Onchain zkVRF

Making randomness collective, trustless, permissionless

Chee, Wenkang, Flying Nobita

Problem

How can we have randomness for onchain turn-based games?

Fairness

Transparent

Decentralized

Randomness contributed by all players

Collective

Trustless

Player’s randomness is committed (hiding & blinding) with circuit testification on every round

Permissionless

All players can contribute (unlike oracles)

Solution

Pre-game commitments, with per-round additive randomness generation

Opportunity

Why Build with Aleo?

Intuitive Language (Leo)

No need to worry about Constraints

Build-in Privacy

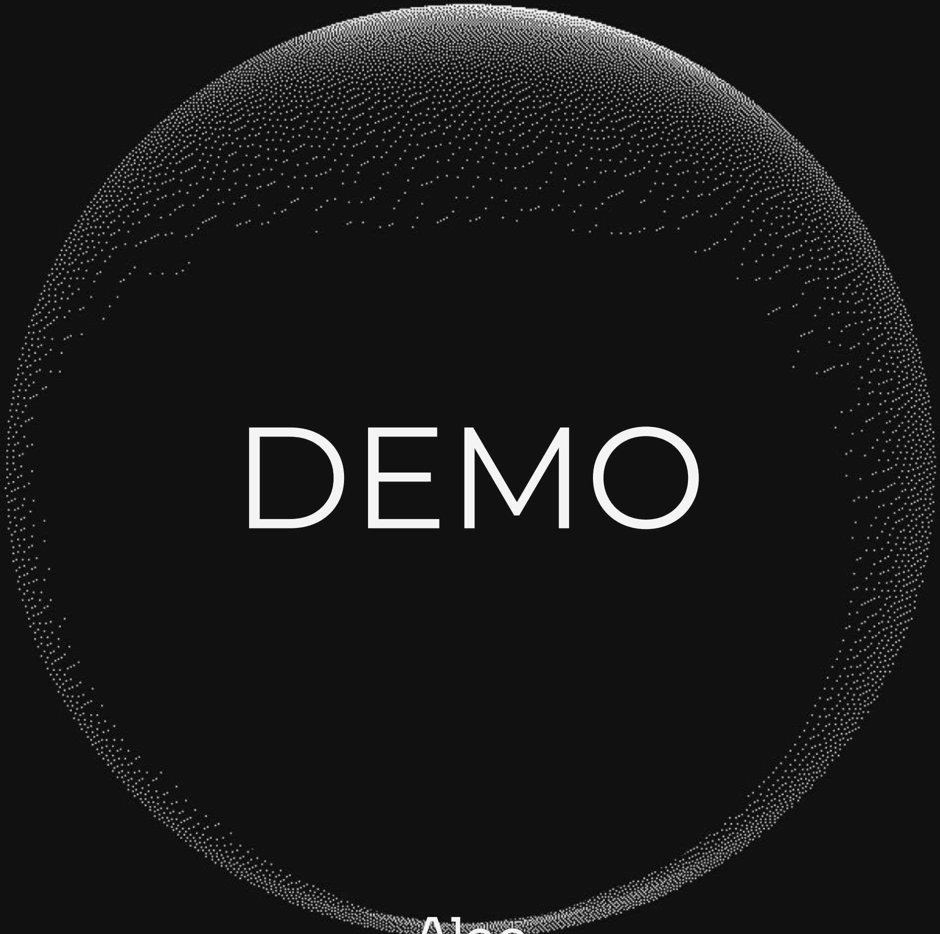
How it works

Pre-game

- User Secret Hash
- Game Hash = combination of everyone’s User Secret Hash

Every Round At Each Player

1. Randomness - hash function of:
    1. User Secret
    2. Game Hash
2. Circuit: User Secret hash == Pre-game User Secret Hash



DEMO

Aleo

Thank you!

Onchain zkVRF

Making randomness trustless, permissionless

Chee, Wenkang, Flying Nobita