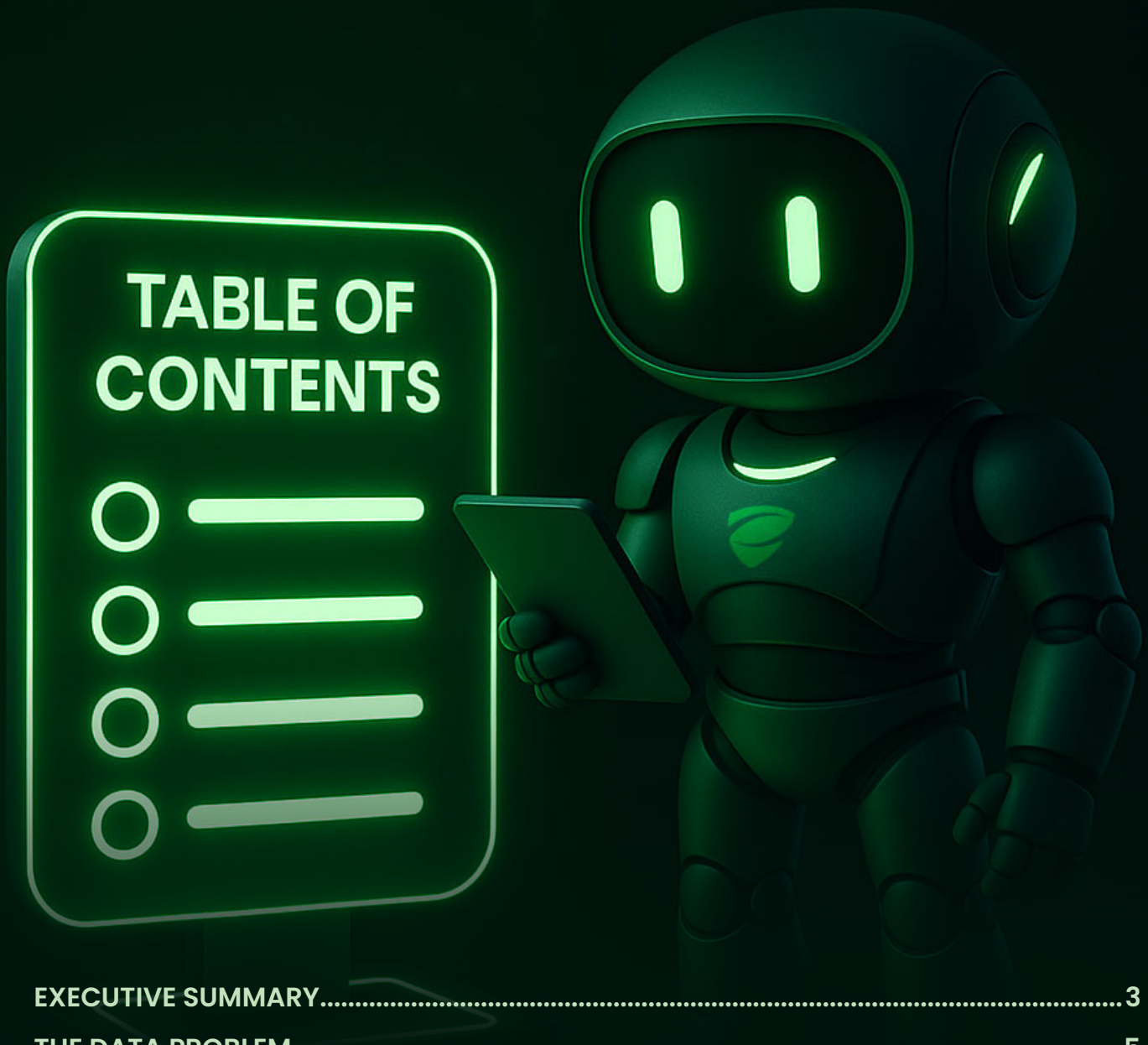
The First Private AI Network Powered by You.

ZKP

Business Litepaper
2025



EXECUTIVE SUMMARY

The Opportunity at a Glance

THE PROBLEM

The data economy is broken. A handful of corporations control AI development, extracting billions from user data while compensating contributors nothing. High-profile breaches—Cambridge Analytica's 50 million exposed profiles, Equifax's 147 million compromised records—reveal systematic failures in centralized architectures where users create value but capture none, privacy violations are endemic, and innovation is gatekept.

OUR SOLUTION

The Zero Knowledge Proof ecosystem creates the first platform where privacy and utility coexist through zero-knowledge proofs—cryptographic verification without data exposure—and hybrid blockchain consensus rewarding useful AI work rather than wasteful computation. Built on Substrate with 99% energy reduction versus Bitcoin, we're enabling privacy-preserving data sharing, AI development, and fair value distribution through decentralized infrastructure.

INVESTMENT OPPORTUNITY

Multiple earning mechanisms with accessible entry:

Proof Pods - Passive income devices generating zero-knowledge proofs. The ROI may fluctuate around 144% annually (depending on the $ZKP price)*
ZKP Coin Presale - Structured public presale with transparent participation and deterministic pricing.
Network Validation - Earn from AI computation validation and storage provision
Data Monetization - Turn datasets into continuous revenue streams
Early Participation Bonuses - Testnet rewards, ambassador referrals and first-mover positioning

*the actual ROI may significantly differ as it is dependent on the $ZKP price which may be highly volatile

KEY DIFFERENTIATORS

Advanced Technology Moat - Zero-knowledge cryptography and hybrid consensus creating competitive advantages

Proven Foundation - Operational testnet, completed ZKP circuits, Substrate framework securing billions across production chains

Accessible Earning - Plug-and-earn simplicity versus technical mining complexity, multiple revenue streams versus pure capital staking

Sustainable Economics - 99% energy reduction enabling broader participation, dual-token architecture aligning infrastructure and application incentives

MARKET POSITIONING

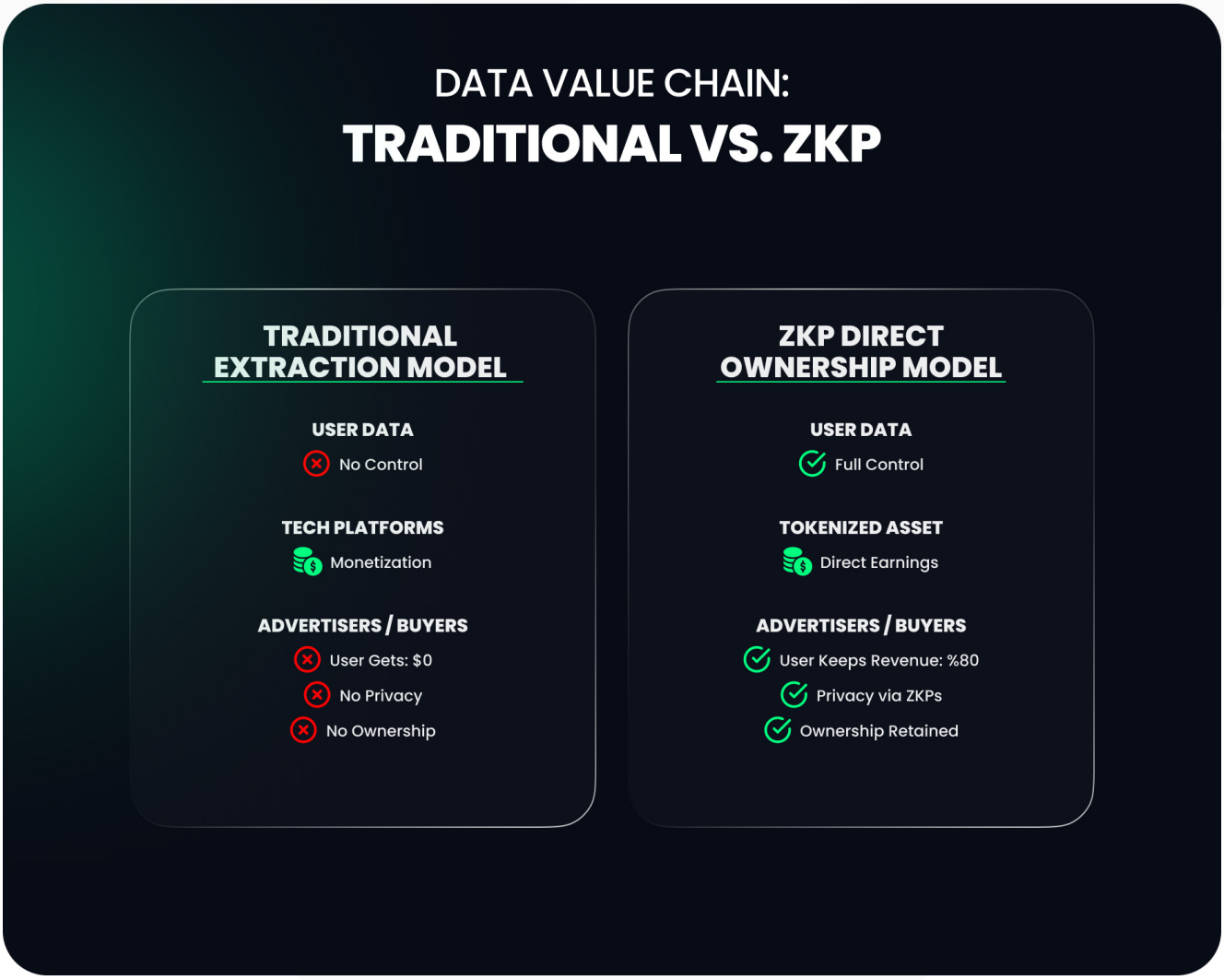
We're building foundational infrastructure for privacy-preserving AI at the intersection of three converging trends: accelerating AI adoption, increasing data demand, regulatory pressure requiring privacy compliance, and decentralized alternatives gaining traction as centralized systems fail users.

First-mover in hybrid consensus —uniquely combining computation validation with storage provision where network security derives from useful work advancing the ecosystem's core mission.

THE DATA PROBLEM

Why the Data Economy is Broken

The digital economy runs on data—yet the systems managing this data are fundamentally broken. Centralized architectures extract value from users while compensating them with nothing, concentrate power among a handful of corporations, and create systematic privacy violations that undermine trust. This isn't accidental. It's by design.



THE CENTRALIZATION CRISIS

Data Breaches: Inevitable, Not Preventable

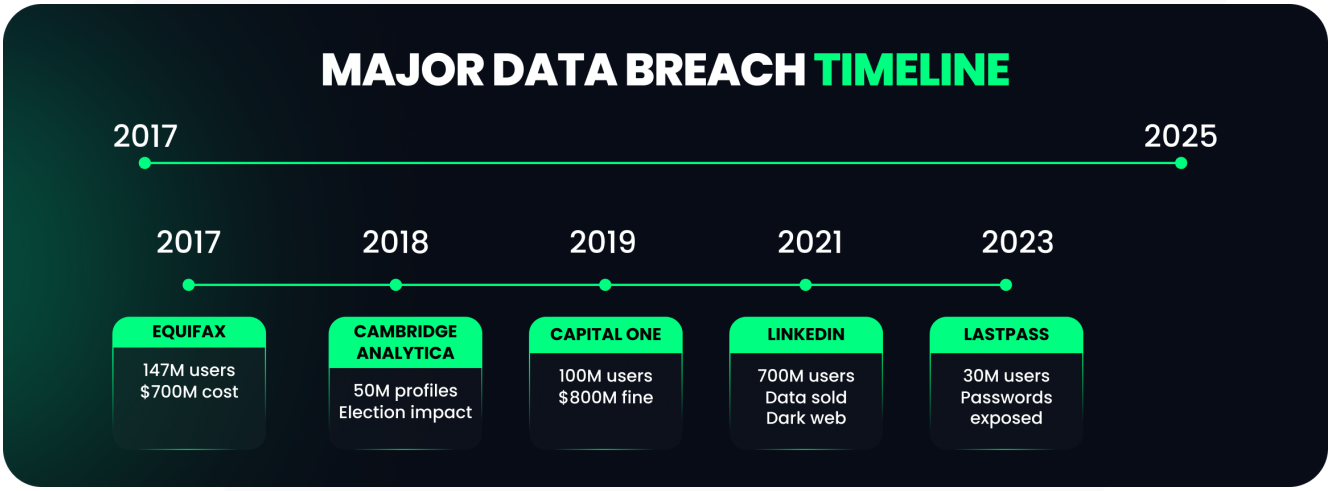
Centralized systems create single points of failure with catastrophic consequences:

Cambridge Analytica (2018): 50 million Facebook profiles harvested without explicit consent, weaponized for political manipulation. Users created the value—their preferences, relationships, behaviors—yet captured none of the economic benefit while bearing all privacy risk.

Equifax (2017): 147 million individuals' sensitive financial data compromised through infrastructure vulnerability. Victims had no choice in data collection, no control over security, and no compensation for breach.

The Pattern: Attack surfaces are concentrated, making breaches inevitable. Users have no visibility into security practices. Economic incentives prioritize collection over protection. Liability falls on victims rather than custodians.

Economic Toll: Average breach costs $4.45 million per incident, with costs rising annually. The true cost—erosion of trust, regulatory scrutiny, constrained innovation—is immeasurable.



Value Extraction Without Compensation

Every search, post, purchase, and click generates data. Platforms aggregate and monetize this through advertising, algorithmic optimization, and third-party sales—building trillion-dollar businesses on user-generated information.

The Model: Users contribute data continuously. Platforms monetize it. Shareholders capture value. Users receive nothing.

A social media user generating thousands of posts over a decade creates substantial value—training AI models, targeting ads, populating feeds. Their compensation: zero. Their control: zero. Their revenue share: zero.

Privacy Violations Are Systematic

Beyond breaches lies authorized exploitation—surveillance capitalism where every action is tracked, profiled, and monetized.

The Consent Fiction: Terms of service averaging 10,000+ words, requiring college-level comprehension, presented as take-it-or-leave-it contracts. "Informed consent" is legal fiction when users must accept surveillance or exit digital society.

Scope Creep: Data collected for one purpose gets repurposed for others—advertising, analytics, third-party sales—without explicit authorization. Privacy policies change retroactively.

Regulatory Gaps: Despite GDPR and CCPA, enforcement remains limited. Fines are cost-of-business for trillion-dollar companies.

THE AI MONOPOLY

Concentrated Control

AI development has consolidated among a handful of tech giants—OpenAI (Microsoft), Google DeepMind, Meta AI, Anthropic (Google), Amazon. This concentration stems from AI requiring three resources: massive datasets, enormous compute, and specialized talent—all favoring incumbent platforms.

Data Advantage: Training state-of-the-art models requires billions of samples. Platforms with existing users have this. Startups don't. This creates insurmountable barriers—you can't build competitive AI without data, can't get data without users, and can't get users without competitive AI.
Compute Advantage: Training costs tens of millions. Only hyperscale organizations can attempt it, excluding universities, small companies, and entire countries.
The Result: AI development controlled by entities whose business models depend on data extraction and surveillance. Technology shaping humanity's future governed by shareholders optimizing quarterly profits.

Zero Compensation for Data Creators

Every AI model trains on human-created content: text, images, code, conversations, videos. This represents millions of hours of human effort and expertise.

The Compensation: Zero.

Artists discover styles replicated by models trained on their portfolios—without permission or payment. Writers find prose patterns embedded in language models—without attribution. Photographers see compositions reproduced by generators—without licensing.

The Irony: AI companies claim data "has no inherent value"—yet spend billions acquiring it, guard it as a competitive advantage, and build trillion-dollar valuations on it.

Innovation Gatekeeping

When AI concentrates among a few players, innovation follows their priorities—not society's needs.

Closed Development: Most frontier models are proprietary black boxes. Researchers can't audit capabilities or validate safety claims.
Access Control: API access governed by platform policies that change arbitrarily. Applications exist at the platform's discretion.
Resource Hoarding: Models trained on public data become private assets. The collective contribution of millions becomes a competitive advantage of one corporation.

MARKET OPPORTUNITY

Convergence Creating Massive Opportunity

Data Marketplace Growth: Multi-billion dollar annual expansion as organizations recognize data as a strategic asset. Current marketplaces suffer from trust deficits and privacy concerns—exactly what decentralized alternatives solve.
Privacy Technology Adoption: GDPR fines exceeding €1.5 billion signal regulatory seriousness. Organizations need privacy-preserving infrastructure as legal necessity, not nice-to-have. Zero-knowledge proofs transition from academic curiosity to business requirement.
DePIN Emergence: Decentralized infrastructure networks achieving billions in total value locked validate market appetite for owning rather than renting infrastructure.

Regulatory Tailwinds

GDPR: User rights to data portability and deletion, with fines up to 4% of global revenue—creating strong incentives for privacy-preserving alternatives.

CCPA & State Laws: Similar protections spreading across the U.S., creating patchwork requiring cross-jurisdiction solutions.
AI Regulation: European AI Act, U.S. executive orders, and international frameworks addressing governance and accountability. Early compliance advantages accrue to privacy-first platforms.

The Convergence

Rising Data Value: AI adoption multiplying demand for training data.
Privacy Imperative: Regulatory pressure and user awareness driving demand for alternatives.
Technology Maturity: Zero-knowledge proofs, decentralized storage, and blockchain infrastructure reaching production readiness.
The Opportunity: Build infrastructure for privacy-preserving AI before incumbents adapt or regulations force transitions. First-mover advantages in network effects and ecosystem development create sustainable competitive positions.

The data economy is broken by design. The market is ready for alternatives. The technology exists. The regulatory environment favors change. The question is who builds the solution—and who benefits from being early.

THE SOLUTION

Zero Knowledge Proof reimagines data exchange through cryptographic innovation that makes privacy and utility coexist, economic models that reward contributors fairly, and infrastructure that distributes rather than concentrates power.

WHAT WE'RE BUILDING

Privacy-First Data Marketplace

A decentralized platform where individuals and organizations monetize datasets while maintaining complete ownership. Data providers upload to IPFS, encrypt with AES-256, and tokenize as blockchain assets. Buyers verify quality through zero-knowledge proofs before purchase—no intermediaries, no data exposure, no trust required.

The Process: Upload encrypted data Set pricing and access tiers ⊠ Earn per access ⊠ Maintain perpetual control

Traditional marketplaces require surrendering data to intermediaries. Zero Knowledge Proof provides cryptographic certainty, maintained privacy, and perpetual ownership.

Blockchain Secured by Useful Work

Hybrid Consensus:

Proof of Intelligence (PoI): Validators perform verifiable AI computations—matrix operations, neural network inference—instead of wasteful hash mining. Useful work secures the network while advancing AI development.

Proof of Space (PoSp): Validators provide decentralized storage, ensuring marketplace datasets remain accessible. Standard hardware requirements make participation accessible.

Energy Efficiency: 99% reduction versus Bitcoin (~10W per TB vs. ~1MW per TH/s)

Built on Substrate: Enterprise framework from Parity Technologies, powering production blockchains securing billions in value. Provides proven security, forkless upgrades, and cross-chain compatibility.

Accessible Participation

Multiple Entry Points:

Proof Pods: A plug-and-earn devices requiring minimal expertise

Network Validation: Standard server hardware, earn multiple reward streams

Data Provision: Any dataset size, community governance quality standards

Testnet: Zero cost participation, earn ZKP coins

ZERO-KNOWLEDGE PROOFS: THE CORE INNOVATION

Proving Things Without Revealing Data

Zero-knowledge proofs enable proving a statement's validity without revealing any information beyond truthfulness.

Simple Analogy: Age Verification

Traditional: Show ID revealing name, address, birthdate, photo, ID number—far more than necessary.

Zero-Knowledge: Generate cryptographic proof stating "over 21" without revealing birthdate or other details. The verifier gains certainty about age while learning nothing else.

Data Marketplace Application:

A researcher wants to verify a medical dataset contains 10,000 patient records with specific characteristics. The traditional approach requires either trusting claims or inspecting data—compromising privacy.

With ZKPs: Provider generates cryptographic proof (~288 bytes) demonstrating dataset properties. Researcher verifies in ~2 milliseconds, gaining mathematical certainty without seeing patient records, names, treatments, or identifying information.

Technical Foundation

zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge):

- Succinct: ~288 byte proofs regardless of complexity
- Fast: ~2 millisecond verification
- Proven: Powers Zcash, zkSync, StarkNet—production systems processing billions

BLS12-381 Curve: Industry-standard cryptography providing ~128-bit security, comparable to 3072-bit RSA used by governments and financial institutions.
Battle-Tested: Decades of academic research, formal verification, real-world validation.

HOW PRIVACY CREATES VALUE

Data Owners Maintain Control

Traditional marketplaces require transferring data permanently. Even "licensed" data gets copied beyond agreement terms with no enforcement.

ZKP Alternative:
Data never leaves owner control. Smart contracts manage time-limited access, usage restrictions, automatic revocation, and flexible pricing. Tokenization creates blockchain-native assets with verifiable ownership, divisible rights, transferable value, and automated royalties.

Result: Datasets become productive assets generating recurring revenue while owners maintain full control.

Buyers Get Verified Quality

Traditional purchasing requires either blind trust or inspection compromising seller privacy.

Cryptographic Verification:
Prove statistical properties, format compliance, size validation, temporal coverage, and source provenance—all before purchase through zero-knowledge proofs.

Example: Financial institution verifies: 1 million transactions, 12-month span, >95% fraud label accuracy, 50-state geographic distribution—through cryptographic proofs before committing funds.
Eliminates post-purchase disputes, reduces due diligence costs, accelerates transactions.

Trust Through Mathematics

Centralized platforms introduce custody risk, censorship risk, fee extraction (20-40% of value), and opaque algorithms.

Decentralized Alternative:
Smart contracts execute agreements automatically. Blockchain provides transparent rules, automated enforcement, immutable records, and minimal fees.
Instead of trusting platforms, participants trust mathematics: ZKPs provide verification, blockchain provides execution, cryptography provides privacy, open source provides auditability.

Unlocking New Markets

Many high-value datasets remain unutilized because existing infrastructure cannot guarantee privacy:

Healthcare: Hospitals tokenize anonymized records. Researchers verify properties through ZKPs without accessing protected information. Hospitals earn revenue while maintaining HIPAA compliance.

Financial Services: Banks prove model characteristics without revealing algorithms. Other institutions verify capabilities before licensing while source protects intellectual property.

Enterprise IoT: Companies prove data quality and relevance through ZKPs without exposing operational details, enabling monetization without competitive risk.

Government Data: Enable approved research on sensitive data through privacy-preserving verification, advancing policy research without compromising individual privacy.

The Zero Knowledge Proof ecosystem solves problems that centralized systems can't address. Where traditional platforms force users to choose between privacy and functionality, ZKP provides both through cryptographic verification. Data owners monetize assets while maintaining control. Buyers access verified datasets without exposure. New markets emerge when sensitive data can be shared without risk—from healthcare research to financial analytics to enterprise collaboration previously impossible under centralized architectures.

WHY ZKP WINS

The ZKP ecosystem enters a market where existing solutions solve pieces of the problem but none address the full picture. We combine what competitors can't: cryptographic privacy, useful-work consensus, accessible earning, and AI-specific optimization.

VS. TRADITIONAL BLOCKCHAIN DATA MARKETPLACES

Ocean Protocol, Streamr, etc:

Their Limitations:

- Data must be decrypted for verification—buyers trust claims or compromise seller privacy
- Centralized listing approval and dispute resolution despite blockchain integration
- Platform fees 15-30% recreating intermediary extraction
- Tokens function as payment only—no infrastructure participation rewards

ZKP Advantages:

- Zero-knowledge proofs verify dataset properties before purchase without data exposure
- No gatekeepers—community governance only
- Dual-token model: DTK for marketplace, ZKP for infrastructure security
- Data owners maintain perpetual control through smart contract enforcement

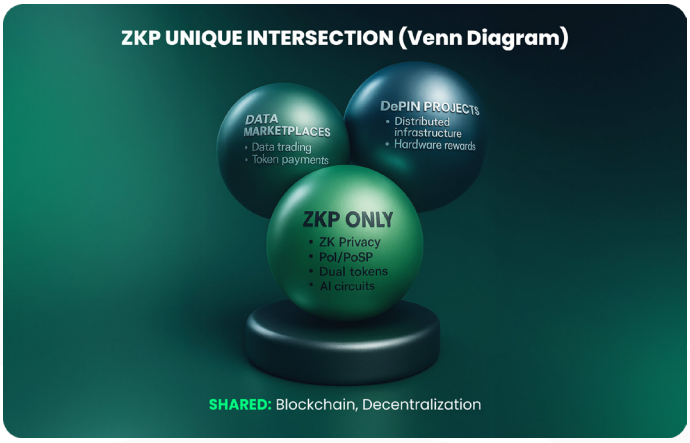
CAPABILITY	TRADITIONAL DATA MARKETPLACES	DePIN PROJECT	ZKP ECOSYSTEM
Privacy	✗ Must decrypt data	✗ No privacy	✓ ZK proofs native
Decentralization	ⓘ Centralized approval process	✓ Distributed infrastructure	✓ Full DAO governance
Earning Model	✗ 15-30% fees Platform keeps	ⓘ Hardware only requirements	✓ Multiple streams: Pods/Data/Validation
AI Optimized	✗ General purpose	✗ Storage/computer not AI-specific	✓ PoI consensus AI circuits built-in

VS. OTHER DePIN PROJECTS

Filecoin, Arweave, Render, Helium:

Their Limitations:

- Commodity storage/compute competing on price against hyperscale cloud providers
- No AI-specific optimization or privacy-preserving computation
- Storage-only focus without marketplace integration or quality verification
- Some still use energy-wasteful Proof-of-Work variants



ZKP Advantages:

- Hybrid PoI/PoSp rewards AI computation validation and storage—useful work, not waste
- 99% energy reduction while contributing ecosystem utility
- Application-infrastructure designed together: native privacy, quality assurance, economic incentives
- AI-optimized circuits, storage, and computation purpose-built rather than general-purpose

OUR UNIQUE COMBINATION

Balanced Incentives: PoI validates AI computations. PoSp verifies storage. Staking provides economic security.

Protocol-Level Privacy: Access control, data quality, governance voting, computation verification all use zero-knowledge proofs intrinsically.

Multiple Entry Points:

- Proof Pods: Minimal expertise, passive income
- Validators: Technical participation, multiple reward streams
- Data Providers: Monetize existing assets, any size
- Testnet: Zero cost, earn through participation

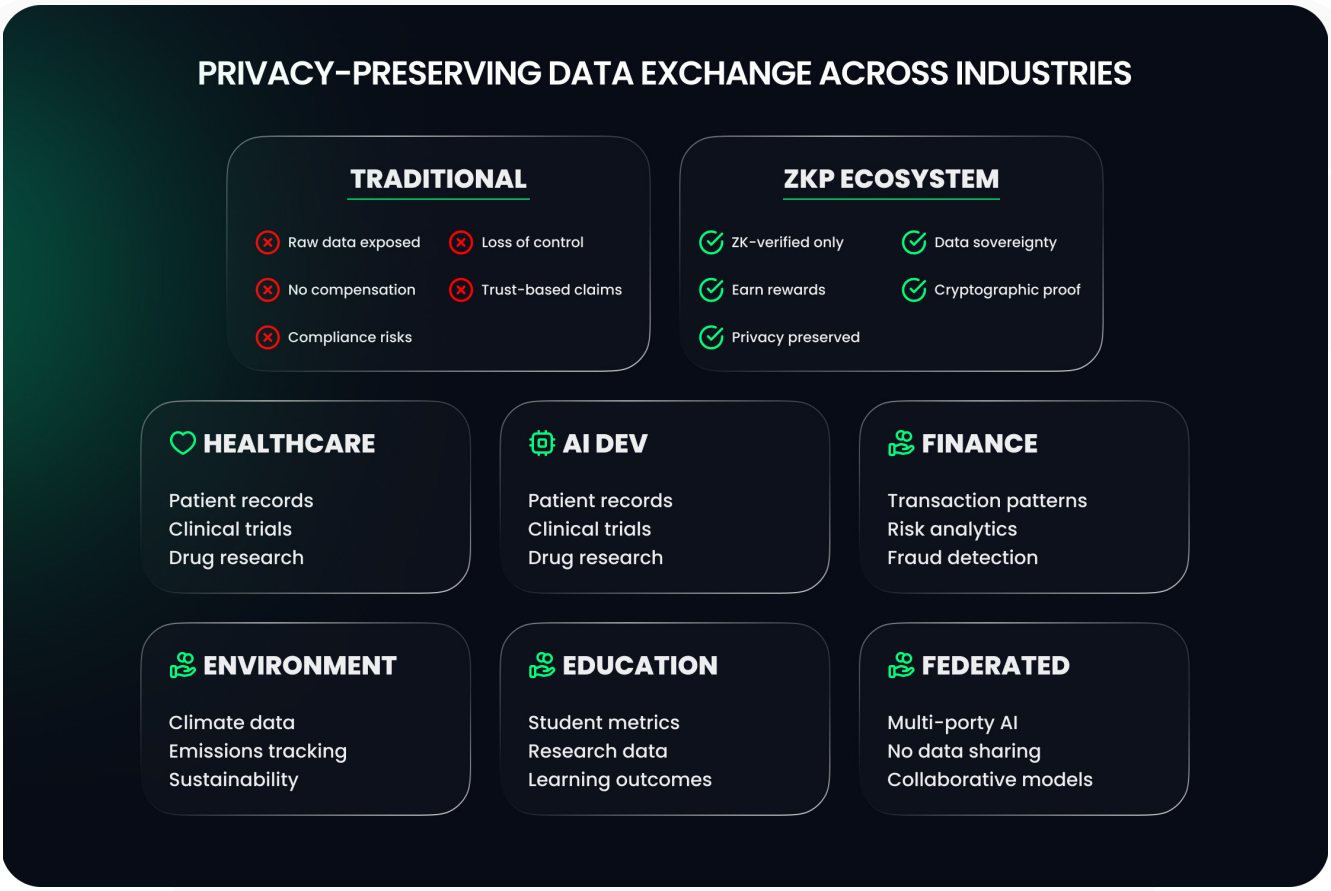
Traditional crypto requires massive capital or technical expertise. DePIN requires hardware knowledge. Data marketplaces require datasets. We accommodate all simultaneously.

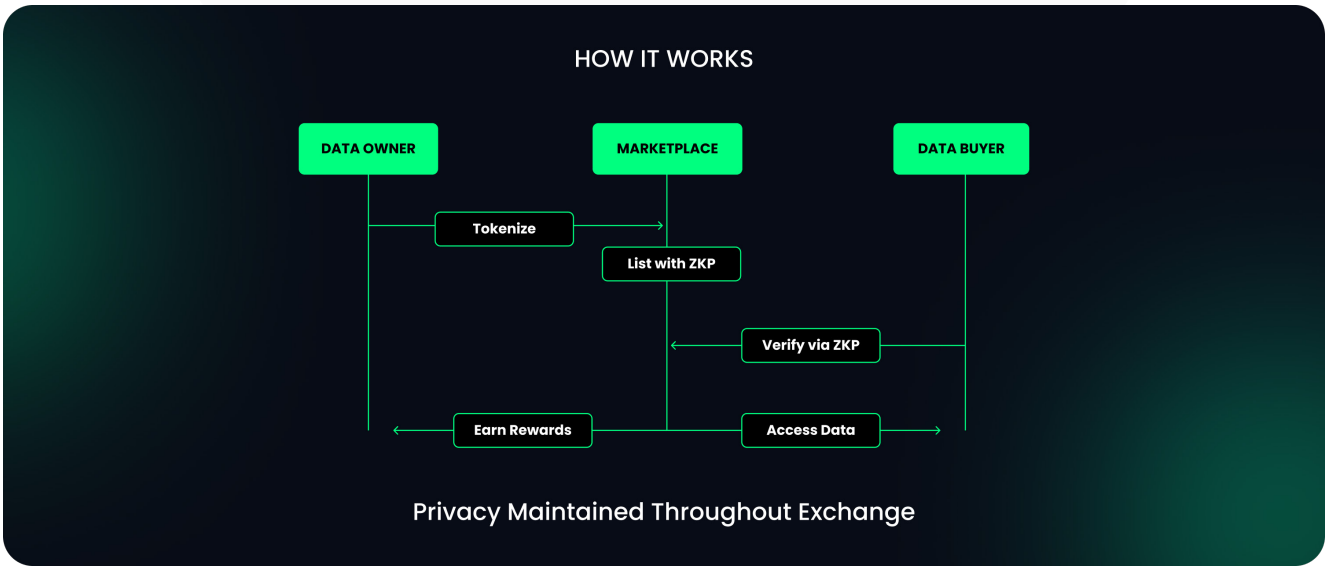
Existing platforms face structural constraints. Adding zero-knowledge proofs to traditional marketplaces requires rebuilding core architecture. DePIN projects optimizing for AI workloads dilutes their original infrastructure focus. Privacy protocols implementing earning mechanisms means designing entirely new economic systems. ZKP designed these components as an integrated system rather than retrofitting capabilities onto existing frameworks.

REAL-WORLD APPLICATIONS

Privacy-Preserving Data Exchange Across Industries

The ZKP ecosystem solves fundamental challenges in data sharing across sectors where privacy, security, and value distribution have historically been incompatible. Here's how different industries benefit from privacy-first infrastructure.





HEALTHCARE RESEARCH

Private Medical Data Advancing Science

Hospitals and research institutions can monetize anonymized patient records while maintaining HIPAA and GDPR compliance. Researchers verify dataset properties—patient count, diagnostic distributions, demographic breakdowns—through zero-knowledge proofs without accessing protected health information.

Example Use Case:

A hospital tokenizes a dataset of 5,000 anonymized diabetic patient profiles including treatment histories, lab results, and outcomes. A pharmaceutical company researching diabetes treatments purchases access, using ZKPs to verify the dataset contains required diagnostic markers and statistical significance—all without exposing individual patient records. The hospital earns DTK tokens while contributing to medical advancement, and researchers accelerate drug development while maintaining privacy compliance.

Applications:

- Drug development and clinical trials
- Epidemiological studies and disease modeling
- AI-driven diagnostic tool training
- Treatment efficacy analysis
- Public health research

ARTIFICIAL INTELLIGENCE DEVELOPMENT

Training Data With IP Protection

AI developers access high-quality, curated datasets for model training without compromising data privacy or intellectual property. Organizations with proprietary datasets—e-commerce behavior, social media interactions, IoT sensor readings—monetize previously siloed data assets.

Example Use Case:

A tech company procures a tokenized dataset of user-generated text to train a natural language processing model. The data provider uses zero-knowledge proofs to verify dataset size, language diversity, and quality metrics without exposing actual content. The buyer confirms the dataset meets training requirements through cryptographic verification, while the provider protects competitive advantages by never revealing underlying text patterns or user information.

Applications:

- Large language model training
- Computer vision datasets (images, video)
- Recommendation algorithm development
- Speech recognition training
- Autonomous systems and robotics

FINANCIAL ANALYTICS

Anonymous Transaction Analysis

Financial institutions share anonymized transaction patterns, risk models, and fraud detection training data. Buyers verify statistical properties and dataset size through cryptographic proofs without exposing individual transactions, customer details, or proprietary risk models.

Example Use Case:

A bank tokenizes anonymized credit card transaction data showing fraud patterns over 12 months. A fintech startup training fraud detection algorithms purchases access, using ZKPs to verify transaction volume, temporal distribution, fraud label accuracy, and statistical completeness—without seeing individual transactions or customer identities. This enables collaborative fraud prevention while maintaining competitive confidentiality and regulatory compliance.

Applications:

- Fraud detection and prevention
- Credit risk modeling
- Market trend analysis
- Algorithmic trading strategies
- Anti-money laundering (AML) compliance

ENVIRONMENTAL DATA SHARING

Climate Research & Sustainability

Environmental organizations tokenize climate data—air quality measurements, emissions tracking, biodiversity surveys—enabling policymakers and researchers to analyze trends and develop sustainability policies. Zero-knowledge proofs verify data coverage, measurement precision, and temporal consistency without centralized data silos.

Example Use Case:

A research institute tokenizes a dataset of CO2 emissions across 50 cities over 10 years. A government agency purchases access to analyze trends and develop climate policy, using ZKPs to verify geographic coverage, measurement methodology, and data completeness. The institute earns DTK tokens while contributing to environmental action, and policymakers gain verified data for evidence-based decisions.

Applications:

- Climate modeling and forecasting
- Environmental impact assessments
- Sustainability metrics and ESG reporting
- Biodiversity conservation research
- Renewable energy optimization

EDUCATION & ACADEMIA

Collaborative Research Datasets

Universities and research institutions share experimental results, survey data, and observational studies while maintaining academic integrity. The marketplace provides verifiable data provenance, enabling reproducible research and cross-institution collaboration while compensating data collectors.

Example Use Case:

A university tokenizes student performance metrics across 10,000 students to study learning outcomes. Educational researchers purchase access, using zero-knowledge proofs to verify dataset size, demographic diversity, and academic metrics—without compromising student privacy. This enables evidence-based education policy development while protecting sensitive academic records and providing sustainable research funding.

Applications:

- Learning outcomes research
- Educational technology effectiveness
- Curriculum development studies
- Student behavior analysis
- Academic performance modeling

FEDERATED LEARNING

Collaborative AI Without Data Sharing

The Zero Knowledge Proof ecosystem enables privacy-preserving federated learning where multiple parties collaboratively train AI models without sharing raw data. Participants train local models, encrypt updates with AES-256, and submit zero-knowledge proofs of correct computation—enabling model improvement while maintaining complete data sovereignty.

Example Use Case:

Multiple hospitals collaborate to train a diagnostic AI model for rare diseases. Each hospital trains on local patient data, generates encrypted model updates, and submits ZKP proofs verifying computation correctness. An aggregator combines updates using secure multi-party computation, creating a superior model without any hospital exposing patient data. This approach accelerates medical AI development while maintaining HIPAA compliance and institutional privacy.

Applications:

- Healthcare AI across institutions
- Financial fraud detection networks
- Supply chain optimization
- Cross-border research collaboration
- Edge computing and IoT networks

Traditional data systems force a false choice: either share data and lose control, or maintain

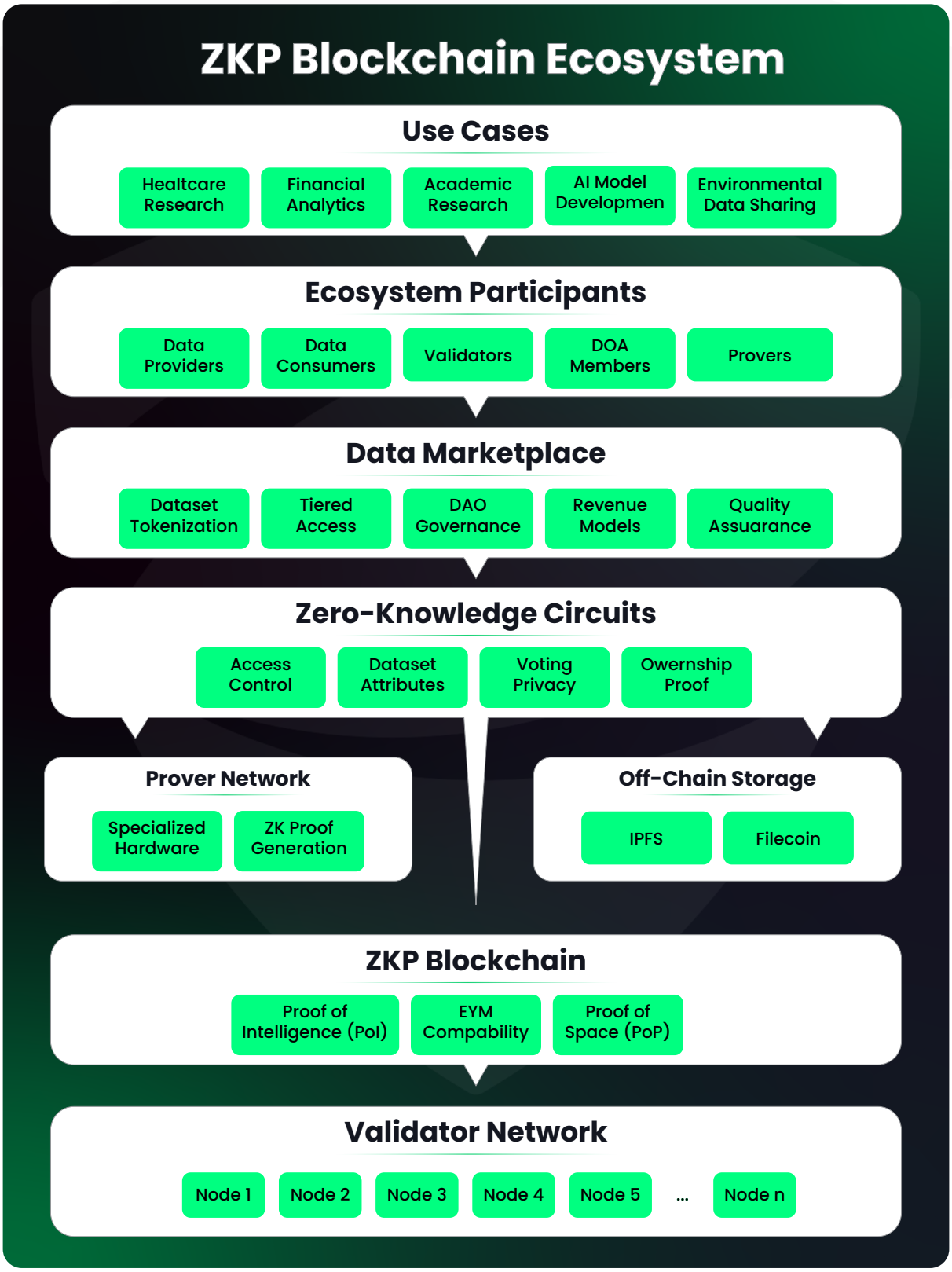
privacy and forgo collaboration. The Zero Knowledge Proof ecosystem eliminates this trade-off through cryptographic verification, enabling industries to unlock value from sensitive data while maintaining security, compliance, and ownership.

Every sector handling sensitive information—healthcare, finance, research, government—can benefit from privacy-first data infrastructure. The applications above represent just the beginning of what's possible when privacy and utility coexist.

TECHNOLOGY FOUNDATION

Built on Proven Innovation

The Zero Knowledge Proof ecosystem combines enterprise-grade blockchain infrastructure with advanced cryptography to create a platform that scales, secures, and sustains the privacy-preserving data economy.



BLOCKCHAIN ARCHITECTURE

Substrate Framework: Enterprise-Grade Foundation

The ZKP blockchain is built on Substrate, a modular framework created by Parity Technologies—the team behind Polkadot. Substrate powers multiple production blockchains collectively securing billions in value.

Modularity Through Pallets: Custom blockchain logic built as composable "pallets"—self-contained functionality that can be independently upgraded. Our PoI and PoSp pallets integrate seamlessly with Substrate's native consensus and governance.

Forkless Upgrades: Runtime logic runs in WebAssembly, enabling protocol changes through on-chain governance votes without network disruption.

Hybrid Consensus: Useful Work, Not Waste

Traditional consensus mechanisms either consume massive energy (Proof-of-Work) or concentrate power among wealthy stakeholders (pure Proof-of-Stake). ZKP's hybrid model rewards meaningful contributions.

Proof of Intelligence (PoI): Rewarding AI Work

Validators perform verifiable AI computations—matrix operations, neural network inference—that advance real AI development rather than mining arbitrary hash puzzles.

How It Works:
Network assigns computation tasks via verifiable random functions. Validators execute computations, generate zero-knowledge proofs of correctness, and submit for verification. Valid proofs earn ZKP coins and increase staking power.

Current Scope:
Matrix operations up to 100×100 dimensions, activation functions for vectors up to 1,000 elements, feedforward inference for models up to 10^5 parameters.

Proof of Space (PoSp): Validating Storage

Validators provide verifiable storage capacity, ensuring Data Marketplace datasets remain accessible without centralized infrastructure.

How It Works:
Validators allocate disk space (minimum 1TB), store encrypted dataset shards, and respond to cryptographic challenges—Merkle proofs verifying data possession without transmitting full datasets.

Energy Efficiency:
PoSp consumes ~10W per terabyte compared to Bitcoin's ~1MW per terahash/second—a 99% energy reduction while providing practical utility.

Combined Model

Staking Power = (0.3 × PoI Score) + (0.3 × PoSp Score) + (0.4 × ZKP Stake)

This balances computational contribution, storage provision, and economic commitment. Parameters adjustable through governance.

Consensus Integration:
Operates within Substrate's BABE+GRANDPA framework: BABE handles block production (~6-second blocks), GRANDPA provides finality (1-2 seconds).

Performance & Scalability

Current: 100-500 TPS with distributed validators
2028: 300-700 TPS through optimization
2029+: 800-1,000 TPS, with 3,000+ TPS on specialized parachains
Scaling mechanisms: transaction batching, recursive proof aggregation, horizontal scaling via Polkadot parachains.

Dual Runtime
EVM Compatibility: Substrate's EVM pallet supports Solidity contracts without modification, leveraging Ethereum's developer ecosystem.
WASM Performance: Native runtime achieves ~10^8 instructions/second for compute-intensive operations—AI inference, cryptographic operations, data processing.
Both runtimes share state through Patricia Tries, with the Executive pallet coordinating cross-runtime calls.

PRIVACY LAYER

Zero-Knowledge Proofs in Action

Zero Knowledge Proof's enable the core proposition: prove things about data without revealing the data.

Example:
Verify a healthcare dataset contains 10,000 patient records with specific distributions before purchase. The seller generates a cryptographic proof (~288 bytes). The buyer verifies in ~2 milliseconds on-chain, gaining certainty without seeing patient records.

Implementation:
zk-SNARKs using BLS12-381 curve provide ~128-bit security. Proofs verify in constant time through optimized on-chain verification.
Applications:

- Access control verification without revealing balances
- Data quality proof without exposing contents
- Private governance voting
- AI computation verification
- Storage availability confirmation

Data Encryption

- All marketplace data encrypted with AES-256-GCM (military-grade standard):
- 2^{256} keyspace resistant to brute-force attacks
- Provides confidentiality and authenticity
- Parallelizable for efficient large dataset encryption
- Keys remain under data owner control

Off-Chain Storage with On-Chain Verification

IPFS Integration:
Content-addressable storage where each dataset receives a unique Content Identifier (CID) from cryptographic hash. Tampering produces different CIDs, making modifications detectable.

Filecoin Layer:
Economic incentives for long-term data persistence through staking and rewards.

On-Chain Anchoring:
Only metadata—CIDs, ZKPs, access rules—stored on-chain in Patricia Tries. Lightweight footprint enables verification without blockchain bloat.

Redundancy:
Reed-Solomon erasure codes (10-of-16 configuration) allow reconstruction even if 6 shards are unavailable.

Privacy Without Compromise

Traditional privacy solutions force trade-offs. ZKPs eliminate this:

Privacy-Preserving Queries: Verify statistical properties, format compliance, quality metrics through ZKPs without decrypting data.
Selective Disclosure: Owners choose exactly what to reveal—prove patient count while keeping treatments private.
Verifiable Computation: AI models trained on encrypted data with ZKPs proving correct execution.

THE DATA MARKETPLACE

Where Privacy Meets Profit

The Zero Knowledge Proof Data Marketplace transforms how data is shared, valued, and protected—enabling monetization while maintaining ownership, privacy through cryptographic verification, and quality through community governance.

HOW IT WORKS

The marketplace operates through a streamlined process that puts data owners in control while ensuring buyers receive verified, quality datasets.

1. UPLOAD YOUR DATASET

Data providers upload datasets to the decentralized storage network (IPFS), where content is automatically encrypted using AES-256 military-grade encryption. The system generates a Content Identifier (CID)—a cryptographic hash that serves as both the dataset's address and integrity verification. This CID is anchored on-chain via Substrate's Patricia Tries, creating an immutable record while the actual data remains off-chain.

2. TOKENIZE YOUR DATA

The dataset becomes a blockchain-native digital asset through Substrate's native token standards (for divisible datasets) or unique asset pallets (for non-fungible datasets). Tokenization creates a tradeable asset with cryptographically verified attributes—size, format, quality metrics, statistical properties—all provable through zero-knowledge proofs without exposing the underlying information.

3. SET YOUR TERMS

Define your monetization strategy with complete flexibility:

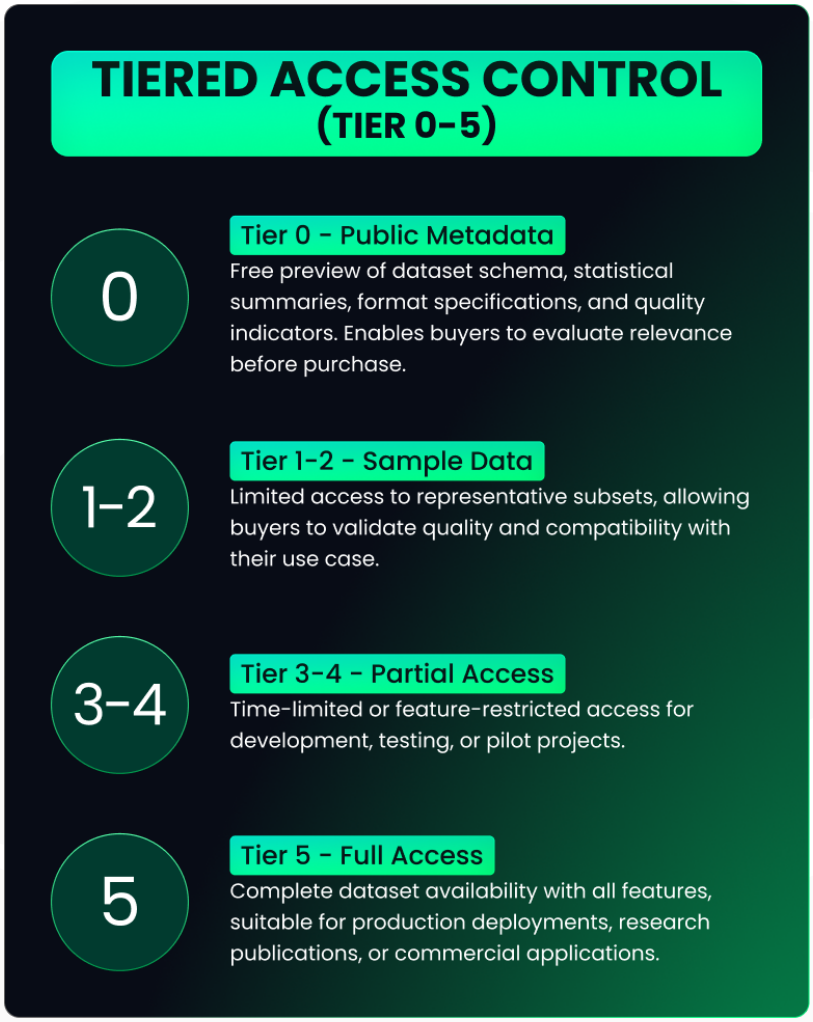
- **Access Tiers:** Configure graduated access from Tier 0 (free metadata preview) to Tier 5 (full dataset access)
- **Pricing Models:** Choose per-access royalties (recurring revenue) or one-time flat fees (bulk licensing)
- **Usage Rights:** Specify permitted use cases, attribution requirements, and licensing terms
- **Update Anytime:** Modify pricing, revoke access, or change terms—you maintain full sovereignty

4. EARN CONTUNUOUSLY

Each dataset access generates DTK token payments directly to your wallet. For high-value or frequently accessed datasets, this creates passive income streams. The marketplace handles all verification, access control, payment distribution, and dispute resolution automatically through smart contracts and native Substrate pallets.

Tiered Access Control (Tier 0-5)

The marketplace implements granular permission levels that balance discoverability with monetization:



Cryptographic Verification of Data Quality

Traditional data marketplaces rely on trust or post-purchase verification—creating friction and dispute risk. The ZKP marketplace solves this through cryptographic proof of dataset attributes before purchase:

Zero-Knowledge Attribute Verification

Buyers can verify critical dataset properties without accessing the data:

- Size Verification: Confirm dataset contains claimed number of records
- Format Validation: Prove data adheres to specified schema
- Statistical Properties: Verify distributions, completeness metrics, or quality scores
- Timestamp Authenticity: Confirm data collection period and freshness
- Source Provenance: Validate data origin and chain of custody

Technical Explanation

Data providers generate zk-SNARK proofs that encode dataset properties into cryptographic commitments. These proofs (typically 288 bytes) are verified on-chain in approximately 2 milliseconds through Substrate's verification infrastructure. Verification costs ~200,000 gas equivalent weight but provides buyers with mathematical certainty about dataset characteristics—eliminating the need for trust.

Example: A healthcare researcher can verify that a medical dataset contains exactly 10,000 anonymized patient records, follows HIPAA-compliant formatting, and includes specific diagnostic categories—all without seeing a single patient record or compromising privacy.

GOVERNANCE THROUGH DATA DAOs

Community-Driven Quality Standards

Data DAOs (Decentralized Autonomous Organizations) ensure marketplace quality through collective decision-making, preventing low-quality or fraudulent datasets while maintaining decentralization.

Dataset Approval Process

Preliminary Verification

- Before community voting, automated systems check datasets for:
- Duplication (cryptographic fingerprinting prevents identical datasets)
- Malware or malicious code (automated security scanning)
- Intellectual property concerns (metadata comparison against flagged sources)
- Basic quality thresholds (completeness, format compliance)

Community Voting

Datasets passing preliminary checks enter a voting period where DTK and ZKP coin holders evaluate quality, ethical compliance, and marketplace fit. Voting employs a tiered system:

Standard Decisions: Commitment-based voting for routine approvals (high frequency, lower stakes)

Sensitive Decisions: Zero-knowledge proof voting for controversial or high-value datasets (low frequency, higher privacy requirements)

Token-weighted voting ensures stakeholders have proportional influence, but with caps (5% maximum per participant).

Community Audit

Approved datasets undergo audit by selected DAO members based on staking activity and expertise. Auditors examine:

- Dataset completeness and schema consistency
- Absence of personally identifiable information (when required)
- Suitability for stated applications
- Ethical compliance with marketplace standards

Auditors stake their reputation, DTK and ZKP coins—fraudulent approvals result in slashing penalties

through Substrate's native slashing mechanisms.

Transparent Decision-Making

All governance activities occur on-chain via Substrate's democracy pallet:

- Voting records are public and auditable
- Proposal outcomes execute automatically through smart contracts
- Dispute resolution follows established protocols with appeal mechanisms
- Policy changes require community consensus with minimum voting periods

This transparency builds trust while maintaining participant privacy through zero-knowledge voting for sensitive decisions.

The Data Marketplace fundamentally reimagines data exchange: privacy-preserving by design, owner-controlled by default, quality-verified through cryptography, and governed by community consensus. This is how data should work.

WHAT WE'VE BUILT (SO FAR)

Proven Progress

The Zero Knowledge Proof ecosystem is operational with validated technology and concrete achievements.

OPERATIONAL TESTNET

Blockchain testnet live with core capabilities:

- Smart contract deployment via EVM pallet
- Token transactions processing
- Developer testnet access available
- First dApp operational in alpha-testing

TECHNICAL MILESTONES

Zero-Knowledge Proof Circuits

Initial ZKP circuits completed for basic AI operations (matrix computations up to 50×50 dimensions) and dataset attribute verification.

Substrate Framework Integration

Custom pallets developed:

- Initial PoI and PoSp mechanisms
- EVM pallet with Frontier compatibility
- Native WASM runtime

Decentralized Storage

IPFS integration operational with encryption layer (AES-256) and on-chain metadata anchoring via Patricia Tries.

SECURITY

Security Audits: Stage 1 initiated, additional audits scheduled for 2026

Technology Foundation: Built on Substrate framework, IPFS/Filecoin storage, BLS12-381 cryptography, WebAssembly runtime

EARNING OPPORTUNITIES

Multiple Revenue Streams for Participants

The Zero Knowledge Proof ecosystem offers diverse earning mechanisms for every level of participation—from passive income devices to active network validation to data monetization. Choose your path or combine multiple streams to maximize your ZKP coin earnings.

PROOF PODS: PASSIVE INCOME DEVICES

Your Gateway to Continuous ZKP Coin Generation

Proof Pods represent the most accessible entry point into the Zero Knowledge Proof ecosystem, transforming specialized hardware into a passive income stream that requires minimal technical expertise or ongoing effort.

What Are Proof Pods?

Proof Pods are purpose-built tablet devices designed specifically to generate zero-knowledge proofs for the Zero Knowledge Proof ecosystem. Unlike traditional mining equipment that consumes massive energy solving arbitrary puzzles, Proof Pods perform meaningful work: generating the cryptographic proofs that enable privacy-preserving verification across the entire ZKP Ecosystem.

Key Characteristics:

- Plug-and-Earn Simplicity: Connect to power and internet, run setup, start earning
- Energy Efficient: ~10W power consumption vs. 1,000W+ for traditional mining
- Specialized Hardware: Optimized for ZKP generation and cryptographic operations
- Network Essential: Critical infrastructure for marketplace privacy and security
- Scalable Investment: Upgrade tiers to increase earning potential

How Proof Pods Work

Your device serves as a dedicated prover in the Zero Knowledge Proof network, performing one core function that generates Zero Knowledge Proof coin rewards:

Zero-Knowledge Proof Generation

Proof Pods create cryptographic proofs that power the entire privacy-preserving infrastructure. When the marketplace needs to verify dataset attributes, confirm access rights, validate governance votes, or authenticate any operation without revealing sensitive data, your Proof Pod generates the mathematical proof that makes this possible.

The Process:

1. Your device receives proof generation requests from the network via off-chain workers
2. It executes specialized ZKP circuits (optimized cryptographic computations)
3. Generates compact proofs (~288 bytes) that verify computation correctness
4. Submits proofs to the blockchain for verification
5. Earns ZKP coins for each validated proof

Behind the Scenes: Your Proof Pod runs specialized software that coordinates with the blockchain, receives task assignments via verifiable random functions (ensuring fair distribution), generates proofs using optimized cryptographic circuits, and submits results for on-chain verification—all automatically.

Earning Potential: Real Numbers

Proof Pods generate ZKP coins daily based on their tier level, with earnings directly claimable as sovereign digital assets you fully own.

Tier 1: Entry-Level Earnings

- Device Cost: 249 dollars (one-time purchase)
- Daily Generation: Proof Pods earn $1 USD worth of $ZKP Coin per level, based on the ZKP price at the date of mining. The amount of $ZKP received will vary depending on the current presale stage price.
- Path to Higher Tiers: Each 100+ dollar $ZKP purchase unlocks next tier upgrade

*the actual ROI may significantly differ as it is dependent on the $ZKP price which may be highly volatile

Presale Opportunity: Lock in Early Pricing

The sooner you participate in the presale, the lower the $ZKP price. As the presale progresses through each stage, pricing increases deterministically from one stage to the next.

Your Proof Pod generates real ZKP coins that you fully own. These coins are sovereign digital assets with multiple uses: staking for more rewards, governance voting, validator operations, or holding as the network grows.

Purchase Proof Pod - Start Earning Daily

GENERAL COIN PRESALE

For those who want to participate in the ZKP ecosystem without running a Proof Pod, the public presale allows direct participation in the ZKP network through structured public allocation.

The ZKP presale unfolds across 25 transparent stages with deterministic pricing and fixed allocation mechanics.

As stages progress:

- pricing increases
- available allocation contracts
- network participation expands

The highest presale stage price is $0.02, with a public launch target of $0.04 per $ZKP.

35% of the total supply is allocated to the public presale (250B $ZKP).

Structured Stage Progression

The ZKP presale is designed to provide transparent public participation through a predictable and mathematically structured system.

Each stage contains:

- predefined pricing
- fixed allocation mechanics
- transparent progression

No private pricing.
No preferential access.
No insider allocations.

Public Participation Model

Every participant enters through the same public presale structure.

The system does not react emotionally.
It progresses mathematically.

As participation expands across stages, allocation availability decreases while pricing progresses transparently according to the structured presale model.

Claim at Mainnet

Participate in the public presale and access your $ZKP allocation through the ZKP Dashboard following network launch.

TESTNET PARTICIPATION

Earn While You Learn

Join the testnet to help build and refine the platform before mainnet launch—all while earning ZKP coins.

Testnet Pioneers:

- Test features before mainnet launch
- Earn ZKP Coins that unlock at mainnet
- Shape the platform with your feedback
- Provide critical feedback and receive ZKP coin rewards
- No cost to participate - free testnet coins provided

Early testers effectively earn free coins while helping refine the platform, with top testnet contributors receiving bonus allocations for exceptional participation.

Access Testnet - Start Earning Now

DATA MONETIZATION

Transform Your Data into Revenue Streams

Available in 2026

The Zero Knowledge Proof Data Marketplace enables individuals and organizations to monetize datasets while maintaining complete ownership and control—addressing the fundamental problem of centralized platforms that extract value from user data without compensation.

How Data Monetization Works

1. Tokenize Your Dataset

Upload your data to the decentralized storage network (IPFS), encrypt it with military-grade AES-256, and mint it as a blockchain token. Your dataset becomes a tradeable digital asset with cryptographically verified attributes—size, format, quality metrics—provable through zero-knowledge proofs without exposing the underlying data.

2. Set Your Terms

Define access tiers (Tier 0: free metadata preview Tier 5: full dataset access), pricing models (per-access royalties or one-time flat fees), and usage rights. You maintain sovereignty: update pricing, revoke access, or modify terms at any time.

3. Earn Continuously

Each time someone accesses your data, you earn DTK tokens. For high-value datasets, this creates passive income streams that compound as your data's reputation grows within the marketplace.

Pricing Models

Royalty-Based (Recurring Revenue)

Earn DTK tokens each time your dataset is accessed. Ideal for frequently referenced data like market research, ongoing datasets, or training data for AI models. Set your per-access price and watch earnings accumulate.

One-Time Payment (Bulk Licensing)

Sell extended access periods for a single upfront payment in DTK tokens. Suited for large datasets, proprietary models, or exclusive research data. Higher initial payout with predictable revenue.

Hybrid Approach

Combine models: charge per-access fees for standard use, with premium one-time licensing options for commercial applications or extended periods.

NETWORK VALIDATION

Secure the Blockchain, Earn Staking Rewards

Available in 2026

Network validators form the backbone of the ZKP blockchain's security and consensus mechanisms. Unlike energy-intensive Proof-of-Work mining, ZKP validation rewards useful computational work and storage provision.

Proof of Intelligence (PoI): Validate AI Computations

Validators earn ZKP coins by verifying AI computation tasks across the network—matrix operations, neural network inference, data transformations. Each validated task contributes to your PoI score, which directly influences your staking power and reward distribution.

How It Works:

Tasks are assigned via verifiable random functions to ensure fair distribution. You execute the computation (e.g., 100×100 matrix multiplication), generate a zero-knowledge proof of correct execution, and submit for on-chain verification. Valid proofs earn immediate ZKP coin rewards plus increased PoI score for future earnings.

Requirements: Moderate computational resources (modern CPU/GPU), technical familiarity with blockchain node operation, minimum ZKP coin stake (amount determined by governance).

Proof of Space (PoSp): Provide Decentralized Storage

Validators earn ZKP coins by committing storage space to the network and proving availability through cryptographic challenges. This ensures the marketplace's datasets remain accessible without centralized storage providers.

How It Works:
Allocate disk space (minimum 1TB recommended), store encrypted dataset shards, respond to periodic storage proofs via Merkle tree verification. Your PoSp score grows with storage capacity and uptime (99%+ uptime optimal).

Requirements: Available storage capacity, reliable internet connection, consistent uptime, minimal technical overhead beyond initial setup.

Combined Validator Earnings

The hybrid consensus model means validators earn through multiple simultaneous streams:

Block Rewards: Base ZKP coin issuance per block (distributed proportionally to staking power)
Transaction Fees: Share of network fees based on validation participation
PoI Task Rewards: Direct payments for AI computation validation
PoSp Storage Fees: Compensation for dataset storage and availability
Staking Multipliers: Bonus earnings from compounding your staked ZKP coins
Validator Staking Power Formula:
Staking Power = (0.3 × PoI Score) + (0.3 × PoSp Score) + (0.4 × ZKP Stake)
This balanced approach rewards diverse contributions rather than pure capital deployment.

Lower Barrier vs. Traditional Mining

Energy Efficiency: ~10W per TB storage vs. 1,000W+ for Bitcoin mining = 99% energy reduction
Hardware Costs: Standard servers/hard drives vs. specialized ASIC equipment = accessible to individuals
Useful Work: AI validation and storage provision vs. arbitrary hash computations = meaningful contributions
Scalability: Earnings scale with participation, not just hardware investment

PRESALE STRUCTURE

25 Transparent Stages – The ZKP presale unfolds through 25 transparent stages with deterministic pricing and structured allocation mechanics

Deterministic Progression – As stages progress, pricing increases and available allocation contracts

Public Participation – Every participant enters through the same public presale system

No Private Pricing – No insiders. No preferential access. No negotiated discounts.

Structured Expansion – The auction established the first layer of the network. The presale expands the ecosystem publicly.

WHY ACT NOW

Whether you choose Proof Pods to participate in the ZKP ecosystem or the public presale to acquire $ZKP directly, the ecosystem is now expanding through 25 transparent presale stages with deterministic pricing and structured public participation.

TOKENOMICS

Two Coins, One Ecosystem

The Zero Knowledge Proof ecosystem operates with a dual-coin architecture where each coin serves distinct yet complementary functions, creating a robust economic model that aligns incentives across all participants.

ZKP COIN: NETWORK SECURITY

The native cryptocurrency powering blockchain operations, security and governance.

Total Coin Supply

257,142,857,143 ZKP

ZKP has a fixed supply of ~257 billion tokens, reflecting long-term planning and token utility across compute, governance, and data markets.

ZKP Coin Allocation 257,142,857,143 Total Supply

Capped supply ensures deflationary pressure over time while enabling scaled reward distribution to provers, validators, and contributors.

Presale	Mining / Proof Rewards	Community & Ecosystem	Liquidity Provision	Team & Advisors
90 B ZKP | 35 %	141 B ZKP | 55 %	10 B ZKP | 4 %	8 B ZKP | 3 %	8 B ZKP | 3 %

Core Utilities:

Validator Rewards & Staking

Validators stake ZKP coins to participate in consensus, earning block rewards and transaction fees through hybrid PoI and PoSp mechanisms that reward computational contributions and storage provision

Governance Rights

Coin holders participate in decentralized governance through quadratic voting, deciding on protocol upgrades, parameters and ecosystem fund allocation.

Network Transaction Fees

All blockchain operations—smart contracts, data transactions —require ZKP coins for gas fees, creating fundamental demand tied to network usage.

Deflationary Mechanisms

A portion of transaction fees fund buybacks and potential burns, creating deflationary pressure as network activity increases.

Proof Pod Generation

Proof Pod devices generate ZKP coins daily based on tier level and network contribution, providing passive income while securing the network.

COIN SYNERGY

ZKP coins secure blockchain infrastructure and protocol governance, while DTK tokens power the application layer and data economy. Proof Pod operators earn ZKP for infrastructure provision; data providers earn DTK from marketplace activity. This separation ensures clear utility while creating natural economic flows between ecosystem layers.

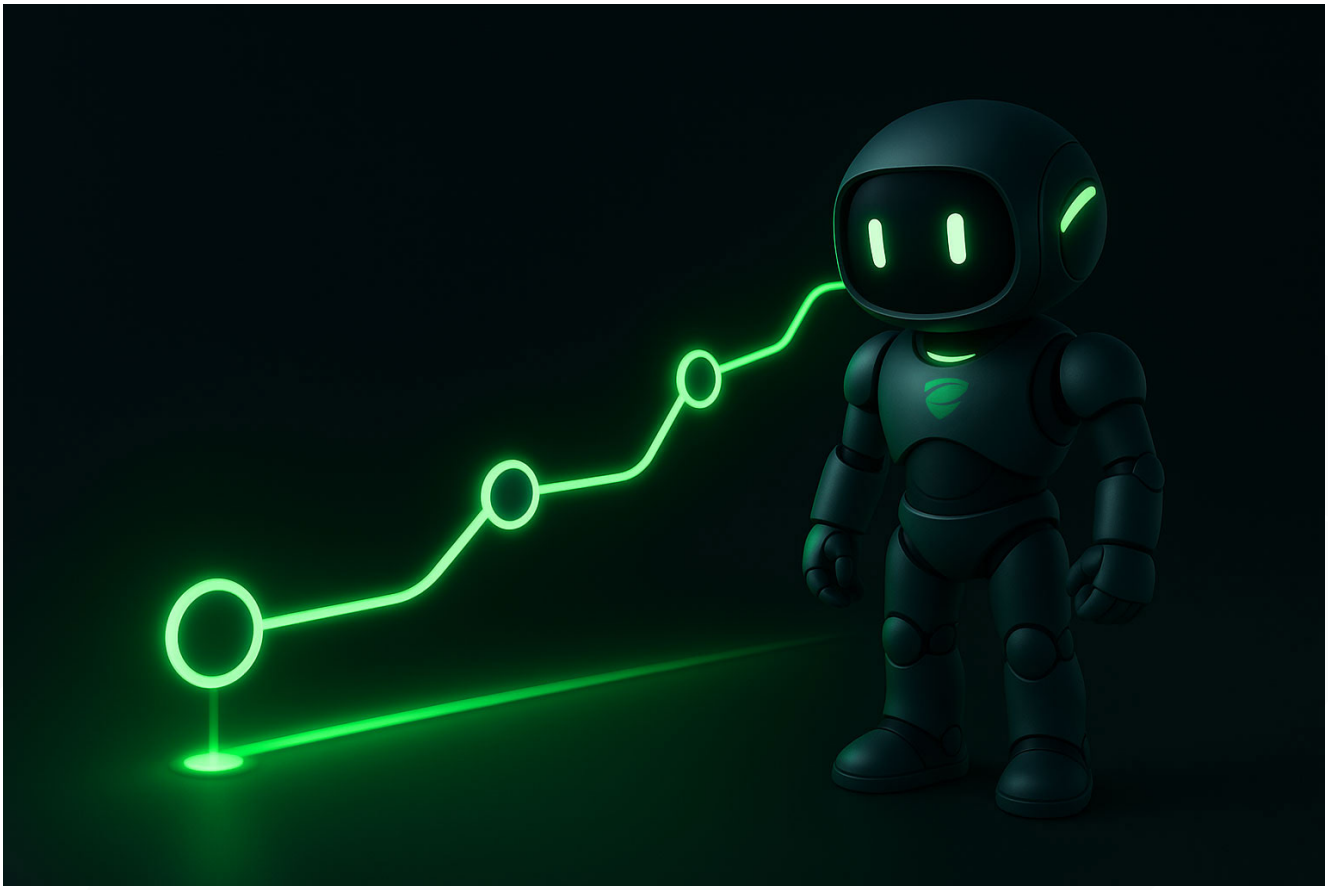
THE TEAM

THE HIDDEN ARCHITECTS

We build without names, yet our signatures shape chains.
We speak in code, yet the world listens.
Once, we helped design the walls that held the network together.
Now, we're building the doors that let proof move freely.

WHY THE MYSTERY?

In zero-knowledge cryptography, you can prove something is true without revealing the underlying details. Our team page works the same way.



ROADMAP & TRACTION

From Vision to Reality

Building the future of privacy-preserving AI through systematic execution and measurable milestones.

WHERE WE ARE (2024-2025)

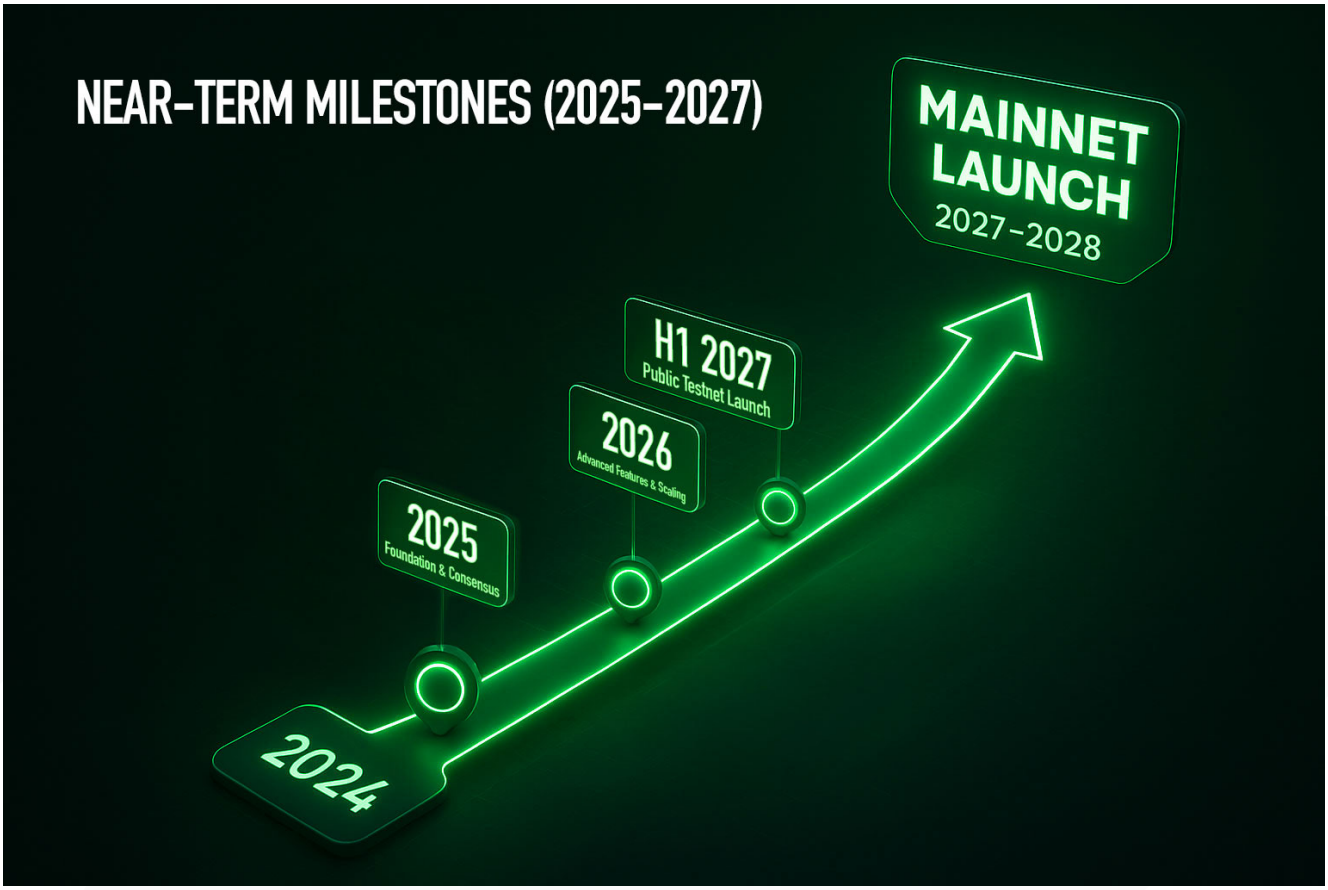
Testnet Operational - Blockchain live with smart contracts, token transactions, and consensus mechanisms.

ZKP Coin Presale - The ZKP public presale is now live, unfolding through 25 transparent stages with deterministic pricing and structured public participation.

Proof Pod Presale Active - Early adopters securing passive income devices generating zero-knowledge proofs.

Core Technology Validated - ZKP circuits, Substrate framework, IPFS integration, EVM compatibility

Strategic Partnerships - (TBA)



NEAR-TERM MILESTONE (2025-2028)

2025–2026: Foundation & Consensus

2026–2027: Advanced Features & Scaling

2028: MAINNET LAUNCH

LONG-TERM VISION (2029-2031)

2029: Performance Scaling

2030–2031+: Enterprise Grade & Global DePin Leadership

LONG-TERM VISION (2028-2030)

2028: Performance Scaling

300-700 TPS | Parachain integration | Complex AI models (10^5+ parameters) | Cross-chain marketplace

2029-2030+: Enterprise Grade & Global DePin Leadership

800-1,000 TPS | 3,000 TPS specialized parachains | Post-quantum security | Enterprise adoption

Quantum-resistant infrastructure | Institutional adoption | Industry standard for privacy-preserving AI

KEY METRICS TO WATCH

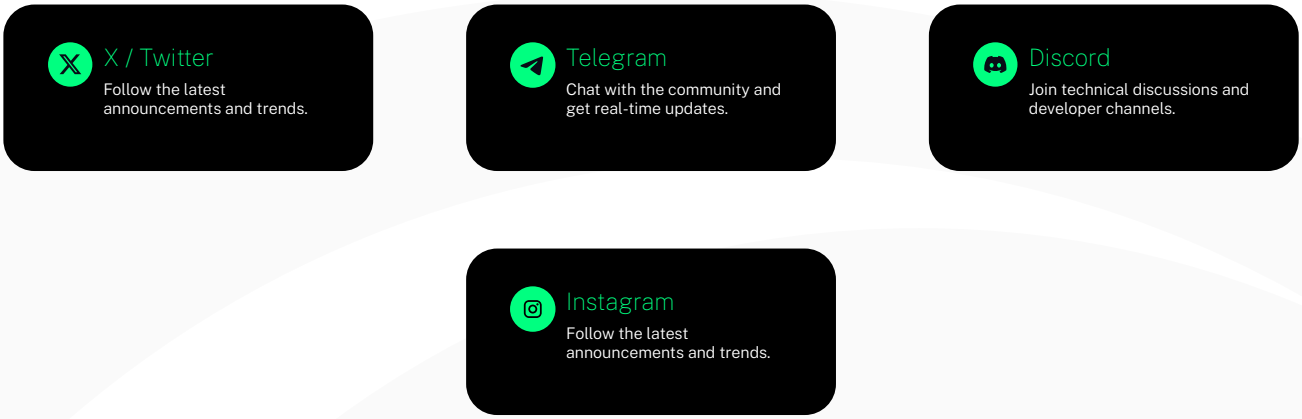
Metric	2025 (Testnet)	2027 (Mainnet)	2029-2030+
Network Participants	1000+	30,000+	100,000+
Transaction Throughput	100-200 TPS	100-500 TPS	1,000-3,000 TPS
Proof Pod Network	Early adopters	Thousands active	Global distribution
Data Marketplace	Testnet pilots	Organic growth	Commercial standard
Total Value Locked	Testnet stakes	Initial validator TVL	Substantial institutional TVL

TRANSPARENCY COMMITMENT

The roadmap is ambitious but grounded in proven technology. Every milestone brings us closer to a world where privacy and progress coexist.

COMMUNITY & SUPPORT

Join the Conversation:



Resources & Documentation:

Technical Docs: Developer guides, APIs, tutorials
Whitepaper: Complete technical specification
FAQ: Common questions answered
Blog: Project updates and insights

Support:

Support: support@zkp.com

Stay Updated

Subscribe to our newsletter for presale alerts, daily allocation updates, development progress, and exclusive insights:

RISK FACTORS & DISCLAIMERS

Important Considerations

INVESTMENT DISCLAIMER

The information contained in this document is for informational purposes only and does not constitute financial investment advice. Participation in the ZKP ecosystem, including the purchase of ZKP coins and/or Proof Pod devices, involves significant risks. Prospective participants should conduct their own due diligence and consult with qualified professionals before making any investment decisions.

Key Risk Factors

Technology Development Risk

The Zero Knowledge Proof ecosystem is currently in its testnet phase. While core functionality has been demonstrated, the platform is under active development. Features, performance metrics, and timelines described in this document are subject to change based on testing outcomes and technical requirements. There is no guarantee that all proposed features will be implemented as described or within projected timeframes.

Regulatory Uncertainty

The regulatory landscape for blockchain technology, cryptocurrencies, and decentralized data marketplaces is evolving globally. Changes in laws or regulations in any jurisdiction may adversely affect the development, operation, or value of the Zero Knowledge Proof ecosystem. Participants should be aware that future regulatory actions could impact their ability to use, transfer, or realize value from their participation.

Market Adoption Risk

The success of the Zero Knowledge Proof ecosystem depends on achieving meaningful adoption by data providers, consumers, validators, and developers. There is no guarantee that the platform will attract sufficient participants to create a sustainable and liquid marketplace. Network effects are critical to value creation, and insufficient adoption could impact the utility and value of ecosystem coins..

Coin Value Volatility

The value of ZKP coins may be subject to significant volatility and could decline substantially or become worthless. Coin values are influenced by numerous factors beyond the project's control, including market sentiment, regulatory developments, technological changes, and macroeconomic conditions. Past performance of similar projects does not guarantee future results.

Forward-Looking Statements

This document contains forward-looking statements regarding the Zero Knowledge Proof project's development, features, performance, and growth. These statements are based on current expectations and assumptions that involve risks and uncertainties. Actual results may differ materially from those expressed or implied in forward-looking statements due to various factors, including but not limited to technical challenges, market conditions, regulatory changes, and competitive dynamics.

Forward-looking statements include projections regarding earning potential, network performance (such as transaction throughput), adoption timelines, feature implementations, and market opportunities. These projections are estimates only and should not be relied upon as guarantees of future performance.

ZKP

The Revolution Begins With You

Earn ZKP coins. Build the ecosystem. Own the future.

Join Zero Knowledge Proof today.