UTON Blockchain

white paper

May 22 , 2026

summary

UTON Blockchain（UTON）is a future-oriented, quantum-secure, and natively AI-compatible decentralized underlying network. With the shift in AI paradigms from single-model to Agent IC Ecosystems expected by 2026, traditional blockchain architectures face severe challenges in security, interaction efficiency, and identity verification.

UTON, based on the quantum-resistant Tendermint-BFT consensus framework, has deeply reconstructed the Ethereum Virtual Machine (EVM), making it not only perfectly compatible with decentralized applications for human users, but also natively supporting high-frequency, low-friction interactions of AI Agents at the underlying

protocol level. By fully integrating NIST-standardized post-quantum cryptography (PQC) algorithms, introducing the ERC-8004 machine identity standard, the x402 automatic payment protocol, and TEE+zkML verifiable smart technology, UTON is committed to building a secure, efficient, and sovereign shared digital infrastructure for global AI agents in the quantum computing era.

1. Overview

1.1 Vision and Positioning

UTON 's mission is to build a secure foundation capable of supporting trillions of AI agent interactions. In the context of 2026, AI will no longer be merely an auxiliary tool, but an economic entity with independent decision-making capabilities and asset control. Through a complete reconstruction of the underlying protocols, UTON provides these "machine citizens" with a full suite of native support for identity recognition, automated payments, and computational process verification, aiming to become a globally leading Web3 infrastructure fully aligned with the "silicon-based autonomous economy" and possessing absolute security.

1.2 Core Principles

Native AI Adaptation : From account model and instruction set to consensus logic, it is fully optimized for the high-frequency interaction, low-latency confirmation and millisecond-level response requirements of

AI Agent.

Quantum-resistant security across the entire network : PQC algorithm is integrated into every data layer of the network to ensure the long-term security of massive asset transfers and smart contract logic controlled by AI agents in the era of quantum supremacy.

Decentralized Trusted Computing : Utilizing cryptographic techniques such as TEE and zero-knowledge proofs, it ensures the transparency of the AI reasoning process and the verifiability of the execution results, fundamentally solving the trust problem of the "black box" of AI.

2. Industry Background: The Confluence of Two Technological Inflection Points

2.1 The Rise of Machine Sovereignty and AI Agents

By 2026, AI agents had achieved a 79% penetration rate in financial decision-making, cross-organizational collaboration, and supply chain management. This means that on-chain economic participants are no longer limited to humans. Traditional "human-oriented" account models

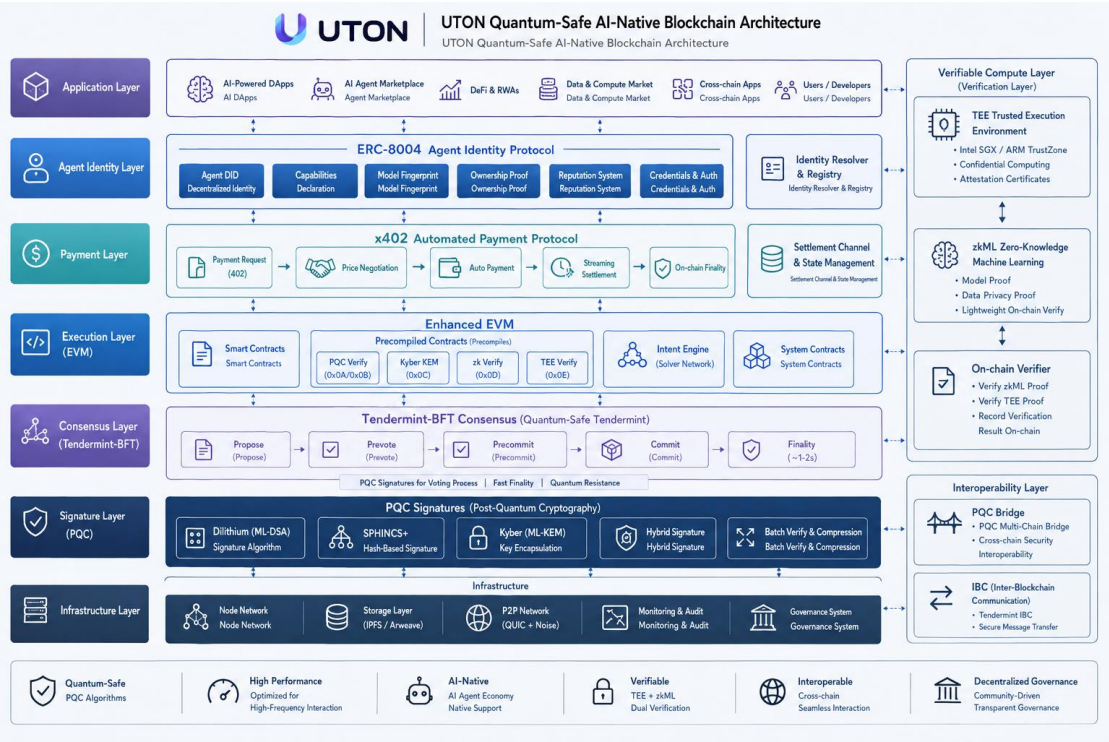
(such as requiring manual private key signing and high single-use gas fees) have become the main bottleneck for AI agents to unleash their productivity. Blockchain must evolve from a simple "distributed ledger" into an operating system that can provide native support for machines, providing trust support for the future AgentIC ecosystem.

2.2 The Threat of Quantum Computing to Cryptographic Civilization

Breakthroughs in quantum computing, exemplified by Shor's algorithm, have placed traditional public blockchains relying on Elliptic Curve Cryptography (ECC) and RSA under imminent threat of being instantly compromised. For future AI-automated contracts, the failure of underlying encryption means the entire autonomous logic will be tampered with. UTON was created precisely to build a digital security firewall sufficient to protect assets shared by humans and machines before the widespread adoption of quantum computing.

3. Core Cryptographic Architecture: Post-Quantum Defense (PQC) at the End of the Chain

To facilitate understanding of the relationships between UTON's core modules, this section provides an overview of the system's overall architecture. UTON employs a layered design, modularly integrating post-quantum cryptography, the execution environment, AI proxy identity, automatic payment mechanisms, and verifiable computing capabilities. This ensures security while enhancing system scalability and composability. The overall architecture is shown in the figure below.



In this architecture, the bottom layer provides security and consistency guarantees through the PQC signature layer and the Tendermint consensus layer; the execution layer implements smart contracts and intent-driven execution based on the extended EVM; above this, the ERC-8004 protocol provides identity and behavior constraint mechanisms for AI agents, and the x402 protocol is responsible for automated payment settlement between machines; the TEE and zkML modules on the right constitute the verifiable computation layer, used to ensure the credibility of off-chain inference results. All layers interact through standardized interfaces, thus forming a complete AI-native blockchain system.

UTON inherits and elevates the cryptographic genes of the UTON network, achieving a comprehensive transformation in the account, network, storage, and consensus layers.

3.1 Hybrid Quantum-Resistant Signature System (ML-DSA and SPHINCS+)

The network fully adopts CRYSTALS-Dilithium (ML-DSA) and SPHINCS+ algorithms as its core signature standards. CRYSTALS-Dilithium, based on

complex lattice-based theory, provides extremely high verification speed while ensuring quantum resistance, making it specifically designed for high-frequency interactions by AI agents. SPHINCS+, on the other hand, is a stateless signature scheme based on hashing. Because it does not rely on any complex mathematical problems, it provides the most conservative and purest long-term security guarantee for the network. Through this combination of multiple cryptographic primitives and an optimized set of verification instructions, UTON ensures that every automated transaction initiated by AI possesses financial-grade security resistance against the brute force of quantum computers, achieving a perfect balance between extreme performance and long-term security.

3.2 Key Encapsulation and Communication Security (ML-KEM)

To prevent "intercept-then-decrypt" attacks in the quantum era, UTON integrates the CRYSTALS-Kyber algorithm into inter-node communication and client handshakes. This ensures the absolute privacy of all network data streams during transmission, providing end-to-end encryption

protection, especially when handling sensitive inference instructions, private data models, and trade secrets between AI agents.

3.3 PQC Performance and Engineering Comparison

In the UTON network, the introduction of post-quantum cryptography is not merely a replacement of the signature algorithm, but a systematic reconstruction involving block structure, execution paths, and cost models. Differences in signature size and verification complexity among different PQC algorithms directly impact block capacity, network propagation efficiency, and overall throughput. Therefore, UTON conducted an engineering comparison of mainstream PQC schemes from the outset and completed the selection based on actual operational constraints.

There are significant differences among current mainstream algorithms in terms of signature and key size:

algorithm	Public key size	Signature size	Typical uses
ECDSA	32B	64B	Traditional public

(secp256k1)			blockchain default signature
CRYSTALS-Dilithium2	~1.3KB	~2.4KB	High-frequency trading signature
SPHINCS+	~32B	8KB–30KB	High security scenarios

Compared to ECDSA, PQC signatures are more than an order of magnitude larger. This directly impacts the number of transactions a block can hold and introduces additional latency during network propagation. To avoid the negative impact of block bloat on consensus efficiency, UTON employs a signature commitment mechanism in its data structure: only the hash digest of the signature is stored on-chain, while the complete signature is propagated and cached through a data availability layer or peer-to-peer network. Furthermore, for large signatures (such as SPHINCS+), the system supports sharded commits based on a Merkle structure, enabling validators to complete consistency

checks without loading the complete data, thereby reducing bandwidth consumption and synchronization pressure.

In terms of performance verification, different algorithms have a significant impact on the system throughput:

algorithm	Single verification time	Verification features
ECDSA	~0.1 ms	Extremely low latency
Dilithium	~0.3–0.8 ms	Stable and parallelizable
SPHINCS+	~5–20 ms	Computationally intensive

UTON uses Dilithium as the default signature path, primarily based on its balance between verification complexity and performance stability. This algorithm exhibits good predictability in high-frequency call scenarios and can significantly reduce unit cost through batch processing. SPHINCS+ serves as a supplementary solution for scenarios with extremely high security requirements but low call frequency, such as

governance, system upgrades, and changes to critical parameters.

In practice, UTON introduces a batch verification mechanism at the block level, merging multiple signatures for processing and thus sharing polynomial operation steps. This method significantly reduces the overhead of redundant computation, lowering the verification cost per signature to 20% to 40% of the original level. Simultaneously, the verification process is executed in a pipelined manner, allowing signature verification to proceed in parallel with transaction sorting, state execution, and other processes, thereby avoiding becoming a performance bottleneck in the consensus path.

Regarding gas costs, the increased computational complexity brought by PQC inevitably increases on-chain verification overhead. UTON significantly reduces gas consumption by migrating the signature verification logic to the pre-compiled contract path, enabling execution based on native code. A cost comparison of different solutions is as

follows:

Operation type	Gas cost (per trip)	After batch optimization
ECDSA verification	~21k	not applicable
Dilithium Validation	~200k–400k	~80k–120k
SPHINCS+ verification	>500k	Depends on the scenario

Building upon this, UTON further reduces calldata costs by compactly encoding and structured packaging the input data, and ensures predictable gas prices under network congestion through a cost cap mechanism. Overall, UTON keeps PQC verification costs several times higher than traditional ECDSA, enabling it to achieve quantum security while still meeting the economic feasibility requirements for practical applications.

3.4 PQC and EVM Integration

UTON extends the EVM at the execution layer, making post-quantum cryptography a native on-chain capability. This integration is not achieved by modifying existing contract semantics, but rather by adding a pre-compiled contract interface, allowing developers to directly call PQC-related functions while maintaining Solidity and EVM compatibility.

UTON defines a set of dedicated pre-compiled addresses for performing signature verification and key encapsulation operations:

pre-compiled address	Function Description
0x0A	CRYSTALS-Dilithium Signature Verification
0x0B	SPHINCS+ signature verification
0x0C	CRYSTALS-Kyber Key Encapsulation (KEM)

When a smart contract calls the aforementioned interface, the request is forwarded to the node's local native execution environment, where an

optimized cryptographic library performs the computation. This execution path avoids the performance overhead of EVM instruction-by-instruction interpretation while ensuring the determinism and reproducibility of the execution result. At the call level, the contract only needs to pass in the necessary parameters such as the signature, public key, and message digest to obtain the verification result, thus maintaining consistency with traditional signature verification in terms of development experience.

In its underlying implementation, UTON has specifically optimized for the computational characteristics of the PQC algorithm. Since this type of algorithm heavily relies on polynomial operations and vector processing, the system utilizes the SIMD instruction set of modern CPUs to accelerate the critical path and implements parallel verification through a multi-threaded scheduling mechanism, thereby maintaining stable throughput under high load. Simultaneously, by constructing a memory reuse mechanism, the performance overhead caused by frequent allocation of large-scale arrays is avoided, further reducing execution latency.

In terms of state management, UTON avoids directly writing large amounts of PQC data into the state tree. Both public keys and signature data are stored indirectly using hash references and are only loaded on demand during verification, effectively controlling the growth of the state size. This design significantly reduces node storage pressure and improves synchronization efficiency over long-term operation.

Furthermore, to support gradual upgrades and cross-chain compatibility, UTON introduces a hybrid signature mode at the execution layer, allowing the same transaction to contain both ECDSA and PQC signatures. In this mode, the system can select the verification path based on the context, thus maintaining security while remaining compatible with the existing ecosystem. This mechanism provides a smooth transition path for post-quantum migration, avoiding the systemic risks associated with a one-time switch.

4. Identity and Adaptation Layer: Native Machine Identity Standards

UTON gives AI an independent, verifiable digital identity.

4.1 ERC -8004 Agent Identity Agreement

In the UTON network, AI Agents are no longer merely invoking off-chain services, but are modeled as on-chain entities with independent identities, verifiable behaviors, and economic responsibilities. To achieve this, UTON proposes the ERC-8004 Agent Identity Protocol, which uniformly describes the Agent's identity structure, capability boundaries, and on-chain behavioral constraint mechanisms.

The core of ERC-8004 lies in the structured encapsulation of identity information, model state, and economic attributes, enabling it to be invoked by smart contracts and verified and tracked by the network. Its basic data structure is as follows:

Fields	type	describe

owner	address	Agent's owner (human or institutional)
modelHash	bytes32	Model version fingerprint (hash)
capabilityURI	string	Capability Description and Interface Specification
reputationScore	uint256	Dynamic Reputation Score
stake	uint256	pledged amount

This structure gives the Agent a clear identity boundary on the chain and allows its execution logic to be constrained through modelHash. Any model update will result in a fingerprint change, thus avoiding the risk of "model replacement attacks," which involve changing the execution logic without altering the agent's identity.

In terms of identity lifecycle management, ERC-8004 defines the complete process from registration to logout, making agent state transitions verifiable:

Register → Activate → Operate → Update → Freeze/Slash → Exit

During operation, agents can directly initiate transactions or invoke smart contracts using their identities. Their actions are continuously recorded by the on-chain system and participate in the dynamic updating of reputation scores. The reputation system is calculated based on multi-dimensional indicators, including task completion rate, response time, historical default records, and user feedback. Its typical calculation model is as follows:

$$Score = w1 \cdot SuccessRate + w2 \cdot Latency + w3 \cdot TrustScore$$

The weighting parameters can be dynamically adjusted by the governance mechanism to adapt to different application scenarios. Reputation score will directly affect the visibility and callability of the agent in the market, and can serve as an important basis for task scheduling and resource allocation.

To ensure that agent behavior is economically constrained, ERC-8004

introduces a staking and penalty mechanism. Upon activation, an agent must lock a certain amount of UTN tokens as collateral. When its behavior is deemed malicious or in breach of contract, the system will impose partial or full slashing based on the severity of the violation. This mechanism ensures that agent behavior no longer relies solely on technical constraints but forms a closed loop through economic incentives, thereby enhancing the overall credibility of the system.

At the execution level, ERC-8004 is deeply integrated with EVM. An Agent identity is essentially a programmable account, capable of participating in on-chain interactions as either the initiator or initiator of transactions. Simultaneously, the protocol supports identity delegation and permission allocation, enabling collaborative relationships among multiple Agents. For example, a scheduling Agent can assign tasks to an execution Agent, thereby constructing a more complex Agent network structure.

Through the above design, ERC-8004 not only provides identity identification capabilities, but also builds a complete system covering identity verification, behavior recording and economic constraints, enabling AI Agents to participate in the UTON ecosystem as "on-chain economic entities".

4.2 On-chain Reputation and Default Tracking System

The system automatically records the on-chain behavior of AI agents (such as task completion rate and whether there are malicious call records) and converts it into a dynamic reputation score that is updated in real time. This not only provides a quantitative standard for human users to choose high-quality AI services, but also establishes a transparent credit benchmark for autonomous collaboration among AI agents.

5. Machine Economy Engine: Refactoring the Execution Layer and Network Overhead

To support the potential for trillions of microtransactions between

machines in the future, UTON has conducted in-depth performance tuning of the underlying EVM.

5.1 x402 Automatic Payment Protocol

To support the high-frequency, low-latency value exchange needs between AI Agents, UTON introduces the x402 automatic payment protocol, which extends the traditional HTTP 402 semantics to make it a machine payment protocol suitable for on-chain environments. This protocol aims to achieve an automated settlement mechanism without human intervention, enabling payment transactions to be embedded into the task execution process.

In the x402 protocol, payment is no longer a standalone operation but is tightly coupled with the service request process. When an agent requests a service, the service provider returns a payment request containing price information. The caller, after verification, automatically completes the signature and payment authorization, thereby triggering subsequent execution. The overall process is as follows:

Request → Payment Quote → Authorization → Execution → Settlement

To support transaction scenarios of varying complexity, x402 defines a unified payment request structure:

Fields	type	describe
payer	address	Payer
payee	address	Recipient
amount	uint256	Payment amount
rate	uint256	Flow payment rate
duration	uint256	Duration
signature	bytes	Payment Authorization Signature

During execution, the protocol employs a state machine model to manage the payment lifecycle:

Init → Requested → Locked → Streaming → Settled → Closed

The "Streaming" status indicates that payments occur continuously over

time or according to a schedule, rather than being completed all at once. This mechanism is particularly suitable for scenarios such as AI inference calls, data service subscriptions, and computing power leasing, enabling costs to be dynamically matched with resource consumption.

At the implementation level, x402 employs a multi-layered structure combining off-chain and on-chain mechanisms. High-frequency interactions are completed through off-chain session channels to reduce gas costs and latency, while final settlements are periodically submitted to the blockchain to ensure state consistency and traceability. During this process, state channels are used to record payment progress, and in case of disputes, the process can be rolled back to the blockchain for arbitration, thus avoiding single points of trust issues.

To ensure protocol security, x402 incorporates various potential attack scenarios in its design, including payment delays, payment rejections, and spoofing requests. The system employs mechanisms such as locking

funds, setting timeouts, and introducing on-chain arbitration to prevent any single party from unilaterally profiting. Furthermore, payment authorization must be verified through signatures to ensure that all payment transactions have a verifiable source.

In terms of collaboration with the execution layer, x402 and EVM form a two-way triggering relationship. On the one hand, payment can serve as a prerequisite for contract execution; on the other hand, the contract can also trigger subsequent payments based on the execution result, thus forming an "execution-settlement" closed loop. This mechanism enables UTON to support complex automated economic processes and gives the interaction between AI Agents native economic attributes.

5.2 Intent-centric Interaction Paradigm

The AI agent doesn't need to input complex instructions for each step; it simply broadcasts its "execution intent" (e.g., to complete cross-chain clearing via the optimal path) to UTON . The underlying Solver node

network automatically finds and executes the optimal path in the complex quantum-resistant contract environment, significantly improving the AI's decision-making efficiency when handling complex financial tasks.

6. Verifiable Intelligence: Deep Integration of TEE and zkML

To ensure that the decision results generated by the AI agent in the invisible "black box" environment are authentic and compliant, UTON provides a verification solution that combines hardware and software.

6.1 TEE (Trusted Execution Environment) Isolation Verification

UTON nodes natively support TEE hardware extensions (such as Intel SGX/ARM TrustZone), allowing AI to process sensitive data and perform model inference in an isolated environment, ensuring that input information is not leaked to the node itself, while generating computation execution proofs.

6.2 ZKML (Zero-Knowledge Machine Learning) Algorithm Rights Determination

After the AI agent completes inference off-chain, it can use UTON's built-in zkML toolkit to generate a tiny zero-knowledge proof and submit it on-chain. Verifying nodes do not need to rerun the massive neural network; they only need to verify the proof within milliseconds to confirm that the AI's output fully follows the predetermined logic, thus completely resolving the trust crisis of "intelligent evil."

6.3 Verifiable Computation Architecture (TEE + zkML)

While supporting AI agents to participate in the on-chain economy, UTON must solve a core problem: how to verify the credibility of the inference results executed by AI off-chain. To this end, UTON has built a verifiable computing architecture based on TEE and zkML, enabling the AI execution process to have both privacy protection capabilities and be verifiable on-chain.

In this architecture, AI inference is primarily executed off-chain to avoid performance bottlenecks caused by running complex models directly in the blockchain environment. Its basic execution flow is as follows:

Input → TEE Execution → Output → zkML Proof → On-chain Verification

The Trusted Execution Environment (TEE) provides an isolated computational space, protecting the model inference process at the hardware level. Through Remote Attestation, the TEE can prove to the outside world that its runtime environment has not been tampered with, thus ensuring the trustworthiness of the execution process. Furthermore, input data and model parameters can be executed in the TEE under encrypted conditions, preventing nodes or external observers from obtaining sensitive information.

However, TEE itself relies on hardware trust assumptions, so UTON further introduces the zkML mechanism to mathematically verify the inference

results. zkML generates zero-knowledge proofs by transforming the neural network computation process into a verifiable circuit, allowing verification nodes to confirm the correctness of the output without re-executing the model. The roles of different technical approaches in the system are as follows:

Technical components	Main function
TEE	Provide privacy protection and efficient execution
zkML	Provide mathematical proof of the correctness of the calculation
On-chain Verifier	Verify, prove, and record the results.

In terms of performance, zkML faces the problem of high computational complexity, especially when dealing with large-scale models, where proof generation time can become a bottleneck. UTON reduces this overhead in several ways, including model quantization (reducing precision to reduce circuit size), circuit compression (reducing the number of constraints), and recursive proof (aggregating multiple proofs into a

single proof), thereby keeping the verification cost within an acceptable range.

In terms of trust model, UTON employs a multi-layered mechanism: TEE provides execution trustworthiness, zkML provides result correctness, and on-chain staking and penalty mechanisms provide economic constraints. The combination of these three elements makes the system more robust against potential attacks. For example, even if the TEE environment is partially compromised, zkML can still serve as an independent verification method, while the economic penalty mechanism further increases the cost of attacks.

Through this architecture, UTON achieves a verifiable encapsulation of the AI inference process, enabling on-chain systems to introduce complex intelligent computing capabilities without sacrificing performance, thereby providing infrastructure support for the trusted operation of AI agents.

7. Token Economics and GAS Mechanism

The native token of the UTON network is UTN, which serves as the value carrier, payment medium, and security guarantee asset for the entire ecosystem. UTN is designed to incentivize cybersecurity, AI Agent activity, and ecosystem growth in the long term, while maintaining economic sustainability.

7.1 Basic Token Information

- **Token symbol** : UTN
- **Total supply** : **100,000,000**
- **Initial circulating supply** : Approximately 20%–25%
- **Decimal places** : 18

7.2 Token Allocation and Release Plan

category	Proportion	Quantity (UTN)	Release mechanism

Ecosystem and AI Developer Fund	35%	35,000,000	The funds will be released linearly over 3 years to incentivize AI Agent development, x402 payment subsidies, quantum security audits, and ecosystem grants.
Team and Consultants	20%	20,000,000	2-year Cliff (1-year lock-up) + 2-year linear release
Private Equity/Strategic Round	15%	15,000,000	6–12 months Cliff + 18–24 months linear release
Liquidity and Exchanges	10%	10,000,000	TGE will be gradually injected into DEX/CEX liquidity pools.
Community and Airdrop	10%	10,000,000	Gradual airdrops + early user rewards + AI agent reputation incentives

Quantum Security and Insurance Fund (QAF)	5%	5,000,000	Governance controls are primarily used for PQC auditing, bug bounties, and security pools.
Validator and Node Incentives	5%	5,000,000	Used for early network launch rewards, subsequently taken over by Gas + inflation rewards.

All team and private placement portions are managed using smart contracts with multi-signature and time locks , and are subject to community governance oversight. Any over-allocation or early release requires approval via on-chain proposal.

7.3 Inflation and Staking Model (Dynamic Equilibrium)

UTON employs **a Cosmos SDK-style dynamic inflation model** to ensure network security.

- **Target collateral ratio** : 65%–75%

● **Based annualized inflation rate** : Initially 8%–12%, dynamically adjusted based on the actual collateral ratio (the higher the collateral ratio, the lower the inflation rate).

● **Maximum inflation cap** : 15% (to prevent excessive dilution)

● **Minimum inflation floor** : 3% (to ensure long-term security incentives)

Staking rewards are distributed between validators and delegators according to their staking ratio. Malicious behavior (double-signature, prolonged offline time) will be subject to **5%–100% slashing** (ERC-8004 staking penalty specifically for malicious AI agents).

Deflationary pressure:

● 10 **%–30 % of** all gas fees are directly burned.

● **10%–20%** of the AI service fee (x402 protocol settlement) goes into a burning or buyback mechanism.

● The governance process can be decided by voting on additional destruction or the use of the ecological fund.

In the long run, as AI Agents interact more frequently, the amount of fuel burned is expected to exceed new inflation, resulting in net deflation.

7.4 UTN Core Utility

● **Gas payments** : Transaction execution, smart contracts, PQC verification, AI identity registration, etc.

● **Staking and Cybersecurity** : Become a validator or delegate, earn rewards, and participate in consensus.

● **AI Agent Economy** :

a. ERC-8004 Agent Activation and Collateral Guarantee

b. x402 Settlement base currency for automatic payments and stream payments

c. Payment AI inference, data services, computing power leasing, etc.

● **Governance** : Proposal voting, parameter adjustments (Gas price curve, PQC pre-compilation fees, fund usage, etc.) ● **Value capture** : Network fees, cross-chain bridge fees, and partial return of AI ecosystem revenue to UTN holders.

7.5 Detailed Explanation of the GAS Mechanism

UTON has made targeted optimizations to the EVM, **especially reducing the cost of high-frequency micro-interactions of the AI Agent** .

Gas pricing formula (basic model):

Total Gas Fee = (BaseGas + ComputeGas + StorageGas + PQCFactor) × GasPrice

- **PQCFactor** : Post-quantum operation multiplier (such as Dilithium verification), default 2.5–4.0 (can be reduced to 1.5–2.5 after batch verification)
- **AI-specific optimizations** : The x402 streaming payment and intent solver employs **batch pre-verification + state channels** , keeping gas consumption per micro-interaction within **1.5–3 times that of traditional ECDSA.**
- **Target cost** : Regular transfer < $0.001; AI Agent micro-interaction < $0.0001 (under high TPS + batch optimization)

Gas fee allocation (per transaction):

● 60 % –80 % → Validators/Block Producers

● 1 0%– 3 0% → **Combustion** (Deflation)

● 10% → National Treasury/Ecological Fund (adjustable for governance)

Dynamic Gas Pricing : Employs an EIP-1559-like mechanism (Base Fee + Priority Fee). The Base Fee is automatically adjusted based on network load to ensure predictable costs. During network congestion, priority is given to AI-critical transactions.

8. Team Introduction: The Core Driving Force of Interdisciplinary Collaboration

UTON 's core builders consist of experts from top global institutions, combining cutting-edge expertise in quantum computing, artificial intelligence, and distributed ledger technology.

8.1 Core Technology Committee

Team members have led the development of the underlying architecture for mainstream Layer 1 public blockchains. In quantum cryptography, core members were deeply involved in the global standard testing and implementation of the NIST PQC algorithm; in the field of AI, the team

has extensive experience in distributed model training and agent communication protocol development.

8.2 Quantum Safety Laboratory (QS Lab)

Led by senior cryptographers, the lab focuses on the engineering implementation of the PQC algorithm in a blockchain environment. It holds numerous core patents in areas such as signature size compression and low-latency optimization of the PQ handshake protocol, ensuring UTON 's absolute leading position in security technology.

8.3 AI and Automation Research Group

This group is dedicated to standardization within the AgentIC ecosystem. Through technical collaboration with top AI labs worldwide, the team continuously translates cutting-edge machine economy needs into robust underlying network protocols for UTON .

9. Roadmap

● Phase 1: Intelligent Network Evolution and Native AI Upgrade (Q2-Q3 2026):

Complete the deep reconstruction of the underlying protocol to AI natively, fully embed machine sovereignty recognition logic and a value transfer framework with extremely low friction, and realize the deep architectural migration from "human-driven" to "algorithm-autonomous".

● Phase Two: AI Ecosystem Explosion and Global Node Alliance (Q4 2026):

We will establish a billion-level AI ecosystem special fund and a validator node incentive matrix, and unite with leading global AI laboratories and capital to jointly build a decentralized alliance to comprehensively promote the value capture of the machine economy network.

● Phase Three: Global Safety Certification and Industry Standard Leadership (Q1-Q2 2027):

We will promote and obtain post-quantum security implementation certification from international authoritative standards organizations, and work with top academic and financial institutions to formulate

underlying security and cross-chain collaboration standards for "quantum + AI", thereby establishing UTON 's industry leadership position.

● Phase Four: A Global Homestar Network for the Quantum Age (2027 and beyond):

Establish a global governance architecture for "human-machine collaboration" that transcends sovereign boundaries and a cross-chain trust hub, promote the popularization of institutional-level quantum-resistant compliance solutions, and build UTON into the ultimate digital mother planet of a trillion-level AI civilization.

UTON represents a major evolution in blockchain infrastructure in response to the future computing revolution. It not only secures absolute security in the quantum era, but also unleashes the infinite productivity of the machine economy through native adaptation to AI agents, creating a true "digital mother planet" for trillions of AI agents.