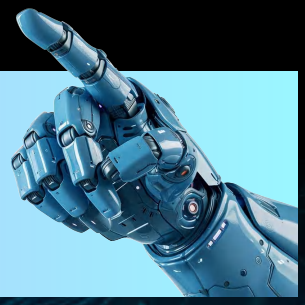
KLWEVGIP (KWP)

WHITE PAPER

Building a decentralized identity and data sovereignty infrastructure for next-generation Web3.0



Klwevgip is committed to building a global basic network with decentralized identity (DID), private data sovereignty, cross-chain interoperability and verifiable AI as its core.

Here, identity is trusted, data is self-controlled, and value flows freely, thus reconstructing the future of Web3.0.

Version: V2.2. 0

Release date: 2025

Klwevgip Foundation

CATALOGUE

KLWEVGIP (KWP)

6. Development Roadmap

6.1 Startup and early stages

6.2 Short-term development planning

6.3 Medium-term expansion route

6.4 Long-term ecological vision

7. Ecosystems and partners

7.1 Ecosystem composition

7.2 Core application scenarios

7.3 Eco-partner matrix

7.4 Community and Developer Program

8. Risk assessment and mitigation measures

8.1 Technical risks

8.2 Market risk

Legal and compliance risks

8.4 Governance and operational risks

8.5 Risk Mitigation Strategies

9. Conclusions and future prospects

9.1 Summary of project core values

9.2 Potential impact under the Web3.0 landscape

9.3 Long-term development direction

10. Appendix

10.1 Description of Terms

10.2 Technical Standard Reference

10.3 Model Parameters Appendix

10.4 Disclaimer

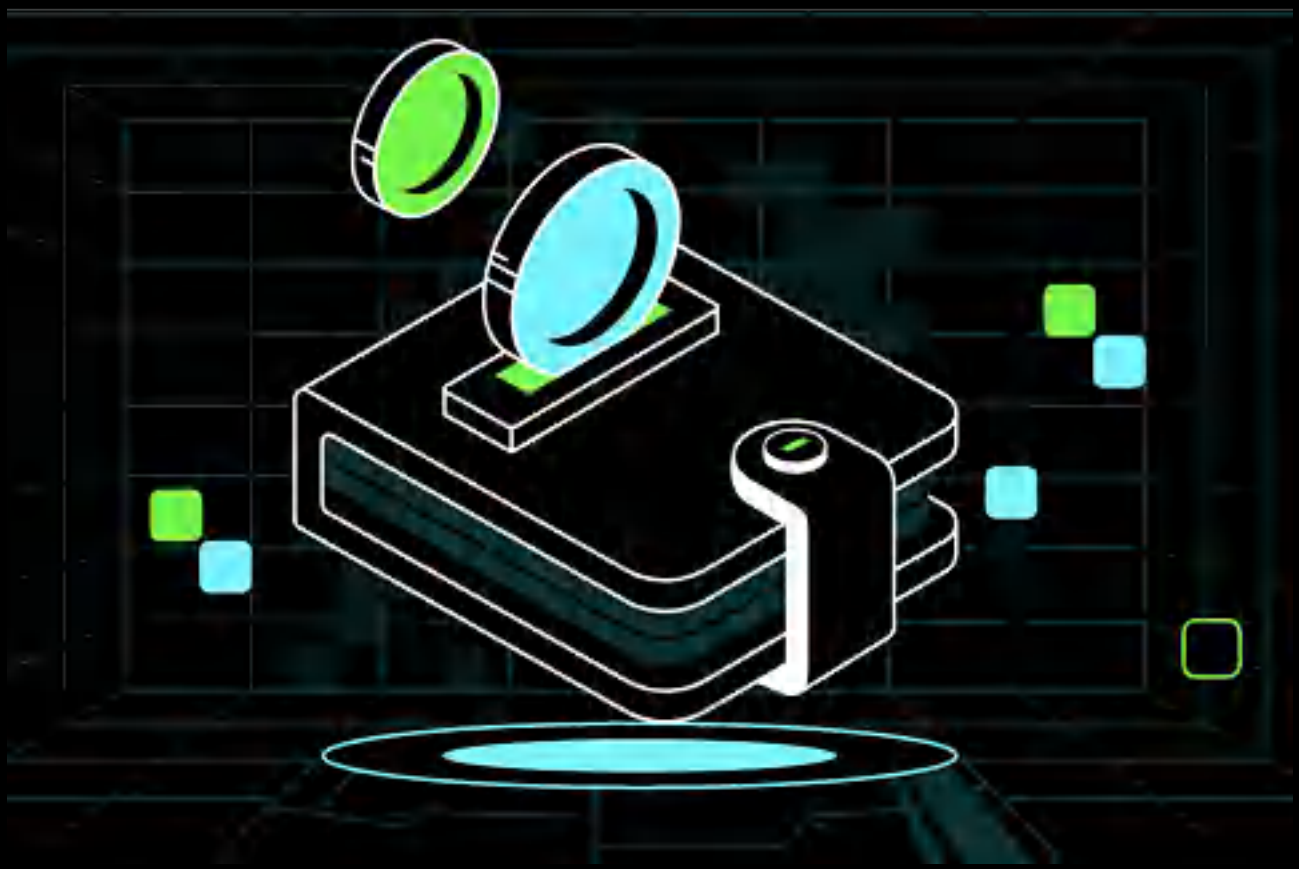
KLWEVGTP (KWP)

Abstract

Abstract

Klwevgip is an infrastructure network for the next generation of Web3.0, aiming to build a unified decentralized identity system, a trusted data sovereignty framework, and an AI-driven intelligent collaboration layer for developers and enterprises around the world. With the rapid development of Web3.0, identity fragmentation, lack of data ownership, cross-chain interoperability barriers, and trust boundaries between privacy computing and AI continue to expand. Klwevgip proposes a solution with a new system architecture, with the goal of becoming the comprehensive base of the "trusted identity layer + data control layer + AI collaboration layer" of the Web3 ecosystem.

As the core asset of network operation, the project token KWP (total amount 30 billion, initial price $0.00025) is used for key links such as resource consumption, identity verification, data authorization, AI service payment, governance voting, and node incentives, forming a sustainable and sustainable growth economic closed loop.



1. Introduction: Challenges And Vision

- 1.1 Web3.0 The background of the times
- 1.2 Core problems existing in the current blockchain
- 1.3 Data sovereignty and identity fragmentation challenges
- 1.4 Klwevgip's mission and vision

1. Introduction: Challenges And Vision

1.1 Web3.0 The background of the times

The Internet is moving from read-only (Web1.0) to interactive (Web2.0), and ultimately towards ownable decentralized networks (Web3.0). The core idea of Web3.0 is that users have sovereignty over assets, identities and data. However, in actual implementation, there are still major problems such as technology fragmentation, identity islands, and difficulty in protecting privacy.

In the era of data-driven AI, how to ensure that users have control over their own data? How to ensure that key behaviors such as privacy computing, AI scheduling, and identity verification have a trustworthy foundation that is transparent, fair, and cannot be tampered with? This is the core problem that has not been solved in the current global technology industry.

1.2 Core bottlenecks of blockchain infrastructure

Although blockchain has huge advantages in transparency and security, it still faces the following challenges when implemented at the production level:

Trust break caused by identity fragmentation

Users have different identities on different platforms, so it is difficult to dispatch data uniformly and verify the authenticity.

Data ownership cannot be implemented

Although users have rights at the legal level, they lack technical means to truly control the scope of data use.

Cross-chain interoperability is complex and costly

The standards of each public chain are different, and assets and messages cannot

naturally communicate with each other.

Insufficient integration of AI and Web3

The transparency of AI training, reasoning, and data sources is low, and the trust foundation is weak.

These problems have limited the development of Web3 and also hindered the real upgrade of the global digital economy.

1.3 The era contradiction between data sovereignty and identity fragmentation

With the tightening of supervision, the strengthening of privacy protection regulations (such as GDPR, CCPA), and the full penetration of AI, the pattern in which Web2 giants control data and users cannot control the fate of data is no longer sustainable.

The data must belong to every user, not the platform itself.
Identity must be user-led, not passively bound.

This is where the design of Klwevgip started.

1.4 Klwevgip's mission and vision

Klwevgip's mission is to:

Build the world's most trusted, interoperable, and privacy-protecting Web3.0 basic protocol, making every interaction between identity, data, and AI transparent, secure, and controllable.

The vision includes:

Become a unified DID foundation layer for Web3
Become the most widely used user data sovereignty tool in the world
Become an intelligent trust infrastructure for Web3 × AI

Become an open hub for cross-chain interoperability

Freedom for users to truly control their identities, assets and data

Klwevgip is not only a technical project, but also a basic project to promote the construction of Web3.0 trusted system.

2. Detailed Explanation Of The Project: Klwevgip System Design

- 2.1 Project positioning and overall architecture concept
- 2.2 Decentralized Identity (DID) System
- 2.3 Data sovereignty and privacy protection mechanism
- 2.4 AI and intelligent collaboration layer
- 2.5 Cross-chain interoperability and multi-chain compatibility
- 2.6 Infrastructure capabilities for developers and enterprises

2. Detailed Explanation Of The Project: Klwevgip System Design

2.1 Project positioning and overall architecture concept

Klwevgip adopts a five-layer system structure of "identity layer + data layer + AI collaboration layer + cross-chain layer + application layer".

Core concepts include:

Absolute control of the user: the right to authorize, use and withdraw data is controlled by the user.

End-to-end privacy protection: Using technologies such as ZKP, homomorphic encryption, and federated learning.

AI verifiability: Ensure that model calls are auditable, traceable, and interpretable.

Cross-chain unified abstraction: Solve the problem of application fragmentation caused by multi-chain splitting.

Klwevgip is a modular project that allows developers to quickly build functions such as DID, privacy, middleware, and AI assistants based on modules.

2.2 Decentralized Identity (DID) System

Klwevgip DID supports mainstream global standards (W3C DID/VC) with extensions:

Unified identity mapping

Verifiable credentials

Revocable credentials

Behavioral reputation model

Selective disclosure of zero-knowledge proofs

Applications include login verification, on-chain reputation, credit scoring, social identity, asset mapping, and more.

2.3 Data sovereignty and privacy protection mechanism

The user can decide the data:

Shared scope

Service cycle

Purpose of use

Whether to allow AI training

Whether withdrawable

The Platform provides privacy technologies including:

ZKP

Multi-party secure computing (MPC)

Decentralized Encrypted Storage

Data authorization log cannot be tampered with audit

This means that for the first time, users have real control over their data.

2.4 AI and intelligent collaboration layer

AI is an important part of the entire Klwevgip, and its main functions include:

Intelligent Authentication and Risk Identification

User reputation analysis

Data usage scenario management

Multi-chain resource scheduling

Model compliance verification

Decentralized AI model market

The AI model operates using a privacy protection mechanism, making training and reasoning transparent and credible.

2.5 Cross-chain interoperability and multi-chain compatibility

Klwevgip's cross-chain layer support:

EVM

WASM

Bitcoin Layer 2

Solana

Cosmos SDK

Polkadot parachain

The message transmission adopts a decentralized relay scheme and is secured by zk-proof verification.

2.6 Basic service capabilities for developers and enterprises

The project offers:

DID SDK

Privacy Data API

AI model interface

Cross-chain messaging API

Enterprise Access Control Tools

Apply rapid deployment templates

Industries supported include:

Web3 Social

DeFi

GameFi

Medical data

Financial risk control

Enterprise and Government Identity Management

3. Technical Architecture

- 3.1 Overview of the overall architecture
- 3.2 Underlying chain and consensus mechanism
- 3.3 Identity and Credential System (DID/VC)
- 3.4 Data storage and encryption model
- 3.5 AI service and model framework
- 3.6 Cross-chain and message transport layer
- 3.7 Application layer and development tool group

3. Technical Architecture

Klwevgip's technical architecture revolves around "trusted identity → data sovereignty → privacy computing → AI scheduling → cross-chain interoperability → application layer ecology" and adopts a modular, scalable, and auditable overall design. The entire network aims to provide a unified identity basic layer and data trust layer for future Web3.0 applications, so that all on-chain and off-chain interactions can be verified, audited, and privacy-protected.

3.1 Overview of the overall architecture

The overall architecture of Klwevgip is divided into five layers:

Identity Layer: DID, VC, reputation model

Data Sovereignty Layer: encrypted storage, access authorization, and withdrawal mechanism

Privacy Compute and AI Collaboration Layer (AI & Privacy Compute Layer): Federated Learning, ZKP, AI Scheduling

Cross-chain interoperability layer: cross-chain bridge, relay network, message abstraction

Application Layer: DApp, enterprise service, developer framework

This architecture ensures that Klwevgip has the ability to evolve in the long term in future AI+Web3 aggregation scenarios.

3.2 Underlying chain and consensus mechanism

Klwevgip adopts a new generation of high-performance consensus mechanism DPoS-IBFT hybrid mechanism, which combines BFT-level security with a high-throughput delegate node structure.

Core benefits include:

- **High performance**

TPS up to 10,000 +

Block time approximately 1-2 seconds

Optimized for high-frequency scenarios such as DID, data authorization, and cross-chain messaging

● High security and auditability

Have Finality

Deny fork attacks

Multi-node signature verification guarantees consensus security

● Decentralization

The number of decentralized validators can be dynamically increased

Nodes enter the set through KWP staking and election

The true contribution affects the node weight

And through future plans to introduce:

Global reputation model adjusts participating node reputation combination

Zero-knowledge proof accelerates consensus validation

Ensure Klwevgip strikes a balance between speed, security, and decentralization.

3.3 Identity and Credential System (DID/VC)

The Klwevgip DID module strictly follows W3C standards and builds a sound credential system (VC), including:

● DID Core Features

DID creation and binding

Unified management of multiple identities

Verifiable on-chain signatures

Support off-chain identity mapping

● Verifiable credentials (VC) system

Identity credentials

Asset certificates

Behavioral credentials

Third-party certification credentials

Certificates issued by organizations and institutions

Each VC can be encrypted, revocable, and optionally disclosed.

● DID Reputation System

Behavioral data (on-chain behavior, lending, contributions, etc.)

AI reputation analysis

Zero Knowledge Credit Credential (ZK-Credit)

Risk level neutralization modeling

Klwevgip's DID system is not only an identity tool, but also the foundation of the future Web3 trust economy.

3.4 Data storage and encryption model

The Klwevgip data layer uses a hybrid storage system:

On-chain storage: identity hash, credential root, authorization record

Off-chain storage: distributed encrypted data (IPFS/Arweave/Filecoin)

Private data warehouse (optional): Enterprise-level encryption nodes

● Safety measures

Homomorphic encryption

Multi-party secure computing (MPC)

Sharded encryption and key revocability

Traceability audit of data usage

● User data control

The user can:

Authorization data

Time-limited authorization

Conditional authorization

Manual withdrawal

Audit third-party usage records

This is the core implementation of Web3 data sovereignty.

3.5 AI service and model framework

Klwevgip's AI system is one of the core competencies of this project.

● AI main functions

Identity and behavioral risk identification

Data authorization strategy analysis

Wallet Behavior Anti-Fraud

Application Growth Recommendation System

DID Reputation Score

Cross-chain resource scheduling and prediction

Model Transparency Audit and Hash Recording

● Privacy-preserving AI

The AI training process follows:

Federated Learning: Data does not leave the local area

Differential Privacy (DP): Prevents the model from backstepping users

ZKML: AI model inference results are verifiable

Auditable training log

AI is not only an algorithm in Klwevgip, but also a part of the infrastructure.

3.6 Cross-chain and message transport layer

Klwevgip provides a unified cross-chain abstraction layer that is compatible with the following chains:

Ethereum/EVM Family

Solana

Polkadot/Substrate

Cosmos SDK

Bitcoin Layer 2

Layer2 networks (Optimistic, ZK)

The cross-chain module adopts:

Decentralized relay network

zk-proof validates cross-chain messages

Asset Mapping and Unified Asset Format

This allows developers to deploy at once and run in multiple chains.

3.7 Application layer and development tool group

Klwevgip provides a complete development toolset:

Contract Framework (Solidity/Rust/Move)

DID SDK (JS/Python/Rust)

AI Interface API

Cross-chain messaging API

GraphQL Data Query Interface

Simulation test environment Sandbox Testnet

Developers can build in a short time:

Web3 login scheme

Data authorization system

Intelligent identity system

AI risk control system

Cross-chain asset management

Crypto Social Apps

Klwevgip aims to lower the innovation threshold of Web3.0 and allow developers to focus on the application itself.

4. Kwp Token Economic Model

- 4.1 Token Basic Information
- 4.2 Token core functions and usage scenarios
- 4.3 Token allocation model
- 4.4 Locking and release mechanism
- 4.5 Incentive system and value capture method

4. Kwp Token Economic Model

KWP is the core value carrier of Klwevgip network, which is used in key links such as resource payment, governance, incentives, and validator pledge. The token design follows the principle of "efficient, secure, and sustained growth" to ensure the long-term sustainability of the economic model.

4.1 Token Basic Information

Token Name : Klwevgip Token

Token short name: KWP

Total circulation: 30,000,000,000 KWP

Initial issue price: $0.00025

Accuracy: 18

Distribution network: Klwevgip mainnet (EVM compatible)

4.2 Token core functions and usage scenarios

The core usage scenarios of KWP include:

Network Gas and resource consumption

DID registration and credential fees

AI service call fee

Data authorization payment

Node Staking and Network Security Incentive

Ecological subsidies and developer incentives

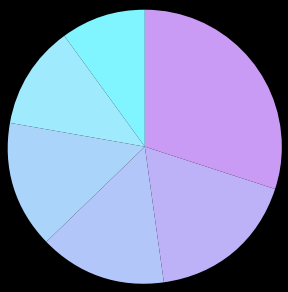
Governance voting and protocol upgrade

KWP is the power source of the whole network.

4.3 Token allocation model

The initial KWP allocation recommendations are as follows:

- Ecology and Community: 30%
- Team & R&D: 18%
- Foundation reserves: 15%
- Node incentive: 15%
- Eco-investors: 12%
- Market and partner expansion: 10%



The distribution model aims at long-term development and avoids short-term inflation and selling pressure.

4.4 Locking and release mechanism

The team and consultants adopt a long-term lock-up mechanism:

12-month lock-up period

36-month linear release

Node income is calculated separately

Ecological funds and incentive plans are gradually released according to application growth.

4.5 Incentive system and value capture method

Includes:

Verify node rewards

DID Issuance and Verification Fee Reshoring

Cross-chain message fees

AI Model Market Revenue

Data authorization sharing mechanism

Through these mechanisms, the demand for KWP will continue to rise with ecological growth.

5. Core Team And Consultants

- 5.1 Team structure
- 5.2 Introduction to Founding Members
- 5.3 Introduction to technology and product team
- 5.4 Business, Ecology and Compliance Team
- 5.5 Advisory Board

5. Core Team And Consultants

Klwevgip's core team consists of experts in distributed systems, cryptography, artificial intelligence, data sovereignty, Web3 infrastructure, and more. In order to ensure that the project has the highest technical level in the next generation Web3.0 architecture, Klwevgip invites experts with deep influence in the fields of blockchain, AI and privacy protection from all over the world to serve as technical consultants or joint research members.

5.1 Team structure vision

Klwevgip's team architecture consists of:

Core Leadership

Blockchain Underlying Protocol Team

Cryptography & DID Team

AI & Privacy ML Team

Interoperability & Infra Team (Interoperability & Infra Team)

Compliance & Strategy Team

5.2 Underlying Architecture and Consensus Mechanism Consultant

Gavin Wood

Founder and Principal Blockchain Architecture Consultant Chief Blockchain Architecture Advisor

Curricula vitae:

Co-founder of Ethereum

Founder of Polkadot

Solidity programming language author

Parity Technologies Founders

Web3 Foundation Core Technology Contributor

Emin Gün Sirer

Co-founder and Distributed Systems & Consensus Advisor

Curricula vitae:

Founder, Avalanche

Professor of Computer Science, Cornell University

Leading researcher in distributed systems and network security

Developing the first P2P highly scalable consensus architecture

Zooko Wilcox

Privacy & Zero-Knowledge Advisor

Curricula vitae:

Founder of Zcash

Zero-Knowledge Proof (ZKP) early core enabler

Over 30 years of experience in cryptography research

Electric Coin Company Founders

5.3 DID and Cryptography Consultant

Christopher Allen

DID & Verifiable Credentials Advisor

Curricula vitae:

Co-author of SSL/TLS protocol

Co-creator of W3C DID/VC standard

Blockchain Commons Founders

More than 30 years of experience in identity protocol design

Dan Boneh

Cryptography & ZK Advisor

Curricula vitae:

Professor of Cryptography, Stanford University

Applied Cryptography Group Founding Members

One of the core inventors of ZKP, MPC, Pairing-Based Cryptography

One of the most influential scholars in the world's cryptography field

Vitalik Buterin

Blockchain Protocol Research Consultant Blockchain Protocol Research Advisor

Curricula vitae:

Ethereum founder

Co-founder of Bitcoin Magazine

Continuing researchers in core directions such as L2, Rollup, and ZKP

An important driving force for the Web3 technology route

5.4 AI, Privacy Machine Learning and Data Sovereignty Consultant

Andrew Trask

Privacy AI & Federated Learning Advisor

Curzicula vitae:

DeepMind Investigator

Founder of OpenMined

Federated Learning and Privacy Machine Learning Field Enabler

Grokking Deep Learning Author

Richard Socher

AI Strategy & Model Development Advisor

Curricula vitae:

Former Chief Scientist at Salesforce

Founder of You.com

Top researchers in NLP and deep semantic modeling

Served as a technical consultant in a number of Silicon Valley technology companies

5.5 Web3 infrastructure, cross-chain and cloud computing consultants

Sergey Nazarov

Decentralized Oracle Advisor

Curricula vitae:

Co-founder, Chainlink

Founding figure of decentralized oracle track

Long-term technical consultant for multiple L1/L2 protocols

External data trustworthy introduction mechanism design expert

5.6 Global Compliance and Regulatory Consultant

Lewis Cohen

Global Crypto Compliance Advisor Global Crypto Compliance Advisor

Curricula vitae:

Founding Partner, DLx Law

Key figures in the design of digital asset compliance models in the United States

Served as legal adviser to a number of L1, stablecoin, and fintech companies

Have in-depth research on SEC, CFTC, MiCA, MAS and other regulatory systems

Klwevgip's vision is not only to build the infrastructure of the next generation of Web3.0, but also to drive the development of global identity, privacy, AI and cross-chain technologies.

6. Development Roadmap

- 6.1 Startup and early stages
- 6.2 Short-term development planning
- 6.3 Medium-term expansion route
- 6.4 Long-term ecological vision

6. Development Roadmap

Klwevgip's development roadmap revolves around four stages: "technology landing → network expansion → ecological growth → global compliance layout" to ensure the complete advancement path of the project from basic agreement to ecological application. The roadmap covers 0-48 months of development planning and will be transparently disclosed based on actual progress.

6.1 Initiation and early stage (0-6 months)

(1) Core protocol development completed

Complete DID basic protocol and VC (verifiable credential) framework

Constructing data sovereignty model and authorization management mechanism

Complete the design of AI model scheduling layer

Complete the first version of the cross-chain unified abstraction layer protocol

(2) Testnet framework construction

Start testnet node

Provide developer access interface (API/SDK)

Build a contract deployment and debugging toolchain

Complete basic logic such as identity registration, verification, and withdrawal

(3) Start consultant pool communication

Initiate formal communication with the Global Advisor (Sections 5.2-5.6)

Confirm the first technical consultants to join

Establish an academic cooperation program (university laboratory cooperation)

6.2 Short-term development planning (6-12 months)

(1) Public Testnet is online

DID, data authorization, and privacy computing modules are fully open

AI model call interface online (scoring, verification, risk identification)

Cross-chain bridge and message verification functions are open

(2) Developer ecosystem launch

Publish developer documentation and SDK

Open Grants Program

Hosting a global hackathon

(3) Technical audit and security testing

Complete an external security agency audit of the protocol

Complete compliance assessment of ZKP, MPC, AI modules

Establish a BUG Bounty reward system

6.3 Medium-term development planning (12-24 months)

(1) Mainnet is officially launched

DID is fully decentralized

AI collaboration layer and federated learning network enabled

The cross-chain module is fully compatible with EVM+WASM+L2 network

(2) Ecological partner expansion

Establish cooperation with wallets, exchanges, and enterprise data platforms

Launching the Global Data Sovereignty Alliance

Provide infrastructure access support for enterprises and Web3 startup teams

(3) Large-scale application implementation

Support Web3 login system (DID Login)

Support decentralized social identity

Support on-chain credit scoring scenarios

Support privacy AI training scenarios

6.4 Long-term ecological vision (24-48 months)

(1) Global deployment

Set up technology and community nodes in North America, Europe and Asia

Regional compliance implementation (compliant with MiCA, MAS, ADGM, Hong Kong VASP and other regulations)

(2) Inter-industry integration

FinTech

Medical and health data management

IoT Trusted Device Identity

Enterprise DID and Privacy Authentication System

(3) Protocol autonomy (DAO governance) formation

Major protocol upgrades dominated by DAO votes

Open ecological capital pool (Ecosystem Treasury)

Establish a global developer governance committee

6.5 Roadmap transparency mechanism

Klwevgip promises:

Regular monthly and quarterly reports released on major developments

DAO community has voting rights on critical roadmap changes

All protocol upgrades and audit reports are open and transparent

The roadmap will be continuously upgraded with ecological expansion and jointly managed by the community.

7. Ecosystems And Partners

- 7.1 Ecosystem composition
- 7.2 Core application scenarios
- 7.3 Eco-partner matrix
- 7.4 Community and Developer Program

7. Ecosystems And Partners

Klwevgip's ecosystem is built around three core competencies:
Identity credibility, data control, and AI intelligent interoperability capabilities.

The ecosystem is composed of users, developers, enterprises, nodes, AI model providers and other parties.

7.1 Ecosystem composition

(1) User (identity and data sovereignty holder)

Each user has a DID identity

Data is fully controlled by the user

Data-as-an-Asset can be earned through data authorization

(2) Developers (DApp builders)

Use the SDK, API provided by Klwevgip

Deploy DID, security model, and cross-chain business logic

Enjoy ecological incentives and financial support

(3) Infrastructure providers (nodes, data nodes)

Run Validation Node

Provide privacy computing nodes

Provide AI model training nodes (federated learning)

(4) Enterprises and institutions

Can access DID login

Privacy data sharing network can be built

Verifiable credentials and data audits are available

7.2 Core application scenarios

(1) Decentralized identity (DID) login system

Replace traditional password/email login

Realize "one login, cross-chain universal"

(2) Web3 social identity and content ownership

On-chain identity signature

Content copyright encryption and authorization tracking

(3) DeFi credit and risk control

ZK-based credit voucher

Credit rating model without KYC

Fraud prevention AI model

(4) AI-driven data market

Data anonymization

Users autonomously manage data sales rights

Federated learning model training reward

(5) Enterprise-level and government trusted data system

Data sharing audit

Privacy computing

Verifiable traceability

7.3 Partner Matrix

Klwevgip's partners will cover:

Public chain ecology

DID Platform

AI computing power provider

Decentralized storage platform

Wallets and Custodians

Web2/Web3 Enterprise

7.4 Community and Developer Program

Global Grants Program

White Hat Safety Rewards

Web3 University Partnership Program

Developer Treasury

Quarterly hackathon events

The ecology of Klwevgip will be promoted by developers and the community.

8. Risk Assessment And Mitigation Measures

- 8.1 Technical risks
- 8.2 Market risk
- Legal and compliance risks
- 8.4 Governance and operational risks
- 8.5 Risk Mitigation Strategies

8. Risk Assessment And Mitigation Measures

Blockchain projects need to face risks in technology, market, supervision, governance and other aspects. Klwevgip adopts a multi-level risk protection system to ensure the long-term security and sustainable development of the protocol.

8.1 Technical risks

(1) Vulnerability risk of consensus mechanism

May cause network outages or status rollbacks.

Mitigation measures: Multiple rounds of audit + BFT strong consistency mechanism.

(2) Security risks of cross-chain bridges

Cross-chain bridges used to be the most attacked area in the industry.

Mitigation measures: zk-proof verification and multi-sign relay network.

(3) Risk of AI model abuse

Improper training data may lead to bias or inference errors.

Mitigation measures: Full Link Audit with Verifiable Model (ZKML).

8.2 Market risk

(1) Token price fluctuations

Both market sentiment and project cycle affect volatility.

Mitigation measures: Adopt a long-term linear release and ecological growth binding mechanism.

(2) Illiquidity risk

There may be insufficient depth at the initial stage of new projects.

Mitigation measures: Introduce market makers and ecological incentive mechanisms.

8.3Legal and regulatory risks

(1) Regulatory differences in different jurisdictions

The global regulatory framework is not uniform.

Mitigation measures: Long-term cooperation with top law firms such as DLx Law.

(2) Data sovereignty regulatory risks

Related to privacy regulations such as GDPR, CCPA, etc.

Mitigation measures: adopt de-identification, ZK privacy layer.

8.4 Governance and operational risks

(1) Risk of centralized governance

If the initial weight is too high, it may lead to disputes.

Mitigation: Gradually shift to DAO governance.

(2) Risk of roadmap delay

Complex technical modules may cause delays.

Mitigation measures: Transparently disclose progress and accept community governance supervision.

9. Conclusions And Future Prospects

- 9.1 Summary of project core values
- 9.2 Potential impact under the Web3.0 landscape
- 9.3 Long-term development direction

9. Conclusions And Future Prospects

Klwevgip's goal is not to build another public chain or ordinary data protocol, but to build:

A globally unified decentralized identity system (DID)

Data sovereignty model that users truly own and control

A trusted collaboration layer combining AI and privacy computing

Cross-chain interoperable Web3 infrastructure network

In the future, Klwevgip will become:

Identity Standards for Web3

Trusted trigger layer for AI data

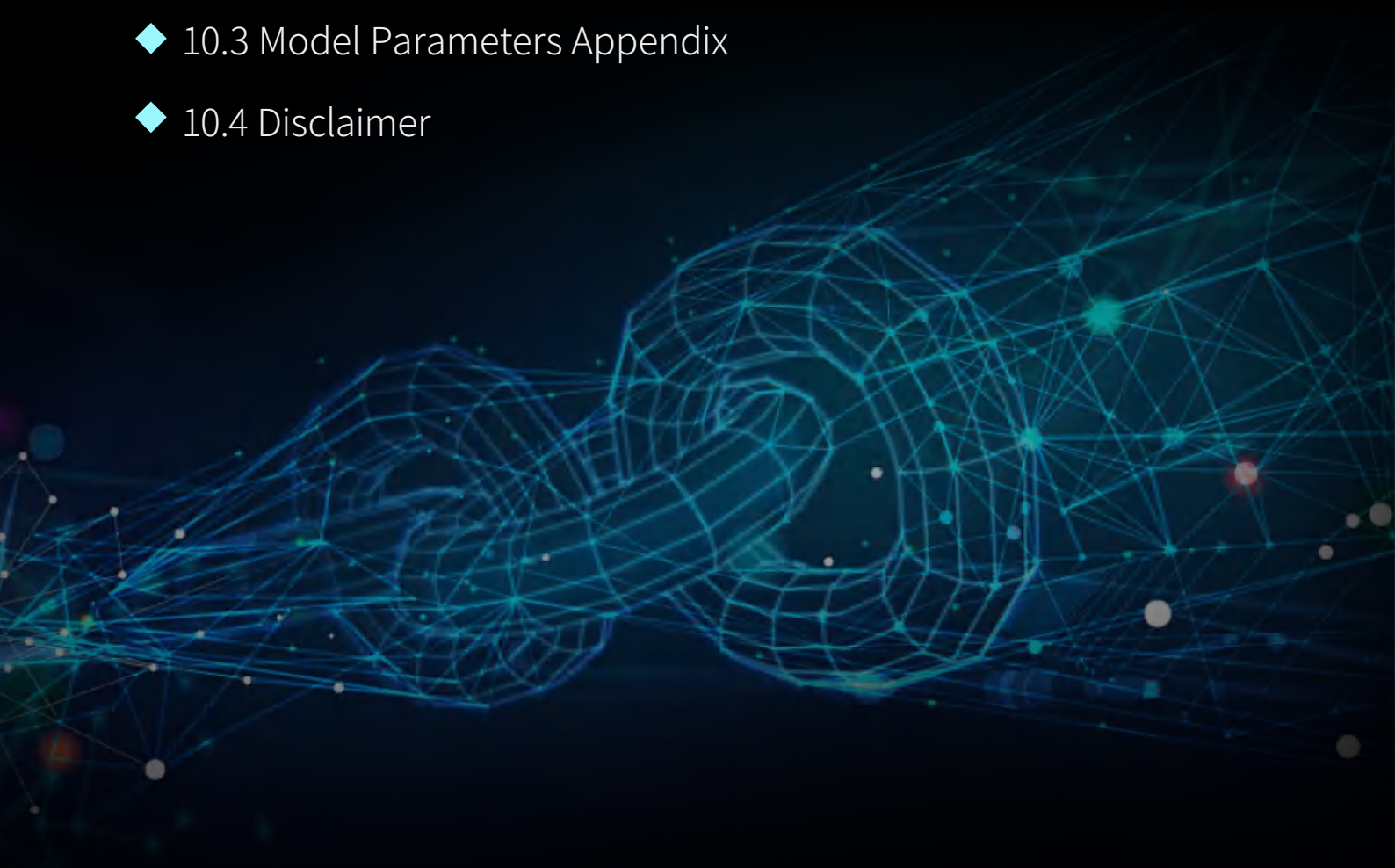
The interoperable hub of multi-chain ecology

An important part of the global data sovereignty system

With the opening of the main network, ecological expansion and the advancement of international cooperation, Klwevgip will gradually build an intelligent, efficient, trusted and global Web3.0 infrastructure.

10. Appendix

- 10.1 Description of Terms
- 10.2 Technical Standard Reference
- 10.3 Model Parameters Appendix
- 10.4 Disclaimer



10. Appendix

10.1 Glossary of Terms

DID: Decentralized Identity

VC: Verifiable credentials

ZKP: Zero Knowledge Proof

MPC: Multi-party Secure Computing

FL: Federated Learning

DAO: Decentralized Autonomous Organization

10.2 Reference to technical standards

W3C DID Specification

W3C VC Specification

ERC Standards

ZK-SNARK and STARK Technical Data

10.3 Model Parameters Appendix

DID Hash Generation Process

Authorization data structure

AI model scoring mechanism

Example of cross-chain message structure

10.4 Disclaimer

This white paper is used for technical description of the project and does not constitute investment advice. The project will be iteratively modified according to the actual situation.