

Cardano Budget Process 2026

Audit Results

Admin wallet : addr1vyk44xqtv3jpk90fuzqfsjzcvm259hshuw2qmzxq98n3n4chyw9hr

Ballot fingerprint : c66f333a5b73775a8938051a3e9779008f9287cc1b9664e096263151

Voting window : 2026-05-26T12:00:00Z to 2026-06-12T12:00:00Z

End epoch : 636

Questions : 69

Results

 [Cardano Budget Process 2026 - Results Tally](#)

Cardano Budget Process 2026

Audit Findings

This report summarizes the independent TypeScript audit of the Ekklesia Hydra voting ballot on Cardano mainnet.

Ballot reviewed: Cardano Budget Process 2026

Admin wallet: addr1vyk44xqtv3jpk90fuzqfsjzcv259hshuw2qmzxq98n3n4chyw9hr

Ballot fingerprint: c66f333a5b73775a8938051a3e9779008f9287cc1b9664e096263151

Voting window: 2026-05-26T12:00:00Z to 2026-06-12T12:00:00Z

End epoch: 636

Questions: 69

Voters in proof package: 113

Scope

The independent audit covered two separate areas:

1. **Cryptographic ballot verification**

- on-chain datum decoding
- ballot JSON Merkle root reconstruction
- results.json hash verification
- proof-package Merkle root verification
- per-voter inclusion proofs
- evidence file hashes
- signed payload and COSE signature checks
- vote-history chain checks
- independent tally recomputation

2. **Eligibility and voting-power verification**

- signed voter evidence checked against an epoch-636 authority snapshot
- DRep entries exported from drep_distr
- one stake voter entry exported from epoch_stake
- current public-chain DRep lookup checked through Blockfrost

Cryptographic Audit Result

The independent verifier confirmed the main ballot evidence path:

- The ballot content reconstructed the on-chain (600) Merkle root
- The results matched the on-chain (601) results hash
- The proof package matched the on-chain evidence Merkle root
- All voter inclusion proofs walked back to the committed evidence root
- All selected evidence files matched their committed vote hashes
- Vote history chains were intact and inside the voting window
- Hydra fanout lineage was confirmed
- The independent re-tally matched the published per-role counts for all 69 questions

Current verifier result:

Shell

```
AUDIT STATUS (527 checks, 1 failures)
```

The remaining cryptographic failure affects one voter:

Shell

```
2293c55fa571fcff89ef1e02de506c3df9dbcf07d601d2f0bb828e5db
```

Failure detail:

Shell

```
COSE payload
```

```
b554982a1236e2a98ddca1953f2b586baa3721e8f17d77f75b5ca8b97e58596f
```

```
does not match signed payload hash
```

```
5263e4b28f1247ca69ff1336ef177ee9722b523fe763b07213befb89129ac757
```

This means one COSE object for that voter carries a different payload hash than the signed payload hash expected by the committed ballot evidence. The voter still has a valid inclusion proof, a matching final evidence file hash, and an intact two-entry vote-history chain. The mismatch should be reviewed by the Ekklesia team to confirm whether the extra COSE object is stale, duplicated, or incorrectly linked.

Script DReps validation

Two voter IDs were recognized as script DRep credentials. A script DRep credential does not directly equal the Ed25519 signing key hash, so the script should not require a direct key-hash match for those voters. The verifier was updated to classify script DRep credentials separately.

Shell

```
227d74b5bb8630ce4d8a87189ad75ef5ef55e6c26c604fb78267e271f9
```

```
2293c55fa571fcff89ef1e02de506c3df9dbcf07d601d2f0bb828e5db
```

They pass the signature check successfully:

Shell

```
[OK] voter
```

```
227d74b5bb8630ce4d8a87189ad75ef5ef55e6c26c604fb78267e271f9
```

```
:
```

```
ed25519+message verified - script credential; direct  
key-hash match not applicable
```

```
[OK] voter
```

```
2293c55fa571fcff89ef1e02de506c3df9dbcf07d601d2f0bb828e5db
```

```
:
```

```
ed25519+message verified - script credential; direct  
key-hash match not applicable
```

These two voter ballots were accepted as valid..

Eligibility Snapshot Result

The eligibility audit was run with the merged epoch-636 snapshot:

Snapshot contents:

- 888 DRep entries from drep_distr for epoch 636
- 1 stake entry from epoch_stake for the stake voter seen in the ballot
- total snapshot entries: 889

Current eligibility result:

Shell

```
AUDIT STATUS (559 ok, 0 unchecked, 2 fail)
```

Following stake address is present in the voter details

Shell

```
e02d7e2c16a003a17a4c4f89673a7f1329f381ca9c9ea08ade2e4ce0af
```

```
snapshotVotingPower=31693327692
```

Two DRep voters remain missing from the epoch-636 authority snapshot:

Missing DRep 1

Shell

voter token:

220060a4f5b30c6f0b03a3e6875f0fa26e4f8ec475869ec7ada0282e88

voterId:

drep1ygp105fplelgu35uc7ljx8tc0j3ld9glas99qvfrgtgm8rg4ujzg7

credential:

03f7d121fe7e8e469cc7bf231d787ca3f6951fec0a50312342d1b38d

Independent cryptographic checks for this voter passed:

Shell

v1 matches committed voteHash

ed25519+message+credential verified - matched drep key
credential

history chain intact (1 entry) + within-window; last voteHash
matches leaf

Eligibility check failed:

Shell

```
[FAIL] eligibility: voter was not found in the provided  
snapshot
```

```
[WARN] public-chain lookup failed: Blockfrost 404
```

Missing DRep 2

Shell

```
voter token:
```

```
22b32ee7b325d63c41a65a976cc065b6ad0e7920b02d65f78321d85082
```

```
voterId:
```

```
drep1yf5kddtr03tp450dkkxymk3nws3qwnux55kwztkj2v3z5eshqugjs
```

```
credential:
```

```
6966b5637c561ad1edb58c4dda337422074f86a52ce12ed253222a66
```

Independent cryptographic checks for this voter passed:

Shell

```
v1 matches committed voteHash
```

```
ed25519+message+credential verified - matched drep key  
credential
```

```
history chain intact (1 entry) + within-window; last voteHash  
matches leaf
```

Eligibility check failed:

Shell

```
[FAIL] eligibility: voter was not found in the provided  
snapshot
```

```
[WARN] public-chain lookup failed: Blockfrost 404
```

Manual db-sync checks for both credential hashes returned no rows from drep_hash / drep_distr, and Blockfrost returned 404 Not Found for both DRep IDs.

Findings Summary

Finding 1: One unresolved COSE payload mismatch

One COSE object for voter 2293c55fa571fcff89ef1e02de506c3df9dbcfd07d601d2f0bb828e5db does not match the expected signed payload hash.

It is not clear how this invalid vote got included in the on-chain result. The vote has been disqualified and not included in the final calculation.

Finding 2: Two signed DRep votes are not supported by the epoch-636 authority snapshot

Two voters have valid signed evidence and valid vote-history checks, but their DRep credentials are not present in the exported epoch-636 drep_distr snapshot and are not recognized by Blockfrost as current DRep IDs.

The vote from the dReps accepted and included in counting. But 0 voting power makes their vote have no impact on the result..