How to Scale a Blockchain

Motivating the Ethereum Rollup-Centric Roadmap

ansgar.eth

Researcher, Ethereum Foundation

Sorry about the confusion!

If you are here for multidimensional resource pricing:

Notes on multidimensional EIP-1559

Devconnect 2022

Update EIP-4844: Fee Market Update

EIPs PR #5707

1. Why Rollups?

2. A Modular Vision

1. Why Rollups?

Execution Chains

Execution Chains

first special-purpose
execution chain

Execution Chains

first special-purpose execution chain

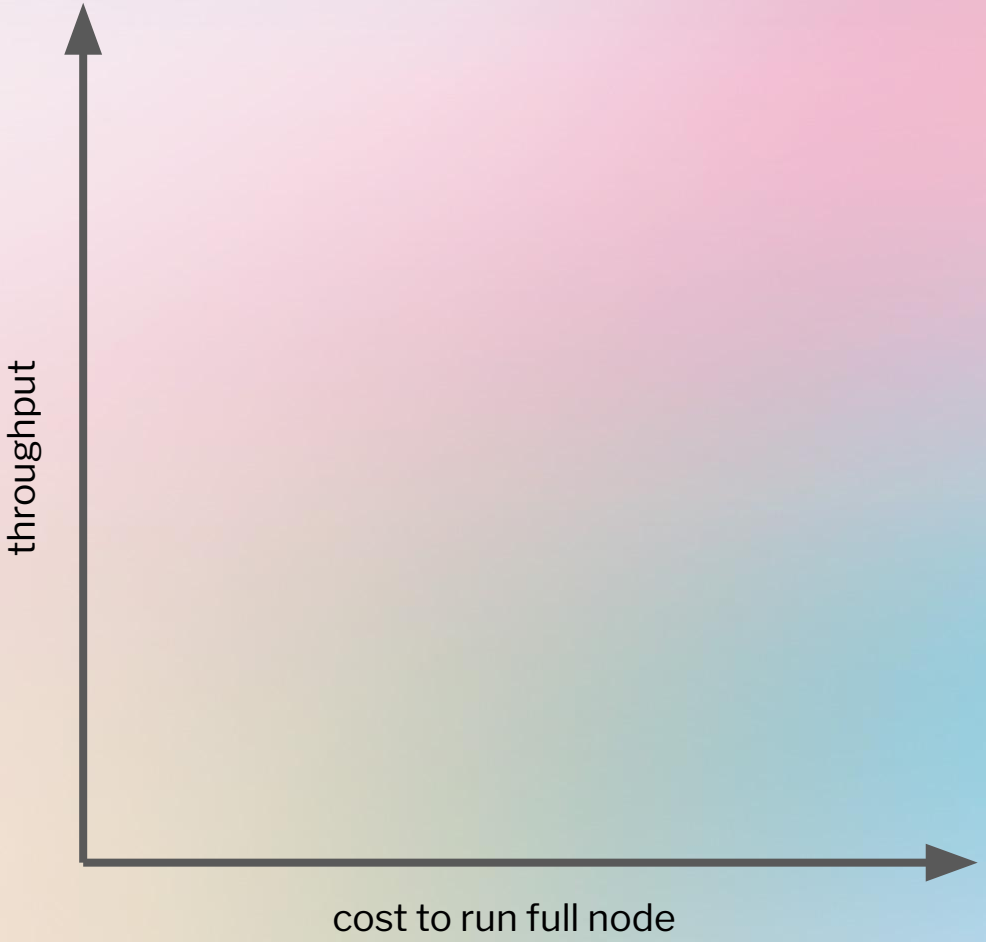
first general-purpose execution chain

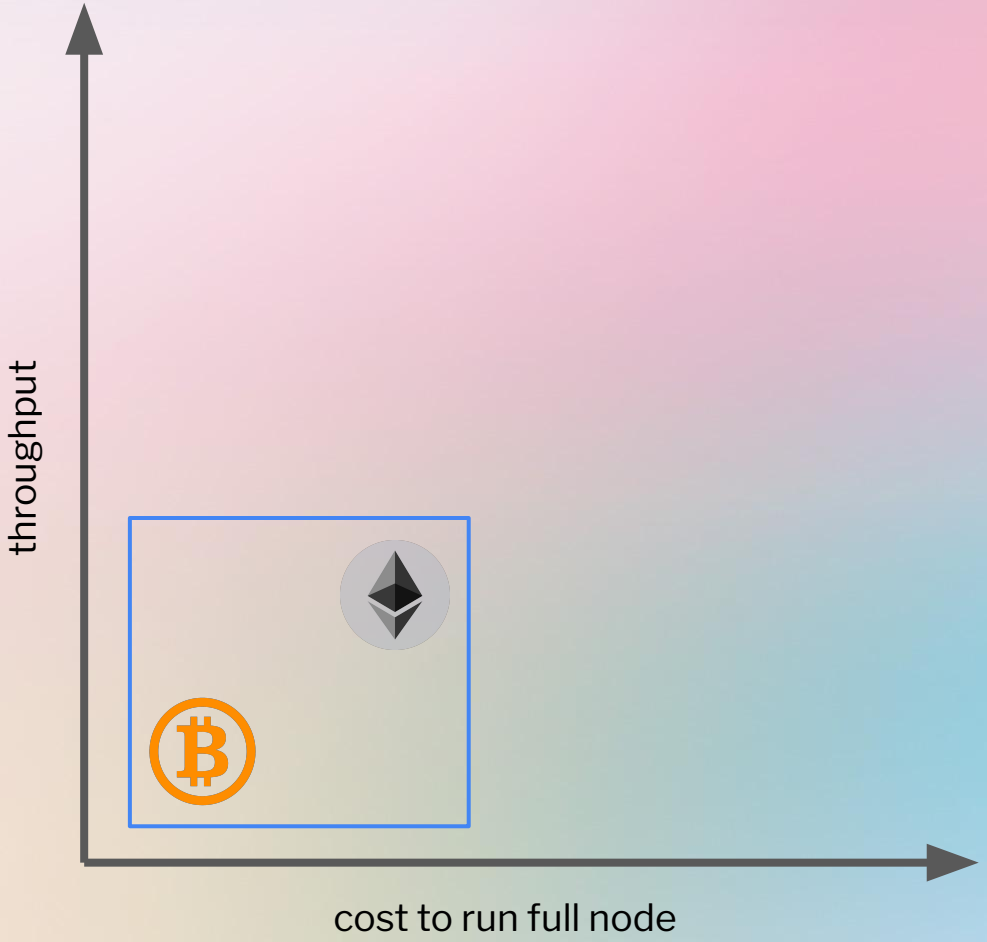
Execution Chains

first special-purpose execution chain

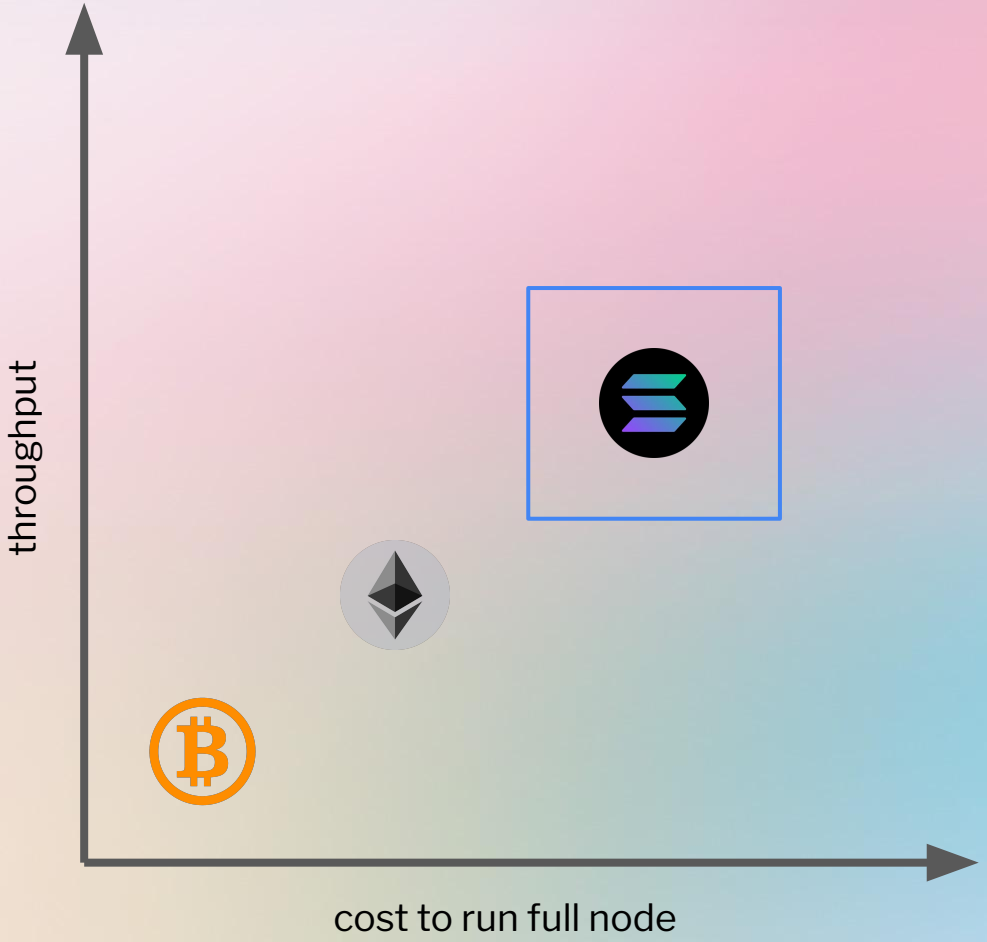
first general-purpose execution chain

- goals: max functionality, max throughput
- but: need to ensure security!

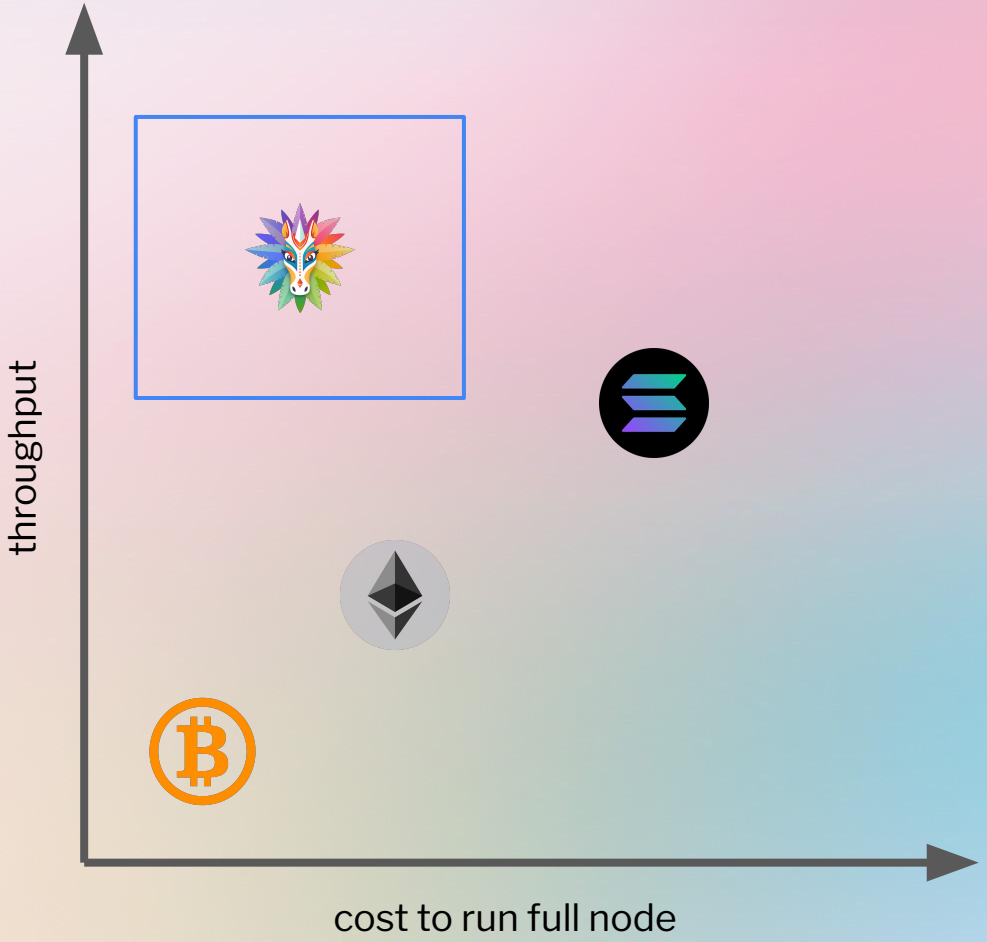

throughput
cost to run full node



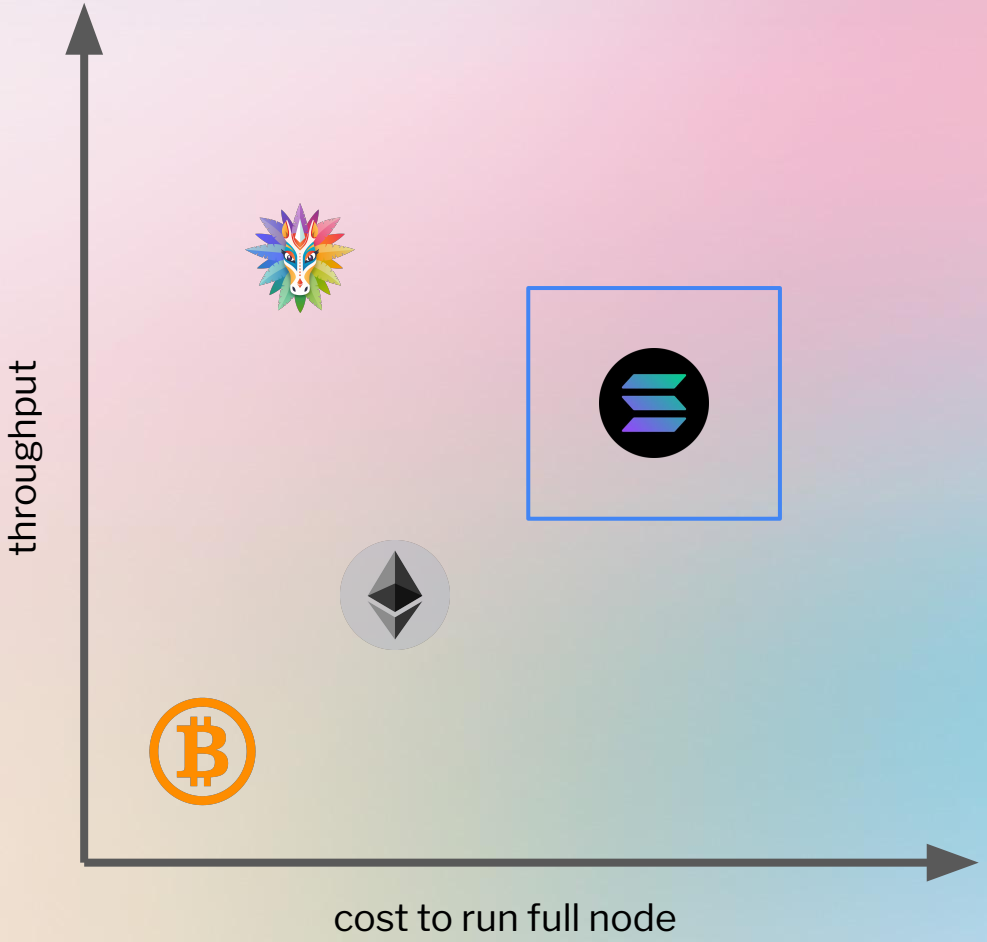
- everyone (who wants to) can run the chain locally
- chain throughput limited by consumer hardware capabilities
- “everyone validating everyone’s transactions” doesn’t scale!



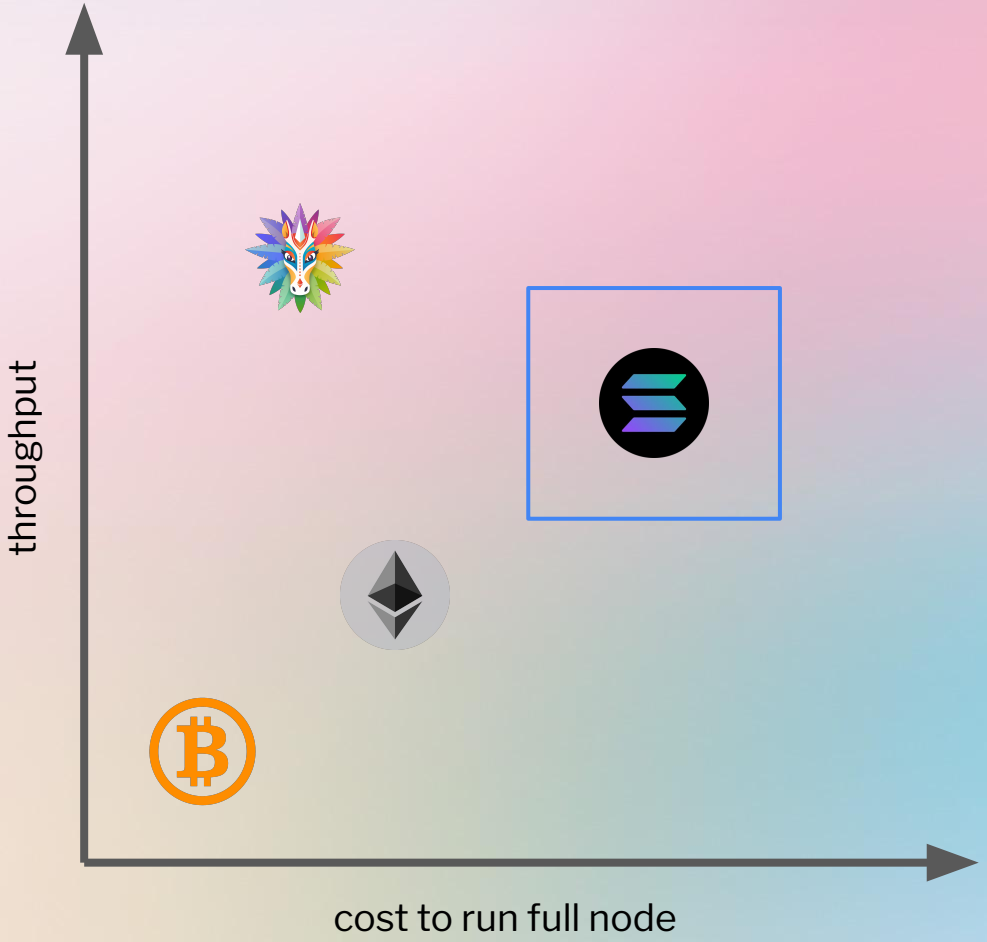
- everyone (who has the money) can run the chain on expensive servers in datacenters
- high throughput
- on disagreement (without local node):
  - go with majority (51% can rewrite rules) or
  - halt and recover via social layer



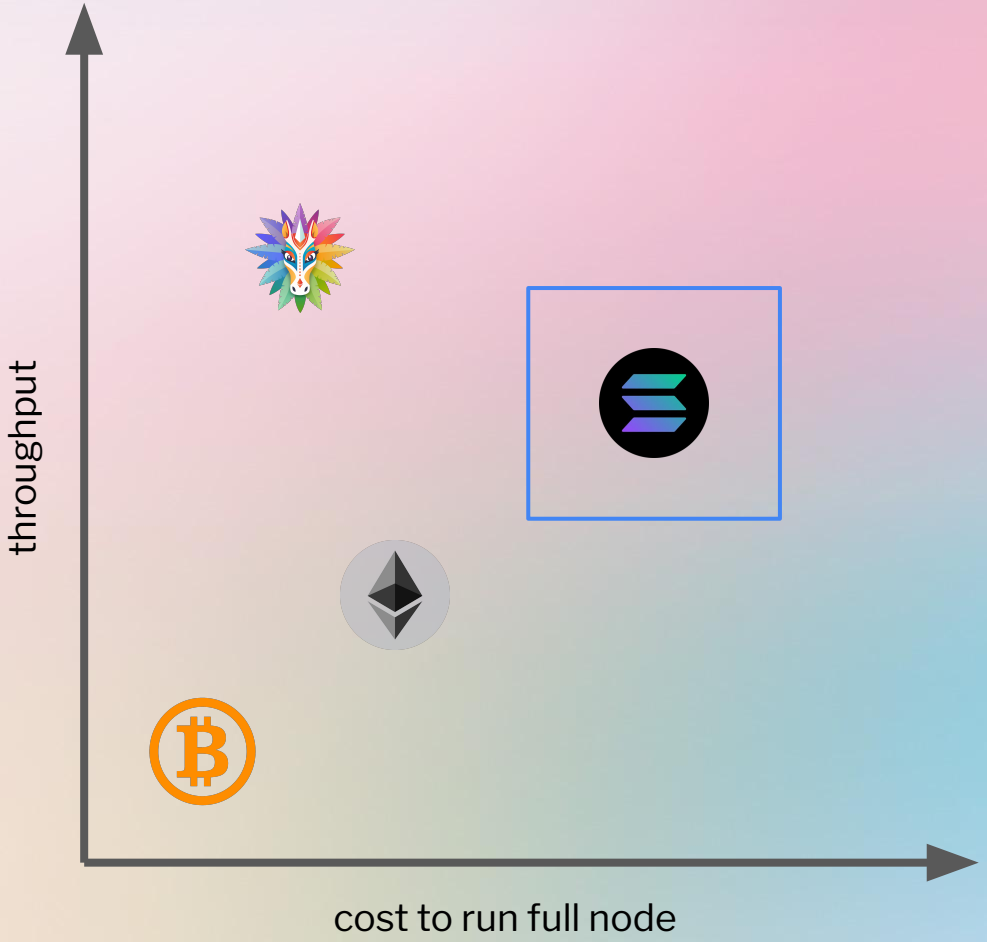
- everyone (who wants to) can run the chain locally
- very high throughput
- unicorn zone: does not exist today
- how can we get there?



- everyone (who has the money) can run the chain on expensive servers in datacenters
- high throughput
- on disagreement (without local node):
  - go with majority (51% can rewrite rules) or
  - halt and recover via social layer



- everyone (who has the money) can run the chain on expensive servers in datacenters
- high throughput
- on disagreement (without local node):
  - go with majority (51% can rewrite rules) or
  - halt and recover via social layer



- everyone (who has the money) can run the chain on expensive servers in datacenters
- high throughput
- on disagreement (without local node):
  - go with majority (51% can rewrite rules) or
  - halt and recover via social layer

automate!

Optimistic Rollups

- apply changes optimistically
- anyone can submit fraud proofs (requires 1 of N honest nodes!)
- fraud proofs are automatically resolved on settlement platform

Optimistic Rollups

- apply changes optimistically
- anyone can submit fraud proofs (requires 1 of N honest nodes!)
- fraud proofs are automatically resolved on settlement platform

ZK-Rollups

- use cryptographic magic (zero knowledge proofs) to ensure computational integrity
- validity proofs are automatically verified on settlement platform

Optimistic Rollups

- apply changes optimistically
- anyone can submit fraud proofs (requires 1 of N honest nodes!)
- fraud proofs are automatically resolved on settlement platform

- if data unavailable: operator can steal funds

ZK-Rollups

- use cryptographic magic (zero knowledge proofs) to ensure computational integrity
- validity proofs are automatically verified on settlement platform

- if data unavailable: operator can lock users out

Optimistic Rollups

- apply changes optimistically
- anyone can submit fraud proofs (requires 1 of N honest nodes!)
- fraud proofs are automatically resolved on settlement platform

- if data unavailable: operator can steal funds

ZK-Rollups

- use cryptographic magic (zero knowledge proofs) to ensure computational integrity
- validity proofs are automatically verified on settlement platform

- if data unavailable: operator can lock users out

=> need to guarantee data availability!

scaling approach: sampling + erasure coding

2. A Modular Vision

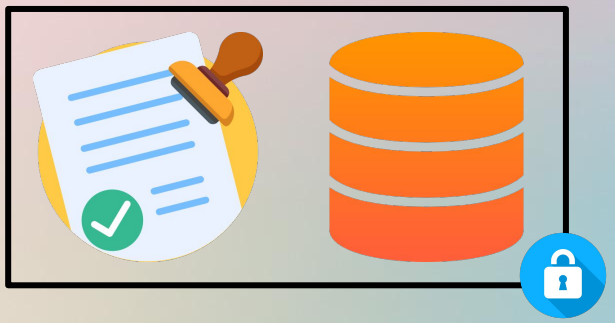
execution chain

execution chain

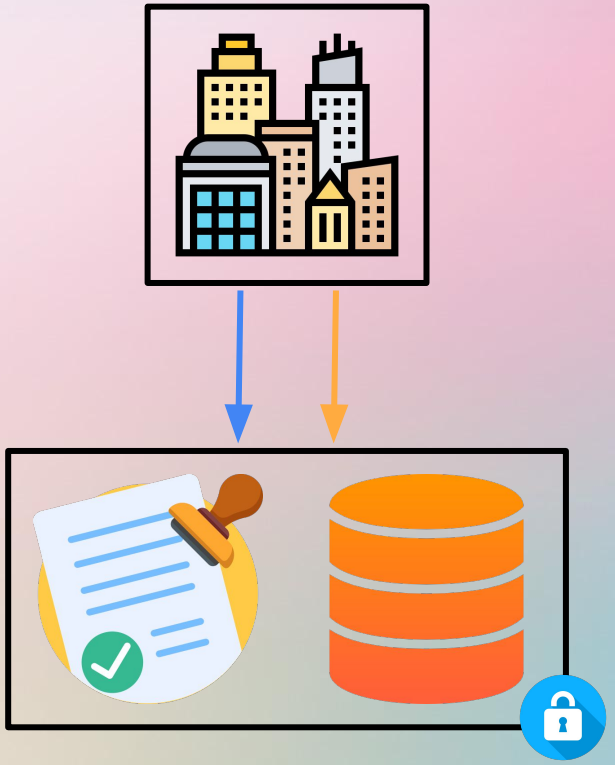
settlement

data availability

execution chain



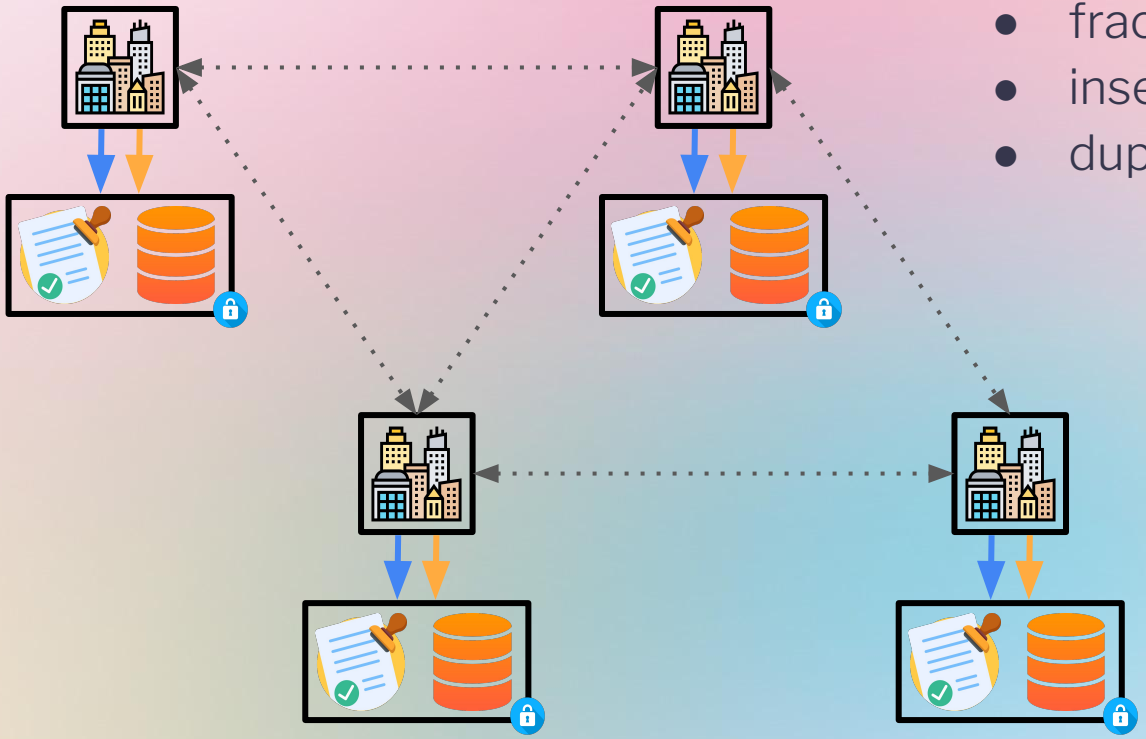
settlement chain



Enshrined Rollup

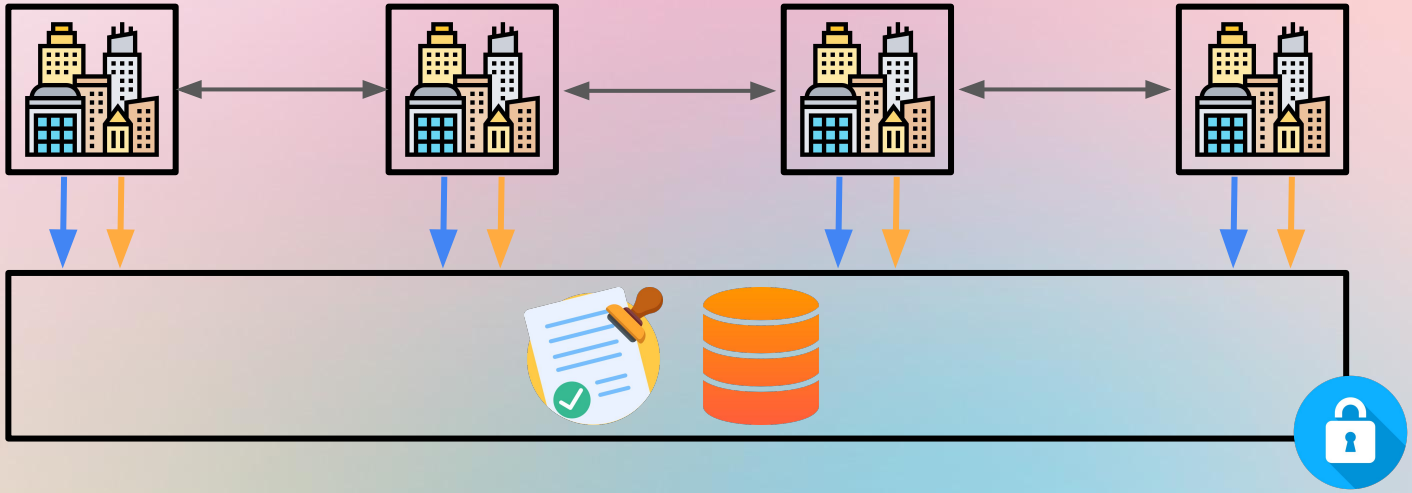
- 1:1 (tight) coupling of execution chain and settlement chain
- same level of security as a pure execution chain

Multichain Vision



- fractured security
- insecure bridges
- duplicated complexity

Shared Settlement Chain



- shared (pooled) security
- secure bridges

Ethereum a Few Years Ago

Ethereum

Pure Execution Chain

- PoW security
- Rollups not yet a thing

research

Phase One and Done: eth2 as a data availability engine

Sharding data-availability

cdetrio 3 Apr '19

At present, the bottleneck constraining throughput on the Ethereum 1.0 chain is state growth. So if we want to scale Ethereum, the logic goes, then 1000 shards where each has independent state would enable 1000x more throughput.

But consider the direction that Eth 1.x seems to be heading. The desire for Eth1.x is to make a large cost adjustment to two resource types: storage and tx data. Currently, storage is underpriced and tx data is overpriced. This incentivizes dapp developers to write contracts that utilize storage more than tx data, which results in storage becoming the throughput bottleneck. Proposals are to increase the price of storage, and decrease the cost of tx data. After these cost adjustments, developers will be incentivized to utilize tx data, and not storage (i.e. they will be incentivized to write stateless contracts rather than stateful). Thus in the near feature (if the Eth 1.x roadmap achieves adoption), we can expect that throughput on Ethereum 1.0 will be constrained by tx data, and not storage.

If we assume that throughput is constrained by tx data, then in order to scale Ethereum, shards on Serenity do not need to be stateful. If the bottleneck is tx data executed by stateless contracts, then 1000 stateless shards would enable 1000x more throughput.

Sounds great, but it requires shards that execute, which aren't planned until Phase 2. In the meantime, we can use Phase 1 as a data availability engine 193, a term that seems to be catching on. Let's think about how this will work.

A rollup-centric ethereum roadmap

ethereum-roadmap, layer-2

vbuterin

4 Oct '20

What would a rollup-centric ethereum roadmap look like?

Last week the Optimism team announced 601 the launch of the first stage of their testnet, and the roadmap to mainnet. They are not the only ones; Fuel 381 is moving toward a testnet and Arbitrum 292 has one. In the land of ZK rollups, Loopring 306, Zksync 299 and the Starkware-tech-based Deversifi 229 are already live and have users on mainnet. With OMG network's mainnet beta 238, plasma is moving forward too. Meanwhile, gas prices on eth1 are climbing to new highs, to the point where some non-financial dapps are being forced to shut down 882 and others 256 are running on testnets.

The eth2 roadmap offers scalability, and the earlier phases of eth2 are approaching quickly, but base-layer scalability for applications is only coming as the last major phase of eth2, which is still years away. In a further twist of irony, eth2's usability as a data availability layer for rollups comes in phase 1, long before eth2 becomes usable for "traditional" layer-1 applications. These facts taken together lead to a particular conclusion: **the Ethereum ecosystem is likely to be all-in on rollups (plus some plasma and channels) as a scaling strategy for the near and mid-term future**.

If we start from this premise, we can see that it leads to some particular conclusions about what the priorities of Ethereum core development and ecosystem development should be, conclusions that are in some cases different from the current path. But what are some of these conclusions?

lightclient

eth2 was a rollup format

2020.10.02 - ethereum

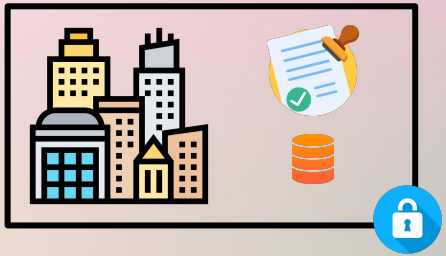
When we transition to a new scaling paradigm, it is good practice to review what we've left behind.

The goal of this post is to convince the reader that a "rollup-centric" approach is not a major departure from sharding and hopefully build a more intuitive understanding of the (hypothetical) system as a whole.

Definition of an Optimistic Rollup

For the purpose of this post, let's specify only the most simple implementation of an Optimistic Rollup (ORU).

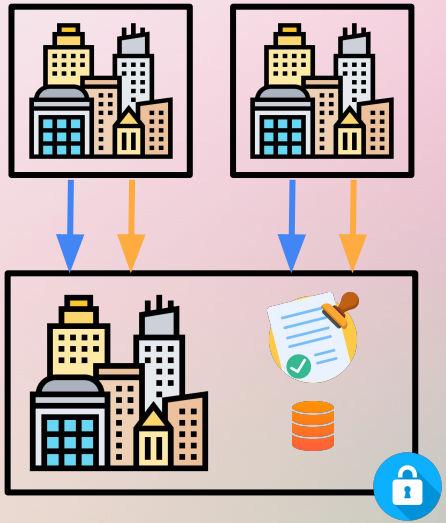
Ethereum a Few Months Ago



Hybrid Execution / Settlement Chain

- PoW security
- Very limited (& expensive) data availability

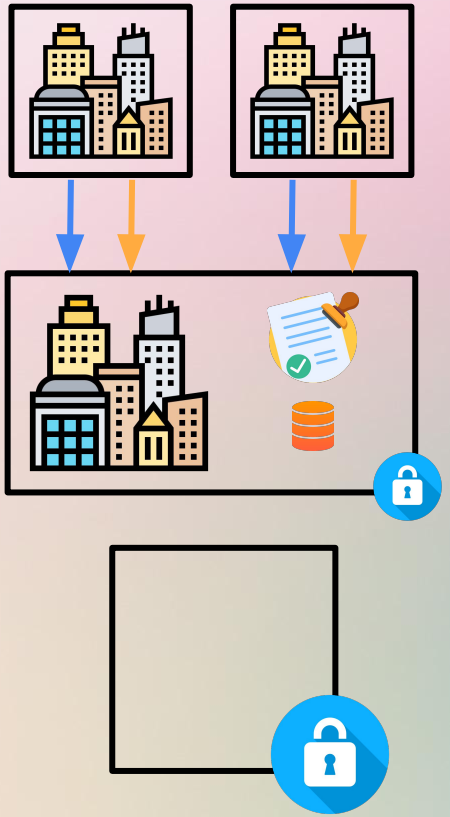
Ethereum a Few Months Ago



Hybrid Execution / Settlement Chain

- PoW security
- Very limited (& expensive) data availability

Ethereum a Few Months Ago



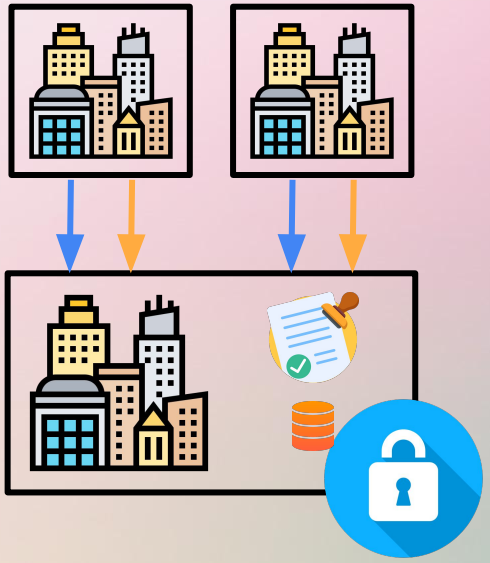
Hybrid Execution / Settlement Chain

- PoW security
- Very limited (& expensive) data availability

Beacon Chain

- empty
- much stronger PoS security

Ethereum Today



Hybrid Execution / Settlement Chain

- PoS security
- Very limited (& expensive) data availability

Side Note: On Security

2 sources of increased post-merge security:

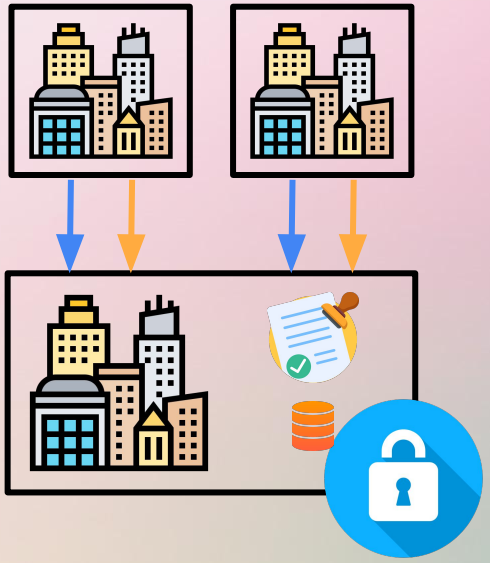
- PoW -> PoS:
  - more efficient, only have to offset lost interest on locked ETH
  - more effective, faults are attributable & can be punished

Side Note: On Security

2 sources of increased post-merge security:

- PoW -> PoS:
  - more efficient, only have to offset lost interest on locked ETH
  - more effective, faults are attributable & can be punished
- End of PoW: no more mining rewards
  => much improved monetary properties
  => higher expected monetary premium (in the long run)
  => higher total ETH market cap
  => can buy more security

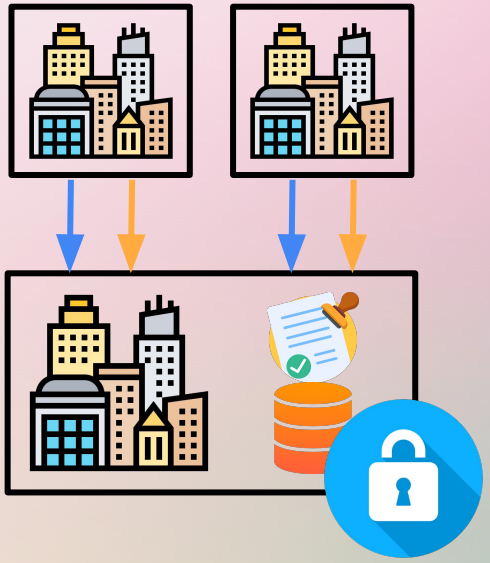
Ethereum Today



Hybrid Execution / Settlement Chain

- PoS security
- Very limited (& expensive) data availability

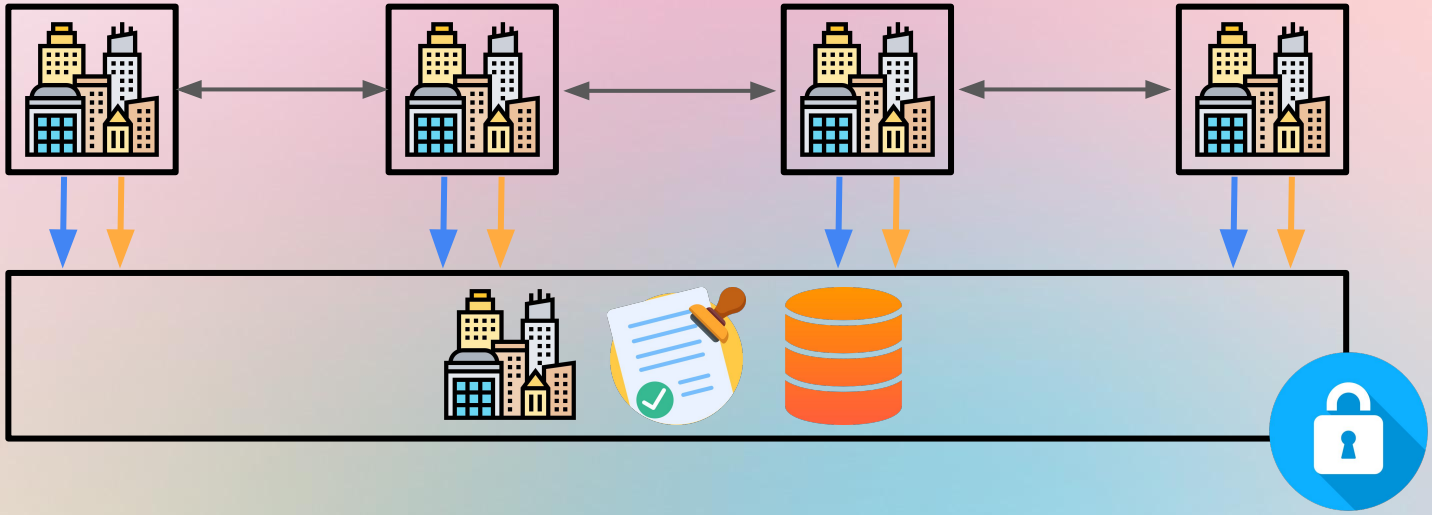
Ethereum Next Year: Proto-Danksharding (EIP-4844)



Hybrid Execution / Settlement Chain

- PoS security
- Improved data availability

Ethereum Soon™ After: Danksharding



- high data availability
- can host multiple high-throughput rollups

The Future Role of the “eth1” Chain

currently: hybrid execution / settlement chain

possible future directions:

The Future Role of the “eth1” Chain

currently: hybrid execution / settlement chain

possible future directions:

- stay a hybrid chain

The Future Role of the “eth1” Chain

currently: hybrid execution / settlement chain

possible future directions:

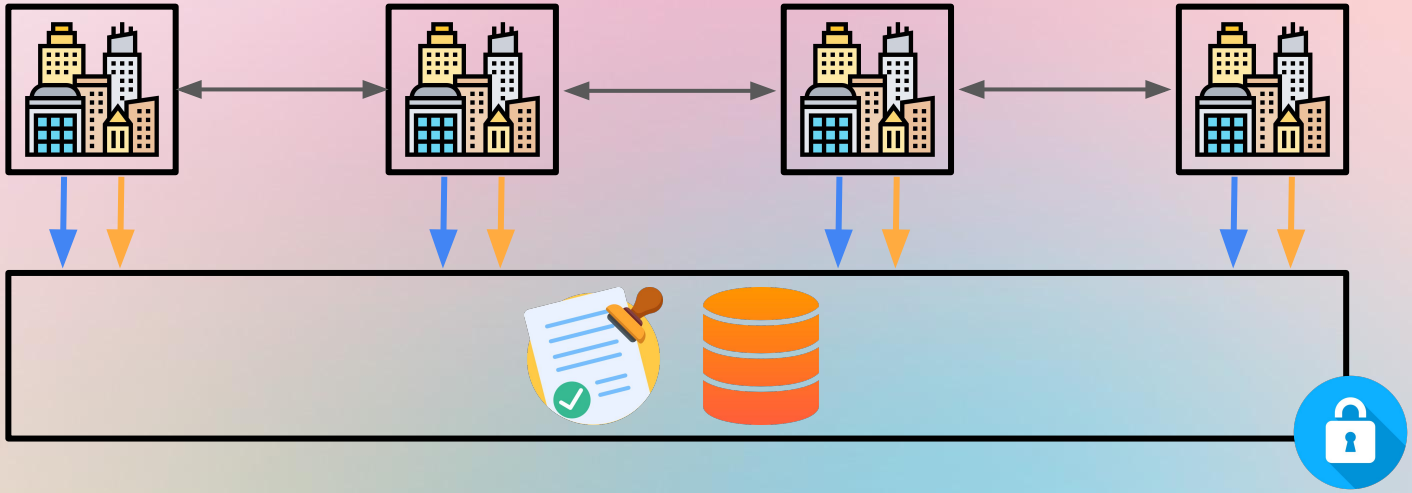
- stay a hybrid chain
- turn over time into primarily a settlement chain

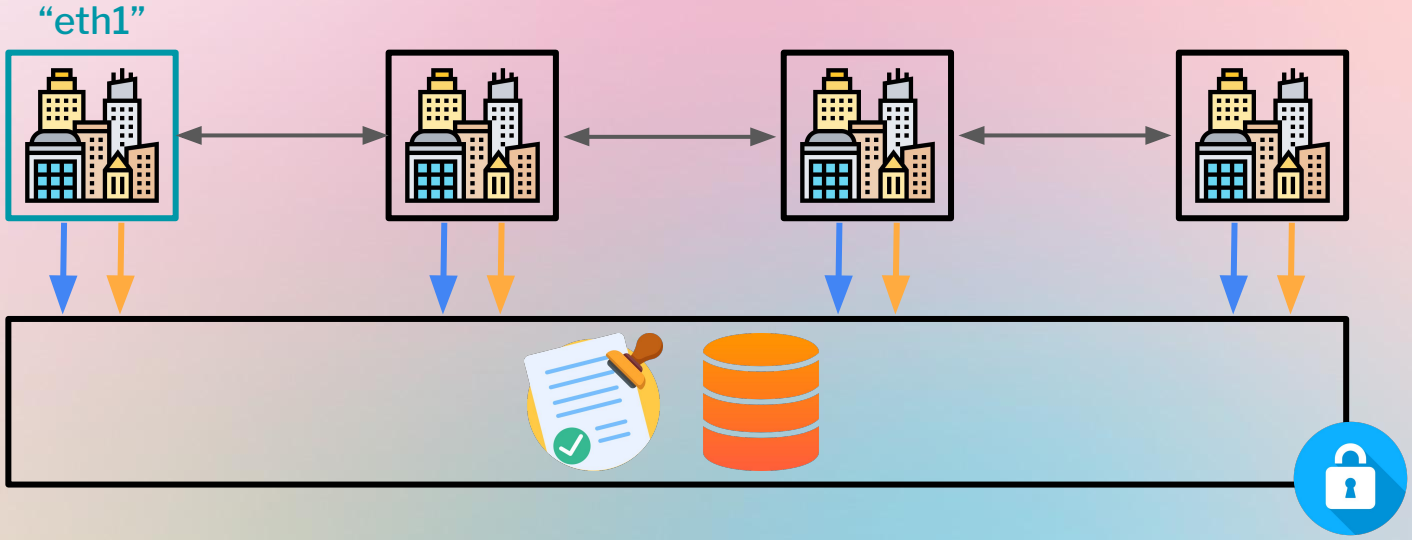
The Future Role of the “eth1” Chain

currently: hybrid execution / settlement chain

possible future directions:

- stay a hybrid chain
- turn over time into primarily a settlement chain
- introduce separate settlement chain, turn “eth1” back into primarily an execution chain




“eth1”

The Future of the EVM

- not certain that future high-throughput execution chains will be EVM based
- many possible EVM performance improvements once no longer constrained by minimal consumer hardware
- but: also many other innovative high-throughput blockchain VMs
- open question: implications for
  - clients
  - programming languages
  - tooling
  - ...

EVM Equivalence?

Pro:

- standardization
- multiple existing client implementations
- potential future enshrined fraud / validity proof support
- defer to L1 governance

EVM Equivalence?

Pro:

- standardization
- multiple existing client implementations
- potential future enshrined fraud / validity proof support
- defer to L1 governance

Contra:

- slower iteration speed of L1
- L2-specific functionality
- L1 and L2 operate at different scales, shared VM might not be optimal

EVM Equivalence?

Pro:

- standardization
- multiple existing client implementations
- potential future enshrined fraud / validity proof support
- defer to L1 governance

Contra:

- slower iteration speed of L1
- L2-specific functionality
- L1 and L2 operate at different scales, shared VM might not be optimal

=> potential for the best of both worlds with a standardized L2 EVM spec?

Summary

- Traditional blockchains have to trade off security and scalability, rollups solve this by outsourcing security to settlement chains

Summary

- Traditional blockchains have to trade off security and scalability, rollups solve this by outsourcing security to settlement chains
- Ethereum’s vision: become the primary settlement chain

Summary

- Traditional blockchains have to trade off security and scalability, rollups solve this by outsourcing security to settlement chains
- Ethereum's vision: become the primary settlement chain
- We are still at the beginning of that transformation, implications for different parts of the ecosystem will only emerge over time

Summary

- Traditional blockchains have to trade off security and scalability, rollups solve this by outsourcing security to settlement chains
- Ethereum's vision: become the primary settlement chain
- We are still at the beginning of that transformation, implications for different parts of the ecosystem will only emerge over time
- Ethereum will (likely) continue to also have execution chain ambitions!

Thank you!

ansgar.eth

Researcher, Ethereum Foundation

@adietrichs