Treasury Proposal: Ideal Network

Proponent: Ideal Labs - 1LX9m9Ee8u653hU1sxvvRNpV1ZjYExa7K8r9zjDws9GDLvp
Communication channels: Matrix | Discord | https://www.idealabs.network/
Date: 14.01.2025
Requested amount: 300,250 USDC (294,585 USDC + 840 DOT)
Short description: A Drand bridge parachain providing publicly verifiable randomness to the Polkadot ecosystem.
Project Category/Type: Software development Infrastructure
Previous treasury proposals:

- https://kusama.polkassembly.io/referenda/442

Discussion Post: https://polkadot.polkassembly.io/post/2693

The Randomness Layer for Polkadot's World Computer

1. Background and Context

Ideal Labs is developing the Ideal Network (IDN) as a comprehensive randomness solution for the Polkadot ecosystem. IDN' vision is to deliver an interoperable and decentralized entropy aggregation layer that serves as the foundational randomness infrastructure for Web3. Through extensive research and development, supported by the Web3 Foundation and ongoing collaborations with leading research institutions, the team has developed a deep understanding of verifiable randomness beacons and their crucial role in enabling fair, trustless protocols. This proposal outlines a pragmatic approach to delivering immediate value to the ecosystem while working toward IDN's long-term vision of a fully decentralized Randomness-Beacon-as-a-Service.

By starting with a bridge to Drand's battle-tested distributed randomness beacon and progressively enhancing IDN's capabilities, IDN aims to serve as the foundational randomness layer for Polkadot's World Computer, enabling fair and unbiased computation across its decentralized architecture.

1.1. Team Introduction

Ideal Labs was formed during the second cohort of the Polkadot Blockchain Academy (PBA) in Buenos Aires. The founding team members met while attending the academy, where the initial concept for the Ideal Network was conceived through discussions about on-chain secret sharing and timelock encryption.

Since graduating from PBA, the team has successfully advanced its original project into a comprehensive infrastructure solution for the Polkadot ecosystem.

Tony Riemer

Protocol Engineer

Former S.E. Fannie Mae, and Capital One.

B.S. Mathematics, UW-La Crosse

PBA alumni

https://www.linkedin.com/in/tony-riemer/
https://github.com/driemworks

Carlos Montoya

Serial Entrepreneur

5x CTO with Exit

M.S. Information Technology, Carnegie Mellon

PBA alumni

https://www.linkedin.com/in/cmonvel/
https://github.com/carloskiron

Juan Girini

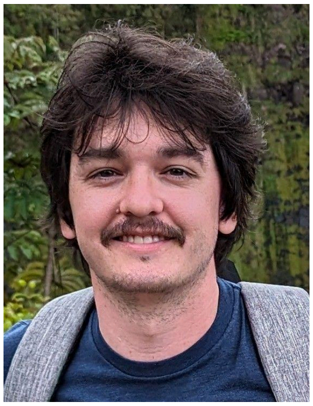
10+ Years Leading Engineering Teams

Former Core Eng. Parity

B.S. Information Systems Engineering, UTN

PBA alumni

https://www.linkedin.com/in/juan-girini/
https://github.com/juangirini



Coleman Irby

10+ Years Software Engineering Experience

Graduate Student of Physics

B.S. Electrical Engineering, University of Mississippi

https://www.linkedin.com/in/coleman-irby-229b13103/
https://github.com/colemanirby

1.2. Team’s Track Record

This work is strengthened through collaborations with key institutions including Web3 Foundation researchers, NIST for beacon protocol design insights, and University of Colorado's research group for novel randomness approaches. These partnerships ensure IDN’s implementation reflects the latest cryptographic advances while meeting Polkadot's practical needs.

The team has built significant foundations, having completed a Web3 Foundation grant for proof-of-concept development, participated in the Decentralized Futures program advancing IDN’s technical capabilities with BLS signatures and timelock encryption, deployed a prototype on Paseo testnet, received Kusama treasury funding for Ideal Lab’s Drand bridge, and has been awarded for Murmur, Ideal Lab’s keyless wallet protocol, at the 2024 Polkadot Hackathon.

1.3. Early traction and demand

Various teams within the Polkadot ecosystem have approached us seeking secure, verifiable randomness capabilities for their applications and parachains. Through discussions with these teams, Ideal Labs has identified an immediate need for randomness solutions that would enable critical features for their protocols.

Asset Hub

The Parity Contracts team is exploring an Asset Hub enhancement that would provide high-quality randomness-as-a-service through precompiles, enabling smart contracts to easily request and consume random bytes at dramatically lower costs compared to solutions like Chainlink VRF. This initiative, driven by contract developers' demand for reliable randomness, aims to provide a simple and intuitive interface that eliminates complex integration requirements while offering verifiable randomness - representing a foundational use case that would significantly benefit the Polkadot ecosystem through its cost-effective and straightforward approach.

Bittensor

Bittensor is a Substrate-based blockchain designed to incentivize and coordinate the collaborative training of machine learning models on a decentralized network. Ideal Labs worked closely with Bittensor while they developed their recently released commit-reveal V3 scheme, which is based on the Drand-bridge pallet previously developed along with the python-bindings of Ideal Lab’s Timelock encryption scheme.

While Bittensor operates as a solochain outside of the Polkadot ecosystem, this collaboration showcases the practical utility of the IDN in diverse applications, where it is used to enhance the security of decentralized machine learning networks. The solution, now in production, is an improvement on their previous scheme that serves as a consensus-critical component of the system.

ChainSafe

ChainSafe has expressed interest in collaborating to explore the development of a blockchain-native gaming framework, leveraging Ideal Network's timelock encryption and verifiable randomness capabilities. Timelock encryption has the potential to play a pivotal role in enhancing fairness and integrity in both traditional and blockchain-based games by ensuring synchronized access to game features and rewards. In traditional gaming, timelock prevents premature access to content, preserving game structure and maintaining player anticipation. For blockchain-based games, where in-game assets often hold real-world value, timelock is vital for economic security, safeguarding investments, and ensuring regulatory compliance. Timelock also enables synchronized, community-wide events and protects long-term rewards, fostering a cohesive and engaging gaming experience.
Some initial ideas have been outlined here as part of an ongoing exploration.

PolkaStorage

PolkaStorage is exploring randomness solutions for their core storage verification system, requiring secure and unpredictable randomness for multiple critical functions including storage challenges, proof of replication, and proof of spacetime verification. Their system needs to prevent storage providers from manipulating or predicting random values to avoid attacks like fake proofs, storage outsourcing, or data discarding. This represents a crucial infrastructure use case that could significantly enhance the security and reliability of decentralized storage on Polkadot through verifiable randomness integration.

2. Roadmap & Timeline

While IDN's vision is to become a native randomness solution for Polkadot, the scope of this proposal focuses on the distribution and cost of randomness to consumers, as opposed to generating randomness natively. This proposal covers the initial phase of the parachain, which is itself a complete product built specifically for the Polkadot ecosystem.

IDN is aimed to be in production by early Q2 2025.
🔎 Check out IDN's full roadmap.

3. Problem Statement

Blockchains face a fundamental challenge in generating unpredictable and unbiased random values within a deterministic computing environment. Polkadot's current randomness solutions are particularly constrained, with the native BABE Verifiable Random Function (VRF) primarily designed for validator selection and suffering from significant limitations. The primary issue lies in the temporal characteristics of existing randomness generation, which produces values only every four hours, unsuitable for low-latency randomness requests, such as in DeFi and Web3 gaming and creating substantial delays and potentially predictable outcomes that undermine the core requirement of true randomness in decentralized systems.

These limitations force Polkadot parachains into suboptimal strategies, compelling developers to create potentially less secure custom mechanisms, rely on expensive external oracles or compromise the fairness of their protocols. The current infrastructure lacks critical privacy-preserving mechanisms like timelock encryption, which prevents the implementation of sophisticated protocols with time-delayed information revelation. The Ideal Network addresses these challenges by providing a trustless and efficient randomness infrastructure that can be seamlessly integrated across the Polkadot ecosystem, enabling fair and unbiased computational environments while introducing privacy-preserving primitives that expand the potential of decentralized applications.

3.1. Current Solutions

The Polkadot ecosystem currently lacks a comprehensive solution for verifiable randomness, with existing approaches all having significant limitations. While simple and free to use, block hash-based randomness is one of the top 10 smart contract vulnerabilities. It has proven catastrophically insecure, as demonstrated by the $150 million Fomo3D exploit on Ethereum. Polkadot's native BABE VRF mechanism, designed for block producer selection, presents security concerns since collators can predict randomness in advance. Commercial VRF services like Chainlink come with substantial costs, high latency, and lack economic alignment with Polkadot.

While some ecosystems have implemented bridges to the Drand network, like Nois for Cosmos and DIA's xRandom for EVM chains, these solutions either rely on complex oracle networks or don't take full advantage of Drand's capabilities like timelock encryption. The Polkadot ecosystem would benefit from a more efficient, natively integrated randomness solution that maintains security and verifiability while aligning with its economic model. Currently, no major integrations of external VRF solutions exist within Polkadot, leaving a significant gap in the ecosystem's infrastructure.

🔎 More details about current solutions can be found here.

3.2. Real-life examples and Use cases

Protocol Security & DeFi

- Fair leader election protocols
- Front-running protection via random transaction ordering
- Fair parachain slot auctions and trustless atomic asset swaps
- Unbiased DEX order matching and liquidity rebalancing
- Timelock-protected trading strategies

Gaming, NFTs & Token Distribution

- Verifiable random drops and loot boxes
- Fair matchmaking and tournament selection
- Dynamic game events and NFT trait generation
- Provably fair card shuffling
- Fair token distributions and airdrops
- Protected criteria reveals and vesting schedules

Governance & Resource Allocation

- Random selection of reviewers and committee members
- Unbiased governance polling and delegation
- Private voting with delayed reveals
- Fair distribution of parachain resources
- Time-bound identity and access management

4. Proposal Scope and Solution

Ideal Labs proposes delivering a trustless Drand bridge that makes secure randomness and timelock encryption accessible across Polkadot through three components:

- a cross-chain randomness delivery service;
- an optimized Drand bridge implementation;
- and a monitoring interface.

This solution enables parachains to access verifiable randomness efficiently by sharing verification infrastructure, reducing overhead, and enabling smart contract and runtime integration through XCM, allowing teams to focus on building applications rather than maintaining randomness infrastructure.

🔎 Check out IDN's Solution Architecture Overview.

4.1. Benefits for Polkadot Stakeholders

The Ideal Network delivers substantial value across the Polkadot ecosystem by providing standardized, secure randomness infrastructure. For developers, it offers seamless XCM integration and reduced costs through shared infrastructure. End users benefit from enhanced fairness and transparency in applications at lower costs. For the broader ecosystem, it provides standardized randomness infrastructure, reduces duplicated efforts, and increases security through professional audits.

4.2. Milestones anld Deliverables

Under this proposal, the Ideal Network will deliver a comprehensive suite of components designed to make secure, verifiable randomness readily accessible across the Polkadot ecosystem.
🔎See the Milestones and Deliverables Breakdown.
Progress updates will be communicated through reports posted on the Polkadot Forum with reshares in the original post on Polkadot's governance platform and the Polkadot Direction matrix channel.
Ideal Labs will maintain a public Kanban board on GitHub to provide real-time tracking of progress, complementing the regular communication updates.

5. FAQ

🔎 If you have additional questions, please refer to the FAQ document available at this link: FAQ Document.

If you couldn’t find your answer, leave a comment!

6. Budget

Internal Work

Tasks	ETA (hs)	Notes
Trustless Drand Bridge	280	Not overlapping with previous funding: see here and here.
IDN Manager Pallet	320	
IDN Consumer Pallet	360	
Ink! IDN Bridge Contract	280	
Network Explorer Interface	360	
IDN Parachain	40	This covers retroactive and future work
Deployment & Monitoring	40	This covers retroactive and future work
TOTAL	1,680	$191,520 @ $114/h

External Costs

Tasks	Cost	Notes
Security Audit		See IDN Phase 1: SR Labs
- Drand Bridge	$24,700	These costs are determined by SR Labs.
- IDN Manager Pallet	$20,900	
- IDN Consumer Pallet	$18,050	
- ink! IDN Bridge Contract	$16,150	
- Network Explorer Interface	$10,450	
IDN Parachain	$5,665	840 DOT (EMA30 = 6.743 USD/DOT) See IDN Hosting & Infrastructure
Deployment & Monitoring	$12,815	See IDN Hosting & Infrastructure
TOTAL	$108,730	