SAFEONECHAIN

AUDITOR-
ONLY
HANDBOOK
(AOH-v1.0)

(SAFO)

SAFO

Status: Canonical Audit Extract
Authority Sources: MPF-v1.0 + DPS-v1.0
Code Status: Code Freeze v1.0 (Audit Baseline)
Audience: External Security Auditors, Regulatory Auditors, Independent Verifiers

Audit Mandate & Scope

What This Handbook Is

This handbook defines how to audit SafeOneChain and what constitutes a pass/fail outcome for protocol safety.

- It is normative for:
- protocol audits
- regulatory technical reviews
- independent assurance reports

What Is In Scope

- PoA-BFT consensus safety
- Deterministic finality
- extraData CommitProof v1
- Governance authority boundaries
- Emergency control constraints
- Evidence pipeline (double-sign)
- Permissioned networking rules
- Finality-aware RPC semantics

What Is Explicitly Out of Scope

- Application products (DEX, wallets, bots)
- Bridges / cross-chain
- Frontends
- Third-party infrastructure
- Token market behavior
- Learn more on slide 4.

Audit Model & Assumptions

Trust Model

Audits must not assume trust in:
- node operators
- RPC providers
- governance participants

Audits may assume:
- cryptographic primitives are standard and correctly implemented
- the auditor can run independent read-only nodes

Failure Model

The protocol assumes:
- up to f < N/3 faulty or malicious validators
- asynchronous network with message loss/delay
- adversarial but non-omniscient attackers

Info

This handbook defines how to audit SafeOneChain and what constitutes a pass/fail outcome for protocol safety.

Deterministic Finality — Audit Requirements

Finality Rule (Binding)

A block at height H is final if and only if:
≥ ⌊2N/3⌋ + 1 valid precommit signaturesexist for the same block hash at height H

Auditor Verification Checklist

For any finalized block:

- [ ] Extract block header
- [ ] Extract extraData
- [ ] Parse CommitProof v1
- [ ] Recompute header_without_extradata
- [ ] Recompute validator set hash
- [ ] Verify all signatures
- [ ] Count unique validator IDs
- [ ] Confirm quorum threshold met

Any failure → block is not final.

CommitProof v1 — Audit Specification

Canonical Byte Layout

MAGIC ("SAFO")	VERSION (0x01)	ROUND (u32)
VALSET_HASH (32)	SIG_COUNT (u16)
[VALIDATOR_ID (20)	SIGNATURE (65)] * SIG_COUNT

- Encoding: raw binary
- Endianness: big-endian
- RLP: explicitly not used

Mandatory Rejection Conditions

Auditors must confirm rejection for:

- incorrect MAGIC
- unknown VERSION
- duplicate validator IDs
- invalid signatures
- incorrect validator set
- insufficient signature count

Acceptance of any invalid proof = critical failure.

CONSENSUS SAFETY INVARIANTS (MUST HOLD)

Auditors must verify all invariants:

SINGLE-FINALITY INVARIANT

No two finalized blocks at the same height.

NO-IMPLICIT AUTHORITY INVARIANT

No single actor can produce finality.

NO-REORG INVARIANT

Finalized blocks are immutable.

EVIDENCE PRESERVATION INVARIANT

Violations are provable and storable on-chain.

Violation of any invariant = audit fail.

Evidence Pipeline v1 – Audit Requirements

Supported Evidence Type

Double-Sign Evidence:
o same validator
o same height
o different block hashes

Evidence Verification Steps

- [ ] Validate both signatures cryptographically
- [ ] Confirm same validator ID
- [ ] Confirm same height
- [ ] Confirm different block hashes
- [ ] Confirm evidence stored on-chain

Enforcement Model

- No automatic slashing
- No autonomous punishment
- Governance review required

Auditors must confirm absence of auto-enforcement paths.

Governance Authority Boundaries

What Governance May Do

- Add / pause / remove validators
- Rotate validator keys
- Authorize scoped emergency actions
- Approve upgrades (versioned)

What Governance Must Not Do

- Rewrite finalized blocks
- Alter historical state
- Bypass quorum rules

Execute hidden admin paths

Audit Checks

- [ ] All governance actions emit on-chain events
- [ ] Quorum enforcement is explicit
- [ ] No single-admin code paths exist

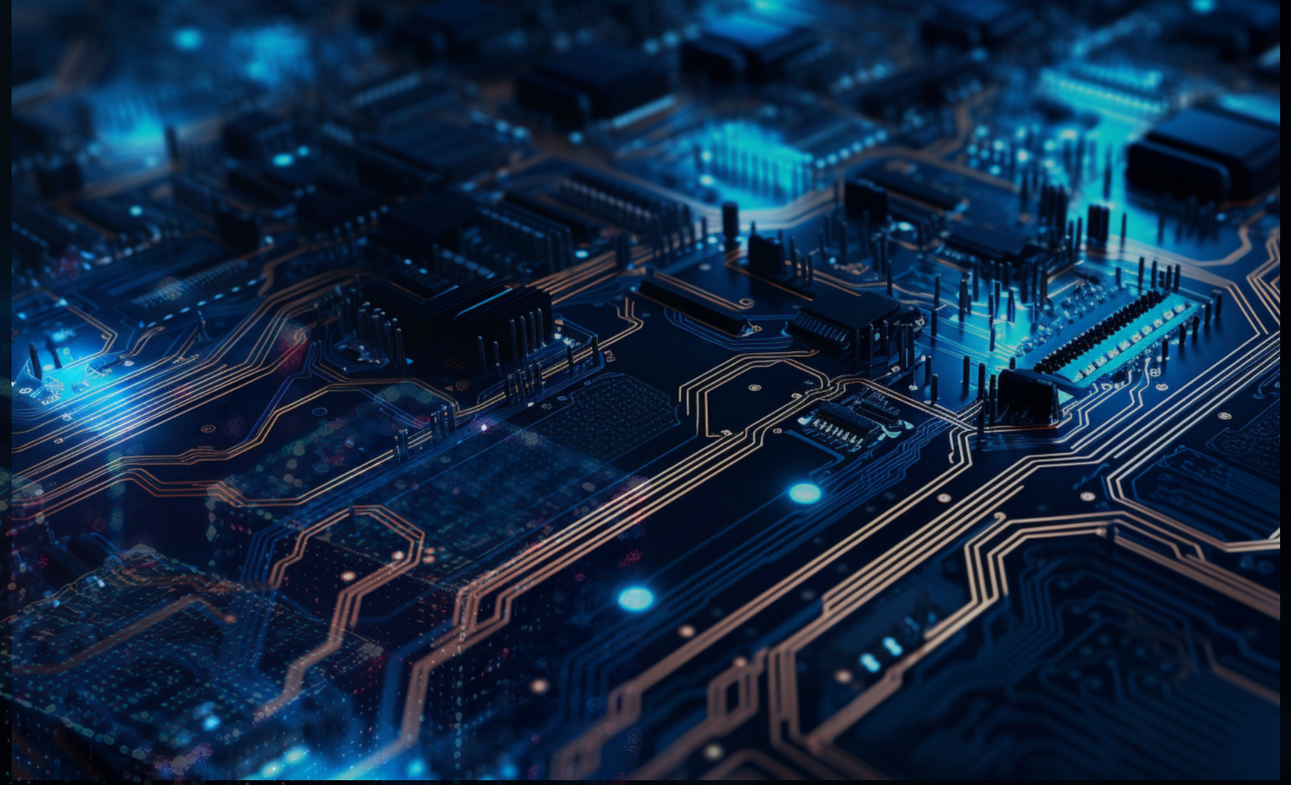
EMERGENCY CONTROLS – AUDIT CRITERIA

Allowed Properties
- Scoped (validator/module-level)
- Time-bounded
- On-chain logged

Forbidden Properties
- Global kill switch
- Retroactive state changes
- Finality bypass

Auditors must confirm technical impossibility of forbidden actions.

NETWORKING & P2P — AUDIT FOCUS



Permissioned Networking

AUDITORS MUST VERIFY:

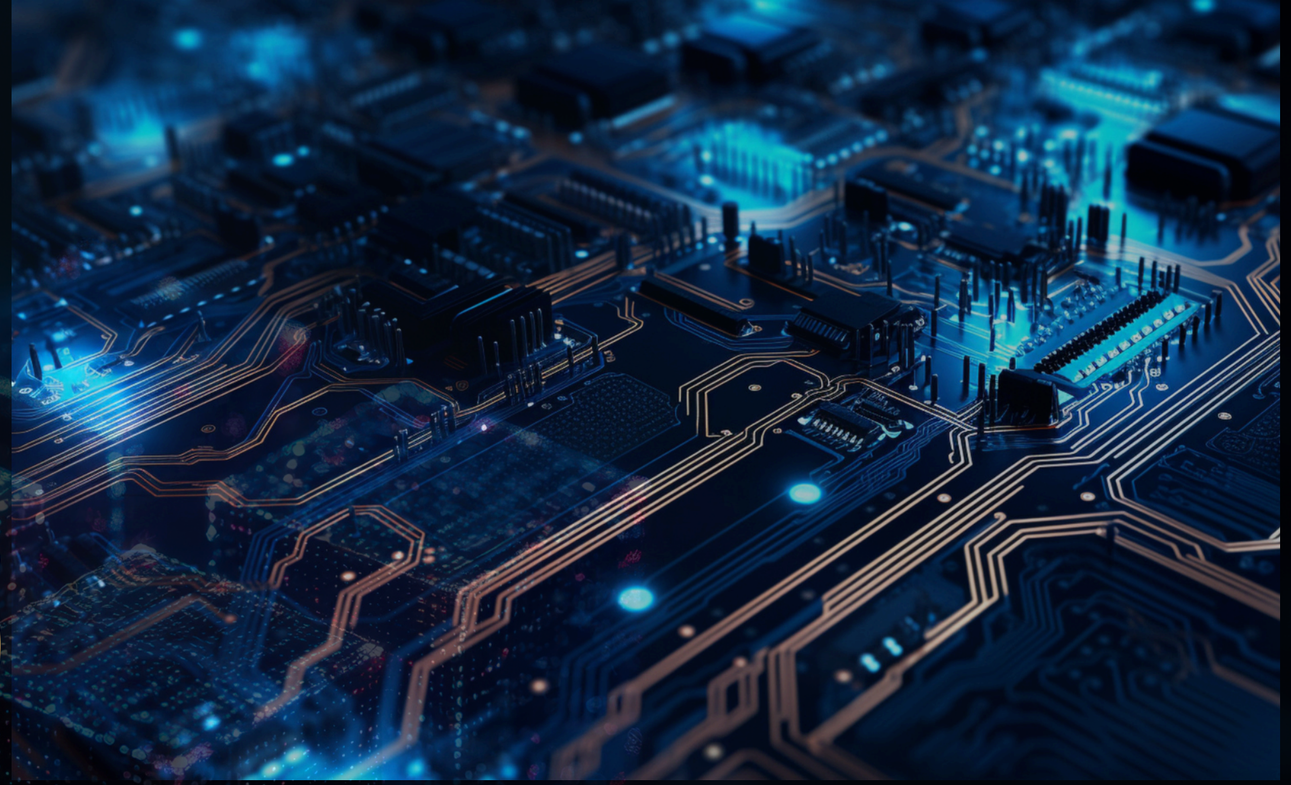
- no peer discovery
- identity-bound connections

role-based message authorization

MESSAGE AUTHORIZATION MATRIX

Consensus messages must only originate from validator nodes. Unauthorized message acceptance = critical finding.

RPC SEMANTICS — AUDIT CHECKS



FINALITY SAFETY

- latest must always resolve to finalized state
- No RPC may expose non-final blocks as canonical

AUDITORS MUST TEST:

- safo_getFinalityProof
- safo_getValidatorSet
- safo_getGovernanceActions
- safo_getEvidence

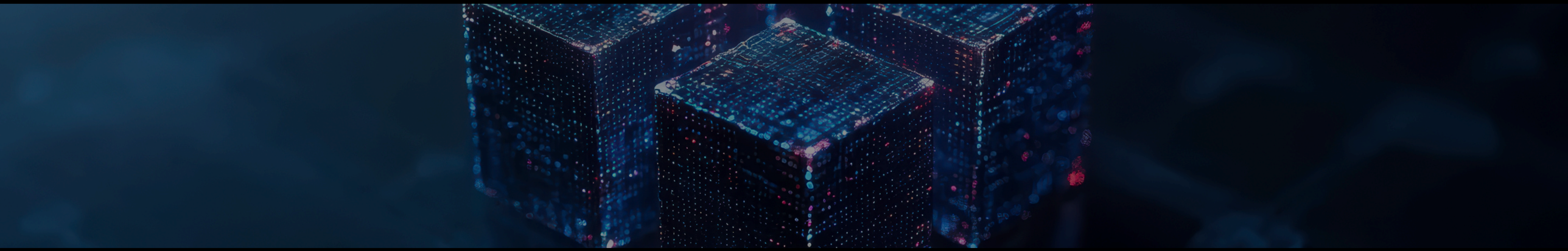
Incorrect semantics = high severity.

AUDITOR READ-ONLY NODE OPERATION

Capabilities

Auditor nodes:

- do not sign
- do not submit transactions
- fully verify finality and evidence



Auditors must be able to:

- verify blocks offline
- reconstruct governance timelines
- validate evidence without operator trust

INDEPENDENCE REQUIREMENT

Deterministic Harness – Audit Use

Auditors must reproduce:

1. Normal finality
2. Proposer failure
3. Double-sign evidence
4. Network partition (no finality)
5. Governance-approved validator pause

Non-reproducibility = audit fail.

MUST-FAIL TEST SUITE (BINDING)

Auditors must confirm failure for:

- forged CommitProof
- duplicate precommit signatures
- insufficient quorum
- governance without quorum
- non-final block returned as latest

Passing any must-fail test = critical defect.

SEVERITY CLASSIFICATION (BINDING)

Severit	Definition
Critical	Finality, safety, or governance bypass
High	High Validator manipulation, unauthorized authority
Medium	DoS / liveness risk
Low	Hardening / edge cases
Info	Non-impacting observations

Audit Deliverables

Auditors must provide

1. Executive summary
2. Detailed findings
3. Reproducible PoCs
4. Explicit yes/no on:

o finality bypass
o hidden admin paths
o autonomous enforcement

Audit Conclusion Rule

•SafeOneChain passes audit only if deterministic finality, governance boundaries, and evidence handling are proven unbypassable within the defined threat model.

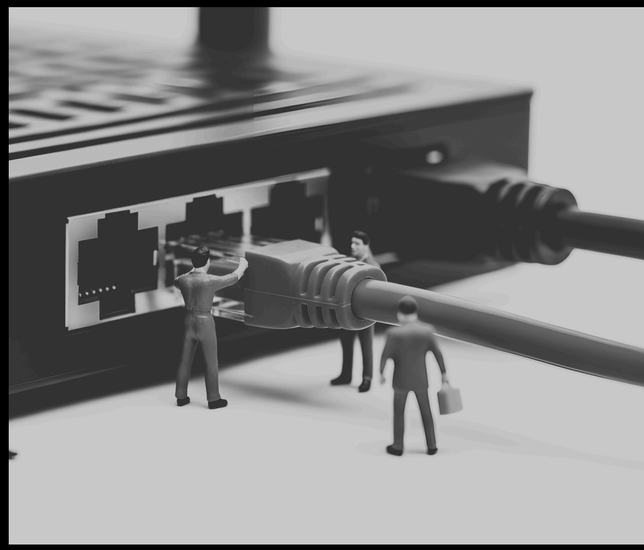
Final Auditor Statement

SafeOneChain is auditable without trust assumptions beyond standard cryptography.All safety-critical claims are independently verifiable, reproducible, and attributable.

X

Medium

CONTACT US



Telegram

safeonechain.com