

Winnables Infrastructure

This document aims to provide an overview of how the system is architected to make everything work at Winnables. For a quick reminder, Winnables is a Blockchain-based raffle system that allows site administrators (admins) to create raffles and site users (players) to purchase tickets to participate to the raffle and attempt to win NFTs or cryptocurrencies. At the end of each raffle (or when the last available ticket has been purchased), an admin can trigger the draw for a random winner.

Winnables's software suite is comprised of 3 main component:

- A set of smart contracts (Core contract + ticket contract)
- An HTTP API which itself can be broken down to
 - A Node.JS service listening for requests
 - A MariaDB database
 - A Redis in-memory base for request caching and user sessions
- And a front-end website providing a clean user interface to allow players to interact with this whole system.

At Winnables, every ticket purchased is numbered. For example, if a raffle has 10,000 tickets, players will be able to purchase tickets numbered from #0 to #9999. To ensure a greater level of fairness, there will be a maximum number of tickets any one player is allowed to hold. This is a measure put in place to prevent players with higher budget to tilt the balance too much in their favour. Of course, you can still increase your chances of winning by purchasing more tickets within a reasonable range. That range will be decided by the admin at the moment of creating the raffle.

When drawing a winner. Winnable's smart contract will request a random number from the decentralized Oracle Chainlink using VRF (Verifiable Random Function) v2. The response is a very large number comprised from 0 to $2^{256} - 1$. Using a modulo (remainder of a division), this number will be brought down to the range of available tickets and a single winning ticket will be drawn. Whoever holds the winning ticket at the moment of drawing the winner will receive the prize.

Winnables Infrastructure

