Martin Galer

A Bootstrapping Mechanism for Sustainable Asynchronous Speculation Games of Chance

Jez
@izebel_eth

Blurr
Refund Contract Deployer

Abstract

We propose a mechanism for bootstrapping a generic onchain speculation game, without requiring an initial or incentivized LP pool (also known as a bankroll). This allows for the creation of new games with no upfront capital commitment, with a few other emergent properties such as: unconstrained bet sizing, negative house edge (+EV bets), eventual solvency, token emissions and more...

1 Premise

1.1 History of Onchain Games of Chance

Onchain speculation games of chance have existed in the cryptocurrency ecosystem since the beginning, offering a blend of transparency, decentralization, and innovation that traditional online gambling platforms could not match. These games leverage blockchain technology to provide provably fair experiences, immutable transaction records, and often decentralized operations, appealing to users seeking fairness and transparency.

SatoshiDice: Pioneering Bitcoin Gambling

Launched in April 2012 by Erik Voorhees, SatoshiDice was the first major onchain speculation game. Players sent Bitcoin to different addresses, each with a specific probability of winning and corresponding payout. The outcome was determined by a combination of the wager's transaction hash and a secret salt, ensuring fairness and transparency. SatoshiDice quickly became immensely popular, accounting for a significant portion of Bitcoin transactions in its early years.

Bustabit: Innovating Crash Games

Introduced in 2015, Bustabit pioneered crash gambling games. Players bet on a multiplier that increases until it crashes, with the option to cash out before the crash. This introduced a social dimension to onchain gambling, as players could see and react to each other's bets and decisions.

Etheroll & EtherCrash: Ethereum Iterations

With Ethereum's smart contract capabilities, the landscape of onchain speculation games expanded beyond Bitcoin. Etheroll, launched in 2017, offered a dice game where players could bet on virtual dice rolls, using smart contracts to allow players to set their own odds and payouts, while ensuring transparency. EtherCrash, launched in 2018, followed the crash game model, where players bet on how long a multiplier would increase before crashing.

1.2 Limitations of Existing Mechanisms

Despite the advancements and popularity of onchain games of chance, several limitations persist, impacting their efficiency and user experience:

- **Need for Initial Liquidity Providers (LP):** Most onchain games require an initial liquidity pool to function. This pool ensures that players can receive payouts promptly. However, establishing this pool can be challenging, as it requires significant initial capital.
- **Incentivizing Liquidity Providers:** To attract and retain liquidity providers, platforms often need to offer incentives such as a share of the profits or tokens. This requirement can complicate the platform's economic model and affect its sustainability.
- **Constraint on Bet Sizing:** The size of bets that players can place is often constrained by the size of the liquidity pool. If the pool is small, it limits the maximum possible bet, potentially discouraging high-stakes players and limiting the game's appeal.
- **Solvency Concerns:** Players must continually evaluate the solvency of the platform they interact with. Notably, EtherCrash had a bad actor drain the LP. Platforms like Rollbit, which offer the blockchain-based Rollercoaster game, continue to suffer from this concern.

2 Proposal

We introduce a novel mechanism that addresses the stated concerns, by utilizing a queue-based payout system to allow the protocol to sustain temporary overall insolvencies.

2.1 High Level Design Choices

The proposed mechanism allows for great flexibility with respect to game design, allowing game creators to specify:

- payout structure and odds
- house edge (+ or -)
- a solvency ratio invariant

without having to deal with:

- initializing or incentivizing a LP pool
- constraining bet size based on the LP pool
- designing token emissions

2.2 Payout Queue System

The core of the new mechanism is a novel payout queue. This system ensures that the protocol remains solvent while managing payouts efficiently and fairly.

After each gameplay iteration, a protocol implementing this mechanism evaluates its ability to pay out based on a predefined solvency ratio.

The queue logic is essentially:

1. a new wager is placed and wins
2. if a queue already exists:
   (a) add wager to the end of the queue
   (b) evaluate whether the front of the queue can be paid out, determined by the solvency ratio
   (c) if yes, pay out the front of the queue
3. if no existing queue:
   (a) evaluate whether the wager can be paid out, determined by the solvency ratio
   (b) if yes, pay out the wager
   (c) otherwise, create a queue of length one

2.3 Solvency Ratio Invariant

The Solvency Ratio Invariant (SRI) defines whether the protocol can pay out new wagers. The solvency ratio is defined as:

$$\text{Solvency Ratio} = \frac{\text{(ETH in the treasury)} + \text{(Eth in the queue)}}{\text{Liabilities of the queue}} \quad (1)$$

The eth in the treasury is the protocol's accumulated eth from losses, edge, etc...

The eth in the queue is the total unpaid won input wagers (minus any taxes).

The liabilities of the queue is the total unpaid winnings of the above input wagers.

At one extreme, an SRI of 1.0 would require the protocol to be fully solvent in order to pay out any wager. In practice, this means that anytime the protocol would be insolvent, it will queue all subsequent won wagers until enough losses/edge builds up to pay the entire queue out.

At the other end, an SRI of 0.0 would indiscriminately pay out the front of the queue with subsequent wagers.

One elegant way to construct an SRI is to define it as:

$$\begin{gathered}\text{(ETH in the treasury)} + \text{(ETH in the queue)} \\ > \\ \textstyle\sum_{i=1}^{n} \text{Wager}_i\text{, where n is the queue length}\end{gathered} \quad (2)$$

With this definition, the protocol can let the queued unpaid won wagers withdraw their input (forfeiting any winnings). This allows "stuck" participants to recoup some eth, while increasing the solvency of the remaining queue.

2.4 Yield-Bearing Wager Denominations

If the wager currency generates native yield, the queue system will naturally increase its solvency ratio over time.

2.5 Token Emissions

Token emissions enable games with a positive house edge to present as +EV for the player by immediately remunerating them with a liquid token. The basic emission framework features a linearly decreasing reward based on game iteration, encouraging early participation and initiating the flywheel effect.

A tax on wagers (similar to a house edge) can incentivize token ownership through a buy-and-burn mechanism, which will price in future cash flows. Additionally, token emissions can be linked to queue length to incentivize wagers when the protocol is temporarily insolvent and a queue exists.

3 Examples

In order to better demonstrate this mechanism, here are a few example simulations of different games of chance.

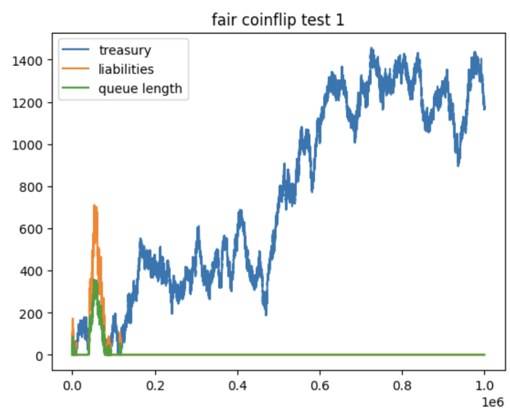
3.1 Fair Coin Flip

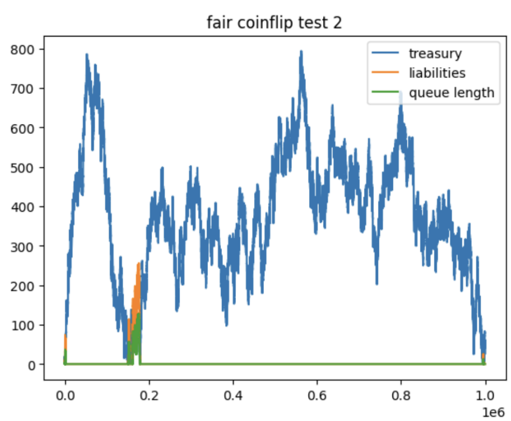
This protocol is defined as a perfectly fair coin flip, with no house edge or taxes included.

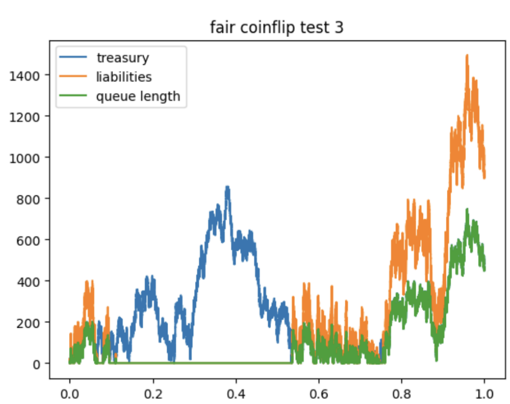
The payout structure is thus:

- 50% chance to win double the wager
- 50% chance of total loss

We then simulate one million iterations with input fee 1.







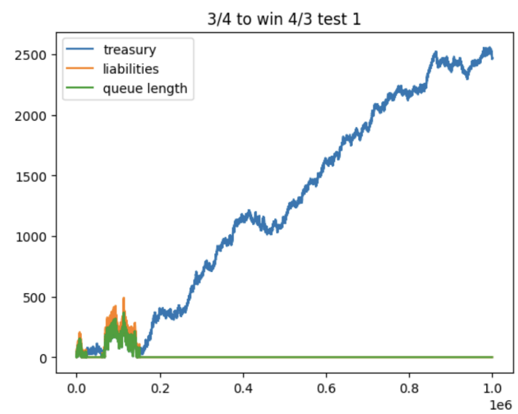
As demonstrated, the state of the perfectly fair coin flip game depends on the outcome variance - with no ability to accumulate treasury via edge, the treasury is vulnerable to bad runs at any point in its lifecycle. The queue mechanism allows the protocol to absorb this variance.

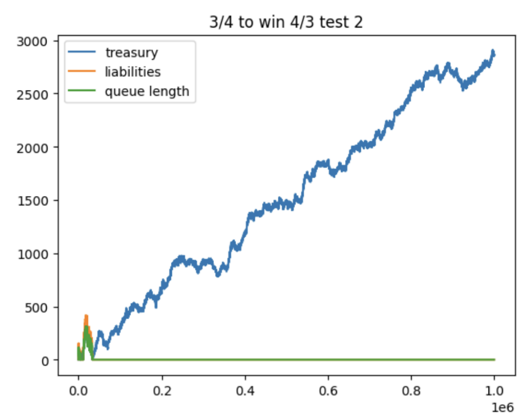
3.2 ”3/4 Chance to Win 4/3”

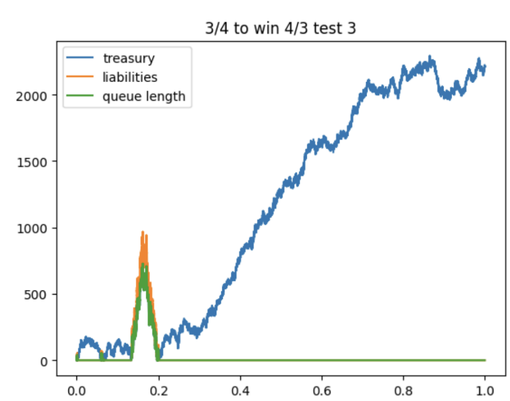
The payout structure for this game is:

- 3/4 chance to win wager * 1.33
- 1/4 chance of total loss

The house edge in this game is thus 0.25%. We then simulate one million iterations with input fee 1.







4 Async vs Synchronous Games

A strong motivation for proposing this mechanism is to remove the constraints from launching an asynchronous game.

It is the author's opinion that asynchronous games are far superior to synchronous games. Synchronous games, such as tournaments or peer-to-peer wagers require much higher levels of coordination, which often limits participation to those who can commit to being available at the same time as other players. Without enough player density, marginal participants may not be able to play on demand.

However, the LP requirements of asynchronous games often proves challenging to aspiring game designers, who may not be able to provide the bankroll, or have no desire to raise one. As a result, designers often default to parimutuel, synchronous game designs where players bring their own capital, thus alleviating the need for a large initial liquidity provision.

By introducing this mechanism and removing the LP requirement and bet size constraints, we hope to see the creation of more novel, asynchronous games.

References

[1] T. Chitra, K. Kulkarni, M. Pai, T. Diamandis, "An Analysis of Intent-Based Markets," *https://arxiv.org/pdf/2403.02525*, 2024.

[2] G. Angeris, T. Chitra, T. Diamandis, K. Kulkarni, "The Specter (and Spectra) of Miner Extractable Value," *https://arxiv.org/pdf/2310.07865*, 2023.

[3] T. Chitra, "Towards a Theory of Maximal Extractable Value II: Uncertainty," *https://arxiv.org/pdf/2309.14201*, 2023.

[4] G. Angeris, T. Chitra, T. Diamandis, A. Evans, K. Kulkarni, "The Geometry of Constant Function Market Makers," *https://arxiv.org/pdf/2308.08066*, 2023.

[5] T. Chitra, P. Erins, K. Kulkarni, "Attacks on Dynamic DeFi Interest Rate Curves," *https://arxiv.org/pdf/2307.13139*, 2023.

[6] T. Diamandis, M. Resnick, T. Chitra, G. Angeris, "An Efficient Algorithm for Optimal Routing Through Constant Function Market Makers," *https://arxiv.org/pdf/2302.04938*, 2023.

[7] T. Chitra, M. V. X. Ferreira, K. Kulkarni, "Credible, Optimal Auctions via Blockchains," *https://arxiv.org/pdf/2301.12532*, 2023.

[8] T. Diamandis, A. Evans, T. Chitra, G. Angeris, "Dynamic Pricing for Non-fungible Resources: Designing Multidimensional Blockchain Fee Markets," *https://arxiv.org/pdf/2208.07919*, 2022.

[9] K. Kulkarni, T. Diamandis, T. Chitra, "Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers," *https://arxiv.org/pdf/2207.11835*, 2022.

[10] G. Angeris, T. Chitra, A. Evans, S. Boyd, "Optimal Routing for Constant Function Market Makers," *https://arxiv.org/pdf/2204.05238*, 2022.

[11] A. Obadia, A. Salles, L. Sankar, T. Chitra, V. Chellani, P. Daian, "Unity is Strength: A Formalization of Cross-Domain Maximal Extractable Value," *https://arxiv.org/pdf/2112.01472*, 2021.

[12] G. Angeris, A. Evans, T. Chitra, "Replicating Monotonic Payoffs Without Oracles," *https://arxiv.org/pdf/2111.13740*, 2021.

[13] G. Angeris, A. Agrawal, A. Evans, T. Chitra, S. Boyd, "Constant Function Market Makers: Multi-Asset Trades via Convex Optimization," *https://arxiv.org/pdf/2107.12484*, 2021.

[14] A. Evans, G. Angeris, T. Chitra, "Optimal Fees for Geometric Mean Market Makers," *https://arxiv.org/pdf/2104.00446*, 2021.

[15] G. Angeris, A. Evans, T. Chitra, "Replicating Market Makers," *https://arxiv.org/pdf/2103.14769*, 2021.

[16] G. Angeris, A. Evans, T. Chitra, "A Note on Privacy in Constant Function Market Makers," *https://arxiv.org/pdf/2103.01193*, 2021.

[17] G. Angeris, A. Evans, T. Chitra, "When Does the Tail Wag the Dog? Curvature and Market Making," *https://arxiv.org/pdf/2012.08040*, 2020.

[18] T. Chitra, A. Evans, "Why Stake When You Can Borrow?," *https://arxiv.org/pdf/2006.11156*, 2020.

[19] G. Angeris, T. Chitra, "Improved Price Oracles: Constant Function Market Makers," *https://arxiv.org/pdf/2003.10001*, 2020.

[20] T. Chitra, "Competitive Equilibria Between Staking and On-Chain Lending," *https://arxiv.org/pdf/2001.00919*, 2020.

[21] G. Angeris, H.-T. Kao, R. Chiang, C. Noyes, T. Chitra, "An Analysis of Uniswap Markets," *https://arxiv.org/pdf/1911.03380*, 2019.

[22] T. Chitra, M. Quaintance, S. Haber, W. Martino, "Agent-Based Simulations of Blockchain Protocols Illustrated via Kadena's Chainweb," *https://arxiv.org/pdf/1904.12924*, 2019.