



PRODAO Whitepaper

Version 12

A Decentralized, Expert-Centric Data Economy for the Web3 Era

Abstract

PRODAO aims to resolve the infringement of individual data control rights and the value imbalance created by today's centralized data economy, and to lead a new expert-centric data economy in the WEB3 era. Our vision is to build a decentralized ecosystem in which individual experts can fully reclaim sovereignty over their own data, receive fair compensation for their contributions to the platform, and scale their expertise to a global level.

The PRODAO Mainnet, built on blockchain and DID (Decentralized Identifier) technology, provides a robust infrastructure that allows experts to securely manage and utilize their own data. By integrating AI technology on top of this, PRODAO enhances the value of data and supports personalized services, while promoting knowledge sharing among experts and the expansion of global networks through decentralized SNS. In particular, through the A2E (Add to Engagement) model, PRODAO implements an innovative virtuous-cycle structure in which every contribution an expert makes to the platform translates into tangible value and rewards.

PRODAO is committed to securing the highest level of network and data security in order to stably operate decentralized expert services, A2E rewards, and DID-based MyData. PRODAO systematically analyzes and proactively responds to every potential vulnerability, including the core consensus algorithm, the P2P network, smart contracts, node operations, and data privacy.

Through this powerful framework, PRODAO seeks to build a decentralized expert ecosystem in which users leverage their data and expertise safely and efficiently, realizing true data sovereignty and fair compensation.

Table of Contents

1. Introduction

- 1.1. Introduction to the PRODAO Project and Its Vision
- 1.2. Problems of the Existing Data Ecosystem and PRODAO's Solutions
- 1.3. The Necessity and Objectives of the PRODAO Mainnet
- 1.4. Core Values and Components of the PRODAO Ecosystem

2. PRODAO Mainnet Architecture

- 2.1. Network Design Principles (Decentralization, Security, Scalability, Interoperability)
- 2.2. Node Structure and Roles (Signer Nodes, General Nodes, etc.)
- 2.3. Data Storage and Management Mechanisms
- 2.4. Network Communication and the P2P Protocol

3. Consensus Algorithm

- 3.1. In-Depth Analysis of PRODAO's PoC (Proof of Contribution) Consensus Algorithm
- 3.2. PoC-Based Block Generation and Verification Process
- 3.3. Prevention of Malicious Behavior and Security Mechanisms (Slashing, etc.)

4. Decentralized Identifier (DID) System

- 4.1. Definition and Importance of DID
- 4.2. Structure and Operation of the PRODAO DID System
- 4.3. DID-Based Data Sovereignty Management and Use Cases
- 4.4. DID Security and Privacy Protection

5. AI Integration

- 5.1. The Role of AI in the PRODAO Ecosystem and Its Fields of Application
- 5.2. Using AI to Enhance Data Value
- 5.3. Personalized Services and Smart Matching
- 5.4. AI Model Training and Management

6. Tokenomics

- 6.1. The Role and Utility of the PROD Token
- 6.2. Details of the A2E (Add to Engagement) Reward Model
- 6.3. Token Distribution and Supply Plan
- 6.4. Token Value Appreciation Mechanisms

7. Smart Contracts and DApps

- 7.1. PRODAO Smart Contract Development Environment
- 7.2. Smart Contracts for Implementing Key Platform Features
- 7.3. PRODAO SDK and Developer Tools
- 7.4. Security Audits and Vulnerability Management

8. Governance

- 8.1. PRODAO Decentralized Autonomous Organization (DAO) Structure
- 8.2. Token-Holder-Based Voting and Decision-Making Process

8.3. On-Chain / Off-Chain Governance Model

9. Roadmap and Future Plans

- 9.1. Key Milestones by Development Phase
- 9.2. Ecosystem Activation Strategy
- 9.3. Partnership and Community Expansion Plan

10. Network and Data Security

- 10.1. Network Security Vulnerability Analysis and Response
- 10.2. Smart Contract Security Audit Plan
- 10.3. Data Protection and Privacy Security Policy

11. Disclaimer and Risk Warning

- 11.1. Immutability and Limitations of the Information in This Whitepaper
- 11.2. Technical Risks
- 11.3. Market and Economic Considerations and Response Strategy
- 11.4. Regulatory and Legal Environment Analysis and Proactive Response Strategy
- 11.5. Operational and Management Risks

1. Introduction

1.1. Introduction to the PRODAO Project and Its Vision

In today's digital era, personal data is called the “new oil” and generates enormous value. Yet most users do not know how their data is being used, and they face an imbalance in which the value generated from their data is concentrated in centralized platforms. This reality infringes on individual data sovereignty and has become a major factor hindering the growth of a healthy data-economy ecosystem.

PRODAO was created to shift this paradigm and to lead a new data economy in the WEB3 era. Our vision is to be “a place where every activity of an expert connects to value”—building a decentralized data ecosystem in which individual experts reclaim full control over their own data, are fairly and transparently compensated for their activities and contributions, and can further scale their expertise globally.

Built on blockchain and DID (Decentralized Identifier) technology, PRODAO provides the PRODAO Mainnet infrastructure that allows expert users to securely manage and utilize their own data. By integrating artificial intelligence (AI) on top of this, PRODAO further enhances the value of data and supports personalized services and the efficient operation of the ecosystem.

In addition, PRODAO provides a decentralized SNS service through which experts can share and promote their knowledge, experience, and content with the world, supporting the formation of global networks and the expansion of their influence. Within PRODAO, experts exercise their expertise and carry out diverse activities, and these activities are recognized as unique value.

Furthermore, by applying the A2E (Add to Engagement) model, the system is designed so that the more an individual expert adds value to the platform and actively participates in the community, the more fairly they are rewarded through PROD tokens. The PROD token is used for various utilities such as service usage and governance participation within the ecosystem, driving the autonomous growth of the PRODAO ecosystem.

A portion of the value obtained through the platform's growth is used for social-contribution activities such as the “Starlight Scholarship Foundation,” and the “Galactic Public-Good Hackathon” helps discover ideas that solve social problems and enables experts to form teams and develop solutions.

As “a space that opens new possibilities in an age of information overload,” PRODAO likens experts to “stars” and the communities they form to “star clusters,” aiming to build an ecosystem in which everyone participates autonomously, develops together, and achieves continuous growth.

PRODAO's Core Vision

Through the following four core visions, PRODAO builds a future data economy led by experts.

Vision 1: Realizing Data Sovereignty and Fair Compensation

We realize a future in which experts exercise full control over their own data and receive fair value and compensation for all of their creative activities, including their knowledge, experience, and networks.

Vision 2: A Front-Runner Among Web3-Based Expert Platforms

By leveraging innovative Web3 technologies such as blockchain, AI, and DID, we guarantee experts' data sovereignty and provide a new dimension of platform that maximizes their potential through a transparent and fair, contribution-based reward system.

Vision 3: A Venue for Decentralized Communication and Collaboration

Prioritizing decentralization and user sovereignty, we support efficient communication and collaboration among experts through an AI-based smart matching system, and return fair value for their contributions through the PROD token reward system.

Vision 4: A Continuous Growth Partner for Experts

Continuously evolving alongside advances in Web3 technology, we become a partner that actively supports experts in creating new opportunities, demonstrating global capabilities, and growing continuously amid the innovative changes of social networks.

PRODAO is a collaborative platform that breaks away from centralized systems, respects and shares experts' capabilities and knowledge, and thereby provides positive value to both individuals and society.

1.2. Problems of the Existing Data Ecosystem and PRODAO's Solutions

1.2.1. Problems of the Existing Data Ecosystem

Existing centralized data platforms carry a number of problems. First, the infringement of data sovereignty. Users do not clearly know how their data is collected, stored, and used, and in many cases data is used commercially without consent. Second, opaque value distribution. Even though users' data contributes to the growth of the platform, they do not receive fair compensation commensurate with that contribution, and most of the value is concentrated in the platform provider. Third, data security and privacy problems. Centralized servers are vulnerable to hacking and data breaches, which undermines user trust. Fourth, the limitations placed on expert activities. Existing platforms impose many constraints on experts effectively sharing and monetizing their knowledge and experience, and, being locked into specific platforms, experts have little freedom of activity. Finally, the absence of a global network. Confined by regional and platform boundaries, it is difficult to exchange and collaborate with experts around the world.

1.2.2. PRODAO's Solutions

Through innovative technologies such as blockchain, DID, and AI, PRODAO resolves the fundamental problems of the existing data ecosystem and presents a new, expert-centric paradigm.

Restoring Decentralized Data Sovereignty

Using DID (Decentralized Identifier) technology, individual experts are given full control over their own data. Based on the expert's explicit consent throughout the entire process of data creation, storage, sharing, and use, they can transparently verify and manage how their data is used. This is a key solution that strengthens privacy protection and prevents data abuse.

Fair and Transparent Value Sharing

Through the A2E (Add to Engagement) model, PRODAO provides a transparent, blockchain-based reward system for all of an expert's contribution activities (data provision, content creation, community participation, etc.). This resolves the unfair value-distribution problems of existing platforms and guarantees fair compensation for experts' activities, inducing continuous participation and ecosystem growth.

AI-Based Value Enhancement and Efficiency Gains

By integrating artificial intelligence (AI) into the PRODAO Mainnet, PRODAO goes beyond merely storing data to enhance its value. Through the analysis of expert data, AI provides personalized information recommendations, greater efficiency in acquiring knowledge, smart matching systems, and more, maximizing the platform's usefulness. In addition, AI-based automated management systems increase the operational efficiency of the ecosystem.

Expanding Expertise and Forming a Global Network

Through decentralized SNS services and DID-based expert profiles, PRODAO creates an environment in which experts around the world can freely communicate and collaborate. This enables the formation of a global expert network beyond regional and platform constraints, and supports experts' knowledge and experience being shared and utilized across a broader scope.

Building a New WEB3-Based Paradigm

Beyond mere technical innovation, PRODAO builds a new data-economy ecosystem led by and participated in by experts. A decentralized system provides fair opportunities to all participants on the basis of transparency and trust, presenting a sustainable growth model for the Web3 era that goes beyond the limitations of existing Web2.

1.3. The Necessity and Objectives of the PRODAO Mainnet

As the core infrastructure of the PRODAO ecosystem, the PRODAO Mainnet is designed to overcome the limitations that arise in existing blockchain networks and to realize PRODAO's vision. Existing public blockchains have limitations that make it difficult to implement large-scale, user-based services or complex logic due to high transaction fees, low processing speeds, and complex development environments. In particular, on a platform like PRODAO where users' data creation and interactions occur frequently, these limitations become even more pronounced.

1.3.1. Core Objectives of the PRODAO Mainnet

As the core infrastructure of the PRODAO ecosystem, the PRODAO Mainnet has the following objectives.

- **High performance and scalability:** It provides high throughput capable of processing thousands of transactions per second or more, and secures scalability in line with user growth, providing an environment suitable for operating large-scale services.
- **Low fees:** It minimizes transaction fees in order to reduce the burden on users and improve service accessibility.
- **Security and stability:** It guarantees the integrity and stability of the network through a powerful consensus algorithm and security mechanisms.

- **Interoperability:** It expands the reach of the PRODAO ecosystem and creates synergy with diverse services through interconnection with other blockchain networks.
- **Developer-friendly environment:** It provides a convenient and efficient development environment for smart contract development and DApp implementation, encouraging participation in the ecosystem.
- **Data sovereignty and privacy protection:** Through a DID-based data management system, it guarantees the sovereignty of personal data and provides powerful privacy-protection features.

1.4. Core Values and Components of the PRODAO Ecosystem

1.4.1. Core Values of the PRODAO Ecosystem

The PRODAO ecosystem is built on the following core values.

- **Data Sovereignty:** Guarantees full control and ownership of one's personal data.
- **Fairness:** Provides a transparent and fair reward-distribution system based on contribution.
- **Transparency:** All transactions and data flows are transparently recorded on the blockchain.
- **Trustworthiness:** Builds trust among participants through a decentralized system and powerful security.
- **Scalability:** Provides a scalable infrastructure that can flexibly respond to growth in users and services.
- **Innovation:** Creates new value by converging the latest technologies such as blockchain, DID, and AI.
- **Community-Centric:** Encourages the community's participation in decision-making through DAO governance and pursues the sustainable growth of the ecosystem.

1.4.2. Key Components of the PRODAO Ecosystem

The PRODAO ecosystem operates through the organic combination of diverse core components.

- **PRODAO Mainnet:** A high-performance, highly scalable blockchain network that serves as the foundation of the ecosystem. All transactions and smart contracts are executed on top of it.
- **PoC (Proof of Contribution) Consensus Algorithm:** PRODAO's own proprietary consensus algorithm that measures experts' contributions and, based on them, generates blocks and distributes rewards.
- **DID (Decentralized Identifier) System:** A distributed identity system that helps securely manage and control experts' identities and data.

- **AI Integration Module:** Artificial-intelligence technology that enhances the value of data, provides personalized services, and increases the operational efficiency of the ecosystem.
- **PROD Token:** The ecosystem's base currency and a utility token used for governance participation, rewards, service usage, and more.
- **A2E (Add to Engagement) Reward Model:** A system that fairly rewards users with PROD tokens according to their contributions.
- **Decentralized SNS Service:** A distributed social-network service through which experts can share and interact with knowledge, experience, and content.
- **Smart Contracts:** Contract code that automates and executes the core logic of the PRODAO ecosystem (token issuance, reward distribution, DAO voting, etc.).
- **PRODAO SDK and Developer Tools:** Tools and libraries that help developers easily build DApps on top of the PRODAO Mainnet and participate in the ecosystem.
- **DAO (Decentralized Autonomous Organization) Governance:** A decentralized management structure through which PROD token holders participate in the ecosystem's key decisions and set its direction.

2. PRODAO Mainnet Architecture

2.1. Network Design Principles (Decentralization, Security, Scalability, Interoperability)

To realize an expert-centric data economy in the Web3 era, the PRODAO Mainnet is built on the following core design principles. These guarantee the stability and efficiency of the network, provide users with an optimal experience, and form a solid foundation for long-term ecosystem growth.

2.1.1. Decentralization

Importance

Decentralization is a core value of blockchain that removes single points of failure, secures censorship resistance, and guarantees the transparency and fairness of the network. Centralized systems can be controlled by specific entities, which can cause various problems such as data manipulation, service outages, and opaque operations. To resolve these problems and guarantee experts' data sovereignty, PRODAO pursues strong decentralization.

PRODAO's Implementation Approach

The PRODAO Mainnet decentralizes the selection of Signer nodes (block-generating and signing nodes) through the PoC (Proof of Contribution) consensus algorithm, and diverse general nodes (Full Nodes and Light Nodes) participate in the network to distribute transaction verification and data storage. In addition, by building the governance model in the form of a DAO (Decentralized Autonomous Organization), it is designed so that the token-holder community—rather than any specific entity—leads the network's key decisions. By ensuring that the network's operation and development are based on the consensus of the entire community, PRODAO realizes true decentralization.

2.1.2. Security

Importance

Security is the most fundamental element of any blockchain network. If a network is vulnerable to hacking or malicious attacks, fatal problems can occur, such as loss of user assets, tampering with data, and service outages. In the PRODAO ecosystem in particular, where experts' sensitive data and valuable assets move about, the highest level of security is essential.

PRODAO's Implementation Approach

The PRODAO Mainnet applies multi-layered security mechanisms. First, it protects all transactions and data transmissions through strong encryption technology. Second, by introducing slashing and penalty systems within the PoC consensus algorithm, it prevents malicious node behavior and induces honest participation in the network. Third, through the DID (Decentralized Identifier) system, it strengthens the security and privacy of user identities and finely controls data-access rights. Fourth, it mandates security audits when developing smart contracts and prevents potential security risks in advance through continuous vulnerability analysis and updates. Finally, through a decentralized node structure, it removes single points of failure and increases the overall stability of the network.

2.1.3. Scalability

Importance

Scalability is the ability of a blockchain network to efficiently process large numbers of users and transactions. Facing the “blockchain trilemma” (the problem that it is difficult to simultaneously satisfy two of the three properties of decentralization, security, and scalability), existing blockchain networks often experience high transaction fees and slow processing speeds due to insufficient scalability. As an expert platform where a vast amount of data creation and interaction is expected, securing high scalability is very important for PRODAO's smooth service operation and user experience.

PRODAO's Implementation Approach

To achieve high scalability, the PRODAO Mainnet considers the following technical approaches. First, it considers introducing sharding technology, dividing the network into multiple independent shards to process transactions in parallel, thereby increasing the throughput of the entire network. Second, it applies efficient data-compression and storage technology to optimize block size, and uses off-chain data-storage mechanisms to reduce the burden on the blockchain. Third, through an optimized consensus algorithm (PoC) and the gRPC network protocol, it enables efficient communication between nodes and fast block finalization. Fourth, PRODAO leaves open the possibility of integration with L2 solutions (e.g., Rollups) and is flexibly designed so that it can additionally secure the required scalability while reducing the burden on the mainnet.

2.1.4. Interoperability

Importance

Interoperability is the ability to smoothly exchange information and assets, and to interact, among different blockchain networks or external systems. The current blockchain ecosystem is fragmented across various networks, so there are many constraints on the exchange of information and the movement of assets between networks. PRODAO considers it important to secure a high level of interoperability in order to expand its expert ecosystem and create synergy with diverse external services. This maximizes the utility of the PRODAO Mainnet and contributes to raising PRODAO's value within the broader Web3 ecosystem.

PRODAO's Implementation Approach

The PRODAO Mainnet considers various interoperability solutions. First, it develops or integrates cross-chain bridge technology to support the smooth movement of PROD tokens and other digital assets with other major blockchain networks such as Ethereum. Second, to interconnect with external data, it uses Oracle solutions so that real-world data outside the blockchain can be securely brought into the PRODAO Mainnet. Third, it builds a DID system that supports international standards and user convenience, designing PRODAO DID to be compatible with other DID-based services. Finally, by providing open APIs and SDKs, it supports external developers in easily integrating with the PRODAO Mainnet and building new DApps, which ultimately accelerates the expansion of the PRODAO ecosystem.

2.2. Node Structure and Roles (Signer Nodes, General Nodes, etc.)

For stable and efficient network operation, the PRODAO Mainnet has a structure in which various kinds of nodes interact organically. Each node is responsible for a specific function of the network and contributes to the healthy operation of the entire ecosystem.

2.2.1. Signer Nodes (Block-Generating and Signing Nodes)

Signer nodes play the most important role in the PoC (Proof of Contribution) consensus algorithm of the PRODAO Mainnet. They verify transactions, generate new blocks, and hold the authority to add blocks to the blockchain. Signer nodes are composed of experts with a high Contribution Score in the PRODAO ecosystem or of entities trusted by the community; and through additional technical implementation, Non-Signer Full Nodes are being configured to secure network maintenance and scalability.

Key Roles

- Actual block generation as a dynamic Signer on a Gravity basis within a Full Node.
- In the PoC consensus structure, nodes selected on a Gravity Top-N user delegate basis perform the Signer role.

- Block generation through an IBFT / Clique-based consensus engine.
- Transaction verification and aggregation: Verifies the validity of all transactions submitted to the network and gathers them to compose a single block.
- Block generation: Proposes and generates a new block composed of valid transactions.
- Block signing and consensus participation: Signs the generated block and participates, together with other Signer nodes, in the consensus process regarding the block's validity.
- Network maintenance: Maintains the health of the network and responds to requests from other nodes through data synchronization.

Selection and Participation

Signer nodes are selected based on PROD token staking and the Contribution Score within the PRODAO ecosystem. A high contribution score and sufficient staking grant eligibility to participate as a Signer node, which strengthens the security and stability of the network. Through a transparent selection process, the system is designed so that anyone can raise their contribution and aspire to become a Signer node.

Responsibilities and Rewards

Signer nodes receive PROD tokens as a reward for block generation, which serves as an incentive for network maintenance. However, if malicious behavior or actions harmful to the network (e.g., double-signing, malfunction) are detected, they are subject to powerful penalties in which their staked PROD tokens are slashed or their contribution score is reduced. This is an essential element for inducing responsible behavior by Signer nodes and maintaining the integrity of the network.

2.2.2. General Nodes (Full Node & Light Node)

In addition to Signer nodes, the PRODAO Mainnet supports general nodes that increase the decentralization and data availability of the network. General nodes are divided into Full Nodes and Light Nodes according to the way they participate in the network and the amount of data they store.

Full Node

A Full Node is a node that fully downloads and stores all block data and transaction records of the PRODAO blockchain from beginning to end and verifies them independently. It is the most important node type, fully preserving the history of the PRODAO Mainnet blockchain and verifying all of the network's rules (consensus algorithm, transaction validity, etc.) by itself, thereby guaranteeing the integrity of the network.

- Complete data storage and verification: Holds all data from the genesis block of the PRODAO Mainnet to the present, and independently verifies each new block and transaction as it is added to confirm its validity.

- **Contribution:** Plays a key role in strengthening the security and decentralization of the network. It provides trustworthy information when other nodes or wallets request data, and participates in transaction propagation and verification.
- **Advantages:** Provides the highest level of security and independence, and allows verification of the true state of the network.
- **Signer node candidate:** PRODAO's Signer nodes (validator nodes) must fundamentally function as Full Nodes.

Light Node Proxy Layer

A Light Node is a node that, rather than storing all of the PRODAO blockchain's data, downloads and verifies only block headers and the minimum necessary transaction information. Because it consumes far less storage space and computing resources than a Full Node, it can be used as a local-node client and as an intermediate node. Light Nodes are designed to run interconnected with mobile devices and DApps/users.

- **Efficient verification:** Because it does not download the full block data, its synchronization and verification speeds are fast. Using block headers and Merkle trees, it can efficiently verify whether a specific transaction is included in a block (SPV: Simplified Payment Verification).
- **Resource efficiency:** It can participate in the network with only a small amount of storage space and bandwidth, giving it high accessibility.
- **Client application support:** It is used mainly by client applications that require fast, lightweight blockchain interaction, such as mobile wallets and web-based DApps.

2.2.3. Inter-Node Interaction and Ecosystem Contribution

On the PRODAO Mainnet, all node types communicate with one another through the gRPC network protocol and share information and transactions. Signer nodes generate and sign blocks, Full Nodes verify and propagate them, and Light Nodes receive and use necessary data from Full Nodes to support application functions. This organic interaction among diverse nodes is an essential element for maintaining the decentralization, security, scalability, and stability of the PRODAO Mainnet. Each node contributes to the growth and development of the PRODAO ecosystem according to its role.

2.3. Data Storage and Management Mechanisms

To store and manage expert data efficiently and securely, the PRODAO Mainnet uses a mixture of on-chain and off-chain data-storage methods. This is a design that leverages the inherent characteristics of blockchain (immutability, transparency) while simultaneously considering the efficiency of large-scale data processing and user privacy.

2.3.1. On-Chain Data Storage (Blockchain-Based Storage)

On-chain data storage refers to data recorded directly on the blockchain. On the PRODAO Mainnet, the following core information is mainly stored on-chain.

Characteristics

- **Immutability and transparency:** Once data is recorded on the blockchain, it cannot be changed or deleted, and all network participants can verify it transparently.
- **Security and trust:** Through encryption technology and distributed-ledger technology, the integrity and reliability of data are strongly guaranteed.
- **Storage of core metadata:** On the PRODAO Mainnet, data that is essential to the core operation of the network and that requires transparency—such as the public information of DIDs (Decentralized Identifiers), PROD token transaction records, smart contract states, and the hash values of off-chain data—is stored on-chain.

Security

Because on-chain data is verified by network consensus and recorded in blocks, tampering is virtually impossible, providing strong security. This is especially suitable for data that requires high security, such as PROD token ownership or the basic information of a DID.

2.3.2. Off-Chain Data Storage and Management (Distributed Off-Chain Storage)

Storing all of the large-volume, unstructured data that experts generate (e.g., professional documents, images, videos, complex code, etc.) on-chain has technical and cost limitations. Therefore, PRODAO manages such data using an efficient off-chain distributed storage system.

Efficiency and Scalability

Off-chain storage reduces the storage cost of large-scale data, provides fast access speeds, and reduces the block-size burden on the mainnet, thereby increasing the scalability of the network. By considering distributed file systems such as IPFS (InterPlanetary File System) and storing data distributed across multiple nodes, it removes single points of failure and improves data availability.

Data Sovereignty and Privacy Protection

Data stored off-chain is interlinked with the DID system so that individual experts have full control over their own data. Through data encryption, access control, and the like, the entities that can view or use the data can be explicitly controlled. For example, only the hash value of the data is recorded on-chain to prove the data's integrity, while the actual data is designed to be accessible only with the expert's consent.

2.3.3. Ensuring Data Integrity and Availability

By combining the advantages of on-chain and off-chain data storage, the PRODAO Mainnet secures both the integrity and availability of data.

- **Integrity:** By recording the hash value of off-chain data on-chain, it is possible to verify on a blockchain basis that the actual data has not been tampered with. If the hash values do not match, the data can be judged to have been altered.
- **Availability:** Because distributed storage systems such as IPFS store data distributed across multiple nodes, even if a problem occurs at a particular node, the data can still be accessed through other nodes, guaranteeing high availability.
- **Security layer:** Through encryption and access-control mechanisms, it strengthens the security of sensitive off-chain data and ensures that only authorized users can access it.

2.4. Network Communication and the P2P Protocol

As a decentralized distributed system, the PRODAO Mainnet has all nodes interact directly with one another using a P2P (Peer-to-Peer) communication protocol. The P2P network is a core technology that allows nodes to autonomously exchange data and maintain the network without a central server.

2.4.1. Core Principles of P2P Communication

The P2P protocol operates on the basis of the following key principles.

Node Discovery and Connection

When a new node joins the network, it attempts to connect with existing nodes. This is done through mechanisms such as bootstrap nodes or a DHT (Distributed Hash Table), through which it discovers other nodes in the network and establishes connections.

Message Propagation

Connected nodes propagate various messages to one another, such as transactions, blocks, and network-state information. This is done efficiently through methods such as the Gossip protocol, allowing messages to spread quickly across the entire network.

2.4.2. The Role of the P2P Protocol in the PRODAO Network

On the PRODAO Mainnet, the P2P protocol performs the following core roles.

- **Transaction propagation:** Transactions submitted by users are quickly propagated through the P2P network to all relevant nodes, including Signer nodes.
- **Block synchronization:** New blocks generated by Signer nodes are propagated through the P2P network to other Signer nodes and Full Nodes for verification and synchronization. This keeps all nodes at the same, latest blockchain state.

-
- Data request and response: Light Nodes and wallet applications request and receive data on specific transaction records or blockchain state from Full Nodes through the P2P network.
 - Strengthening network robustness and decentralization: By having nodes communicate directly with one another rather than relying on a single central server, the network gains strong resistance to failures at any single point or attempts at censorship. This strengthens the decentralized nature of the PRODAO Mainnet and guarantees stable operation.

3. Consensus Algorithm

3.1. In-Depth Analysis of PRODAO's PoC (Proof of Contribution) Consensus Algorithm

The PRODAO Mainnet secures both the security and efficiency of the network through its proprietary consensus algorithm, PoC (Proof of Contribution). PoC compensates for the energy inefficiency of the existing Proof of Work (PoW) method and the capital-concentration problem of the Proof of Stake (PoS) method, and provides a mechanism that directly rewards “contribution,” a core value of the PRODAO ecosystem. Rather than favoring nodes that simply hold many assets, it aims to induce nodes that create real value for and actively participate in the ecosystem to gain block-generation authority, thereby building a healthier and fairer network.

3.1.1. Contribution Score Criteria and Calculation Logic

The core of the PoC algorithm depends on how fairly and accurately each node's “Contribution Score (CS)” is calculated. The CS is calculated by quantitatively and qualitatively evaluating the various activities an expert performs within the PRODAO ecosystem.

Key Metrics and Weights for Measuring Contribution

The CS is calculated based on the following four major metrics, each of which is assigned a weight according to its importance to the PRODAO ecosystem.

Amount of DID Information Added and Qualitative Evaluation (Weight: 40%)

- **Measurement method:** Evaluates the amount of information an expert adds to their DID (Decentralized Identifier) (e.g., field of expertise, career, certifications, degrees, etc.) and the qualitative reliability of that information (e.g., third-party attestation, blockchain-based verifiability).
- **Significance:** Because a DID is an expert's core profile and the basis of trust, accurate and rich DID information is regarded as the most important contribution to raising the trustworthiness of the expert ecosystem.

Content Interaction (Weight: 30%)

- **Measurement method:** Measures the engagement of other users (views, likes, comments, shares, citations, etc.) with content an expert creates or shares on the platform (posts, papers, projects, etc.).
- **Significance:** The creation of high-quality content and active interaction are important contributions that raise the informational value of the ecosystem and promote communication among users.

Data Sharing (Weight: 20%)

- Measurement method: Measures the amount and utilization of data that an expert, with their own consent, shares within the ecosystem in anonymized or de-identified form.
- Significance: Shared data becomes a core resource that is used for AI training, the development of new services, and more, increasing the overall value of the ecosystem.

Frequency and Influence of Community Participation (Remaining Weight)

- Measurement method: Evaluates active participation and positive influence within the community, such as forum participation, governance voting, bug reporting, and ecosystem promotion activities.
- Significance: Community activity is an essential element for the sustainable growth and development of the ecosystem.

Final Contribution Score (CS) Calculation

The final CS is calculated by multiplying the measured value for each metric by its weight and summing the results. The CS is updated periodically and is designed to reflect the expert's continuous contributions. If a specific malicious act is detected, the CS may be reduced.

Transparency and Fairness

The CS calculation logic is transparently disclosed within the smart contract so that all participants can verify it. This secures the fairness of contribution evaluation and provides clear guidelines on how participants can raise their contributions.

3.1.2. PoC-Based Block Generation and Verification Process

The PoC consensus algorithm maintains the stability of the network by generating and verifying blocks through the following steps.

Signer Node Selection

The PRODAO Mainnet periodically selects, in accordance with the PoC consensus algorithm, the top nodes with the highest Contribution Score (CS) in the network into the Signer node pool. This process combines voting and randomness elements to secure fairness and unpredictability.

Transaction Collection and Block Proposal

Among the selected Signer nodes, the node currently holding block-generation authority (the leader node) collects the valid transactions propagated across the network and proposes a new block containing them. The proposed block includes the hash value of the previous block, the list of transactions, a timestamp, and the signature of the proposing Signer node.

Block Verification and Consensus

The proposed block is propagated to the other Signer nodes. Each Signer node independently verifies the validity of the proposed block (transaction validity, signature validity, etc.). When a certain number or more of the Signer nodes (e.g., two-thirds or more) confirm the block's validity and sign it, consensus is reached.

Block Finalization and Chain Addition

The block for which consensus has been completed is finally added to the blockchain and finalized. A finalized block cannot be reversed, and it is synchronized to all Full Nodes to reflect the latest state of the network.

Reward Payout and Contribution Update

The Signer node that successfully generated the block and the Signer nodes that participated in the consensus receive PRODAO tokens as a reward. At the same time, the Contribution Score (CS) of all nodes that contributed to block generation and network maintenance is updated. This provides participating nodes with a continuous incentive to contribute.

3.1.3. Prevention of Malicious Behavior and Security Mechanisms (Slashing, etc.)

The PoC consensus algorithm includes powerful mechanisms that prevent malicious behavior in order to maintain the security and integrity of the network.

Staking

A node wishing to participate as a Signer node must stake a certain amount of PRODAO tokens as collateral. This imposes an economic constraint—that the staked tokens may be forfeited if the node behaves maliciously—thereby inducing honest participation.

Slashing

- **Definition:** A powerful penalty mechanism that forfeits some or all of the staked PRODAO tokens if a Signer node commits a malicious act that harms the network—such as double-signing or improper block proposal/verification—or violates the rules of the consensus network protocol.
- **Objective:** To provide a strong deterrent against malicious behavior and to maintain the security and reliability of the network. Slashed tokens may be burned or returned to the network reward pool.
- **How it works:** The targets of slashing are validators (PRODAO's Signer nodes) that have deposited a stake as collateral in order to participate in the consensus process. These nodes stake PRODAO tokens to participate in the network, and it is these staked PRODAO tokens that are subject to slashing.
- **Trigger conditions:** Slashing is triggered when a specific violation specified in the network's consensus rules (e.g., inclusion of an invalid transaction, an invalid signature) is detected. Such violations are usually detected automatically by smart

contracts or the network protocol.

- **Penalty:** Depending on the severity and type of violation, a certain proportion of the staked tokens (e.g., 1%–100%) is forfeited.
- In PRODAO's case, some of the forfeited (slashed) PROD tokens are burned, contributing to reducing the total circulating supply and increasing scarcity, while the remainder may be redistributed elsewhere in the ecosystem (e.g., the community treasury, the reward pool).
- **Procedure:** Detection of the violation and submission of evidence; approval of slashing by network consensus; slashed tokens are burned (inducing deflation) or moved to the network reward pool.
- **Reward rules:** Incentives that validators receive when they contribute to the healthy participation of the network.
- **Block-proposal reward:** Paid to the validator that successfully proposed a block.
- **Block-verification reward:** Paid to validators that voted on a valid block and contributed to consensus.
- **Reward form:** Paid in PROD tokens.
- **Reward distribution:** Per block generation, at the end of each epoch, and so on.

Contribution Score (CS)-Based Penalties

In addition to slashing, if behavior that negatively affects network operation (e.g., frequent offline status, attempts to propose defective blocks, etc.) is detected, the Contribution Score (CS) of the relevant node may be reduced. A CS reduction imposes a disadvantage on obtaining future block-generation authority, inducing continuous good-faith participation. Through these multi-layered security mechanisms, PRODAO's PoC consensus algorithm achieves both strong security and efficiency.

3.1.4. Implementation Method for the Participant Contribution and Reputation System Algorithm

This is an algorithm that is essential for implementing the core logic to build a participant contribution and reputation system on the PRODAO Mainnet, and for maintaining the health of the ecosystem by evaluating participants' activities, providing rewards according to contribution, and sanctioning malicious behavior.

In short, this system performs the following functions.

- **Identity verification and eligibility check:** Confirms whether a participant is eligible to contribute to the PRODAO Mainnet.
- **AI-based abuse detection:** AI performs a first-pass filter to check whether there is anything suspicious in a contribution activity.
- **Contribution-score calculation:** Considering the participant's trustworthiness (based on reputation and VC), calculates and accumulates a score for the actual contribution.

- Application of abuse penalties: When abuse is confirmed, imposes penalties such as contribution-score reduction, staked-token slashing, and participation restrictions.
- Abuse-severity determination: Judges the severity of abuse based on reported data.

Definitions of Key Symbols and Variables

- P: A specific participant.
- A_i : Contribution activity type i .
- D_i : The detailed data of contribution activity i .
- $CS(P)$: The current total Contribution Score of participant P .
- $Rep(P)$: The current reputation score of participant P (range: $[0,1]$).
- $VC(P)$: The VC (Verifiable Credential)-based trust level of participant P (range: $[0,1]$).
- $SPROD(P)$: The quantity of PRODAO tokens staked by participant P .
- CA_{abuse} : The severity of confirmed abuse (e.g., 'LOW', 'MEDIUM', 'HIGH', 'CRITICAL').

Main Algorithm Functions and Formulas

Contribution-Activity Processing and Contribution-Score (CS) Calculation

Function: $f_{ProcessContribution}(P, A_i, D_i)$

This function defines the process of handling participant P 's contribution activity A_i and data D_i and updating the Contribution Score (CS).

- Identity and eligibility verification (DID/VC-based): $VDID(P) \in \{0,1\}$: validity of participant P 's DID (0 = invalid, 1 = valid). $VVC(P) \in \{0,1\}$: whether participant P holds a valid VC (0 = not held, 1 = held). Condition: unless $VDID(P) = 1$ and $VVC(P) = 1$ (or the minimum requirements are met), the contribution is rejected.
- AI-based initial abuse detection: $f_{AI}(D_i) \in [0,1]$: an AI-based quality/abuse-suspicion score for the contribution data D_i (the closer to 1, the more normal). Condition: if $f_{AI}(D_i) < TAI_Suspicion$, that contribution enters a REPORT_FOR_REVIEW state and awaits further review ($TAI_Suspicion$ is the AI suspicion threshold).
- Base activity score calculation: $S_{base}(A_i, D_i)$. A base score is calculated according to the type of each contribution activity A_i and the quantitative/qualitative metrics of the data D_i . Example: $S_{base}(\text{data provision}, D_{\text{data}}) = \alpha_1 \cdot (\text{data volume}) + \alpha_2 \cdot (\text{data quality})$.
- Trust coefficient calculation: $CTrust(P)$. Calculated by integrating participant P 's reputation score $Rep(P)$ and VC-based trust level $VC(P)$. $CTrust(P) = \beta_1 \cdot Rep(P) + \beta_2 \cdot VC(P)$ (where β_1, β_2 are DAO-defined weights). $CTrust(P) \in [0,1]$.
- Final activity contribution score calculation: $S_{final}(P, A_i, D_i) = S_{base}(A_i, D_i) \cdot CTrust(P)$. The final score is calculated by multiplying the base activity score by the participant's trust coefficient.
- Total Contribution Score (CS) update: Each contribution type A_i is assigned a weight $W(A_i)$ defined by DAO governance. $CS_{new}(P) = CS_{old}(P) + S_{final}(P, A_i, D_i) \cdot W(A_i)$. $CS(P)$

is updated on the blockchain.

Abuse-Penalty Application Function: $fApplyPenalty(P, CAbuse)$

This function applies penalties to a participant P for whom abuse has been confirmed, according to the severity $CAbuse$.

- CS (Contribution Score) reduction: $CS_{reduced}(P) = \max(0, CS(P) - \Delta CS(CAbuse))$. $\Delta CS(CAbuse)$: the amount of CS reduction according to severity (e.g., $k_1 \cdot CS(P)$ for 'LOW', $k_2 \cdot CS(P)$ for 'HIGH'). $k_1 < k_2 < \dots < k_N$ (DAO-defined ratios).
- Slashing of staked PROD tokens: $\Delta SPROD(CAbuse)$: the quantity of PROD tokens to be slashed according to severity. $SPROD_slashed(P) = SPROD(P) \cdot SlashingRate(CAbuse)$. $SlashingRate(CAbuse)$: 1.0 (100%) for 'CRITICAL', 0.5 (50%) for 'HIGH', etc. $PerformSlashing(P, SPROD_slashed(P))$: executes the forfeiture of tokens on the blockchain.
- Participation restriction: $BanType(CAbuse)$: the type of participation restriction according to severity (e.g., 'NONE', 'TEMPORARY', 'PERMANENT'). $SetParticipationBan(P, BanType(CAbuse))$: sets the participation-restriction state.
- Reputation-score update: $Repnew(P) = \max(0, Rep(P) - \Delta Rep(CAbuse))$. $\Delta Rep(CAbuse)$: the amount of reputation-score reduction according to severity.

Abuse-Detection and Severity-Determination Function: $fDetermineAbuseSeverity(P, Dreported)$

This function determines whether abuse has occurred and its severity by synthesizing AI-analysis results, community reports, cross-verification data, and the like. (This process proceeds through a combination of AI models, decentralized oracles, DAO governance voting, etc.)

- Input: P (participant), $Dreported$ (reported activity data).
- Output: $CAbuse \in \{'NONE', 'LOW', 'MEDIUM', 'HIGH', 'CRITICAL'\}$.
- Blockchain integration: The participants map should in practice be managed as a state variable of a blockchain smart contract, and data updates should be made through transactions.
- Oracle and AI integration: Functions such as $AI_Model.predictQualityScore$, $AI_Model.analyzeAbuse$, $DAO_Governance.getVoteResult$, and $DecentralizedOracle.verify$ require API integration with actual AI services, decentralized oracle networks, and the DAO governance system.
- Weights and thresholds: All weights and thresholds— α_1 , α_2 , β_1 , β_2 , $W(A_i)$, $TAI_Suspicion$, k_1 , k_2 , ..., $SlashingRate$, ΔRep , and so on—are designed to be flexibly adjustable through DAO governance.

4. Decentralized Identifier (DID) System

4.1. Definition and Importance of DID

A DID (Decentralized Identifier) is a new form of digital identity identifier generated on the basis of distributed-ledger technology (DLT) or another distributed system. Unlike existing centralized identity systems (e.g., website logins, national identification numbers, etc.), a DID is not subordinate to any specific institution or service provider; it allows an individual to create, manage, and control their own identity information themselves.

In the PRODAO ecosystem, DIDs are very important for the following reasons.

- **Securing data sovereignty:** A DID is a core tool that allows individual experts to exercise full ownership and control over their own data. They can clearly control who can access which information and when.
- **Strengthening privacy:** A DID makes it possible to authenticate identity or prove the validity of specific information without directly exposing an individual's sensitive information, thereby protecting privacy. It enables “selective disclosure,” sharing only the necessary information.
- **Interoperability:** A DID can smoothly interconnect with services and applications outside the PRODAO ecosystem. This allows PRODAO experts to use their identity and data across diverse Web3 environments.
- **Reliability and transparency:** Because a DID recorded on the blockchain cannot be tampered with, and the change history of identity information can be verified transparently, reliability is increased.
- **Intermediary-free authentication:** It enables direct identity authentication between individuals or between services without a centralized intermediary, reducing unnecessary cost and complexity.

4.2. Structure and Operation of the PRODAO DID System

The PRODAO DID system has the following key components and mode of operation.

- **DID (Decentralized Identifier):** A unique identifier for each individual expert, generated on the PRODAO Mainnet. Beyond an expert's verified credentials (VCs), degrees, records of participation in specific projects, and major achievements, it can also be issued as an NFT—a unique and immutable digital asset representing ownership of an expert's original creations such as unique digital art, music, design, 3D models, and other works.

- These NFTs are strongly linked to the expert's DID, proving that the expert is the actual creator and leaving an immutable on-chain record of the authenticity and ownership of the digital asset. This composes the expert's profile in a richer and more trustworthy way and protects the creator's rights.
- Use: NFT-ized creations and credentials are used to raise an expert's trustworthiness in employment, collaboration, and project participation, permanently recording the expert's achievements and creative activities in a tamper-proof form. This becomes an important element that represents an expert's reputation and trustworthiness within the PRODAO ecosystem in a visual and verifiable form.
- DID Document: A JSON-LD document containing metadata linked to a DID. This document includes the public key, service endpoints, and information related to “Verifiable Credentials” by which the DID owner can prove other claims in a cryptographic manner. DID documents are mainly stored off-chain, while the DID itself is recorded on-chain.
- Verifiable Credentials (VC): Data in which a specific institution (e.g., a university, a credential-issuing body, an employer) issues, encrypts, and signs an individual's identity information (e.g., degree, certification, career) in a digital manner. This VC is managed directly by the DID owner and, when necessary, can be presented to another party in the form of a Presentation to prove one's claims.
- Issuer: The entity that issues the VC (e.g., the PRODAO platform, an educational institution, a company).
- Holder: The individual (expert) who has a DID and owns and manages VCs.
- Verifier: The entity that receives and confirms the validity of a VC (e.g., a service provider, another expert).

How It Works

- DID creation and registration: The expert creates their DID on the PRODAO Mainnet and registers it on the blockchain.
- VC issuance: A university issues a graduation certificate as a VC and links it to the expert's DID. Alternatively, the PRODAO platform may issue a VC for an expert's specific activity (content creation, community contribution, etc.).
- VC storage and management: The expert (holder) stores their VCs in a personal wallet or distributed storage that securely manages them.
- VC Presentation: When an expert uses a specific service (e.g., a professional-knowledge-sharing service, a job platform), they selectively present the information required by that service (the verifier) in the form of a VC. At this time, only the minimum necessary information—not the individual's entire information—may be transmitted in encrypted form.
- VC verification: The service (verifier) verifies the validity of the presented VC (the validity of the issuer's signature, whether the content of the VC has been tampered with, etc.) through the DID information recorded on the blockchain.

4.3. DID-Based Data Sovereignty Management and Use Cases

PRODAO's DID system focuses on strengthening experts' data sovereignty.

- **Consent-based data use:** When an expert shares or uses data linked to their DID, explicit consent must always be obtained. Through smart contracts, the conditions for data access and use are clearly set, and the expert can withdraw their consent at any time.
- **Selective information disclosure:** Among the numerous pieces of information linked to their DID (education, career, field of expertise, project participation history, activity data, etc.), an expert can selectively disclose only the necessary parts. For example, when they wish to prove only a specific part of their career for participation in a particular project, they can keep other personal information private.
- **Data monetization:** Expert data managed on a DID basis can create value and be rewarded within the PRODAO ecosystem. For example, an expert can consent to providing data for AI-model training and receive PROD token rewards for it.
- **Personalized services:** Anonymized data collected with the expert's consent is analyzed through AI models and used to provide personalized services such as content recommendations, collaboration-opportunity matching, and learning-path suggestions tailored to the individual's interests and field of expertise.
- **Transparency of data-use history:** Through the DID system, an expert can transparently verify records of when, to whom, and for what purpose their data was used.

4.4. DID Security and Privacy Protection

PRODAO's DID system aims for the highest level of security and privacy protection.

- **Encryption technology:** All sensitive data is stored and transmitted using strong encryption technology. Through public-key encryption, the confidentiality and integrity of data are secured.
- **Distributed storage:** Sensitive data linked to a DID document is stored in encrypted form in a distributed storage system such as IPFS rather than on a central server. This removes single points of failure and minimizes the risk of data breaches.
- **Access control:** Through a sophisticated smart-contract-based access-control mechanism, the DID owner can finely set and manage access rights to their own data.
- **Non-deterministic DIDs:** PRODAO designs DIDs so that they do not include information that can identify a specific individual, and it strengthens privacy by applying the concept of “pairwise DIDs,” generating diverse DIDs as needed and using each only for a specific activity.

-
- **Auditability:** The DID change history recorded on-chain and the hash values of off-chain data provide auditability, raising the transparency and reliability of the system.
 - **Continuous security audits:** The smart contracts and protocols related to the DID system undergo regular external security audits to identify and remediate potential vulnerabilities.

5. AI Integration

The PRODAO ecosystem integrates artificial intelligence (AI) not as a mere add-on feature but as a fundamental driving force that creates the platform's core value, innovates the user experience, and maximizes the security and efficiency of the network. In particular, considering PRODAO's characteristic that user data is decentralized and preserved in a mobile Web3 P2P environment, AI is not a simple auxiliary tool but an important driving force that realizes PRODAO's core values of “enhancing data value” and “accompanying experts' growth.”

5.1. The Role of AI in the PRODAO Ecosystem and Its Fields of Application

AI performs diverse roles across the entire PRODAO ecosystem and is applied in the following core fields.

- Value enhancement and evaluation: Objectively evaluates and optimizes the value of distributed data, expert knowledge, content, and the AI models themselves, maximizing the efficiency of the PoC (Proof of Contribution) algorithm.
- Service optimization and personalization: Innovates the user experience and promotes interaction within the ecosystem through personalized information provision and efficient resource matching.
- Network security and integrity maintenance: Contributes to securing the safety and reliability of the network through abuse detection, anomaly detection, data-reliability verification, and the like.
- Knowledge discovery and insight extraction: Discovers new patterns and insights from vast, decentralized knowledge and data to support experts' decision-making.

5.2. Using AI to Enhance Data Value

Using AI, PRODAO maximizes the potential value of distributed data and builds a virtuous cycle that returns this value back to the ecosystem.

- Automated data curation and refinement: AI analyzes data collected through the P2P network or provided by users (metadata, attribute attestations, etc.) to automatically classify, tag, and structure it, and it contributes to refining data by identifying duplicate or abnormal data. This increases the efficiency of the data marketplace.
- Data value-evaluation model: AI algorithms analyze diverse attributes of data—such as its uniqueness, scarcity, freshness, accuracy, frequency of use, and provenance (DID/VC-based)—to calculate an objective value score for each dataset. This score is used as a core metric of the “MyData provision” contribution within the PoC algorithm.
- Privacy-preserving insight extraction: Rather than directly centralizing the raw data distributed on users' mobile phones, PRODAO uses PETs such as Federated Learning

and Homomorphic Encryption so that AI models extract collective insights, trends, and correlations from the data, thereby leveraging the collective value of the data while protecting individual privacy.

- Decentralized data aggregation and synthesis: Using only anonymized or zero-knowledge-proven data attributes, without sensitive information, AI generates large-scale, meaningful synthetic datasets or performs statistical aggregation to build the datasets needed for specific industries or research fields.

5.3. Personalized Services and Smart Matching

Through AI-based intelligent matching and personalization functions, PRODAO optimizes the user experience and improves the efficiency of resource allocation within the ecosystem.

The creation of AI personas provides customized services and smart matching so that PRODAO users can have experiences optimized for them. AI analyzes a user's contribution activities, content-consumption patterns, search history, collaboration history, and DID/VC-based expertise profile to build a dynamic "AI persona." Throughout this process, user consent and privacy-enhancing technologies are applied.

Smart Matching Functions

- Expert-user/project matching: Analyzes a user's questions and project requirements to recommend the most suitable experts in the relevant field (individual members or star clusters). AI comprehensively considers the experts' expertise, reputation, activity history, and more.
- Data-AI model/consumer matching: Recommends data providers (users) who hold a specific type of data needed for AI-model training to AI-model developers or data consumers; in this process, only the data attributes are verified through zero-knowledge proofs.
- Content recommendation and curation: Based on a user's interests, learning level, and past interactions, recommends personalized professional content, news, community discussions, and more, providing the most useful information to the user amid the flood of information.
- Discovering collaboration opportunities: AI analyzes the profiles and activities of diverse experts to discover potential collaboration opportunities and recommend teams that can create synergy.

5.4. AI Model Training and Management

PRODAO applies a decentralized approach across the entire life cycle of AI models (training, deployment, management, auditing) to secure transparency and fairness.

Decentralized AI Training (Federated Learning and Incentives)

- The core training of AI models within PRODAO is conducted mainly through Federated Learning. Rather than on a central server, an AI model is trained locally on each individual user's mobile device with their own data, and only the encrypted “change in model weights” is transmitted to the server to update the final model. In this process, the raw data never leaves the user's device.
- Participation in AI-model training by providing data is rewarded in PROD tokens in accordance with the PoC algorithm, inducing active participation.

AI Model Governance and On-Chain Management

- All AI models developed, deployed, and used within the PRODAO ecosystem are version-managed on-chain and are subject to the control of DAO governance. The addition of new AI models, updates to existing models, changes to key parameters, and the like are decided through votes by PROD token holders.
- This helps prevent the deployment of malicious AI models and secures the transparency and reliability of the models.

Model Evaluation and Auditing

- Evaluation and auditing of AI models' performance, fairness, bias, security vulnerabilities, and the like are conducted in a decentralized manner. Independent audit nodes or expert groups verify a model's behavior, and the results are recorded on-chain.
- PRODAO encourages open-source AI-model development and operates a community-based code-review and vulnerability-reporting system.

AI Model Marketplace

- PRODAO provides a decentralized marketplace where verified AI models (e.g., data-analysis models for specific fields, content-generation models) can be shared and traded. Model developers receive fair compensation for their model contributions, and other participants can use the AI functions they need.
- This contributes to increasing the liquidity and utilization of AI assets within the PRODAO ecosystem.

6. Tokenomics

The PRODAO ecosystem aims for sustainable growth and decentralized value creation through a robust token-economy model centered on the “PROD” token. Beyond being a mere digital asset, the PROD token drives all economic activity in the ecosystem, provides fair compensation for participants' contributions, and acts as the core driving force leading the platform's long-term development.

6.1. The Role and Utility of the PROD Token

As the “lifeline and economic engine” of the PRODAO ecosystem, the PROD token is the core utility token that connects the activities of all participants, creates value, and leads the platform's continuous growth.

6.1.1. PROD Token Details

The details of the PROD token are as follows.

- Token Name: PRODAO.
- Token Symbol: PROD.
- Total Supply: 10,000,000,000 PROD (10 billion). The total issuance of the PROD token is fixed in order to guarantee the token's scarcity and build a predictable token economy.
- Decimals: 18. 1 PROD token can be divided into 10^{18} minimum units, enabling precise transactions and reward payouts.
- Blockchain Network: PRODAO Mainnet. The PROD token is a native token issued and operated on PRODAO's own mainnet. This is to optimally support PRODAO's unique consensus algorithm (PoC) and specialized functions.
- Token Standard: Native token. Rather than following a specific external blockchain standard, the PROD token is a native token designed to be compatible (for example, with ERC-20) in accordance with the unique protocol and rules of the PRODAO Mainnet. However, wrapping functionality for cross-chain compatibility may be considered in the future as needed.

6.1.2. Key Utilities and Use Cases of the PROD Token

The PROD token is deeply integrated into the various services and functions of the PRODAO platform, inducing user participation and acting as a driving force for the sustainable growth of the ecosystem.

A2E (Add to Engagement) Rewards and Incentives

- It is a means of fair compensation for all contributions through which experts create value on the PRODAO platform. These are paid in accordance with the PoC (Proof of Contribution) algorithm.

- Examples of use: DID-based profile completion and verification, sharing of professional knowledge and content, Q&A; and forum activity, provision of personal data and consent to its use, participation in AI-model training, and more. In addition, when top-quality creative content such as digital art, design, or music is contributed to the PRODAO platform and gains high engagement or positive reactions, it may be linked to additional rewards in the form of NFTs or to PROD token incentives.

Network Transaction Fees (Gas Fees)

- Used as the gas fee for all transactions occurring on the PRODAO Mainnet (DID updates, execution of data-sharing contracts, smart-contract calls, etc.). A portion of these fees is burned.

Service Fees and Subscription Fees

- Used as a means of payment for paid services within the PRODAO platform (e.g., AI-matching fees, usage fees for advanced AI-persona features, costs for purchasing advertising slots, premium subscription fees, access rights to specific expert groups, communication/SNS features, etc.).

Data Access and Use

- When, with a specific expert's consent, one views or uses paid datasets such as anonymized personal data, professional research data, or know-how in the PRODAO data marketplace, one pays the relevant expert in PROD tokens.
- Used to pay subscription or usage fees for advanced analysis, prediction, and consulting services that use AI models trained on PRODAO's vast expert data.

Governance Participation

- PROD token holders can participate in the governance of PRODAO's Decentralized Autonomous Organization (DAO) and exercise voting rights on key decisions (e.g., algorithm changes, roadmap decisions, proposals to add services, advertising-slot policies, etc.). This ensures that the ecosystem develops through the collective intelligence of the community.

Staking

- To strengthen the stability and security of the network, PROD tokens are staked to participate as a Signer node (validator) or to provide collateral for specific services. Staking also contributes to increasing scarcity by reducing the circulating supply of the network.

NFT Issuance/Trading Costs

- Within the PRODAO ecosystem, PROD tokens may be used as fees when an expert issues intellectual assets such as their digital art, music, design, or exclusive datasets as NFTs, or when trading such NFTs on the marketplace.
- NFT-based premium services: Users who hold a specific NFT may be granted differentiated service benefits such as access to premium galleries within the PRODAO

platform, rights to use advanced AI models, or eligibility to join specific expert groups; PROD tokens are used to pay for these or when issuing the relevant NFT.

6.2. Details of the A2E (Add to Engagement) Reward Model

At the core of PRODAO's token economy is a virtuous cycle in which a user's "contribution" leads to a "reward," and the rewarded tokens are "utilized" within PRODAO services and thereby "recycled" again. The A2E model defines in detail the "contribution-reward" process that is the starting point of this cycle.

Contribution-Score (CS)-Based Rewards

- Every participant's contribution activity is measured as a Contribution Score (CS) in accordance with the PoC algorithm. The CS is calculated through composite metrics such as "activity volume," "expertise," "reliability," and "influence," and is directly linked to the distribution of PROD token rewards.
- Through abuse-prevention mechanisms, the improper acquisition of CS is prevented, and malicious behavior leads to CS reduction and token slashing.

Types of Rewarded Activities

- DID-based profile completion and verification: Rewards for activities that add MyData such as one's expertise, career, and education to one's DID and raise its trustworthiness through verification institutions.
- Sharing of professional knowledge and content: Paid when high-quality expert reports, articles, solutions, and the like are posted to PRODAO's Knowledge Hub and that content induces positive interaction such as views, likes, and comments.
- Q&A; and forum activity: Earn Contribution Score (CS) and rewards by answering questions in PRODAO's expert Q&A; or participating in meaningful discussions in the forums.
- Provision of personal data and consent to its use: Rewards that arise when a user provides anonymized personal data to the data marketplace with their consent and that data is used for AI-model training or other services.
- Participation in AI-model training: Rewards for activities that contribute to AI-model training on one's own device through Federated Learning and the like.
- Ecosystem verification and curation: Rewards for activities that verify other users' contributions (data, content, etc.) and curate high-quality information.
- Network operation (Signer node): Rewards for activities that contribute to block generation and transaction verification by participating as a Signer node of the PRODAO Mainnet.

Reward Cycle and Distribution

- PROD token rewards are distributed regularly (e.g., daily, weekly) from the A2E reward pool in proportion to the CS each participant has earned.
- The size of the reward pool and the distribution ratios can be transparently managed and adjusted through DAO governance.

6.3. Token Distribution and Supply Plan

The issuance model of the PROD token is designed to aim for the long-term stability and sustainable growth of the PRODAO ecosystem. The total supply of 10 billion (10,000,000,000 PROD) is issued at the same time as the creation of the genesis block and is distributed to each entity according to a pre-planned allocation. This distribution record is permanently recorded within the genesis block and disclosed transparently.

6.3.1. Token Allocation

Category	Ratio	Token Amount (PROD)	Purpose & Description
Network Operations	30%	3,000,000,000	Mainnet DAO operations; research, security & standards activities; infrastructure maintenance and long-term stability
Validator Incentives	20%	2,000,000,000	Validator rewards; consensus participation and PoC contribution; community incentives
Ecosystem & Developers	20%	2,000,000,000	Developer grants; L2 / DApp expansion; partner-ecosystem activation
Team & Core Contributors	15%	1,500,000,000	Early protocol design and technical contributors
Strategic Expansion	15%	1,500,000,000	Global expansion; AI & MyData research; strategic technology partnerships
Total	100%	10,000,000,000	Activation and operation of the PRODAO Mainnet ecosystem

- No investment, equity, or profit rights.

6.3.2. Initial Balances Within the Genesis File Structure

The genesis block of the PRODAO Mainnet is defined through a JSON-format genesis file. This file specifies the network's initial state and operating rules, and the addresses of all the initial allocation recipients defined above and the quantities of tokens to be allocated to those addresses are accurately recorded in the minimum unit, taking the Decimal setting into account. As the immutable first record of the PRODAO blockchain, this guarantees that all nodes can synchronize and operate the network from the same starting point.

6.4. Token Value Appreciation Mechanisms

With the total supply of the PROD token fixed at 10 billion, effective token-burning and redistribution mechanisms are essential to maintain the long-term value of the token and to promote the sustainable growth of the ecosystem. These mechanisms play an important role in systematically managing the circulating supply of the token and continuously promoting ecosystem activity.

6.4.1. Strategy for Supply-Demand Balance

- Continuous demand creation: Tokens that flow to users as A2E rewards are continuously recycled and consumed through diverse on-chain/off-chain activities such as paying network transaction fees, purchasing data/services (AI matching/personas, advertising, subscription fees, etc.), staking, and governance participation. The activation of the PRODAO ecosystem leads directly to an increase in demand for the PROD token.
- Circulating-supply management (Tokenomics design): The fixed total supply of 10 billion guarantees long-term scarcity. In addition, the vesting and lock-up schedules applied to the tokens of the team, advisors, early investors, and the like minimize the impact of a sudden increase in circulating supply on the market.

6.4.2. PROD Token Burning Mechanism

The burning of PROD tokens aims to gradually reduce the total supply to create deflationary pressure and to induce long-term value appreciation by increasing the token's scarcity.

Burn Targets and Sources

- A portion of network transaction fees: A certain proportion of the gas fees for all transactions occurring on the PRODAO Mainnet is permanently burned. This means that the more the network is used, the more tokens are burned, directly contributing to the token's value.
- A portion of PRODAO service fees: A certain proportion of the PROD revenue generated through paid services within the PRODAO platform (e.g., AI-matching fees, usage fees for advanced AI-persona features, costs for purchasing advertising slots, premium subscription fees, etc.) is burned. This is a key link through which the platform's business success leads directly to token value appreciation.
- A portion of tokens slashed from Signer nodes: A portion of the PROD tokens forfeited (slashed) from Signer nodes by the abuse-prevention mechanism is burned. This strengthens network security while simultaneously reducing the circulating supply.
- Burning method: The burning of PROD tokens is carried out by sending tokens to a burn address, making them permanently inaccessible. Burning is executed transparently on a periodic basis (e.g., monthly, quarterly) according to specific rules, through automated smart contracts or governance-approval procedures. All burn

records are disclosed on-chain so that anyone can verify them.

6.4.3. PROD Token Redistribution Mechanism

Token redistribution aims to promote continuous contribution and growth by distributing the non-burned inflowing tokens and the tokens of the reward pool to the diverse entities that activate the ecosystem.

Redistribution Targets and Sources

- The remaining portion of network transaction fees: The network fees remaining after burning are paid mainly to Signer nodes as an additional incentive beyond the block-generation reward, providing motivation for maintaining the network.
- The remaining portion of PRODAO service fees: The service fees remaining after burning are used mainly as continuous development and operating funds for PRODAO's core development and operations teams, or flow into the community treasury.
- The remaining portion of tokens slashed from Signer nodes: The slashed tokens remaining after burning flow into the community treasury or are reallocated to the A2E reward pool and used for contribution rewards.

These token-burning and redistribution mechanisms optimize the value flow of the PROD token and drive sustainable growth through the efficient allocation of resources within the ecosystem.

7. Smart Contracts and DApps

By providing an optimal environment for the development of robust and secure smart contracts, the PRODAO Mainnet enables developers to efficiently build and deploy innovative decentralized applications (DApps) on top of the PRODAO ecosystem. This is the core technical foundation for realizing PRODAO's decentralization vision.

7.1. PRODAO Smart Contract Development Environment

To induce the participation of a broad developer community and maximize development productivity, PRODAO provides the following smart-contract development environment.

- **Programming-language compatibility:** The PRODAO Mainnet supports EVM (Ethereum Virtual Machine)-compatible languages, especially Solidity, lowering the entry barrier for existing Ethereum developers. This allows a vast developer base to easily integrate into the PRODAO ecosystem.
- **Support for development tools and frameworks:** It provides compatibility with widely used smart-contract development frameworks and integrated development environments (IDEs) such as Truffle, Hardhat, and Remix, simplifying the development, testing, and debugging of smart contracts.
- **Stable testnet environment:** It provides a stable testnet environment for verifying the functionality of smart contracts and fixing potential bugs before mainnet deployment. Developers can safely experiment with and validate their code in this environment.
- **Comprehensive documentation and developer support:** It provides detailed and clear developer documentation, API references, and step-by-step tutorials so that developers can easily understand and use the features of the PRODAO Mainnet and how to write smart contracts. In addition, it operates an active developer community and dedicated support channels to help resolve technical issues.
- **Oracle solution integration:** It supports integration with Oracle solutions such as Chainlink that can securely bring real-time data from the external world (e.g., market prices, external events) onto the blockchain. This allows smart contracts to perform more complex functions interconnected with the real world.
- **Use of security libraries and standards:** It recommends and supports the use of verified smart-contract security libraries and standards such as OpenZeppelin. This is essential for developers to write secure and efficient contracts and to be protected from common vulnerabilities.

7.2. Smart Contracts for Implementing Key Platform Features

The core features of the PRODAO Mainnet are implemented in a decentralized and automated manner through smart contracts. This guarantees the platform's transparency and reliability, and direct, intermediary-free interaction among users.

- **PROD token contract:** Defines the basic token-economy functions such as minting, transferring, and burning of the PROD token. By complying with standard token specifications such as ERC-20 (or an equivalent native standard), it secures potential compatibility with other blockchain systems.
- **A2E (Add to Engagement) reward contract:** Implements the logic that automatically calculates and distributes PROD token rewards based on each user's Contribution Score (CS) in accordance with the PoC (Proof of Contribution) consensus algorithm. This is a core contract that guarantees the transparency and fairness of the reward process.
- **DID (Decentralized Identifier) contract:** A core contract that manages the registration, updating, and verification of experts' DIDs and the referencing of DID documents. By complying with the W3C DID standard, it raises the interoperability of the distributed identity system.
- **Staking and slashing contract:** Manages the PROD token staking of Signer nodes and other participants, and includes logic that automatically executes slashing when network-rule violations or malicious behavior occur. This strengthens network security and induces responsible behavior by nodes.
- **Governance contract:** Implements the core functions of PRODAO's Decentralized Autonomous Organization (DAO). It includes management of token holders' voting rights, proposal and voting processes, and logic for automatic execution according to voting results (e.g., protocol upgrades, parameter changes), enabling community-led operation of the ecosystem.
- **Data access and use contract:** Provides functions through which an expert sets and manages access rights to their own off-chain data and controls explicit consent to the use of the data. The logic for distributing PROD token rewards for data use may also be integrated into this contract.
- **Decentralized SNS contract:** A contract that records on-chain the hash values of core data related to basic social-network functions such as creating posts, writing comments, and “liking,” and that manages interaction among users in a decentralized manner.

7.3. PRODAO SDK and Developer Tools

PRODAO provides a powerful SDK (Software Development Kit) and a comprehensive set of developer tools so that developers can easily build innovative DApps on top of the PRODAO Mainnet and participate in the ecosystem. This is a core element that promotes the growth of the developer community and accelerates the expansion of the PRODAO ecosystem.

7.3.1. PRODAO SDK

The PRODAO SDK is a modular library designed to allow DApp developers to easily access and integrate the core functions of the PRODAO Mainnet.

- **Blockchain interaction API:** Provides a standardized API for efficient interaction with the PRODAO Mainnet. Through it, developers can easily perform blockchain-related tasks such as token transfers, smart-contract calls, and transaction signing.
- **DID module:** Provides a module that allows functions related to DID creation, management, and VC (Verifiable Credential) issuance and verification to be easily integrated into a DApp, accelerating the development speed of DID-based applications.
- **A2E reward module:** Supports integration, in conjunction with PRODAO's A2E reward system, of functions that measure a user's contribution within a DApp and calculate PoC-based PROD token rewards.
- **Smart-contract interfaces:** Provides type definitions and convenient interfaces for interacting with the key smart contracts deployed on the PRODAO Mainnet (e.g., the token contract, the governance contract), improving development convenience.

7.3.2. Developer Tools

In addition to the SDK, PRODAO provides various auxiliary tools to improve developer productivity.

- **CLI (Command Line Interface) tool:** Provides a powerful command-line tool that can be used to interact with the PRODAO Mainnet and to deploy and test smart contracts in a terminal environment.
- **IDE (Integrated Development Environment) plugins:** Develops plugins for widely used IDEs such as Visual Studio Code to more conveniently integrate the writing, syntax highlighting, debugging, and deployment of smart-contract code.
- **Testnet and Faucet:** Provides a stable testnet environment in which developers can test DApps and experiment with network functions without consuming real tokens, along with a Faucet that makes it easy to obtain test tokens.
- **Detailed documentation and tutorials:** Provides detailed developer documentation, code examples, and step-by-step tutorials so that even novice developers can start easily, and these are continuously updated.

- Developer community and support channels: Operates active developer-community channels such as GitHub and Discord so that developers can share information with one another and receive support for resolving technical issues.

By using the PRODAO SDK and these developer tools, developers can easily integrate the powerful decentralization features of the PRODAO Mainnet into their own DApps and quickly provide innovative services to users, contributing to the expansion of the ecosystem.

7.4. Security Audits and Vulnerability Management

The security of smart contracts is the most important element for the reliability and sustainability of the blockchain ecosystem. To secure the security of deployed smart contracts and proactively manage potential vulnerabilities, PRODAO implements the following rigorous procedures and policies.

Regular Code Audits

- Internal audits: The PRODAO development team performs its own security audits from the smart-contract development stage, using rigorous code review and static/dynamic analysis tools.
- External expert audits: Before mainnet deployment, and whenever there are major protocol updates and contract deployments, PRODAO always commissions an independent external security audit from a specialized blockchain-security firm. This is essential for identifying and removing known vulnerabilities such as reentrancy attacks, integer overflow/underflow, and access-control issues. All audit reports may be disclosed transparently.
- Continuous security monitoring: For deployed smart contracts, PRODAO analyzes and monitors on-chain data in real time to detect abnormal activity or signs of potential attacks at an early stage.
- Bug Bounty Program: PRODAO operates a bug bounty program that pays appropriate rewards when ethical hackers and security researchers discover and responsibly report vulnerabilities in PRODAO's smart contracts and systems. This is an effective method of strengthening security by leveraging the collective intelligence of the community.
- Incident Response Plan: In preparation for the occurrence of serious security vulnerabilities or actual attacks, PRODAO establishes a clear and rapid incident-response plan to minimize damage and quickly recover the system. This includes communication protocols, recovery procedures, and more.
- Open-source and standards compliance: As much as possible, PRODAO develops smart contracts based on code with already proven high safety, using broadly verified open-source libraries such as OpenZeppelin and ERC standards.
- Version management and upgradeability: All smart contracts undergo rigorous version management and are designed using modularization, proxy patterns, and the like so

that upgrades for future bug fixes or feature improvements are possible. (Upgradeable contracts require additional security audits and governance-approval procedures.)

8. Governance

In its early stage, PRODAO performs the role of a core operations team for building a robust protocol and activating the ecosystem, but it ultimately aims to transition to a transparent, fair, and community-led Decentralized Autonomous Organization (DAO). This is to guarantee the long-term sustainability and democratic development of the platform. PRODAO's governance model presents principles and procedures designed in accordance with this forward-looking goal.

8.1. PRODAO Decentralized Autonomous Organization (DAO) Structure

PRODAO aims to gradually transition to a DAO structure operated by the collective intelligence of the community, without the control of a single central authority. This structure will implement a transparent and automated decision-making process using blockchain technology.

- Core principle: PRODAO aims for full decentralization in which all important protocol changes, fund executions, policy decisions, and the like are ultimately made through votes by token holders.

Key Participating Entities (After Transition)

- PROD token holders: As the most fundamental participants in PRODAO governance, they will exercise voting rights in proportion to the amount of PROD tokens they hold or stake.
- Signer nodes: As core entities participating in block generation and transaction verification on the PRODAO Mainnet, they may have greater influence in specific decisions in recognition of their contribution to network operation.
- Expert star clusters and stars: “Star clusters” (expert groups) and “stars” (individual experts) may play important roles in proposal creation, in-depth discussion, or voting on specific technical/professional fields, based on their specialized knowledge and contribution score (CS) in a particular field.
- Governance smart contract: Records the rules and execution logic of all governance processes on-chain, guaranteeing automatic execution according to voting results.
- Community treasury: A fund pool under the control of the DAO, to be used to fund various projects approved by the community.

8.2. Token-Holder-Based Voting and Decision-Making Process

PRODAO's final decisions will be made through a systematic voting process based on the PROD token.

Proposal Creation

- A participant who holds a certain amount of PROD tokens or more, or who meets a specific Contribution Score (CS), can create a PRODAO Improvement Proposal (PIP).

Discussion & Feedback

- Submitted proposals are publicly discussed in community channels such as the official forum, and the proposal may be improved during this process.

Voting Initiation & Period

- The final, revised proposal—after sufficient discussion—is put to an on-chain vote, and during a designated period PROD token holders use their tokens to express approval or disapproval. Voting power is proportional to the amount of PROD tokens held/staked.

Result Tallying & Execution

- After the voting period ends, a proposal that meets a specific quorum and approval threshold is deemed to have passed. A passed proposal is either automatically executed by the governance smart contract (on-chain changes) or carried out through the DAO's multi-signature wallet (off-chain activities).

8.3. On-Chain / Off-Chain Governance Model

Pursuing both efficiency and security, PRODAO plans to adopt a hybrid approach that combines on-chain and off-chain governance models in the future.

8.3.1. On-Chain Governance

- Characteristics: Recorded directly on the blockchain and immutable, with voting results automatically enforced through smart contracts. Provides high transparency and security.
- Fields of application: Applied to major changes that form the foundation of the ecosystem, such as core protocol changes (e.g., adjusting PoC algorithm parameters), smart-contract upgrades, large-scale fund executions, and token-economy adjustments.
- Mechanism: Uses a voting system based directly on the on-chain holdings of PROD tokens.

8.3.2. Off-Chain Governance

- Characteristics: A decision-making process that takes place outside the blockchain; it is flexible, low-cost, and facilitates complex discussion and the gathering of diverse opinions.
- Fields of application: Used for decisions that do not require immediate on-chain execution, such as ideation and initial proposals, detailed discussion and proposal improvement, and small-scale community initiatives.

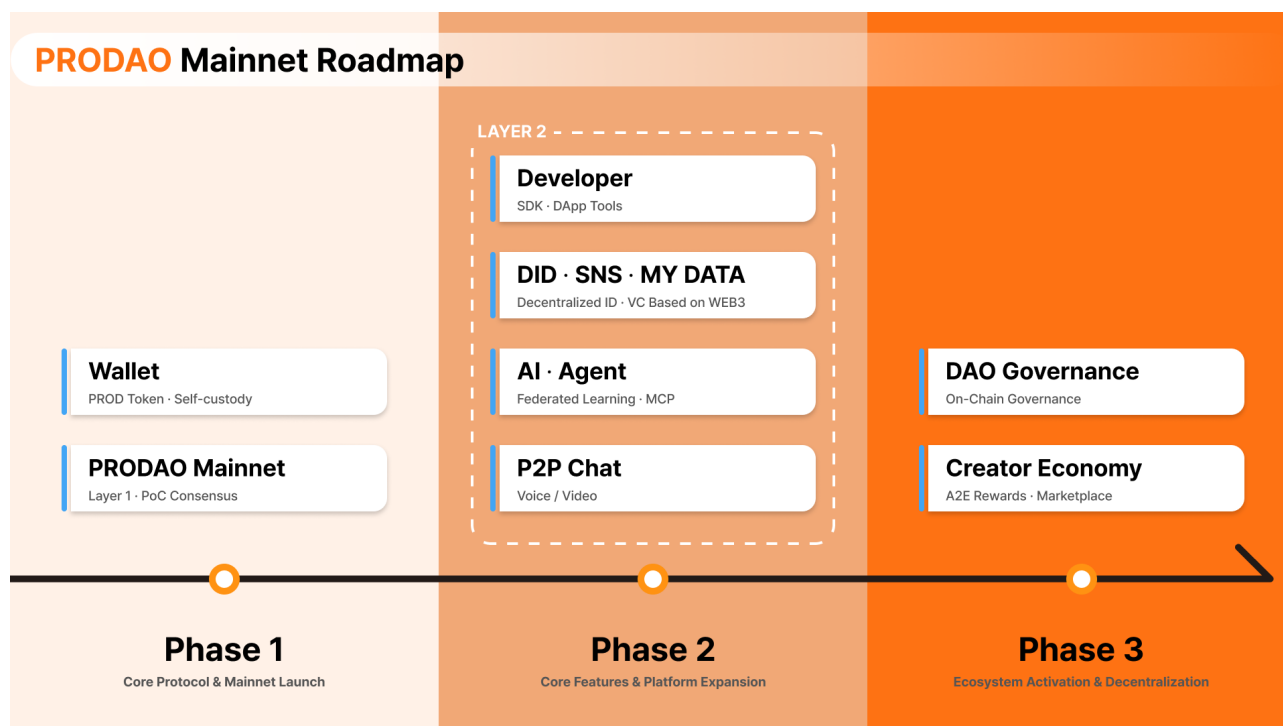
- Mechanism: Gathers public opinion mainly using off-chain voting tools such as the PRODAO forum, Discord channels, or Snapshot.

8.3.3. On-Chain / Off-Chain Interaction

PRODAO's governance model will adopt an approach in which the completeness of proposals is raised through off-chain discussion and consensus, and only validated proposals are ultimately put to an on-chain vote. This reduces unnecessary on-chain transaction costs and induces careful decision-making through sufficient prior review.

This hybrid model will be a core strategy of PRODAO governance, maintaining the principle of decentralization while simultaneously pursuing the efficiency and agile development of the ecosystem.

9. Roadmap and Future Plans



PRODAO begins with secure P2P communication and evolves into a next-generation decentralized ecosystem that unifies DID-based digital identity, AI services, developer platforms, and enterprise applications on a single Layer 1 blockchain.

PRODAO's roadmap focuses on realizing the vision of “a galaxy in which every activity of an expert becomes value” through core technology development, ecosystem activation, and a gradual transition to decentralization. Each phase builds on the success of the previous phase and will increase the value of the platform through continuous innovation and community participation.

9.1. Key Milestones by Development Phase

PRODAO's development will proceed through the following major phases.

9.1.1. Phase 1: Core Protocol Development & PRODAO Mainnet Launch

- Completion of PRODAO Mainnet (Layer 1) development: Building a proprietary high-performance blockchain architecture and basic infrastructure.
- Implementation and initial stabilization of the PoC (Proof of Contribution) consensus algorithm: Development of the core logic of the contribution-proof-based reward system and its application to the testnet.
- Deployment of core smart contracts: Deployment of the PROD token contract, the basic DID (Decentralized Identifier) contract, and the initial staking and A2E reward contracts.

- Public testnet launch: Operation of a public testnet to gather tests and feedback from developers and the early community.
- Official PRODAO Mainnet launch: Operation of the mainnet based on the stabilized protocol and issuance of the PROD token.

9.1.2. Phase 2: Core Feature Implementation & Platform Expansion

- Implementation of advanced smart contracts: A complete DID ecosystem including VCs (Verifiable Credentials), a sophisticated A2E reward contract for AI-integrated PoC, and evolved staking and governance contracts.
- AI integration and service expansion: Integration of initial AI models for data value evaluation, personalized matching, abuse prevention, and more. Building and applying Federated Learning infrastructure.
- Development and release of major DApps: Beta release of PRODAO's core DApps such as the Knowledge Hub, expert Q&A, and the data marketplace.
- Release of the PRODAO SDK and developer tools: Provision of a comprehensive SDK, CLI tools, IDE plugins, and detailed documentation and tutorials for DApp developers.

9.1.3. Phase 3: Ecosystem Activation & Deepening Decentralization

- Advancement of AI services: Expansion of AI-persona functions, activation of the AI-model marketplace, and introduction of more complex AI-based analysis and consulting services.
- Gradual transition to DAO governance: Phased transition to a complete on-chain governance system based on PROD token holders, and strengthening of the DAO community's decision-making authority.
- Global ecosystem expansion: Service localization, multilingual support, and operation of onboarding programs for international experts and communities.
- Strengthening strategic partnerships: Data integration and service expansion through cooperation with companies and institutions across various industries and with technology partners.
- Strengthening interoperability: Review of the introduction of cross-chain bridges or interoperability solutions with other blockchain networks.

9.2. Ecosystem Activation Strategy

For sustainable growth, PRODAO will pursue the following multifaceted ecosystem-activation strategy.

- Optimization of the A2E (Add to Engagement) reward model: Through the continuous advancement of the PoC algorithm, PRODAO clarifies rewards for high-quality

contributions and thereby induces users' active participation and value creation.

- Expert onboarding program: Provides customized onboarding programs and incentives to cultivate “star clusters” by specific industry, securing and activating high-quality expert groups.
- Nurturing the DApp ecosystem: Provides development grants, hackathons, technical mentoring, and more so that external developers can build innovative DApps on the PRODAO Mainnet, creating a rich application ecosystem.
- Enhancing content and data liquidity: Continuously improves intuitive platform features that allow experts to easily share their knowledge and data and other participants to consume it efficiently, activating the flow of content and data within the ecosystem.
- Continuous UX/UI improvement: Provides a user-friendly interface and an intuitive user experience (UX) so that even users unfamiliar with blockchain can easily use the PRODAO platform.
- Web2-Web3 bridging: Develops technical and business strategies that can smoothly channel existing Web2-based expert communities and data sources into the PRODAO ecosystem.

9.3. Partnership and Community Expansion Plan

Aiming for an open ecosystem, PRODAO will expand the platform's influence through diverse partnerships and the building of a strong global community.

9.3.1. Strategic Partnerships

- Corporate and institutional partnerships: Cooperates with research institutions, universities, and industry-leading companies to pursue professional-data integration, joint AI-model development, the building of proof-of-concept cases, and the expansion of the expert network.
- Technology partnerships: Strengthens the technical capabilities and stability of the PRODAO Mainnet through cooperation with blockchain-infrastructure providers, oracle-service providers, privacy-enhancing-technology (PETs) specialist firms, and the like.
- Media and influencer partnerships: Cooperates with major blockchain and technology media and influential figures to widely promote PRODAO's vision and value and to attract potential users.

9.3.2. Global Community Expansion

- Building regional communities: Builds a PRODAO ambassador program and regional communities in major regions around the world to encourage active participation by local experts and users.

- Education and mentoring programs: Through the “Starlight Scholarship,” provides mentoring and scholarships to talented people in IT and science, and through the “Galactic Social Hackathon,” supports the development of solutions that contribute to solving social problems, thereby creating social value for the ecosystem and cultivating talent.
- Participation in and hosting of global conferences and events: Participates in major blockchain and AI conferences and hosts its own online/offline events to promote PRODAO's technical capabilities and vision worldwide.
- Open-source contribution and cooperation: Actively contributes to and cooperates with relevant open-source projects in the blockchain and AI fields, contributing to the development of the overall technology ecosystem and building PRODAO's technical reputation.

10. Network and Data Security

Because the PRODAO Mainnet must stably support core features such as decentralized expert services, the A2E reward system, and DID-based MyData, network security is an element that must be secured as the highest priority. To protect the network from various cyberattacks and system errors and to keep user assets safe, PRODAO establishes and executes a systematic vulnerability-analysis and response strategy.

10.1. Network Security Vulnerability Analysis and Response

The PRODAO Mainnet establishes comprehensive and advanced measures to maximize the security of the network layer and to proactively respond to potential vulnerabilities.

- **Optimal network architecture:** Through an architecture with highly distributed node deployment and strong redundancy, the PRODAO Mainnet fundamentally blocks single points of failure and secures the highest level of resistance to DDoS (Distributed Denial of Service) attacks and Sybil attacks.
- **Leading consensus-mechanism security:** Through its unique characteristic of being based on the contributions of network participants, PRODAO's PoC (Proof of Contribution) consensus algorithm provides strong resistance to certain types of attacks that existing PoW (Proof of Work)- or PoS (Proof of Stake)-based networks may face. In addition, upon detecting malicious behavior, it firmly ensures network integrity through an immediate slashing mechanism.
- **Regular penetration testing and in-depth vulnerability analysis:** Through cooperation with world-class security specialist institutions, PRODAO performs regular penetration testing and in-depth vulnerability analysis of the PRODAO Mainnet's network infrastructure, protocols, and all inter-node communication paths to identify and remove potential threats in advance.
- **Intelligent security monitoring and rapid updates:** Using AI-based systems, PRODAO monitors network traffic, node status, anomalies, and the like in real time to immediately detect and respond to potential threats. Discovered vulnerabilities are patched quickly as the top priority, and updates are deployed after rigorous verification procedures, maintaining optimal security stability.
- **Top-level secure communication and node management:** All inter-node communication is fully protected through strong encryption protocols. In addition, PRODAO provides Signer node operators with the highest level of clear guidelines for strengthening hardware and software security, further raising the security level of the entire network.
- **Proactive incident response plan:** PRODAO establishes a clear and efficient Incident Response Plan to minimize damage and quickly recover the system in the event of a network security incident, and strengthens its response capabilities through periodic

drills.

10.2. Smart Contract Security Audit Plan

All of PRODAO's core smart contracts implement a systematic, multi-layered audit plan to guarantee the highest level of security integrity. (For the detailed methodology, see 7.4. Security Audits and Vulnerability Management.)

- Complete pre-deployment security audits: Before the PRODAO Mainnet launch, and before all core smart contracts are deployed, PRODAO always commissions a comprehensive security audit from an independent external specialist audit institution with a high reputation in the field of blockchain security. This focuses on perfectly identifying and removing all known vulnerabilities—such as reentrancy attacks, integer overflow/underflow, and access-control issues—in advance.
- Continuous re-auditing and ongoing review: When platform features are expanded or smart contracts are updated, PRODAO performs a rigorous re-audit of the relevant contract, and it also conducts periodic security checks and in-depth code reviews of already deployed contracts to actively respond to the latest security threats.
- Operating a global bug bounty program: PRODAO permanently operates a bug bounty program that pays exceptional rewards when ethical hackers and security researchers around the world discover and responsibly report potential vulnerabilities in PRODAO smart contracts. This is an effective method of innovatively strengthening security by leveraging the collective intelligence of the global security community.
- Transparent disclosure of audit reports: PRODAO transparently discloses the external audit reports of its core smart contracts to secure the community's trust and to raise the verifiability of PRODAO's security to the highest level.
- Compliance with proven best practices and global standards: By actively using broadly verified open-source security libraries such as OpenZeppelin and thoroughly complying with global best practices and standards in smart-contract development and security, PRODAO maximizes the stability and reliability of its code.

10.3. Data Protection and Privacy Security Policy

PRODAO prioritizes the safe protection of experts' sensitive data and personal information, and it makes it a core principle to firmly guarantee users full control over their own data.

- Realizing DID-based data sovereignty: All of a user's identity information and personal data is managed on a DID basis, and the user has absolute ownership and control over their own data. Sensitive data is not stored directly on-chain; only the data's hash value or reference information is recorded on the blockchain, perfectly guaranteeing the integrity of the data.
- Consent-based data-use principle: No user data is used within the PRODAO platform or provided externally without explicit, granular consent. The data access and use

contract manages the user's consent process with perfect transparency and provides a powerful mechanism to withdraw consent at any time.

- Strong encryption and strict access control: All sensitive data (stored off-chain) shared within the PRODAO ecosystem with user consent is protected by applying the highest level of encryption protocols both in transit and at rest. In addition, PRODAO strictly enforces role-based access control and the principle of least privilege to thoroughly restrict data access.
- Proactive data anonymization and pseudonymization: Datasets that may be used in the data marketplace and elsewhere undergo thorough anonymization or pseudonymization so that individual identification is impossible. This is a core mechanism of PRODAO that maximizes data utility while perfectly guaranteeing privacy protection.
- Introduction of leading privacy-enhancing technologies (PETs): By actively introducing cutting-edge privacy-enhancing technologies such as Federated Learning, PRODAO enables AI models to be trained and analyzed without centralizing the original data, fundamentally blocking the risk of personal-information leakage and presenting a new paradigm of data use.
- Global regulatory compliance: PRODAO thoroughly complies with all relevant legal requirements and international standards, including GDPR (General Data Protection Regulation) and related national data-protection laws, to protect user data and firmly establish PRODAO's legal responsibility and reliability.
- Raising security awareness and education: PRODAO conducts regular and in-depth security education for the PRODAO team, Signer node operators, and community members to raise awareness of the latest security threats and to mandate compliance with PRODAO's strong security policies.

11. Disclaimer and Risk Warning

This whitepaper has been prepared to aid understanding of the PRODAO project and cannot, under any circumstances, be regarded as investment solicitation, legal advice, tax advice, or any other professional advice. You must fully recognize and carefully judge the potential risks that may arise in connection with participating in the PRODAO ecosystem and purchasing PROD tokens.

11.1. Immutability and Limitations of the Information in This Whitepaper

The information contained in this whitepaper reflects the plans and intentions as of the time of writing and may change at any time depending on future market conditions, technological developments, changes in the regulatory environment, the project's progress, and the like. Nothing stated in this whitepaper guarantees the final outcome or a definitive plan of the project. The PRODAO team is under no obligation to update the contents of the whitepaper, and the latest information must be confirmed through PRODAO's official website and announcement channels.

11.2. Technical Risks

PRODAO is built on innovative blockchain and AI technologies. However, these new technologies carry the following inherent risks.

- **Smart-contract vulnerabilities:** Although the smart contracts composing the PRODAO Mainnet undergo thorough security audits, the possibility of unexpected bugs, vulnerabilities, or hacking attacks always exists. This can lead to token loss, malfunction of features, or system paralysis.
- **Network security risks:** The PRODAO Mainnet may be exposed to various network attacks (e.g., 51% attacks, DoS/DDoS attacks, Sybil attacks), which can affect the stability and availability of the network.
- **Uncertainty of technical implementation:** The technical vision and roadmap presented in this whitepaper may not be fully implemented as planned. Unexpected technical difficulties, development delays, or changes to core features may occur.
- **Data privacy and security risks:** In the process of handling MyData and personal information, there is a risk of data leakage, misuse, or abuse, and perfect defense against these is not guaranteed.

11.3. Market and Economic Considerations and Response Strategy

The PROD token and the overall virtual-asset market inherently carry high volatility and have hard-to-predict characteristics. PRODAO closely recognizes these market and economic characteristics and establishes a multifaceted and innovative strategy to successfully navigate them, strongly promoting the long-term stability and value growth of the platform.

- **Market price volatility:** The value of the PROD token may fluctuate due to various external factors such as market supply and demand, the progress of the PRODAO project's technology development and ecosystem activation, macro trends in the virtual-asset market, and regulatory changes. To respond to this volatility, PRODAO continuously strengthens the token's core utilities (A2E rewards, service fees, governance participation, etc.) and broadly expands actual use cases within the ecosystem, thereby firmly building intrinsic resistance to external market volatility. PRODAO's proprietary PoC (Proof of Contribution) consensus algorithm and its AI-based, differentiated value-creation model will create continuous demand for the token, decisively contributing to long-term value stabilization.
- **Liquidity management:** PRODAO recognizes that the market liquidity of the PROD token may be limited in the early stage. To address this, PRODAO plans to actively pursue listings on major global cryptocurrency exchanges after the mainnet launch and to support the formation of healthy liquidity pools, continuously expanding market accessibility. In addition, by having the token actively circulate within the PRODAO ecosystem in diverse forms such as knowledge sharing, data purchases, and AI-service use, PRODAO will strongly create its own demand for liquidity.
- **Securing competitive advantage:** Intensifying competition with blockchain projects that have a similar vision, or with existing large-scale centralized platforms, is unavoidable. However, through its clearly differentiated strengths—the technical capabilities of the proprietary PRODAO Mainnet (Layer 1), the innovative PoC-based A2E model integrating AI technology and DID, and the building of a highly specialized, expert-centric decentralized ecosystem—PRODAO will secure a distinctive position in the market and continuously strengthen an overwhelming competitive advantage.
- **Value creation and reward transparency:** The PROD token is not a security for investment purposes and does not guarantee any form of profit. A2E rewards are fair compensation and a strong incentive for participation in and contribution to the ecosystem, and their value may fluctuate according to market conditions and ecosystem performance. Rather than the token's speculative nature, PRODAO makes real value creation through ecosystem participation and the continuous growth of the community its core goals, maintaining the healthiest and most transparent tokenomics.

11.4. Regulatory and Legal Environment Analysis and Proactive Response Strategy

The global regulatory environment for virtual assets and blockchain technology is dynamically evolving, and policy changes by each government may occur unpredictably. PRODAO recognizes that such changes in the regulatory and legal environment may have a significant impact on its operation and development. To minimize these potential risks and secure the long-term stability of the platform, PRODAO strongly executes a proactive and active response strategy.

- Close monitoring of the regulatory environment: Laws and regulations regarding blockchain technology and virtual assets are continuously evolving worldwide, and in many cases clear standards have not been established. To respond to this regulatory uncertainty, PRODAO closely cooperates with global legal experts and international advisory groups well-versed in the blockchain and virtual-asset fields to closely monitor and deeply analyze the regulatory trends of all major jurisdictions.
- Flexible response to changes in laws and policies: The enactment of new laws, the amendment of existing laws, or changes in regulators' interpretations may affect PRODAO's method of service provision, token operation, and even the legality of the project. PRODAO will quickly and effectively adjust the platform's functions and operating methods so that it can respond proactively and flexibly to any regulatory change, fully complying with all relevant laws and regulations.
- Establishing global compliance principles: Not limited to the laws of a single country, PRODAO establishes and implements a strong strategy to comply, at the highest level, with all relevant regulatory and legal requirements of major jurisdictions worldwide where it may provide services or where the token may circulate. This includes AML (Anti-Money Laundering), CFT (Combating the Financing of Terrorism), and KYC (Know Your Customer) policies, providing a solid foundation for the project's long-term reliability and global expansion.
- Use of top-level legal counsel: PRODAO strategically cooperates with leading legal advisory firms specialized in the blockchain and virtual-asset fields to ensure that all business decisions and technical implementations are made in a direction that minimizes legal risk. Through this, PRODAO perfectly builds a proactive response system for regulatory changes and most effectively manages potential legal risks.

11.5. Operational and Management Risks

PRODAO also considers risks that may arise in the process of its operation and management.

- Team-capability and attrition risk: The departure of the core development team or management, or a lack of capability, can cause significant setbacks to project development and operation.

- Partnership risk: The partnerships specified in this whitepaper may not proceed as expected, or problems with partner companies may negatively affect the development of the PRODAO ecosystem.
- Governance risk: A decentralized governance model may face unexpected problems in its early stage (e.g., low participation rates, the passing of malicious proposals, community fragmentation).

PRODAO will do its best to address all potential risks related to the project, including those specified above, but does not guarantee that these risk factors are always controllable or can be completely eliminated.

END.