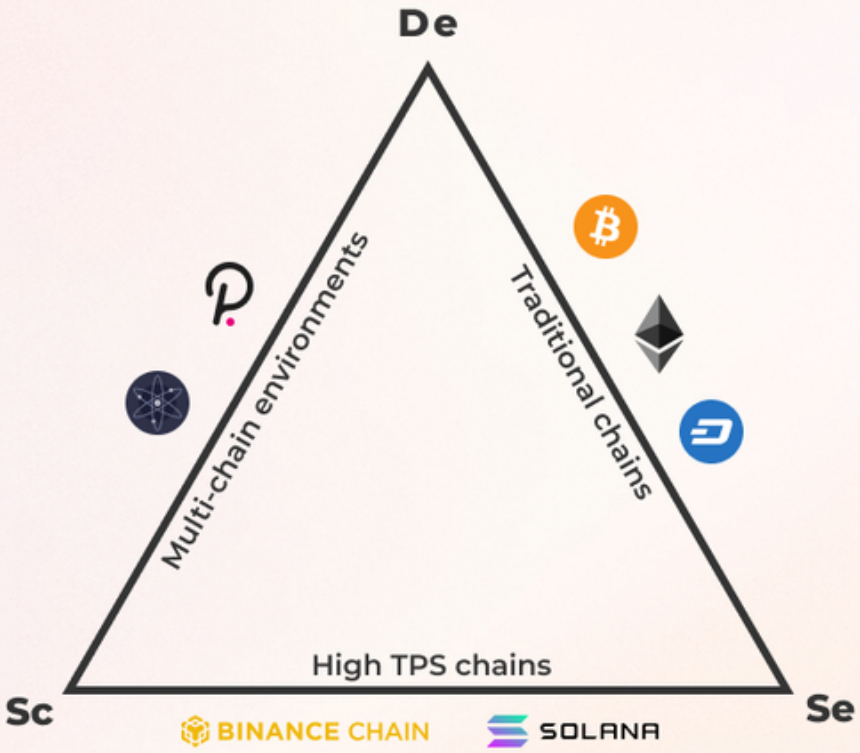
# SCALING ETHEREUM

# The Blockchain Trilemma

**De**centralization
How many nodes?
How many node owners?
Can be hardforked easily?

**Sc**alability
How many transactions per second?
Where is TPS bottleneck?
How it affects network fee?

**Se**curity
51% attackable?
Sybil attackable?
ISP level attackable?




utorg.pro

# ETHEREUM SCALING

Goal:

1. Decrease Gas Fees
2. Increase Tx per sec
3. Increase Throughput

- State Channels
- Optimistic Rollup
- ZK Rollup
- Validium
- Volition
- Sidechains
- Plasma

# STATE CHANNELS

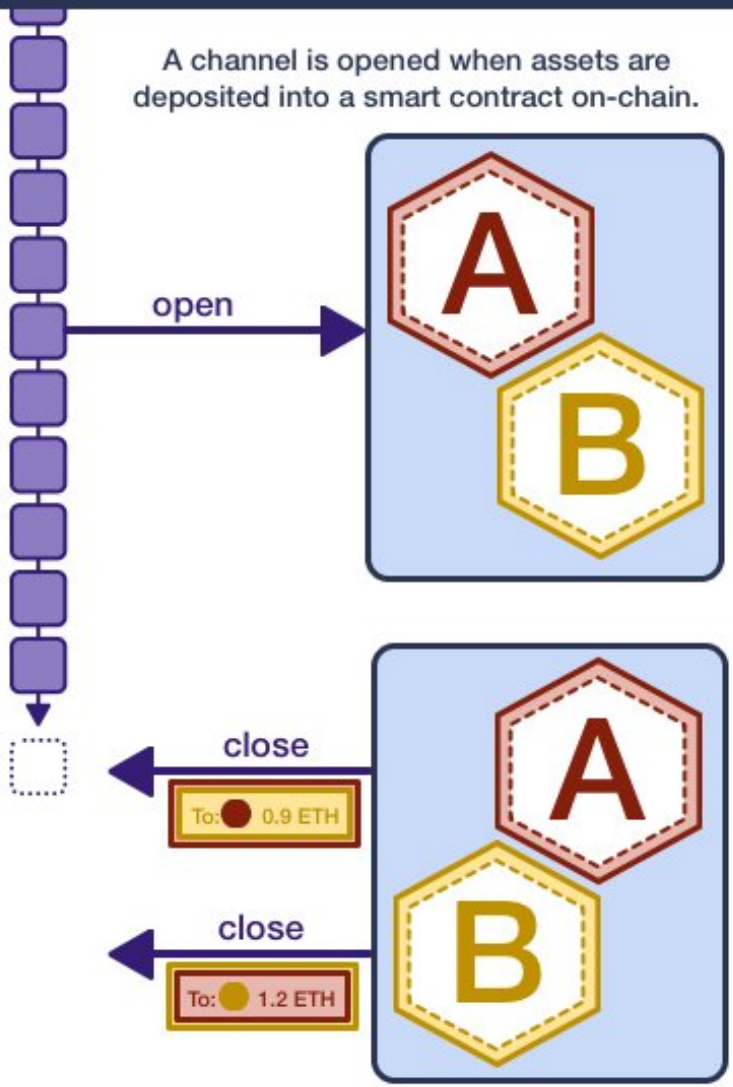
- Deploy smart contracts called Channels
- Parties involved put data and assets into the channel
- Do transactions off chain via signatures and objects
- Close channel and submit final state into blockchain

How can we scale Auction House?

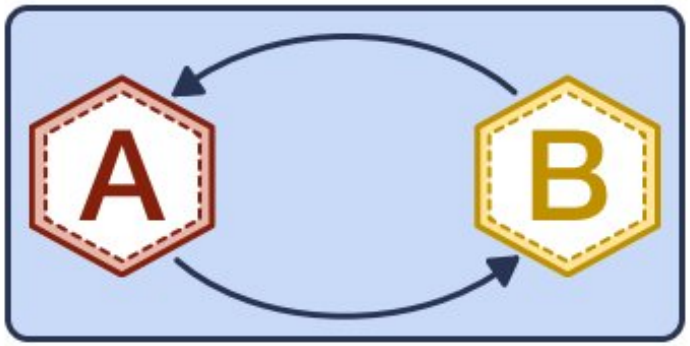
connext

STATE CHANNELS

# State Channels




To close the channel, a participant can sign the highest value ticket and submit it the chain. The smart contract will settle the state channel on-chain.




Participants in the channel transact off-chain by creating, signing and sending (incrementing) tickets.


Oct 2023
https://inevitableeth.com/

# SIDECHAINS

- Separate blockchain from ETH
- Could implement Plasma Framework

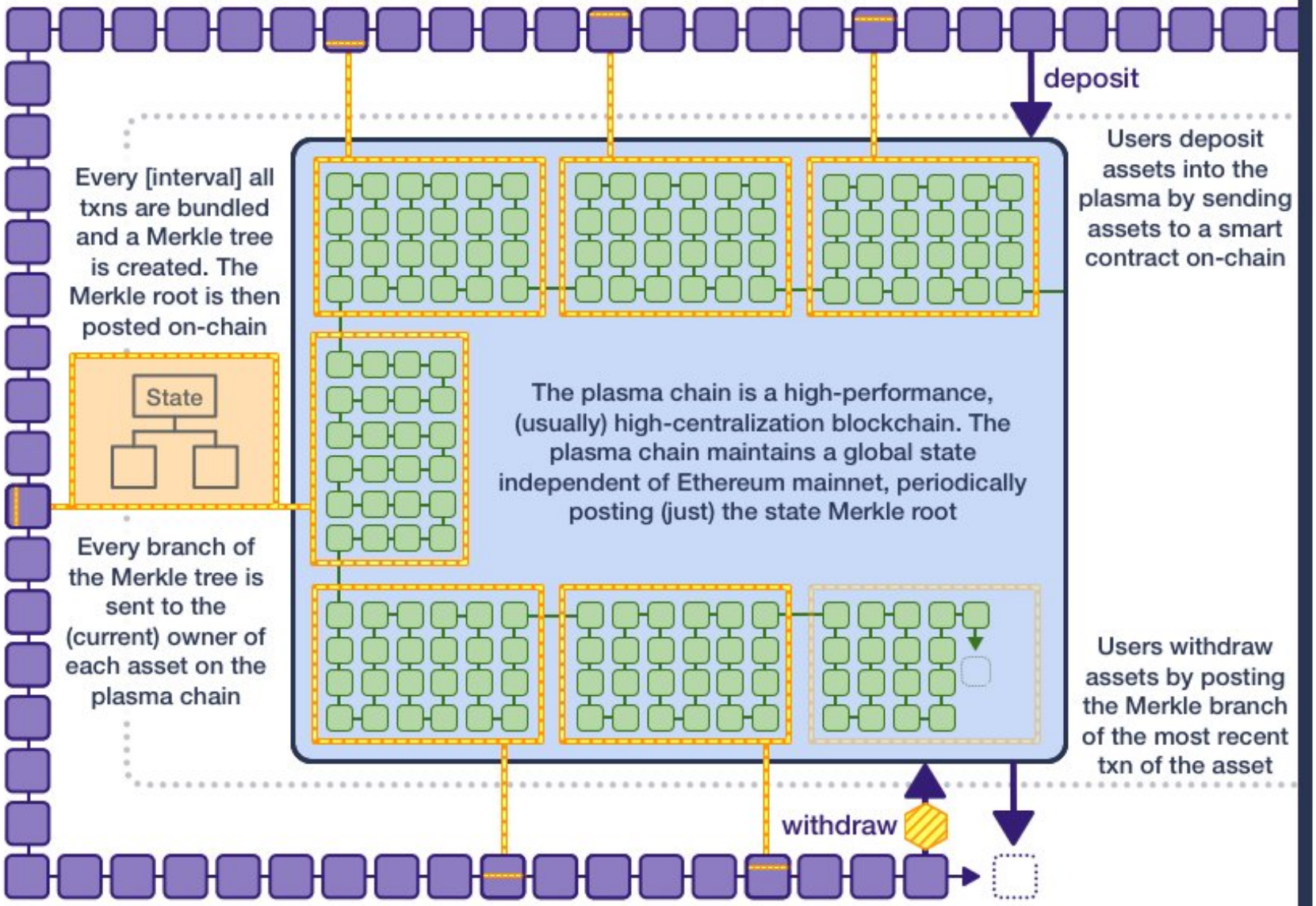
fantom

polygon

Gnosis Beacon Chain

BNB CHAIN

# Plasma




Oct 2023
https://inevitableeth.com/

# LAYER 2 ROLLUPS

“Trust-minimized L2s (Rollups) are chains that can be exited by interacting directly with L1 alone, eliminating the need to rely on L2 operators for the security of the funds."

-L2Beat.com

# ROLLUP STAGES

## Rollup Maturity Stages for Decentralization (as proposed by Vitalik & L2Beat)

Source: Galaxy Digital Research

| Description / Qualifications | Questions to Evaluate for each Stage (per L2Beat) |
|---|---|
| **Stage 0** "Full Training Wheels" | |
| Rollup is effectively run by the operators; data is posted on L1 allowing for reconstruction of the state used to compare state roots with proposed roots. | Does the project call itself a rollup? |
| | Are L2 state roots posted on L1? |
| | Does the project provide Data Availability (DA) on L1? |
| | Is software capable of reconstructing the rollup's state open source? |
| **Stage 1** "Limited Training Wheels" | |
| Rollup has fully functional proof system, decentralization of proof submission, and provision for user exits without operator coordination. Rollup transitions to being governed by smart contracts; Security Council may be in place to address bugs. | Does the project use a proper proof system? |
| | Are there at least 5 external actors that can submit a fraud proof? |
| | Can the users exit without the operator's coordination? |
| | Do users have 7+ days to exit in case of unwanted upgrades (excl. Security Council & governance)? |
| | Is the Security Council properly set up? |
| **Stage 2** "No Training Wheels" | |
| Rollup fully managed by contracts; proving is permissionless; safeguards against governance attacks (ample time to exit w/ upgrades; Council confined to adjudicating undeniable bugs). | Is the fraud proof system permissionless? |
| | Do users have at least 30 days to exit in case of unwanted upgrades? |
| | Is the Security Council restricted to act only due to errors detected on chain? |

Data: Vitalik "Proposed milestones for rollups taking off training wheels" blog post, L2Beat "Stages" rollup maturity framework

# OPTIMISTIC ROLLUPS

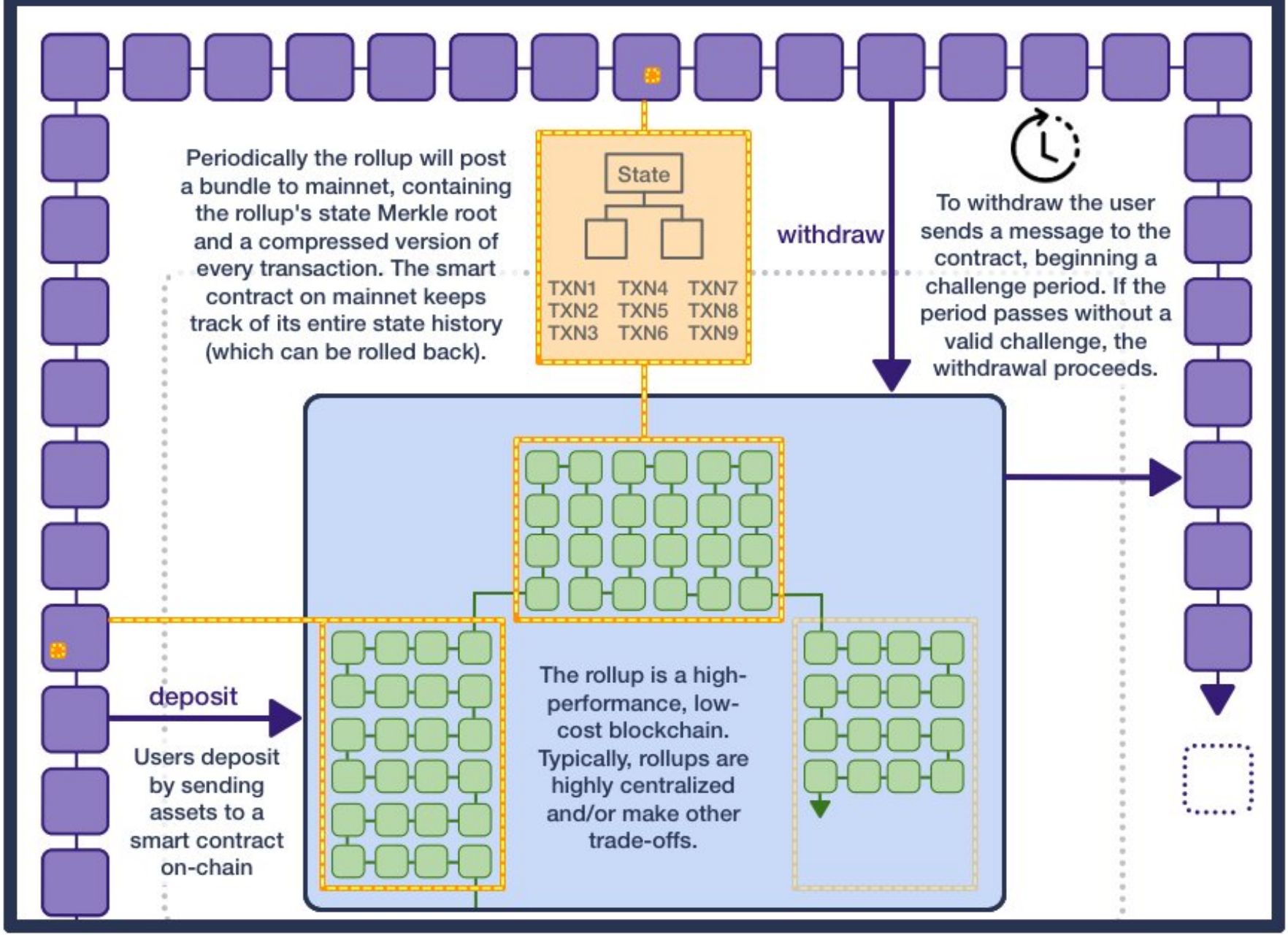
- Compute Transactions
- Batch Transactions
- Combine minimal data into a small proof
- Submit proof the proof to main chain
- Optimistically assume all proofs are valid
- Have a challenge period to allow disputes

ARBITRUM

boba

OP

# Optimistic Rollups



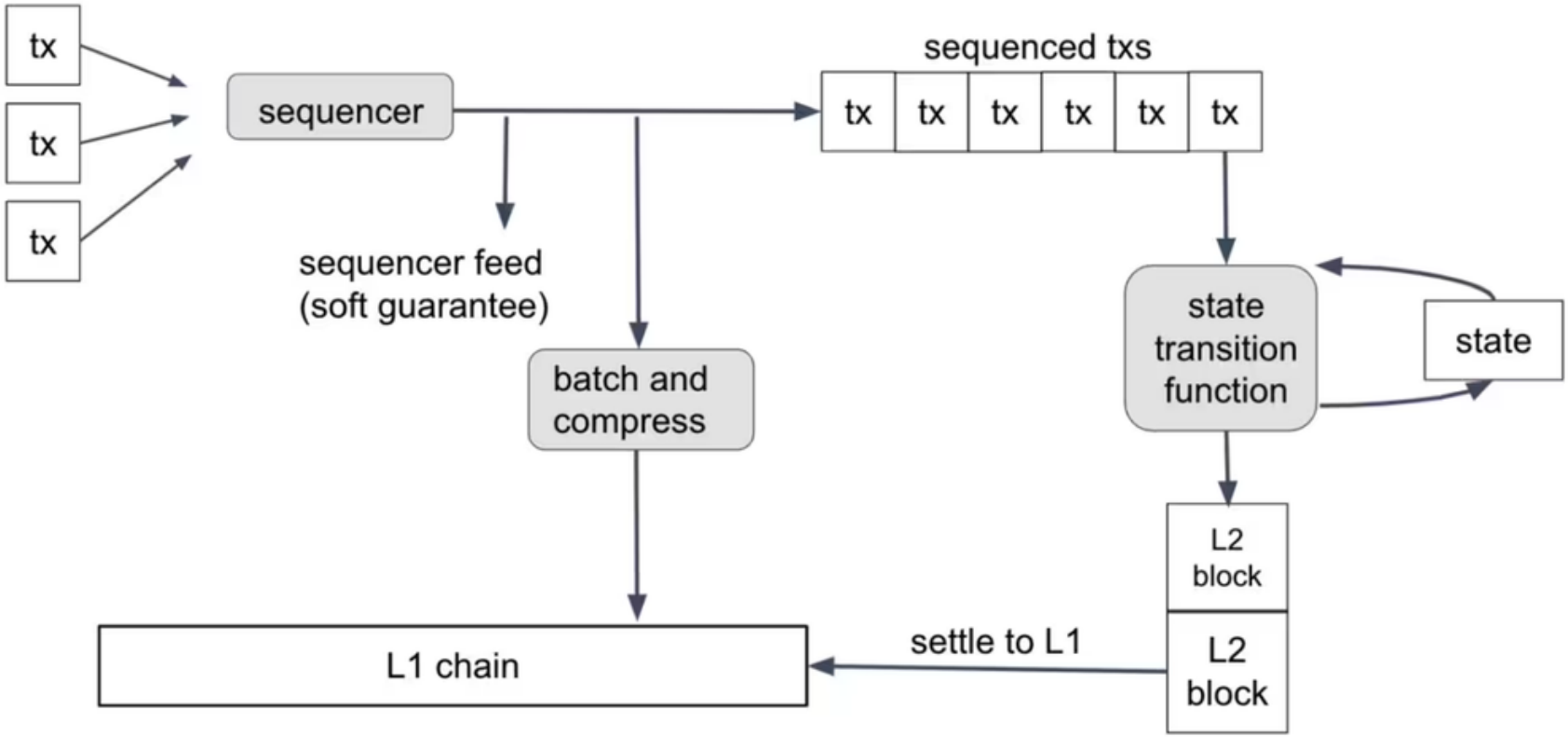

Oct 2023
https://inevitableeth.com/

# OPTIMISTIC ROLLUPS

- Sequencers
- Validators
  - Proposers
  - Verifiers

# Typical Transaction Settlement Process on Optimistic Rollup

Source: Galaxy Digital Research




Source: Arbitrum Nitro white paper

Oct 2023
https://www.galaxy.com/insights/research/optimism-arbitrum-pt2-decentralization/

# OPTIMISTIC ROLLUPS

| Parameter | Ethereum (L1) | Rollup (L2) |
|---|---|---|
| Nonce | ~3 | 0 |
| Gasprice | ~8 | 0-0.5 |
| Gas | 3 | 0-0.5 |
| To | 21 | 4 |
| Value | 9 | ~3 |
| Signature | ~68 (2 + 33 + 33) | ~0.5 |
| From | 0 (recovered from sig) | 4 |
| **Total** | **~112 bytes** | **~12 bytes** |

# Optimism's Security Model

The Optimism blockchain is a work in progress. Constantly pushing to improve the security guarantees that users have while using Optimism is a top priority. At the moment, **it's important to understand that the security of the Optimism blockchain is dependent on a** multisig wallet managed by several anonymous individuals. This multisig wallet can be used to upgrade core Optimism smart contracts without upgrade delays.

Please also keep in mind that just like any other system, **the Optimism codebase may contain unknown bugs** that could lead to the loss of some or all of the assets held within the system. Optimism's smart contract codebase has been audited repeatedly but **audits are not a stamp of approval** and **a completed audit does not mean that the audited codebase is free of bugs.** It's important to understand that using Optimism inherently exposes you to the risk of bugs within the Optimism codebase, and that you use Optimism at your own risk.

# Permissions

**The system uses the following set of permissioned addresses:**

- **SecurityCouncil** 0x3666...8767

  The admin of all contracts in the system, capable of issuing upgrades without notice and delay. This allows it to censor transactions, upgrade bridge implementation potentially gaining access to all funds stored in a bridge and change the sequencer or any other system component (unlimited upgrade power). It is also the admin of the special purpose smart contracts used by validators. This is a Gnosis Safe with 9 / 12 threshold.

- **SecurityCouncil participants** 0x4758...Bf09 0xf6B6...C863 0x5A1F...81dF 0x0275...7Bae 0x5280...2e44 0x566a...3710 0x8e62...a3C5 0x8891...a217 0x8688...9623 0x0E50...eBf5 0x526C...49EF 0xf8e1...fEfd

  Those are the participants of the SecurityCouncil

- **ArbitrumProxyAdmin** 0x5547...2dbD

  This contract is an admin of SequencerInbox, RollupEventInbox, Bridge, Outbox, Inbox and ChallengeManager contracts. It is owned by the Upgrade Executor.

- **UpgradeExecutorAdmin** 0x5613...0678

  This contract is an admin of the Update Executor contract, but is also owned by it.

- **GatewaysAdmin** 0x9aD4...0aDa

  This is yet another proxy admin for the three gateway contracts. It is owned by the Upgrade Executor.

- **Sequencer** 0xC1b6...47cc

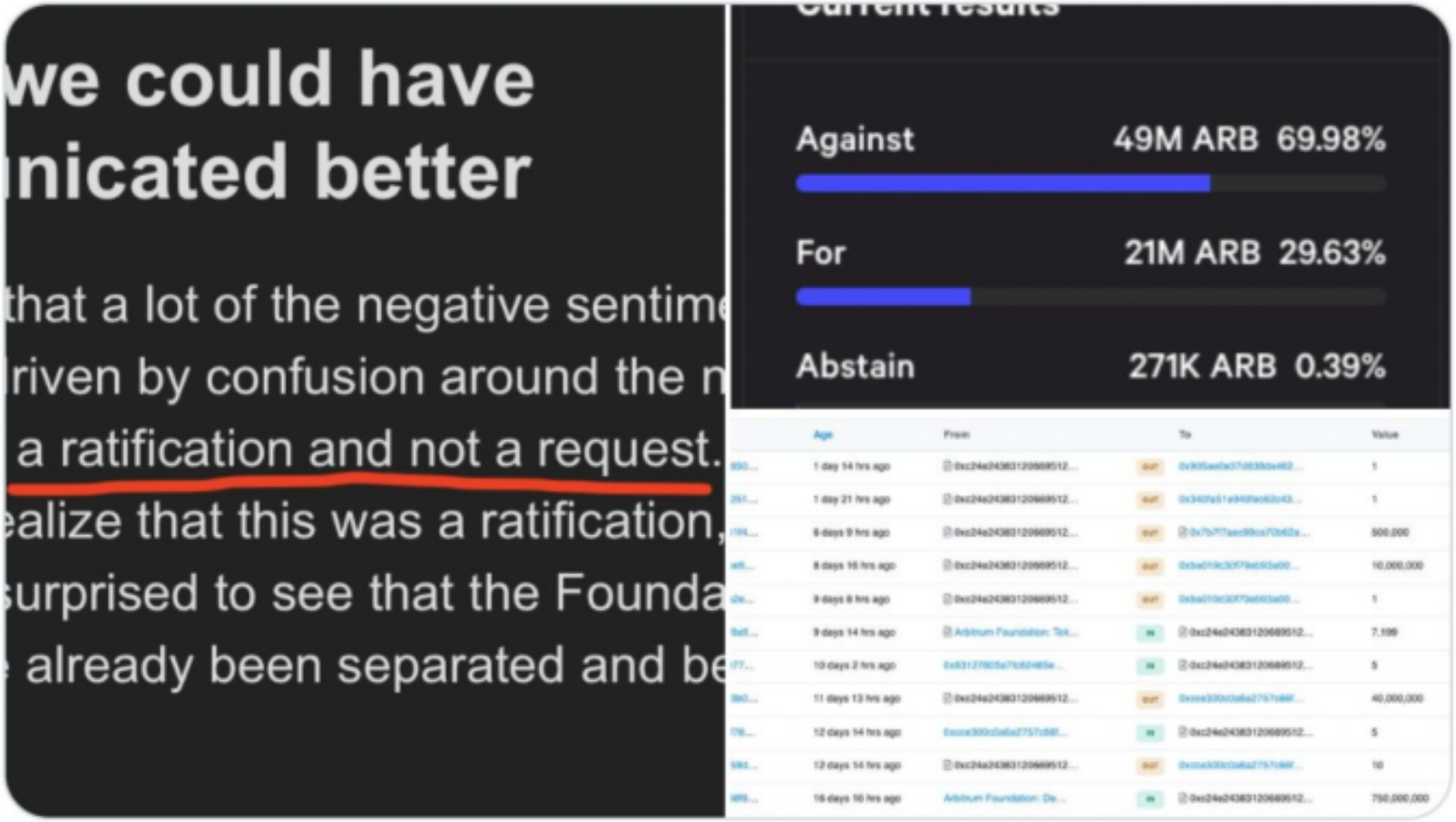
  Central actor allowed to set the order in which L2 transactions are executed.

**Eden Au** @0xedenau · Apr 2

Arbitrum foundation made a proposal (AIP-1) to allocate 750M ARB tokens for admin and op costs, but $ARB holders voted against it

Now they said the vote was just a formality, and they have already spent 50.5M (6.7%) of the proposed 750M $ARB

Your vote is not vote



# ZK ROLLUPS

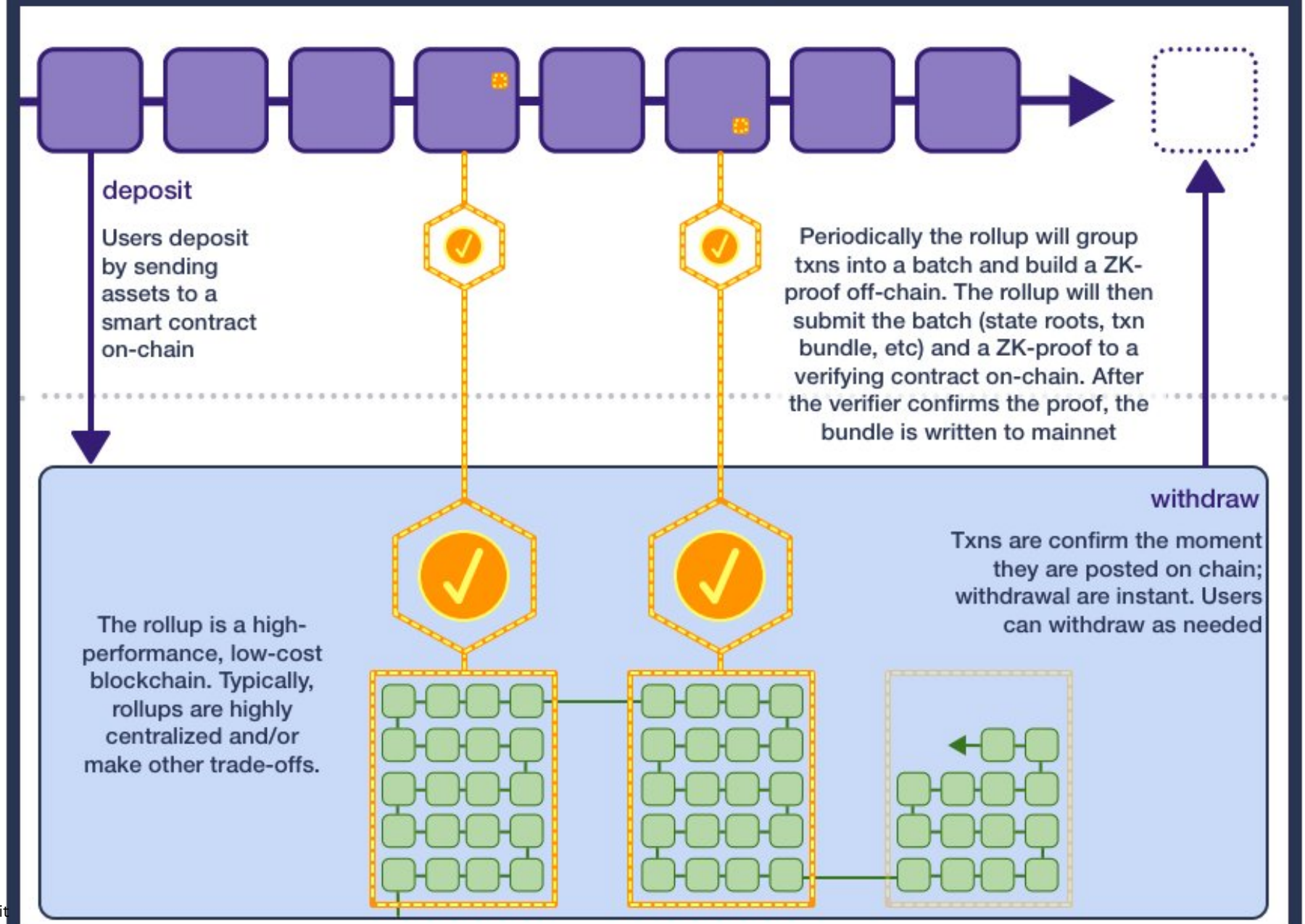
- Submit proofs onchain
- Store and serve data off chain
- 9000 TPS
- Finality for Transactions
- Computationally heavy
- Currently Application Specific

LOOPRING

zkSync

zkspace

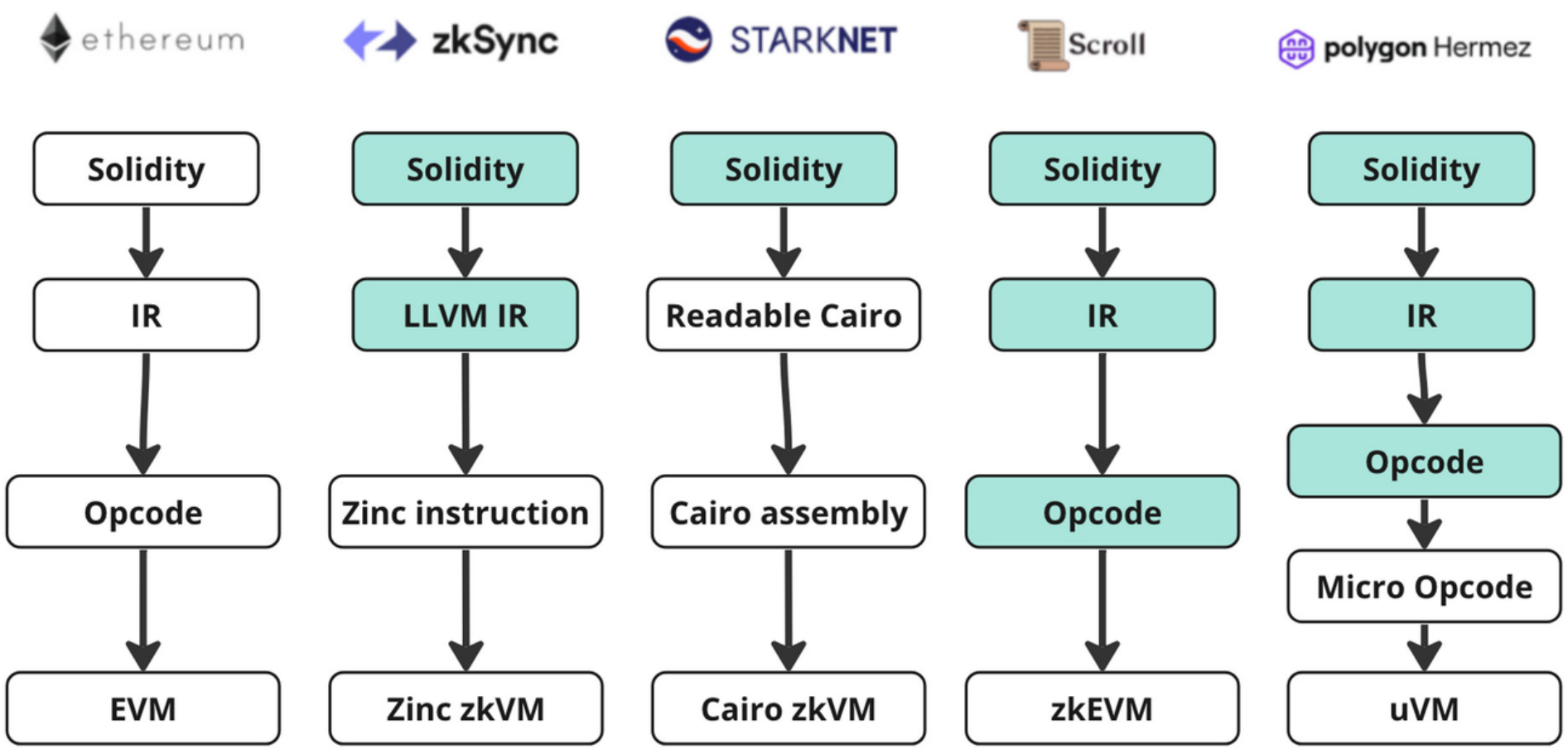
# Zero-Knowledge Rollups




Oct 2023
https://inevitableeth.com/


Oct 2023
https://vitalik.ca/general/2022/08/04/zkevm.html

# TYPE 4




Oct 2023
https://dewhales.substack.com/p/the-future-of-blockchain-scalability-291

# VALIDIUM

- Submit proofs on-chain
- Store and serve data off-chain
- Execution of smart contracts off-chain
- Good for privacy
- 9000 TPS

STARKWARE

# VOLITION

- Same as Validium but has a choice to choose on-chain and off-chain data availability and smart contract execution

ImmutableX

# INTEROPABILITY

Cant do transaction between blockchains

Layer 0
OP Superchain
AVAX Subnet
Cosmos
DOT

# LAYER DESCRIPTIONS

| Layer | Description | Examples |
|---|---|---|
| **Layer-2 (L2)** | L2 is a collective term to describe a specific set of scaling solutions for L1. | • Optimistic Rollups<br>• ZK Rollups |
| **Layer-1 (L1)** | Generally refers to a blockchain with a native cryptocurrency. It includes the basic rules and protocols that govern how the network operates and how transactions are processed and validated. | • Bitcoin<br>• Ethereum<br>• Cronos |
| **Layer-0 (L0)** | Refers to the underlying infrastructure that supports the operation of L1s, helping with scalability and interoperability. | • Cosmos<br>• Polkadot<br>• Avalanche |

crypto.com/university

Crypto.com Research

Oct 2023
https://crypto.com/university/what-are-layer-0-protocols

# PROMINENT LAYER-0 NETWORKS

| | Cosmos | Polkadot | Avalanche |
|---|---|---|---|
| **Consensus** | Tendermint Core | Nominated Proof of Stake | Avalanche Consensus (X-Chain), Snowman Consensus (P and C-Chains) |
| **Ecosystem Structure** | Hub — Zones | Relay Chain — Parachains | Subnets (No sharding) |
| **L1 Chains in Ecosystem** | Zones | Parachains | Subnets |
| **Cross-Chain Technology** | Inter-Blockchain Communication Protocol (IBC) | Cross-Chain Message Passing (XCMP) | Avalanche Warp Messaging (AWM) |
| **Development Toolkit** | Cosmos SDK | Substrate | Avalanche-CLI |
| **Finality** | ~3 seconds for finality | 12 to 60 seconds for finality between parachains. External blockchains take longer (-60 minutes) | Sub 3-second finality, with the majority happening in sub 1-second |
| **Security (Main-net & L1s)** | Shared security is supported by interchain security | Shared security | Shares nodes, but doesn't share security |

crypto.com/university

Crypto.com Research

Oct 2023
https://crypto.com/university/what-are-layer-0-protocols

# ORACLES

Trusted Data injection into the blockchain.

Blockchain is a state machine, and it has no way of getting data off chain on its own.

Three types of oracles:

1. Hardware Oracle
2. Software Oracle
3. Human Oracle

# ORACLES

Oracles can be decentralized too.

Chainlink is the largest decentralized oracle service.

Chainlink is an EVM blockchain that uses POS.

Chainlink operates with 3 categories of smart contracts:

1. Reputation Contract: Payment to add good nodes to the network
2. Order-Matching Contract: Request to fetch some data
3. Aggregating Contract: Answering nodes come to consensus on whose data are to be accepted.

Chainlink

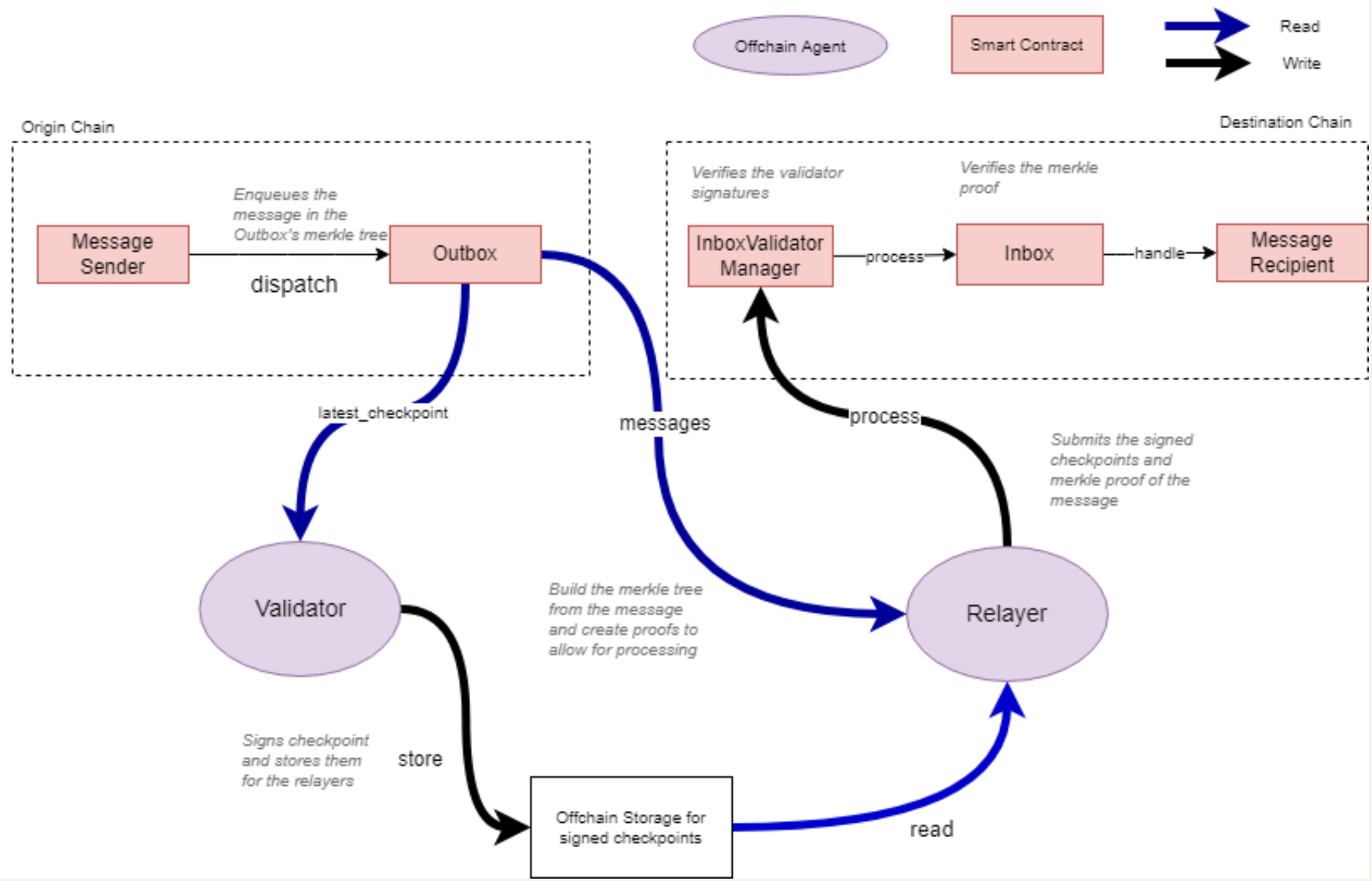
# BRIDGES

Allows data transfer and transactions between blockchains.

Types of Bridge:

- Native
- Oracle Based
- Arbitrary Message (AMB)
- Liquidity Network

# BRIDGES EXAMPLE: HYPERLANE

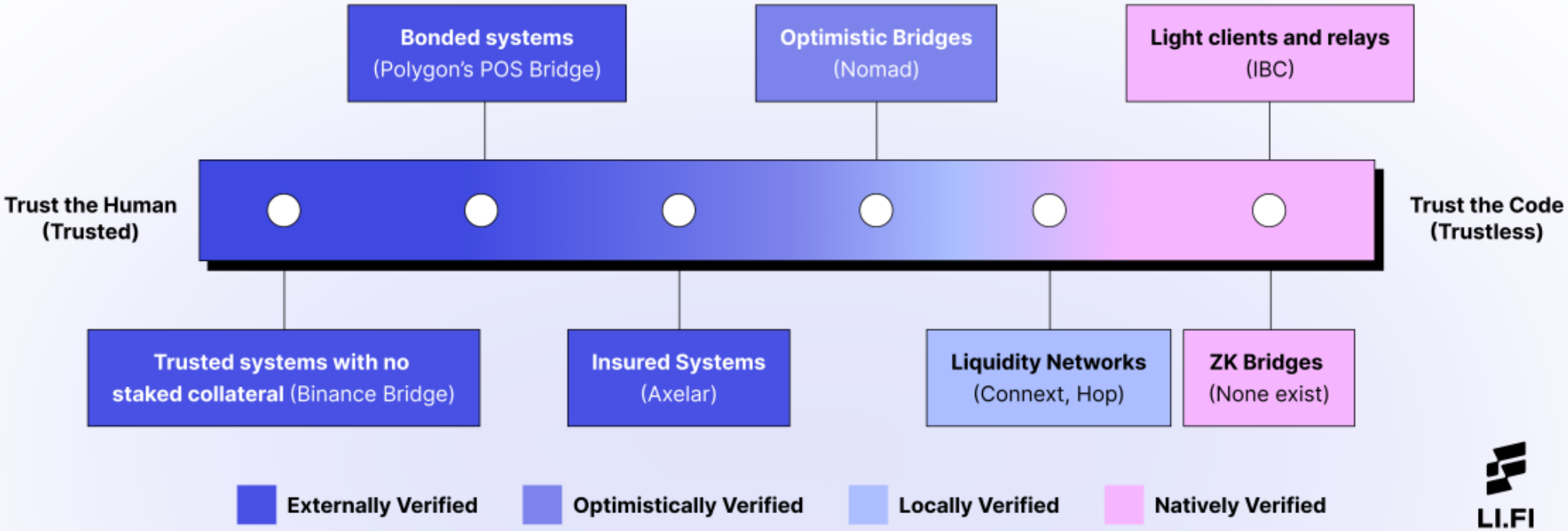


LI.FI RESEARCH

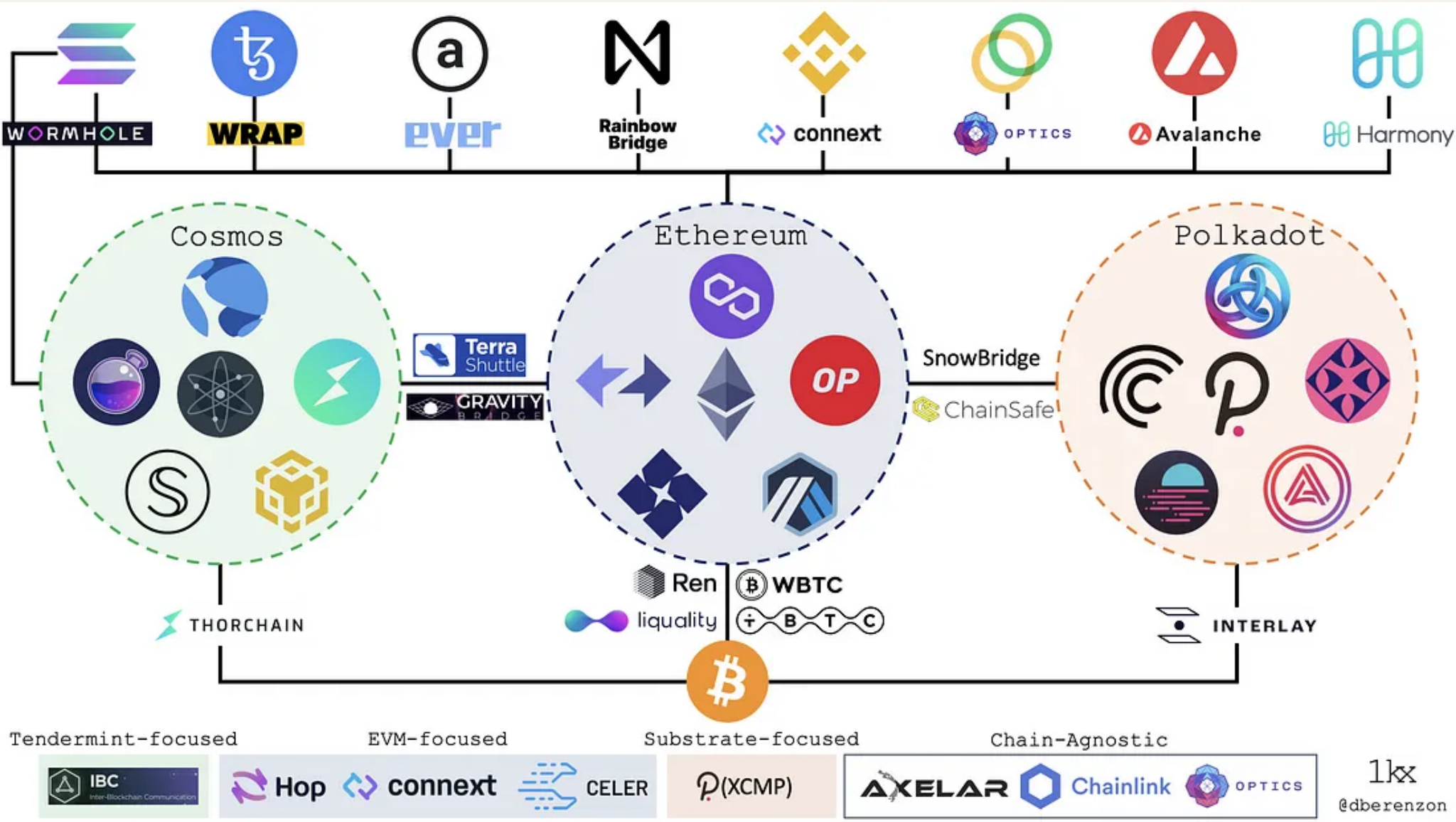
# Token Bridge Performance

| Messaging Bridge | Capital Efficiency (30 day bridge volume / TVL) | Total Bridged Volume (USD) | TVL at Peak (USD) | Total Transaction Count |
|---|---|---|---|---|
| Axelar - Satellite | 1.023717819 | $1.25B | $100M | 253,281 |
| Nomad - Nomad Bridge | NA - Bridge Inactive | $912.9M | $198.8M | 37,197 |
| Wormhole - Portal | 0.4678723404 | $33.83B | $4.67B | 961,442 |
| LayerZero - Stargate | 1.502252252 | $2.4B | $4.1B | 117,306 |
| Celer IM - cBridge | 1.860574659 | $10.6B | $779.2M | 882,772 |
| anyCall - Multichain | 0.5182481752 | $86.96B | $10.46B | 4,016,038 |
| Hyperlane | - | - | - | - |

# The 'Trust Spectrum' in Bridges




LI.FI


WORMHOLE
WRAP
ever
Rainbow Bridge
connext
OPTICS
Avalanche
Harmony
Cosmos
Ethereum
Polkadot
Terra Shuttle
GRAVITY BRIDGE
OP
SnowBridge
ChainSafe
Ren
WBTC
liquality
BTC
THORCHAIN
INTERLAY
Tendermint-focused
EVM-focused
Substrate-focused
Chain-Agnostic
IBC
Hop
connext
CELER
(XCMP)
AXELAR
Chainlink
OPTICS
1kx
@dberenzon

LI.FI RESEARCH

# Arbitrary Messaging Bridges: A Comparison Framework

| | Bridge Design - Theoretical Security | | | | Practical Security Measures | | Protocol History | | Connectivity & Usage | |
|---|---|---|---|---|---|---|---|---|---|---|
| Messaging Bridge | Consensus Mechanism | # Validators Needed for Collusion | # Signers Needed to Censor Messages | Permissionless-ness | Audits | Open Bounties (with Immunefi) | Time Since Launch | Hacks | Network Connectivity | dApps Building on Them |
| Axelar | Delegated Proof of Stake + Weighted Threshold Signature Scheme | 2/3rd = 33 / 48 Validators | 16 Validators* *Lower for chains with fewer validators | Permissionless, via delegated PoS | 27 Multiple audits by Ackeeblockchain, Cure53, NCC, Oak Security, Commonprefix labs, and others. | < $2.25 M | 7 months (Since February 2022) | NA | 23 | Satellite, Injective, StellaSwap, MetaFi, Finoa, Prime Protocol |
| Nomad | Optimistic | N/A | 1 Updater or Watcher* *Only Updater can cause downtime issues at a channel level | Permissoned Updater and Watcher | 1 Quantstamp | < $1M | 8 months (Since January 2022) | $190M smart contract hack | 6 | Connext, Hummingbot, ElasticSwap, NFTHashi |
| Wormhole | Multi-Sig | 13 / 19 Guardians | 7 Guardians | Permissoned Guardians | 3 - Neodyme, Kudelski (x2) (5 more audits scheduled for Q3 2022) | < 10M | 13 months (Since August 2021) | $320M smart contract hack | 14 | Portal Bridge, Injective, Swim Protocol, Mayan Finance, Unlockd Finance |
| LayerZero | Independent Oracle and Relayer | 2 / 2 | 1 Oracle or Relayer* *Oracle and Relayer systems can be decentralized (ex: Chainlink's oracle network) | Can be permissionless (open choice; up to the developer building on L0) | 3 SlowMist, Ackee, Zellic | < 15M (announced but not open yet) | 6 months (Since March 2022) | NA | 11 | Stargate, Angle Protocol, Gh0stly Gh0sts, Holograph, InterSwap |
| Celer IM | Specialized Proof of Stake or Optimistic Rollup-like model | 2/3 Staked Value | 7 Validators (at current staked value) | Permissionless via governance (SGN validators are elected by CELR stakers) | 3 SlowMist, PeckShield, CertiK | < $2M | 5 months (Since April 2022) | NA | 9 | SynFutures, Mystiko, Swing, FutureSwap, Rubic, Aperture |
| anyCall | Secure Multi-Party Computation (SMPC) + Equally-Weighted Threshold Signature Scheme | 13 / 24 Validators | 12 Validators | Permissionless (anyone can run a fast MPC Node) | 2 BlockSec (for both the older version and current version) | < $2M | 5 months (Since April 2022) | $3M smart contract hack | 11 | Curve, Fantom Animals, Hundred Finance, Fiver for gas |
| Hyperlane | Delegated Proof of Stake + Sovereign Consensus | Possible * Specific details about Abacus' validator set are not publically available yet | Validators can censor messages (Validators' stake is slashed for censoring messages) | Permissionless, via delegated PoS | Info to be published soon | - | 2 months (July 2022) | NA | 7 | - |

# BRIDGE MATRIX

Hi, these are what I believe to be the best bridging routes **without CEX** (lowest fees/slippage) and bridges for each network.

**NOTE THAT ALL BRIDGE PRICING/BRIDGE ROUTING IS DYNAMIC AND THERE ISN'T REALLY EVER ONE "BEST" E**

**Tools like Movr, Li.finance, Rango and Chainswap are examples of tools that select the best path in real-time**

I'll update this chart if I find that Wormhole is consistently better, but **Synapse gives you the native gas token** upon arrival so it's pretty good

**NOTE 1: This chart does not include slippage and transaction fees! Please be mindful when you are bridging!**

**NOTE 2: Bridging from basically any chain to ETH will cost a lot regardless of bridge used.**

**NOTE 3: All bridges are doing amazing work for the space and help to foster the success of multichain networking.**

**Please DYOR and check out every bridge as some will suit your needs better than others**

**Other good bridges: Connext**

**Algorand Bridge (Only ETH ↔ ALGO)** **Gnosis Bridge (ETH ↔ Gnosis) OR Hop Protocol**

**Rango (referral link) actually does all the routing for you, and has a guaranteed airdrop for high volume/high scoring bridgooors**

| TO 👉 FROM 👇 | Ethereum | BSC | Solana | Terra | Avalanche | Polygon | Cronos | Near | Aurora | Cosmos |
|---|---|---|---|---|---|---|---|---|---|---|
| Ethereum | | cBridge | Wormhole | Wormhole | cBridge | cBridge | Multichain | 🌈 Bridge | 🌈 Bridge | Gravity |
| BSC | cBridge | | Allbridge | Terra Bridge | Multichain | Multichain | EvoDefi | Terra ➡ Allbridge ➡ 🌈 | cBridge | Bridge to Terra th Osmosis usin Osmosis |
| Solana | Wormhole | Wormhole | | Wormhole | Wormhole | Wormhole | Wormhole ➡ EvoDefi | Wormhole to Terra ➡ Allbridge to Aurora ➡ 🌈 | Wormhole to Terra ➡ Allbridge to Aurora | Wormhole to Ter Terra again |
| Terra | Terra | Terra | Wormhole | | Wormhole | Wormhole | Terra to BSC ➡ EvoDefi | Allbridge to Aurora ➡ 🌈 Bridge | Allbridge to Aurora | Allbridge to Aur |
| Avalanche | cBridge | Abracadabra | Wormhole | Wormhole | | cBridge | EvoDefi | Synapse to Harmony ➡ Terra ➡ Allbridge ➡ 🌈 | cBridge | Terra |
| Polygon | cBridge | cBridge | Wormhole | Wormhole | cBridge | | EvoDefi | Synapse to Harmony ➡ Terra ➡ Allbridge ➡ 🌈 | cBridge | cBridge/Synaps Harmony then T |

Bridging | Cross-Chain Bridge Aggregators | Potential Airdrops

Resources Used:

https://coinsbench.com/about-evm-opcode-gas-ethereum-accounts-9f0896f09d04
https://ethereum.org/
https://hardhat.org/
https://docs.ethers.io/v5/
https://www.openzeppelin.com/
https://takenobu-hs.github.io/downloads/ethereum_evm_illustrated.pdf
https://www.skillsoft.com/