

ETHEREUM AND SMART CONTRACTS



Created: Oct 2022
Last Edited: Oct 2022

UofT: CSCD71F22
-David Liu, Founder of dApp Technology Inc.

ETHEREUM SCALING

- 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



**STATE
CHANNELS**

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

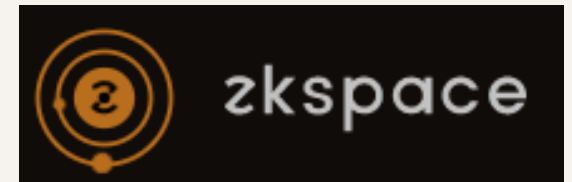
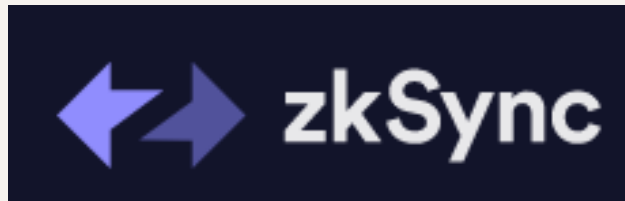


OPTIMISTIC ROLLUPS

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

ZK ROLLUPS

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



VALIDIUM

- Submit proofs onchain
- Store and serve data off chain
- 9000 TPS



VOLITION

- A combination of ZK Rollups and Validium



ImmutableX

SIDECHAINS

- Separate blockchain from ETH

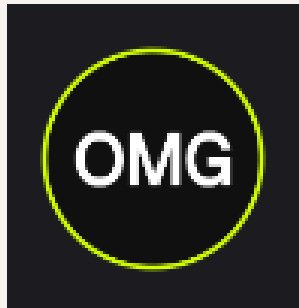


Gnosis Beacon Chain



PLASMA

- Separate blockchain from ETH
- Submits periodical batched Block Data to the main chain



RELAYERS

Takes a signed transaction, and pay for the submission on behalf of an EOA.

BRIDGES

Allows data transfer and transactions between blockchains.

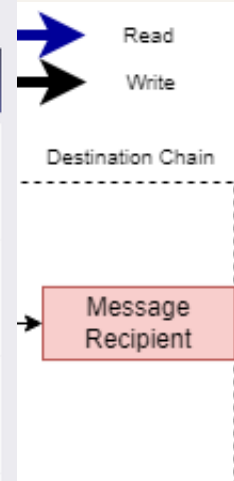
Types of Bridge:

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

BRIDGES EXAMPLE: HYPERLANE

LI.FI RESEARCH Arbitrary Messaging Bridges: A Comparison Framework

Messaging Bridge	Bridge Design - Theoretical Security				Practical Security Measures		Protocol History		Connectivity & Usage	
	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
Astar	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	Permissioned Updater and Watcher	1 Quantstamp	< \$1M	8 months (Since January 2022)	\$100M smart contract hack	6	Connect, Hummingbot, ElasticSwap, NFTHashi
Wormhole	Multi-Sig	13 / 19 Guardians	7 Guardians	Permissioned 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, Umoed Finance
LayerZero	Independent Oracle and Relay	2 / 2	1 Oracle or Relay* *Oracle and Relay systems can be decentralized (ex: Chainlink's oracle network)	Can be permissionless (open choice; up to the developer building on L0)	3 Stonemist, Ackee, Zelic	< 15M (announced but not open yet)	6 months (Since March 2022)	NA	11	Stargate, Angle Protocol, Ghostly Ghosts, 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 (SON 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 publicly 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	-



and stores them for the relayers

store

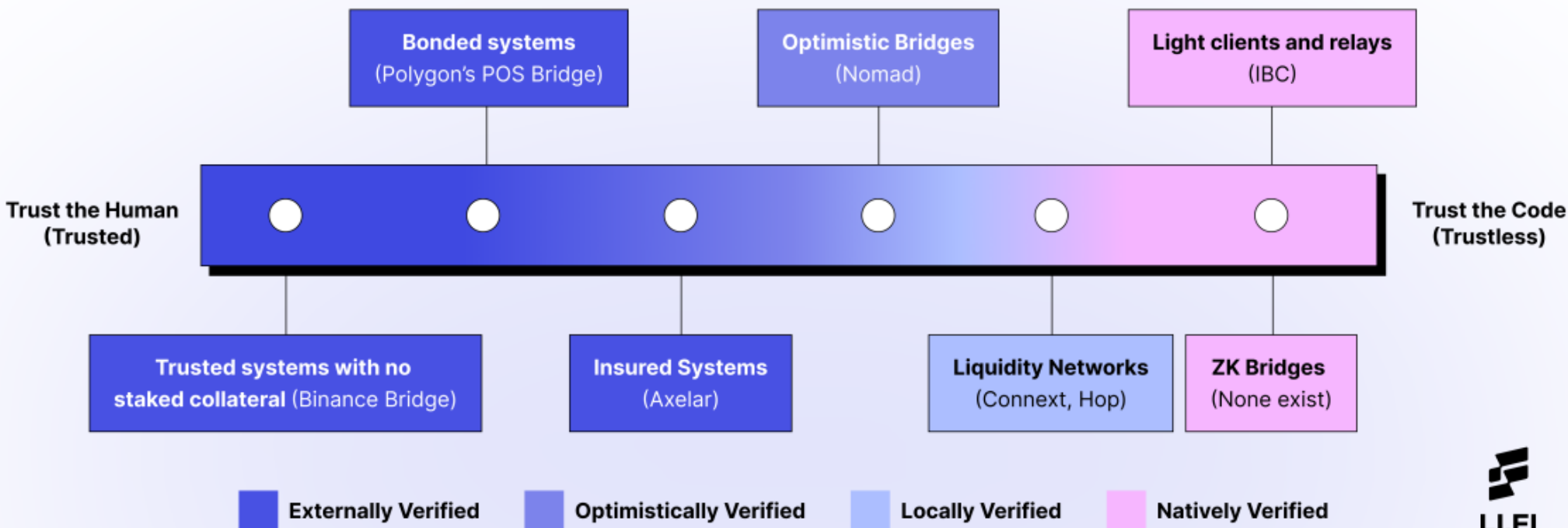
Offchain Storage for signed checkpoints

read








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



Arbitrary Messaging Bridges: A Comparison Framework

Messaging Bridge	Bridge Design - Theoretical Security				Practical Security Measures		Protocol History		Connectivity & Usage	
	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	Permissioned Updater and Watcher	1 Quantstamp	< \$1M	8 months (Since January 2022)	\$190M smart contract hack	6	Connex, Hummingbot, ElasticSwap, NFTHashi
 Wormhole	Multi-Sig	13 / 19 Guardians	7 Guardians	Permissioned 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, Unlocked Finance
 LayerZero	Independent Oracle and Relay	2 / 2	1 Oracle or Relay* *Oracle and Relay systems can be decentralized (ex: Chainlink's oracle network)	Can be permissionless (open choice; up to the developer building on L0)	3 SlowMist, Ackee, Zelle	< 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

NOTE THAT ALL BRIDGE PRICING/BRIDGE ROUTING IS DYNAMIC AND THERE ISN'T

Tools like Movr, Li.finance, Rango and Chainswap are examples of tools that select

I'll update this chart if I find that Wormhole is consistently better, but **Synapse gives you the native gas token up**

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

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 n

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

Other good bridges: [Connex](#)

[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 hig

TO  FROM 	Ethereum	BSC	Solana	Terra	Avalanche	Polygon	Cronos	Near	
Ethereum		cBridge	Wormhole	Wormhole	cBridge	cBridge	Multichain	Bridge	
BSC	cBridge		Allbridge	Terra Bridge	Multichain	Multichain	EvoDefi	Terra → Allbridge → Bridge	
Solana	Wormhole	Wormhole		Wormhole	Wormhole	Wormhole	Wormhole → EvoDefi	Wormhole to Terra → Allbridge to Aurora → Bridge	Worm → A
Terra	Terra	Terra	Wormhole		Wormhole	Wormhole	Terra to BSC → EvoDefi	Allbridge to Aurora → Bridge	Allbric
Bridging	Cross-Chain Bridge Aggregators		Potential Airdrops						> <

BEYOND ETHEREUM AND BITCOIN

Bitcoin Competitors:

- XRP
- Tron
- Litecoin
- Monero
- Bitcoin Cash
- Bitcoin SV
- eCash
- Zcash

Ethereum Competitors:

- Cardano
- Solana
- Secret Network
- Stellar
- Algorand
- Near Protocol
- Hadera

BEYOND ETHEREUM AND BITCOIN

Application Specific:

- Vechain
- Chainlink
- Flow
- Polymath
- Audius

Layer Zero

- Polkadot
- Layer Zero
- Cosmos Hub
- Ren
- Osmosis

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/>

<https://li.fi/>