Ethereum needs native L2

Martin Köppelmann

Founder of Gnosis, Ethereum community member

“Rollups inherit the security of Ethereum”


SECURED BY
ETHEREUM

#	NAME	RISKS	TYPE	STAGE
1	Arbitrum One		Optimistic Rollup	STAGE 1
2	Base		Optimistic Rollup OP	STAGE 0
3	OP Mainnet		Optimistic Rollup OP	STAGE 1
4	Mantle		Optimium OP	N/A
5	Blast		Optimistic Rollup OP	STAGE 0
6	Linea		ZK Rollup	STAGE 0
7	Scroll		ZK Rollup	STAGE 0
8	ZKsync Era		ZK Rollup	STAGE 0

Funds can be stolen if

1. an invalid state root is

Funds can be stolen if

lished state. Fraud proofs assume at least one honest and able validator,

Funds can be stolen if

ular and emergency upgrades must be

upgrades.

1. no validator checks the published state. Fraud proofs assum
2. a contract receives a malicio

Funds can be stolen if

1. validators relay a fake message to Gnosis chain to mint more tokens than there are locked on Eth
2. v
es
3.
4.

isting holders from being able to bring their funds back to Ethereum,

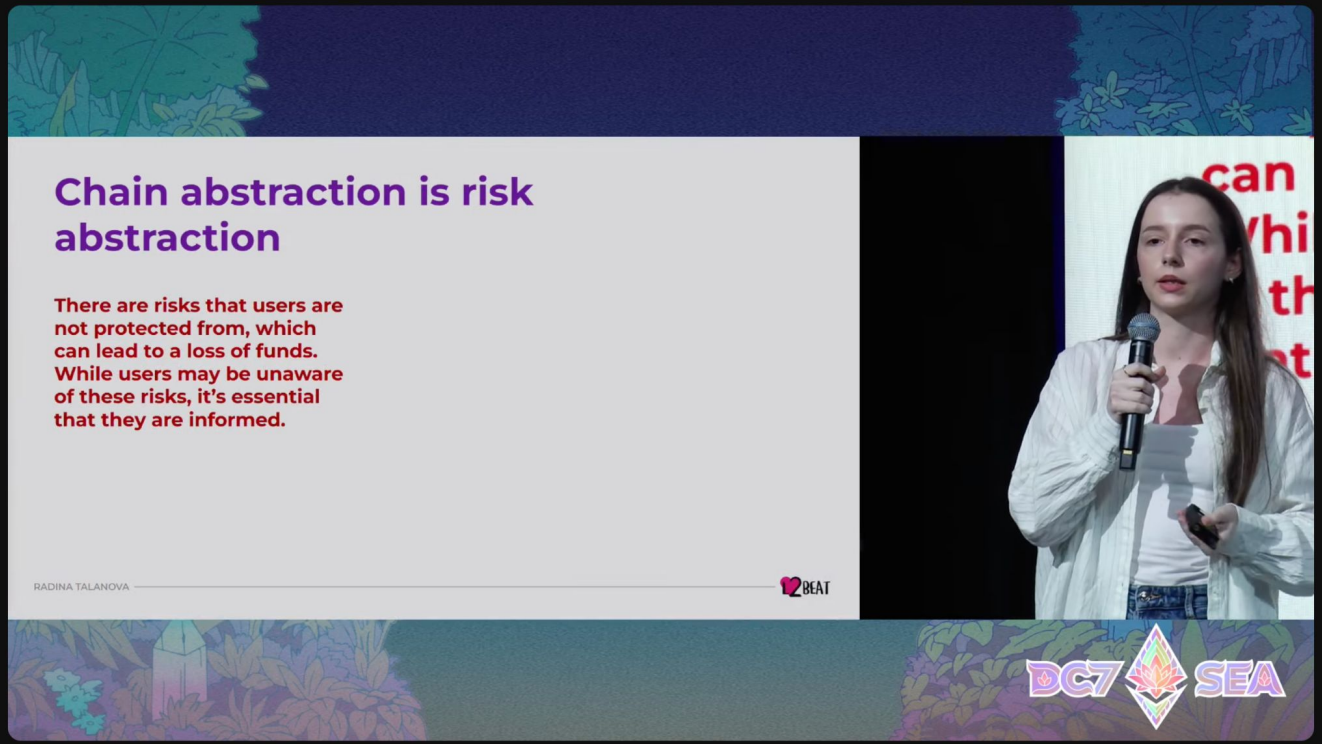
withdraw tokens from Ethereum

Funds can be stolen if

1. a contract receives a malicious code upgrade. There is a 17d 8h delay on code upgrades,
2. a contract receives a malicious code upgrade. There is a 17d 8h delay on code upgrades unless upgrade is initiated by the Security Council in which case there is no delay,
3. none of the whitelisted verifiers checks the published state. Fraud proofs assume at least one honest and able validator (CRITICAL).

or,

g1



Radina Talanova, *Chain Abstraction is Risk Abstraction*

But there are other risks even L2
Beat does not cover...

Description

State contention causes MEV, prevents parallelization, breaks gas simulation, causes transactions to revert, etc. etc. We'll discuss state contention in practical and theoretical systems (e.g. OS threads and type systems) and how/why synchronization primitives developed. We'll cover why state is contentious, what state is contentious, what can be accomplished by making state non-contentitious, and strategies for refactoring existing systems to reduce contention.

Martin Köppelmann 🦉💳
@koeppelmann

Great talk by @_prestwich where he explains that a user of Aave or Compound on centralized sequencer chains like Base, Optimism, or Arbitrum can be prevented from withdrawing funds FOREVER.
Turns out, having home validators with the ability to build blocks ACTUALLY MATTERS.

> imposes only an extremely small borrow cost.[10] Furthermore, the collateral is reusable for all censorship, as the borrow is never held open. As a result, a user of AAVE or Compound on Optimism (or Arbitrum or any other centrally-sequenced rollup) has **no guarantee that they will be able to withdraw collateral *ever***. The sequencer can censor any withdrawal from any lending market at any time. Forced inclusion is simply not sufficient to protect users against censorship.

8:32 PM · Nov 14, 2024 · **1,946** Views

View post engagements

5 9 40 4

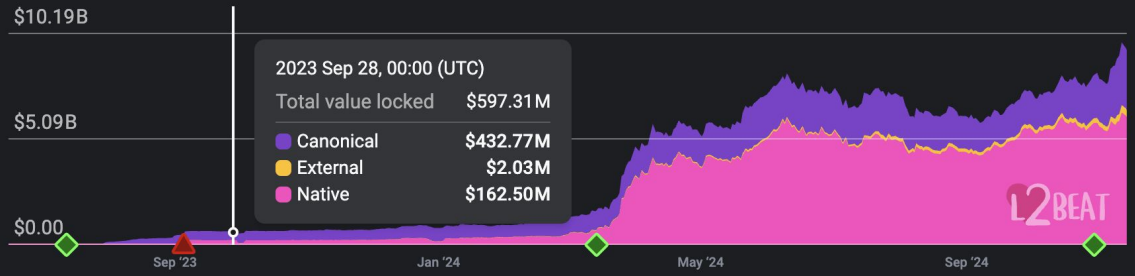
What does the *security of Ethereum* actually mean?

Security is culture and process.

1 Value Locked

2023 Jun 16 — 2024 Nov 13

7D 30D 90D 180D 1Y MAX



USD ETH Tokens

If most assets are not bridged from Ethereum, and sequencing is also not done by Ethereum the connection to Ethereum is reduced to occasional checkpointing.

Rollups can choose one...

- Their own sequencing
- Fast/ almost instant confirmation (if you trust the sequencer)
- Only delayed “reads” into Ethereum
- Capture their own MEV

Rational choice if you want to optimize for contectivness to Tradfi, other chain + UX advantages

- Ethereum as sequencer (“based”)
- Slower, but synchronous (fastest) reads into Ethereum L1 state
- Liveness guarantees of Ethereum

Rational choice if you want to optimize for connectivity to Ethereum “economic zone”

Rollups can choose one...

- Their own sequencing
- Fast/ almost instant confirmation (if you trust the sequencer)
- Only delayed “reads” into Ethereum
- Capture their own MEV

Rational choice if you want to optimize for contectivness to Tradfi, other chain + UX advantages

- Ethereum as sequencer (“based”)
- Slower, but synchronous (fastest) reads into Ethereum L1 state
- Liveness guarantees of Ethereum

Rational choice if you want to optimize for connectivity to Ethereum “economic zone”

Less than 1% of TVL of rollups choose to be “based”

My proposal is for Ethereum itself to develop zk-proven EVM equivalent rollups and deploy 128 equal instances of it.

What would it mean to be built by Ethereum?

Don’t even think of introducing a multisig

At least two independent implementation (proof systems)

Rigorous testing, thousands of eyes scrutinizing every line of code

L2

Wide range of designs

Based L2

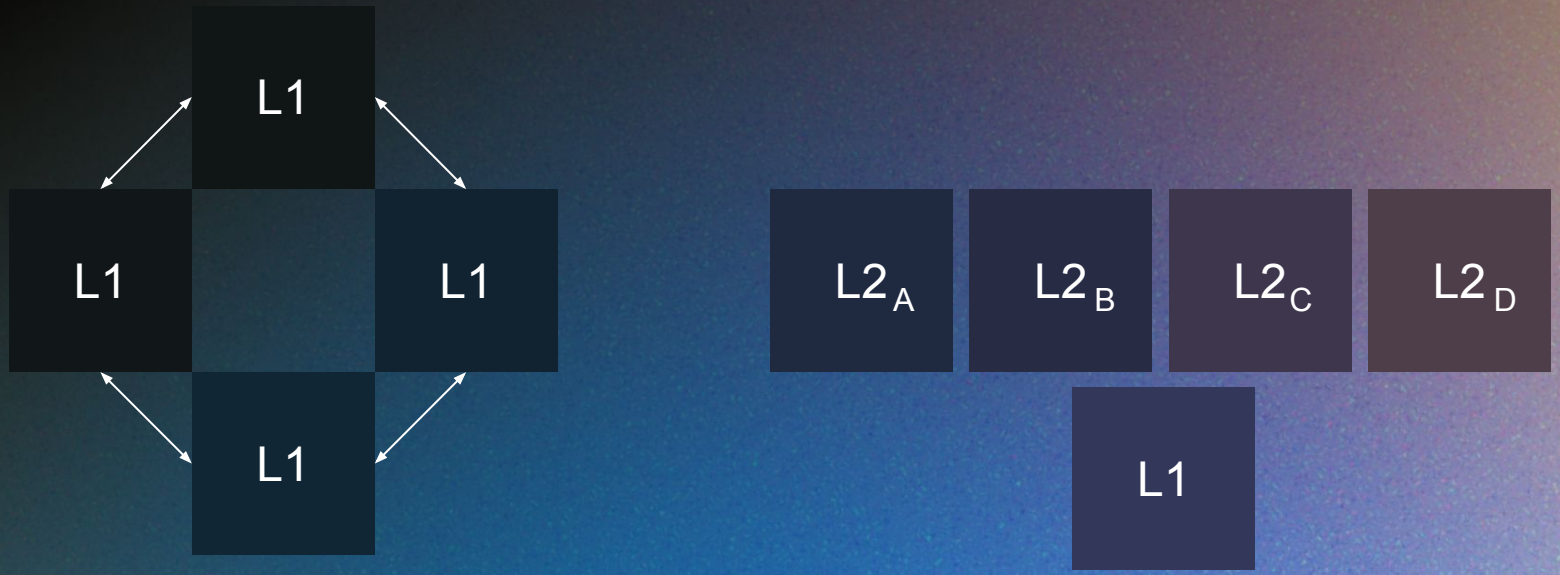
Sequencing / block building by Ethereum

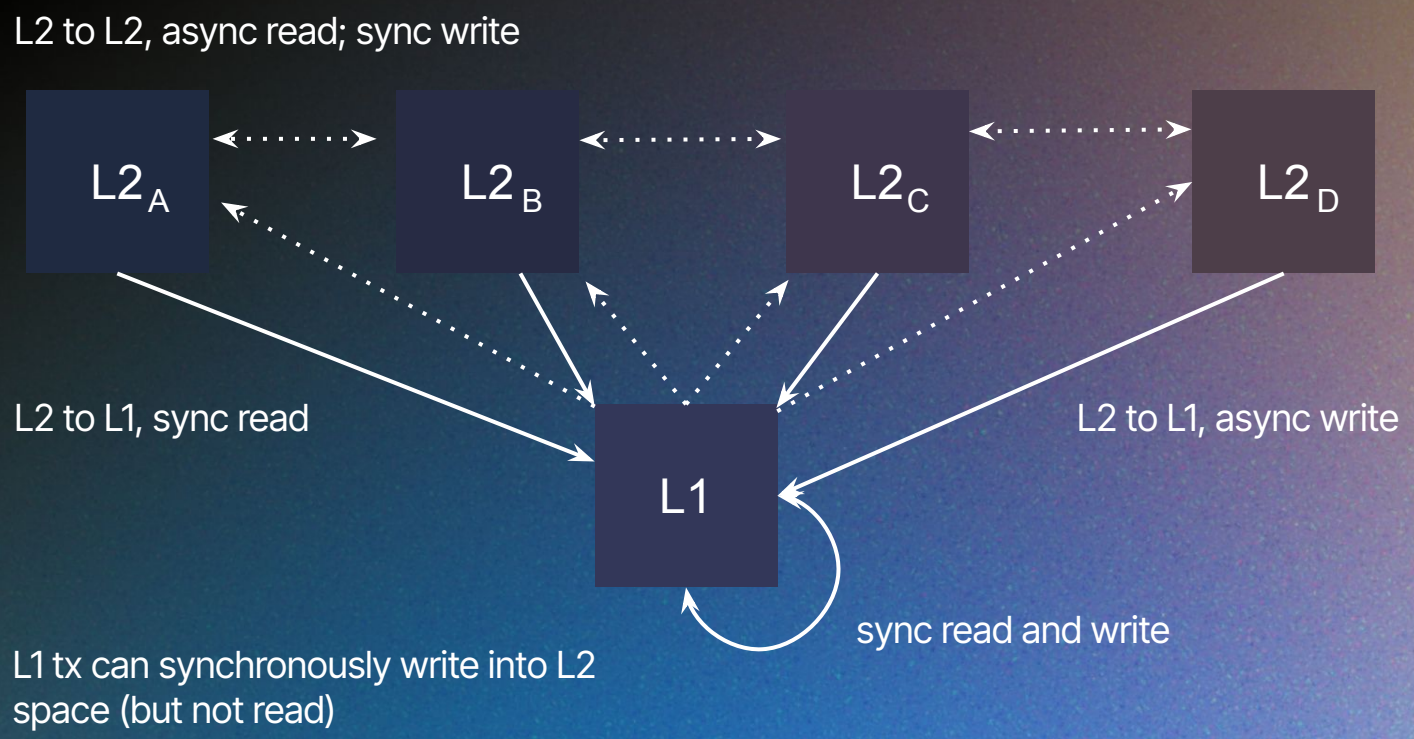
Native L2

Built and governed by Ethereum

	Sequencing Tx Ordering	Reads into L1	**Economics** from ETH Perspective	**Governance**
Rollup	Own mechanism. Sequencer usually centralised	Asyncronous	DA Costs	Project / Security Council
Based Rollup	Via Ethereum blobs	Syncronous	DA Costs, MEV	Project / Security Council
Native Rollup	Via Ethereum blobs	Syncronous	DA Costs, MEV, Congestion Fees	Governed by Ethereum

Is this sharding?




L2 to L2, async read; sync write
L2 A
L2 B
L2 C
L2 D
L2 to L1, sync read
L2 to L1, async write
L1
sync read and write
L1 tx can synchronously write into L2 space (but not read)

Everything introduced until now could be done without a single technical change of Ethereum L1

Connect ETH validator rewards to correctness proofs of native L2, make EVM chain proofing a cheap to use primitive (that also none-native rollups can use)

$L2_a$

Address = hash(address + salt a)

$L2_b$

Address = hash(address + salt b)

$L2_c$

Address = hash(address + salt c)

$L2_d$

Address = hash(address + salt d)

Each chain has its unique address space

L1

A message (after correctness proof) coming from L2 could actually have the distinct L2 address as msg.sender)

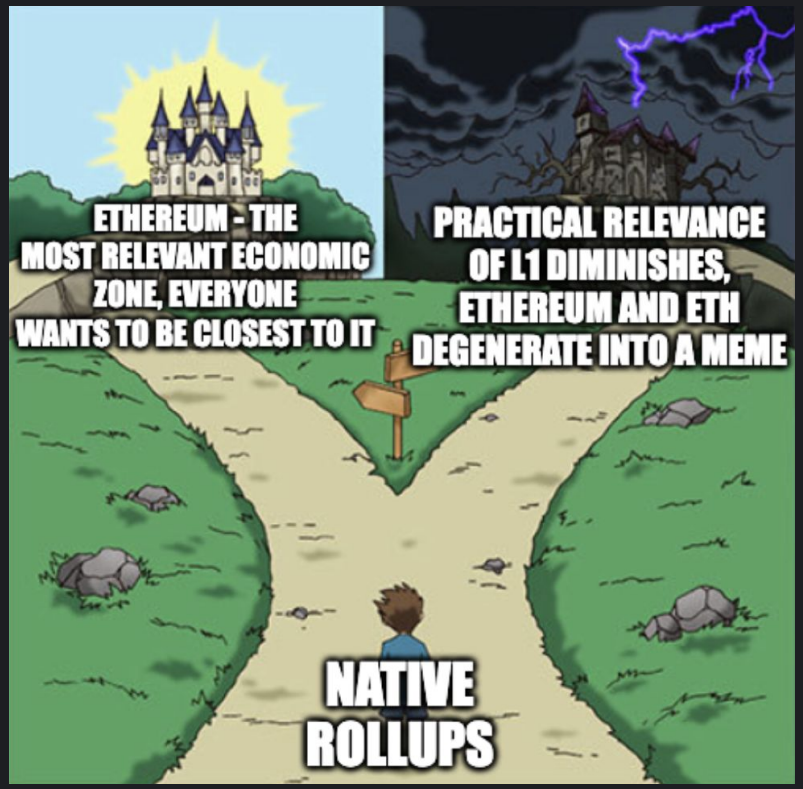
Ethereum “economic zone” becomes less relevant compared to others

Rollup-Ethereum relation slowly becomes just a MEME

Ethereum tx ordering matters less

Less assets via native bridge

Ethereum security matters less


ETHEREUM - THE MOST RELEVANT ECONOMIC ZONE, EVERYONE WANTS TO BE CLOSEST TO IT
PRACTICAL RELEVANCE OF L1 DIMINISHES, ETHEREUM AND ETH DEGENERATE INTO A MEME
NATIVE ROLLUPS


NATIVE ROLLUPS
WEAKEN ALIGNMENT WITH
EXISTING ROLLUPS
THE ETH MEME GETS WEAKER.
EVERYONE
IS PREACHING
ETH IS MONEY
NATIVE ROLLUPS

Who can make the decision what route to choose?

Everyone here!