Provably Fair Assessment for Espresso

April 5th 2020 — Gorman Labs Verified

https://gormanlabs.com

This provably fair assessment was provided by Gorman Labs,
a Software Innovation Company.

Summary

This document is written as proof of verification of a “provably fair” winner selection process in Espresso.

Espresso’s Winner Selection Process

Espresso’s Winner Selection Process was built entirely custom in order to provide provably fair and randomized data in the most secure way to all underlying Espresso Pools. Espresso’s main system for attaching a winner to a pool is called the Oracle. Espresso’s Oracle relies on a publicly exposed API deployed on The Graph. It pulls data from The Graph automatically every 5 minutes to find Espresso Pools that have broadcasted their need for a winner to be selected. This means that the Espresso Pool has either met the targeted amount of entries quota and or has reached its expiration date. When the Espresso Pool with the above criteria is found the blockchain is then queried to determine the amount of participants in the pool. In turn it submits an API request to a well known and publicly available API in the control of Random.org to ask for a random number between 0 and the amount of pool participants. When Random.org replies to the API request with the random number, the Espresso Oracle immediately finalizes the Espresso Pool that originally required the winner. When the Espresso Pool receives this transaction it successfully becomes finalized and the winner, creator and farmers are all rewarded.

The Espresso Winner Selection Process acts as a secure intermediary between all Espresso Pools and Random.org.

Central Point Of Failure

The major central points of failure with any type of gaming pool are knowing the winning number and or knowing the identity of a particula ticket holder before the pool is over. In Espresso there is no identity attached to the “ticket” because the platform doesn’t issue numbers or tickets and does no identity tracking. In Espresso’s Platform the entrypoint is the address of the users Ethereum Wallet. For example other platforms have failed in the past by becoming a central point of failure and issuing numbers either chosen by a user or issuing random numbers that they know and can attach to identities. Decentralizing the Espresso platform removes any centrally generated numbers and also makes all entries anonymous. Additionally, the winner is not generated directly by Espresso and is not generated until all participants have been established and additional participants are no longer being accepted.

Contract Security

Every Espresso Gaming Pool Smart Contract is secured through the use of cryptography. Submission details of a gaming pool can only be received via the party with the corresponding private key that each Espresso Gaming Pool Smart Contract is hardcoded and governed to accept. In this case, the Espresso Oracle is the only part of the system that holds this private key. The Oracle system is deployed in a highly secure VPN (virtual private network) inside of AWS. This system is not exposed to the public and has zero public facing APIs. This means that you must be authenticated and connected directly to this private network in order to reach any part of the Oracle System and it is otherwise non-existent to the rest of the world. Additionally the Espresso Oracle uses AWS Secrets Manager to further secure the private key.

Results

Our audit concluded that the process that is described above is provably fair by our analysis of the systems involved. Using Random.org is a major consideration when it comes to the decision making of True Random number selection. The Random.org number generator is considered a TRNG (True Random Number Generator) by their own claims. Any modification of the systems in place post assessment would need to be reassessed for fairness. Additionally, AWS, VPN and Secrets Manager is a very secure set of technologies to run a platform such as Espresso.

> *“So much of life, it seems to me,*
>
> *is determined by pure randomness.”*
>
> Sidney Poitier

Random.org Supporting Criteria

- https://www.random.org/analysis/
- https://www.random.org/media/
- https://www.random.org/randomness/