Building upon the original framework outlined in our previouspost, the L2BEAT research team has updated the risk categories and their respective scoring methodology, incorporating community feedback.

To provide a clearer analysis, we have divided the risks into two main categories: DA Layer Security

and DA Bridge Security

. This separation allows for a more focused evaluation of the specific risks and security considerations inherent to each component.

[

dascheme

1684×466 77 KB

](https://europe1.discourse-cdn.com/flex017/uploads/l2beat/original/1X/61d34834ab683c9bc09c1a7d40f284fbefb1cfb1.png)

DA Layer Security

1. Economic Security

Economic security measures the level of trust in the majority consensus of the DA layer, quantified by the amount of funds the DA layer committee would need to burn to perform a successful data withholding attack. We have updated this category to distinguish more clearly between cryptoeconomic security and reputational factors, considering the nature and amount of slashable assets.

- Green
- Sufficient Slashable Funds:

Bribery risk is quantifiable onchain, and the total slashable funds exceed the total value secured.

- Sufficient Slashable Funds:

Bribery risk is quantifiable onchain, and the total slashable funds exceed the total value secured.

- Yellow
- Limited Slashable Funds:

Total slashable funds are less than the total value secured, meeting a minimum threshold of 1/3 of the total value secured.

- Indirect Economic Security through Reputational Risk:

If there is no direct economic security in the form of a stake, but the bribery risk is publicly verifiable off-chain (i.e., based on the reputational risk of well-known entities). There are a minimum of 5 external actors as part of the committee.

- Limited Slashable Funds:

Total slashable funds are less than the total value secured, meeting a minimum threshold of 1/3 of the total value secured.

- Indirect Economic Security through Reputational Risk:

If there is no direct economic security in the form of a stake, but the bribery risk is publicly verifiable off-chain (i.e., based on the reputational risk of well-known entities). There are a minimum of 5 external actors as part of the committee.

- Red
- Insufficient Slashable Assets:

Committee members hold less than 1/3 of the total value secured in slashable assets bonded to the DA layer.

- Minimal Reputational Deterrent:

The committee members are not fully publicly disclosed, reputational risk is insufficient to deter malicious behaviour.

- Insufficient Slashable Assets:

Committee members hold less than 1/3 of the total value secured in slashable assets bonded to the DA layer.

- Minimal Reputational Deterrent:

The committee members are not fully publicly disclosed, reputational risk is insufficient to deter malicious behaviour.

2. Fraud Detection Mechanism

This category assesses how effectively users can protect themselves against a malicious majority of DA validators or committee members. It evaluates the mechanisms in place for detecting data-withholding attacks and invalid erasure-coded data on the DA layer.

- Green
- Robust Detection:

Data withholding attacks and invalid erasure-coded data can be detected on the DA layer. Data Availability Sampling (DAS) is available with robust block reconstruction for erasure coding fraud proofs (if applicable), and a minimum number of light nodes are present on the network to be able to detect invalid blocks and reconstruct the data collectively.

- Robust Detection:

Data withholding attacks and invalid erasure-coded data can be detected on the DA layer. Data Availability Sampling (DAS) is available with robust block reconstruction for erasure coding fraud proofs (if applicable), and a minimum number of light nodes are present on the network to be able to detect invalid blocks and reconstruct the data collectively.

- Yellow
- Basic Detection:

DAS without robust block reconstruction, no erasure-coding validity proofs, or lacking the minimum number of light nodes on the network to allow full data reconstruction.

- Basic Detection:

DAS without robust block reconstruction, no erasure-coding validity proofs, or lacking the minimum number of light nodes on the network to allow full data reconstruction.

- Red
- No Detection Mechanism:

Lacks any fraud detection mechanism on the DA layer.

- No Detection Mechanism:

Lacks any fraud detection mechanism on the DA layer.

DA Bridge Security

1. Committee Security

Committee security evaluates the committee attesting to the DA bridge concerning its size, member diversity, and data availability attestation and retrievability threshold. The scoring follows the Stages framework committee requirements, with adjustments to make it applicable to DA public networks.

- Green
- Robust and Diverse Committee:

The committee requires that the minimum proportion of honest members (or the network stake) necessary to safely attest to the availability of the data does not exceed 1/3. Entering the operators set is permissionless, subject only to stake requirements and an honest majority of committee members (or a decentralized governance process).

- Robust and Diverse Committee:

The committee requires that the minimum proportion of honest members (or the network stake) necessary to safely attest to the availability of the data does not exceed 1/3. Entering the operators set is permissionless, subject only to stake requirements and an honest majority of committee members (or a decentralized governance process).

- Yellow
- Limited Committee Security:

The committee requires the minimum proportion of honest members to not exceed 1/3, with a minimum of 5 external actors. The entering or exiting of committee members from the active operators set can be triggered or vetoed by a centralized entity.

- Limited Committee Security:

The committee requires the minimum proportion of honest members to not exceed 1/3, with a minimum of 5 external actors.

The entering or exiting of committee members from the active operators set can be triggered or vetoed by a centralized entity.

- Red
- No Committee Security:

The committee does not meet essential security requirements due to inadequate size, lack of diversity, or threshold parameters. This is also the case if no effective DA bridge exists, making the system rely on an honest sequencer assumption.

- No Committee Security:

The committee does not meet essential security requirements due to inadequate size, lack of diversity, or threshold parameters. This is also the case if no effective DA bridge exists, making the system rely on an honest sequencer assumption.

2. Upgradability

This category examines the upgradeability of the DA bridge and its dependencies, focusing on mechanisms that allow users sufficient time to exit in case of an upgrade. It is important to note that the immutability of the DA bridge is a desirable property only when the bridge has achieved the defined level of security. An immutable bridge with no committee security (i.e., scoring Red above) will score Red in this dimension, to emphasize that mutable insecure systems are better than immutable insecure systems due to their ability to improve over time.

- Green
- Secure Upgradeability:

The bridge should have at least a 30-day delay on upgrades, regardless of who initiates the upgrade. Immediate upgrades from a Security Council should be limited to onchain provable bugs.

- Secure Upgradeability:

The bridge should have at least a 30-day delay on upgrades, regardless of who initiates the upgrade. Immediate upgrades from a Security Council should be limited to onchain provable bugs.

- Yellow
- Moderate Upgradeability Security

: The bridge should have at least a 7-day delay on upgrades. Immediate (0-day delay) upgrades are allowed through a decentralized governance process or a properly set up Security Council as defined in the Stages framework.

- Moderate Upgradeability Security

: The bridge should have at least a 7-day delay on upgrades. Immediate (0-day delay) upgrades are allowed through a decentralized governance process or a properly set up Security Council as defined in the Stages framework.

- Red
- Uncontrolled Upgradeability:

A smart contract (e.g., multisig) without a timelock or an EOA can upgrade the bridge. Upgrade delay is below 7 days. If no delay exists due to the lack of a DA bridge, the system is insecure as it relies on an honest sequencer assumption.

- Uncontrolled Upgradeability:

A smart contract (e.g., multisig) without a timelock or an EOA can upgrade the bridge. Upgrade delay is below 7 days. If no delay exists due to the lack of a DA bridge, the system is insecure as it relies on an honest sequencer assumption.

Note:

While user exit cannot be guaranteed (as it also depends on individual L2 designs), the aim is to provide users with enough time to be aware of an upgrade and try to exit the system if they choose. Users should also check the specific exit window of the individual project of interest.

3. Relayer Failure

The relayer is the entity responsible for forwarding DA commitments from the DA layer to the DA bridge on Ethereum. A permissioned relayer poses a liveness risk to the DA bridge if users cannot independently post DA commitments in case of relayer failure or misbehavior.

- Green
- Self-propose

: Users can self-propose DA commitments permissionlessly if the centralized relayer fails to do so.

- Self-propose

: Users can self-propose DA commitments permissionlessly if the centralized relayer fails to do so.

- Yellow
- Governance Rotation

: There exists a Security Council or a decentralized governance system able to rotate the permissioned relayer in case of relayer failure or misbehavior. If the system allows a whitelist for relayers, it should comprise at least 5 external actors.

- Governance Rotation

: There exists a Security Council or a decentralized governance system able to rotate the permissioned relayer in case of relayer failure or misbehavior. If the system allows a whitelist for relayers, it should comprise at least 5 external actors.

- Red
- No Mechanism

: The DA bridge halts in case of failure of the permissioned relayer.

- No Mechanism

: The DA bridge halts in case of failure of the permissioned relayer.

FAQ

1. What assets count towards economic security?

Slashable native

assets explicitly bonded by committee members to the DA layer's social contract on a public network are counted towards economic security. Non-native

assets do not count towards economic security unless purposefully created for intersubjective faults, with the possibility for slashing (e.g., through forking) and explicitly bonded to the DA layer's social contract.

1. How can a committee satisfy the "public members" requirement?

Committee members must be publicly announced through any public channel available to the project. The full list of entities belonging to the committee should be disclosed with respective public keys or addresses.

1. Is there a difference between erasure-coding validity proofs and invalidity proofs?

Validity proofs such as KZG polynomial commitments allow sampling light nodes to verify the sample integrity by checking the openings against the commitments with each sample. In a fraud-proof-based scheme, light nodes need to wait for the full length of the fraud-proof window before considering a block finalized. Checking the integrity of the data is usually performed by full nodes, which need to collect sufficient data to attempt block reconstruction and generate erasure-coding fraud proofs should reconstruction fail. Due to this requirement, block reconstruction time in worst-case scenarios (i.e., selective disclosure attacks) being less than the fraud-proof window becomes necessary to achieve a robust fraud detection mechanism.

1. Are the DA Layer Committee and the DA Bridge Committee always the same?

Typically, the DA layer committee and the DA bridge are the same, but this is not always the case. For example, a DA bridge could receive data availability attestations from Celestia via an external oracle, such as Chainlink CCIP. In this scenario, the DA bridge's security would be provided by the external oracle committee, while the economic security of the DA layer would remain with the DA layer validators.