Guess the Seed: A Blockchain-Based Competitive Game Powered by LLMs

amaury.delille, arthur.lefebvre, remi.brenaut

July 2025

Use Case Description

Generative AI has made it possible to create realistic and compelling images from textual prompts or numerical seeds. In this project, we explore a creative competition where participants try to guess the seed value (a sentence, a keyword) that was originally used to generate a given image. This introduces an engaging challenge that tests participants' intuition and understanding of image generation behavior.

To bring fairness, transparency, and automation to this competition, we implement it as a smart contract on the Tezos blockchain using the SmartPy language.

Why Use a Smart Contract?

A smart contract ensures that:

- **The game is trustless:** No central authority is needed to hold funds or enforce the rules.
- **All participants are treated fairly:** Game logic (entry fee, guesses, deadlines, rewards) is encoded transparently and cannot be changed during the game.
- **Rewards are distributed automatically:** Once the game concludes, the winner receives the reward directly from the contract.

Using a public blockchain like Tezos also allows for permanent records of participation, verifiable randomness (off-chain), and low-cost smart contract execution.

Architecture

The system is composed of three main components: a frontend interface where users interact with the game, an off-chain backend that handles image generation and similarity computation, and an on-chain smart contract deployed on Tezos to enforce game rules and handle rewards. All of those components interact with each-other to ensure the good functionning

of the dApp. The following diagram summarizes how these components interact throughout the game lifecycle.

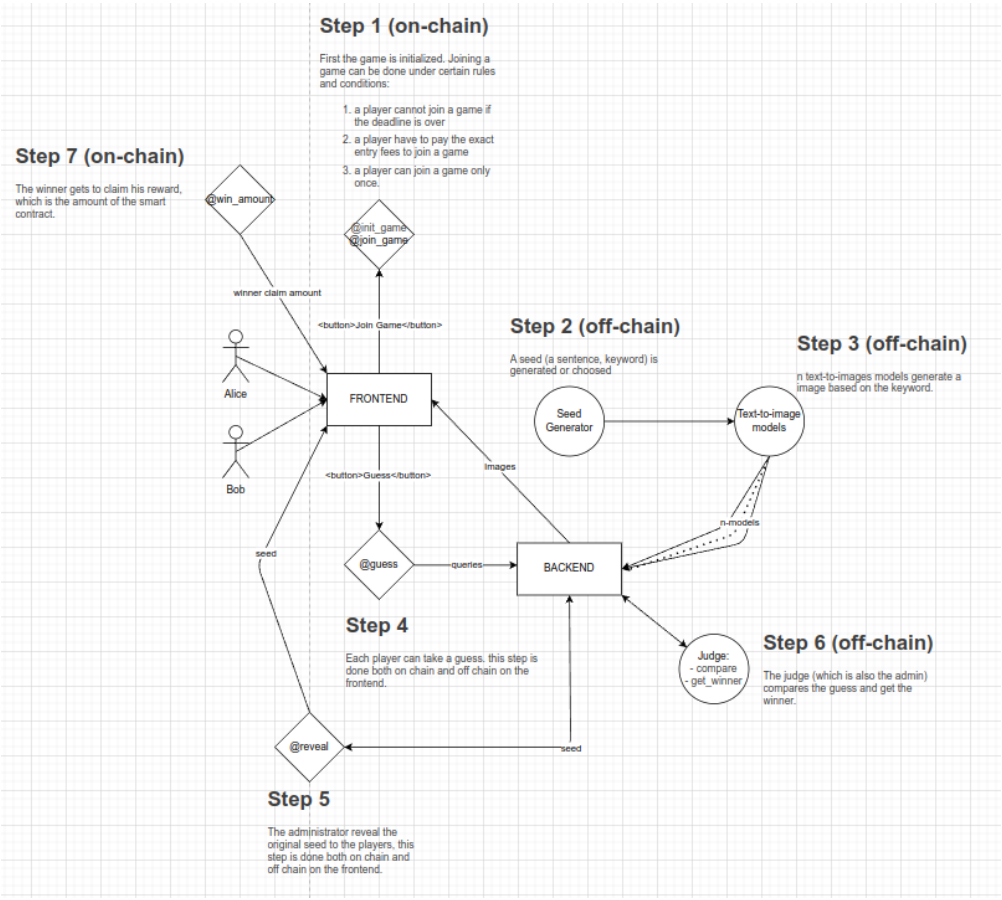

Figure 1: Diagram architecture

The Machine Learning Component

The heart of this game lies in comparing human guesses to the original seed. For that, we use a powerful and efficient language model: `Qwen/Qwen3-Embedding-0.6B`. This model transforms text inputs (like the original seed and the player guesses) into high-dimensional embeddings, numerical vectors that capture semantic meaning.

Once embedded, we compute the **cosine similarity** between the original seed and each player's guess. The guess with the highest similarity is considered the closest, and the corresponding player is declared the winner.

This judgment is performed off-chain using the following steps:

1. Encode the original seed into a vector using the embedding model.
2. Encode each player's guess the same way.
3. Compute cosine similarity between the seed and each guess.

4. Determine the highest-scoring guess and assign the corresponding address as the winner.

This hybrid AI+blockchain design ensures both creative freedom (natural language guessing) and rigorous, automated evaluation. This system can be found in the file named `model.py`, it is a prototype of our machine learning system, this file is not mean to be run itself.

Main Features of the Smart Contract

Our smart contract supports the following features:

1. **Player Registration:** Anyone can join a game by paying a fixed entry fee (e.g., 1 tez).
2. **Guess Submission:** After joining, a player can submit one guess for the seed that generated the image.
3. **Deadline Enforcement:** Players can only join or submit guesses before the predefined deadline.
4. **Winner Declaration** After the deadline, the organizer computes the closest guess off-chain and sets the winner address.
5. **Reward Claim:** The winner can claim the entire amount of tez stored in the contract. This amount comes from the entry fee.

Future Improvements

This project may be extended in the future by:

- Automating winner selection using zero-knowledge proofs or a trusted randomness oracle.
- Storing the generated image's hash or metadata on-chain for added auditability.
- Supporting multiple rounds of gameplay with a single contract.

Conclusion

This project demonstrates how smart contracts on Tezos can enable new forms of decentralized, creative competition. By combining AI with blockchain, we unlock novel game mechanics that are fair, trustless, and censorship-resistant.