ENF PROTOCOL · TECHNICAL DOCUMENT · SPECIFICATION V0.1 · DRAFT

Prototype Node Architecture Specification

Electric Network Frequency consensus primitive — engineering unknowns and build targets for first testnet node

PRE-PROTOTYPE | NOT PEER REVIEWED | OPEN ENGINEERING QUESTIONS FLAGGED | JUNE 2026

CONTENTS

WHY THIS WASN'T BUILT BEFORE

Remote-controlled aircraft existed in the 1950s. GPS guidance was operational by the 1970s. Lightweight composite airframes were widespread by the 1980s. None of that produced drone warfare until someone crossed the rooms between communities that were not talking to each other. The innovation was integration, not invention.

> The ENF Protocol is the same structure. Power engineers have studied grid frequency for decades. Forensic scientists proved ENF signals are tamper-evident; courts accept them as evidence. Cryptographers built Byzantine Fault Tolerance. Distributed systems engineers built peer-to-peer networking. Consumer electronics drove camera miniaturization as a byproduct of smartphones. Every component in this specification existed before this document was written.
>
> This is not an invention problem. It is an assembly problem. This specification is the assembly plan.

SECTION 01

Purpose and Scope

This document specifies the architecture of a single ENF Protocol testnet node with sufficient precision to identify the engineering unknowns that must be resolved before implementation begins. It is not a whitepaper, an investor document, or a completed design. It is a build target — the minimum specification needed to answer "can we build it?" with real data instead of estimates.

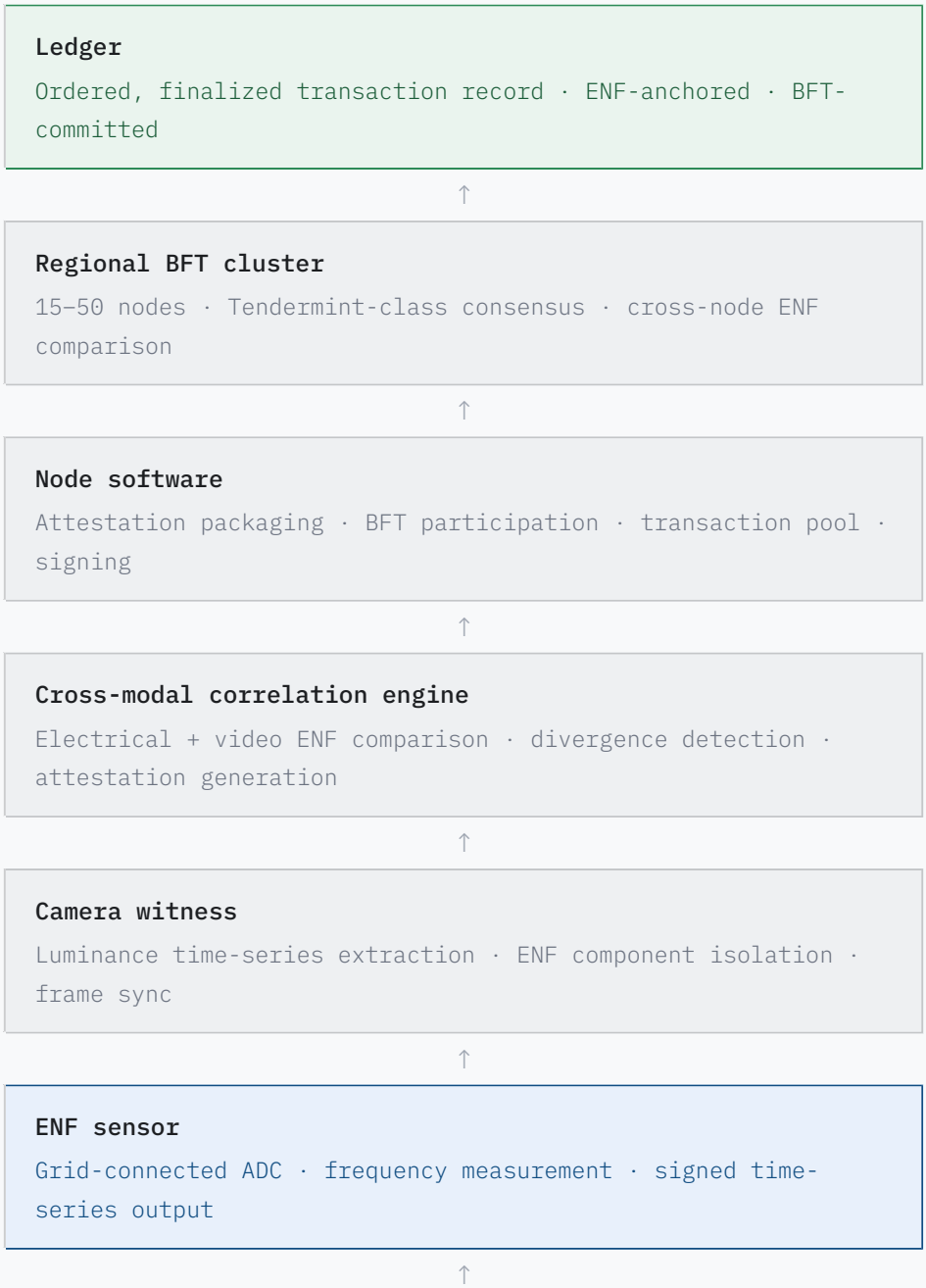
The document addresses each layer of the node stack in order, from physical grid interface to ledger, specifying: what the layer must produce, what inputs it requires, what format those inputs and outputs take, and where the open questions are. Open questions are flagged explicitly with UNKNOWN markers.

> **STATUS**
>
> All performance figures in this document are estimates derived from the properties of analogous systems. No ENF Protocol node has been built. This specification is the first step toward building one. Every UNKNOWN in this document is a testnet measurement target.

SECTION 02

Stack Overview

A complete node consists of six functional layers above the physical grid. Each layer consumes the output of the layer below it and produces a defined artifact for the layer above.



0

Power grid

Physical ENF source · 60 Hz nominal (North America) · continuously fluctuating

Each arrow represents a specification problem. This document works through each one.

SECTION 03

Layer 0 — Power Grid Interface

The grid is the physical source. No node component controls it. The node's interface to the grid is through a standard wall outlet, from which the ENF sensor draws both power and signal.

Requirements

PARAMETER	VALUE	NOTES
Grid connection	Standard mains outlet	North America: 120V 60Hz; Europe: 230V 50Hz
Node grid dependency	Continuous	UPS backup required for uptime; but UPS power must not be used as ENF source — see Layer 1
Geographic constraint	Same grid interconnection	Nodes in different interconnections (e.g. WECC vs. ERCOT) cannot directly compare ENF signals
Minimum signal quality	TBD	UNKNOWN — REQUIRES MEASUREMENT

> **CRITICAL CONSTRAINT**
>
> A node running on UPS (battery) backup loses its ENF signal source. The sensor must measure grid frequency from the mains input, not from battery-converted power. This means nodes have a hard dependency on live grid connection for ENF capture, even if computation can continue on battery. UPS architecture must separate mains sensing from compute power supply.

SECTION 04

Layer 1 — ENF Sensor

The ENF sensor measures the instantaneous frequency of the mains supply and produces a signed time-series of frequency readings. This is the primary ENF signal. The camera witness (Layer 2) provides a secondary, independent signal for cross-correlation.

Hardware options

APPROACH	COST ESTIMATE	ACCURACY	STATUS
Dedicated ENF capture board (e.g. NI USB-6001 class)	$150–$400	High — purpose-built ADC	OPTIONAL FOR TESTNET
Sound card line-in (with voltage divider + transformer isolation)	$20–$60	Medium — limited by ADC depth	Viable for testnet
Raspberry Pi GPIO + ADC hat	$30–$80	Medium — jitter from OS scheduling	VIABLE WITH REAL-TIME KERNEL
Microcontroller (STM32 class) dedicated to sampling	$15–$40	High — no OS jitter	Preferred for production

Output specification

```
{
  "layer": "enf_sensor",
  "node_id": "string (ed25519 public key)",
  "grid_region": "string (e.g. WECC-CA, NPCC-NY)",
  "sample_rate_hz": 1000,
  "window_seconds": 60,
  "nominal_hz": 60.0,
  "samples": [
    {
      "t_unix_ms": 1748000000000,
      "freq_hz": 59.9873,
      "snr_db": 42.1
```

```
      }
      // ... one entry per ms
    ],
    "window_hash": "sha256 of samples array",
    "signature": "ed25519 signature over window_hash"
  }
```

Open questions

UNKNOWN ENF-S-01

What is the minimum useful sample rate? Literature suggests 1 kHz is sufficient for ENF extraction, but the minimum rate that provides adequate entropy for consensus needs empirical measurement. Candidate range: 200 Hz – 2 kHz.

UNKNOWN ENF-S-02

What is the minimum window length for an ENF sample to be uncorrelated with adjacent windows? This determines the minimum time between attestations. Estimate from literature: 30–120 seconds, but grid-region dependent. Must be measured per-region in testnet.

UNKNOWN ENF-S-03

How much entropy (in bits) does a 60-second ENF window actually contain? This is the load-bearing security question. If ENF drift is predictable enough that an adversary can anticipate the signal, the attestation is weakened. Requires spectral analysis of real ENF capture data from target grid regions.

SECTION 05

Layer 2 — Camera Witness

The camera witness extracts ENF signal from video by analyzing luminance fluctuation in each frame. Artificial lighting driven by grid power flickers at the grid frequency and its harmonics. The camera captures this flicker passively, producing an independent

ENF time-series that can be cross-correlated against the electrical sensor reading.

Hardware requirements

PARAMETER	MINIMUM	PREFERRED
Frame rate	120 fps	240+ fps
Shutter mode	Rolling shutter (usable)	Global shutter (preferred)
Sensor	Any CMOS	High-SNR monochrome
Lighting environment	Fluorescent or LED (grid-driven)	Fluorescent preferred — stronger flicker signal
Cost estimate	$30 (Raspberry Pi camera module)	$80–$200 (global shutter USB camera)

> **CRITICAL ENVIRONMENTAL DEPENDENCY**
>
> DC-powered LED lighting does not flicker at grid frequency and produces no usable ENF signal. Nodes in environments with DC-converted lighting (common in modern server rooms and some offices) cannot use camera-based ENF extraction. Testnet nodes must be deployed in environments with verifiably AC-driven lighting.

Processing pipeline

```
RAW FRAME (N pixels × M rows)
  ↓
LUMINANCE EXTRACTION
  Mean luminance per frame → scalar time-series L[t]
  ↓
BANDPASS FILTER
  Isolate 55–65 Hz band (NA) or 45–55 Hz band (EU)
  Remove DC component, harmonics above 3rd order
  ↓
FREQUENCY ESTIMATION
  Zero-crossing detection or FFT on L[t] window
  Output: freq_hz per window
  ↓
```

```
  CAMERA ENF TIME-SERIES
    Same format as sensor output, flagged source="camera"
```

Open questions

UNKNOWN ENF-C-01

What is the minimum frame rate that reliably captures 60 Hz ENF signal from LED lighting? Nyquist requires 120 fps minimum. Practical minimum with real noise may be higher. Must be measured with target camera hardware under target lighting conditions.

UNKNOWN ENF-C-02

H.264 and H.265 video compression aggressively smooths luminance variation between frames. Does lossless or raw capture significantly outperform compressed video for ENF extraction? Compression format constraint affects node hardware requirements substantially.

UNKNOWN ENF-C-03

Rolling shutter cameras introduce row-dependent timing offsets. Quantify the error this introduces into frequency estimation and determine whether it is small enough to be tolerable or requires global-shutter hardware.

SECTION 06

Layer 3 — Cross-Modal Correlation Engine

The correlation engine is the security-critical layer. It receives two independent ENF time-series — one from the electrical sensor, one from the camera — and determines whether they agree within a tolerance threshold. Agreement produces a signed attestation. Divergence triggers a tamper alert and suppresses attestation output.

Correlation algorithm (proposed)

```
INPUTS
  S_elec[t]  — electrical sensor frequency time-series
  S_cam[t]   — camera frequency time-series
  Both over identical window W (e.g. 60 seconds)

STEP 1: Normalize
  S_elec_norm = (S_elec - mean(S_elec)) / std(S_elec)
  S_cam_norm  = (S_cam  - mean(S_cam))  / std(S_cam)

STEP 2: Cross-correlate
  XC = cross_correlate(S_elec_norm, S_cam_norm)
  peak_r = max(XC)          // Pearson r at optimal lag
  peak_lag_ms = argmax(XC)  // Timing offset between sensors

STEP 3: Threshold check
  IF peak_r >= R_min AND abs(peak_lag_ms) <= LAG_max:
    PASS → generate attestation
  ELSE:
    FAIL → log tamper alert, suppress output

PARAMETERS (all TBD — testnet measurement targets)
  R_min     = minimum acceptable correlation coefficient
  LAG_max   = maximum acceptable inter-sensor lag (ms)
```

Attestation output format

```
{
  "layer": "attestation",
  "node_id": "string",
  "window_start_unix_ms": 1748000000000,
  "window_end_unix_ms":   1748000060000,
  "grid_region": "WECC-CA",
  "enf_fingerprint": "sha256 of S_elec normalized window",
  "correlation_r": 0.9741,
  "correlation_lag_ms": 12,
  "sensor_window_hash": "...",
  "camera_window_hash": "...",
  "attestation_hash": "sha256 of above fields",
  "signature": "ed25519 signature over attestation_hash"
}
```

Open questions

UNKNOWN ENF-X-01

What is the correct value for R_min? Setting it too low allows weak correlations to pass, reducing security. Setting it too high causes false negatives under normal environmental noise. Must be calibrated empirically across multiple environments and lighting conditions.

UNKNOWN ENF-X-02

The replay attack question: if an adversary records a valid (S_elec, S_cam) pair from a previous window and injects it, the correlation will pass. Prevention requires that the attestation include a binding to current ledger state (e.g. hash of the previous block) so a replay from a different point in the chain is invalid. This binding mechanism is not yet specified.

UNKNOWN ENF-X-03

What is the computational cost of cross-correlation over a 60-second window at 1 kHz sample rate on testnet hardware? At 60,000 samples per channel, FFT-based cross-correlation is O(N log N) — feasible on a Raspberry Pi 4 but latency must be measured to confirm it fits within the BFT consensus round time.

SECTION 07

Layer 4 — Node Software

The node software orchestrates the layers below it, participates in BFT consensus, maintains the transaction pool, and signs all outbound messages. It is the only layer that communicates with other nodes.

Responsibilities

FUNCTION	DESCRIPTION	STATUS
Attestation scheduling	Trigger sensor + camera capture on fixed-interval windows; collect correlation engine output	SPECIFIABLE
Transaction pool	Receive, validate, and gossip pending transactions to peers	STANDARD BFT PATTERN
Block proposal	When selected as proposer, assemble block from pool + current attestation + previous block hash	STANDARD BFT PATTERN
BFT voting	Participate in prevote/precommit rounds; compare own ENF attestation against proposer's	ENF-SPECIFIC — NOT YET SPECIFIED
Peer ENF comparison	Request and verify ENF attestations from peer nodes to detect regional divergence	ENF-SPECIFIC — NOT YET SPECIFIED
Key management	Ed25519 node keypair; signing of all outbound messages	STANDARD

Block structure (proposed)

```
{
  "height": 1042,
  "prev_hash": "sha256 of previous block",
  "timestamp_unix_ms": 1748000060000,
  "enf_attestation": { ... },   // from Layer 3
  "transactions": [ ... ],
  "proposer_id": "node public key",
  "proposer_signature": "...",
  "commit_signatures": [        // from BFT precommit round
    { "node_id": "...", "signature": "..." },
    // ... ≥ ⌈2n/3⌉ + 1 signatures required
  ]
}
```

Open questions

UNKNOWN ENF-N-01

During BFT voting, how should a validator node treat a block proposal whose ENF attestation diverges from its own local ENF reading? Options: (a) reject the block; (b) flag and pass to federation arbitration; (c) accept if ≥ threshold of other nodes agree with the proposer. The correct rule determines the protocol's resilience to locally disrupted ENF capture.

UNKNOWN ENF-N-02

What is the target block time? ENF window length (minimum ~30 seconds, estimated) constrains the minimum block time. If blocks must include a fresh ENF attestation, block time cannot be shorter than the attestation window. This is a fundamental throughput ceiling that must be quantified.

SECTION 08

Layer 5 — Regional BFT Cluster

The BFT cluster is a set of 15–50 nodes in the same grid interconnection region, running a Byzantine Fault Tolerant consensus protocol. The cluster agrees on the ordering and finality of blocks. ENF attestations serve as an additional consistency check across nodes — if a node's ENF signal diverges from the regional consensus, it is treated as a fault.

Protocol selection

PROTOCOL	MESSAGE COMPLEXITY	FINALITY	NOTES
Tendermint / CometBFT	O(n²)	Instant per block	Most mature; widely deployed; good tooling
HotStuff (linear)	O(n)	Instant per block	Lower message overhead; used in Diem/Aptos lineage
PBFT	O(n²)	Instant per block	Older; well-studied; less tooling

Tendermint/CometBFT is the recommended starting point for the testnet due to mature tooling and extensive documentation. ENF attestation comparison can be added as a pre-vote validity check without modifying the core protocol.

Cluster sizing model

```
n  = node count
f  = tolerable faults = ⌊(n-1)/3⌋
q  = quorum = ⌈2n/3⌉ + 1

Minimum viable:   n=7,  f=2,  q=5
Conservative:     n=21, f=6,  q=15
Recommended:      n=33, f=10, q=23
Upper practical:  n=50, f=16, q=34

Above n≈50: O(n²) message overhead begins degrading throughput
on 100 Mbps node links with 5 KB consensus messages.
```

Open questions

UNKNOWN ENF-B-01

What is the correct ENF divergence rule for BFT voting? Specifically: if a validator's local ENF attestation has correlation_r below R_min with the proposed block's attestation, should that validator abstain from voting or vote against? The answer affects liveness vs. safety tradeoffs.

UNKNOWN ENF-B-02

How are nodes geographically distributed within a region to maximize ENF signal diversity? Nodes in the same building may capture nearly identical ENF signals. Spread across a region increases independence but increases network latency between nodes. The optimal geographic distribution strategy is not yet defined.

Layer 6 — Ledger

The ledger is the finalized, ordered record of transactions. Once a block is committed by BFT quorum, it is appended to the chain and considered final. The ENF attestation embedded in each block provides a physically anchored timestamp for every committed transaction.

Storage requirements (testnet)

COMPONENT	ESTIMATE	BASIS
Block headers	~2 KB/block	Hash + attestation + metadata
ENF attestations	~500 bytes/block (compressed)	Fingerprint + correlation metrics + signatures
Transactions	Variable — depends on tx size	Application dependent
Raw ENF time-series archive	~14 MB/hour/node at 1 kHz	8 bytes × 1000 samples × 3600 seconds

> **DESIGN DECISION**
>
> Raw ENF time-series do not need to be stored on-chain indefinitely. The `enf_fingerprint` hash in the attestation is sufficient for most verification purposes. Raw archives should be retained by nodes for a configurable window (suggested: 90 days) to support dispute resolution, then pruned. This is analogous to Ethereum's blob pruning under EIP-4844.

Application interface

```
// Minimum ledger query interface for testnet
GET /block/{height}         → block + attestation + tx list
GET /block/{height}/enf     → ENF attestation only
GET /tx/{hash}              → transaction + block height + ENF fingerprint
GET /enf/region/{region}    → recent ENF fingerprints for region
POST /tx                    → submit transaction to pool
```

SECTION 10

Open Engineering Questions

The following questions are the critical path for moving from specification to testnet. Each one is a measurement target — it cannot be answered analytically and requires empirical data from real hardware in real environments.

ENF-S-01

Minimum useful sample rate?

Literature: 1 kHz. Practical minimum with real noise TBD. Affects hardware cost.

ENF-S-02

Minimum window for decorrelated attestations?

Determines minimum block time. Estimated 30–120 sec. Grid-region dependent.

ENF-S-03

Entropy bits per 60-sec ENF window?

Load-bearing security question. Requires spectral analysis of real capture data.

ENF-C-01

Minimum frame rate for LED ENF extraction?

Nyquist: 120 fps. Practical minimum under noise TBD. Affects camera cost.

ENF-C-02

Compression vs. raw capture delta?

H.264/5 smooths luminance. How much does this degrade ENF extraction?

ENF-C-03

Rolling shutter error magnitude?

Quantify timing error introduced by rolling shutter on frequency estimation.

ENF-X-01

Correct value of R_min?

Correlation threshold for attestation pass/fail. Requires calibration across environments.

ENF-X-02

Replay attack prevention mechanism?

Attestation must bind to chain state to prevent injection of previously recorded signals.

ENF-X-03

Correlation latency on target hardware?

Must fit within BFT round time. FFT-based O(N log N) on RPi4 — measure.

ENF-N-01

ENF divergence rule for BFT voting?

What does a node do when its local ENF disagrees with a proposed block's attestation?

ENF-N-02

Minimum block time given ENF window?

Fundamental throughput ceiling. Cannot be shorter than attestation window length.

ENF-B-01

ENF divergence rule for BFT safety/liveness?

Abstain vs. vote-against when attestation correlation fails. Tradeoff analysis needed.

ENF-B-02

Optimal geographic node distribution?

Balance ENF signal diversity against network latency within a region.

SECTION 11

Testnet Target Configuration

The minimum viable testnet to answer the critical path questions above. This is not a production deployment. It is an instrumented measurement environment.

PARAMETER	TESTNET TARGET	RATIONALE
Node count	7	Minimum BFT viability (f=2). Large enough to test consensus, small enough to manage manually.
Geographic spread	3+ cities, same grid interconnection	Tests ENF signal consistency across distance within one region.
ENF sensor hardware	Sound card line-in (isolated)	Cheapest viable option. Replace with MCU-based sensor if timing jitter proves problematic.
Camera hardware	Raspberry Pi Camera Module 3	120 fps capable; low cost; known driver stack.
Lighting environment	Fluorescent or AC-LED	DC-LED environments excluded from testnet.
Compute	Raspberry Pi 4 (4GB) or equivalent mini PC	~$60–$80. Tests viability of commodity hardware.
Consensus protocol	CometBFT (Tendermint v2)	Mature, well-documented, Go implementation available.
Block time target	60 seconds initially	Matches conservative ENF window estimate. Reduce if S-02 measurement permits.
Instrumentation	Full raw ENF logging; all correlation metrics recorded	Every unknown in Section 10 requires measurement data. Log everything.

Estimated testnet hardware cost

```
Per node:
  Raspberry Pi 4 (4GB)       $80
  Camera module 3            $25
  Sound card (USB, isolated) $30
  MicroSD 64GB               $12
  Power supply + case        $20
  ──────────────────────────────
  Per node total:           $167

7-node testnet:           $1,169
Plus: network switch, cables, misc: ~$100
```

```
──────────────────────────────────────
Total testnet hardware:  ~$1,270
```

FEASIBILITY NOTE

A 7-node testnet measuring all critical-path unknowns in Section 10 costs approximately $1,300 in hardware. The primary cost of the testnet is not hardware — it is engineering time to build the sensor capture stack, correlation engine, and CometBFT integration. That work is estimated at 3–6 months for one experienced engineer. Hardware is not the barrier.

SECTION 12

What This Specification Does Not Cover

The following are real problems that must be solved before a production network is viable. They are out of scope for this document because they cannot be specified without testnet measurement data, or because they are governance rather than engineering questions.

OUT-OF-SCOPE ITEM	WHY DEFERRED
Cross-federation settlement protocol	Requires first solving single-federation design. Bridge node architecture is a follow-on specification.
Token economics / issuance model	Not an engineering question at this stage. Depends on governance decisions not yet made.
KYC / compliance layer	Application-layer concern. The base protocol is compliance-agnostic by design.
Formal security proof	Requires resolved values for ENF-S-03 (entropy bits) and ENF-X-01 (R_min). Cannot be written before testnet measurement.
Network peer discovery	Standard distributed systems problem. Use libp2p or equivalent. Not ENF-specific.
Governance of reference nodes	Political and organizational question. Engineering cannot resolve it.

OUT-OF-SCOPE ITEM	WHY DEFERRED
Off-grid adversary hardening	Requires hardware attestation (TPM-class) added to node spec. Follow-on work after basic sensor stack is validated.
Production deployment architecture	Premature. Build testnet first.

Specification v0.1 · Pre-prototype · Not peer reviewed · All performance estimates are analytical derivations pending empirical measurement. Open engineering questions in Section 10 are the critical path. This document should be considered a living specification — sections will be updated as testnet measurements resolve unknowns. Prepared by flipkoin · GoComputerHelp · Regina, Saskatchewan · Treaty 4 territory — oskana kâ-asastêki · June 2026.