

# NOVERA

Intelligence Meets Blockchain.

**WHITEPAPER • VERSION 1.0**

AI-native Layer-1 architecture • Quantum-ready security design • Native NVR coin

September 2026

01 EXECUTIVE OVERVIEW

# A Network Built for the Next Security Era

Novera is a proposed independent Layer-1 blockchain designed around three principles: native network ownership, AI-assisted security intelligence, and cryptographic agility for a post-quantum future.

| MAXIMUM SUPPLY | PRESALE ALLOCATION | INITIAL PRESALE PRICE |
|---|---|---|
| **2.0B NVR** | **350M NVR** | **$0.002** |
| fixed cap | 17.5% of supply | dynamic stages |

## Core thesis

- **Independent by design**
  NVR is intended to be the native coin of Novera Mainnet rather than a token issued on another chain.
- **Security as infrastructure**
  The architecture places risk analysis, network observability and cryptographic upgradeability close to the protocol layer.
- **AI as an operational layer**
  The AI Security Engine is designed to transform live network state into structured risk and developer signals.
- **Long-horizon cryptography**
  Novera targets migration paths toward standardized post-quantum primitives as standards, libraries and operational best practices mature.

DESIGN PRINCIPLE

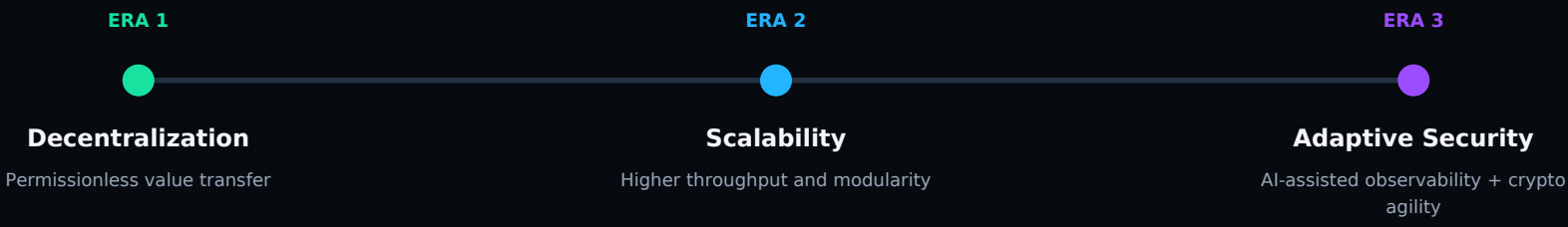
### Built for today. Engineered for what comes next.

This whitepaper describes the intended protocol direction and economic model. Features described as planned, targeted or proposed are not representations that production deployment is complete.

# Blockchain Security Is Becoming a Moving Target

## The environment is changing

Public blockchains were designed around assumptions about cryptography, network behavior and operational risk that continue to evolve. The next generation of infrastructure must be able to observe itself, adapt its security posture and upgrade critical cryptographic components without redesigning the entire network.




### Quantum transition

Widely used public-key schemes may require migration as quantum-capable adversaries become a practical concern.

### Operational complexity

Validators, wallets and applications need clearer signals when abnormal activity emerges.

### Data overload

Raw on-chain data is abundant, but turning it into timely, structured intelligence remains difficult.

# Intelligence as a Native Layer

Novera is designed as a layered system in which execution and consensus remain deterministic while an intelligence layer observes network state and exposes structured outputs to applications and operators.

LAYER 03

## APPLICATIONS

Wallets, protocols, explorers and data products consume structured network intelligence.

LAYER 02

## INTELLIGENCE LAYER

Risk scoring, anomaly signals, network observability and queryable data products.

LAYER 01

## NOVERA MAINNET

Independent Layer-1 execution, consensus, fees and validator economy.

### Architectural boundary

AI outputs are intended to inform operators and applications rather than silently alter deterministic consensus rules. Protocol-critical state transitions should remain auditable, reproducible and governed by explicit network rules.

04 AI SECURITY ENGINE

# From Raw Chain State to Actionable Signals

01

### Network intelligence

Reads transaction volume, validator behavior, fee dynamics and topology to surface changes in network conditions.

02

### Risk analysis

Scores unusual flows, coordinated activity and abnormal fee patterns for operator and application visibility.

03

### Developer intelligence

Exposes structured signals and query interfaces instead of forcing teams to interpret raw logs.

04

### On-chain data intelligence

Transforms high-volume ledger data into queryable datasets for analytics, applications and network services.

**TRUST MODEL**

The intelligence layer should be treated as decision-support infrastructure. Risk scores may be probabilistic and can produce false positives or false negatives; high-impact actions should remain governed by transparent protocol rules and human-verifiable controls.

# Cryptographic Agility, Not Marketing Certainty

Novera is designed around a migration-first security philosophy: cryptographic components should be replaceable as standards evolve. “Quantum-ready” in this document refers to architecture and migration planning, not a claim that the network is immune to all future quantum attacks.



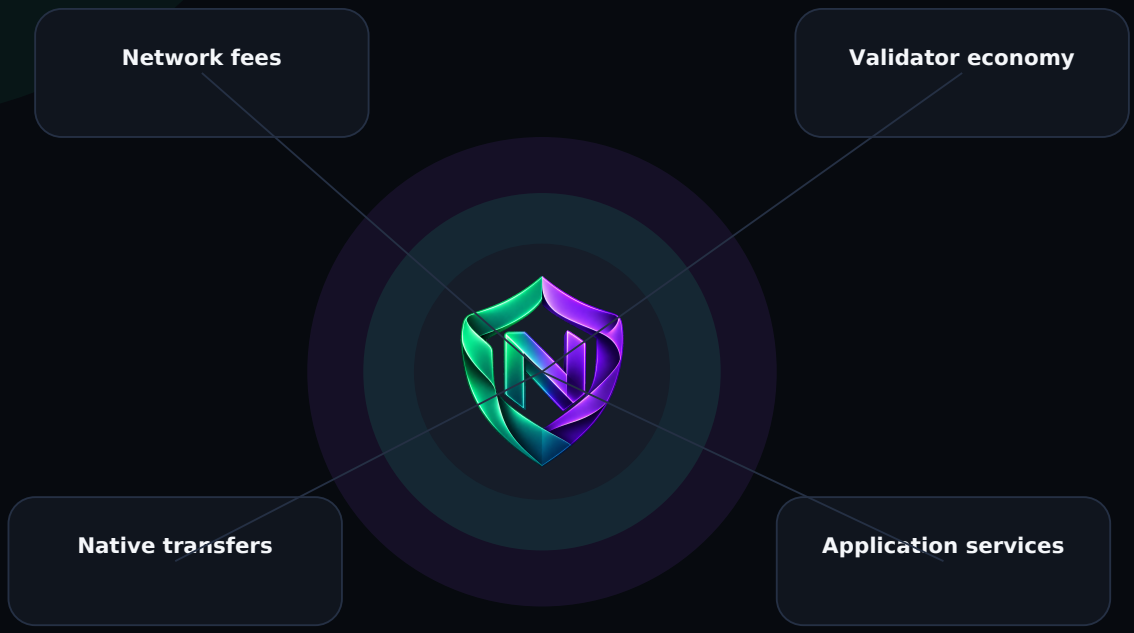

## Design objectives

- **Post-quantum signature pathways**
  Evaluate standardized algorithms and hybrid migration patterns suitable for wallets, validators and critical protocol operations.
- **Cryptographic agility**
  Avoid hard-wiring one primitive so future upgrades can be introduced without replacing the network architecture.
- **Key lifecycle controls**
  Support rotation, versioning and explicit deprecation procedures as cryptographic guidance evolves.
- **Implementation discipline**
  Security depends on audited code, robust randomness, safe libraries, hardware practices and operational controls - not algorithm choice alone.

06 NVR NATIVE COIN

# The Economic Asset of Novera Mainnet

NVR is designed to be the native coin of the Novera network. Its role is to coordinate network usage, fees, validator incentives and ecosystem activity within a single Layer-1 economy.



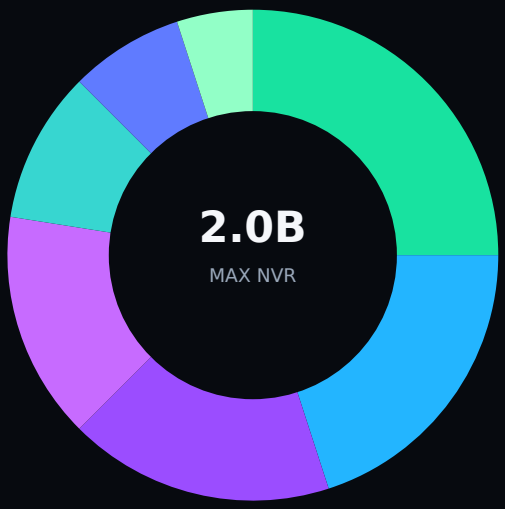

## Utility before speculation

The intended value proposition of NVR is network utility. Market price, liquidity and exchange availability are external outcomes and are not guaranteed by the protocol design. References to third-party exchanges or market-data platforms do not imply endorsement, partnership or confirmed listing unless separately announced by the relevant parties.

07 COINOMICS

# Fixed Supply, Network-first Allocation

| MAXIMUM SUPPLY | PRESALE | TEAM ALLOCATION |
|---|---|---|
| 2,000,000,000 NVR | 350,000,000 17.5% | 0 0% |




| | | |
|---|---|---|
| Network & validator rewards | 500,000,000 NVR | 25% |
| Ecosystem development | 400,000,000 NVR | 20% |
| Presale | 350,000,000 NVR | 17.5% |
| Foundation reserve | 300,000,000 NVR | 15% |
| Liquidity | 200,000,000 NVR | 10% |
| AI & research | 150,000,000 NVR | 7.5% |
| Community | 100,000,000 NVR | 5% |

Allocation percentages describe the target maximum-supply distribution. Release schedules, validator reward curves, reserve governance and liquidity deployment should be published in auditable implementation documents before mainnet activation.

# Transparent Contribution Accounting

The presale distributes up to 350,000,000 NVR, equal to 17.5% of maximum supply. The current interface displays an initial price of $0.002 per NVR and staged price increases.

STEP 1

**Create account / connect wallet**

STEP 2

**Select supported payment route**

STEP 3

**Send contribution to displayed address**

STEP 4

**On-chain verification**

STEP 5

**Balance recorded server-side**

STEP 6

**Claim / distribution when enabled**

## Accounting controls

- **On-chain verification**
  Payments should be checked for network, destination, asset, amount and confirmation depth before balances are credited.
- **Server-side pricing**
  Coin amounts, staged prices and referral rewards should be calculated from authoritative server state, not browser-submitted values.
- **No custody of seed phrases**
  The product should never request or store wallet seed phrases, private keys or recovery phrases.

09 SECURITY MODEL

# Defense in Depth Across Every Layer

### Wallet boundary

Signing proves wallet control without transferring custody of private keys.

### Identity & sessions

Passwords stored with a memory-hard hash; sessions via revocable HttpOnly cookies; rate limits against brute force.

### Contribution verification

Every contribution reconciled against blockchain data before internal credit is created.

### Protocol security

Deterministic state transitions, explicit upgrade rules and auditable validator behavior.

### Infrastructure hardening

Least privilege, secrets isolation, logging, monitoring, patch management and deployment controls.

### Independent review

Smart-contract/protocol audits, penetration testing and public issue disclosure before production milestones.

10 ROADMAP

# From Architecture to Network Expansion

01

## Foundation

COMPLETED / DESIGN

- Layer-1 architecture
- Security framework
- Protocol design

02

## Presale

CURRENT

- NVR presale
- Transparent reporting
- Referral program

03

## Mainnet deployment

PLANNED

- Novera Wallet
- Exchange integration work
- Claim / distribution portal

04

## Network expansion

PLANNED

- Validator participation
- Liquidity programs
- Developer onboarding

05

## AI infrastructure

PLANNED

- Network intelligence
- Developer tools
- On-chain data products

11 NETWORK GOVERNANCE

# Upgradeability Without Hidden Control

A credible Layer-1 needs predictable rules for how the protocol changes. Novera’s target governance model separates day-to-day network operation from high-impact protocol upgrades and reserve decisions.

### VALIDATORS

- Produce and verify blocks
- Follow deterministic protocol rules
- Earn network rewards subject to final economics

### PROTOCOL GOVERNANCE

- Publish upgrade specifications
- Use defined activation thresholds
- Maintain backward-compatibility plans

### FOUNDATION / ECOSYSTEM

- Fund research and ecosystem work
- Publish reserve transparency
- Avoid unilateral consensus control

## Governance principles

Final governance mechanics - including validator thresholds, upgrade delays, treasury controls and emergency procedures - should be documented and independently reviewed before mainnet launch. Governance should minimize single-party discretion over consensus-critical changes.

# Technology, Market and Execution Risk

### Protocol risk

New Layer-1 software can contain implementation errors, consensus failures or vulnerabilities.

### AI model risk

Anomaly models can be wrong, manipulated or become less effective as behavior changes.

### Cryptography risk

Post-quantum standards and implementation guidance continue to evolve; migrations may introduce complexity.

### Market risk

NVR may experience volatility, limited liquidity or no exchange availability.

### Regulatory risk

Rules affecting digital assets, distribution, custody and exchange access vary by jurisdiction and may change.

### Execution risk

Roadmap milestones are targets, not guarantees. Development timelines and scope can change.

Nothing in this whitepaper is financial, investment, legal or tax advice. Participation in digital-asset networks can involve loss of some or all contributed value. Prospective participants should perform independent due diligence and assess applicable laws in their jurisdiction.

13 TECHNICAL PRINCIPLES

# Implementation Standards for a Credible Mainnet

### Deterministic core

Consensus-critical logic must produce the same result for every honest node.

### Observable by default

Metrics, events and risk signals should be designed into the protocol and node stack.

### Upgradeable cryptography

Key algorithms should be versioned behind stable interfaces with migration procedures.

### Least trust

Wallet and contribution workflows should minimize custody and avoid unnecessary secrets.

### Auditable economics

Supply, emissions, vesting and reserves should be independently reconstructable from public data.

### Fail-safe upgrades

Major releases should include testnet validation, rollback planning and explicit activation conditions.

### Developer ergonomics

SDKs, RPCs and structured intelligence outputs should make safe integration easier than unsafe shortcuts.

### Open verification

Security claims should be backed by code, tests, documentation, audits and reproducible evidence.



# NOVERA

A network, not a temporary token.

**Novera is the network.**
**NVR powers it.**

This document is a project whitepaper and technical/economic design overview. It may be updated as architecture, implementation, security review, network economics and regulatory requirements evolve. The latest official version should always supersede earlier copies.

**VERSION 1.0 • SEPTEMBER 2026**