Safer.fun

Revolutionizing Memecoin Launches on Solana

Adam Boubabda, Walid Sofiane, Alper Ozyurt, Eren Gazi

October 2024

Abstract

Safer.fun is a groundbreaking platform designed to create a more fair and secure environment for memecoin creation on the Solana blockchain. By neutralizing to the greatest extent exploitative practices like sniping and rugging developers, we empower genuine users, fostering a vibrant and trustworthy memecoin ecosystem. Our innovative pre-launch auction system and post-launch token distribution rules ensure a fair playing field, enhancing user experience and strengthening Solana's reputation as the leading platform for memecoin marketplaces. **While our current focus is on PumpFun, we are characterized by being a pre-launch platform that is platform-agnostic, ensuring fairness across the chain. We can seamlessly pre-launch on token launch platforms like PumpFun, as well as decentralized exchanges like Raydium.**

Contents

Executive Summary

The memecoin market on Solana is booming, attracting a diverse array of users, including newcomers eager to participate in the crypto revolution. However, malicious actors like snipers and unethical developers are exploiting vulnerabilities, systematically extracting liquidity, and harming the user experience. **Safer.fun** addresses this critical problem by introducing a novel protocol that ensures fair token launches. Our solution not only empowers and protects genuine users but also enhances the overall health and attractiveness of the Solana ecosystem for newcomers.

1 Introduction

The Solana blockchain has emerged as a leader in user onboarding, particularly with the rise of memecoin mania attracting both seasoned traders and newcomers with a penchant for high-risk, high-reward investments. Platforms like **Pump.fun** have revolutionized coin creation, achieving unprecedented user community (PumpFun Daily Users on Dune Analytics) and revenue growth—over $100 million in just 217 days—with a simple 0.02 SOL for token creation and 1% fee on every trade. (Ryan Watkins Twitter Status, Kkashi Twitter Status,Dune Analytics - PumpFun by Adam)

Despite this success, the rapid growth has exposed significant vulnerabilities. Malicious actors exploit the system, undermining trust and deterring genuine users. Our goal with **Safer.fun** is to introduce randomness in order to create a pre-layer platform which aims to safeguard the memecoin ecosystem by providing more fair and ethical token launches.

As mentionned before, while it currently relies on Pump.fun because of the hype and the flow of daily users, it can easily be broaden and adapted any to other memecoin platforms (e.g. Moonshot).

2 The Problem

Malicious Actors Undermining the Ecosystem

- **Snipers**: Automated bots that instantly buy newly created coins, anticipating natural buyers to enter the market. They then dump their holdings for minimal profit once they recouped their fees, repeatedly exploiting this tactic to siphon funds from genuine users.
- **Rugging Developers**: Developers who exploit their position as the first buyer of the coin. They engage in two main types of rug-pull strategies:
  - **Short/Medium-Term Rug**: These developers act similarly to snipers, quickly selling off their holdings to secure a small profit as soon as

possible—often right after recouping their fees. They spam coin creations and capitalize on being the first buyer to repeatedly extract value from natural users.

- **Long-Term Rug**: Developers who hold onto their tokens for a more extended period, possibly building trust within the community before eventually dumping their holdings. This type of rug can occur after a significant amount of time and community investment.

These practices are not mere trading strategies; they are systematic exploits that drain liquidity and erode trust. For example, the top sniper has already extracted over $4 million from the Solana memecoin market (Source), showcasing the scale of the problem.

These systematic exploits are facilitated by the inherent safety advantages these actors possess:

- **Developers** are safe because they are the first buyers; no one can dump on them. Their maximum loss is limited to their creation and trading fees.
- **Snipers** are relatively safe because they are always second buyer (after the dev). They enter with amounts low enough not to incentivize the developer to sell on them but sufficient to gain a small profit when a natural buyer enters. Their maximum loss is minimal, usually just their trading fees.

These practices ruin the experience for both natural buyers and genuine developers who want to push a project forward.

Note: These two malicious actors often escalate their schemes by creating fake trading volume to lure in their targets. Once enough genuine users believe real trading is happening, the fake volume is dumped all at once, causing losses for the genuine users. Our solution, designed to target snipers and rug-pulling developers, will also indirectly address this type of malicious behavior.

3 Our Solution

Introducing Safer.fun: A Fair Launch Protocol

3.1 Our Philosophy

First and foremost, our goal is not to impose strict control or go against the core principles of crypto and DeFi. While we aim to make it fair for genuine participants and create a smoother experience, there's a fine balance to strike, as some protections may require a bit more control. However, our features and conditions on memecoin creation are designed and optimized not to impede real players but to discourage and even make it impossible for malicious actors to

exploit the system.

Our protocol effectively neutralizes **snipers** through of pre-launch auction and heavily impedes **short/medium-term rugging developers** through our post-launch token distribution constraints.

However, long-term rugging poses a different challenge. Since these developers hold onto their tokens for an extended period before selling off, they operate within the normal dynamics of market participation. At some point, to maintain a decentralized and free market, we must relinquish control over token amounts and allow participants to trade freely. Imposing indefinite constraints would contradict the core principles of decentralization and could impede genuine market growth.

Therefore we acknowledge that long-term rugging cannot be entirely prevented without overstepping ethical boundaries and infringing on the freedoms inherent in the crypto ecosystem.

Disclaimer: While the aforementioned exploits will be heavily reduced, trading remains risky. When someone earns money, someone else loses money. Trade memecoins at your own risk.

3.2 Our Approach

Our solution is a two-step approach designed to eliminate malicious actors while promoting fair participation:

3.2.1 Pre-Launch Auction System

Neutralize sniping, by allowing it to everyone! We democratize early access by introducing a pre-launch auction. This mirrors how snipers naturally compete by submitting tips to validators to gain priority in transactions. The auction goes as follows:

- **Developer** submits his token creation inputs, including his buy amount in SOL, and sets the duration for an auction window during which pre-buyers can bid to secure a rank among early buyers. The developer is always the first buyer.
- **Pre-Buyers** participate in an open auction to bid for early buying positions.
- **Auction Mechanics**:
  - Bidders send their purchase amount in SOL and an auction fee, both amount are used to compute their rank among early buyers.

- While choosing these inputs, bidders see their prospective rank among current pre-buyers before confirming.

- Real-time ranking allows bidders to increase their fees or size amount. Participants are encouraged to regularly check the auction to decide if they want to increase their bid to secure a rank or re-secure a rank they may have lost. Withdrawal is also permitted at any time, but with a minimal protocol fee to prevent spamming.

- The auction fee becomes more expensive as time passes.

- The auction lasts for a predefined time, after which an exit-only window allows participants to reassess their positions. During this period, it is each participant's responsibility to revisit the coin to confirm they are comfortable with all the people who will be buying before them.

- The remaining time of the windows is always displayed to the users.

- the exact formula of the score of each pre-buyer putting a bid is the following : In the bidding process, pre-buyers are ranked based on their contribution of SOL, their bid amount, and a time-weighting factor. The rank or score of each pre-buyer is computed using the following formula:

$$\text{Rank}_i = \left(\frac{b_i(t)}{q_i}\right) \times \left(1 + \beta \times \frac{T - t}{T}\right)$$

  where: $b_i(t)$ is the current bid of pre-buyer i at time t, q_i is the total SOL amount available for bidding by pre-buyer i, T is the total time allocated for bidding (e.g., 900 seconds or 15 minutes), t is the current time in the bidding process, β is a time-weighting parameter, typically set to 0.1, which gives more weight to bids placed earlier in the process.

- **Note:** Dev can't cancel a coin creation, but can withdraw from it too, this is meant to not create abuse by creating a fake hype around a token and then cancel it.

Through our pre-launch auction we create a natural equilibrium by giving everyone equal opportunity to secure early buying positions, thus neutralizing snipers by allowing it to everyone. Now it remains to address the potential for immediate post-launch dumping of the dev and pre-buyers, by imposing specific constraints.

3.2.2 Post-Launch Token Distribution Constraints

To prevent immediate dumping of both the dev and pre-buyers, which ultimately promotes a smooth organic growth:

- **Token Distribution in Batches**: Each pre-buyer receives their tokens in batches. Each batch contains a random percentage of the buyer's total token allocation.
- **Unlock Conditions**: Each batch unlocks when both a random time and a random market capitalization threshold are met.
  - **Random Market Cap**: Ensures that unlocks are tied to the token's performance, encouraging positive community engagement.
  - **Random Time**: Introduces unpredictability, which prevents market manipulations aimed solely at triggering token unlocks.
- **Rank-Based Distribution**:
  - Depending on a pre-buyer's rank in the presale, their unlock conditions for market cap, time, and batch size will vary. Later buyers will on average see earlier distributions than earlier ones, balancing the ability for community members to act before those who paid more fees to secure earlier positions.

By staggering token unlocks, we prevent scenarios where the first natural buyer becomes a target for dumping, thereby avoiding merely transposing the sniping problem. As a pre-buyer, you're part of the community and shouldn't intend to crash the coin quickly. The incremental ability to sell as the coin matures and gains engagement aligns with this philosophy.

Incentivizing positive behavior is achieved by motivating early participants to support the token's growth in order to unlock their holdings, while randomness in the system prevents manipulation by bad actors attempting to artificially trigger unlock conditions and compute exact exploitative strategies.

Actually, to prevent manipulation, although random market cap and batch sizes could be exploited through flash buys and sells, the inclusion of a random time condition makes such exploitation unfeasible due to the associated trading fees that would result from spamming a flash buy and sell.

Our solution ensures a fair start for all participants, while preserving the core principles of decentralization. By promoting a smooth and equitable launch, we boost the token's appeal, drive higher trading volumes, and increase its potential to 'moon'.

Notes:

- In order to generate random times and market cap values on the blockchain without revealing them in advance, we employ a continuous rolling mechanism based on verifiable random functions and clockwork program of Solana. In every couple of seconds, we simultaneously roll two random variables—one for time and one for market cap. If both exceed their respective thresholds, the random event is triggered. The event then determines a random percentage of the total pre-buyer's tokens to distribute. The thresholds are different at all times to approximate the desired distributions, ensuring unpredictability while adhering to the intended behavior, a method that can be mathematically proven to approximate any distribution .
- The random market cap thresholds dynamically decay over time to ensure that tokens are eventually delivered to both pre-buyers and developers, preventing indefinite delays.

3.2.3 Post-Launch Community Benefit

While our pre-launch auction system democratizes early access and neutralizes snipers, we acknowledge that contributing to auctions might lead to higher upfront costs for participants compared to the potential losses incurred from a sniper scalping the natural buyer. Essentially, as we have opened up early access to everyone, the competition for favorable ranks may drive up the auction fees significantly.

To mitigate this concern and provide tangible benefits to the community, we have implemented a mechanism where a consequent percentage (to define) of the auction fees is reinvested back into the token. Specifically:

Community Benefit: A portion of the collected auction fees is used to purchase the token in the open market through a short/medium-term Dollar-Cost Averaging (DCA) strategy. The purchased tokens are then immediately burned. This approach serves multiple purposes:

- **Price Support**: By buying tokens during the launch phase, we create upward pressure on the token's price, contributing to a more stable and robust market.
- **Supply Reduction**: By burning the purchased tokens, we demonstrate that we won't use them to generate profit in the future. Additionally, this action slightly reduces the total supply, which can potentially increase the token's value over time.
- **Smoother Launch**: The combination of price support and supply reduction helps in smoothing out price volatility during the critical launch period.

- **Community Incentive**: Participants see a direct benefit from their auction contributions, as their fees actively enhance the token's market position and potential growth.

This reinvestment strategy not only offsets some of the costs associated with participating in the auction but also aligns the interests of all participants toward the token's success. By channeling a portion of the auction fees back into the token, we foster a positive feedback loop that benefits the entire community.

4 Market Opportunity

- **Growing Memecoin Market on Solana (and on the other chains too)**

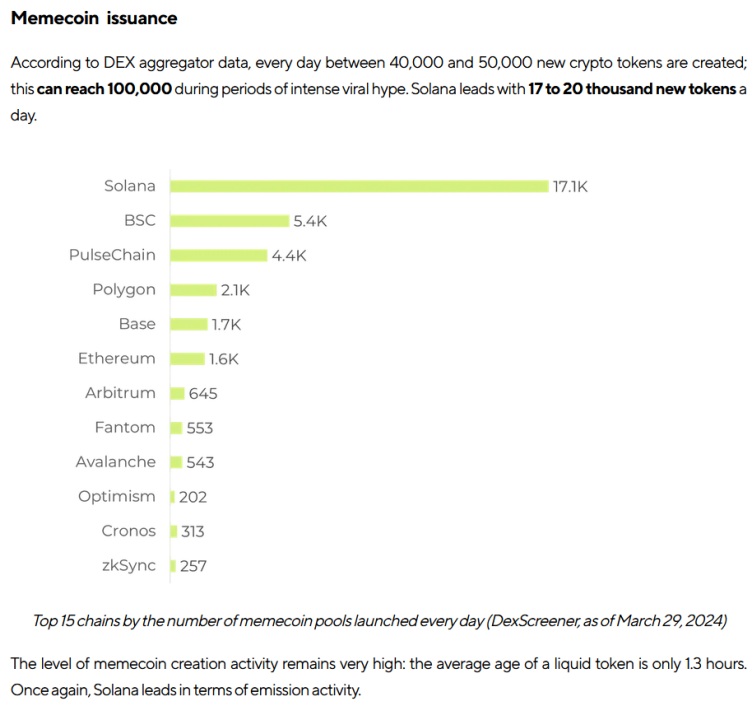

Figure 1: Source: https://bdc.consulting/insights/MarketResearch/memecoins

- **User Base Expansion**: With platforms like Pump.fun experiencing explosive growth, there's a clear demand for fairer memecoin launches.
- **Need for Fairness**: The prevalence of malicious actors presents a gap in the market for a secure, user-friendly platform.

- **Revenue Potential**: Pump.fun's model has generated over $100 million, indicating more than significant revenue opportunities with an adapted business model.

5 Business Model

Sustainable Revenue Streams

- **Auction Fees**:
  - A percentage of the auction fees is retained as revenue, while the rest is used, as mentioned earlier, to DCA back into the coin to support its launch.
- **Staking Pre-Buy Funds**:
  - While the presale window is open, participants' deposited SOL is liquid staked through JitoSol.
  - We maintain a wallet where all pre-buy funds of all tokens are staked, earning yield over time.
  - Upon coin launch, we unstake the necessary amounts to execute the corresponding buys.
- **Withdrawal Fee**:
  - A minimal fee is applied when withdrawing from a coin pre-sale, serving as a safeguard to prevent our protocol wallet from being siphoned.

Complete Platform Adaptability

- **Partnerships**:
  - The goal is to integrate with memecoin platforms like Pumpfun. However, the versatility of our platform allows for easy collaboration with other memecoin platforms, such as Moonshot.

6 Go-to-Market Strategy

Strategic Steps to Capture the Market

- **Leverage Existing Platforms**: Integrate with popular platforms like Pump.fun and Moonshot to tap into their user bases.
- **Education**: Engage with the crypto community through social media to build trust and awareness. Provide resources and explanations to help users understand the benefits of our platform and the risks of trading traditional memecoin launches.

7 Competitive Analysis

Standing Out in the Market

- **Competitors**:
  - **None**: No platform is trying to act against those malicious actors at the moment. No actions were taken to stop them, apart from incentivizing people not to dump bc Meteora x Moonshot proposes lifetimes fees for devs top holders before bonding. But our platform can definitely integrate with that too as a bonus (that would come with parnering with moonshot! A leading platform but lacks mechanisms to prevent malicious activities.
- **Our Advantage**:
  - **Security Focus**: Unique protocol designed to neutralize snipers and impede unethical developers.
  - **Fairness**: A focus on fairness and equality of opportunity for all early buyers.
  - **Adaptability**: Ability to integrate with and improve upon all existing memecoins platforms.

8 Team Expertise

Adam Bouabda
-ETH Zurich Math Msc student and Research Assistant.
-Uniswap Foundation Research Fellow.
-Sui Foundation Research Award Winner.

Alper
-EPFL Cs Bsc student
-IronNode and AFEL head blockchain developer/engineer
-4x blokchain hackathon winner

Walid
-EPFL Master in financial engineering / Bsc in mathematics / Research assistant
-2x SUI academic research awards recipient
-2x hackathon winner (in DeFi and TradFi)
-Currently a data science and ML intern at Cadena Platforms

Eren
-Bilkent University CS Bsc student
-AFEL software developer/engineer

9 Vision and Mission

Our Commitment

- **Vision**: To be the leading platform that fosters a fair, secure, and vibrant memecoin ecosystem on Solana. To empower users by eliminating exploitative practices, enhancing trust, and promoting sustainable growth in the memecoin market.

10 Conclusion

Safer.fun is a movement towards fairness and security in the rapidly evolving world of memecoins. By addressing the critical vulnerabilities in current systems, we offer a solution that benefits genuine users, developers, and the broader Solana ecosystem.

A Note on Risk:
Remember, trading very early memecoins is risky. While we strive to make the process as fair as possible, we do not guarantee that participants will not lose money. Our aim is to prevent individuals from systematically extracting liquidity from genuine players, thereby protecting new users and enhancing their experience.

11 Considerations

Intellectual Property Concerns
Memecoins are primarily driven by image and community. The success of a coin depends on the community that builds around it, provided that early participants don't undermine each other. There is a risk that a coin idea could be stolen during the auction phase and launched independently on platforms like Pump.fun. For that, we allow devs to choose auction windows down to 1 min to mitigate that issue. However, for even optimal effectiveness, platforms like Pump.fun should fully integrate our protocol to prevent these workarounds.

12 Contact Information / emails of the team members

Emails: erengazi.mutlu@ug.bilkent.edu.tr, walid.sofiane@epfl.ch, alper.ozyurt@epfl.ch, abouabda@ethz.ch
Website: https://safer.fun

13 Additionnal useful References

Here are other informative references about pump.fun and its success over the last months :

- Pump.fun Twitter Announcement: https://twitter.com/pumpdotfun/status/1823190311876575338
- Revenue Growth Analysis: https://twitter.com/RyanWatkins_/status/1830630230568124675
- Pump.fun Analytics: https://dune.com/adam_tehc/pumpfun
- Pump.fun vs. Moonshot Comparison: https://dune.com/hashed_em/pumpdotfun-vs-moonshot
- Sniper Wallet Analysis: https://dune.com/adam_tehc/pump-fun-alpha-wallets

14 Appendix

In the following appendix we expand on some of our thoughts that have led us to the idea as it is as well as a detailed explanation of the simulation attempts. For a detailed explanation of our protocol mechanics and the reasoning behind our approach, please refer to our whitepaper available on our website. Many other methods either transpose the problem—creating new bad actors—or contradict the core ethics and philosophy of crypto and DeFi.

14.1 Why Is This a Problem? Isn't It Just Trading?

At first glance, one might think these practices are simply part of trading, accepting the risks involved as in a casino. However, in a casino, no player other than the house (here, platforms like Pump.fun) has a positive expected return. In the current memecoin ecosystem, certain participants—snipers and some developers—have systematic advantages that give them a positive expectation at the expense of regular users.

Systematic Exploits Arise from Safety Nets:

- **Developers' Safety:**
  - Developers are safe because they are the first buyers; no one can dump on them.
  - Their maximum loss is limited to their creation and trading fees.
- **Snipers' Relative Safety:**
  - Snipers buy with a low enough amount not to incentivize the developer to sell on them but enough to gain a small profit when a normal buyer enters with a larger amount.
  - They plan to sell immediately after the natural buyer's purchase.
  - If the developer doesn't sell on them, their maximum loss is just their trading fees (less than the developer's fees).
  - In rare cases where the developer does sell on them, the sniper's maximum loss is slightly higher.

The Need to Eliminate Snipers:
Snipers should be fully eliminated. They are bots that extract money from every coin, ruining the experience for natural buyers and genuine developers who want to promote a project. To eliminate them, we need to make it unprofitable for them to continue this behavior.
Balancing Developer Advantages Ethically:
Developers are akin to the house in their own created coin; it's tolerable for them to have a higher profit expectation, although they should still face certain conditions. Since they are the first buyers, no one can dump on them. Limiting a developer's profit isn't feasible without:

- **Locking Their Funds:**
  - Too constraining and merely shifts the advantage to the first sniper.
- **Increasing Fees:**
  - **Trading Fees:** Not under our control and ethically questionable.
  - **Creation Fees:** Would discourage participation, especially from those with smaller portfolios, contradicting the inclusive philosophy.

We respect that developers have the right to be the first buyers.

Finding the Fine Line:

Addressing this problem requires a delicate balance—erasing systematic, unfair profits as much as possible while remaining ethical, keeping our philosophy intact, and not merely transferring the problem elsewhere.
At the very least, natural market equilibrium should prevent any pre-buyer from making a guaranteed profit by dumping on those who come after them. However, in reality, some profit opportunities might still exist because participants may not fully calculate the potential gains that pre-buyers ahead or behind them could achieve. The withdrawal window can help mitigate this by allowing participants to adjust their positions if someone attempts to snipe a higher rank.
But what about the first natural buyer after the token launch? Isn't there a risk that all pre-buyers will try to dump their tokens on this buyer, causing natural buyers to be hesitant or fearful?
To address this concern, we impose specific constraints on pre-buyers. It's crucial that these constraints are ethical and do not impede genuine participants. We believe this approach aligns with our philosophy: pre-buyers are community members who should not have malicious intentions like immediately dumping on new natural buyers. Instead, they should strive for the coin's overall performance and longevity.

14.2 Token Unlock Timing to Ensure Fairness and Deter Sniping

We implement a mechanism where later pre-buyers may receive earlier token distributions compared to those who secured earlier ranks. This approach serves multiple purposes:

1. **Balancing Advantages Among Pre-Buyers**:
   - Later pre-buyers, who may have paid lower auction fees and secured later ranks, are given the opportunity to have their tokens unlock earlier than those who paid higher fees for earlier ranks.
   - This allows community members who joined later to potentially act before those who paid more to secure early positions.

- It prevents individuals who might have secured early positions through high fees (possibly attempting to snipe) from having an undue advantage in selling their tokens first and profiting at the expense of others.

2. **Deterring Post-Launch Snipers**:
   - Once the pool is launched on Pump.fun, new buyers from Pump.fun will enter the market.
   - If all pre-buyers have their tokens locked for, say, the first 10 seconds, the first Pump.fun buyer could exploit this window to buy and sell (scalp) without competition, effectively acting as a sniper.
   - By having some pre-buyers' tokens unlock earlier—especially those of later pre-buyers—Pump.fun snipers are deterred because they risk being dumped on by these pre-buyers.
   - This risk discourages pumpfun snipers from attempting to exploit the initial trading period, promoting a fairer market environment. Also, it is important that while it may seem that at the end we are transposing the problem from the sniper to the pre-buyer getting his liquidity first, it is not the case since the person which is the most likely to get the liquidity first will be among the last pre-buyers, meaning he will already feel slippage in his token allocation (due to prebuyers before him) which makes the profit less and non systematic for this prebuyer that will get his liquidity first.
   - **Hence the rules of the game are : create a fair playground and no problem transposal and using common rugs on the platform will yield on avergae a negative return.**

Community-Centric Selling Approach:
As a pre-buyer, you're a community member and shouldn't have the intention to crash the coin quickly. Therefore, our token distribution system provides an incremental ability to sell as the coin gains traction and engagement over time. This aligns with our philosophy that participants should support the coin's growth rather than seek immediate profits at the expense of others.
Balancing Developer Token Unlocks:
Allowing such pre-buy mechanisms effectively mitigates the sniper issue. Meanwhile, the developer, being the first buyer, will, on average, have higher prerequisites for getting their tokens unlocked. Their token distribution is skewed towards longer unlock times compared to lower-ranked pre-buyers. This ensures that the developer cannot immediately sell off their holdings, promoting stability and trust in the early stages of the coin's life.

14.3 Balancing Constraints to Prevent Exploitation

The dynamics of coin launches resemble a domino effect—imposing excessive restrictions on a strong participant can inadvertently enhance the advantages of those who come after them. Our approach aims to strike a delicate balance:

- **Neutralizing Sniping through Global Accessibility**:
  - By making early access available to everyone via auctions, we democratize the process and diminish the advantage of traditional snipers.
- **Case-by-Case Restrictions**:
  - We impose specific constraints on the developer and each pre-buyer individually, ensuring fairness without overly hindering genuine participants.
- **Deterring Post-Launch Snipers**:
  - By introducing randomness heavily skewed towards earlier unlocks for later pre-buyers, we make potential Pump.fun snipers wary, as they become possible targets for these pre-buyers.

It's a cyclical process—we continuously fine-tune the auction mechanics and the parameters of the randomness in token distribution to maintain equilibrium. Our goal is to find the fine line that prevents exploitation without merely transposing the problem elsewhere (which could create new bad actors capable of systematic exploitation, attracting existing malicious participants). We also ensure that our solutions align with the core ethics and philosophy of the crypto and DeFi ecosystem, avoiding approaches that are overly restrictive or contrary to these principles.

A simulation attempt: how do bad actors affect the coin in safer.fun and directly in a pump.fun like pool.

A way to visualise classical rug pulls from devs and snipers in a pump.fun pool is through simulating the price trajectory of 1000 memecoins created by first a malicious dev that dumps on early buyers and then from a honest dev but that had to deal with a sniper sniping the pool early and selling after 10 seconds. We also implemented a panic-stress behaviour from buyers and sellers reflected by more number of sellers than buyers after the fump from either the dev or the sniper, we go now in details through each case :

Scenario 1: Developer Rug-Pull Simulation:

In the second code, we simulate a more aggressive strategy by a developer-sniper who enters the pool, buys tokens, and then dumps them after driving up the price.
Initialization:

The pool is initialized similarly with **10 SOL** and **1 billion tokens**. Buyers interact every **10 seconds**, purchasing between **0.15 and 1 SOL** worth of tokens, increasing the token price.

Developer-Sniper Buy:

The developer-sniper buys **3 to 4 SOL** worth of tokens early on and holds them while regular buyers continue interacting with the pool.

Rug-Pull (Sell-Off):

After **60 seconds**, the developer-sniper sells all of their tokens, causing a dramatic crash in the token price. The developer sells a large quantity, causing the price to drop drastically, leading to panic.

Aftermath:

After the developer's sell-off, buyers and sellers continue interacting with the pool in smaller quantities, with buyers buying **0.05 to 0.2 SOL** worth of tokens and sellers selling **0.02 to 0.1** times their remaining token amounts. This zigzag behavior simulates market instability after a major sell-off.

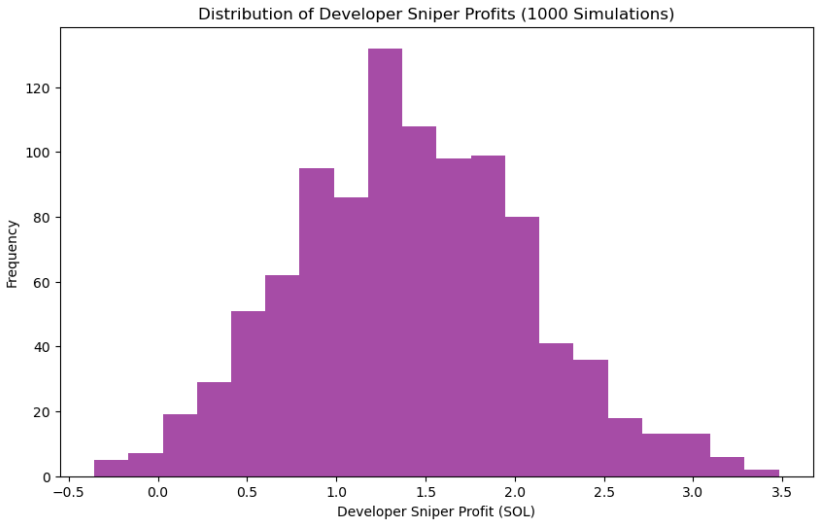

Figure 2: This graph displays the systematic profit distributions of the bad dev that dumps after 60 seconds, showing large profits. Note that the most dangerous aspect of this simulation is that the dev receives their liquidity first on classical platforms (with no randomness included), making dumping on early buyers almost systematically risk-free and highly profitable.

Scenario 2: Sniper Attack Simulation:

In the first code, a sniper is introduced into the pool, alongside regular buyers

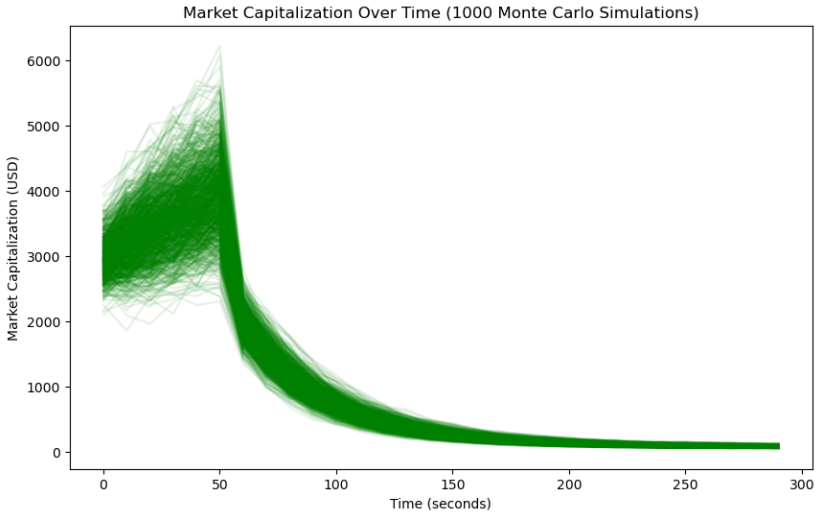

Figure 3: This graph displays the token trajectory of the 1000 simulated coins, the pattern is clear and general, there is a huge price drop and the volume (and the coin in general) is dead.

and sellers. Here's a step-by-step breakdown:

Initialization:

The pool starts with **10 SOL** and **1 billion tokens**. Buyers interact with the pool every **10 seconds**, buying small amounts of tokens (between **0.15 and 1 SOL**) in the early phase to gradually push the price up.

Developer Buy:

The developer buys **3 to 4 SOL** worth of tokens, setting the stage for future market interaction. The sniper enters the pool soon after, purchasing **0.5 to 0.7 SOL** worth of tokens.

Sniper Sell:

After **20 seconds**, the sniper sells all of their tokens, resulting in a significant profit. The sniper's profit is the difference between the **SOL** they receive from selling the tokens and the amount they spent on the purchase.

Panic Phase:

Following the sniper's dump, smaller buyers and sellers begin interacting with

the pool, simulating random market fluctuations. Buyers buy **0.05 to 0.2 SOL**, while sellers start selling **0.02 to 0.1** times their remaining tokens, causing the price to zigzag.

Results:

The simulation tracks the token price, remaining token supply, and market capitalization over time for each Monte Carlo run. It also calculates the sniper's profit, showing the potential outcomes from multiple simulations. The insights about the results can be read in the caption of the pictures.

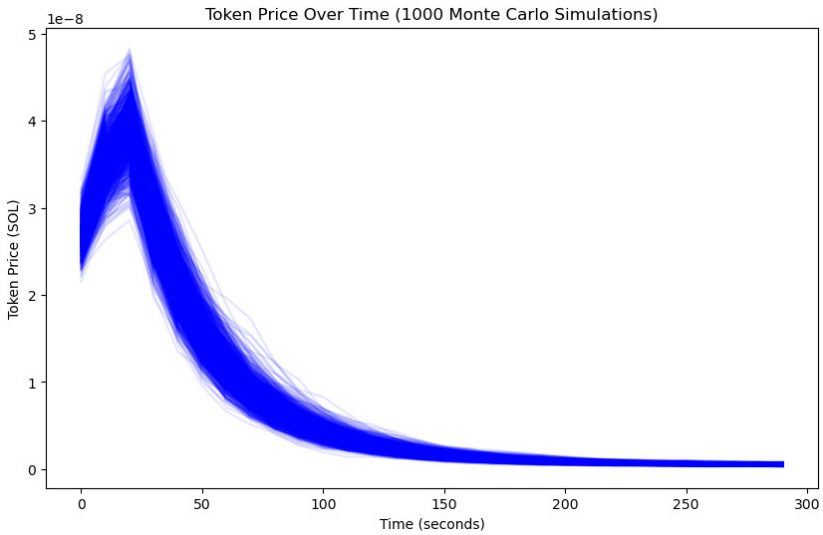

Figure 4: This graphs of the token trajectories form a sniper rugg pull also displays the clear patern of high volume then abrupt sell and dead coin, the rugg pull happens before the one displayed of the dev as it appears in the second number 10 instead of 60. This is a common traits of snipers that enter the pool as early as possible and sell as fast as possible.

We now move to the simulation of safer.fun platform and explain how the monte carlo simulation attempt is run.

The Monte Carlo simulations presented here demonstrate the impact of developer behavior and randomized unlocking mechanisms on the token's price and market capitalization over time. The simulations consider two types of developer behavior—an aggressive developer and a normal developer—and their influence on token liquidity during the pre-buying and selling phases. The total simulation time of a token is 35 minutes where 15 minutes is for prebuyers to compete for the places to recieve their tokens at a better price and then a 20

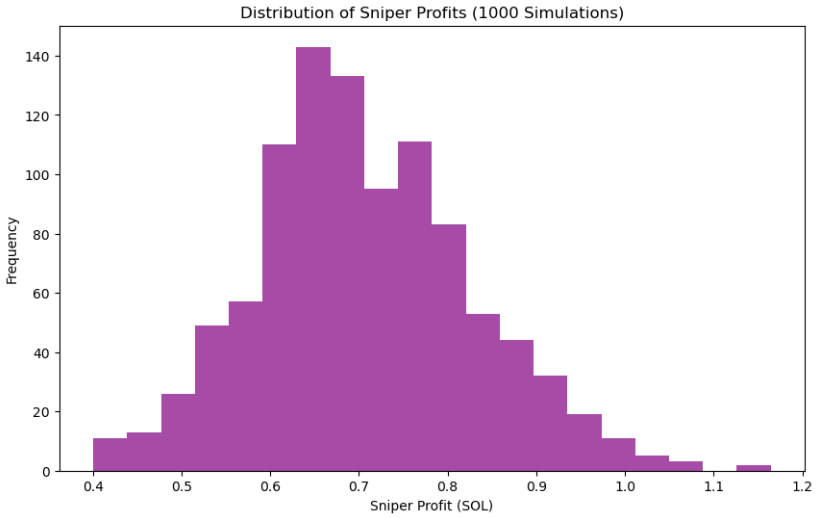

Figure 5: The same way as a dev, the sniper that optimizes his algorithm to always secure one of the early spots will also have a systematic and almost risk free win, however, the dev is always superior and the amount that snipers put are generally smaller, hence profits will be lower as diplayed in the distribution of the profits in the graph compared to the one of the dev.

minutes simulation of the token dymnamics in the real pool.

Pre-buying and Bidding Process:

In both simulations, the developer initiates the process by creating a token pool with a specific amount of SOL and setting parameters such as the buyback amount and order lifetime. Once the pool is created, pre-buyers are randomly generated. Some pre-buyers employ strategies such as bidding once, bidding every two minutes, or waiting until the end of the bidding period, while one pre-buyer uses an aggressive strategy to always bid the highest.

During the pre-buying phase, each pre-buyer places their bids over a 15-minute period (900 seconds). The bids are placed according to the strategies chosen by each pre-buyer. The protocol ranks pre-buyers based on the amount of SOL bid and the timing of the bids, applying a time-weighted formula to calculate the final ranking. After the bidding period concludes, token allocations are calculated for the developer and pre-buyers based on the bonding curve that governs the token pricing.

Unlocking Mechanism:

The unlocking mechanism for both the developer and pre-buyers ensures that tokens are released gradually over time during the withdrawal period (20 minutes). The unlocking process is driven by randomized time and Mcap thresholds. Liquidity is unlocked when both the current Mcap of the token pool meets or exceeds a predefined threshold, and the current time surpasses a time threshold. The randomized unlocking process involves both time and Mcap thresholds:

- **Time Thresholds**: The unlocking process is divided into four stages, where each stage is governed by a time threshold. These thresholds are randomly generated within certain intervals (e.g., between 1 and 300 seconds, 301 and 600 seconds, etc.).

- **Mcap Threshold**: For tokens to be unlocked, the market capitalization (Mcap) of the pool must exceed a threshold, which is generated randomly within a $\pm 10\%$ range of the current Mcap. If the Mcap condition is met at a given time threshold, a portion of the tokens (between 5% and 25% of the total liquidity) is unlocked for either the developer or the pre-buyers.

This unlocking mechanism adds an element of randomness, making it more difficult to predict exactly when tokens will become available for sale. The developer and pre-buyers must wait until both conditions are satisfied before they can sell their tokens, which helps avoid immediate and large-scale sell-offs that could destabilize the market. **The unlocking mechanism translates perfectly our 3 axis of randomness to avoid rug pulls : time threshhold, Mcap threshhold and liquidity amount.**

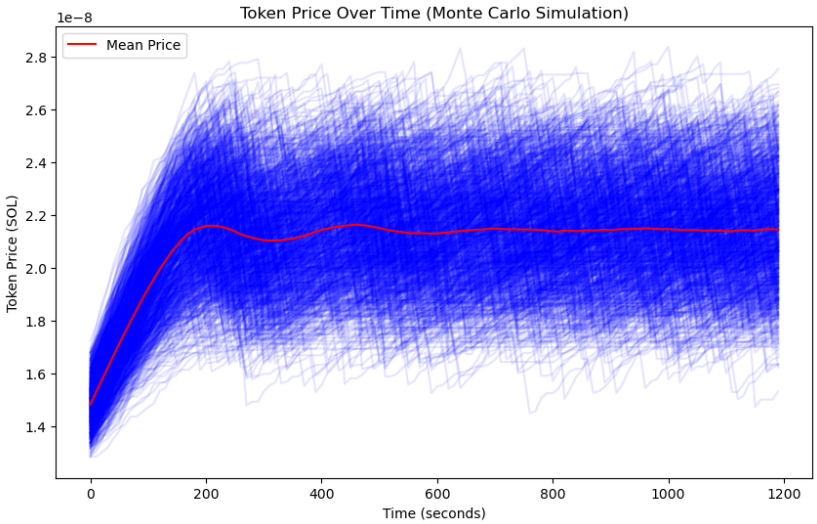

Figure 6: This figure displays the token trajectory of the 1000 simulations in the case of a bad dev inside safer.fun. Th interesting observation to do in this case is that the mean token price does not experience any abrupt drawdown and that on average the price evolves smoothly.

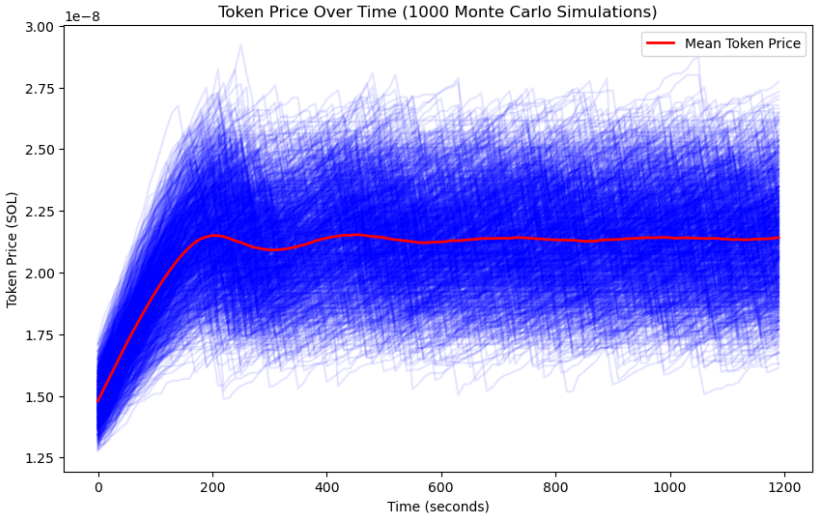

Figure 7: The same thing happen in the case of a honest dev, smooth trajectory on average.