RoboChain (ROBO) — Decentralized Robotic Technology Ecosystem Innovation

Abstract

The rapid iteration of robotic technology (covering service robots and industrial robots) is reshaping the global pattern of production and living services, evolving from single-device automation to full-domain intelligence featuring collaboration among "devices-data-computing power-scenarios". It is expected to completely solve the three core challenges of production efficiency, service quality, and resource optimization. However, large-scale industrial implementation still faces bottlenecks such as data silos, uneven computing power distribution, inefficient cross-entity collaboration, and insufficient security and compliance. As a decentralized cryptocurrency empowering the global robotic technology ecosystem, RoboChain (ROBO) leverages the distributed trust, smart contract automation, and data traceability characteristics of blockchain technology, combined with core technologies such as computer vision and multi-device collaboration, to build a trinity ecological system of "technological collaboration-value circulation-compliance guarantee". It breaks down centralized barriers, allowing participants including robot enterprises, research institutions, computing power service providers, and end-users to share the dividends of industrial upgrading. This white paper elaborates on ROBO's technical architecture, economic model, application scenarios, and development roadmap, aiming to accelerate the commercialization of robotic technology and drive the robotics industry into a new era of decentralized collaboration.

1. Project Background and Vision

1.1 Opportunities and Bottlenecks in the Robotics Industry

Currently, robotic technology is steadily evolving from basic automation to advanced intelligent autonomy. Global leading robot enterprises and technology companies are actively deploying core areas such as computer vision, AI algorithms, and multi-device collaboration. According to industry data, the global robotics market size exceeded 600 billion US dollars in 2025, with the infrastructure construction of industrial and service robots growing at an average annual rate of over 25%. It is expected that intelligent autonomous robots will achieve large-scale commercial application in scenarios such as manufacturing, healthcare, logistics, and home services by 2030. The wide application of robotic technology can not only improve industrial production efficiency by more than 40%, but also reduce labor costs by 35% and resource waste by 20%, demonstrating enormous social and commercial value.

Despite the rapid industry development, large-scale implementation still faces four core bottlenecks: First, the difficulty in releasing data value. Data required for robot operation, such as environmental perception, operation execution, and fault feedback, is scattered among enterprises, equipment operators, and users, forming data silos. Additionally, issues such as data privacy leakage and ambiguous copyright ownership are prominent, lacking a secure circulation mechanism. Second, the imbalance in computing power resource allocation. Advanced robot model training and real-time decision-making require massive computing power, which is unaffordable for small and medium-sized R&D teams, while global idle computing power resources have not been effectively integrated. Third, inefficient cross-entity collaboration. There is a lack of a unified trust and value distribution system among robot enterprises, component suppliers, scenario operators, and users, leading to cumbersome processes in collaborative R&D and service settlement. Fourth, prominent security and compliance risks. Robot operational errors may cause production accidents or service disputes, and there is a lack of unified global technical standards and regulatory frameworks, making liability definition difficult. The decentralized nature of blockchain technology provides an optimal solution to these bottlenecks, and ROBO serves as the core carrier connecting robotic technology and the decentralized ecosystem.

1.2 Core Vision of ROBO

With the core vision of "empowering robotic collaborative innovation and building a decentralized intelligent robotics ecosystem", ROBO relies on the robotic technology route and blockchain trust infrastructure to achieve three core goals:

- Build the world's first robotic technology value circulation network, enabling secure, efficient collaboration and fair distribution of multi-source data, computing power resources, technological achievements, and robot services;
- Incentivize all ecological participants through a crypto-economic model, lower the threshold for robotic technology R&D and application, and accelerate the transformation process from technological breakthrough to scenario implementation;
- Construct a "safe, controllable, compliant, and transparent" ecological system, solve the problems of robot safety risks and liability definition through dual guarantees of technology and mechanisms, and promote the standardized development of the industry.

2. Core Technical Architecture

ROBO adopts a three-layer architecture of "blockchain underlying layer + robot adaptation layer + industry application layer", deeply integrating the characteristics of robotic technology (high real-time performance, multi-device heterogeneity, high data sensitivity) with the advantages of blockchain (distributed trust, traceability, immutability). Through cross-layer technical collaboration and modular design, it creates a decentralized robotics ecosystem with high security, high compatibility, high scalability, and high real-time performance, realizing seamless collaboration across the entire chain of "devices-data-computing power-scenarios". The following is a detailed technical breakdown of each layer:

2.1 Blockchain Underlying Layer: An Efficient and Secure Ecological Foundation

The blockchain underlying layer is the trust and technical cornerstone of the ROBO ecosystem. It is developed based on in-depth customization of the Polygon PoS mainnet. To meet the needs of high-frequency data interaction, low-latency response, and high privacy protection in robotic scenarios, it constructs a hybrid architecture of "main chain-side chain-distributed storage". The core technical modules are as follows:

2.1.1 Consensus and Network Optimization Module

- Consensus Mechanism Upgrade: Adopts a hybrid consensus of PoS (Proof of Stake) + BFT (Byzantine Fault Tolerance). On the basis of Polygon's native PoS, it optimizes the verification node election mechanism — nodes holding and staking ROBO in the ecosystem can participate in verification. The number of verification nodes is dynamically maintained at 100-200, and selected through a two-dimensional screening of "staking amount weight + node credit score" to ensure consensus security. The introduction of the BFT mechanism enables the consensus fault tolerance rate to reach 1/3, ensuring network stability under extreme conditions.
- Sharding and Side Chain Expansion: Adopts dynamic sharding technology to automatically divide shard chains by "scenario dimension" (industrial, medical, logistics, etc.). Each shard independently processes transactions and data storage corresponding to the scenario, and realizes asset and data intercommunication between shards through the Inter-Shard Communication Protocol (ICP). At the same time, three functional side chains are deployed: Data Transaction Side Chain (processing high-concurrency data authorization transactions), Computing Power Settlement Side Chain (optimizing the efficiency of computing power rental payments), and Robot Control Side Chain (ensuring real-time operation command on-chain). The main chain is only responsible for asset liquidation and ecological governance across shards/side chains, achieving a performance balance of "stable main chain and fast side chains".
- Network Performance Indicators: Block confirmation speed is 1.5 seconds per block, TPS per shard reaches 2500+, cross-shard transaction latency ≤ 3 seconds, and the entire network supports more than 1 million online devices simultaneously. It meets the scenario requirements of industrial robot cluster collaboration and high-frequency interaction of service robots. Through the node dynamic load balancing algorithm, single shard congestion is avoided, and network scalability supports linear expansion (the number of shards can be increased to 20 as needed).

2.1.2 Data Security and Privacy Protection Module

- In-depth Application of Zero-Knowledge Proofs (ZK-SNARKs): Adopts the ZK-SNARKs protocol optimized by the Groth16 algorithm, and designs a dedicated proof circuit for robot sensitive data (such as industrial production process parameters and medical service privacy data). Data owners can generate "data validity proofs", and third parties can verify the authenticity and compliance of data without obtaining the original data. The proof generation time is ≤ 500ms, and the verification time is ≤ 10ms, balancing privacy and efficiency.

- Federated Learning (FL) Collaboration Framework: Builds a decentralized federated learning platform, adopting a hybrid model of "horizontal federation + vertical federation": Horizontal federation supports homogeneous robots (such as industrial robotic arms in different factories) to share model parameters, and vertical federation supports joint training across entities (such as robot enterprises + computing power service providers). Model parameters are transmitted through encrypted channels (AES-256-GCM), and only model update summaries and contribution certificates are stored on-chain, ensuring no data leakage during training. Differential privacy technology ($\varepsilon=1.5$) is introduced to further prevent the leakage of original data through model reverse inference.

- Distributed Storage Solution: Integrates IPFS (InterPlanetary File System) as the off-chain data storage layer. The blockchain main chain only stores core metadata such as data hashes, copyright information, and transaction credentials. Original data (such as high-definition robot operation videos and large-capacity sensor data) is encrypted and stored in IPFS nodes. It adopts "data sharding storage + multi-replica backup" (3 replicas by default), combined with the hash verification mechanism of blockchain, to ensure data immutability and permanent traceability. It supports data lifecycle management (automatically adjusting IPFS node storage strategies according to storage duration) to reduce long-term storage costs.

2.1.3 Smart Contract and Security Audit Module

- Smart Contract System: Supports dual-language development of Solidity and Vyper, and provides a dedicated contract template library for robotic scenarios (including 12 types of prefabricated templates such as data authorization contracts, computing power rental contracts, robot collaboration contracts, and patent transaction contracts). Developers can quickly deploy contracts through simple configuration. Contracts support an upgradeable mechanism (Proxy Pattern), allowing vulnerabilities to be fixed or functions to be optimized without interrupting services. The upgrade process requires approval through DAO governance voting.

- Security Audit Mechanism: Embeds automated audit tools (integrating Slither static analysis and Mythril dynamic detection) to perform real-time vulnerability scanning (covering more than 20 types of security risks such as reentrancy attacks, integer overflows, and permission control flaws) on deployed contracts. Introduces third-party security audit nodes, which need to stake 1 million ROBO to conduct manual reviews of high-value contracts (such as patent transaction contracts), and the audit results are traceable on-chain. Establishes a vulnerability response mechanism. White-hat hackers can submit discovered vulnerabilities through the bug bounty program and receive ROBO rewards after verification (reward amounts are divided by vulnerability severity: Critical level 50,000-100,000 tokens, High level 10,000-50,000 tokens).

2.2 Robot Adaptation Layer: The Core Hub of Technology Integration

The adaptation layer is the "translator" and "dispatching center" of the ROBO ecosystem. It is responsible for breaking down the technical barriers between the blockchain network and robot terminals, realizing heterogeneous device compatibility, multi-source data standardization, and on-demand computing power scheduling. The core technical modules are as follows:

2.2.1 Multi-Source Data Standardization Module

- Data Access Protocol Adaptation: Supports mainstream robot data transmission protocols, including Modbus, Profinet, EtherNet/IP for industrial scenarios, MQTT, CoAP, WebSocket for service robots, and DICOM, HL7 for medical robots. Develops a protocol conversion gateway (integrated hardware + software), allowing traditional robots to access the ecosystem through the gateway without modifying the original hardware. The gateway supports edge computing preprocessing (data cleaning, format conversion) to reduce cloud transmission pressure.
- Data Encryption and Structured Processing: Adopts a dual mechanism of "transmission encryption + storage encryption". The transmission process is encrypted through TLS 1.3, and the storage process selects adaptive algorithms for different data types (AES-256 for structured data, simplified homomorphic encryption for unstructured data). Data structuring adopts Protocol Buffers (Protobuf) format, defining unified data field specifications (such as sensor data including 16 core fields such as device ID, timestamp, coordinate information, value, and precision level), supporting a data compression ratio of 1:5 to improve transmission and storage efficiency.
- Data Copyright and Traceability Mechanism: When data is uploaded to the chain, a unique copyright identifier (hybrid signature based on device ID + timestamp + data hash) is automatically generated, and copyright ownership information is written into the blockchain for immutability. The full lifecycle records of data (collection-preprocessing-on-chain-authorization-usage-destruction) are uploaded to the chain in real time, supporting quick traceability by device ID, time range, and data type. A data usage log chain is introduced. When third parties use data, they need to record the purpose, duration, and processing results of the use. The log chain is associated with the main chain to ensure that data is not abused.

2.2.2 Computing Power Collaboration and Scheduling Module

- Construction of Computing Power Resource Pool: Integrates three types of computing power resources: personal idle computing power (GPU/CPU, supporting NVIDIA CUDA and AMD ROCm architectures), professional computing power clusters (data center-level GPU clusters, supporting TensorFlow and PyTorch frameworks), and cloud service provider computing power (API docking with AWS, Alibaba Cloud, etc.). All computing power nodes need to pass a computing power benchmark test (based on MLPerf benchmarks) when accessing, generating a computing power level score (from 1 to 10), which serves as the basis for pricing and task allocation.
- Intelligent Scheduling Algorithm: Adopts a scheduling logic of "demand matching + dynamic optimization", training a scheduling model based on reinforcement learning. Input parameters include task type (model training/real-time inference), computing power requirements (computing power level, duration, latency requirements), price budget, and node credit score. The scheduling model can achieve three optimizations: task splitting (splitting large-scale training tasks into subtasks for parallel processing), node selection (prioritizing matching high-credit-score + low-latency nodes), and load balancing (avoiding excessive computing power load on a single node). Scheduling latency ≤ 100ms, task matching success rate ≥ 98%.
- Computing Power Verification and Fault Tolerance Mechanism: Adopts dual verification of "proof of work + result verification": After completing a task, a computing power node needs to submit a work certificate (such as the hash of intermediate parameters for training tasks), and the main node randomly selects 10% of the subtasks for result review. Introduces a fault tolerance mechanism. If a node fails to complete the task on time or the result is incorrect, part of the staked ROBO will be deducted, and a backup node will be activated to take over (backup nodes are pre-allocated in advance, and handover latency ≤ 2 seconds). Establishes a node credit score system, where the credit score is linked to computing power contribution, task completion quality, and response speed. Nodes with a credit score ≥ 80 can receive an additional 10% ROBO reward.

2.2.3 Multi-Device Collaboration Adaptation Module

- Device Access and Identity Authentication: Adopts a Decentralized Identity (DID) system. Each robot device generates a unique DID identifier, associated with metadata such as device model, manufacturer, compliance certification information, and security level. When a device accesses the ecosystem, it is authenticated through "DID + digital signature". After successful authentication, a temporary communication key is assigned, which is automatically rotated every 24 hours. Supports hierarchical device permissions (administrator permissions, operation permissions, data reading permissions). Permission changes need to be recorded through smart contracts to ensure access security.
- Multi-Robot Collaboration Protocol: Develops the RoboSync collaboration protocol, supporting three types of collaboration modes: task allocation collaboration (such as path planning collaboration of logistics robot clusters), data sharing collaboration (such as process parameter sharing of industrial robots), and fault mutual assistance collaboration (such as backup device handover when a robot fails). The protocol adopts the Raft consensus algorithm to ensure the consistency of multi-device command synchronization

(synchronization error ≤ 50ms). Supports cross-scenario collaboration (such as the docking of industrial robots in factories with delivery robots in logistics parks), realizing data intercommunication through standardized interfaces.

- Real-Time Control and Emergency Response: For scenarios with high real-time requirements such as industrial robots and medical robots, edge computing nodes are deployed (deployed close to devices, latency ≤ 10ms). Core control commands (such as robotic arm operations and emergency shutdowns) are processed locally by edge nodes and then asynchronously uploaded to the chain, balancing real-time performance and traceability. The emergency response module supports preset emergency rules (such as equipment failures, data anomalies, and security risks). When a rule is triggered, emergency operations are automatically executed (such as shutdown, switching to backup devices, and sending early warnings to administrators). Emergency operation logs are uploaded to the chain in real time to facilitate subsequent traceability.

2.3 Industry Application Layer: The Landing Carrier of Ecological Value

The application layer is the value realization terminal of the ROBO ecosystem. Based on the technical support of the underlying blockchain and adaptation layer, it provides integrated "technology + token + service" solutions for different industry scenarios. The core technical support and scenario landing details are as follows:

2.3.1 Technical Support for Data Transaction and Sharing Scenarios

- Data Transaction Smart Contracts: Supports three modes: "fixed-price transaction", "auction transaction", and "subscription-based transaction". The contract has built-in automatic settlement logic (ROBO is transferred to data providers in real time after the transaction is completed, and the platform charges a 3% handling fee);
- Data Authorization Management: Supports fine-grained authorization (authorization by time range, number of uses, and user). Access rights are automatically revoked after the authorization expires, enforced through smart contracts without manual intervention;
- Data Value Evaluation: Embeds a data value evaluation model that scores based on 6 dimensions including data type, accuracy, completeness, scarcity, and application scenario, generating a reference price to assist data providers in pricing.

2.3.2 Technical Support for Decentralized Computing Power Service Scenarios

- Computing Power Rental Contracts: Supports three rental modes: by hour, by task, and by computing power unit. The contract automatically records the duration and consumption of computing power usage for real-time settlement;

- Model Training Collaboration: Provides a distributed training framework that supports parallel training of multiple nodes. Model parameters are synchronized through encrypted channels. After training is completed, the model ownership belongs to the initiator, and the parameter summary is stored on-chain as evidence;
- Real-Time Inference Services: Pre-trained models are deployed on edge computing nodes. Robot terminals can quickly call inference services through APIs, with inference latency ≤ 50ms, supporting batch request processing (≤ 1000 requests per second).

2.3.3 Technical Support for Multi-Robot Collaboration Service Scenarios

- Task Scheduling Smart Contracts: Defines task allocation rules, profit distribution ratios, and liability division standards, supporting dynamic adjustment of task parameters (such as changes in production task priorities);
- Collaborative Control Center: Provides a visual collaborative control interface that supports real-time monitoring of the operating status of multiple robots (position, power, task progress, fault information) and manual intervention and adjustment;
- Fault Diagnosis and Repair: Integrates an AI fault diagnosis model that automatically identifies fault types by analyzing robot operation data (accuracy rate ≥ 92) and recommends repair solutions. In case of severe faults, it automatically dispatches backup devices.

2.3.4 Technical Support for Technology R&D and Commercialization Scenarios

- R&D Crowdfunding Contracts: Supports phased crowdfunding (seed round, R&D round, landing round). Fund unlocking at each phase requires reaching preset milestones (such as completion of technical prototypes, approval of patent applications), reviewed by DAO governance nodes;
- Patent On-Chain and Authorization: Hashes of patent information (specification abstracts, claims, legal status) are uploaded to the chain. The authorization process is automatically executed through smart contracts, and authorization fees are settled in real time without intermediaries;
- Robot Rental Contracts: Supports short-term rental, long-term rental, and per-use rental. The contract has a built-in equipment wear evaluation mechanism. After the rental period expires, the deposit refund ratio is automatically adjusted according to the wear condition.

2.4 Cross-Layer Technical Support System

2.4.1 Identity Authentication and Access Management

- Builds a global identity system based on the W3C DID standard, covering ecological participants (enterprises, developers, users, devices, nodes). Each participant corresponds to a unique DID, associated with digital certificates and credit scores;
- Adopts an Attribute-Based Access Control (ABAC) model. Permissions are linked to participant attributes (such as token holdings, credit scores, compliance certification status), supporting dynamic permission adjustments. Adjustment records are traceable on-chain;
- Multi-Factor Authentication (MFA): Critical operations (such as large-value ROBO transfers, contract upgrades, and device permission changes) require triple verification of "password + hardware key + biometrics" to enhance account security.

2.4.2 Cross-Chain Interaction Module

- Supports cross-chain interaction with mainstream public chains (Ethereum, BSC, Polygon mainnet). Adopts cross-chain bridge technology (based on HashTimeLock contracts) to realize cross-chain transfer of ROBO tokens, with cross-chain latency ≤ 15 minutes and handling fee ≤ 0.1%;
- Supports cross-chain data intercommunication. Through the Cross-Chain Interoperability Protocol (CCIP), robot-related data on other public chains (such as patent information and device certification information) is synchronized to the ROBO ecosystem to ensure data consistency.

2.4.3 Monitoring and Operation and Maintenance Module

- Ecological Monitoring Center: Real-time monitoring of network status (TPS, latency, node online rate), device status (access volume, operating failure rate), transaction status (transaction volume, handling fees, burning volume), and computing power status (computing power utilization rate, task completion rate), supporting abnormal alarms (SMS, email, APP push);
- Automatic Operation and Maintenance Mechanism: Supports automatic node upgrades (software updates of core nodes without downtime), automatic fault repair (minor faults are automatically processed through scripts, and major faults trigger manual intervention processes), and automatic data backup (incremental backup of core data daily, full backup weekly).

2.5 Technical Advantage Comparison

Technical Dimension	Traditional Centralized Robot Systems	RoboChain (ROBO) Ecosystem
Data Security	Centralized storage, prone to leakage and tampering	Distributed storage + encryption technology, data "usable but not visible", full-process traceable
Computing Power Distribution	Computing power concentrated in large enterprises, high threshold for small and medium-sized teams	Global computing power integration, on-demand rental, cost reduced by 55%-70%
Device Collaboration	Collaboration possible only for devices of the same brand/protocol, poor compatibility	Cross-brand/cross-protocol adaptation, collaboration latency ≤ 50ms, success rate ≥ 98%
Real-Time Performance	High real-time performance for local control, but poor data traceability	Edge computing + off-chain processing, balancing real-time performance and traceability
Compliance	Lack of technical support for data privacy and liability definition	Blockchain evidence storage + smart contracts, automated compliance processes, traceable liability
Scalability	Fixed system architecture, high expansion cost	Sharding + side chain architecture, supporting linear expansion, unlimited device access volume

3. Economic Model Design

ROBO adopts an economic model of "fixed total supply + ecological incentives + value anchoring + deflationary adjustment", ensuring that the token value is deeply bound to the development of the robotics ecosystem, balancing short-term liquidity and long-term sustainability, and achieving a win-win situation for ecological participants.

3.1 Basic Token Information

- Token Name: RoboChain
- Token Symbol: ROBO
- Total Supply: 800 million tokens (fixed total supply, no additional issuance)
- Issuance Mechanism: Private placement + ecological incentives + public sale + team

reserve + reserve fund. The specific distribution is as follows:

Purpose	Distribution Ratio	Lock-Up Period
Ecological Incentive Fund (data contribution, computing power rewards, technology R&D, scenario landing)	32%	Unlocked in 1 year, 25% released equally quarterly, issued directionally as needed
Private Placement (strategic investment, robot enterprise cooperation, computing power service providers)	25%	Unlocked in 1 year, released equally monthly after the lock-up period (Note: The lock-up period for institutional users shall not exceed 7 days)
Public Sale (community users, retail investors, ecological participants)	10%	Lock-up period not exceeding 7 days, circulating immediately after unlocking
Team and Core Advisors	13%	Unlocked in 3 years, released equally monthly after the lock-up period, linked to performance appraisal
Reserve Fund (market fluctuation adjustment, emergency R&D, compliance and security construction)	20%	Release rhythm determined by DAO governance, earmarked for specific purposes

3.2 Core Token Functions

1. Value Circulation Medium: ROBO is the only value carrier in the ecosystem, used in all scenarios such as robot data transactions, computing power rental, multi-robot collaboration service settlement, technology patent transfer, and robot rental, realizing efficient cross-entity and cross-scenario value circulation;

2. Ecological Governance Certificate: ROBO holders can participate in major ecological decisions, including technical route adjustments, incentive rule optimization, scenario expansion directions, and compliance policy formulation. Voting rights are positively correlated with the number of tokens held and the lock-up period, realizing ecological self-governance;

3. Incentive and Staking Tool: Data contributors, computing power providers, technology developers, and compliance service providers can obtain ROBO rewards by providing value to the ecosystem; users can improve data security levels, prioritize access to computing power resources and service permissions, and obtain staking returns by staking ROBO;

4. Risk Guarantee Reserve: A special risk fund is established in the ecosystem, composed of part of the transaction handling fees and reserve funds, to cope with sudden situations such as robot safety accident compensation, technical risks, and market fluctuations, ensuring the stable operation of the ecosystem.

3.3 Deflationary and Adjustment Mechanisms

To ensure the long-term value stability of ROBO and build a sustainable economic ecosystem, a dual adjustment mechanism is established: First, the deflationary mechanism. All transactions in the ecosystem charge a 3% handling fee, of which 1.5% is used for ROBO burning and 1.5% is injected into the ecological incentive fund. As the ecological transaction activity increases, the burning volume increases synchronously, realizing a slow decrease in the total token supply and strengthening the value anchoring ability. Second, the dynamic adjustment mechanism. Regularly assess the ecological development status through DAO governance, and fine-tune the handling fee ratio and incentive distribution rules to ensure that the economic model matches the ecological development rhythm and balances the interests of all parties.

4. Core Application Scenarios

ROBO focuses on the core application areas of robotic technology, builds four closed-loop scenarios, and promotes the landing of ecological value. Considering the United States as a frontier market for robotic technology R&D and commercialization, combined with its market-oriented operation needs, strict compliance standards, and technological innovation atmosphere, the landing applications of the following four core scenarios in the United States will be further refined and detailed to highlight regional adaptability and commercial value.

4.1 Robot Data Transaction and Sharing Scenario

This scenario solves the problems of data silos and value monetization in the U.S. robotics industry. Combined with U.S. data compliance requirements such as the California Consumer Privacy Act (CCPA), it builds a full-link compliant ecosystem of "data encryption-authorized transaction-value distribution". Taking Tesla's Fremont Gigafactory in California, USA as an example, industrial robots in the factory (such as welding robots and assembly robots) can authorize through the ROBO ecosystem to anonymize and encrypt high-precision operation data during production (including welding temperature parameters, assembly error records, equipment energy consumption curves, component adaptation data, etc.) using Zero-Knowledge Proofs (ZK-SNARKs) technology before uploading to the chain, avoiding the leakage of core production processes. The factory adopts a "subscription-based transaction" model, setting a monthly subscription price of 12 ROBO for every 100MB of high-precision data. It launches differentiated authorization plans for U.S. local robot enterprises and research institutions: commercial enterprises need to pay an additional 2 ROBO/100MB compliance review fee for subscriptions, while research institutions (such as MIT Robot Laboratory and Stanford Artificial Intelligence Research Institute) can enjoy an ecological incentive discount of 3 ROBO/100MB for participating in technical collaborative R&D.

U.S. local robot enterprise Boston Dynamics subscribes to this data by paying ROBO to optimize the motion control algorithms of its industrial robots, improving the operational stability of robots in automotive manufacturing scenarios by 28% and reducing the equipment failure rate from 5.2% to 1.8%. The Stanford University research team uses this anonymized data to train a robot fault prediction model, and the relevant research results have been successfully transformed into industrial-grade solutions, additionally obtaining 5 ROBO/100MB data revenue from ecological incentives. The entire data transaction is automatically settled through smart contracts, and transaction records are synchronized to U.S. compliance regulatory nodes for filing, meeting the data traceability requirements of CCPA. By sharing data, Tesla's factory can stably obtain 80-120 ROBO revenue per month, which is converted into an annual additional income of approximately 150,000 U.S. dollars according to the ecological transaction exchange rate, realizing the commercial monetization of data assets. In addition, the ecosystem has built a data transaction compliance review channel for the U.S. market, with a compliance team composed of former senior advisors of the U.S. SEC providing real-time review services, and the review fee is charged at 1% of the transaction amount in ROBO.

4.2 Decentralized Computing Power Service Scenario

Targeting the extreme computing power needs of U.S. robot R&D enterprises (especially Silicon Valley start-ups), combined with the characteristics of U.S. computing power resource distribution (abundant Silicon Valley data center clusters and personal idle GPU resources), ROBO builds a decentralized computing power scheduling platform to realize efficient matching and compliant utilization of computing power resources. Computing power providers include U.S. local individual users (users with high-end GPUs such as NVIDIA RTX 4090 and AMD RX 7900 XTX) and professional computing power clusters (such as Silicon Valley AWS data centers and Google Cloud computing power nodes). When accessing, they need to pass a computing power benchmark test based on MLPerf to generate a computing power level score (1-10), and U.S. local nodes can obtain an additional 5% computing power reward due to regional advantages (low latency). Individual users can set a pricing of 4 ROBO per GPU hour, and professional computing power clusters are priced according to computing power levels, with level 10 computing power (suitable for large-scale model training) priced at 20 ROBO per hour.

Silicon Valley start-up Agility Robotics (focusing on humanoid service robot R&D) needs to train robot dynamic balance and environment adaptation models. If using traditional AWS cloud computing power services, the cost of a single training (1 billion parameter model) exceeds 200,000 U.S. dollars, and data transmission latency is relatively high. By accessing the ROBO ecosystem, the enterprise pays 120,000 ROBO to lease a U.S. local distributed computing power cluster (integrating 1,200 personal idle GPUs and 2 professional computing power nodes in Silicon Valley), and completes model training in only 10 days using a "task splitting + parallel training" model. The cost is reduced by 62%, and data is transmitted through AES-256-GCM encrypted channels during training, with model parameter summaries stored on-chain as evidence to ensure core technology security. Because this model improves the passing efficiency of robots in complex terrain by 35%, the enterprise additionally obtains 200,000 ROBO rewards from the ecological incentive fund for subsequent technical iterations.

In addition, the ecosystem has launched a "computing power subsidy program" for the U.S. market. Eligible U.S. robot start-ups (established for ≤ 3 years, with ≥ 2 core technology patents) can apply for a maximum 50% computing power rental subsidy. The subsidy funds are allocated from the U.S. special ecological incentive fund. The application process is reviewed by DAO governance nodes, and the review results are announced on-chain within 3 working days. Currently, 32 U.S. robot R&D enterprises have accessed the computing power platform, with the computing power utilization rate increased from 65% in the traditional model to 92%, and the average R&D cycle shortened by 40%.

4.3 Multi-Robot Collaboration Service Scenario

Facing core U.S. fields such as manufacturing, logistics, and healthcare, combined with U.S. industrial automation standards (such as ANSI/RIA R15.06 robot safety standards), it builds a robot service system featuring collaboration among "devices-cloud-scenarios", realizing service settlement and incentives through ROBO. Focus on landing two U.S.-specific scenarios:

1. Multi-Robot Collaboration Scenario at Amazon's Kentucky Logistics Center: The logistics center accesses 1,500 autonomous driving logistics robots (including Amazon's own Kiva robots and third-party robots), realizing task allocation, path planning, and loading/unloading connection collaboration through the RoboSync collaboration protocol of the ROBO ecosystem. The cloud platform dynamically allocates tasks based on real-time order data, setting a payment of 30 ROBO for every 100 order sorting tasks. Revenue is automatically distributed in the ratio of "robot enterprises (40%), computing power providers (25%), data contributors (20%), and ecological operations (15%)". For logistics peak periods (such as "Black Friday"), the system automatically activates the "emergency computing power scheduling" mechanism through smart contracts, additionally calling idle computing power nodes in the eastern United States to ensure robot response latency ≤ 30ms. When a robot fails, the system uploads fault information to the blockchain within 1 second and automatically dispatches a backup robot to take over. Robots participating in the takeover can receive an incentive of 8 ROBO per time. This solution improves the logistics center's sorting efficiency by 50%, reduces labor costs by 45%, increases order processing volume by 60% during "Black Friday", and reduces the order delay rate from 8% to 1.2%.

2. Medical Robot Collaboration Scenario at Johns Hopkins Hospital in the United States: Surgical robots and rehabilitation robots in the hospital realize data collaboration and service scheduling through the ROBO ecosystem, strictly complying with U.S. HIPAA medical data privacy regulations. Patient-related medical data is collaboratively trained through the federated learning framework, with original data not uploaded to the chain, only model update summaries uploaded to the chain. Surgical robots and rehabilitation robots collaboratively formulate patients' post-operative rehabilitation plans, with a payment of 50 ROBO for completing one patient's rehabilitation service. Revenue is distributed among the hospital, robot enterprises, and computing power service providers. The ecosystem has customized a "safety emergency response module" for medical scenarios. If an abnormality occurs in robot operation, the system automatically triggers an emergency shutdown

command, and the operation log is stored on-chain in real time to facilitate subsequent liability traceability. After the scenario is implemented, the patients' post-operative rehabilitation cycle is shortened by 20%, the accuracy of rehabilitation training is improved by 33%, and the medical dispute rate is reduced by 28%.

4.4 Robot Technology R&D and Commercialization Scenario

ROBO is deeply adapted to the policies, regulations, and market needs of different countries and regions, providing localized full-process support for robot technology R&D crowdfunding, patent transactions, and commercialization landing, breaking down industry barriers and regional restrictions. The following are specific application scenarios in the United States, the European Union, China, and Southeast Asia:

4.4.1 United States: Dual Scenario Landing of Intelligent Service Robot Commercialization and Technology R&D Crowdfunding

As a frontier market for robot technology R&D and commercialization, the United States has opened high-level intelligent robot operation permits in fields such as healthcare, home services, and logistics. The ROBO ecosystem is deeply adapted to its market-oriented needs and compliance requirements, forming a full-link U.S.-specific scenario of "R&D crowdfunding-technological transformation-commercial operation":

1. Technology R&D Crowdfunding Scenario: Silicon Valley start-up CareBot (focusing on elderly care service robot R&D) launches a phased crowdfunding project relying on the ROBO ecosystem. Targeting the U.S. market demand with a serious aging population (accounting for over 17% of the population over 65 years old), it focuses on the R&D of elderly health monitoring and emergency rescue functions. The project sets three-phase crowdfunding goals: seed round 80,000 ROBO (completion of technical prototype), R&D round 120,000 ROBO (completion of clinical trials), and landing round 200,000 ROBO (realization of mass production). Fund unlocking at each phase requires reaching preset milestones, reviewed by U.S. local DAO governance nodes (including medical experts and robot technology experts). To attract U.S. local investors, the project promises: investors can enjoy 40% of the patent authorization revenue in North America according to the crowdfunding ratio, and investors holding more than 10,000 ROBO can participate in product function iteration decisions.

After the crowdfunding was launched, U.S. local investors (including individual users and Silicon Valley angel investors) and computing power service providers actively participated. Among them, U.S. local computing power service provider NVIDIA participated by staking 1,000 GPUs of computing power, obtaining an additional 20,000 ROBO incentives. All crowdfunding goals were completed in only 8 days. After the project was implemented, CareBot's elderly care robots passed U.S. FDA medical device certification and were purchased by 20 U.S. nursing institutions. Relevant technical patents were authorized to Medtronic, a leading U.S. medical device enterprise. Investors obtained an average of 42,000 ROBO revenue per quarter, with an investment return rate of 35%.

1. Commercial Operation Scenario: California-based intelligent food delivery robot operator Serve Robotics accesses the ROBO ecosystem, deploying 2,000 intelligent food delivery robots in core cities such as San Francisco, New York, and Los Angeles, adapting to U.S. urban traffic rules and catering industry needs. Users book food delivery services through a mobile APP (supporting dual payment in U.S. dollars and ROBO, with a 10% discount for ROBO payment). The basic delivery fee within 3 kilometers in urban areas is 5 ROBO, the delivery fee for cross-regions (3-10 kilometers) is 8 ROBO, and an additional 1 ROBO per kilometer is charged for distances over 10 kilometers. Revenue is automatically distributed through smart contracts in the ratio of "robot enterprises (45%), computing power providers (20%), data contributors (25%), and ecological operations (10%)".

In response to strict U.S. data privacy regulations, scenario data authorized by users (such as delivery routes and user pickup times) is encrypted and uploaded to the chain through zero-knowledge proof technology, only used to optimize local service models. Data contributors can obtain 60-90 ROBO revenue per month. Currently, the operator's daily order volume exceeds 18,000, with ROBO settlement accounting for 82%. The operating cost is 58% lower than that of traditional manual delivery. It plans to expand the number of robot deployments to 5,000 by 2027, covering 10 core U.S. cities. In addition, the enterprise has initiated the U.S. SEC compliance filing process, completing Anti-Money Laundering (AML) and Know Your Customer (KYC) certifications through the ROBO ecosystem's compliance service module, laying the foundation for subsequent expansion in the U.S. capital market.

4.4.2 European Union: Robot Patent Collaborative Transaction and Compliant Operation Scenario

Relying on the European Union's collective negotiation guidelines for Standard Essential Patents (SEPs) in robotic technology released in October 2025, the ROBO ecosystem builds a decentralized patent transaction platform, adapting to the patent collaboration needs of enterprises such as Siemens and ABB, while meeting GDPR data compliance requirements. In the patent transaction scenario, the European Robot Patent Alliance (ERPA) led by Siemens and ABB accesses the ROBO ecosystem, uploading core SEPs patents such as robot motion control and intelligent perception to the chain for confirmation. The patent authorization price is set through smart contracts (annual authorization fee of 800,000 ROBO per enterprise), and in strict compliance with the EU's anti-monopoly regulations that the ERPA share shall not exceed 18% of SEP demand, opening patent authorization rights to other small and medium-sized robot enterprises in the EU. Patent authorization revenue is automatically settled in the ratio of patent holders (65%), ecological technology service providers (15%), and compliance audit institutions (20%). All transaction records are permanently traceable on-chain, meeting EU anti-monopoly and patent supervision requirements. A small and medium-sized EU robot enterprise obtains patent authorization by paying ROBO, without the need to negotiate separately with multiple enterprises. The authorization cost is reduced by 55%, and priority technical support rights are obtained through ROBO staking. In the commercial scenario, logistics parks in cities such as Munich, Germany and Barcelona, Spain access the ROBO ecosystem. Industrial robots realize cross-park cargo transportation through multi-device collaboration. The park operator pays 40 ROBO per transportation service, and revenue is distributed among robot enterprises, equipment operators, and data compliance service providers. At the same time, robot operation data needs to meet GDPR compliance requirements. For the part anonymized and used for model optimization, data providers can obtain ROBO from ecological incentives, achieving a balance between compliance and value monetization.

4.4.3 China and Southeast Asia: Industrial Robot Collaboration and Low-Cost R&D Scenarios

Targeting China's advantages in manufacturing automation upgrading and Southeast Asia's low-cost operation needs, the ROBO ecosystem creates differentiated application scenarios. In China, an intelligent manufacturing industrial park accesses the ROBO ecosystem, relying on the complete industrial robot infrastructure in the region to realize real-time data collaboration of multi-brand and multi-type industrial robots. The park management dynamically allocates production tasks through smart contracts, paying 10 ROBO per hour of production capacity optimization to equipment operators and data providers. In the technology R&D scenario, a domestic university robot team raises 250,000 ROBO through the ROBO ecosystem for optimizing the industrial robot collaboration model under complex working conditions. Combined with the production data of domestic manufacturing industry, the error rate of the model in multi-device collaboration is reduced from 15% to 3%. After the project is implemented, it obtains an additional 80,000 ROBO subsidy from the ecological incentive fund, and the technical achievements have been applied to many domestic automobile factories. In the Southeast Asian market, focusing on the labor-intensive industries and short-distance service needs in countries such as Vietnam and Indonesia, a Southeast Asian enterprise launches low-cost industrial robots and community service robots. Users can book services by paying ROBO. The hourly rental fee for industrial robots is only 2 ROBO, and the service fee per order for community service robots is 1 ROBO. At the same time, users are supported to stake ROBO to become service nodes and participate in operation sharing. To address the limited computing power resources in Southeast Asia, the enterprise rents global idle computing power through ROBO for simplified robot model training. The training cost is 70% lower than that of traditional cloud computing power, accelerating the popularization of robot technology in emerging markets.

Through country-specific scenario adaptation, ROBO realizes global collaboration in technology R&D, patent transactions, and commercial operation, not only complying with the policy and compliance requirements of different regions, but also connecting cross-regional value circulation through the token ecosystem, promoting the global landing of robot technology.

5. Compliance and Security Framework

The integration of robotic technology and cryptocurrency needs to balance technological innovation, commercial value, and compliance security. ROBO builds a comprehensive guarantee system from three dimensions: compliance supervision, security guarantee, and liability definition, ensuring the sustainable development of the ecosystem.

5.1 Compliance Supervision Adaptation

ROBO strictly follows the financial regulatory policies, robotics industry regulations, and data security regulations of major countries and regions around the world, formulating differentiated compliance solutions for different scenarios: financial transaction scenarios follow Anti-Money Laundering (AML) and Know Your Customer (KYC) rules to prevent financial risks; data transaction scenarios comply with global data privacy protection regulations (such as GDPR and Personal Information Protection Law) to ensure the legality and compliance of data collection, storage, and circulation; robot operation scenarios connect with industry regulatory authorities of various countries, follow the hierarchical supervision requirements of robots, promote the collaboration of technical standards and regulatory rules, take the initiative to accept supervision, and obtain relevant operation permits.

6. Full-Link Security Guarantee

Taking "safety and controllability" as the core principle of the ecosystem, it builds a dual security system of technology and mechanism: technically, it adopts zero-knowledge proofs and end-to-end encryption technology to ensure data security, ensures that robot operation logs are auditable through the traceability characteristics of blockchain, embeds a security vulnerability response mechanism to encourage white-hat hackers to discover vulnerabilities and give ROBO rewards, and conducts regular security audits; mechanically, it establishes a security committee composed of robot technology experts, network security experts, and representatives of regulatory agencies to supervise the security of technical applications in the ecosystem, formulate security standards and emergency handling processes, and impose penalties on non-compliant entities (such as deducting staked tokens and restricting ecological permissions).