Chainlink VRF

Get Started

Access verified randomness atvrf.chain.link .

Chainlink VRF (Verifiable Random Function)is a provably fair and verifiable random number generator (RNG) that enables smart contracts to access random values without compromising security or usability. For each request, Chainlink VRF generates one or more random values and cryptographic proof of how those values were determined. The proof is published and verified onchain before any consuming applications can use it. This process ensures that results cannot be tampered with or manipulated by any single entity including oracle operators, miners, users, or smart contract developers.

Security Considerations

Be sure to review your contracts with thesecurity considerations in mind.

Use Chainlink VRF to build reliable smart contracts for any applications that rely on unpredictable outcomes:

- Building blockchain games and NFTs.
- Random assignment of duties and resources. For example, randomly assigning judges to cases.
- Choosing a representative sample for consensus mechanisms.

To learn more about the benefits of Chainlink VRF v2, see our blog postChainlink VRF v2 Is Now Live on Mainnet. For help with your specific use case,contact us to connect with one of our Solutions Architects. You can also ask questions about Chainlink VRF onStack Overflow .

Two methods to request randomness

Chainlink VRF v2 offers two methods for requesting randomness:

- Subscription : Create a subscription account and fund its balance with LINK tokens. Users can then connect multiple consuming contracts to the subscription account. When the consuming contracts request randomness, the transaction costs are calculated after the randomness requests are fulfilled and the subscription balance is deducted accordingly. This method allows you to fund requests for multiple consumer contracts from a single subscription.
- Direct funding : Consuming contracts directly pay with LINK when they request random values. You must directly fund your consumer contracts and ensure that there are enough LINK tokens to pay for randomness requests.

Choosing the correct method

Depending on your use case, one method might be more suitable than another. Consider the following characteristics when you choose a method:

Subscription methodDirect funding methodSuitable for regular requestsSuitable for infrequent one-off requestsSupports multiple VRF consuming contracts connected to one subscription accountEach VRF consuming contract directly pays for its requestsVRF costs are calculated after requests are fulfilled and then deducted from the subscription balance. Learnhow VRF costs are calculated for the subscription method .VRF costs are estimated and charged at request time, which may make it easier to transfer the cost of VRF to the end user. Learnhow VRF costs are calculated for the direct funding method .Reduced gas overhead and more control over the maximum gas price for requestsHigher gas overhead than the subscription methodMore random values returned per single request. See the maximum random values per request for theSubscription supported networks .Fewer random values returned per single request than the subscription method, due to higher overhead. See the maximum random values per request and gas overhead for theDirect funding supported networks .You don't have to estimate costs precisely for each request. Ensure that the subscription account has enough funds.You must estimate transaction costs carefully for each request to ensure the consuming contract has enough funds to pay for the request.Requires a subscription accountNo subscription account requiredVRF costs are billed to your subscription account.Manage and monitor your balanceNo refunds for overpayment after requests are completedFlexible funding method first introduced in VRF v2.Compare the VRF v2 subscription method to VRF v1.Similar funding method to VRF v1, with the benefit of receiving more random values per request than VRF v1.Compare direct funding in VRF v2 and v1 .

Supported networks

The contract addresses and gas price limits are different depending on which method you use to get randomness. You can find the configuration, addresses, and limits for each method on the following pages:

- Subscription Supported networks
- Direct Funding Supported networks

To learn when VRF v2 becomes available on more networks, follow us onTwitter or sign up for ourmailing list .