SUPRA

DYOR SERIES
V1.0 | FEB 2024

Supra dVRF
Distributed Verifiable Random Function

Unbiased On-Chain Randomness
Powered by DKG

IN A NUTSHELL

Supra dVRF generates randomness with lightning-fast response times for a seamless experience—ideal for gaming, chance events, lotteries and NFT crafting.

USE CASES

Random Sampling

VRFs are used to randomly select block leaders, assign validators to shards, generating loot box rewards, and are useful for DAO-related activities.

NFT Crafting

Generate NFT attributes according to rarity scores, evolve in-game assets with Dynamic NFTs, and provide on-chain provenance of the asset's fidelity.

GameFi

Fairplay is inherently engaging, making on-chain lotteries, odds-based games, matchmaking, character spawning, and landing critical hits a more enjoyable experience.

KEY BENEFITS

Distributed Key Generation

Clans serve dVRF requests using Non-Interactive Distributed Key Generation and threshold cryptography to aggregate partial unique signatures, ensuring guaranteed output delivery that is tamper-proof and unbiased.

Blockchain Agnostic

Request randomness directly to your dApp on Supra's blockchain or get it delivered to your desired destination chain.

Low-Latency

No more waiting around for your loot. On-chain randomness can be had in a matter of seconds, even during times of high traffic when other networks suffer degraded performance.

Publicly verifiable on-chain

Aggregated keys and randomness outputs are publicly verifiable on-chain, demonstrating the transparency needed to lend credibility to chance events online.

PROBLEM IT SOLVES

Asymmetrical Knowledge and Bias

Everyone has a chance with unpredictable and unbiasable outcomes, and dVRF brings the receipts to prove it. Nodes can only generate randomness by aggregating partial signatures upon request in a provable secure manner.

Slow Response Times Are History

VRF Clans service 'Pull' requests, aggregate keys, and publish cryptographic proofs to destination chains within a matter of seconds.

Minimize Gas Fees

A highly efficient and elegant design means on-demand yet cost-effective RNG service for a range of Web3 use cases.

OUR VISION

Fairness & Integrity

Randomness ensures fairness, and promotes integrity in decentralized networks, financial matters, and in games. It is essential when it comes to achieving fair outcomes whether it be between best friends or strangers online.

Security Against Exploits

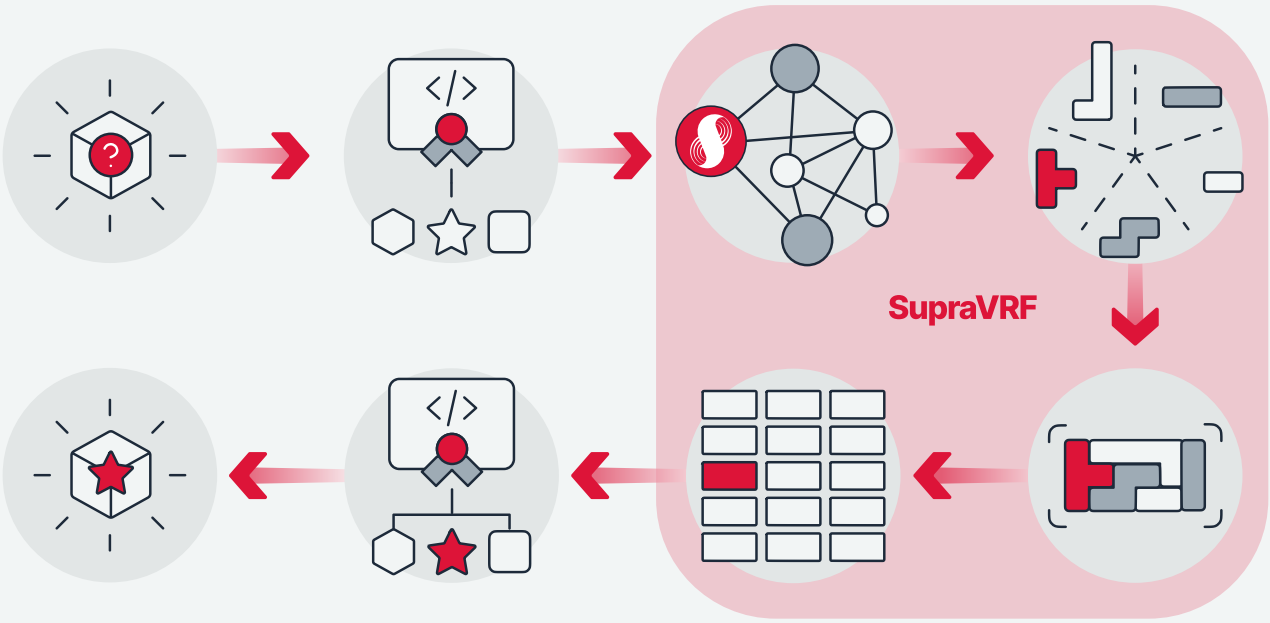
Predictable patterns are often exploited in DeFi, and many times by bots. By introducing elements of unpredictability, dVRF makes it impossible for malicious actors to execute front-running attacks or manipulate outcomes to their advantage.

Trustlessness & Tamper Resistance

Ensuring that dApps are tamper-proof and unbiasable ultimately accelerates adoption and provides longevity for dApps. It turns out that users stick around longer when they know things aren't stacked against them.

HOW IT WORKS

Consider the process behind a DeFi user opening a loot box. First, dVRF clans "listen" for random number generation (RNG) requests, take inputs and construct partial signatures (aka VRF outputs) to generate tamper-proof randomness along with an on-chain proof of its fidelity.



This request is done by distributed sets of nodes to maintain the unpredictability and integrity of the whole experience. These VRF nodes produce partial signatures, akin to the scattered pieces of a puzzle, which prevents tampering or unfairly anticipating outputs beforehand.

Next, VRF clans aggregate these partial signatures to collaboratively form a threshold signature. This aggregated signature is then securely written onto the destination blockchain, providing a history of provenance and public verifiability. The generated random number is inextricably linked to the potential prizes available, meaning a number corresponds to the contents of the opened loot box.

Every step, from the initial request for RNG to the delivery of the loot box contents, is transparently recorded on the blockchain. This transparency not only ensures the integrity of the process but also allows users and observers to validate outcomes, lending credibility to chance events which use random sampling and RNG.

WHO IS IT FOR?

GameFi Developers

Tamper-proof unpredictability mimics real-life randomness and improves engagement.

DeFi Developers

Adding a cost-effective layer of verifiable randomness attracts larger audiences in an industry that increasingly demands on-chain provenance.

DAO Boards

Lend credibility to the decentralized governance process by implementing elements of provable randomness.

Generative Artists

Combine generative art with the dVRF to craft a collection of thousands of NFTs, and provide everlasting proof that the distribution was done without bias.

ADDITIONAL NOTES & RESOURCES

Read litepaper

Watch video breakdown

View whitepaper