TR.I.G.O

TRustless
Implementation of
Gambling
Online

Powered by OASIS

ETHGlobal Cannes 2025

The problem:

Would you play Poker with him ?

Probably not...
But that's what might be happening in some online casinos

The problem:

There is just **no way to be certain** that the online gambling site is playing fair.

- the number of ways the site could be cheating is extremely high,
- the difficulty of tampering with the games is too low, and
- the likelihood catching the House red-handed and face consequences might be close to none.

In other words, the first gamble is whether you are the mark or not

The solution:

TR.I.G.O. makes it possible to significantly reduce the risks the player is taking.

For example in poker games, it ensures the house cannot mess things up by preparing decks instead of shuffling, or mess with the shuffled deck of cards, peek on the cards given to the player

TR.I.G.O. leverages the features of **OASIS Sapphire and ROFL**, an EVM blockchain that allows to use (P)RNG in Smart Contracts and have them run in a **TEE** that ensures confidentiality of data.

What TR.I.G.O. does :

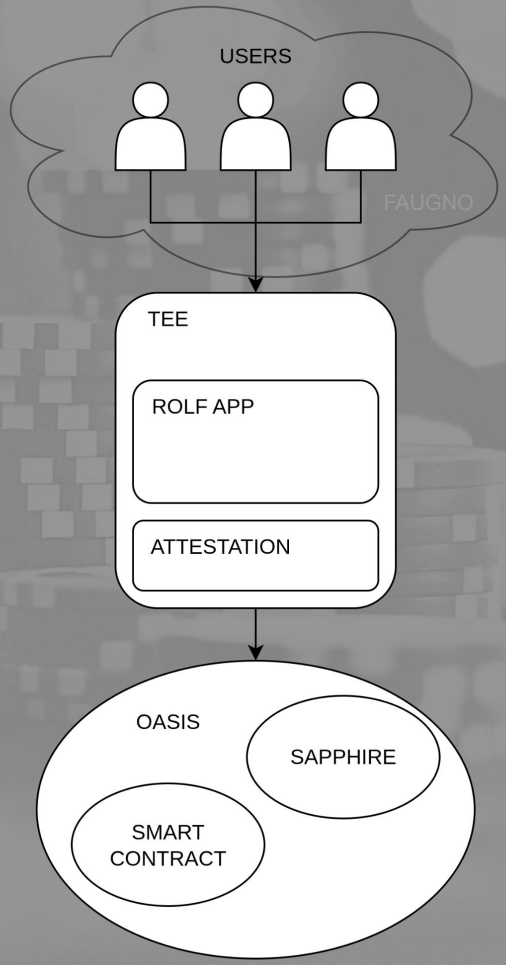
- deck shuffling is done in the **smart contract**
- provides a **commitment** on the deck state
- the cards are **verifiably** handed out in the right order
- cards are encrypted with **user's public key** to ensure no one else can see them
- is game agnostic, **can be used to play any game**: Poker, Black Jack, Ma Jong, Domino...
- game rules can be encoded in **ROFL**

and... might even allow P2P gambling without even the House !

Demo:

As a POC we implemented a simple game of **Black Jack** where users plays against the House (Smart Contract)

The House and the Player share a **commitment** on the shuffled deck of cards and check that the cards were given in the right order respecting the initial shuffle

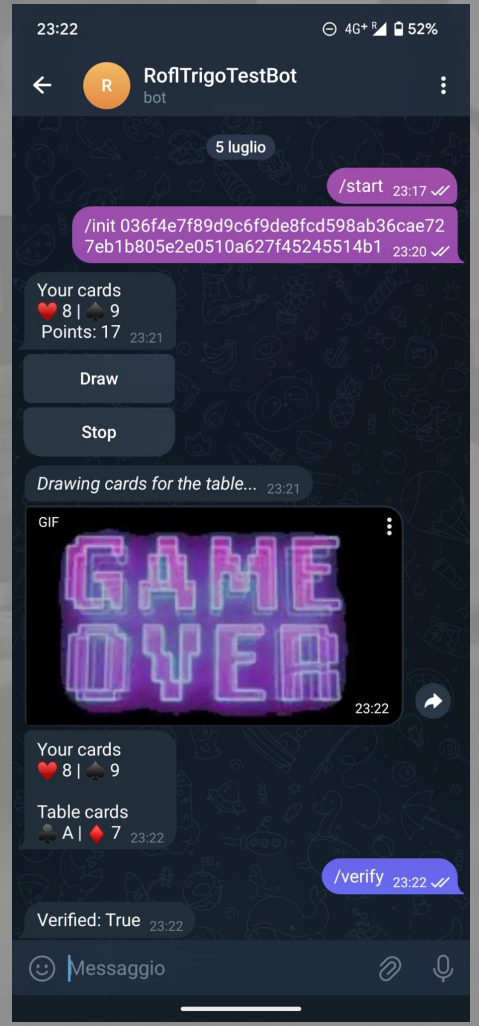


Start the game:

A player joins the game and sends a public key. The public key will be used to encrypt the cards he/she receives to ensure that no one else can know the card value.

The Smart Contract shuffles the deck and provides the commitment (hash of the deck)

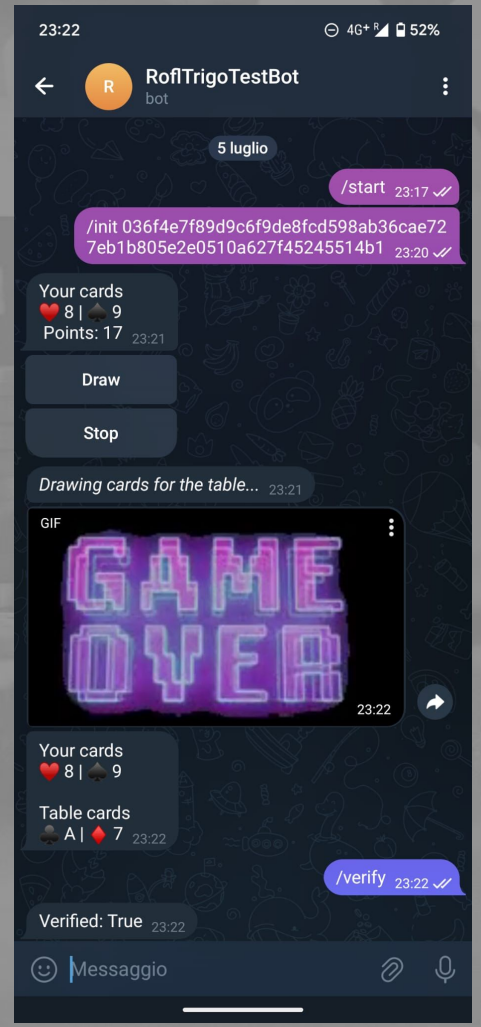
There are about $8*10^{80}$,
more than the atoms in the universe!



Game rounds:

The player can ask for new cards or decide to stop.

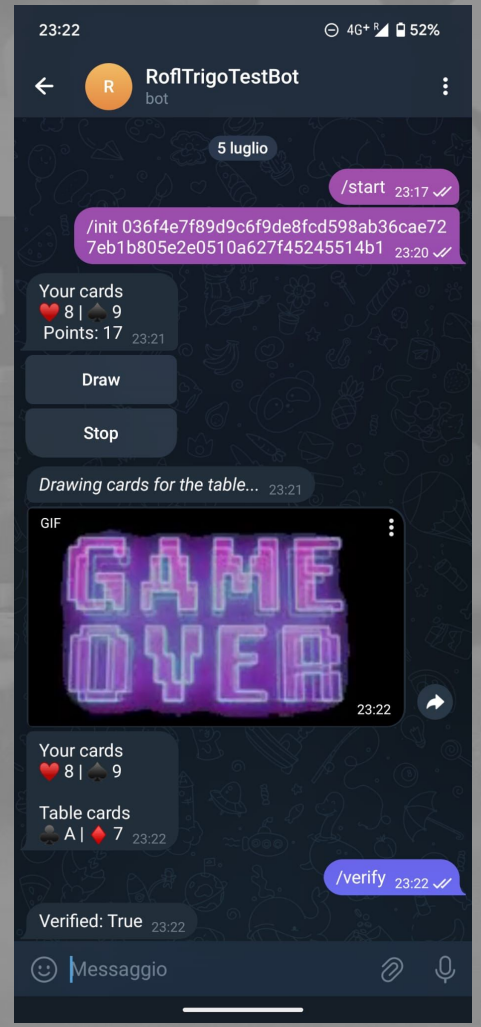
Then the House (ROFL) will pick cards from the deck to get a higher score without exceeding a score of 21



Verify the deck:

At the end of the game the player can **“/verify”** the game by comparing the whole deck used in the game with the initial commitment.

If they match the game was fair, the House could not cheat !



Thanks

... and play safe,
use TR.I.G.O