Understanding VRF

Grasping the essence of Gelato VRF and its pivotal role in blockchain randomness. After reading this page:

- You'll grasp the importance and challenges of generating randomness on the blockchain.
- You'll learn how Gelato VRF works and why it's trustworthy. *

What is Verifiable Random Function (VRF)

A VRF or Verifiable Random Function is a unique blend of cryptographic techniques that generates pseudorandom numbers in a publicly verifiable manner. Think of VRF as a way to generate random numbers where:

- The entity possessing a secret key can compute the random number and also provide a proof of its correctness.
- Anyone with the public key can verify that the random number was indeed computed correctly, ensuring the integrity of the result.
-

In simple terms, VRFs are like cryptographic hash functions but with an added layer of public verification. They're an essential tool in systems where the trustworthiness of random outputs is highly important.

Gelato VRF and Trustworthy Randomness

Gelato VRF offers real randomness for blockchain applications by leveraging Drand, a trusted decentralized source for random numbers. With Gelato VRF, developers get random values that are both genuine and can be checked for authenticity.

Applications of Gelato VRF:

The potential applications of a reliable and transparent random number generator on the blockchain are vast. Here are just a few use cases:

- Gaming and Gambling:
- Determine fair outcomes for online games or decentralized gambling applications.
- Decentralized Finance (DeFi):
- Use in protocols where random selections, like lottery systems, are required.
- NFT Generation:
- Randomly generate traits or characteristics for unique digital assets.
- Protocol Decision Making:
- In protocols where decisions need to be randomized, such as selecting validators or jurors.
-

Last updated3 months ago On this page *What is Verifiable Random Function (VRF) * Gelato VRF and Trustworthy Randomness * Applications of Gelato VRF: