DAC.digital

Gdańsk, 7.03.2023

VAIOT Limited
Mosta, MST 1180, Malta
Suite 1, Level 2,
Cornerstone Business Centre,
16th September Square

Code review report

1. Review Scope

a. Raffle.sol - used for conducting lotteries with native tokens. Its main functions include:
   - opening lotteries
   - adding participants to lotteries
   - selecting lottery winners
   - paying out the appropriate prizes to winners.

b. RaffleWinnerPicker - used for selecting lottery winners. Its main functions include:
   - opening lotteries
   - adding participants to lotteries
   - selecting lottery winners.

2. Observations/Finding

The Solidity code appears to be sound, and no critical issues have been identified in terms of security or performance. There are some missing checks that could prevent potential transaction failures, but the team of developers ensured that they have been handled on the backend, which is the primary user and consumer of the smart contracts.

Upon reviewing the lottery flow, it was determined that the solution is coherent and incorporates the necessary randomness element provided by Chainlink's VRF.

The main consumer of smart contracts is the backend, which imposes appropriate validations and ensures that the solution is safe and reliable. The backend was outside the scope of the review.

3. Recommendations

To avoid transaction failures when paying out funds to winners in the Raffle.sol contract, it is necessary to check whether the funds transferred by the lottery creator in the form of msg.value are equal to the total prize pool that is established for all winners. The team has ensured that this has been handled on the backend, but to increase reliability and ensure a bullet-proof solution, it is important to include such a check.

To avoid transaction failures and exceeding gas limits, limits could be added for arrays passed to certain methods in smart contracts, such as addLotteryParticipants. However, since the backend is the main and only user, this has already been addressed there. Nevertheless, implementing such limits would contribute to reducing potential issues in the future.

For the sake of clarity, easier testing, and future maintenance, the order of checks in "addLoteryParticipants" could be modified. It is suggested to first check if the lottery exists and then if it is open.

To facilitate deployment on various test networks and chains without the need to change the smart contract code, the VRFConsumerBaseV2 address could be passed in the constructor instead of being hardcoded.

4. Reviewers

Patryk Wojciechowski - is an experienced software developer specializing in frontend technologies and Ethereum blockchain solutions. With expertise in Web3, he has the ability to build decentralized applications that interact with smart contracts. Additionally, he has a strong background in backend development, allowing for a well-rounded skill set and the ability to build end-to-end solutions.