On the Path to a Rollup-Centric Future

Harry Kalodner
Offchain Labs
WHERE WE WERE

ANCIENT HISTORY

• 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 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.

- 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

$2B+
TOTAL VALUE LOCKED

55%+
ROLLUP MARKET SHARE

305+
DAPP INTEGRATIONS

500k+
UNIQUE ADDRESSES

BLUE CHIPS

UNISWAP
SUSHISWAP
AAVE
CURVE
YEARN

NATIVE

DOPEX
VESTA FINANCE
SPERAX
GMX
TRACER

INFRATRASTRUCTURE

CHAINLINK
Gnosis SAFE
INFURA
THE GRAPH
ALCHEMY
**Top 50 Gas Spenders (Sending Accounts that pay a lot of Gas)**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Address</th>
<th>Fees Last 3hrs</th>
<th>% Spent Last 3hrs</th>
<th>Fees Last 24hrs</th>
<th>% Spent Last 24hrs</th>
<th>Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Arbitrum: Sequence</td>
<td>$24,074.46 (12.06 ETH)</td>
<td>1.94%</td>
<td>$64,714.83 (31.67 ETH)</td>
<td>0.59%</td>
<td>🔥</td>
</tr>
<tr>
<td>2</td>
<td>Coinbase 4</td>
<td>$6,708.32 (2.25 ETH)</td>
<td>0.53%</td>
<td>$58,073.69 (29.44 ETH)</td>
<td>0.48%</td>
<td>🔥</td>
</tr>
<tr>
<td>3</td>
<td>Ethereum</td>
<td>$6,708.39 (2.25 ETH)</td>
<td>0.50%</td>
<td>$54,272.17 (26.17 ETH)</td>
<td>0.53%</td>
<td>🔥</td>
</tr>
</tbody>
</table>

**Top Accounts by ETH Balance**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Address</th>
<th>Tag</th>
<th>Balance</th>
<th>Percentage</th>
<th>Tag Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0x0000000000000000000000000000000000000000</td>
<td>ENS Deposit Contract</td>
<td>12,150,065.000302 Ether</td>
<td>10.21756024%</td>
<td>195,436</td>
</tr>
<tr>
<td>2</td>
<td>0xc323ac23b38239e8a0a367650d6505b7097c02</td>
<td>Wrapped Ether</td>
<td>5,914,618.2180610 ETH</td>
<td>4.97388419%</td>
<td>7,565,226</td>
</tr>
<tr>
<td>3</td>
<td>0xdad41a90e1d702e4b160a1f085623a0d5937d9f</td>
<td>Kraaken 13</td>
<td>2,115,000.000405 ETH</td>
<td>1.77984798%</td>
<td>85</td>
</tr>
<tr>
<td>4</td>
<td>0x46bde7d96d0f313d61a283f31d432400039d37b</td>
<td>Binance 7</td>
<td>1,996,000.000237 ETH</td>
<td>1.67658644%</td>
<td>1,066</td>
</tr>
<tr>
<td>5</td>
<td>0x72b40e055771770603d7ab379677733860802e</td>
<td>Wrapped ERC20</td>
<td>1,916,000.000000409 ETH</td>
<td>1.60033013%</td>
<td>448</td>
</tr>
<tr>
<td>6</td>
<td>0x7e4001e30786926e51a312076000000762559</td>
<td>Uniswap 1</td>
<td>1,496,000.00018827 Ether</td>
<td>1.2301150%</td>
<td>103</td>
</tr>
<tr>
<td>7</td>
<td>0xb9f4558369e4b25b773607650d6505b7097c02</td>
<td>Compound: cETH Token</td>
<td>803,342.46612161 ETH</td>
<td>0.79486029%</td>
<td>274,184</td>
</tr>
<tr>
<td>8</td>
<td>0xb1d68f9b03737c65a5347680e7d502d51ae96</td>
<td>Gemini 3</td>
<td>829,986.09501661 Ether</td>
<td>0.78165904%</td>
<td>336</td>
</tr>
<tr>
<td>9</td>
<td>0x2cd14076dd0359607d7bf472c5a25c068c6</td>
<td>Lido: Curve-Liquidity Pool Contract</td>
<td>810,865.19601641 ETH</td>
<td>0.69197608%</td>
<td>34,769</td>
</tr>
<tr>
<td>10</td>
<td>0x116a24e82bd01a5d5c1d5041b853b36d8d1d5</td>
<td>Arbitrum: Bridge</td>
<td>817,355.17600049 Ether</td>
<td>0.51518891%</td>
<td>50</td>
</tr>
</tbody>
</table>

**How much are rollups paying for Ethereum’s security?**

<table>
<thead>
<tr>
<th>Name</th>
<th>One day security costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arbitrum One</td>
<td>$70,949.80</td>
</tr>
<tr>
<td>Optimism</td>
<td>$64,195.94</td>
</tr>
<tr>
<td>Baba</td>
<td>$22,949.62</td>
</tr>
<tr>
<td>dYdX</td>
<td>$17,067.80</td>
</tr>
<tr>
<td>ZKSync</td>
<td>$15,057.64</td>
</tr>
<tr>
<td>Starkware</td>
<td>$9,799.68</td>
</tr>
<tr>
<td>Loopring</td>
<td>$3,978.75</td>
</tr>
<tr>
<td>Aztec Protocol</td>
<td>$2,085.44</td>
</tr>
<tr>
<td>Metis</td>
<td>$1,072.06</td>
</tr>
<tr>
<td>Polygon Hermez</td>
<td>$173.77</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$207,330.49</strong></td>
</tr>
</tbody>
</table>

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

- **Data Availability**: Transaction calldata is posted to Ethereum
- **L1-L2 Bridging**: Bridge contract can self-enforce validity of transaction on Arbitrum One
- **Security Mechanism**: Utilize fraud proofs, when malicious behaviour takes place, security is guaranteed by Ethereum L1
- **When 51% Attack Occurs**: Able to withstand a 99% attack on validators

**SIDECHAINS**

- **Data Availability**: Only block headers are available to Ethereum; in some cases they are not available at all
- **L1-L2 Bridging**: Bridge contracts rely on trusted set of parties to attest validity of transaction on Sidechain
- **Security Mechanism**: Rely on ⅔ of an independent validator set to be honest; Ethereum doesn’t guarantee security of the chain
- **When 51% Attack Occurs**: Fails when only 34% of validators are attacked
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
SEQUENCING & EXECUTION

SEQUENCING, THEN DETERMINISTIC EXECUTION

GETH AT THE CORE

SEPARATE EXECUTION FROM PROVING

OPTIMISTIC ROLLUP
**ABITRUM NITRO**

**SEQUENCING & EXECUTION**

**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)
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

NODE FUNCTIONALITY

ARBOS

GETH CORE

COMPILE TO NATIVE

RUN AS NODE

COMPILE TO WASM

USE FOR PROVING
A rollup-centric ethereum roadmap

What would a rollup-centric ethereum roadmap look like?

Last week the Optimism team announced the launch of the first stage of their testnet, and the roadmap to mainnet. They are not the only ones; Fuel is moving toward a testnet and Arbitrum has one. In the land of ZK rollups, Loopring, Zksync and the Starkware-tech-based Deversifi are already live and have users on mainnet. With OMG network’s mainnet beta, 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 and others 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

INTRODUCING ANYTRUST

DATA AVAILABILITY COMMITTEE

L1 CHAIN

L2 BLOCK

L2 BLOCK

STATE

STATE TRANSITION FUNCTION

BATCH AND COMPRESS

SEQUENCER FEED (SOFT GUARANTEE)

SEQUENCER

TX

TX

TX

TX

TX

TX

TX

TX

TX

TX
- 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?