Authored Blobs

Overview

A new blob type, called an "authored blob," is being introduced to simplify the verification process of blob signers in rollups that use a fork-choice rule, where one or more sequencers are whitelisted. This change addresses the inefficiencies and complexities in the current method of verifying blob authenticity.

Previously, the process of verifying the signer of a blob in Celestia involved multiple steps, including retrieving PayForBlobs (PFBs) from the PFB namespace, verifying the signer, and matching blobs to their corresponding PFBs. For rollups using zero-knowledge proofs (such as Sovereign), this process was even more complex, requiring additional steps in the circuit to map and verify blob commitments and signers.

The introduction of the authored blob includes a new field for the signer directly within the blob structure. Validators now simply need to verify that the signer's field in the blob matches the expected sequencer, eliminating the need to separately retrieve and match PFBs. This simplification reduces computational complexity and streamlines the validation process for rollups, making it easier to verify the signer of a blob against the expected sequencer.

Analysis

xTarget Summary

- **Type**: Protocol and Implementation
- **Platform**: Go
- **Artifacts**:
  - go-square: commit a446cee3ad5fd5be5e59dc9a027bc35b4f6100cb[1]
  - celestia-app: commit 306c58745d135d31c3777a1af2f58d50adbd32c8[2]

Engagement Summary

- **Dates**: 16.09.2024. -20.09.2024.
- **Method**: Manual code review, protocol analysis

1 https://github.com/celestiaorg/go-square/tree/v2.0.0

2 https://github.com/celestiaorg/celestia-app/commit/306c58745d135d31c3777a1af2f58d50adbd32c8

go-square

`BlobProto` as a representation of a blob (binary large object) is extended with an additional field named signer[3]. Signer is sdk.AccAddress that paid for this blob. This field is optional and can only be used when share_version is set to 1 which was until this change always been set to zero.

Writing blob to sparse share: This signer attribute will be written to a share only when share_version is set to 1. This is done in the `SparseShareSplitter` `Write` function here[4].

Parsing individual blobs from shares: On each sequence start signer is read from the share here[5] and thus included in the sequence which is later used to create a blob[6].

celestia-app

Prepare Proposal

The new square version (`squarev2`), that includes the option of having the signer of Blob, is used from v3 app version. Thus based on the app version `PrepareProposal` decides[7] which square version to use.

Process Proposal

The new square version (`squarev2`), that includes the option of having the signer of Blob, is used from v3 app version. Thus based on the app version `ProcessProposal` decides[8] which square version to use.

ValidateBlobTx

It includes a check if the PFB msg signer is the same as the blob signer if there is any here[9]. It is used in `CheckTx` and `ProcessProposal`.

Conclusion

Authored Blobs is a small feature whose purpose is a better user experience when verifying that the sequencer is the one who created the blob and sent it to Celestia. As expected audit of this component proved that basically there is no attack surface. The implementation is simple and what was done through this audit is a low level code review. The code review proved that the feature is implemented as expected in go-square and celestia-app and no mistakes have been noticed.

3 https://github.com/celestiaorg/go-square/blob/a446cee3ad5fd5be5e59dc9a027bc35b4f6100cb/proto/blob/v1/blob.proto#L17
4 https://github.com/celestiaorg/go-square/blob/a446cee3ad5fd5be5e59dc9a027bc35b4f6100cb/share/split_sparse_shares.go#L38-L41
5 https://github.com/celestiaorg/go-square/blob/a446cee3ad5fd5be5e59dc9a027bc35b4f6100cb/share/parse_sparse_shares.go#L41
6 https://github.com/celestiaorg/go-square/blob/a446cee3ad5fd5be5e59dc9a027bc35b4f6100cb/share/parse_sparse_shares.go#L55
7 https://github.com/celestiaorg/celestia-app/blob/306c58745d135d31c3777a1af2f58d50adbd32c8/app/prepare_proposal.go#L58-L77
8 https://github.com/celestiaorg/celestia-app/blob/306c58745d135d31c3777a1af2f58d50adbd32c8/app/process_proposal.go#L133-L155
9 https://github.com/celestiaorg/celestia-app/blob/306c58745d135d31c3777a1af2f58d50adbd32c8/x/blob/types/blob_tx.go#L82-L89