

v3.4-ZKP-002 – Notarless Trust & Cryptographic Consensus Enforcement

Document Title	Notarless Trust & Cryptographic Consensus Enforcement
Version	v3.4
Document ID	v3.4-ZKP-002
Date	2025-03-22
Author	Take Back Your Data – Cryptographic Trust Group
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the logic for notarless trust within MaxOneOpen, replacing external notaries with self-verifying cryptographic consensus. It ensures that forks can independently validate state and actions without needing a central authority.

2. Notarless Consensus Model

- All participating nodes generate and verify ZK-proofs in parallel
- Consensus is reached via proof-matching, not vote-counting
- No single point of failure or confirmation delay exists
- Consensus trails are checkpointed into certified fork snapshots

3. Cryptographic Trust Enforcement

Enforcement Type	Scope	Trigger Logic
Proof Match	Runtime outputs	Consensus ZK circuit
Rejection Vote	Invalid trace	Proof mismatch + fallback
Fork Snapshot Hash	Global state checkpoint	Scheduled consensus
Rollback Trigger	Conflict or drift	Audit hash discrepancy

4. Certification Hooks

- Forks must operate independently of centralized validators
- All decisions must have ZK-provable justification
- Proof generation and validation must be reproducible and replayable

5. Certification Triggers

- Centralized consensus fallback disqualifies the fork
- Inconsistent or opaque proof trails are non-compliant

6. Certification Relevance

Certified MaxOneOpen forks must demonstrate notarless consensus using cryptographic trust anchors. Trust must be provable, replayable and free of external dependencies.