

NOVEMBER 2024

L2BEAT

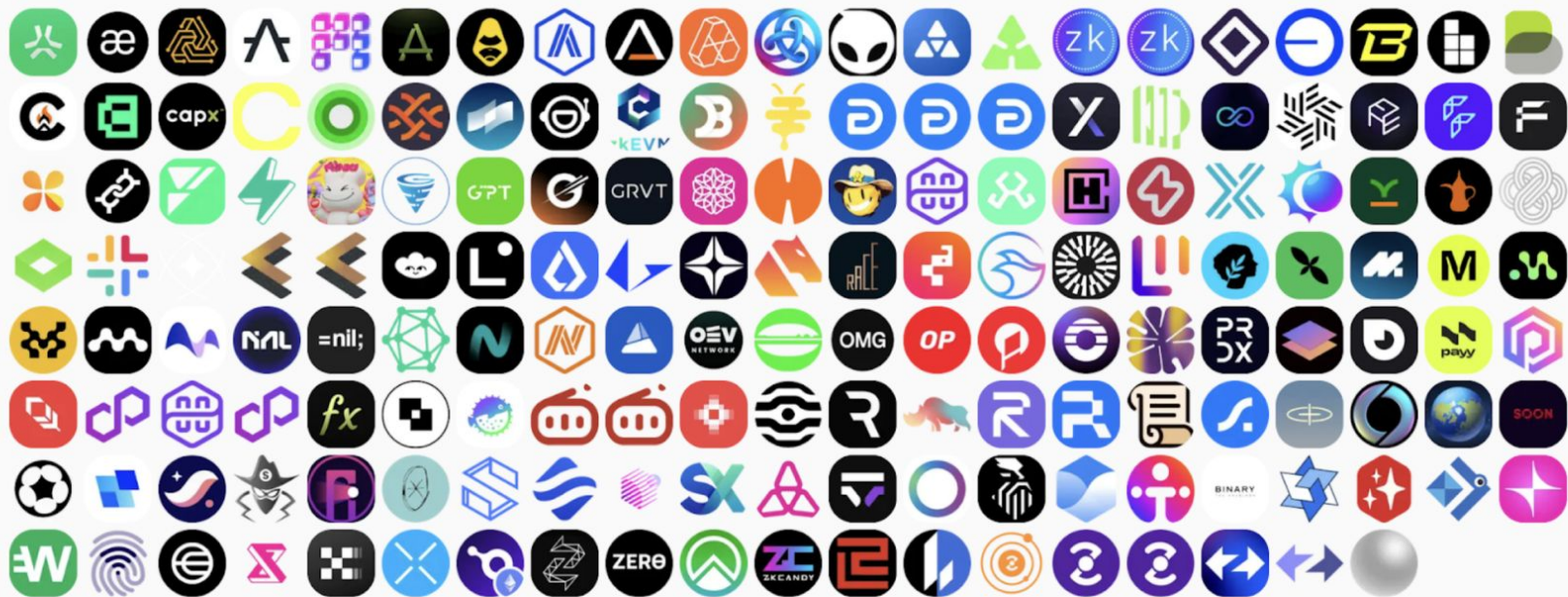
THE REAL STATE OF L2s

by Bartek Kiepuszewski



4 years after announcing Rollup centric roadmap - **Where are we today ?**

We have launched almost 50 Rollups
and over 50 alt-DA L2s



4 years after announcing Rollup centric roadmap - **Where are we today ?**

We have put almost **40B\$ of TVL on L2s**

Value Locked

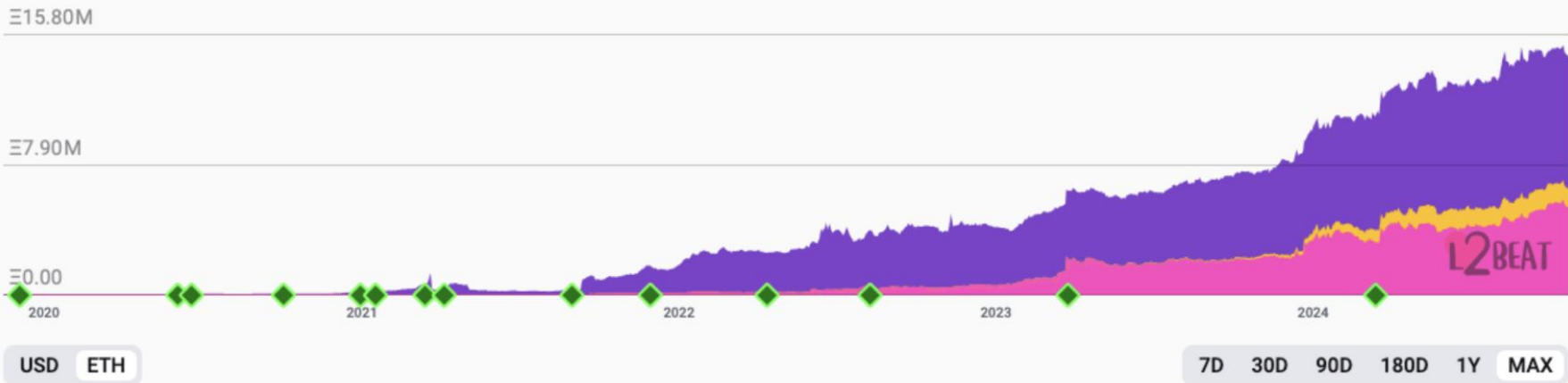
Source: L2BEAT.com

Total value locked stacked by type

2019 Nov 15 — 2024 Oct 22

Ξ14.50M

∞ / All time



4 years after announcing Rollup centric roadmap - **Where are we today ?**

We have made a good progress on scaling Ethereum

TPS

Source: L2BEAT.com

Daily average transactions per second

2020 May 31 — 2024 Oct 21

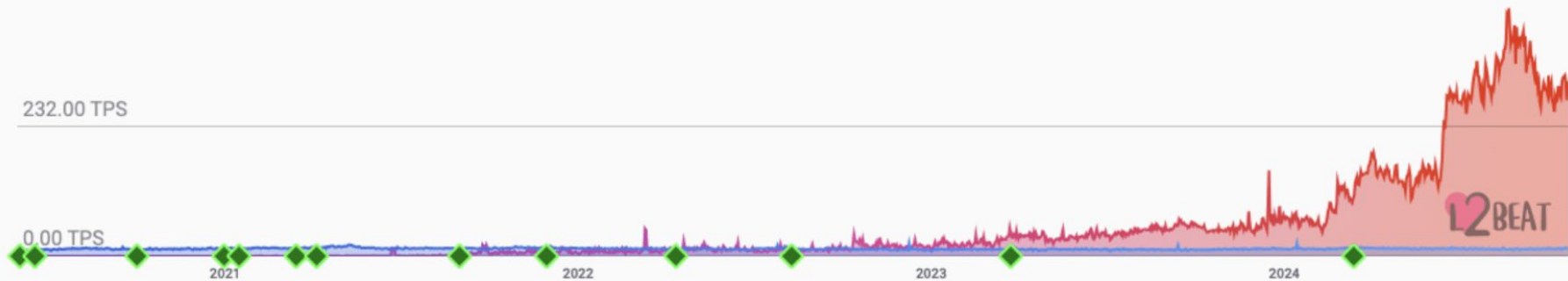
311.01 TPS

Scaling factor: 22.79x ⓘ

464.00 TPS

232.00 TPS

0.00 TPS



LOG

LIN



ETH Mainnet Transactions

30D

90D

180D

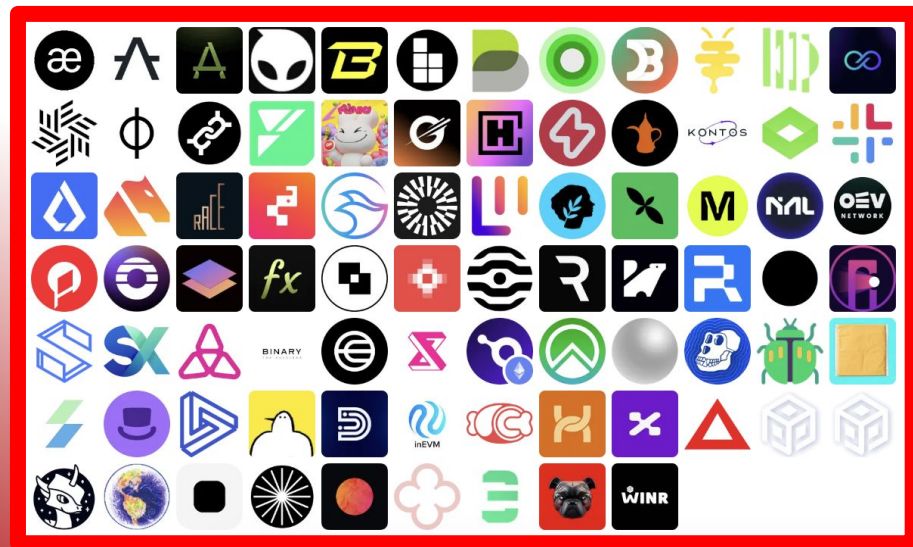
1Y

MAX

But...

Most L2s **do not**
have a proof system

Proof systems









































Most L2s **do not**
use Security Councils

Security Councils



**Most alt-DA L2s are set up with
abysmal DA trust assumptions**

16	 HYCHAIN	Optimum 	DAC	1/1 DAC Members
17	 Sanko L3 on Arbitrum One	Optimum 	DAC	1/1 DAC Members
18	 Myria	Validium 	DAC	2/5 DAC Members
19	 Aleph Zero EVM 	Optimum 	DAC	1/2 DAC Members
20	 Edgeless	Optimum 	DAC	1/1 DAC Members
21	 Everclear Hub 	Optimum 	DAC	1/2 DAC Members
22	 Pay Chain	Validium 	DAC	1/2 DAC Members
23	 GPT Protocol	Validium 	DAC	1/2 DAC Members
24	 Witness Chain 	Validium 	DAC	1/2 DAC Members
25	 Degen Chain L3 on Base	Optimum 	DAC	1/1 DAC Members
26	 L3X  L3 on Arbitrum One	Optimum 	DAC	1/1 DAC Members
27	 Molten L3 on Arbitrum One	Optimum 	DAC	1/1 DAC Members
28	 PlayBlock   L3 on Arbitrum Nova	Optimum 	DAC	1/2 DAC Members
29	 PoP Apex L3 on Arbitrum One	Optimum 	DAC	1/1 DAC Members
30	 PoP Boss L3 on Arbitrum One	Optimum 	DAC	1/1 DAC Members
31	 RARI Chain L3 on Arbitrum One	Optimum 	DAC	1/1 DAC Members

Data Availability Committees

- Arbitrum Nova (5/6)
- XAI (8/9)
- ImmutableX (5/7)
- Mantle (9/10)*



In most L2s permissioned
operators **can steal or
freeze**
your funds



So why we should care about proof systems?

**→ Proof System allows for permissionless exit
in case all permissioned actors are down**

Proof System (Stage1) improves trust
assumptions for the Security Council

Proof System (Stage2) allow you to remove any
intermediary (profound regulatory implications)



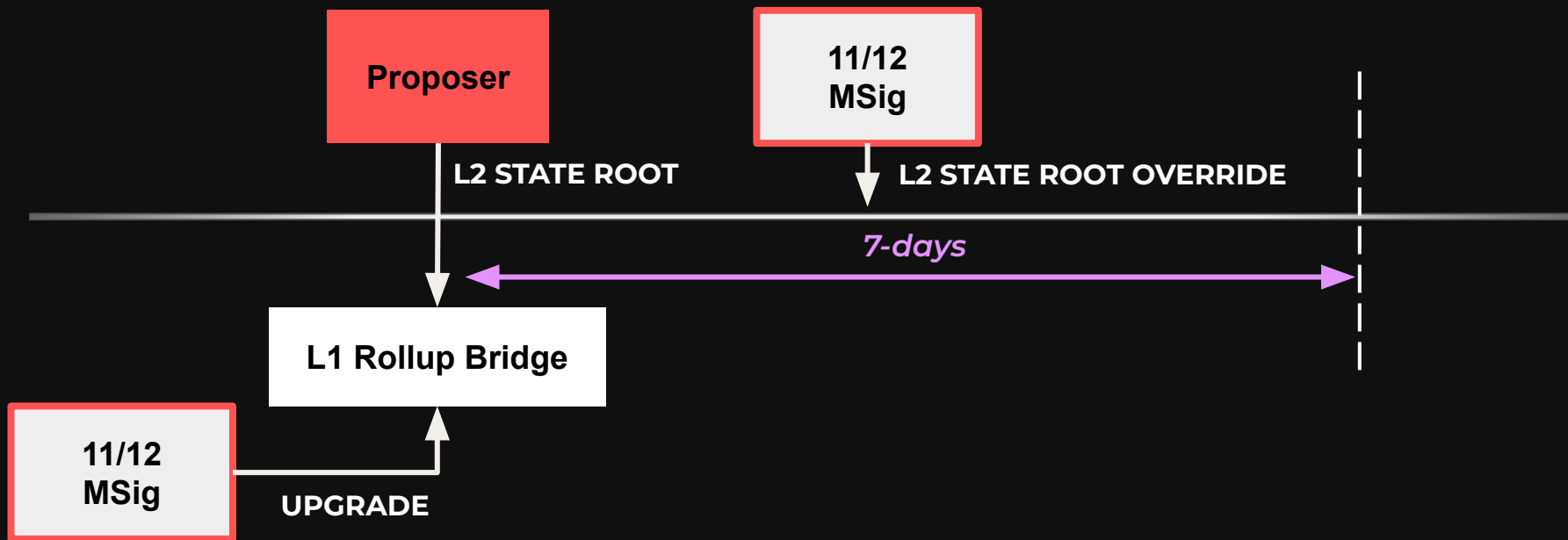
V3 Product Sunset

Proof System allows for permissionless exit
in case all permissioned actors are down

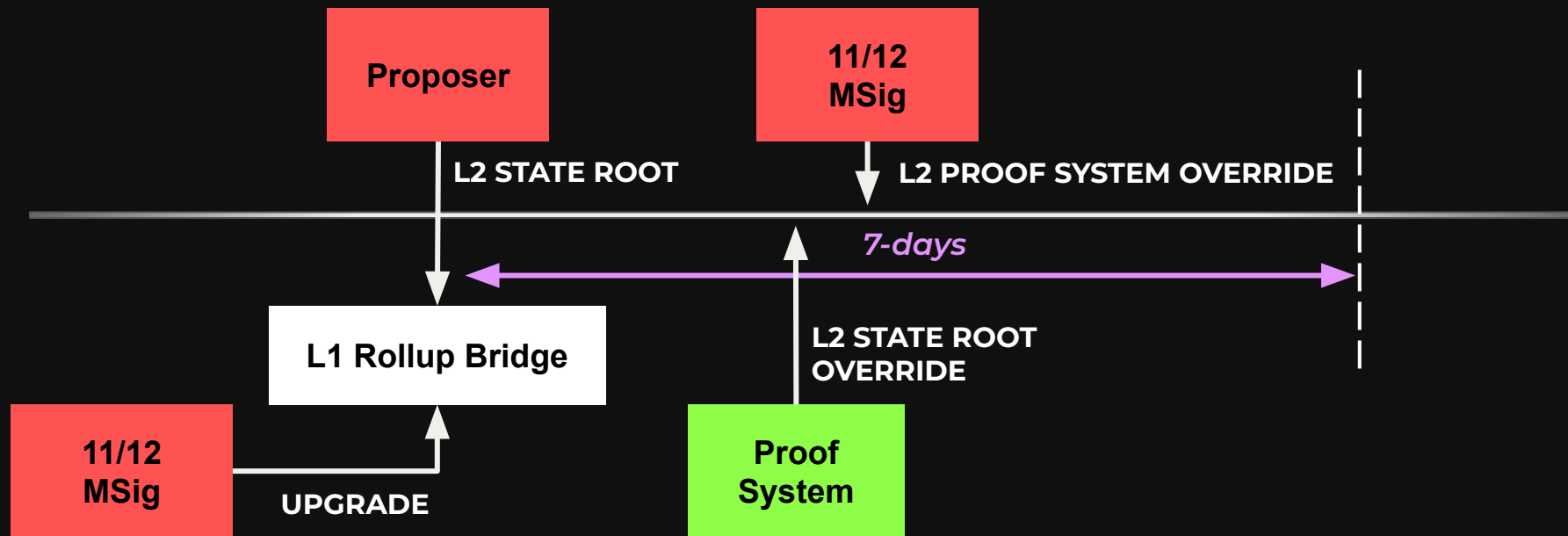
➔ **Proof System (Stage1) improves trust
assumptions for the Security Council**

Proof System (Stage2) allow you to remove any
intermediary (profound regulatory implications)

Malicious Proposer needs to bribe **2/12** to steal funds.



Malicious Proposer needs to bribe **11/12** to steal funds.



Proof System allows for permissionless exit
in case all permissioned actors are down

Proof System (Stage1) improves trust
assumptions for the Security Council

➔ **Proof System (Stage2) allow you to
remove any intermediary (profound
regulatory implications)**



Tomasz K. Stańczak

@tkstanczak



In the recently published 6-part Ethereum roadmap discussion, [@VitalikButerin](#) highlighted that "our task is to bring the rollup-centric roadmap to completion (...) while preserving the robustness and decentralization that makes the Ethereum L1 special."

We are announcing the Rollup Roadmap (surge.wtf) — our commitment to the future of the Ethereum rollup ecosystem. We want teams building on Ethereum to utilize the best set of open-source solutions that provide optimal performance while leveraging Ethereum's security. We believe that we have built these tools at Nethermind and plan to improve them further.

We are building Surge — a Stage 2 at launch, based rollup ([@taikoxyz](#) stack), which will allow us to showcase the tools, infrastructure, protocol design, and future directions that will benefit all EVM rollups and, over time, the Ethereum mainnet. The name "Surge" represents our alignment with the Ethereum roadmap and the work of all core development teams.

xit

→ Proc
rem
regu

Why Security Councils and not simple MultiSigs ?

Multichain's recent problems have some suspicious of a rug pull

Multichain's exploit is potentially the result of administrator keys being compromised. While it's possible those keys were taken by an external hacker, many security experts and other analysts think this exploit could be an inside job or rug pull, due in part to recent issues suffered by Multichain.

Multichain's recent problems have some suspicious of a rug pull

Multichain's exp
it's possible tho
analysts think t
suffered by Mul

UK Court Ordered Oasis to Exploit Own Security Flaw to Recover 120k wETH Stolen in Wormhole Hack

Around \$140 million worth of wrapped ether, stolen last year in a hack on the Wormhole token bridge, has been recovered using a counter-exploit on the Oasis.app vault in which it was being held. A UK court ordered Oasis to carry out the recovery action.

Multichain's recent problems have some suspicious of a rug pull

Multichain's exploit
it's possible that
analysts think that
suffered by

UK Court Ordered Oasis to Exploit Own Security Flaw to Recover 120k



Pop Punk ✓  @PopPunkOnChain · Oct 16



Radiant's multisig had 11 signers, but only required 3 signatures to execute transactions.

Attacker controlled *at least* 3 of them and were able to execute this attack.

3/11 is uncomfortably low for a protocol of this size.

Security Council vs Proof Systems vs Stages

	Who can steal funds ?
STAGE 0 Rollup with no Security Council	Malicious operator
STAGE 0 Rollup with Security Council	Malicious operator + dishonest Security Council minority
STAGE 1 Rollup with a proof system	Dishonest Security Council majority
STAGE 2 Rollup with a multiproof system	No-one

Do we have the right incentives?

Do



vitalik.eth ✓ @VitalikButerin · Sep 12

...

I take this seriously. Starting next year, I plan to only publicly mention (in blogs, talks, etc) L2s that are **stage 1+**, with *maybe a short grace period* for new genuinely interesting projects.

It doesn't matter if I invested, or if you're my friend; **stage 1** or bust.

Multiple
[Show more](#)

The ecosystem's standards need to become stricter: so far, we have been lenient and accepted any project as long as it claims to be "on a path to decentralization". By the end of the year, I think our standards should increase and we should only treat a project as a rollup if it has actually reached at least stage 1.

After this, we can cautiously move toward stage 2: a world where rollups truly are backed by code, and a security council can only intervene if the code "provably disagrees with itself" (eg. accepts two incompatible state roots, or two different implementations give different answers). One path toward doing this safely is to [use multiple prover implementations](#).



vitalik.eth ✓ @VitalikButerin · Sep 12

I take this seriously. Starting next year, I plan to only publicly mention (in blogs, talks, etc) L2s that are **stage 1+**, with *maybe a short grace period* for new genuinely interesting projects.

It doesn't matter if I invested, or if you're my friend; **stage 1** or bust.



vitalik.eth ✓ @VitalikButerin · Mar 28

Replying to @VitalikButerin

Fourth, continue improving on security.

We need to raise our standards. By the end of the year, I think we should only refer to rollups that are at least **stage 1** as "rollups".

code, and a security council can only intervene if the code "provably disagrees with itself" (eg. accepts two incompatible state roots, or two different implementations give different answers). One path toward doing this safely is to use multiple prover implementations.

<input type="checkbox"/> Rollups only Type Stack Stage Purpose RaaS Host Chain <input type="checkbox"/> Exclude						
#	NAME	RISKS	TYPE	STAGE	TOTAL VALUE LOCKED	
1	Arbitrum One		Optimistic Rollup	STAGE 1	\$15.30B ▲ 18.5%	
2	Base		Optimistic Rollup OP	STAGE 0	\$9.14B ▲ 17.5%	
3	OP Mainnet		Optimistic Rollup OP	STAGE 1	\$6.49B ▲ 17.8%	
4	Mantle		Optimium OP	N/A	\$1.89B ▲ 23.5%	
5	Blast		Optimistic Rollup OP	STAGE 0	⚠ \$1.53B ▲ 19.2%	
6	Scroll		ZK Rollup	STAGE 0	\$1.12B ▲ 16.5%	
7	Linea		ZK Rollup	STAGE 0	\$1.02B ▲ 26.5%	
8	ZKsync Era		ZK Rollup ↔	STAGE 0	\$979.22M ▲ 23.4%	
9	Starknet		ZK Rollup	STAGE 0	\$775.06M ▲ 27.2%	
10	Manta Pacific		Optimium OP	N/A	\$621.36M ▲ 31.9%	

Rollups

STAGE 0

No proof system rollups

STAGE 1

Proof system rollups + Security
Council

STAGE 2

Multiproof systems

Validiums + Optimiums

alt-DA L2s

Rollups

STAGE 0

No proof system rollups

STAGE 1

Proof system rollups + Security
Council

STAGE 2

Multiproof systems

Validiums + Optimiums

STAGE 0+ ?

(proof system rollups)

alt-DA L2s

IT. IS. TIME. TO. GROW. UP.



Rollups

STAGE 0

Proof system rollups

STAGE 1

**Proof system rollups
+ Security Council**

STAGE 2

Multiproof systems

Rollups

STAGE 0

Proof system rollups

STAGE 1

Proof system rollups
+ Security Council

STAGE 2

Multiproof systems

alt-DAs

alt-DA L2s
with proof system

and

reasonable DA
guarantees

Rollups

STAGE 0

Proof system rollups

STAGE 1

Proof system rollups
+ Security Council

STAGE 2

Multiproof systems

alt-DAs

alt-DA L2s
with proof system

and

reasonable DA
guarantees

“Others”

Rollups
with no proof system

alt-DA L2s
with no proof system
Or
no DA guarantees

Type ▾

Stack ▾

Stage ▾

Purpose ▾

RaaS ▾

Host Chain ▾

☐ Exclude associated tokens

Rollups 51

Validiums & Optimiums 65























Others

#	NAME	RISKS	TYPE ⓘ	STAGE	TOTAL VALUE LOCKED ⓘ	PAST DAY TPS ⓘ
Stage 2 & 1 projects						
1	Arbitrum One		Optimistic Rollup	STAGE 1	\$15.44B ▲18.1%	25.66 ▲26.9%
2	OP Mainnet		Optimistic Rollup	STAGE 1	\$6.55B ▲18.7%	10.80 ▲13.3%
3	ZKsync Lite		ZK Rollup	STAGE 1	\$59.90M ▲24.3%	0.02 ▲67.3%
4	DeGate V1		ZK Rollup	STAGE 2	\$52.32M ▲3.92%	0.52 ▲43.3%
5	dYdX v3		ZK Rollup	STAGE 1	\$42.56M ▼18.4%	0.00 0.00%
6	Fuel v1		Optimistic Rollup	STAGE 2	<\$1K ▲30.0%	No data
Stage 0 projects						
7	Base		Optimistic Rollup	STAGE 0	\$9.09B ▲18.0%	78.85 ▲0.41%
8	Blast		Optimistic Rollup	STAGE 0	\$1.55B ▲20.8%	6.05 ▲0.92%
9	Scroll		ZK Rollup	STAGE 0	\$1.15B ▲18.2%	1.54 ▲22.2%
10	Linea		ZK Rollup	STAGE 0	\$1.03B ▲28.1%	2.74 ▲20.2%

Rollups 45

Validiums & Optimiums 60

Others 11

#	NAME	RISKS	PROPOSER	CHALLENGER	UPGRADER
1	 Blast		1 EOA Blast	3/5 Blast	3/5 Blast
2	 BOB		1 EOA Conduit	4/6 BOB	4/6 BOB
3	 Linea		2 EOAs Linea	None	4/8 Linea
4	 Lisk		1 EOA Gelato	6/9 Gelato	6/9 Gelato
5	 Mode		1 EOA Mode	4/6 Mode	5/7 + 10/13 OP Foundation + Superchain SC
6	 World Chain		1 EOA Alchemy	1 EOA Alchemy	3/6 Alchemy
7	 Fraxtal		1 EOA Fraxtal	3/5 Fraxtal	3/5 Fraxtal
8	 Gravity		1 EOA Conduit	1 EOA Conduit	4/7 Conduit
9	 Manta Pacific		1 EOA Manta	1 EOA Manta	5/7 Manta
10	 Mantle		1 EOA Mantle	3/7 Mantle	6/11 Mantle
11	 Metis		1 EOA Metis	4/9 Metis	4/9 Metis

It's not enough to “declare” the proof system

- we will put a lot of effort to analyse different proof systems
 - both ZK and Optimistic.
- auditing standards are needed
- trust assumptions must be clearly communicated
- proof system cannot be “hidden” behind unreasonably small whitelist
- evaluation by L2BEAT researchers

Further details: l2beat.com

Thank you!



bartek.eth

@bkiepuszewski