ARBITRUM

On the Path to a Rollup-Centric Future

Harry Kalodner
Offchain Labs

WHERE WE WERE

- 2014
  - Arbitrum initially developed as a class project at Princeton
- 2017
  - Arbitrum research and development resumes
- July 2018
  - Arbitrum paper published and presented at Usenix Security
- August 2018
  - Offchain Labs founded
- October 2018
  - Arbitrum first posted on ethresear.ch

WHERE WE WERE

- February 2020 - first testnet support
  - Only supports DAC
  - Application Specific Chains - No contract deployment
- October 2020
  - New testnet with general contract deployment
- March 2021
  - New Testnet - Mainnet release candidate
  - Adds arbitrary messaging bridge
- May 2021
  - Mainnet beta is live and open to developers! - Only 12 people
  - Added a sequencer
- August 2021
 - Mainnet is open to users

WHERE WE WERE

- April 2022
  - Nitro testnet is launched
- July 2022
  - Arbitrum Nova chain launched for developers
  - Data Availability committees are back!
- July 2022
  - Arbitrum Rinkeby upgraded to nitro
- August 2022
  - Arbitrum Nova fully open
  - First mainnet chain using Nitro technology
- August 2022
  - Arbitrum one upgraded to nitro

ARBITRUM ONE

ARBITRUM ONE IS THE LEADING ETHEREUM LAYER-2 SCALING SOLUTION. AN OPTIMISTIC ROLLUP TECHNOLOGY, ARBITRUM ONE PROVIDES ULTRA-FAST, 10-50X CHEAPER TRANSACTIONS WITH SECURITY DERIVED DIRECTLY FROM ETHEREUM.
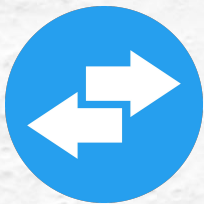
LOW-COST TRANSACTIONS

- No expensive cryptography
- No on-chain re-execution
- Minimal Layer 1 footprint

FULLY TRUSTLESS

- Security rooted in Ethereum
- Interactive fraud proofs

DROP-IN COMPATIBLE

- Full EVM support
- One-click porting
- Works with existing Ethereum languages and tooling

ARBITRUM ONE

ECOSYSTEM

$2B+
TOTAL
VALUE
LOCKED

55%+
ROLLUP
MARKET
SHARE

305+
DAPP
INTEGRATIONS

500k+
UNIQUE
ADDRESSES
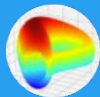
ARBITRUM ONE

Top 50 Gas Spenders (Sending Accounts that pay a lot of Gas)

Rank	Address	⇅ Fees Last 3hrs	⇅ % Spent 3hrs	⇅ Fees Last 24hrs	⇅ % Spent 24hrs	Analytics
1	Arbitrum: Sequencer	$24,074.46 (8.06 Eth)	1.95%	$64,714.83 (21.67 Eth)	0.59%	
3	Coinbase 4	$6,708.31 (2.25 Eth)	0.53%	$58,073.69 (19.44 Eth)	0.48%	
2	Ethermine	$6,708.59 (2.25 Eth)	0.56%	$54,272.17 (18.17 Eth)	0.53%	

source: https://etherscan.io/gastracker

Top Accounts by ETH Balance

Sponsored: ⚠ Trade thousands of native tokens across multiple blockchains with **Atlas DEX**. Swap Now!

A total of > **1,999,999** accounts found (118,913,468.667 Ether)

(Showing the last 10,000 top accounts only)

First ‹ Page 1 of 400 › Last

Rank	Address	Name Tag	⌄ Balance	Percentage	Txn Count
1	0x00000000219ab540356cbb839cbe05303d7705fa	Eth2 Deposit Contract	12,150,066.000069 Ether	10.21756924%	195,436
2	0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	Wrapped Ether	5,914,618.21997612 Ether	4.97388419%	7,565,226
3	0xda9dfa130df4de4673b89022ee50ff26f6ea73cf	Kraken 13	2,113,030.00243456 Ether	1.77694758%	65
4	0xbe0eb53f46cd790cd13851d5eff43d12404d33e8	Binance 7	1,996,008.28377982 Ether	1.67853844%	1,088
5	0x73bceb1cd57c711feac4224d062b0f6ff338501e		1,910,504.53020949 Ether	1.60663426%	484
6	0x9bf4001d307dfd62b26a2f1307ee0c0307632d59		1,490,000.0180927 Ether	1.25301199%	103
7	0x4ddc2d193948926d02f9b1fe9e1daa0718270ed5	Compound: cETH Token	933,342.64512161 Ether	0.78489229%	274,184
8	0x61edcdf5bb737adffe5043706e7c5bb1f1a56eea	Gemini 3	929,498.95358134 Ether	0.78165994%	336
9	0xdc24316b9ae028f1497c275eb9192a3ea0f67022	Lido: Curve Liquidity Farming Pool Contract	810,965.19801846 Ether	0.68197926%	34,709
10	0x011b6e24ffb0b5f5fcc564cf4183c5bbbc96d515	Arbitrum: Bridge	617,359.37880949 Ether	0.51916691%	50

source: https://etherscan.io/gastracker

How much are rollups paying for Ethereum's security?

CryptoFees.info + L2Beat.com = ❤️

Name	One day security costs	
Arbitrum One	$70,949.80	⌄
Optimism	$64,195.94	⌄
Boba	$22,949.62	⌄
dYdX	$17,067.80	⌄
ZKSync	$15,057.64	⌄
Starkware — Shared Prover Applications	$9,799.68	⌄
Loopring	$3,978.75	⌄
Aztec Protocol	$2,085.44	⌄
Metis	$1,072.06	⌄
Polygon Hermez	$173.77	⌄
Total	$207,330.49	⌄

Source: https://l2fees.info/l1-fees

ARBITRUM ONE

Average Daily Gas Paid Ethereum vs Arbitrum ⓘ

ETH in USD - Arbitrum   ETH in USD - Ethereum

🕐 12h ago

Source: https://pro.nansen.ai/multichain/eth-vs-arbitrum
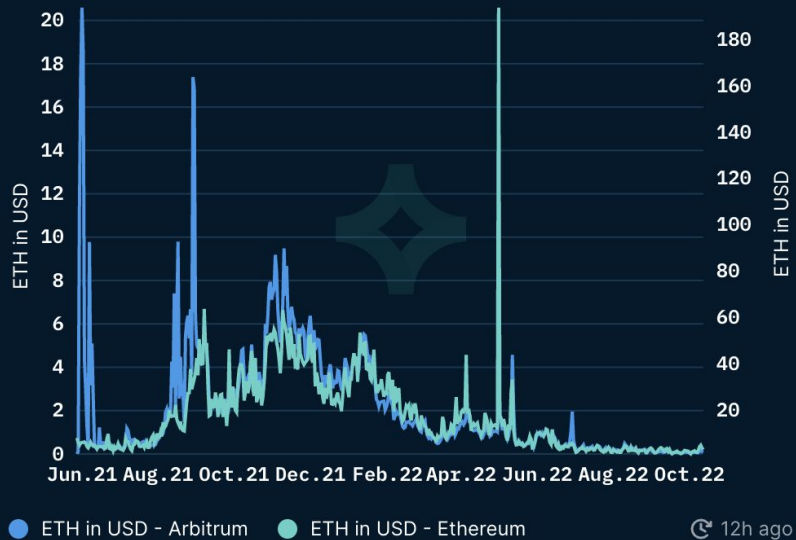
Name	Send ETH	Swap tokens
Loopring	$0.01	$0.33 ⌄
ZKSync	$0.02	$0.05 ⌄
Arbitrum One	$0.02	$0.07 ⌄
Optimism	$0.07	$0.10 ⌄
Boba Network	$0.08	$0.21 ⌄
Aztec Network	$0.14	- ⌄
Polygon Hermez	$0.25	- ⌄
Ethereum	$0.50	$2.52 ⌄

Source: https://l2fees.info/l1-fees

ARBITRUM ONE

IN ALIGNMENT WITH VITALIK'S VISION IN A ROLLUP-CENTRIC ETHEREUM ROADMAP, ROLLUPS ARE AN ESSENTIAL STEP FOR THE FUTURE OF ETHEREUM AND ARE WIDELY RECOGNIZED BY THE ETHEREUM COMMUNITY.

	ARBITRUM ONE ✓	SIDECHAINS ✗
Data Availability	Transaction calldata is posted to Ethereum	Only block headers are available to Ethereum; in some cases they are not available at all
L1-L2 Bridging	Bridge contract can self-enforce validity of transaction on Arbitrum One	Bridge contracts rely on trusted set of parties to attest validity of transaction on Sidechain
Security Mechanism	Utilize fraud proofs, when malicious behaviour takes place, security is guaranteed by Ethereum L1	Rely on ⅔ of an independent validator set to be honest; Ethereum doesn't guarantee security of the chain
When 51% Attack Occurs	Able to withstand a 99% attack on validators	Fails when only 34% of validators are attacked

ARBITRUM NOVA

N Committee Members

Certificate includes aggregated signature of N-1 members on data hash

Validators and nodes can get data from any member, validate against hash

Secure if 2 or more committee members are honest

ABITRUM NITRO

SEQUENCING, THEN DETERMINISTIC EXECUTION

GETH AT THE CORE

SEPARATE EXECUTION FROM PROVING

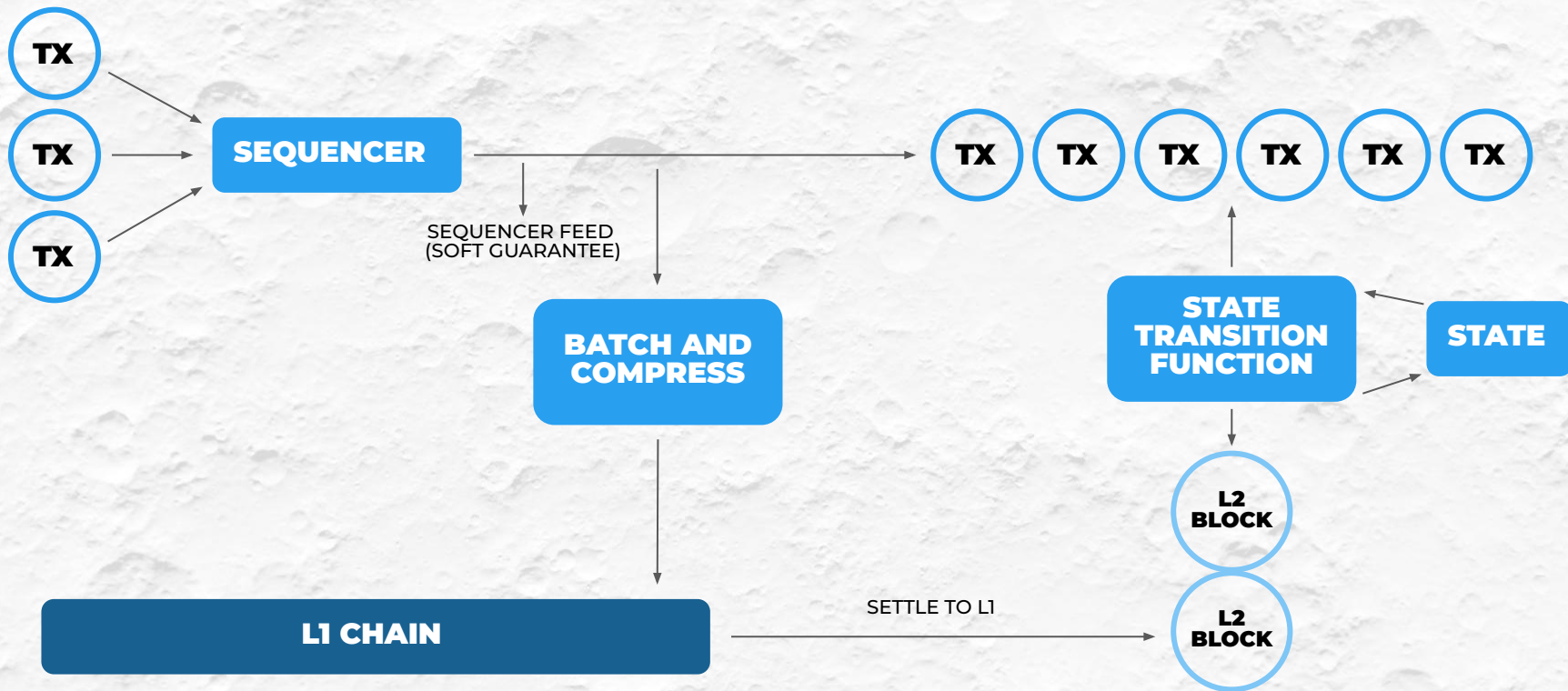OPTIMISTIC ROLLUP

ABITRUM NITRO

SEQUENCING, THEN DETERMINISTIC EXECUTION

GETH AT THE CORE

SEPARATE EXECUTION FROM PROVING

OPTIMISTIC ROLLUP

ABITRUM NITRO

TX

TX
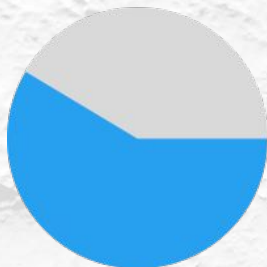
TX

SEQUENCER

SEQUENCER FEED
(SOFT GUARANTEE)

TX **TX** **TX** **TX** **TX** **TX**

BATCH AND COMPRESS

STATE TRANSITION FUNCTION

STATE

L2 BLOCK

L1 CHAIN

SETTLE TO L1

L2 BLOCK

ABITRUM NITRO

SOFT FINALITY (~1 Sec)

• How: subscribe to sequencer feed, compute state transition function

• Guarantee: correct, if sequencer's feed was correct

FINALITY (~10 Mins)

• How: read compressed batches from L1, compute state trans func, wait for L1 finality

• Guarantee: as good as your L1 finality assumption

CERTIFICATION (Days)

• How: wait for L2 blocks to be certified on L1

• (only used by L1 contracts)
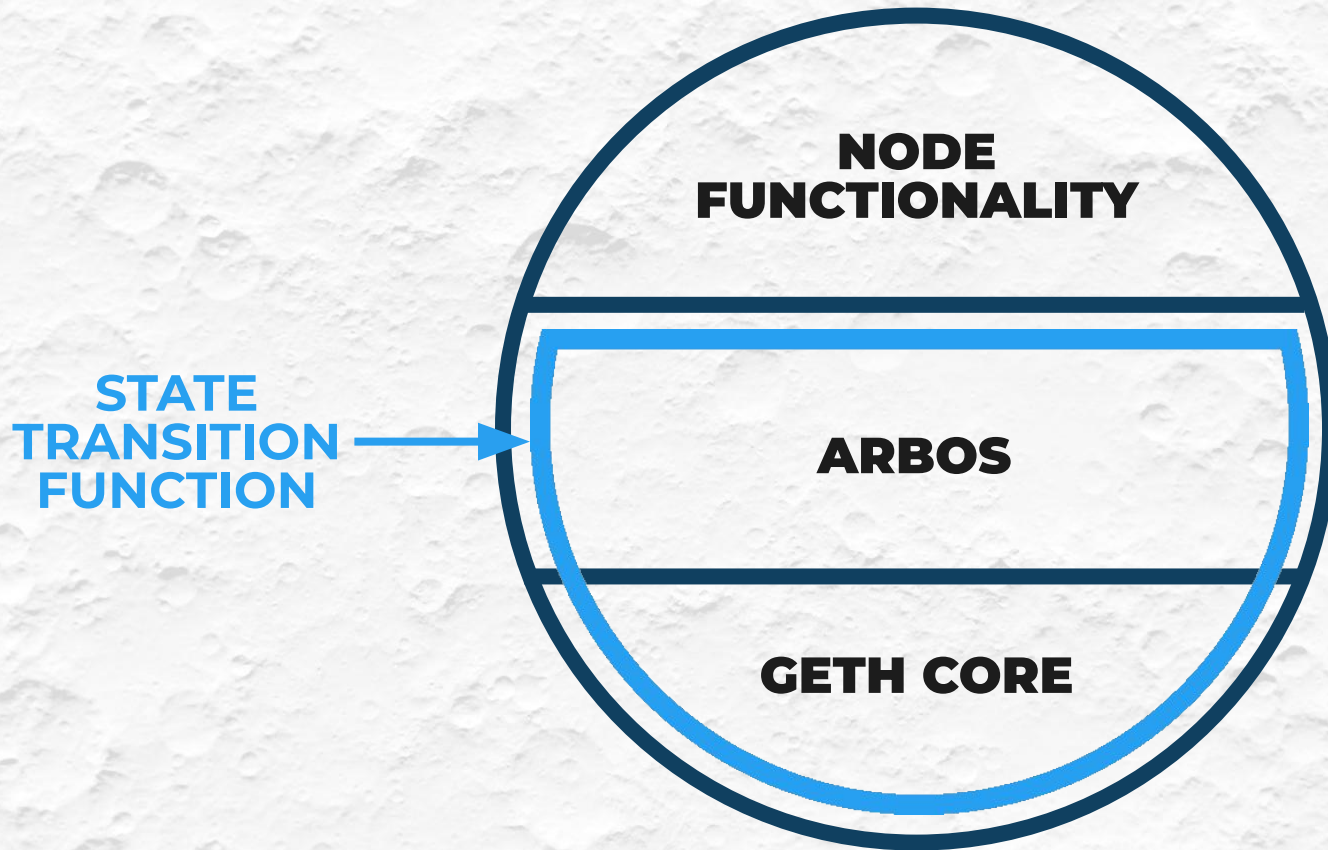
ABITRUM NITRO

SEQUENCING, THEN DETERMINISTIC EXECUTION

GETH AT THE CORE

SEPARATE EXECUTION FROM PROVING

OPTIMISTIC ROLLUP

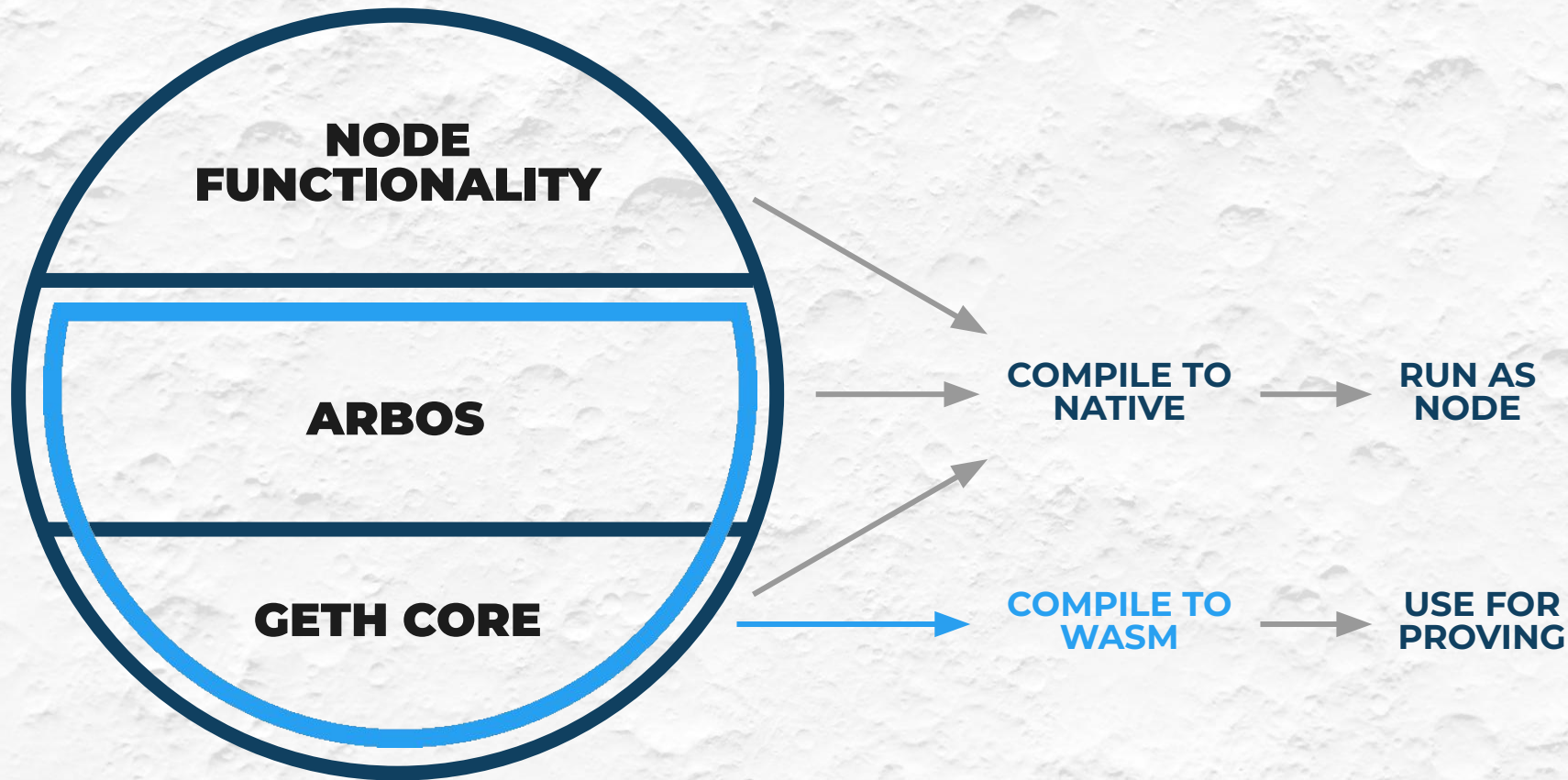# ABITRUM NITRO

SEQUENCING, THEN DETERMINISTIC EXECUTION

GETH AT THE CORE

SEPARATE EXECUTION FROM PROVING

OPTIMISTIC ROLLUP

ABITRUM NITRO

✨ Fellowship of Ethereum Magicians ✨

A rollup-centric ethereum roadmap
ethereum-roadmap, layer-2

vbuterin   4 ✏️   Oct '20

What would a rollup-centric ethereum roadmap look like?

Last week the Optimism team announced 511 the launch of the first stage of their testnet, and the roadmap to mainnet. They are not the only ones; Fuel 329 is moving toward a testnet and Arbitrum 254 has one. In the land of ZK rollups, Loopring 252, Zksync 250 and the Starkware-tech-based Deversifi 200 are already live and have users on mainnet. With OMG network's mainnet beta 198, plasma is moving forward too. Meanwhile, gas prices on eth1 are climbing to new highs, to the point where some non-financial dapps are being forced to shut down 787 and others 239 are running on testnets.

The eth2 roadmap offers scalability, and the earlier phases of eth2 are approaching quickly, but base-layer scalability for applications is only coming as the last major phase of eth2, which is still years away. In a further twist of irony, eth2's usability as a data availability layer for rollups comes in phase 1, long before eth2 becomes usable for "traditional" layer-1 applications. These facts taken together lead to a particular conclusion: **the Ethereum ecosystem is likely to be all-in on rollups (plus some plasma and channels) as a scaling strategy for the near and mid-term future.**

ABITRUM NITRO
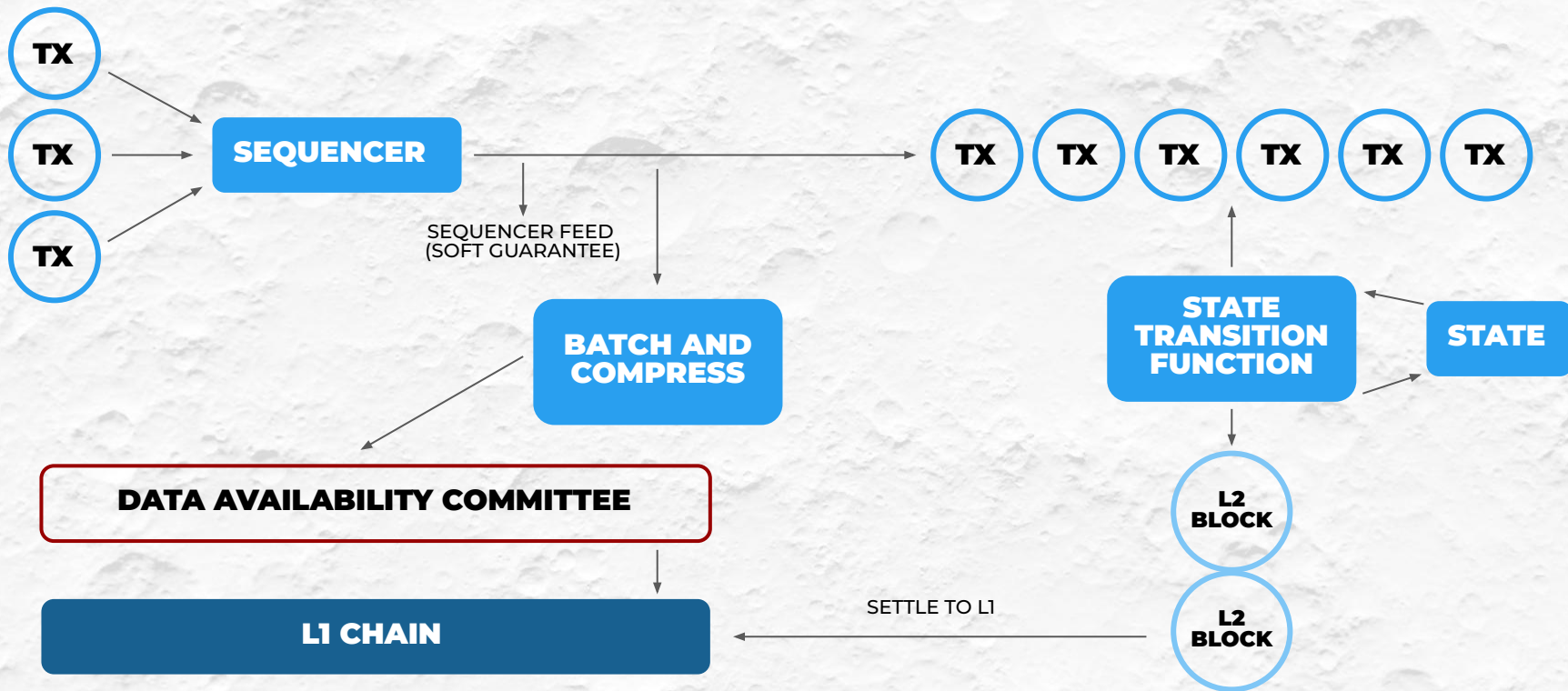
- No existing rollup has yet reached the fully decentralized future

- Arbitrum is the only Optimistic Rollup with live fraud proofs
    - But currently validation is permissioned

- Arbitrum's Sequencer provides fast finality guarantees
    - But only assuming you trust the sequencer

- Handling the possibility of critical bugs
    - Community conversation needs to be had, would Ethereum fork to fix a bug?
    - What kind of emergency path makes sense?