The L2BEAT research team would like to introduce a risk framework designed to evaluate the security profile of data availability (DA) solutions. This framework extends our previous efforts in assessing the security of different L2 architectures and aims to provide a risk classification system specific to DA providers. At this stage, we invite broad community feedback to refine and enhance our framework.

Context

Data Availability (DA) layers need to guarantee that users have access to L2 transaction data. In ZK rollups, users need to be able to access transaction data or state diffs to recreate and advance the state (e.g., for withdrawals). Additionally, in Optimistic rollups users need the data to be able to challenge a dishonest state root proposer.

To ensure that data was made available, L2 state validating bridges on the settlement layer require proof that, at some point in time, the data was publicly available on the DA layer. Should L2s publish data directly to Ethereum in the form of blobs or calldata, this requirement is inherently satisfied since all data is posted onchain, and validating bridges can access its commitment. On the other hand, if L2 chooses an external DA provider, only data commitment is posted to Ethereum (while full data is posted to that DA provider). In this case, Ethereum must be “convinced” that full data was indeed made available. This is done via a so-called DA bridge, which simply attests that some data of a given commitment was made available to the external system (so this DA bridge works as an Oracle to Ethereum).

[

General-DA-Scheme3

1641×441 78.9 KB

](https://europe1.discourse-cdn.com/standard20/uploads/l2beat/original/1X/6de085a06e941412e640a0d0a121a3d5c84c34e5.png)

From Ethereum’s point of view, the security assumptions of external DA providers are not only dependent on the intrinsic characteristics of the DA solution itself, but also on how well its security properties are mapped to the data attestation posted to the DA bridge on Ethereum.

The following section aims to categorize the security guarantees that DA solutions need to provide for L2s to inherit the security properties of the settlement layer.

1 - Economic Security

Economic security measures the level of trust we can place in the majority consensus, seen as the amount of funds a committee would need to burn to successfully deceive the DA bridge. It is scored as:

Levels

- Green: Bribery risk is quantifiable onchain and total slashable funds > total value secured
- Committee members hold slashable assets on a public network
- Committee members hold slashable assets on a public network
- Yellow: Bribery risk is publicly verifiable offchain (e.g., reputational risk) or total slashable funds < total value secured
- Committee members bribery risk is publicly verifiable, but not slashable
- Committee members bribery risk is publicly verifiable, but not slashable
- Red: Bribery risk is not publicly verifiable or quantifiable (e.g., anon committee)

2 - Fraud Detection Mechanism

The fraud detection mechanism category measures how effectively users can protect themselves against a malicious majority of committee members, such as validators.

The issue with data availability attestations is that should data be unavailable, we cannot easily say - as an independent observer - if the missing transaction was never published by the block producer or it was published but for some reason we did not receive it. As outlined in the fisherman dilemma, a data withholding attack is not an attributable fault and no slashing mechanism can be achieved at smart contract level. Thus, there needs to be a mechanism for slashing on the DA layer to prevent a nothing-at-stake problem. In some projects, this mechanism is data availability sampling (DAS). Light clients failing to perform DAS would stop processing new block headers, forcing a halt and resolving to social consensus to slash malicious validators.

This data availability verification cannot be performed by Ethereum, which due to the passive nature of smart contracts, cannot actively sample data from external sources. Hence the risk analysis for Optimiums and Validiums needs to focus on the point of view of an offchain observer, like a lightnode, and assess its ability to detect fraud on the DA layer. It is scored

as:

Levels

- Green: Data withholding attacks and invalid data can be detected on the DA layer
- DAS with block reconstruction, has erasure coding fraud proof
- DAS with block reconstruction, has erasure coding fraud proof
- Yellow: DAS without block reconstruction, has erasure coding fraud proof
- Red: No fraud detection mechanism

In the future, these levels could be expanded to include additional levels specific to DAS security, such as anonymous sampling to protect against selective share disclosure attacks. For more details, see this post on different DAS security levels.

Note that while current Proto-Danksharding (EIP-4844) does not have fraud protection mechanism against dishonest majority, future Danksharding plans to have a DAS mechanism in place allowing for efficient light clients.

3 - Attestation Security

Attestation security evaluates the robustness of the DA bridge's ability to verify data commitments without introducing additional trust assumptions. It assesses whether the DA bridge can securely confirm that the data availability attestations are backed by the DA layer's economic security, ensuring that the signatures from the DA layer are accurately verified and tracked on-chain. It is scored as:

Levels

- Green:
- Verifies attestations are backed by DA layer-defined economic security, committee signatures are verified and the set of signers is tracked onchain. In the case of zk-proof data commitments, the correctness and threshold of the validator signatures should be verified as part of the proof. Signature equivocation is not allowed.
- Commitment frequency should respect DA finality and committee membership unbonding period
- Verifies attestations are backed by DA layer-defined economic security, committee signatures are verified and the set of signers is tracked onchain. In the case of zk-proof data commitments, the correctness and threshold of the validator signatures should be verified as part of the proof. Signature equivocation is not allowed.
- Commitment frequency should respect DA finality and committee membership unbonding period
- Yellow:
- Possible signature equivocation, different set of signers (typically much smaller) than DA layer itself
- Possible signature equivocation, different set of signers (typically much smaller) than DA layer itself
- Red: No bridge or no requirement satisfied

4 - Exit Window

The exit window criterion examines the upgradeability of the DA bridge, specifically focusing on the mechanisms in place for withdrawals and the time allowed for users to exit in case of an upgrade. This category considers the presence of timelocks or other security measures that ensure users have adequate time to withdraw their funds before any changes to the bridge contract are implemented. It is scored as:

Levels

- Green: Immutable bridge, or upgrade timelock allowing enough time for users to exit
- Yellow: Security council can upgrade the bridge, or an EOA with timelock
- Red: Smart contract (e.g., multisig) without timelock, or an EOA can upgrade the bridge

5 - Accessibility

Accessibility measures the ease with which data can be accessed directly from the Ethereum network. This category distinguishes between DA solutions that are integrated into the Ethereum protocol (enshrined) and those that are not. It is scored as:

Levels

- Green: Enshrined in the Ethereum protocol
- Red: Not enshrined

It is important to note that this risk category applies only to Ethereum L2s and not Sovereign Rollups using DA Layers independently.

This risk framework is intended to guide L2 users in understanding the different DA providers risk profiles, as well as developers and researchers in enhancing the security of L2 scaling solutions. We invite the community to share their feedback to finalize this risk framework, ensuring it accurately assesses the risks of data availability solutions.