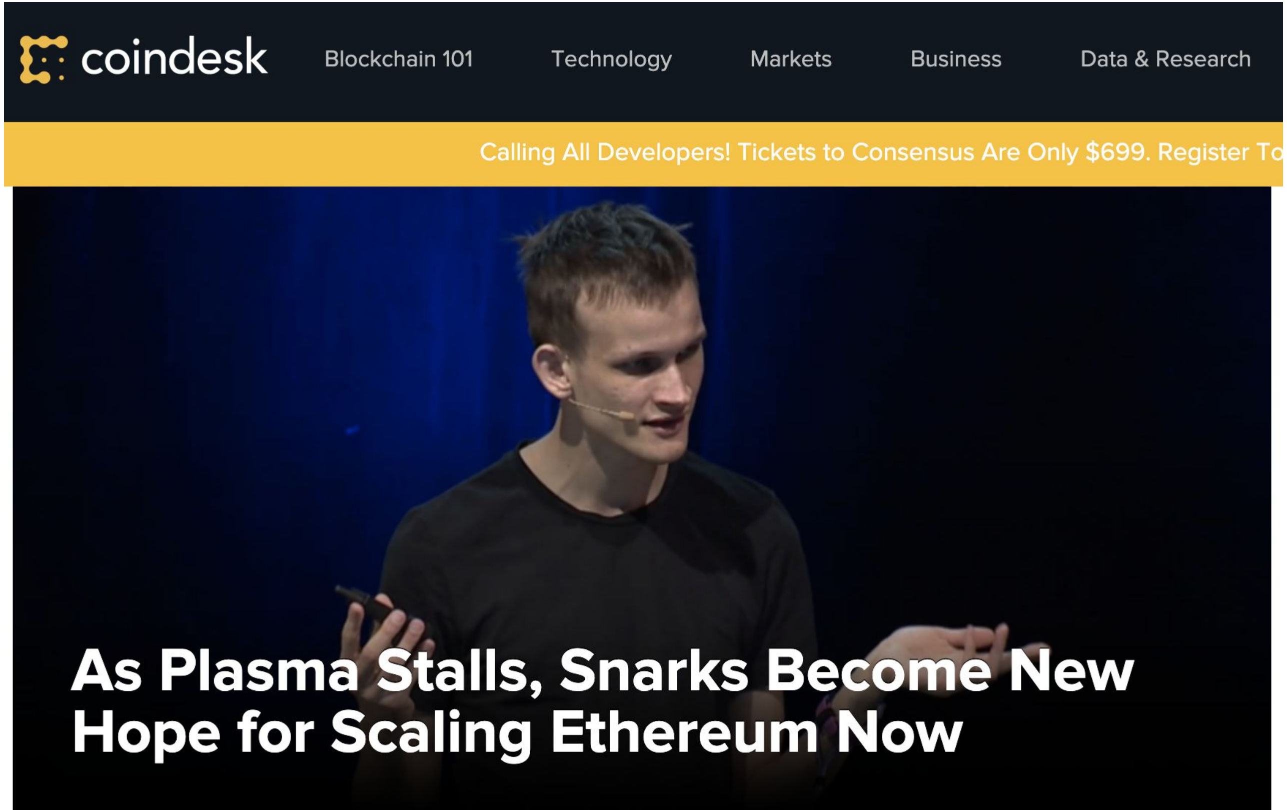
Light storage and bandwidth requirements

No assumption about data availability

No mass exits

Arbitrary granularity payments

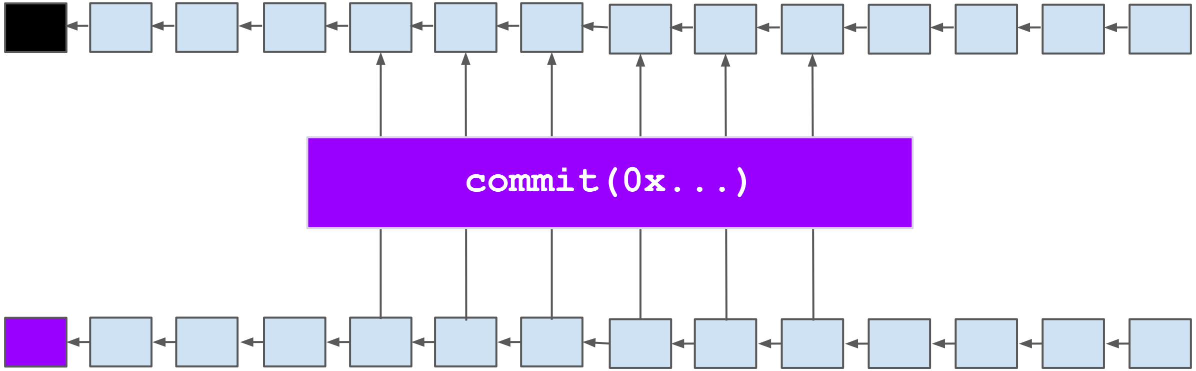
SNARKs? STARKs? Is Plasma dead?



Calling All Developers! Tickets to Consensus Are Only $699. Register To

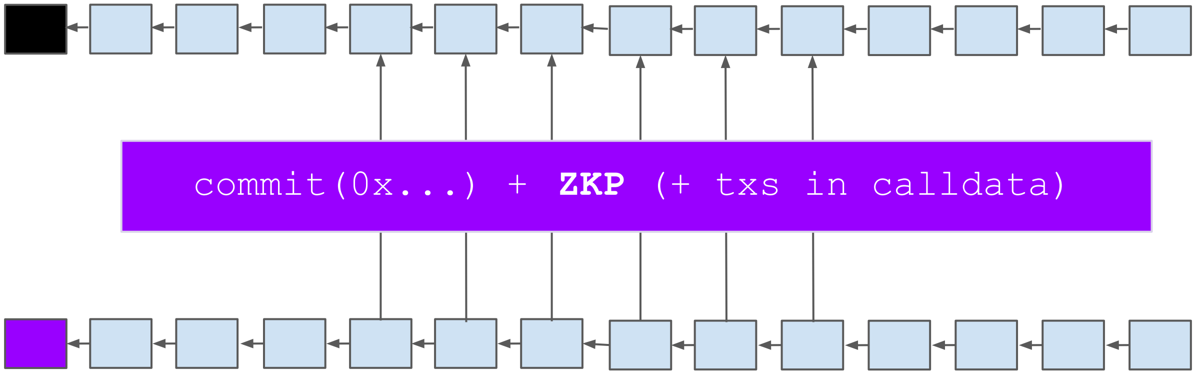
As Plasma Stalls, Snarks Become New Hope for Scaling Ethereum Now

Plasma + Fraud Proofs



If fraud → challenge

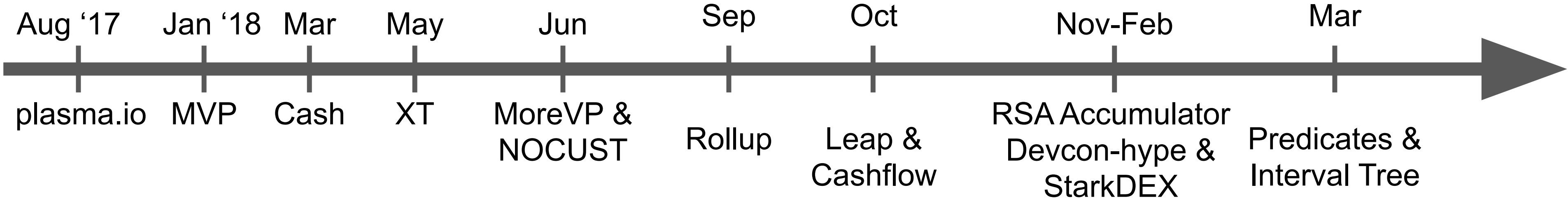
Plasma + Validity Proofs (Zero Knowledge Proofs - S{N,T}ARK)



Fraud is prevented by the validity proof.

Validity Proof caveat: expensive, slow, maybe trusted setup

A brief history of Plasma (22 months)



Aug ‘17	plasma.io
Jan ‘18	MVP
Mar	Cash
May	XT
Jun	MoreVP & NOCUST
Sep	Rollup
Oct	Leap & Cashflow
Nov-Feb	RSA Accumulator Devcon-hype & StarkDEX
Mar	Predicates & Interval Tree

Takeaways

L2 complementary to L1

Plasma Cashflow is Plasma Cash is Plasma™

L2 security == L1 security

Fraud Proofs vs Validity Proofs?

Achieved clear design for the “final form” of Plasma
Investors: Fund projects that have delivered.
Engineers: Join the teams that have delivered.

Thank you for your attention
Q & A ?

@gakonst / me@gakonst.com
gakonst.com/ethereal2019.pdf