Artificial Intelligence

# pAI Token

## WHITE PAPER

Decentralized Artificial Intelligence Token
An Innovative Dual-Track Mining Model

pAI Token

# Prologue

## The Ultimate Question of the Universe — Value and Intelligence

In the universe of information explosion, entropy increase is an irreversible destiny; in the age of awakening intelligence, the generation of meaning is accelerating. What makes civilization "civilized" is not how much computing power we possess, but whether we can forge order amidst noise, precipitate "value" amid uncertainty, and find for it an immortal anchor—one that depends on no central authority and can be repeatedly verified by any rational agent.

The financial history of humankind is the evolution of "value containers"; the computational history of humankind is the iteration of "intelligence containers." From shells and metals to sovereign credit, we learned to balance between power and trust; from steam and electricity to deep learning, we learned to extract laws between data and models. However, when centralized credit and centralized computing power both reach a gravitational singularity, order becomes distorted: value is monopolized by a few ledgers, intelligence is confined to a few data centers. The year 2008 marked the thermal death of the financial paradigm, while the 2020s' "closed-source supercomputer worship" represents the redshift of the intelligence paradigm.

The universe abhors a vacuum, and evolution rejects stagnation. On the ruins of the old world, Satoshi Nakamoto ignited the fire of creation, telling us: trust can be replaced by mathematics. Ethereum placed a Turing machine upon the law code, telling us: contracts can be order. Yet when we look further ahead, a harder proposition approaches: in the century when AI becomes the new productive force, who will define the "value of intelligence"? Who will determine the ownership and exchange among data, computing power, and models? Who will ensure that this unprecedented technological dividend will not again be swallowed by the black hole of centralization?

**Thus, pAI emerges.**

**pAI (Proof of AI Token) is not a patch on existing tokenomics—it is a paradigm rewrite. We refuse to outsource the "AI economy" to any foundation, corporation, or permissioned list; instead, we solder AI's value circuit onto Ethereum—the world's permissionless and immutable computer. To achieve this, pAI returns to first principles: distribution is order. If distribution is unfair, governance is false; if distribution is mutable, value is hollow. Bitcoin used PoW to solidify "time + energy" into scarcity; we go a step further—embedding both "instant contribution and long-term commitment" into the monetary constitution through a dual-track mining model.**

**The first track is traditional PoW: forged by dual Keccak256, it accounts and settles instantly, paying tribute to real computing power, censorship resistance, and permissionless participation.**

**The second track is linear release: measured by the integral of “time × computing power,” it delays rewards and releases them daily—filtering short-term noise into long-term signal, allowing true builders to be seen and rewarded over time.**

This “double helix” distribution couples the pulse of currency with the metabolism of the community: 41% for instant incentives to ignite the network; 10% for time incentives to maintain ecological equilibrium; and 49% for initial liquidity and application capital to open interfaces with the real world. No pre-mining, no ICO—only on-chain rules that anyone can verify and anyone can join. pAI is not a security; it is an economic program self-proving on-chain. It is not a promise; it is an open process reproducible and challengeable by any node.

Bitcoin is the first stable element on the “periodic table of value”; Ethereum orchestrated those elements into the chemical reactions of contracts and applications. The mission of pAI is to inscribe “intelligence” into that periodic table: to make the flow of computing power, data, and models priced; to make AI service calls settleable; to make every training and inference transactable in a permissionless market as traceable, composable units of value. It will naturally interoperate with decentralized markets like Uniswap and open standards such as EIP-2612, enabling free exchange between value and intelligence without centralized gateways.

This is not a whitepaper—it is the Genesis Code of an intelligence–value isomorphic universe. With auditable contracts, verifiable parameters, and reproducible economics, it offers our answer: why “AI × Blockchain” is not a slogan but a new order; why “distribution” is not a marginal issue but the first cause of money and governance; why next-generation open intelligence must grow within a system that no one can shut down.

**The old world is aging; the new epoch is being compiled.**

**Welcome to Year One of pAI—where intelligence becomes value, and value nourishes intelligence.**

**— pAI Core Protocol Contributors, as the first coders of law**

**— The Decentralized Community, as the temporary guardians of the new order**

# Contents


**Chapter I The Narrative & Paradigm ........ 6**

1.1 The Call of the Value Internet ........ 7

1.2 The Dialectic ........ 7

1.3 The Mission Statement of pAI ........ 9

1.4 Name and Semiotics ........ 10

**Chapter II The Technological Firmament ........ 11**

2.1 Design Philosophy ........ 12

2.2 Contract Foundation ........ 13

2.3 Security Axioms ........ 14

2.4 On-Chain Verifiability ........ 15

**Chapter III The Four Laws of Dual-Track Mining ........ 16**

3.1 Law One (Instant) ........ 17

3.2 Law Two (Delayed) ........ 18

3.3 Law Three (Difficulty) ........ 19

3.4 Law Four (Anti-Reentrancy) ........ 20

3.5 Dual-Track Synergy ........ 21

**Chapter IV Tokenomics Charter ........ 22**

4.1 Total Supply and Composition ........ 23

4.2 Genesis and Liquidity ........ 23

4.3 PoW Reward Curve ........ 24

4.4 Vesting Pool ........ 25

4.5 Inflation and Scarcity ........ 26

**Chapter V Protocol Mechanics and Interfaces ........ 28**

5.1 PoW Core Flow ........ 29

5.2 Vesting Flow ........ 30

5.3 Difficulty Adjustment and Bounds ........ 31

5.4 Key States and Events ........ 32

5.5 Developer Interfaces ........ 33

**Chapter VI Security Matrix ........ 35**

6.1 Attack Surface Modeling ........ 36

6.2 Code Security ........ 37

6.3 Operational Security ........ 38

6.4 Contingency Plans ........ 39

6.5 Governance and Parameter Guardrails ........ 40

**Chapter VII The Application Cosmos ........ 41**

7.1 The AI Economy ........ 42

7.2 DeFi Integration ........ 42

7.3 Cross-Chain Interoperability ........ 43

7.4 Store of Value and Settlement ........ 44

7.5 Community Governance and Incentives ........ 44

**Chapter VIII Roadmap and Milestones ........ 46**

8.1 Phase I (Q4 2025) ........ 47

8.2 Phase II (2026 H1) ........ 47

8.3 Phase III (2026 H2) ........ 48

8.4 Phase IV (2027+) ........ 49

**Chapter IX Disclaimer ........ 50**

pAI Token

# Chapter I

## The Narrative & Paradigm

## 1.1 The Call of the Value Internet

For the past thirty years, humanity has been immersed in the singular explosion of the information internet. Countless bytes, links, and algorithms have interwoven into a vast cognitive web, redefining the boundaries of communication, dissemination, and perception. Yet this system, centered on “replication,” while bringing about an abundance of information, has proven incapable of bearing the weight of “value.” Data can be infinitely copied, but meaning cannot be infinitely diluted; algorithms can optimize attention, but they cannot define trust. Thus, at the peak of efficiency, we collided with the wall of trust.

Internet 1.0 achieved information interconnection; Internet 2.0 forged monopolies of platforms and social networks; and the emergence of Web3 is the rebellion and reconstruction of centralized trust. Humanity has finally begun to ask: after the freedom of information, how can value be free?

Blockchain is the first engineering answer to this question—it is not a database but a consensus machine; it endowed “trust” with physical properties for the first time. Ethereum took a step further, making value programmable and enabling order to execute automatically. However, there remains a chasm between the information internet and the value internet: data lacks ownership, intelligence lacks pricing, and computation cannot yet become an asset. AI models grow increasingly powerful, yet their training and profits remain confined within closed systems. This asymmetry is the new “centralization trap” of the intelligent age.

The birth of pAI is the call of the value internet to the intelligent internet. It does not seek to construct another hierarchy of power, but to make the “value flow” between computing power, data, models, and humans open, transparent, and verifiable once again. While the information internet solved the problem of “communication,” the value internet represented by pAI is solving the problem of “trust and distribution.”

## 1.2 The Dialectic

Every technological evolution is a dialectical process of civilization.

CeFi (Centralized Finance) is the starting point of order. It relies on institutional credit to establish the foundational framework for capital flow. It represents the "thesis" of efficiency, yet it simultaneously sows the "antithesis" of trust. When crises arise, all trust dissolves into illusion.

DeFi (Decentralized Finance) is the force of rebellion. It replaces intermediaries with smart contracts and rewrites rules through algorithms. It is the eruption of freedom, the revolution of trust—but it also brings new instability: stacked protocols, inflationary incentive structures, and short-sighted speculative cycles. DeFi possesses freedom but lacks order; it opens the door to a new world but has yet to build a stable horizon.

**pAI emerges as the synthesis.**

It transcends financial rebellion and advances toward intelligent autonomy. It no longer focuses solely on "how to trade," but rather asks "how to measure and distribute the production of intelligence." Through its dual-track mining mechanism, pAI transforms "instant contribution" (proof of work) and "long-term participation" (proof of time) into a unified consensus system—an innovation not only of economic design but also of the ancient philosophical pursuit of fairness, now digitally redefined.

**Within this dialectical framework:**

· CeFi is trust replaced;

· DeFi is trust algorithmized;

· pAI is trust intelligentized.

It is not a continuation of the financial system, but a third paradigm where value and intelligence coexist symbiotically.

## 1.3 The Mission Statement of pAI

Every civilization's monetary system embodies a philosophy of distribution.

In a centralized currency system, the right to issue money is order itself; in a decentralized system, the distribution mechanism is the foundation of trust. Bitcoin, through PoW, proved that "time and energy equal fairness." Ethereum, through the Gas mechanism, defined that "computation equals resource." pAI seeks to prove that "intelligence equals productivity, and participation equals equity."

**The dual-track mining mechanism manifests this mission concretely:**

**Track One: Traditional PoW Mining (41%)**

Instant rewards symbolize real contribution and competitive value; it honors computing power and the essence of work itself.

**Track Two: Linear Release Mining (10%)**

Time accumulation represents long-term trust and sustained commitment; it transforms holding and building into one unified behavioral logic.

**The remaining 49%** of initial allocation ensures ecological ignition, liquidity, and application deployment—fueling the network's "civilizational expansion phase."

**The meaning of this design extends beyond economics into philosophy:**

pAI transforms monetary distribution from a redistribution of wealth into a redefinition of the right to create value.

・In traditional economies, value originates from capital;

・in cryptographic economies, value originates from computing power;

・in intelligent economies, value will originate from the synergy of human and machine intelligence.

pAI's mission is to make such intelligent contributions quantifiable, provable, and accumulative.

It is not merely a token distribution model—it is a new social contract: a covenant that defines fairness in an intelligent civilization.

## 1.4 Name and Semiotics

In the world of semiotics, every name is a code of metaphor.

The symbol "pAI" is both a technical abbreviation and a philosophical declaration.

**The letter p carries two dimensions of meaning:**

· Proof — representing "provable existence." It is the soul of cryptography and the logical origin of trust. Without proof, intelligence is illusion; with proof, intelligence becomes an asset.

· People — representing human participation. It signifies that this system is not governed by algorithmic dictatorship but by community co-governance. It reminds us that all on-chain rules ultimately serve humanity—not cold code.

And AI, in this context, transcends "Artificial Intelligence." It heralds a new economic form: Autonomous Intelligence.

Within the context of pAI, AI is no longer a product of centralized corporations, but an open, decentralized ecosystem of intelligence. Every model, every dataset, every unit of computing contribution is a cell of this organism—and pAI is its bloodstream—circulating through every node, sustaining the life cycle of value and intelligence.

**Therefore, pAI is not merely the name of a token — it is a symbol of a new civilization.**

· It stands for a belief: that intelligence should not be monopolized, and value should not be distorted.

· It stands for an order: a decentralized intelligent contract co-signed, co-maintained, and co-benefited by both humans and machines.

Under this symbol, Proof and People, Algorithm and Humanity, finally find a new equilibrium in the pulse of the blockchain.

This is the true meaning of pAI—Proof of AI, Proof for All.

# pAI Token

# Chapter II

## The Technological Firmament

## 2.1 Design Philosophy

All contradictions in blockchain systems can ultimately be reduced to a triadic tension: Decentralization, Security, and Usability. These three forces form the "cosmic triangle" of every cryptographic system, within which no design can simultaneously achieve absolute optimization across all dimensions. Thus, every protocol must answer the same essential question: where does our Pareto frontier lie within this tension?

> **Bitcoin chose extreme security and decentralization, sacrificing throughput for pure immutability; Ethereum, in its pursuit of programmability, rebalanced the triangle through its Gas mechanism to preserve both computability and safety. The design philosophy of pAI is to open a new surface along this frontier curve:**
>
> · In decentralization, pAI maintains a pure PoW distribution mechanism, rejecting any pre-mining, private placements, or foundation-based centralized minting.
>
> · In security, the system centers on verifiable contract logic, built with the latest Solidity features for arithmetic safety and reentrancy protection, and introduces an event-level traceability system.
>
> · In usability, pAI adopts the EIP-2612 Permit signature authorization mechanism, greatly lowering interaction thresholds and ensuring seamless user experience without compromising security.

In other words, pAI does not take a mediocre compromise within the triangle; rather, it creates a new efficiency space through structural innovation — compressing usability loss while preserving decentralization and security, pushing all three dimensions toward a coexistence threshold never before achieved in human history.

Just as blockchain represents the relativity of financial history, pAI represents the quantum mechanics of the intelligent economy—it does not seek isolated extremes, but coherence and verifiability across the entire system.

## 2.2 Contract Foundation

Any sustainable protocol must rest upon transparent logic and minimal semantics.

The foundational layer of pAI is written in Solidity 0.8.30, not merely as a technical choice but as a philosophical declaration. From version 0.8 onward, Solidity enabled overflow checks, custom error handling, and gas optimization paths by default—elevating code from "runnable" to "provably secure."

At the standardization level, pAI adheres to the ERC-20 standard to ensure seamless interoperability with the Ethereum ecosystem, including DeFi protocols, wallets, and DEXs. ERC-20 transforms token behavior into a universal language—where transfers, approvals, queries, and events are all predictable, inheritable, and verifiable.

Furthermore, pAI integrates the EIP-2612 Permit extension, allowing users to authorize transactions through off-chain signatures.

In the traditional process, authorization (approve) and transfer (transferFrom) require two on-chain interactions and two gas fees. Through Permit, users complete both actions with a single signature and a single on-chain call.

**This mechanism achieves three essential goals:**

· Lower cost — reduces gas consumption by about 50%;

· Improved experience — removes the extra approval step;

· Enhanced security — includes expiration and nonce anti-replay fields in signatures to prevent forged calls.

This foundation makes pAI naturally compatible with Metamask, Ledger, Trezor, and other hardware or software wallets, as well as Uniswap, SushiSwap, and Balancer decentralized markets.

Contract is protocol, protocol is order. The goal of pAI's design is to make order itself the most trustworthy intelligent agent.

## 2.3 Security Axioms

In the universe of smart contracts, security is not a feature—it is an axiom.

**The code architecture of pAI strictly follows the CEI (Check–Effects–Interactions) paradigm—the golden rule of blockchain security engineering. Before performing any external interaction (such as transfers, minting, or callbacks), the system must execute:**

- Check — verify input, state, and permissions;
- Effects — update internal state, minimize reentrancy windows;
- Interactions — only then call external contracts or emit events.
- This execution order prevents reentrancy attacks and ensures atomic state transitions.

At the arithmetic level, Solidity 0.8.30 enables overflow and underflow checks by default. In performance-critical sections, pAI strategically uses unchecked blocks—disabled only where mathematically safe—achieving a balance between safety and efficiency.

**Additionally, the system replaces string errors with Custom Errors, saving roughly 50% of gas and improving clarity. For example:**

- error InvalidProofOfWork();
- error AlreadyMinedInBlock();
- error VestingPoolDepleted();

These errors can be directly recognized by block explorers and serve as auditable markers, forming a contract-level logging and audit system.

**The Minimized Trust Principle governs all design:**

- No multisig master keys;
- No administrators with unilateral parameter control;
- Every state, rule, and event is on-chain and fully traceable.
- Security here is no longer mere defense—it is a geometric property of consensus.

## 2.4 On-Chain Verifiability

The essence of decentralization is not anonymity—it is verifiability.

The entire operational architecture of pAI forms an observable mathematical system.

**In contract design, all critical actions emit events, such as:**

・Mint() — logs each successful mining and reward issuance;

・DifficultyAdjusted() — records difficulty adjustments and new block targets;

・EraTransition() — marks mining reward halving events;

・HashPowerSubmitted() and VestingRewardClaimed() — track each miner′ s hashrate trajectory and vesting reward claims in linear release mining.

**These events not only power DApp UIs but also serve as fundamental data sources for on-chain analytics. Through them, any third party can:**

・Monitor network difficulty and hashrate trends in real time;

・Track remaining balances in the linear release pool;

・Calculate each miner′ s actual contribution and average yield;

・Audit ecosystem inflation rates and circulating supply.

Moreover, the contract provides multidimensional query interfaces such as getMiningStats(), getMinerVestingStats(), and calculatePendingVestingReward(), allowing any node to reproduce network states without intermediaries. This makes pAI′ s economic system a fully transparent public dashboard, where anyone can judge system health through data, not belief.

Such structural transparency forms the third layer of security in decentralized systems: audit as consensus, transparency as defense.

**In traditional finance, transparency is the result of regulation;**

**in pAI, transparency is the origin of order.**

**Under this technological firmament, rules are physics, and code is law.**

pAI Token

# Chapter III

## The Four Laws of Dual-Track Mining

## 3.1 Law One (Instant)

In the cosmic structure of pAI, the first law is the Law of Immediacy—Proof of Work (PoW). It represents the system′ s original heartbeat, a direct measurement of time and energy. Bitcoin uses SHA256 to convert computing power into trust, while pAI adopts a dual Keccak256 (SHA3) algorithm to construct a new computational order with higher entropy and collision resistance.

**Workflow:**

・The miner generates the first hash layer using nonce and the current challengeNumber.

・The system performs a second Keccak256 computation to obtain digest.

・If digest < miningTarget, it is recognized as a valid solution.

The smart contract automatically verifies and executes the mint() function to complete accounting and rewards.

Unlike traditional simulated on-chain mining, pAI′ s PoW operates under completely decentralized conditions. Anyone who computes and submits a valid solution can immediately receive on-chain rewards.

During each epoch, the network′ s target output remains stable—approximately one pAI block for every 40 Ethereum blocks. Every 2048 epochs, the system adjusts difficulty to maintain the target block rate of eight minutes.

The reward mechanism follows a seven-stage halving curve, gradually decreasing from 100 pAI/epoch to 0.78125 pAI.

This exponential decay function ensures strong early incentives while achieving inflation convergence over time.

PoW represents the instant path of token distribution and the logical origin of pAI′ s fairness—it allows all computing power to compete for value on-chain under the same rules, same equations, and same probabilities.

## 3.2 Law Two (Delayed)

The second law represents reverence for time.

Traditional PoW rewards are paid instantly, but the sustainability of an intelligent economy requires a mechanism of delayed gratification — this is Vesting Mining (Linear Release Mining).

**In the linear release model, reward acquisition is no longer tied to immediate problem-solving but to the integral of "time × hashrate":**

・Each miner periodically submits proof of hashrate using submitHashPower().

・The system accumulates it as accumulatedHashPower.

・After at least one day, the miner may execute claimVestingReward() to receive the reward.

**The actual reward is determined by the formula:**

・actualReward = baseReward × (accumulated / required)

・where baseReward = daysPassed × 0.5 pAI, and required = daysPassed × 10.

If miners continuously submit sufficient computing power, they receive full rewards; if insufficient, the reward is proportionally reduced.

The philosophy: computing power is instantaneous, trust is temporal.

PoW rewards verify work; Vesting rewards verify persistence. The former is proof of energy, the latter is proof of endurance.

The 10,000,000 pAI vesting pool ensures long-term incentive balance, enabling short-term miners and long-term builders to coexist within one economic ecosystem.

In the logic of an intelligent economy, delay is not punishment—it is a filter that purifies noise into signal.

## 3.3 Law Three (Difficulty)

The third law belongs to system dynamics.

In the blockchain universe, Difficulty is the gravitational constant of self-regulation. It ensures that block generation remains stable and prevents computational power spikes from destabilizing the network.

**pAI' s adaptive algorithm adjusts every 2048 epochs by comparing the actual block rate to the target rate (40 Ethereum blocks ≈ 8 minutes) using the following logic:**

```
if (ethBlocks < TARGET_BLOCKS_PER_PERIOD) {

// Mining too fast → Increase difficulty

uint256 excessPct = ((TARGET - ethBlocks) * 1000) / TARGET;

uint256 decrease = (target / 2000) * excessPct;

miningTarget -= decrease;

} else {

// Mining too slow → Decrease difficulty

uint256 shortagePct = ((ethBlocks - TARGET) * 1000) / TARGET;

uint256 increase = (target / 2000) * shortagePct;

miningTarget += increase;

}
```

The difficulty range is set between 2^16 and 2^234, ensuring that the system neither accelerates uncontrollably due to hashrate surges nor halts due to hashrate declines.

This "interval-adaptive" mechanism enables pAI to dynamically absorb fluctuations in global computing power, maintaining long-term block stability.

2048 epochs serve both as a mathematical window and an ecological adjustment cycle.

In short periods, it tolerates volatility; in long periods, it synchronizes inflation with time.

Thus, pAI functions as a self-balancing system—responsive to changes in hashrate while resistant to speculative manipulation.

## 3.4 Law Four (Anti-Reentrancy)

The fourth law is the guardian of order.

In the world of smart contracts, reentrancy attacks and double-spend exploits are typical sources of chaos. pAI eliminates these risks through structured security strategies.

**The system follows the principle that "each Ethereum block can only mine one valid pAI reward":**

· if (lastRewardEthBlockNumber == block.number)

· revert AlreadyMinedInBlock();

This constraint removes the possibility of duplicate mining within a single block, ensuring each reward event is unique.

**At the code level, pAI strictly adheres to the CEI (Check-Effects-Interactions) paradigm:**

· Check conditions;

· Update state;

· Execute interactions.

All minting and reward logic use a "state-update-first" structure to ensure that no external call sequence can trigger recursive execution.

In addition, reward events (Mint, VestingRewardClaimed) embed timestamps and epoch indices, allowing any duplicate submission to be easily identified and rejected.

The system uses Ethereum's block hash blockhash(block.number - 1) as the next round's challengeNumber, creating a temporal linkage across challenges.

This ensures that each PoW solution is anchored to blockchain history—unforgeable and unpredictable.

Anti-reentrancy is not a patch but a physical constant of the system—like the speed of light in the universe, it defines the uniqueness of time and events.

## 3.5 Dual-Track Synergy

In pAI′ s economic ecosystem, the dual-track system is not oppositional but complementary.

Traditional PoW mining is a high-frequency competition field representing instant contribution; Vesting Mining is a low-frequency accumulation mechanism representing long-term trust. The coexistence of these two tracks balances short-term activity and long-term stability.

**The equilibrium lies in the coupling of rate and steady state:**

· Professional miners use high hashrate to participate in PoW, pursuing instant rewards while providing network security.

· Long-term participants submit stable proofs in Vesting, pursuing sustained income while contributing resilience and stickiness to the system.

**Economically, the two create complementary flows:**

· Instant incentives from PoW bring liquidity; buffered incentives from Vesting absorb volatility.

· When PoW difficulty rises and miners migrate, the stable output of the Vesting pool serves as a buffer for price and community confidence.

· In game-theoretic terms, pAI′ s dual-track architecture forms a Nash equilibrium—no single participant group can alter the system′ s long-term state through short-term behavior.

Technically, both mining modes share the same challenge source (challengeNumber), meaning the entire network′ s security is driven by a unified entropy seed.

Socially, it enables the coexistence of various participant types—developers, miners, and token holders—all contributing to network evolution at their own rhythm.

Therefore, pAI is not merely a mining system—it is a model of social collaboration.

It transforms computing power into labor, time into trust, and holding into participation.

In this experiment of fair distribution for the intelligent age, pAI defines — through mathematics—a new boundary of order: instant and delayed coexistence, competition and cooperation in harmony.

This is the true equilibrium of the intelligent value system.

pAI Token

# Chapter IV

## Tokenomics Charter

## 4.1 Total Supply and Composition

pAI′ s economic system sets an eternal cap of 100,000,000 tokens—a total that symbolizes a closed-loop order while aligning with computational aesthetics. This figure is not arbitrary; it was determined through multiple rounds of economic simulation and inflation modeling to ensure the coexistence of ecosystem sustainability and long-term scarcity.

**The total supply is structured as follows:**

· 49% (49,000,000 pAI): Initial allocation for liquidity, ecosystem development, and governance reserves;

· 41% (41,000,000 pAI): Fair distribution via instant mining (PoW), forming the backbone of hashrate consensus;

· 10% (10,000,000 pAI): Linear release (Vesting Mining) to incentivize long-term contributors.

This three-segment distribution follows a cyclical logic of "short-term incentives — mid-term construction — long-term governance."

The PoW phase ensures early users can participate in distribution through real computing power, while the linear release mechanism establishes social stickiness through delayed incentives.

The initial allocation carries a public role in ecosystem governance—maintaining network security, market liquidity, and development support.

In essence, pAI′ s total-supply design is a "constitutional constraint of intelligent currency" —no central authority can mint more or amend it; the issuance cap is embedded in the smart contract itself, becoming a verifiable economic physical constant.

## 4.2 Genesis and Liquidity

In the genesis stage of token economics, the 49,000,000 pAI initial allocation plays a dual role as the system′ s "blood and bones." Its use and constraints are strictly encoded in contract logic and multisig governance, divided into three parts:

**DEX Liquidity Bootstrapping Pool (~30%)**

Approximately 14,700,000 pAI will be injected directly into major decentralized exchanges (e.g., Uniswap, SushiSwap, Balancer), paired with ETH or USDC to form initial liquidity. This portion will be time-locked at the contract level and LP tokens will be burned to prevent early manipulation or withdrawal risks.

**Ecosystem Development Fund (~50%)**

24,500,000 pAI will support ecosystem partners, AI compute alliances, DApp developers, cross-chain bridges, and market expansion initiatives. Funds will be released in tranches via DAO proposals, with each disbursement confirmed by on-chain voting to uphold decentralized fiscal discipline.

**Governance and Security Reserves (~20%)**

9,800,000 pAI will be stored in a multisig cold wallet, custodied by a community-elected Security Council, for future contract upgrades, security audits, protocol migrations, and emergency responses. Any transfer requires a 3-of-5 signature threshold.

The genesis 49M is the bedrock of system order, not a capitalization tool. Through smart locks and transparent voting, it ensures resources always serve the protocol itself—not any individual or institution. Liquidity can launch, governance can self-govern, and the ecosystem can self-grow.

## 4.3 PoW Reward Curve

pAI′ s PoW distribution logic centers on a "time curve" rather than a "block curve," using a seven-halving model combined with an exponential decay formula so issuance smoothly converges on a century scale.

**Initially, each valid mining epoch rewards 100 pAI. After completing 2048 epochs × 7 rounds, the system automatically triggers a halving event, with rewards transitioning as follows:**

100 → 50 → 25 → 12.5 → 6.25 → 3.125 → 1.5625 → 0.78125

The entire process spans roughly 100 years, approaching but never reaching zero. This "tail decay" ensures perpetual incentives, preventing hashrate exit and security decay.

**Advantages of the model:**

・Ample early incentives: encourages early miners and nodes to join;

・Smooth mid-term release: reduces market sell-pressure volatility;

・Extended long tail: sustains the life cycle of the economic ecosystem.

Moreover, halving parameters and epoch intervals are encoded in the smart contract and cannot be altered.

In other words, pAI′ s PoW is a contract signed by time—each pAI is a physical proof co-signed by computing power and time.

## 4.4 Vesting Pool

As pAI′ s second distribution track, the linear release mechanism (Vesting Mining) bears the dual mission of "long-term incentives" and "time-based consensus."

**Under this system, each miner′ s daily base release quota is 0.5 pAI, subject to the following conditions:**

・At least 10 hashrate submissions per day

・A minimum interval of 10 minutes between submissions to ensure data authenticity and continuity;

・ Each submission is verified by submitHashPower() and accumulated into accumulatedHashPower;

**Reward formula:**

・actualReward = baseReward × (accumulated / required)

・where baseReward = daysPassed × 0.5 pAI, and required = daysPassed × 10.

If a miner fails to meet the daily hashrate standard, the reward for that day is proportionally reduced and cannot be retroactively claimed.

By combining "time integral + hashrate threshold," this mechanism yields distribution that is both rigid and elastic.

The 10,000,000 pAI vesting pool runs at a constant rate, averaging about 1,000,000 pAI released per year over roughly ten years.

This process is independent of PoW halvings, forming a long-term, stable incentive substrate.

Economically, this structure both delays sell pressure and strengthens contributor persistence.

The vesting pool is the network's "slow-burn engine"—it optimizes for steady-state growth rather than speed.

## 4.5 Inflation and Scarcity

At the macroeconomic level, pAI's monetary design follows an Era-based inflation model. Each Era corresponds to a full halving cycle; the system automatically computes the annual new issuance and current circulating supply, thereby deriving the annualized inflation rate dynamically:

**Era Block Reward (pAI) Annualized Inflation (est.)**

- Era1 100 ≈ 22.4%
- Era2 50 ≈ 11.2%
- Era3 25 ≈ 5.6%
- Era4 12.5 ≈ 2.8%
- Era5 6.25 ≈ 1.4%
- Era6 3.125 ≈ 0.7%
- Era7 1.5625 ≈ 0.3%
- Era8 0.78125 ≈ 0.15%

This design yields an exponentially decaying inflation rate, converging near zero after the eighth Era.

Meanwhile, the vesting pool becomes the main issuance source in later stages, acting as a balancing factor for ecosystem maintenance and user incentives.

**Importantly, pAI′ s monetary strategy is not purely deflationary but structurally scarce:**

· The supply cap is fixed, but ecosystem liquidity adjusts dynamically with participant behavior.

· When hashrate declines or participation decreases, the release rate slows automatically; as the ecosystem expands and user activity rises, validated compute increases and the release rate naturally accelerates.

This feedback-driven monetary system gives pAI′ s economy a self-breathing function—adjusting during growth and stabilizing during convergence.

The ultimate outcome is an intelligent economy where annualized inflation tends toward zero, holding returns trend toward long-term compounding, and monetary value is defined by behavior rather than issuance alone.

pAI Token

# Chapter V

## Protocol Mechanics and Interfaces

## 5.1 PoW Core Flow

**Within pAI' s operating logic, the PoW core flow is the system' s underlying pulse. Each valid block event emerges from the dynamic interplay of four variables: challenge, nonce, digest, and target.**

・challenge: The current mining challenge number, derived from the previous block hash blockhash(block.number - 1). It updates automatically after each block to ensure randomness and prevent precomputation.

・nonce: The random number submitted by the miner to generate a hash result. Each miner may try unlimited nonces until computing a digest that meets the target condition.

・digest: The core computation result. The miner computes Keccak256 twice over challenge + msg.sender + nonce to obtain digest.

・target: The current difficulty threshold. When digest < target, mining succeeds.

**Contract verification logic:**

・bytes32 digest = keccak256(abi.encodePacked(challenge, msg.sender, nonce));

・digest = keccak256(abi.encodePacked(digest));

・if (uint256(digest) > miningTarget) revert InvalidDigest();

Upon verification, the system triggers mint(), logs events, distributes rewards, and updates challengeNumber and epochCount.

**This mechanism fuses randomness, security, and determinism:**

・Randomness derives from the combination of block hash and nonce;

・Security relies on the collision resistance of double hashing;

・Determinism is enforced by automatic verification in the smart contract.

PoW is the protocol' s time generator—each valid block not only creates pAI but also advances the system' s state clock, providing a baseline for subsequent difficulty adjustments and vesting calculations.

## 5.2 Vesting Flow

Unlike the high-frequency events of instant mining, Vesting Mining is a low-frequency, continuous, state-driven process.

It uses submitHashPower() as the entry point and claimVestingReward() as the redemption endpoint, with the "time × hashrate" accumulation logic in between.

**The entire flow comprises three stages:**

・Hashrate submission (submitHashPower)

・Each miner submits multiple proofs within a period; the system records submission time and hashrate value.

```
function submitHashPower(uint256 power) external {

Miner storage miner = miners[msg.sender];

miner.accumulatedHashPower += power;

miner.lastSubmission = block.timestamp;

emit HashPowerSubmitted(msg.sender, power);

}
```

Time accumulation (Time Accumulation)

**The system computes daysPassed = (now - lastClaim) / 1 days and combines it with accumulated hashrate to produce a "time-weighted hashrate":**

weighted = accumulatedHashPower × daysPassed.

This weight represents the miner's real contribution in the time dimension.

Reward claim (claimVestingReward)

After meeting the daily standard of ≥ 10 submissions, the miner may call:

```
function claimVestingReward() external {

Miner storage miner = miners[msg.sender];

uint256 reward = baseReward * (miner.accumulated / required);
```

miner.accumulated = 0;

miner.lastClaim = block.timestamp;

_mint(msg.sender, reward);

emit VestingRewardClaimed(msg.sender, reward);

}

Rewards scale with both time and hashrate; unmet portions are proportionally reduced.

This mechanism converts short-term computational behavior into long-term economic participation.

SubmitHashPower proves behavior; claimVestingReward cashes in trust.

By means of smart contracts, it binds labor, time, and value into an unfalsifiable mathematical relationship.

## 5.3 Difficulty Adjustment and Bounds

To ensure long-term stability of the network’s block rate, the pAI protocol embeds an adaptive difficulty adjustment system.

Using 2048 epochs as one adjustment cycle, each cycle compares the actual block rate to the target (40 Ethereum blocks ≈ 8 minutes) and adjusts miningTarget accordingly.

**Core logic:**

```
if (ethBlocks < TARGET_BLOCKS_PER_PERIOD) {

// Mining too fast → increase difficulty

miningTarget -= (miningTarget / 2000) * ((TARGET_BLOCKS_PER_PERIOD - ethBlocks) * 1000 / TARGET_BLOCKS_PER_PERIOD);

} else {

// Mining too slow → decrease difficulty
```

miningTarget += (miningTarget / 2000) * ((ethBlocks - TARGET_BLOCKS_PER_PERIOD) * 1000 / TARGET_BLOCKS_PER_PERIOD);

}

To prevent extreme swings, the system imposes a ±50% cap on single-step adjustments and constrains the target range to 2^16–2^234.

When hashrate surges, difficulty increases proportionally; when participation declines, difficulty eases, keeping the average block rate on a steady rhythm.

**This range-constrained adjustment yields high elasticity and stability:**

・Short-cycle disturbance resistance: tolerates hashrate volatility;

・Long-cycle self-balancing: converges toward the 8-minute target;

・Economic anti-speculation: prevents abrupt hashrate migration from shocking price.

・In short, pAI′s difficulty curve is an "economic rhythm controller,"

ensuring at a mathematical level that the network does not drift off course due to external energy imbalance.

## 5.4 Key States and Events

Every key action in the pAI protocol is accompanied by Event logs and State Variable updates, forming a complete system of traceability and audit.

**Primary states and events include:**

epochCount: current mining epoch counter;

miningTarget: current difficulty threshold;

challengeNumber: current mining challenge number;

lastRewardEthBlockNumber: previous reward block number;

totalSupply: total issued token supply;

vestedSupply: cumulative linear-release amount;

Mint(address, uint256, uint256, uint256, bytes32): PoW success event;

VestingRewardClaimed(address, uint256): linear-release reward event;

DifficultyAdjusted(uint256, uint256): difficulty adjustment record;

EraTransition(uint256, uint256): halving-stage transition event.

All events include indexed fields and can be tracked directly by DApp frontends, analytics tools, and third-party explorers (e.g., Etherscan, Dune, Nansen).

**This means any user or auditor can reconstruct a panoramic on-chain view of protocol operation:**

・Monitor block rate, difficulty curve, miner counts, and hashrate distribution in real time;

・Verify transparent issuance of Vesting rewards;

・Track circulating supply and inflation trends.

This transparent metrics and observability stack is the core of pAI′ s trust architecture.

**Data is order; events are evidence.**

**In pAI, external auditors are unnecessary—the contract itself is the most perfect auditor.**

## 5.5 Developer Interfaces

The pAI protocol provides a complete interface suite for developers and ecosystem applications, balancing standards compliance with extensibility.

Generic ERC-20 interface

**Following Ethereum standards, developers can call:**

・function balanceOf(address account) external view returns (uint256);

・function transfer(address recipient, uint256 amount) external returns (bool);

・function approve(address spender, uint256 amount) external returns (bool);

· function transferFrom(address sender, address recipient, uint256 amount) external returns (bool);

· These work seamlessly with front-end wallets (Metamask, Ledger, etc.).

· Permit signature authorization (EIP-2612)

**Supports off-chain signatures and gasless approvals:**

function permit(

address owner,

address spender,

uint256 value,

uint256 deadline,

uint8 v, bytes32 r, bytes32 s

) external;

Developers can integrate this to enable a one-signature approve+transfer flow, improving UX and reducing gas costs.

PoW and Vesting query interfaces

function getMiningStats(address miner) external view returns (

uint256 currentChallenge, uint256 target, uint256 epochCount, uint256 difficulty

);

function getMinerVestingStats(address miner) external view returns (

uint256 accumulatedPower, uint256 lastClaim, uint256 pendingReward

);

These functions let DApps, pools, and analytics platforms readily access real-time state and statistics.

# Chapter VI

## Security Matrix

## 6.1 Attack Surface Modeling

Security is not a state but an ongoing game.

In pAI, security architecture is not an add-on; it is protocol DNA. Through Attack Surface Modeling, it identifies potential threats and implements multi-dimensional defenses across contract, economic, and social layers.

### (1) Reentrancy

**A common attack type. pAI strictly follows the CEI (Check–Effects–Interactions) paradigm:**

・State updates precede any external calls;

・mint() and claimVestingReward() update balances internally before emitting events;

・All mutating functions carry a nonReentrant guard to prevent recursive triggers.

### (2) Replay

Via EIP-2612 Permit' s nonce and deadline fields, pAI prevents replay at the signature level. Any expired or duplicate signatures are rejected.

### (3) Front-running

System event design does not depend on transaction ordering. Because PoW submissions are unique (protected by AlreadyMinedInBlock()), even if an attacker copies another' s transaction, they cannot profit twice within the same block.

### (4) Sybil Hashpower Attack

pAI' s mining logic binds msg.sender to challengeNumber. Each address computes its own hash outcome, and cloning addresses cannot yield linear gains. The cost of a Sybil attack grows exponentially with hashrate.

### (5) Mining Pool Game Theory

The system supports coexistence of solo miners and pools. Since rewards are tightly coupled to submission timing, pools cannot monopolize returns by delaying submissions; the 2048-epoch difficulty adjustment prevents any single pool from controlling the global block rhythm.

These five core surfaces form pAI' s "threat spectrum."

## 6.2 Code Security

Code security is the first line of protocol stability. pAI strengthens contract safety at the semantic level, with all logic adhering to “verifiable, explainable, minimized trust.”

### (1) Custom Errors

・Replaces the traditional require("ErrorString") pattern.

・Declarative error definitions:

・error InvalidDigest();

・error AlreadyMinedInBlock();

・error UnauthorizedClaim();

This saves roughly 50% gas and improves debugging readability. Each error is uniquely identifiable for tracing on Etherscan and in debuggers.

### (2) Gas Optimization

・Use unchecked blocks in internal loops only where mathematically safe to disable overflow checks;

・Mark frequently called read-only functions as view/pure to reduce gas;

・Use indexed event fields to optimize log indexing;

・Apply storage packing/boolean compression (bit packing) to reduce SSTORE costs.

### (3) Read-only Reentrancy Protection

・pAI introduces improved locks distinguishing “write locks” and “read locks”:

・writeLock prohibits external calls during state mutation;

・readLock allows query-only interactions, preventing off-chain probing from causing timing skew.

Thus, even with flash loans or simulated nodes attempting “informational front-running,” attackers cannot precompute reward allocation or difficulty updates.

## 6.3 Operational Security

The second layer of security for smart protocols lies in operations and governance.

**pAI′ s core assets and upgrade powers are tightly constrained:**

**(1) Multi-Sig Treasury**

All ecosystem funds, governance reserves, and security vaults are managed by a multisig wallet (e.g., Gnosis Safe).

**Execution rules:**

・At least 3/5 signers must confirm for transfers;

・Each action is recorded on-chain and emits TreasuryActionExecuted;

・All signer lists are public and community-auditable.

**(2) TimeLock**

Critical governance actions (parameter changes, upgrade proposals) must be publicly announced 48 hours in advance, entering a cooling period.

This provides a review window and prevents “flash governance attacks.”

**(3) Security Audit**

Full third-party audits occur before mainnet deployment and after major upgrades, covering:

・Permission boundary checks;

・Event integrity verification;

・Math-model correctness;

・Fuel-consumption curve review.

**(4) Bug Bounty**

Permanently open; white-hat reports via security platforms are rewarded from 100 to 50,000 pAI based on severity and reproducibility.

## 6.4 Contingency Plans

The highest form of security is preserving order amid crisis.

**pAI designs a three-tier emergency response for extreme on-chain anomalies:**

**(1) Difficulty Drift**

**If block rate deviates by ±200% due to sudden hashrate surges or mass miner exit, the system enters "Emergency Difficulty Mode":**

・During the cooldown, cap miningTarget adjustments to ≤ 25%;

・Enable an EMA (Exponential Moving Average) smoothing function to compute future targets and avoid step changes.

**(2) Rollback Mitigation**

・Upon detecting chain reorgs or splits, the system compares epochCount and challengeNumber historical snapshots. On conflict, it automatically reverts to the last confirmed state.

・It also emits ChainReorgDetected() for manual review by the multisig Security Council.

**(3) Rapid Coordination Mechanism**

**If contract or economic anomalies arise (e.g., reward misallocation, abnormal hashrate concentration), trigger the Council's "Fast Governance Mode":**

・All governance transactions enter a 1-hour response window;

・The DAO publicly announces freezes on related function calls;

・After voting, execute restoration or parameter adjustments.

**Core idea: "Order before repair."**

**pAI does not pause; it restores stability with minimal intervention.**

**Security is not static defense, but elastic recoverability.**

## 6.5 Governance and Parameter Guardrails

The ultimate risk of any decentralized system lies in its governors.

pAI adheres to Minimal Custody and Maximal Verifiability — DAO governance cannot violate the on-chain constitution.

### (1) Verifiable Parameters

Core parameters such as miningTargetRange, epochInterval, and vestingRate have contract-defined bounds:

・require(newTarget >= 216 && newTarget <= 2234, "OutOfBounds");

・require(newVestingRate <= MAX_VESTING_RATE);

・No governance proposal can exceed these physical limits.

### (2) On-chain Audit Line

All parameter changes, fund transfers, and contract calls automatically emit GovernanceActionExecuted() with hashes for real-time third-party tracking.

### (3) Community Watchers

The DAO runs an open registry of watcher nodes to monitor key on-chain events. On detecting anomalies, they can signal a freeze vote and initiate a cooling period.

### (4) Cooling-off and Reconfirmation

All parameter changes require two voting rounds separated by 24 hours to prevent governance capture.

**These guardrails ensure:**

・No one can unilaterally alter protocol logic;

・All changes are verifiable;

・Community oversight has enforceable power.

・The end state of security is self-supervising order.

pAI' s Security Matrix is not merely a shield; it is a distributed immune system: it relies on transparency, not trust; coherence, not walls.

pAI Token

# Chapter VII

## The Application Cosmos

## 7.1 The AI Economy

pAI's primary mission is to make intelligence a priceable means of production. In the traditional AI economy, compute, data, and models are long enclosed within the walls of centralized platforms, forming "algorithmic oligopolies." pAI, through on-chain incentives and verifiable settlement, enables autonomous coordination across the entire AI supply chain.

Compute leasing: Researchers or enterprises can rent distributed GPU/TPU capacity from nodes via pAI smart contracts. Leases settle in pAI; once computation finishes, nodes submit on-chain a Proof of Inference, and the system immediately releases payment. All compute contributions are recorded with hash signatures, forming a traceable compute ledger.

Model trading: Trained AI models are minted on-chain as NFTs with parameter hashes and version numbers. After buyers pay in pAI, they obtain invocation rights; revenue is automatically split to the original developers and the compute providers who contributed to training, realizing distributed tokenization of model income.

Dataset marketplace: Data owners may upload encrypted shards for training inside secure sandboxes operated by AI nodes. Access counts and inference call volumes are metered by contract and paid in pAI. Privacy is preserved while value is unlocked.

Inference metering: Here pAI acts as "AI fuel." Each API call, inference request, or micro-agent interaction settles in pAI, enabling fine-grained, programmable intelligent economics.

Ultimately, pAI reconstructs a decentralized AI economic loop in which every link—compute, model, data, inference—is measurable, revenue-sharing, and governable.

## 7.2 DeFi Integration

Financially, pAI is not an isolated token but an AI-native asset within DeFi. It combines a stable mining emission curve with composable financial properties.

Collateralized lending: Users can supply pAI to Aave, Compound, and similar protocols to obtain stablecoin liquidity. Loan-to-value ratios adjust dynamically based on pAI's inflation curve and historical volatility to balance capital efficiency and risk symmetry.

LP market making: pAI/ETH, pAI/USDC, and other pools provide trading depth. Liquidity providers use Uniswap v3's concentrated liquidity to supply pAI within chosen price ranges and earn fees.

Yield aggregation: Yearn/Beefy-style strategies can aggregate PoW rewards and LP yields into compounding portfolios. Holders can auto-rebalance across pools—achieving "passive mining + passive market making."

Derivatives markets: Because pAI has a deterministic issuance model, it can serve as a long-term inflation anchor for futures, options, and hashrate certificates. For example, “hashpower options” let miners pre-sell future pAI emissions to hedge electricity or hardware costs.

pAI’s DeFi properties make it more than a token—it is a financial language: it can circulate, be collateralized, leveraged, and fractioned—while always maintaining a verifiable source of value.

## 7.3 Cross-Chain Interoperability

A true intelligent economy cannot be confined to a single chain. pAI adopts a cross-chain interoperability architecture to coordinate mainnet–sidechain–multichain deployments.

L2 scaling: Deploy PoW light clients on Arbitrum and Optimism, using rollups to aggregate and submit block proofs—achieving low-gas mining with near-instant confirmations. Miners compute on L2 and submit results to Ethereum mainnet for verification and settlement.

Cross-chain bridges: Via cross-chain messaging protocols such as LayerZero and Axelar, pAI can be natively mirrored to BNB Chain, Polygon, Base, etc. Bridge contracts adopt a Proof-of-Mint mechanism to ensure each cross-chain mint corresponds to a mainnet lock.

Messaging layer integration: pAI’s event model (Mint, VestingRewardClaimed) aligns with interchain message buses so external protocols can subscribe to mining events in real time for AI task scheduling or DeFi yield synchronization.

**Multichain deployment is not blind duplication but functional layering:**

- Ethereum: value settlement layer;
- Arbitrum/Optimism: computation and interaction layer;
- BNB/Polygon: liquidity diffusion layer.

This design makes pAI a cross-chain intelligent-value protocol with unified identity, issuance, and logic across a multiverse of chains.

## 7.4 Store of Value and Settlement

As the AI compute economy scales rapidly, traditional stablecoins struggle to support micro-payments and instantaneous settlement for intelligent tasks. pAI is therefore defined as an AI-native Settlement Token.

Store of value: The dual-track PoW + Vesting mechanism gives pAI innate anti-inflation traits. Its release curve is predictable, and total supply is fixed—providing a stable "unit of reserve" within the AI ecosystem.

Instant settlement: With EIP-2612 Permit, AI agents can initiate signed on-chain payments automatically, enabling millisecond-level inference settlement. No trusted third party and no cross-border delays.

Ecosystem compatibility: pAI can serve alongside ETH and USDC as settlement currency in DeFi; its gasless authorization suits AI APIs and micro-payment endpoints, becoming a standard unit for on-chain service invocation.

Market significance: pAI provides the infrastructure for pricing and settlement of "intelligent labor." AI no longer relies on fiat or stablecoins; it uses a value medium generated by itself—marking the true monetization of the agent economy.

## 7.5 Community Governance and Incentives

In pAI, the community is not an appendage but the system's extended neural network. Governance and incentives are integrated within one economic loop.

**Governance:**

· Any address holding pAI ≥ 10,000 may submit a Proposal;

· Proposals enter a 48-hour cooling-off before voting;

· Execution requires > 51% participation and ≥ 60% approval;

· The multisig governance module GovernorExecutor executes and posts results on-chain.

**Incentive allocation:**

**From the initial 49M reserve, 15% is earmarked as a long-term Community Incentive Pool for:**

・Developer grants and hackathons;

・Open-sourcing AI models or tools;

・Community content and node-runner incentives;

・Bridge, liquidity pool, and partner matching funds.

**Closed-loop logic:**

・Proposal → Voting → Execution → Fund Flow → On-chain Feedback.

・All governance actions emit GovernanceActionExecuted(), verifiable by any node.

This coherent structure means pAI is not merely a protocol but a self-evolving economic organism:

It replaces commands with consensus, centralization with incentives, and authority with data.

pAI Token

# Chapter VIII

## Roadmap and Milestones

## 8.1 Phase I (Q4 2025)

The genesis phase focuses on dual validation: operability and credibility. In Q4 2025, core tasks include mainnet launch, contract security audits, DEX liquidity seeding, and the initial formation of a global miner network.

**Mainnet deployment:**

・Deploy PoW and VestingMining core contracts to Ethereum mainnet and activate the Genesis Block via the multisig governance module.

・Mainnet release codename: Singularity-1.0, integrating EIP-2612, the event traceability system, and the linear-release mechanism.

**Security audits:**

Two international security firms (anticipated CertiK and SlowMist) will perform full-scope audits covering permission boundaries, economic models, attack surfaces, and gas optimization. Reports will be posted on-chain.

**Liquidity construction:**

・Establish pAI/ETH and pAI/USDC pairs on Uniswap and SushiSwap; seed the first fair-launch liquidity round totaling ~2,000,000 pAI.

・LP tokens adopt a 180-day timelock governance guard to stabilize early markets.

**Miner organization:**

・Form the pAI Mining Collective (PMC) to provide clients and remote compute access guides for solo and pool nodes.

・This phase’s core goal is to validate the technical path and bootstrap the ecosystem.

## 8.2 Phase II (2026 H1)

In H1 2026, pAI moves from “operable” to “scalable.” The focus is infrastructure build-out and first application launches.

**Mining-pool system:**

Release a reference pool protocol (pAI-Pool v1), allowing third parties to run pools via open APIs. Pool reward split fixed at 95% to users, 5% to ops, deterring centralized hash monopolies.

**Block explorer:**

Launch a visualization dashboard (pAI Explorer) to monitor difficulty curves, block rates, PoW distribution, and Vesting status in real time.

**DEX incentive program:**

Start a 6-month liquidity mining campaign with dual incentives (pAI + ETH) on major pairs. Rewards follow a decaying schedule to deter short-term mercenary capital.

**First AI DApps:**

・Deploy three exemplar apps;

・Inference Hub — decentralized inference metering and billing;

・Model NFT Market — on-chain model minting and revenue sharing;

・pAI Pay — gasless micro-payment plugin for AI APIs.

Strategically, this stage activates the first energy cycle of the ecosystem: mining → trading → consumption.

## 8.3 Phase III (2026 H2)

As the ecosystem matures, pAI evolves from a “single-chain value system” into a “multi-layer cooperative compute network.” H2 2026 emphasizes cross-chain connectivity and open markets for compute and models.

**Compute market (pAI Compute Market):**

・Miners lease idle compute to researchers or enterprises with smart-contract billing and automatic settlement.

・Proof of Inference is co-signed by on-chain verifier nodes, forming traceable resource attestations.

**Model market (pAI Model Hub):**

・Model uploads, authorization, and revenue distribution are fully on-chain.

・ Supports parameter encryption and sandboxed inference; developers can build secondary DApps atop models.

**Cross-chain and L2 deployments:**

・L2: roll out light-node sync modules on Arbitrum and Optimism for low-gas mining and instant verification.

・Multichain: bridge via LayerZero to BNB Chain, Polygon, and Base for asset interoperability and message sync.

**Ecosystem SDK:**

Release the pAI SDK supporting third-party AI/DeFi/GameFi integrations for mining interfaces, settlement APIs, and governance functions.

## 8.4 Phase IV (2027+)

From 2027 onward, pAI progresses from a technical system to an economic-civilization system. Keywords: autonomy, financialization, globalization.

**Multichain prosperity:**

・Deploy mutually recognized nodes on at least five public chains to form a unified Multi-chain Intelligence Asset Layer.

・Synchronize token supply and mining progress across chains to ensure consistent, verifiable economic data.

**Deep DeFi integration:**

・Introduce derivatives (pAI Futures), Hashpower Options, and stable AI reserve products (AI Vault).

・DeFi protocols and AI services share liquidity, making "intelligence as yield" a reality.

**Enhanced governance:**

・Upgrade the DAO to a tricameral structure (Technology, Ecosystem, Treasury).

・Introduce sub-DAOs; local communities can propose, execute, and budget independently.

・Global nodes achieve asynchronous consensus via Snapshot voting.

pAI Token

# Chapter IX

## Disclaimer

This whitepaper explains the technical principles, economic mechanisms, and ecosystem plans of the pAI project and is for informational purposes only. It does not constitute investment advice, an issuance solicitation, or a legal commitment of any kind. The pAI team and its affiliates make no express or implied warranties regarding the completeness, accuracy, or future realization of the contents herein. Actual project progress, technical paths, and economic parameters may change due to market conditions, regulatory policies, technical constraints, or community governance decisions; updates will be announced through official channels.

Participants using pAI products, engaging in mining or trading, or joining ecosystem governance should understand the potential risks of blockchain technology and digital assets, including but not limited to price volatility, smart-contract vulnerabilities, network attacks, regulatory changes, and insufficient liquidity. pAI tokens do not represent equity, debt, revenue rights, or any other legal rights; their value is determined entirely by market supply-demand and community consensus. Users bear full responsibility for holding or using pAI.

Furthermore, the pAI protocol and its ecosystem components are open-source. Anyone may deploy, fork, or build derivatives. The official team assumes no responsibility for consequences arising from third-party use, forks, or integrations. The project will not be liable for compensation or accountability for asset losses caused by force majeure, technical flaws, or failures of third-party services.

By reading this whitepaper or participating in pAI-related activities, participants are deemed to have fully understood and accepted the above risk disclosures and disclaimers. pAI advocates an open, transparent, and self-disciplined crypto ethos and reminds all users to participate in the construction and development of the intelligent economy with rational, long-term, and responsible attitudes.