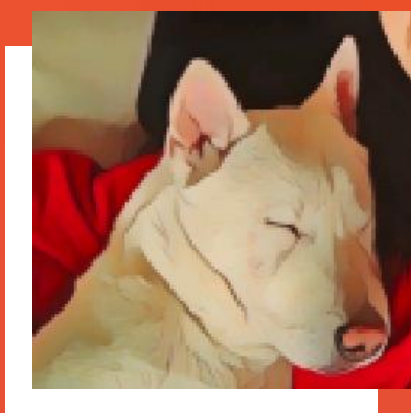




2023

WHAT KIND OF ETHEREUM ROLLUPS ARE WE LOOKING FOR?



Maggie

Tech Lead

Foresight Ventures

THE FIRM

Foresight Ventures

A research-driven crypto investment & incubation powerhouse with premier media network.

 foresightventures.com

 [@ForesightVen](https://twitter.com/ForesightVen)

Foresight New

The largest Multilingual Web3 Media in the Asia- Pacific.

 foresightnews.pro

 [@Foresight_News](https://twitter.com/Foresight_News)

Foresight X

An accelerator that provides funding and dedicated support to fuel Web3 start-ups.

 foresightx.net

 [@ForesightVen](https://twitter.com/ForesightVen)

CONTENTS

- \\ **Controversies Over 'What is Ethereum L2 and Rollups'.**
- \\ **What Kind Of Ethereum Rollups Are We Looking For?**

Controversies Over 'What is Ethereum L2 and Rollups'.

Dankrad: Validiums are not L2s .



Scarling	Tech	L2
Rollup	Validity/Fraud Proofs with data on L1 Ethereum.	✓
Plasma	Fraud Proofs with data kept off-chain.	✓
Validium	Validity Proofs with data kept off-chain.	✗
State Channel	Transact off-chain. Submit the state of channel on-chain.	✓
Sidechain	Seperate blockchain interact with ETH through bridges.	✗

Controversies Over 'What is Ethereum L2 and Rollups'.

It is unclear from Ethereum's statements whether Validiums are considered as L2s.






HOW DO VALIDIUMS SCALE ETHEREUM?

1. Off-chain data storage

Layer 2 scaling projects, such as optimistic rollups and ZK-rollups, trade the infinite scalability of pure off-chain scaling protocols (e.g., [Plasma](#)) for security by publishing some transaction data on L1. But this means the scalability properties of rollups is limited by data bandwidth on Ethereum Mainnet ([data sharding](#) proposes to improve Ethereum's data storage capacity for this reason).

Validiums achieve scalability by keeping all transaction data off-chain and only post state commitments (and validity proofs) when relaying state updates to the main Ethereum chain. The existence of validity proofs, however, gives validiums higher security guarantees than other pure off-chain scaling solutions, including Plasma and [sidechains](#). By reducing the amount of data Ethereum has to process before validating off-chain transactions, validium designs greatly extend throughput on Mainnet.

Picture from: <https://ethereum.org/en/developers/docs/scaling/validium/>




































Scarling	Tech	L2
Rollup	Validity/Fraud Proofs with data on L1 Ethereum.	
Plasma	Fraud Proofs with data kept off-chain.	
Validium	Validity Proofs with data kept off-chain.	
State Channel	Transact off-chain. Submit the state of channel on-chain.	
Sidechain	Seperate blockchain interact with ETH through bridges.	

Controversies Over 'What is Ethereum L2 and Rollups'.

L2BEAT is distinguishing Ethereum rollups from layer 2 solutions using non-ETH DA.

Show rollups only

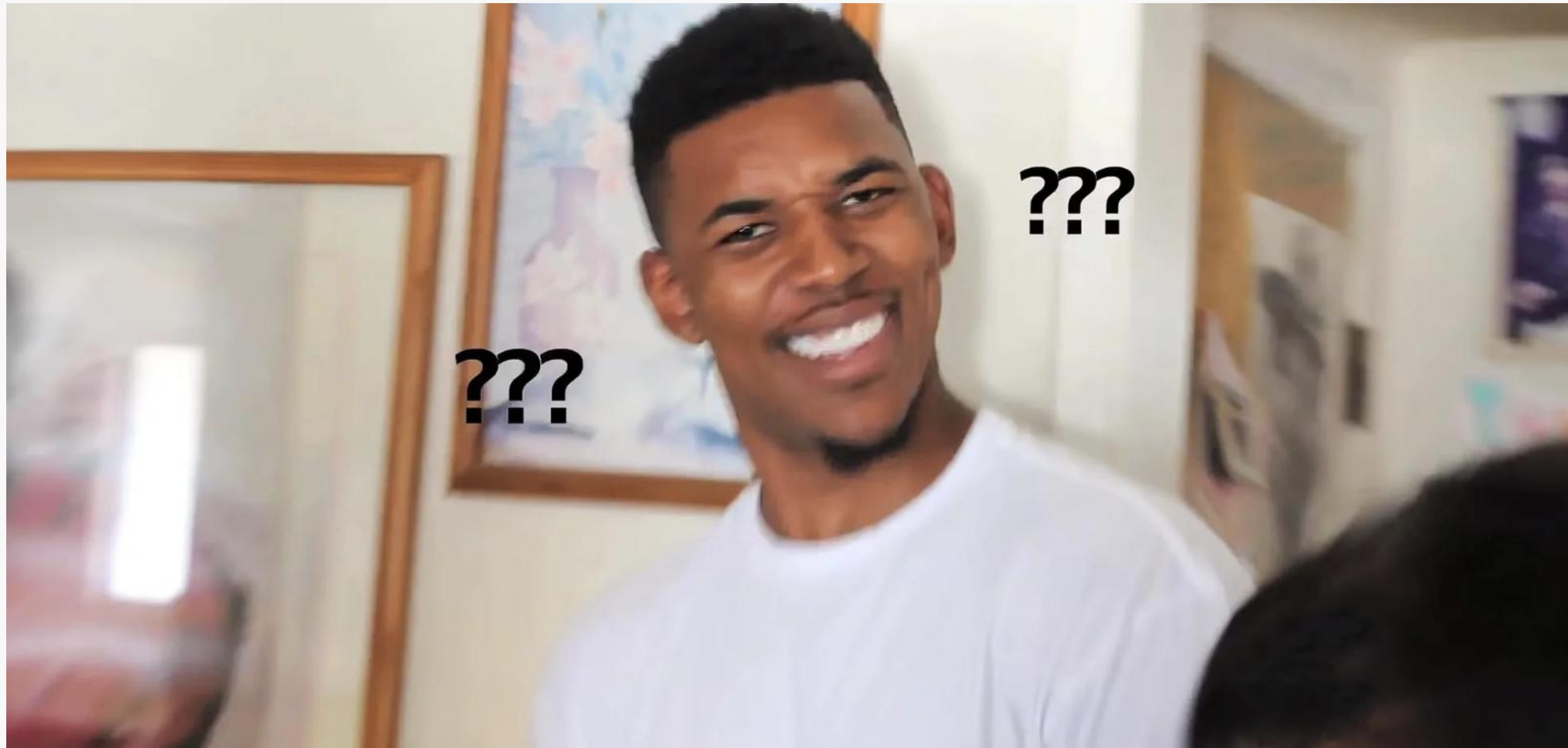
[Active projects](#) [Upcoming projects](#) [Archived projects](#)

#	NAME	RISKS ⓘ	TECHNOLOGY ⓘ	STAGE ⓘ	PURPOSE ⓘ	TOTAL ⓘ	MKT SHARE ⓘ
1	 Arbitrum One 		Optimistic Rollup 	STAGE 1	Universal	\$5.34B  4.89%	55.34%
2	 OP Mainnet 		Optimistic Rollup 	STAGE 0	Universal	\$2.54B  3.08%	26.32%
3	 zkSync Era 		ZK Rollup 	STAGE 0	Universal	\$400M  8.06%	4.14%
4	 dYdX		ZK Rollup 	STAGE 1	Exchange	\$334M  1.01%	3.46%
5	 Base 		Optimistic Rollup 	STAGE 0	Universal	\$245M  6.61%	2.54%
6	 Starknet		ZK Rollup	STAGE 0	Universal	\$143M  45.07%	1.48%
7	 Loopring		ZK Rollup 	STAGE 0	Tokens, NFTs, AMM	\$98.09M  3.18%	1.01%
8	 zkSync Lite		ZK Rollup 	STAGE 1	Payments, Tokens	\$76.97M  4.06%	0.80%

Picture from: <https://l2beat.com/scaling/summary> (Aug. 26, 2023)

Controversies Over 'What is Ethereum L2 and Rollups'.

Let's put aside the debate about these definitions.



What Kind Of Ethereum Rollups Are We Looking For?



Use Ethereum ▾ Learn ▾ Developers ▾ Enterprise ▾ Community ▾

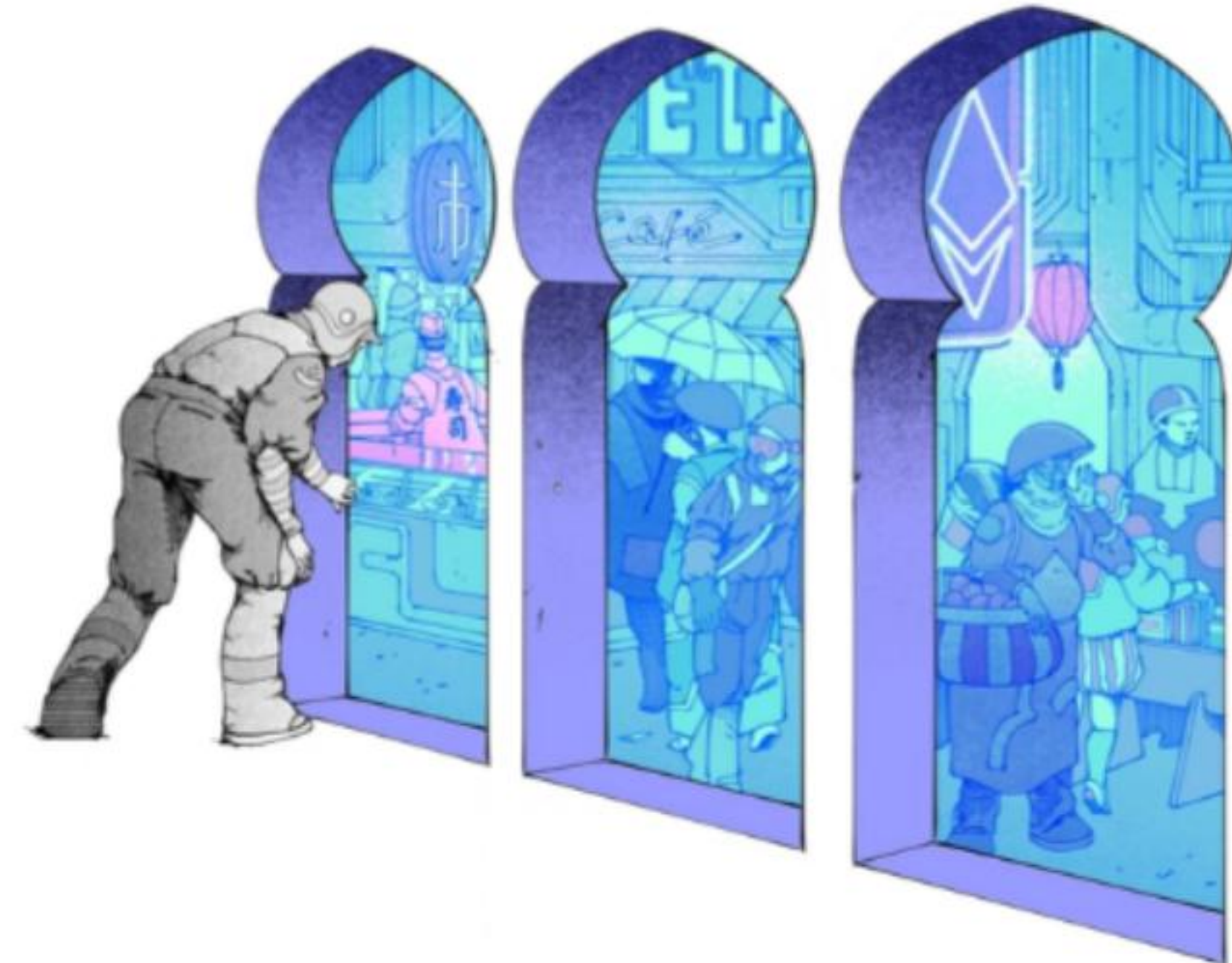


Languages EN

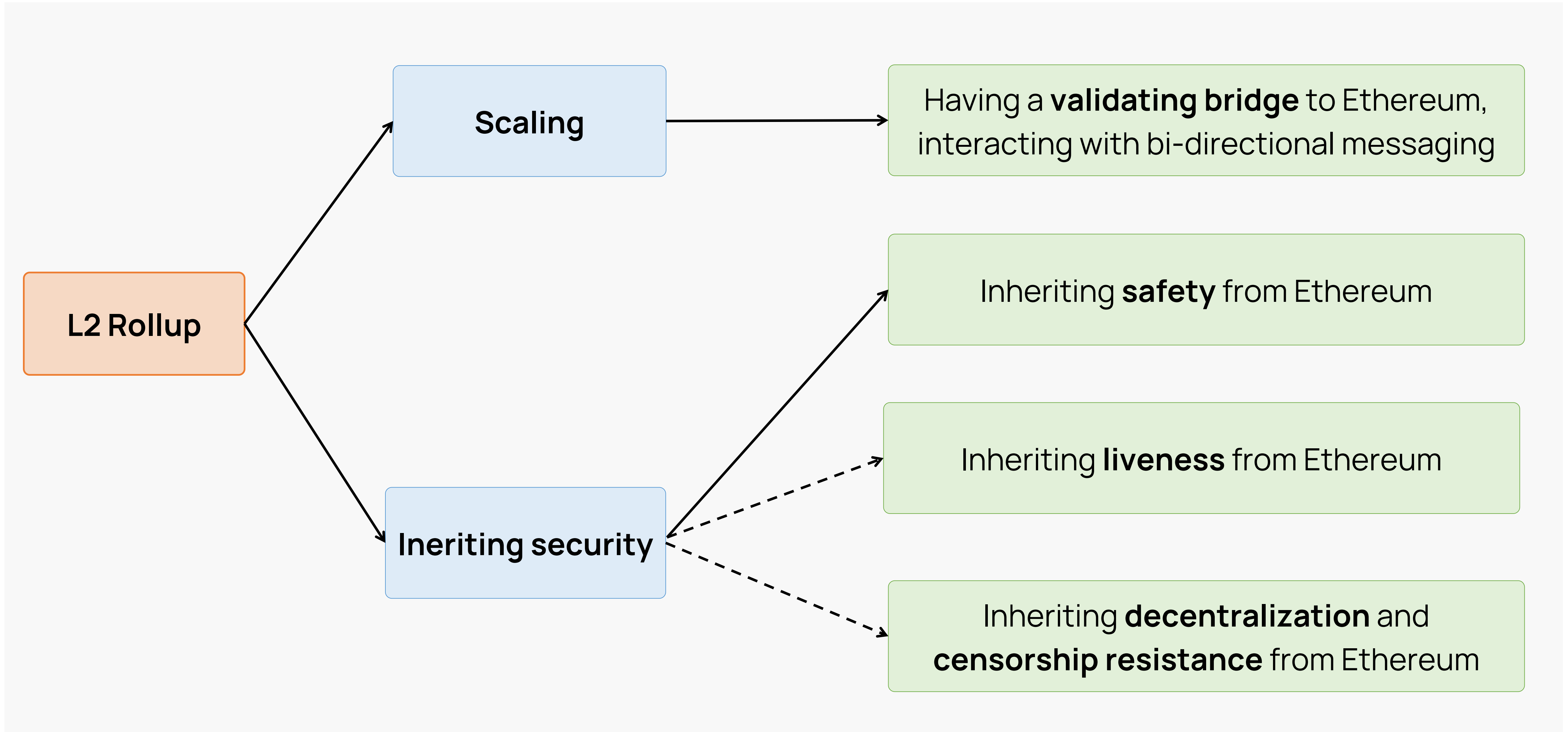
What is layer 2?

Layer 2 (L2) is a collective term to describe a specific set of Ethereum scaling solutions. **A layer 2 is a separate blockchain that extends Ethereum and inherits the security guarantees of Ethereum.**

Now let's dig into it a bit more. To do this we first need to explain layer 1 (L1).



What Kind Of Ethereum Rollups Are We Looking For?



Inheriting Safety From Ethereum



Rollups use Ethereum for data availability, transaction ordering and settlement.       

Reverting rollup transactions requires reverting Ethereum

DA

Inheriting **safety** from Ethereum

	Ethereum-centric			Celestia-centric		
	Monolith	Rollup	Validium	Sovereign Rollup	Settlement Rollup	Celestium
Data Availability	Ethereum	Ethereum	Off-chain	Celestia	Celestia	Celestia
Consensus	Ethereum	Ethereum	Ethereum	My Chain	Cevmos	Ethereum
Settlement	Ethereum	Ethereum	Ethereum	My Chain	Cevmos	Ethereum
Execution	Ethereum	My Chain	My Chain	My Chain	My Chain	My Chain

Inheriting Safety From Ethereum

Inheriting **safety** from Ethereum

DA



Rollups use Ethereum for data availability, transaction ordering and settlement.

Reverting rollup transactions requires reverting Ethereum

Ethereum

Block

Block

Block

Block

Upload by sequencer

Upload by proposer

Upload by prover

L2 Rollup

Tx Batch

State Root

Validity Proof

Execute and generate zk proof

Inheriting Safety From Ethereum

Inheriting **safety**
from Ethereum

DA

State
validation



Rollups use Ethereum for data availability, transaction ordering and settlement.



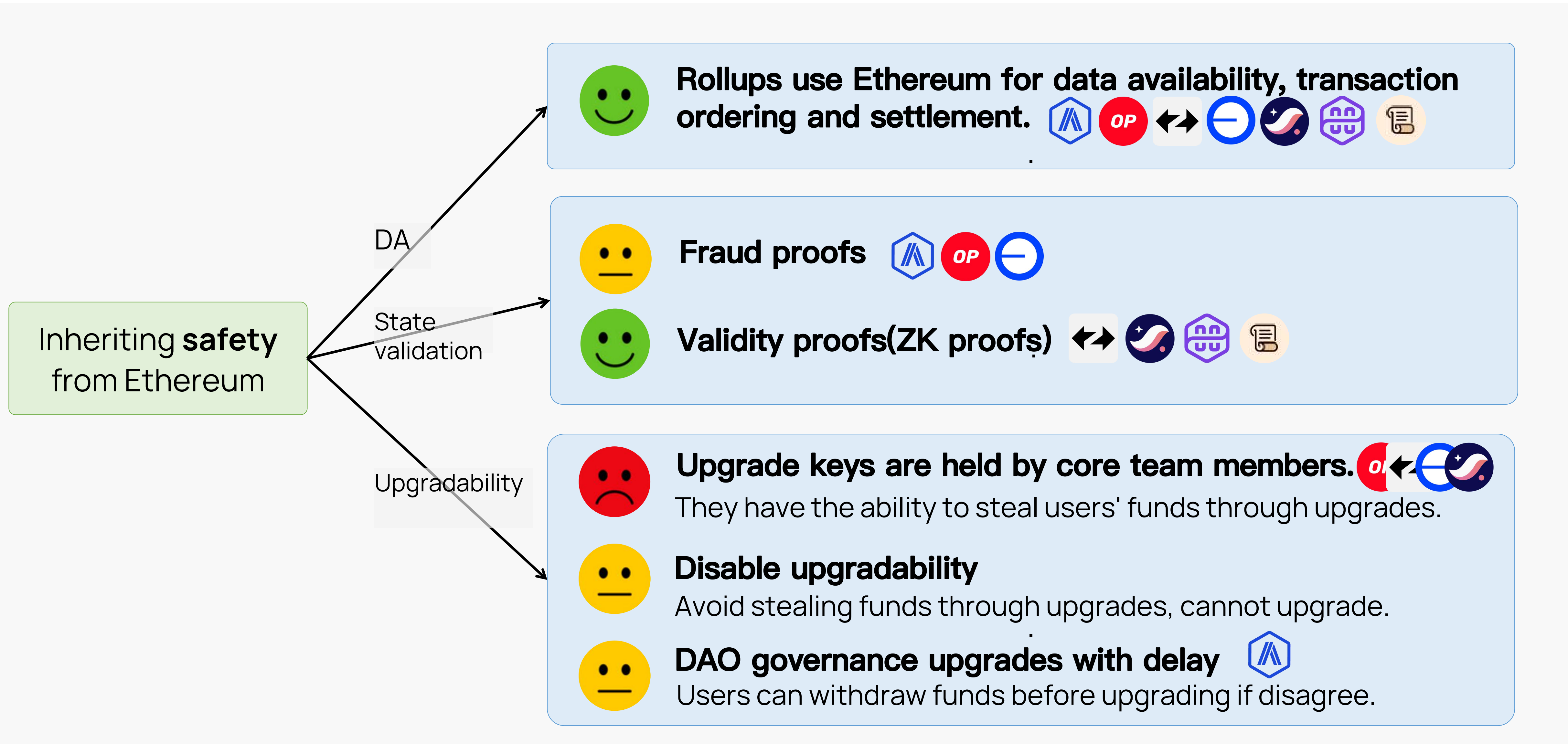
Optimistic rollups use fraud proofs for state validation
EVM equivalent, slower finality.



ZK rollups use validity proofs(ZK proofs)
Enhanced security, faster finality, not fully EVM equivalent.



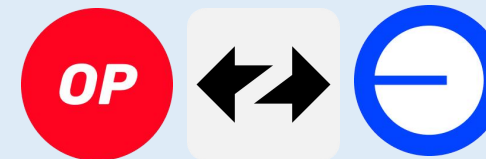
Inheriting Safety From Ethereum



Inheriting Liveness From Ethereum



No escape mechanism



Rollup would stop and users would not be able to withdraw assets.



Forced exit and forced execution

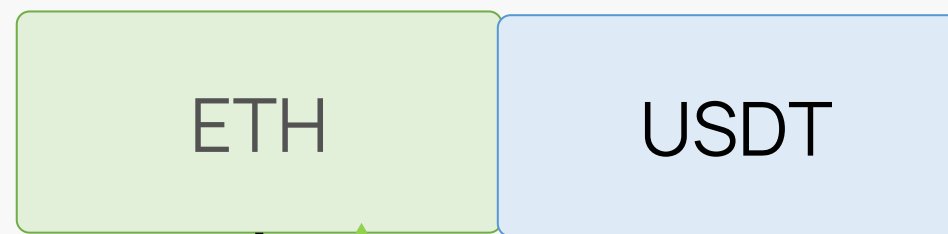


User withdraw collateral when sequecner and proposer failure.

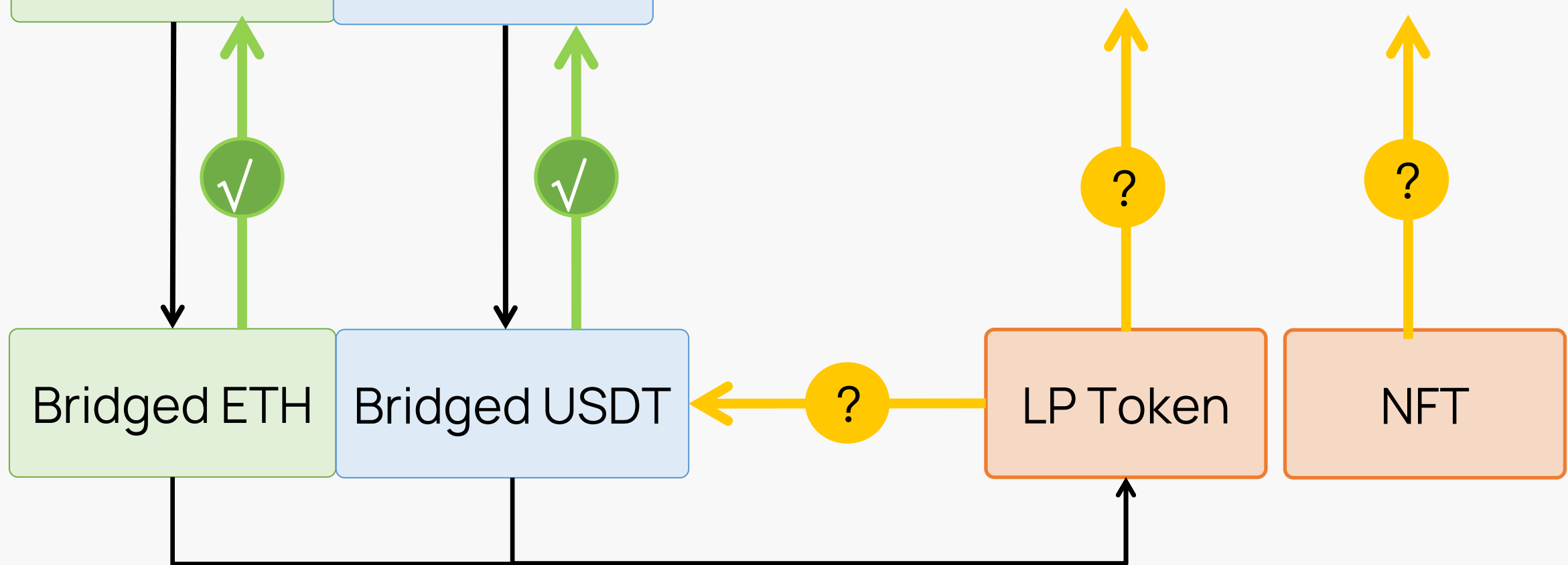
Sequencer and proposer failure

Inheriting **liveness** from Ethereum

Ethereum



L2 Rollup



Inheriting Liveness From Ethereum

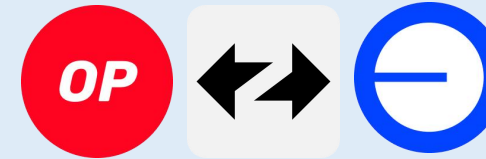
Inheriting **liveness**
from Ethereum

Sequencer and
proposer failure

Decentralization



No escape mechanism



Rollup would stop and users would not be able to withdraw assets.



Forced exit and forced execution



User withdraw collateral when sequencer and proposer failure.



Self sequence and self propose



Anyone can act as a sequencer and proposer to make it live.

Inheriting **decentralization** and **ensorship resistance** from
Ethereum.

Inheriting Decentralization and Censorship Resistance from Ethereum.

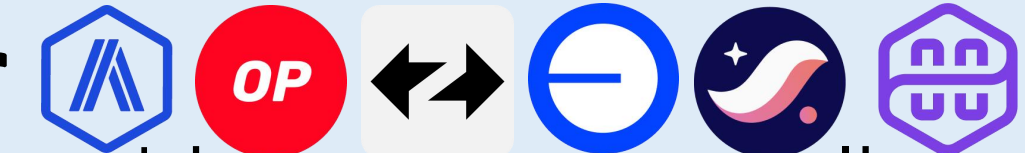
Inheriting **decentralization** and **censorship resistance** from Ethereum.

Sequencer

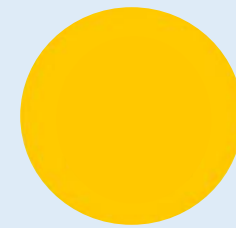
Prover



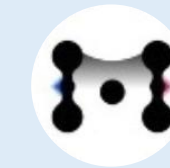
Sole centralized sequencer



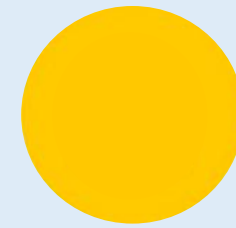
Single point of failure, not censorship resistance, malignant MEV.



PoS/BFT decentralized sequencers

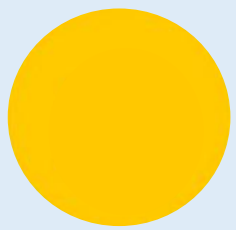


Stake to join the sequencer set, run BFT to consensus tx batches.



MEV auctions

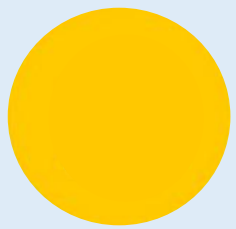
Auctioning off sequencing rights to the highest bidder.



Proof-of-efficiency



Permissionless sequencer, anyone can submit tx batches.



Shared sequencers

Node network provides sequencing-as-a-service to multiple rollups



Decentralized ZKP prover

Other Things to Consider

How to balance incentives between sequencers and ZKP provers?

After the EIP4844 upgrade, blob data only saved for 1-3 months, will it affect the Rollups?

How do we reduce Rollups' transaction fees?

What kind of Ethereum rollups are we looking for?

- We want to rollups inherit not only the **safety** of Ethereum but also its **liveness, decentralization, and censorship resistance**.
- It's very difficult to create an L2 Rollup without introducing any additional trust assumptions. The features of **upgradability, decentralized sequencers, and trusted setup for zero-knowledge proofs** can all introduce additional trust assumptions.
- The upgrade of **L1 rollup smart contracts should be governed by a DAO** and **have a delay** to allow users to have enough time to exit if they disagree with the upgrade. However, this method also added some security assumptions to the system.
- Instead of using a single sequencer, **use decentralized sequencers** to achieve better liveness, decentralization, and censorship resistance.



 @ForesightVen

 @Foresight_News

 @0xmaggie5

CONNECT WITH US!