L2BEAT

Scaling Ethereum with Rollups

an investigation by Piotr Szlachciak

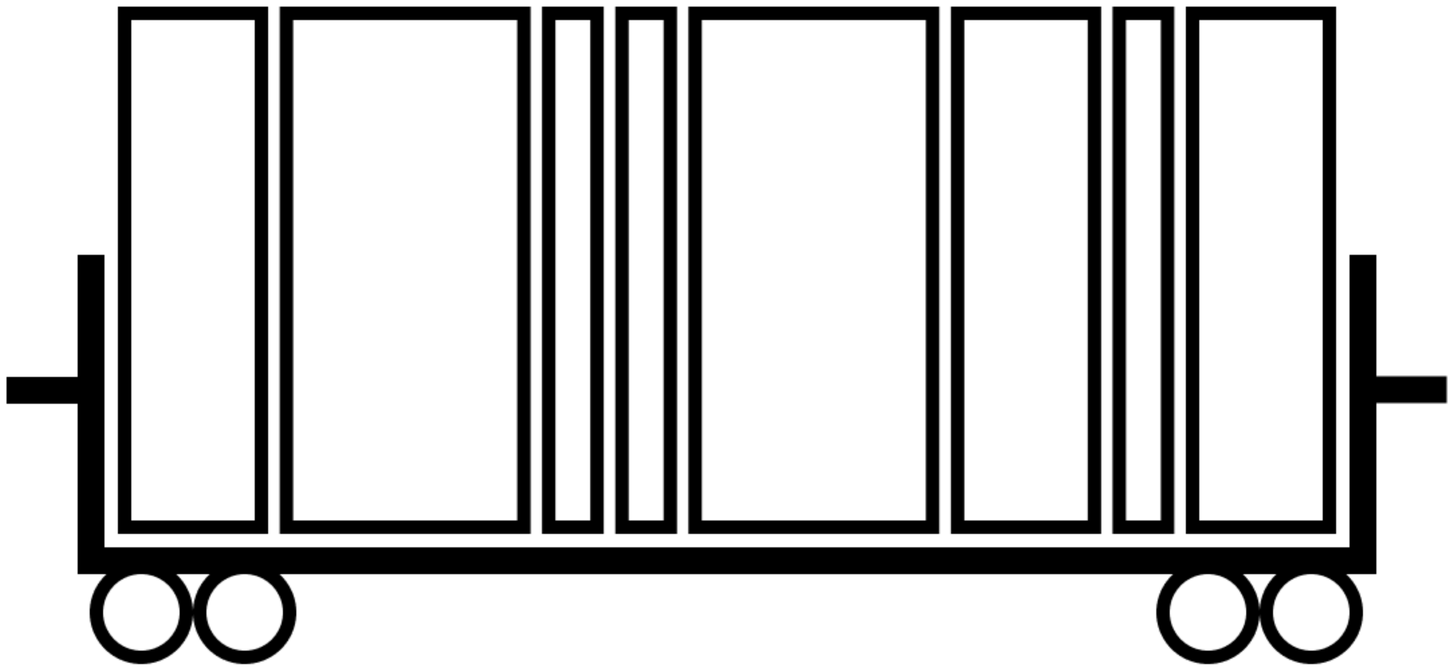
Diagnosis

The Blockchain cannot scale on its own.

Increasing available blockspace decreases decentralization while not really solving the problem of scale.

Solution: Rollups

Blockchain is like a train



A block with transactions

Natalie Scissaris
Hairstylist

PRICE LIST

Women's Cut/Style.....55
Men's Cut/Style.....30
Blow Out.....35
Girl's Cut/Style.....35
Boy's Cut/Style.....22

Gas price list
Ethereum Mainnet

Transaction 21,000
Calldata byte 16
Storage read ..... ~2,000
Storage write 20,000
Create contract ... 32,000

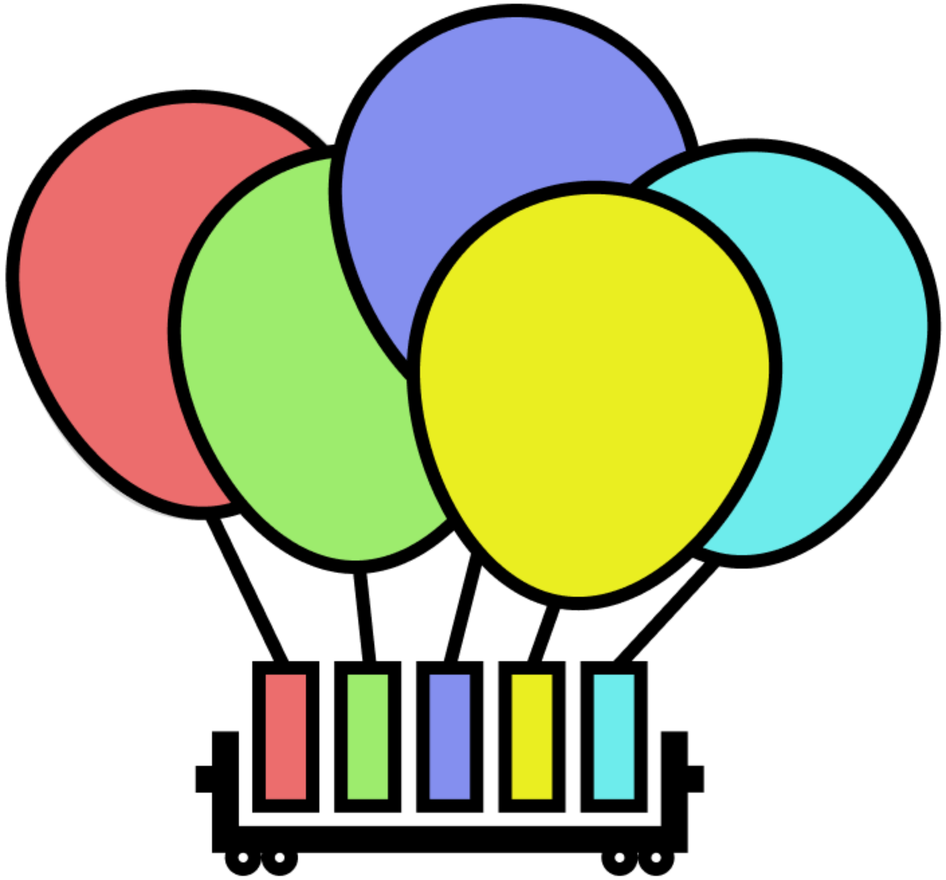
Do anything ... A LOT OF $

Verdict: do as little as possible on chain.

The state transition

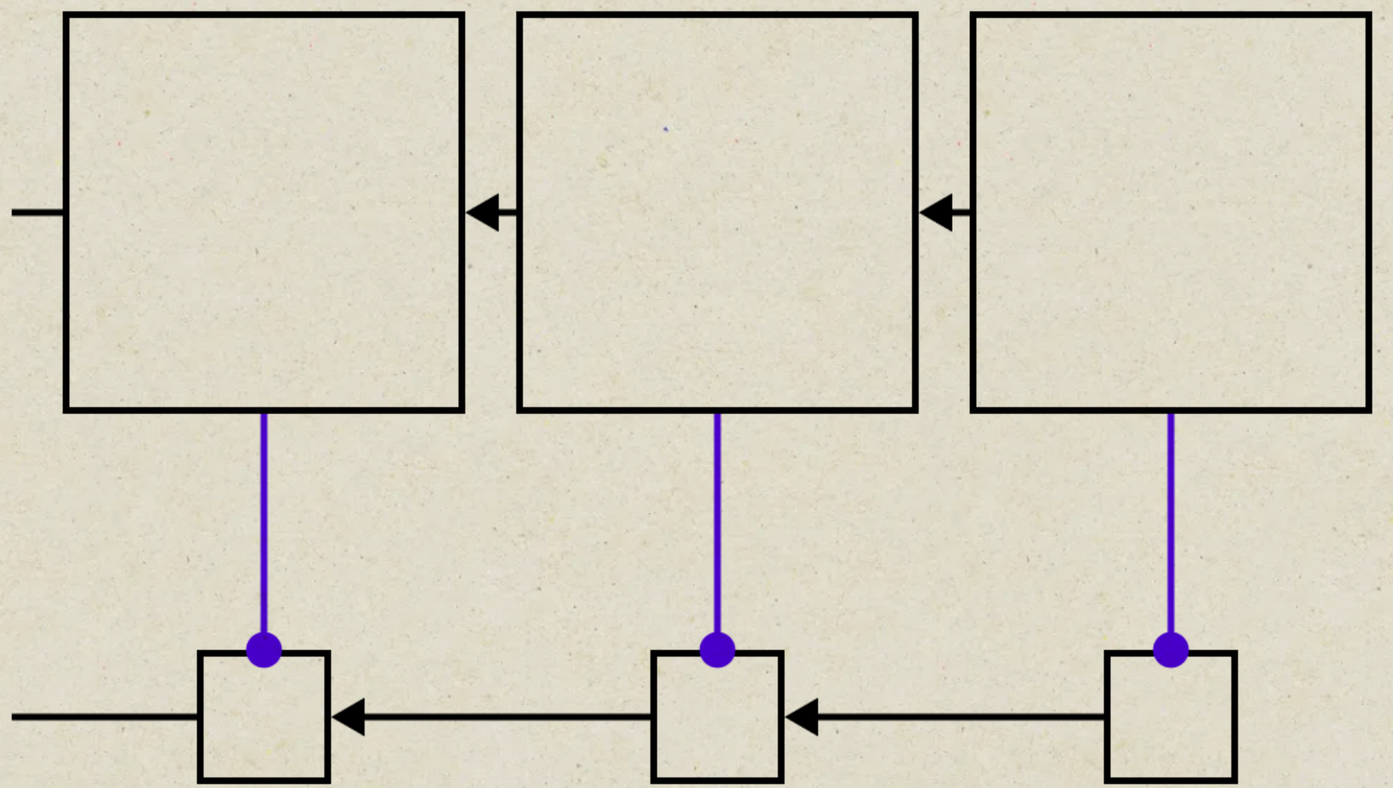
nextState = previousState + transaction data

If we know the initial state and all transaction data we can know every state along the way.



A block with rollup transactions

Moving in and out



The blockchain state tree

Good job

Now we have a cheap rollup chain running in parallel and we can go in and out easily. That's the end of our worries, right?

Right?

Optimistic rollups

Examples:

- Arbitrum
- Optimism
- Fuel

Pros:
Simple

Cons:
7 day wait

Left to right: Validator (prosecutor)
Blockchain (judge), Block producer (attorney)

Kris Kaczor 🦆
@krzKaczor

How I attempted to break @fuellabs_ v1, a short story about the importance of running validators for optimistic rollups.

Let's start from the beginning: 🧵👇

4:08 PM · May 12, 2022 · Twitter Web App

214 Retweets **42** Quote Tweets **689** Likes

Hack you fuel

Excerpt from
“Unfunny Twitter Jokes, volume 2”

“

Two rollups walk into a bar. The barman asks: Can I see your ids? Optimistic Rollup says: If nobody can prove I'm underage in 7 days that means I'm over 18. ZK Rollup says: I can prove to you I'm over 18, but I won't show you my id.

Zero knowledge rollups

Examples:

- zkSync
- dYdX
- StarkNet

Pros:
No wait

Cons:
Complex

Mathematician creating a ZK proof

This all sounds great.

So where can I find those rollups? Well...

No.	Name	State validation	Data availability	Upgradeability	Sequencer failure	Validator failure
1.	Arbitrum	Fraud proofs (INT)	On chain	Yes	Transact using L1	No mechanism
2.	dYdX ❖	ZK proofs (ST)	On chain	Yes	Force trade/exit to L1	Escape hatch (MP)
3.	Optimism OP	In development	On chain	Yes	Transact using L1	No mechanism
4.	Loopring	ZK proofs (SN)	On chain	Yes	Force exit to L1	Escape hatch (MP)
5.	Metis Andromeda OP	In development	External (MEMO)	Yes	Transact using L1	No mechanism
6.	Boba Network OP	In development	On chain	Yes	Transact using L1	No mechanism
7.	zkSync	ZK proofs (SN)	On chain	21d or no delay	Force exit to L1	Escape hatch (ZK)
8.	ZKSpace	ZK proofs (SN)	On chain	8 days delay	Force exit to L1	Escape hatch (ZK)
9.	Immutable X ❖	ZK proofs (ST)	External (DAC)	14 days delay	Force exit to L1	Escape hatch (MP)
10.	DeversiFi ❖	ZK proofs (ST)	External (DAC)	14 days delay	Force exit to L1	Escape hatch (MP)
11.	Sorare ❖	ZK proofs (ST)	External (DAC)	14 days delay	Force exit to L1	Escape hatch (MP)

Rollup operators: "I've got new rules"

I'm sorry ladies, but you need to be whitelisted to submit a fraud proof

Fraud proofs require implementing the EVM in Solidity.

Validity proofs require implementing the EVM in ZK math.

Turns out it itsn't easy to do that.

I heard you like EVM, so I put EVM inside your EVM

How to contribute to this space?

Learn

Develop L2s themselves

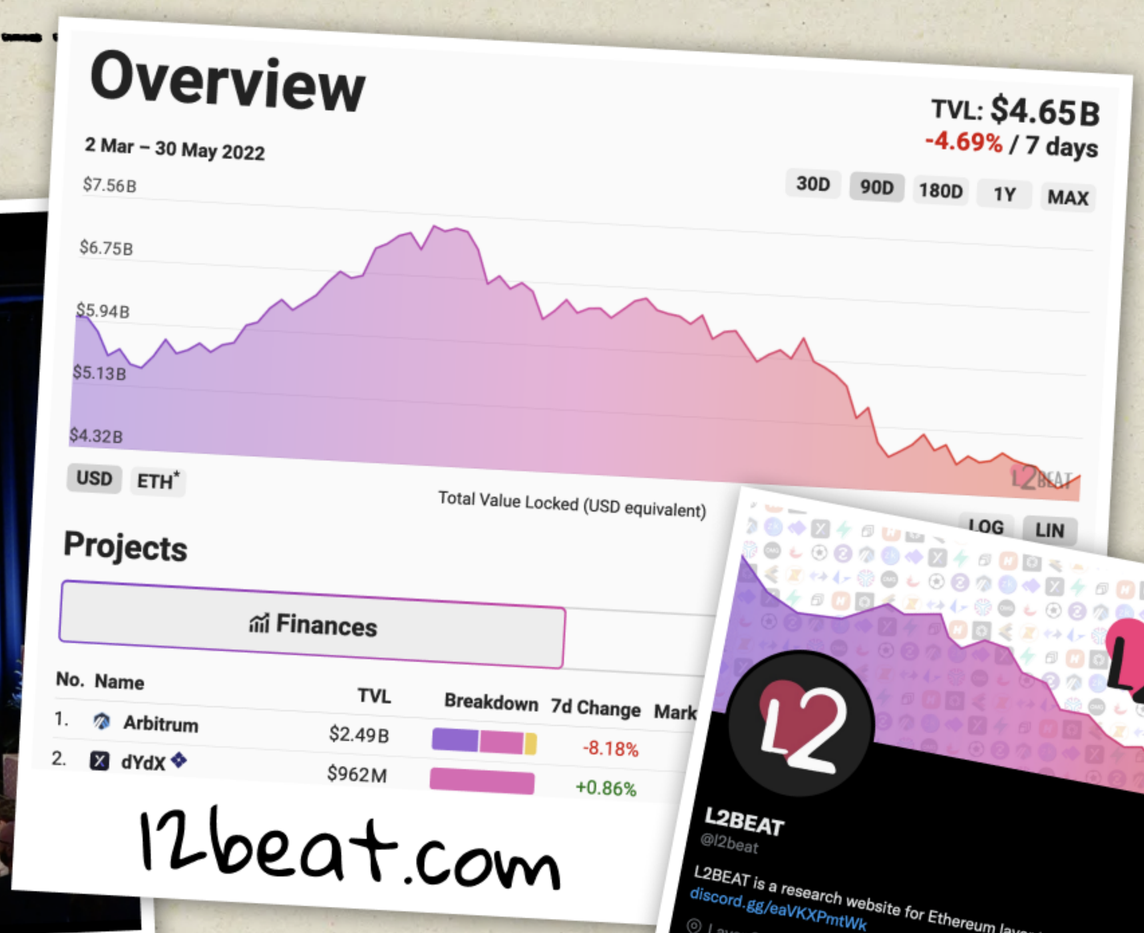
Become an L2 researcher

Use your devops skills

Write contracts on L2s

L2BEAT is where you learn

Amsterdam conference



l2beat.com

Twitter

THANK YOU

MADE IN L2BEAT