Lesson 5

Week 2

Lesson 5 - Understanding and Analysing Layer 2

Lesson 6 - Agnostic Layer 2 Transaction Lifecycle

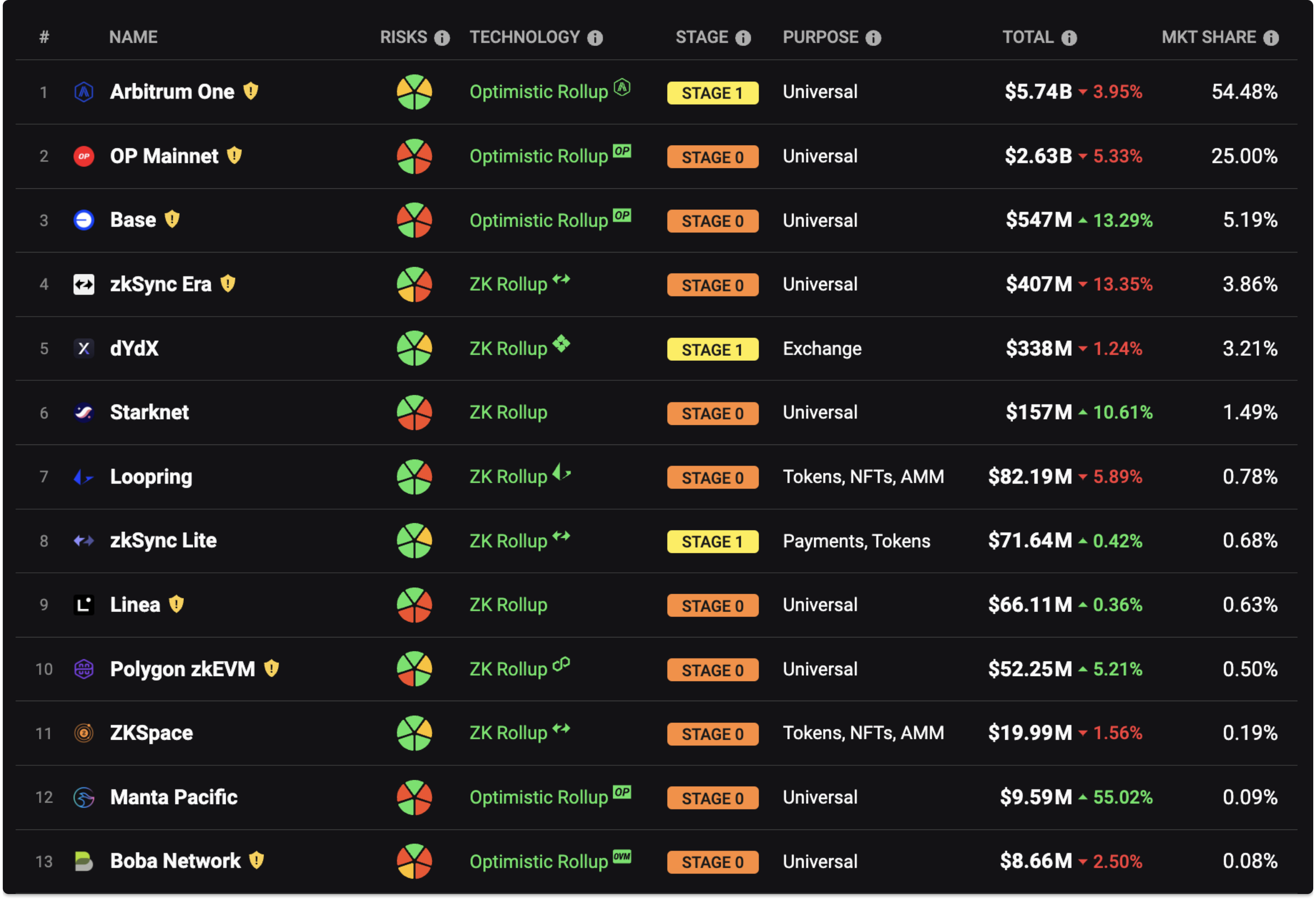
Lesson 7 - Optimistic Rollups v ZK Rollups

Lesson 8 -What's next in Layer 2 part 1 : Decentralised Sequencers

Today's topics

- Categorising L2s
- Analysis criteria
- Rollup stages
- Op Stack and ZK Stack summary

> ## Layer 2 Theory
>
> We can categorise the L2 chains in a number of ways.
> The Ethereum documentation makes distinctions between generalised L2s and application specific L2s.
>
> ### Generalised Layer 2
>
> These include Arbitrum 1, Optimism, Boba and Starknet. The philosophy behind these is that anything possible on Ethereum mainnet should be transferable to the L2.
>
> ### Application specific layer 2s
>
> These include Loopring, ZkSync, ZkSpace and Aztec.
> These L2s are optimised for specific application space.
>
> ### L2 Beat Overview
>
> See Summary
>
> L2 Systems
> Active projects see chart



#	NAME	RISKS	TECHNOLOGY	STAGE	PURPOSE	TOTAL	MKT SHARE
1	Arbitrum One		Optimistic Rollup	STAGE 1	Universal	$5.74B ▾ 3.95%	54.48%
2	OP Mainnet		Optimistic Rollup	STAGE 0	Universal	$2.63B ▾ 5.33%	25.00%
3	Base		Optimistic Rollup	STAGE 0	Universal	$547M ▴ 13.29%	5.19%
4	zkSync Era		ZK Rollup	STAGE 0	Universal	$407M ▾ 13.35%	3.86%
5	dYdX		ZK Rollup	STAGE 1	Exchange	$338M ▾ 1.24%	3.21%
6	Starknet		ZK Rollup	STAGE 0	Universal	$157M ▴ 10.61%	1.49%
7	Loopring		ZK Rollup	STAGE 0	Tokens, NFTs, AMM	$82.19M ▾ 5.89%	0.78%
8	zkSync Lite		ZK Rollup	STAGE 1	Payments, Tokens	$71.64M ▴ 0.42%	0.68%
9	Linea		ZK Rollup	STAGE 0	Universal	$66.11M ▴ 0.36%	0.63%
10	Polygon zkEVM		ZK Rollup	STAGE 0	Universal	$52.25M ▴ 5.21%	0.50%
11	ZKSpace		ZK Rollup	STAGE 0	Tokens, NFTs, AMM	$19.99M ▾ 1.56%	0.19%
12	Manta Pacific		Optimistic Rollup	STAGE 0	Universal	$9.59M ▴ 55.02%	0.09%
13	Boba Network		Optimistic Rollup	STAGE 0	Universal	$8.66M ▾ 2.50%	0.08%

Analysis Criteria

- purpose
- types of L2
- criteria for analysis
  - TVL
  - data availability
  - performance / scalability
  - fees
  - risk https://l2beat.com/scaling/risk
  - governance / upgradability
  - failure of sequencer / proposer (liveness)
- performance
- components

Modular Rollup Theory

History of Rollups
2020 monolithic rollups - categorised by proof type

later it was realised that proofs should be separated from execution, and proofs should be very general

then projects started to break out the data availability

The end result of this (this is focussed on the OP stack)
we get 3 primary layers

- consensus
- execution
- settlement
  so similar to our ideas about modular blockchains

Consensus

- data availability
- derivation

Data availability

```
 Ethereum blocks / calldata
Ethereum 4844
Celestia
```

Derivation

This takes the DA layer and the state of the rollup, parses it and produces the inputs to the chain via Engine API payloads (for OP stack).
The payloads are what we use for execution.
Source of this data could be

- From what the sequencer has posted to the L1
- L1 blocks
- Special deposit contracts

> The ability to derive L2 payloads from anything on L1, or a DA layer is a potentially very powerful ability.
>
> ### Execution layer
>
> This is where we take the previous state of the system, the execution payloads and produce our next state.
> The execution could be using the EVM, or something else, there may need to be rollup specific features to the EVM, for example handling L1 <-> L2 messages.
>
> ### Settlement
>
> Settlement is the external view of your chain and the ability to prove that.
> We are usually interested in a state root, and we have a validation function based on
>
> - previous state
> - next state
> - execution layer
> - data availability layer

Rollup Stages

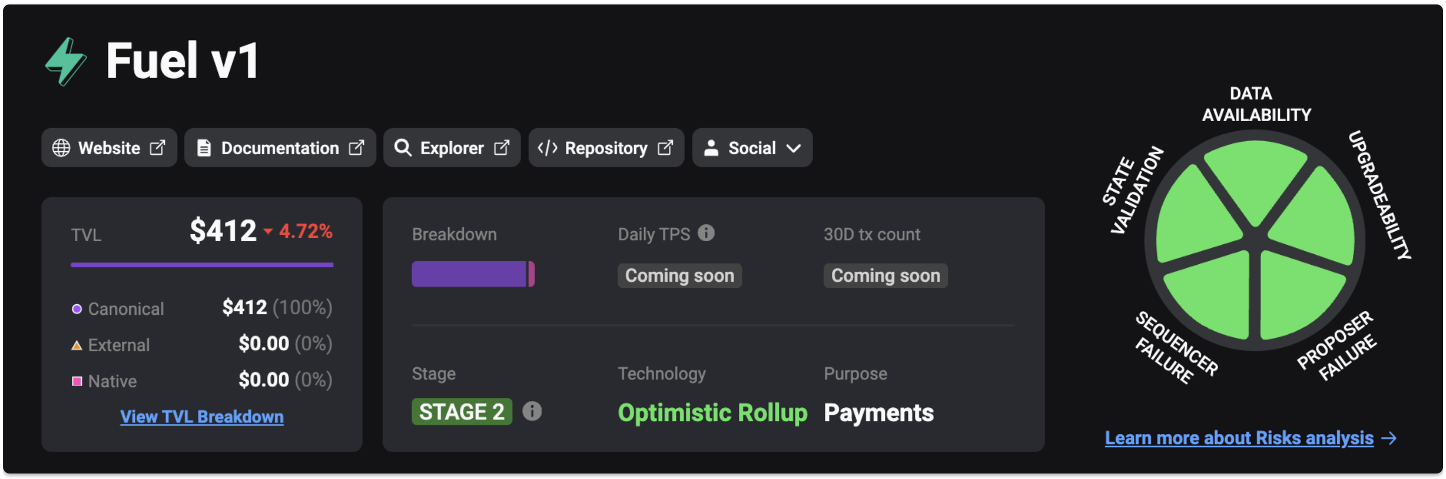
See Article
A concept introduced by L2Beat to indicate maturity, based on ideas from Vitalik .

1. **Stage 0 — Full Training Wheels:** At this stage, the rollup is effectively run by the operators. Still, there is an source-available software that allows for the reconstruction of the state from the data posted on L1, used to compare state roots with the proposed ones.
2. **Stage 1 — Limited Training Wheels:** In this stage, the rollup transitions to being governed by smart contracts. However, a Security Council might remain in place to address potential bugs. This stage is characterized by the implementation of a fully functional proof system, decentralization of fraud proof submission, and provision for user exits without operator coordination. The Security Council, comprised of a diverse set of participants, provides a safety net, but its power also poses a potential risk.
3. **Stage 2 — No Training Wheels:** This is the final stage where the rollup becomes fully managed by smart contracts. At this point, the fraud proof system is permissionless, and users are given ample time to exit in the event of unwanted upgrades. The Security Council's role is strictly confined to addressing soundness errors that can be adjudicated on-chain, and users are protected from governance attacks.

Stage 2 Projects

Of the top 22 rollups from L2Beat, only 2 have reached stage 2

Fuel



Fuel v1

TVL $412 ▾ 4.72%

Canonical $412 (100%)
External $0.00 (0%)
Native $0.00 (0%)
View TVL Breakdown

Breakdown

Daily TPS: Coming soon

30D tx count: Coming soon

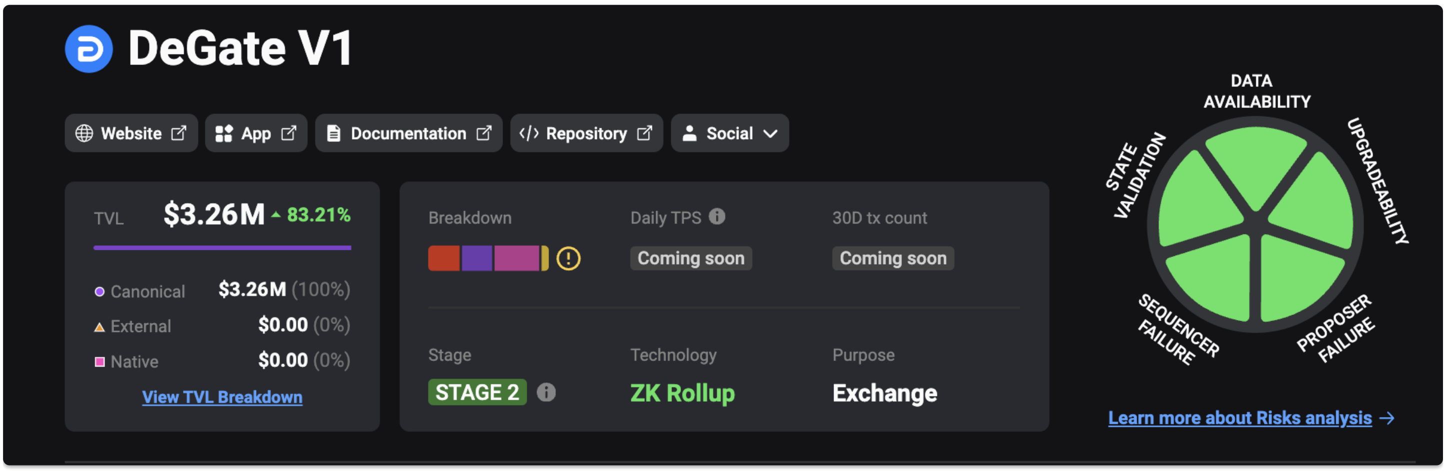
Stage: STAGE 2

Technology: Optimistic Rollup

Purpose: Payments

Fuel aims to be a complete optimistic rollup with low transaction costs, high speed and high throughput.

DeGate V1



DeGate V1

TVL $3.26M ▴ 83.21%

Canonical $3.26M (100%)
External $0.00 (0%)
Native $0.00 (0%)
View TVL Breakdown

Breakdown

Daily TPS: Coming soon

30D tx count: Coming soon

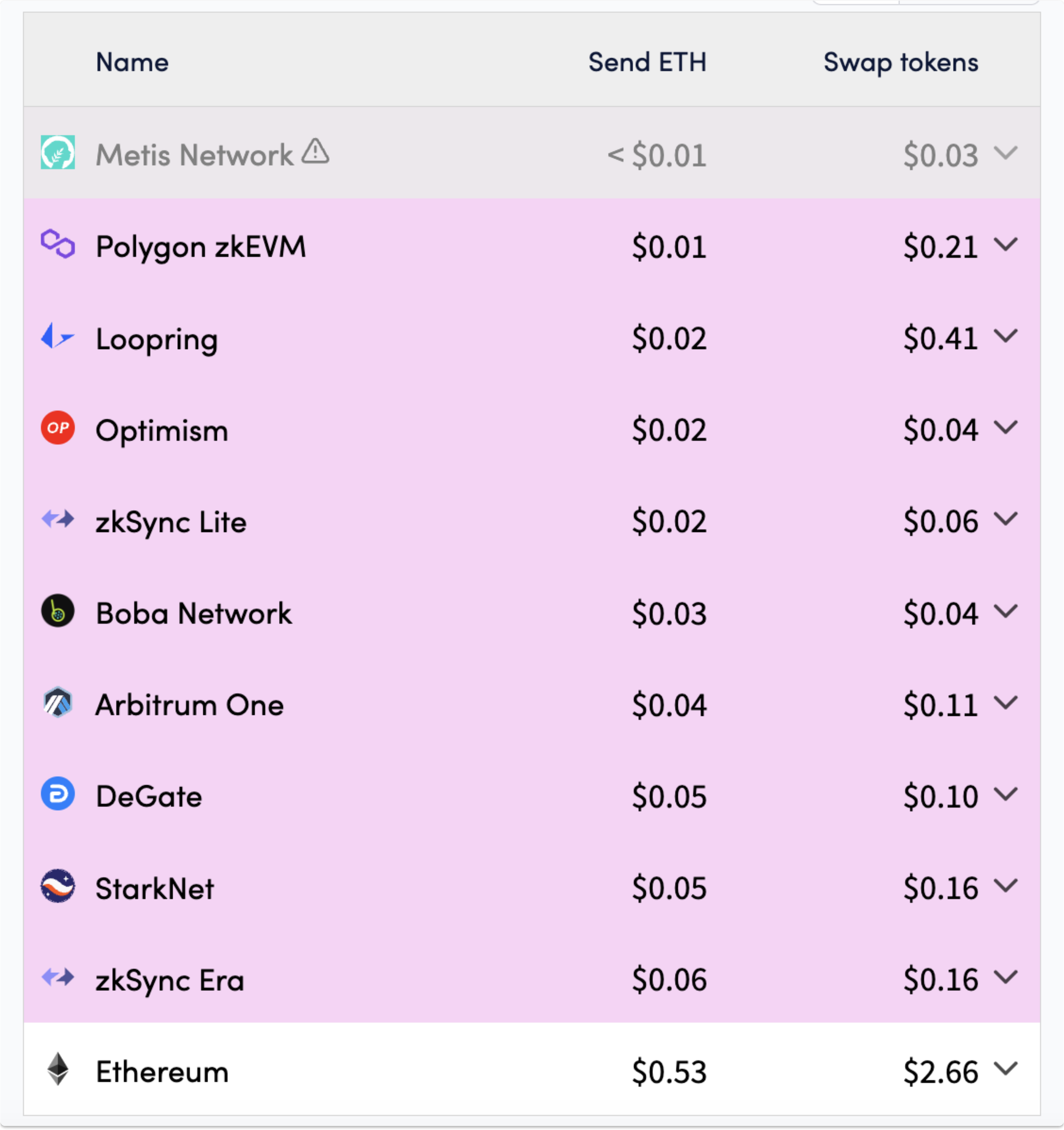
Stage: STAGE 2

Technology: ZK Rollup

Purpose: Exchange

DeGate is an app-specific ZK rollup that enables a trustless, fast and low-fee decentralized order book exchange, helping users to trade easy and sleep easy. DeGate smart contracts are forked from Loopring V3.

Fees on a layer 2



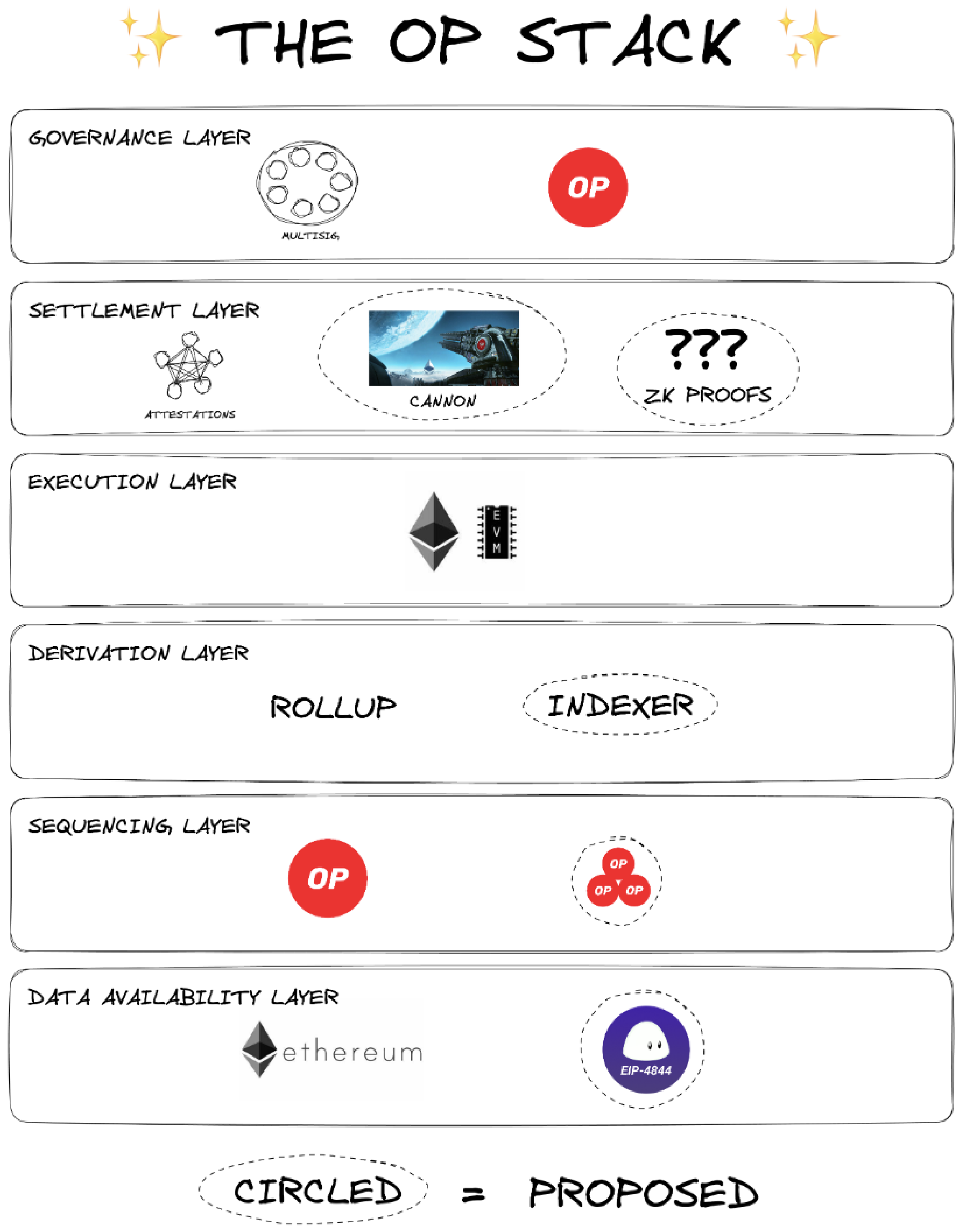
Name	Send ETH	Swap tokens
Metis Network ⚠	< $0.01	$0.03
Polygon zkEVM	$0.01	$0.21
Loopring	$0.02	$0.41
Optimism	$0.02	$0.04
zkSync Lite	$0.02	$0.06
Boba Network	$0.03	$0.04
Arbitrum One	$0.04	$0.11
DeGate	$0.05	$0.10
StarkNet	$0.05	$0.16
zkSync Era	$0.06	$0.16
Ethereum	$0.53	$2.66

OP Stack

See Docs
See Introduction video

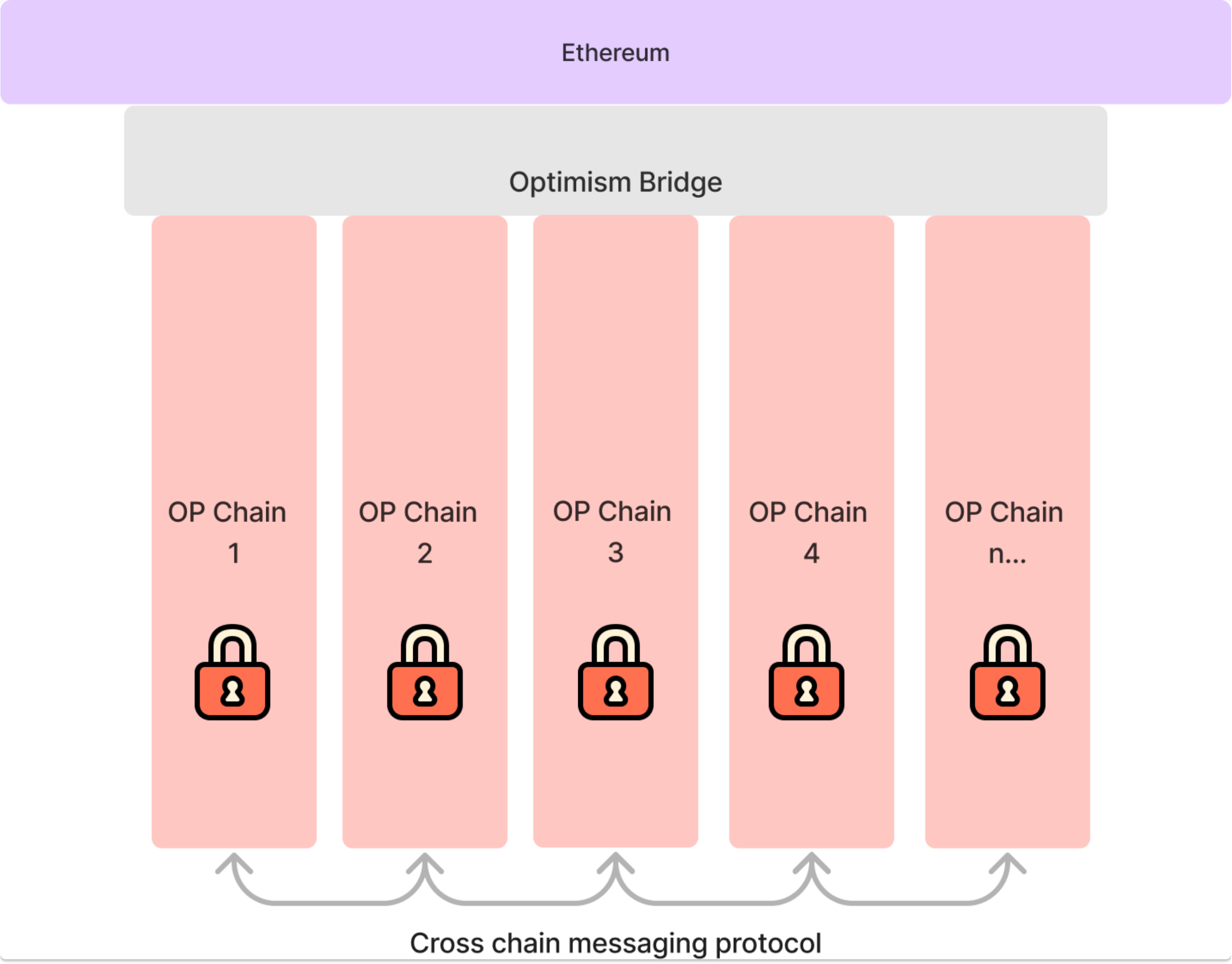
The OP Stack is the open-source development stack that powers Optimism.

Optimism Bedrock is the current iteration of the OP Stack.



Optimism Superchain

This is a proposed network of L2s that share security, communication layers, and a common development stack - the OP Stack.



Layers

Data Availability

The Data Availability Layer defines where the raw inputs to an OP Stack based chain are published. An OP Stack chain can use one or more Data Availability module to source its input data. Because an OP Stack chain is derived from the Data Availability Layer, the Data Availability module(s) used have a significant impact on the security model of a system. For example, if a certain piece of data can no longer be retrieved from the Data Availability Layer, it may not be possible to sync the chain.

Ethereum DA

Ethereum DA is currently the most widely used Data Availability module for the OP Stack. When using the Ethereum DA module, source data can be derived from any piece of information accessible on the Ethereum blockchain. This includes Ethereum calldata, events, and 4844 data blobs.

Sequencing

The Sequencing Layer determines how user transactions on an OP Stack chain are collected and published to the Data Availability Layer module(s) in use. In the default Rollup configuration of the OP Stack, Sequencing is typically handled by a single dedicated Sequencer. Rules defined in the Derivation Layer generally restrict the Sequencer’s ability to withhold transactions for more than a specific period of time. In the proposed future, Sequencing will be modular such that chains can easily select and change the mechanism that controls their current Sequencer.

Single Sequencer

The default Sequencer module for the OP Stack is the Single Sequencer module in which a dedicated actor is given the ability to act as the Sequencer. The Single Sequencer module allows a governance mechanism to determine who may act as the Sequencer at any given time.

Multiple Sequencer (proposed)

A simple modification to the Single Sequencer module is the Multiple Sequencer module in which the Sequencer at any given time is selected from a pre-defined set of possible actors. Individual OP Stack based chains would be able to determine the exact mechanism that defines the set of possible Sequencers and the mechanism that selects a Sequencer from the set.

Derivation

The Derivation Layer defines how the raw data in the Data Availability Layer is processed to form the processed inputs that are sent to the Execution Layer via the standard Ethereum Engine API . The Derivation Layer may also use the current system state, as defined by the Execution Layer, to inform the parsing of raw input data. The Derivation Layer can be modified to derive Engine API inputs from many different data sources. The Derivation Layer is typically tied closely to the Data Availability Layer because it must understand how to parse any raw input data.

Rollup

The Rollup module derives Engine API inputs from Ethereum block data, Sequencer transaction batches, Deposited transaction events, and more.

Indexer (proposed)

The Indexer module is a proposed Derivation Layer module that would derive Engine API inputs when transactions are sent to, events are emitted by, or storage is modified in specific smart contracts on a Data Availability Layer module like Ethereum DA.

Execution

The Execution Layer defines the structure of state within an OP Stack system and defines the state transition function that mutates this state. State transitions are triggered when inputs are received from the Derivation Layer via the Engine API. The Execution Layer abstraction opens up the door to EVM modifications or different underlying VMs entirely.

EVM

The EVM is an Execution Layer module that uses the same state representation and state transition function as the Ethereum Virtual Machine. The EVM module in the Ethereum Rollup configuration of the OP Stack is a lightly modifiedversion of the EVM that adds support for L2 transactions initiated on Ethereum and adds an extra L1 Data Fee to each transaction to account for the cost of publishing transactions to Ethereum.

Settlement Layer

The Settlement Layer is a mechanism on external blockchains that establish a view of the state of an OP Stack chain on those external chains (including other OP Stack chains). For each OP Stack chain, there may be one or more Settlement mechanisms on one or more external chains. Settlement Layer mechanisms are read-only and allow parties external to the blockchain to make decisions based on the state of an OP Stack chain.

The term “Settlement Layer” has its origins in the fact that Settlement Layer mechanisms are often used to handle withdrawals of assets out of a blockchain. This sort of withdrawal system first involves proving the state of the target blockchain to some third-party chain and then processing a withdrawal based on that state. However, the Settlement Layer is not strictly (or even predominantly) financial and, at its core, simply allows a third-party chain to become aware of the state of the target chain.

Once a transaction is published and finalized on the corresponding Data Availability layer, the transaction is also finalized on the OP Stack chain. Short of breaking the underlying Data Availability layer, it can no longer be modified or removed. It may not be accepted by the Settlement Layer yet because the Settlement Layer needs to be able to verify transaction *results*, but the transaction itself is already immutable.

OptimismPortal

This is the bridge between L2 and L1 that allows messaging.

ZKStack

See article
We will cover this in more detail in future lessons.

The ZK Stack is a modular, open-source framework that is both free and designed to build custom ZK-powered L2s and L3s.
There are 2 key features

- Sovereignty
- Seamless Connectivity

The aim of the zk stack is to create a hyperscalable unified liquidity network.

Comparison with Madera / OPStack

Madara from Starkware is more focussed on providing a sequencer that can be used for L3s
OP stack - it is harder to have interoperability
ZK stack has the advantage that the prover has lower memory requirements.

> All of these try to solve the fragmentation of liquidity, but the chains involved are still distinct in that they don't for example share accounts