# Kaiji :  A Poker Game on Starknet using ZK-Proof

## 1 - Why Kaiji ?

Kaiji is an implementation of the popular Texas holdem poker on Starknet, employing STARK proof technology for a fully trustless and fair experience. By removing the dealer and centralization, Kaiji ensures peer-to-peer interactions that are transparent and beyond reproach.

Through STARK proofs, every move and outcome is validated on-chain, guaranteeing players an authentic and manipulation-free game.

Kaiji's innovation lies not just in its technology, but also in its reestablishment of trust. Players rely on mathematics and cryptography, not intermediaries, as they enjoy a revitalized poker experience compared to online centralized poker system. With Kaiji, poker enters a new era of integrity, where the virtual table is synonymous with security and innovation, reshaping the way we perceive and engage with the game.

## 2 - Implementation

The implementation is based on the Mental Poker Scheme of Barnet.

### A. Current implementation

During this HackerHouse hackathon, as Cairo beginner, we implemented the gaming logic in Rust but we are gonna translate it in Cairo soon. The game is set up in a heads-up way (1vs1), 6 players table coming soon with a tournament system !

Cairo part :

The contract set players using their address and ArgentX account, the deck is directly encrypted and verified through ZK proof (verifying their is 52 unique cards) and each players receive 2 cards. Players decrypt their own cards using their private keys.
Their is a betting/check phase, and public cards are revealed. Hands value are calculated and the winner is determined.

But the most important part is the future ! With more time to build our Poker game, we have been thinking about the best implementation possible for us !

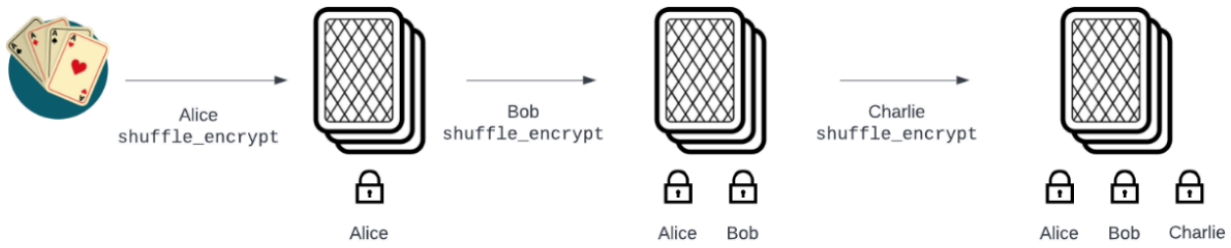
### B. Future implementation

Through this HackerHouse project, we realised how deep and wonderfull are the world of randomness in computer science.

For the moment, there is no real randomness function in Cairo, so we are very interested to explore new ways to build such a useful function. The function will be so useful that the whole Starknet gaming ecosystem will benefit from it !

The future implementation logic :

In this implementation, there is no dealer, every players encrypt and shuffle the deck using a fully randomness function, and pass it to the next players that repeat it. We require each player to join the shuffle so that no subset of players can control the sequence of shuffled cards or encryption. Effectively, each player contributes to the randomness of the ultimate deck, and unless there's collusion among all players, the shuffling remains equitable.




When a players receive his 2 cards, others players decrypt it, without being able to know its value because the card owner is the last person to decrypt it. This mechanism is described on following scheme. Alice receive her cards, ask Bob and Charlie to decrypt it, so they only see hash, and she finally decrypt to know the real value of her own cards. Throughout the dealing sequence, only Alice possesses the ability to observe the plaintext following her final decryption. Throughout this process, Bob, Charlie, and blockchain validators are unable to view her card.