Lottery dApp

Ryan D. Miller, Colin Steidtmann and Seung Y. Lee

Hackathon Team
{Ryan.D.Miller05,colinsteidtmann,seung.youn.lee}@gmail.com

Abstract. Verified randomness allows for blockchains to fairly select winning participants in probability-driven events between decentralized parties. Blockchain-based lossless lotteries are an example of this capability and offer numerous advantages over traditional lotteries around transparency and accessibility. Most notably, they eliminate risk, as a winner's rewards are generated through DeFi protocols and Yield Farming, rather than as a claim on the other participants' stakes; non-winners get their stake back.

[NAME OF DAPP] proposes to use this same principle towards limited edition product drops. These drops have existed for many years in the form of event tickets, but most recently they have been popularized by apparel and even technology companies for physical goods, such as Sneakers, Bags, and gaming systems. Currently, these drops are dominated by rent-seeking middlemen using bots and other methods to capture as much of the product as they can for resale. As such, we seek to democratize these drops using a decentralized lottery where product supporters can increase their odds through brand interaction, promotion and community building.

Keywords: Lottery · Rare Items · DeFi · Smart contracts · Blockchain · Ethereum · ChainLink.

1 Introduction

1.1 Summary

Limited edition product drops have become a key marketing strategy for any product or service that can generate brand equity from 'hype' – a type of grassroots marketing value. However, these drops are vulnerable to manipulation, particularly by Bots who buy up a large portion of the limited product. This artificially inflates the prices on the secondary market, with Bots capturing most of this value.

The potential for brand harm by Bots pricing out some consumers is often outweighed by the additional value to the brand as resale markets act to accelerate hype.

A better solution to the current paradigm would shift the capture of resale value from purely rent seeking middlemen (the Bots) to those who value the brand or service most – the brands biggest supporters.

1.2   History

Yeezy sneakers, Supreme gear, PlayStation 5s, Hot NFT collections. What do they all have in common? They're highly desired products with a limited supply.

Once the province of event tickets such as concerts, sports events and even Burning Man, limited edition product releases – referred to as 'drops' - have become a mainstay of brand marketing. They rely on 'Hype', grassroot driven excitement, and FOMO, fear of missing out. Once relegated to word of mouth in niche circles, social media technologies have brought these hushed forums into virtually every pocket with a phone and Twitter account.[?]

Drops originated in Japanese streetwear brands in the 1990s before spreading to the United States, where the technique was popularized by brands like Supreme and The Hundreds. Drops provide a way for companies to generate a steady drumbeat of press coverage and brand awareness. In the process of shopping a drop, customers often learn everything about the brand story, or the artists that made it. It's powerful from the brand perspective, so much so that even large, established companies use them in between proper, fully fledged product releases. For example, drops now play a prominent role in Nike's direct-to-consumer strategy.[?]

While sneaker companies have been one of the most visible beneficiaries of drop culture, perhaps the largest beneficiary have been resellers. Around 50% of all Nike sneakers that were released in the first quarter of 2021 were available on StockX (a leading reseller marketplace) and had a price premium of 50% or more. Cowan estimates the sneaker resale market at $2B in the US alone, part of a larger $24B resale market.[?]

But herein lies a downside of this marketing strategy – if a reseller gains an advantage over other customers in purchasing a limited release item, they can snatch up much of the entire drop for themselves, and thereby extract unearned value from the resale market they control.

1.3   The Problem: Rent-Seeking Using Bots

Drop products are priced to their target consumers. For years performers priced tickets below the market-clearing price, either out of fairness or out of concern for the long-term value of their brand.[?] In addition, as many tickets are given away or sold to primary channels at contracted rates, premiums are kept in check. Traditional resale markets for tickets reflected a 'truer' premium, but historically these were limited to smaller individual resellers whose labor added a degree of fluidity to the market – thereby adding some value to the exchange as a whole. Think of the lone ticket scalper outside of Yankee stadium.

Beginning with the streetwear drop culture spearheaded by Supreme, this began to change. While relatively low retail prices give consumers of varying financial means an opportunity to buy, high demand for the product feeds into the resale market, and product hits the secondary market at inflated prices. For example, Supreme box logo crewnecks that originally sold for $158 resell for a minimum of $500.[?]

These Supreme drops would occur at their physical store every Thursday, with people queuing in line sometimes for days for the chance to score a drop item. In order to ensure drops were getting into the hands of their actual customers, limits to purchasing were enforced, and Supreme security personnel both inside and outside monitor activity to see if people trade places in line for cash, or if items were being purchased purely for resale.[?]

Still, this didn't prevent resellers with the means to do so from paying individuals to wait in line for them, knowing they would more than recoup the cost in the secondary market.

However, as more retailers began offering drops online, the process that used to involve camping out has now entered the world of high-tech arbitrage - in particular, automated Bots - web scrapers, automated shopping cart 'sniper' bots, and login and checkout abusers.[?] These Bots are run by everyone from individual 15-year-old kids sitting in a basement somewhere making $200,000 a year reselling sneakers, to organized reseller syndicates called "cooks" who deploy professional scraping software[1] to scour the website for the stock-keeping units, or SKUs, associated with new inventory. As new SKUs came online, the bots would add each item associated with that unique ID number to a shopping cart, and once the sale started they would try to complete the checkout process using a preloaded credit card or gift card information. Non-bot-using customers hate them because it's almost impossible to check out faster than a bot can. Frequently, one or two bots buy up a large chunk of the product simply to resell it – a poor customer experience for everyone.[?]

These bots have led to hugely inflated prices in a secondary market controlled by purely rent-seeking individuals, making many of the products inaccessible to the people who actually value them mostly. Nike sees this as a problem: *"We are constantly looking at the best way to combat bots across our digital ecosystem. Nike is fully committed to making sure that our real, loyal consumers are the ones who get fair access to our products and that we continue to evolve best-in-class solutions in the marketplace."*[?]

In 2016, Congress enacted the BOTS Act (Better Online Ticket Sales Act) attempting to legally close this loophole for event tickets.[?] But in 5 years only a single case has been brought to court by the FTC, who are tasked with enforcing the act.[?] Meanwhile, Bots are still wreaking havoc on ticket markets. Take for instance Burning Man, whose core values are "Radical Inclusion, Diversity, and Equity". They admit that their 2019 public ticket sale (the last year the event was held due to COVID) was dominated by Bots.[?] That's a direct affront to their values.

Regardless of the BOTS lack of bite, the legislation does not cover other products. As such, companies are taking it upon themselves to combat Bots in the name of equity for their loyal consumers. *"People are still asking for transparency, and they are still frustrated and angry"*.[?]

Primary retailers tried using raffles rather than first-come first-served sales, but those too have been defeated by bots. This has led them to fighting fire with

---

[1] Cybersole, GaneshBot, and Kodai to name a few.

fire, utilizing anti-bot software such as Akamai, at great cost. Akamai brings in just under $200M a year and is growing 40% annually.[**?**]

It's turned into a cat and mouse game, with Bots becoming more sophisticated in response. Disturbingly, with the COVID-driven increase in ecommerce, and current worldwide supply chain issues, the problem with Bots is only getting worse. *"People will try to jump the line and leverage automation to grab anything that has a limited inventory. It used to be concert tickets, then purses and tennis shoes, and now it's vaccine reservations and even more mundane things."*[**?**]

1.4   Solution Attributes

While Bots damage customer experience, they have created a conundrum. The inflated resale market is now integral to how drops work, as it serves as a metric for a brand's success: the more valuable a product, the higher its resell price tag.

Brands would prefer to replace the brand value generated by Bots inflating the market with brand value generated as close to the customer as possible. Therefore, a better solution to the problem must two key characteristics :

1. Eliminate the Bots, but not resale
2. Offer a mechanism to signal value and grow hype (must compensate for lost hype due to lower secondary market inflation).

2   Paper Roadmap

This whitepaper describes a blockchain powered lottery platform – our solution to the problem with limited release product drops.[2]

We first generalize a decentralized lottery dApp from first principles, giving an overview of the platform. [Section 3] We then define the two user roles within the platform, along with their characteristics and general flows. [Section 4]

Next, the paper describes the initialization and operation of the lottery itself - parametrization, launch, and selection of winners. It then proposes several models to incentivize all users to fulfill their obligations to the platform and each other. [Section 5]

The economics of the platform follow, highlighting value creation and flows across the platform. [Section 6]

Lastly, we will revisit the specific use case outlined in problem statement and describe a platform at launch [Section 7]; before briefly discussing scaling and the future, from governance to features. [Section 8]

---

[2] We speak in the art of what is possible, so certain considerations around gas and LINK optimization, or even mechanics behind a multiple blockchain platform are not explored in-depth. However future iterations of this Whitepaper, and the platform built off of its ideas, will naturally take these considerations into detail.

3   Blockchain Lottery

When the demand for a certain good exceeds its supply, market forces raise the price of the good such that it equals the minimum willingness to pay of those who want it most. When the quantity of a good is highly limited, but price is variable, auctions are often the most effective mechanism for revealing an individual's willingness to pay.
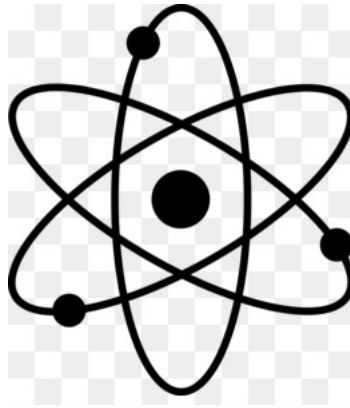

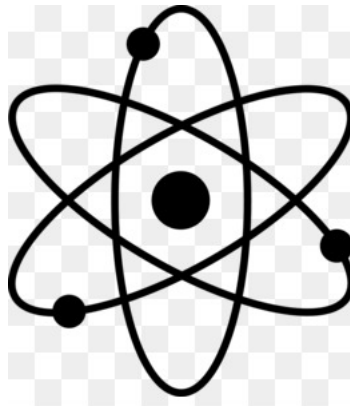**Fig. 1.** S Curve shifting in response to Q decreasing

Fig. 2. Auction mechanism informs S curve shift in response to re-establish equilibrium

But in the case where both quantity and price are fixed, such as in a limited release 'drop', auction mechanisms are no longer effective, as there is no

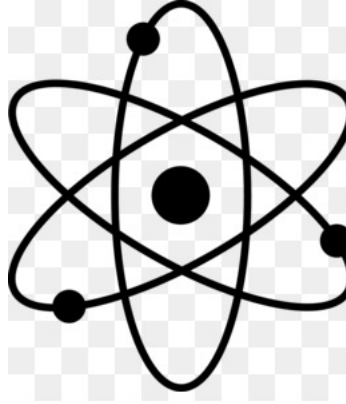differentiation among buyers whose willingness to pay is higher than the fixed price.

Fig. 3. Adding a variable price ceiling with multiple demand curves

Most of these sales are first come first serve, a model easily gamed through technology or collusion by those who seek to capture economic rents from these limited goods by buying then reselling them at inflated prices.[3]

One method to overcome rent-seeking resellers is through a raffle mechanism. Buyers willing to pay the fixed price enter the raffle and are chosen at a set time by random chance. However, it does not address degree of preference of each buyer, and can still be gamed by technology and collusion.

Therefore, we propose a hybrid model combining a raffle with an individual's *overall preference* for a limited good. Overall preference is one's willingness to pay - signaled by the premium they would pay on top of the price of that good, combined with a measure of non-monetary value one is willing to exchange for the good - signaled by hype-generating brand interactions.

A blockchain system can allow this to happen decentrally and automatically. Individuals stake money through a no-loss mechanism – either they win and automatically purchase the item at their stake price, or do not win and receive their money back. The winning Participants are randomly selected with the individual odds for each determined by the strength of their Overall Preferences.

We call this hybrid model blockchain based system [LOTTERY = whatever we plan on calling it.]

---

[3] The original sellers of these are willing to give up the premium they could charge through an auction due to value they receive from the resellers in promotion and marketing. However, we consider that rents rather than earned by those middlemen because those same activities can be undertaken by the end customer themselves who actually value the item. Our platform seeks to disintermediate resellers through the point systems discussed below.

4   Users

The [LOTTERY] platform is composed of Sponsors, who create lotteries, and Participants, who stake funds to win them. As a decentralized platform, any entity in the world can be a Sponsor, and any entity in the world can be a Participant; thus, any user can be both a Sponsor and a Participant. The interface when using the platform as a Sponsor or Participant differ greatly, although every user has access to both. However, most users will utilize the platform as just one of these user types.
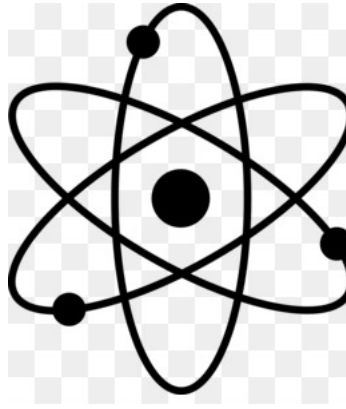

Fig. 4. SIMPLE DIAGRAM OF USERS AND PARTICIPANTS

All users are permanently tied to one or more wallet addresses which serve as their primary identification within the system.[4] This is the only requirement for interacting with the system. However, they can add additional information tied to that wallet including a username, Avatar, and social media accounts. This is more critical for Sponsors in order to identify themselves and their Lotteries to Participants.

4.1   Sponsors

Sponsors create a lottery by defining its parameters and writing them to a smart contract, along with collateralizing the lottery by staking the total value of the lottery into the contract – called the "Purse" (Purse = Price x Quantity) of the lottery's goods.[5]

---

[4] We recommend a dedicated wallet for the platform.

[5] This can be modified as the platform matures and Sponsors develop reputational scores. See the section on Collateral below which also discusses what Sponsors can stake as value.

Sponsors have full control over the parameters of their lotteries, and these parameters are completely transparent to Participants.

Some examples of Sponsors:

- Clothing and Accessory Brands (Nike, Supreme, Yeezy)
- Electronics and Gaming Platforms (Playstation, ASIC Cards)
- Ticketed Events (Musicians, Sports Teams)
- Certain fungible and non-fungible token releases
- Physical Art Collections

Sponsors can mint 'Sponsor Tokens' at a nominal cost per token paid to the platform in addition to any gas fees paid for minting. These are ERC-20 tokens unique to the Sponsor, held in the Sponsor's wallet, and issued to Participants. When transferred to a Participant, the nominal cost paid to the platform is returned to the Sponsor. Only the Sponsor's wallet can mint and transfer these tokens, and once they are issued to a specific Participant's wallet they are locked in that wallet and no longer transferable. Sponsor tokens represent 'points', and these points are applied to a Participant's ticket(s) to improve the probability their selection in the Sponsor's lotteries.
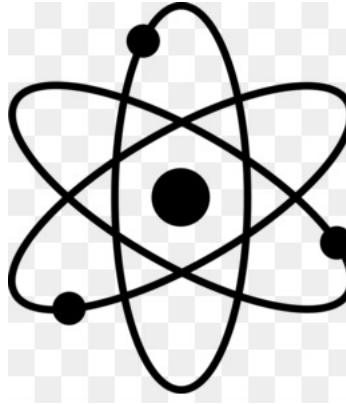

Fig. 5. TOKENS TO POINTS TO BETTER ODDS TO MORE HYPE CREATING VALUE FOR BRANDS

These tokens are given purely at the Sponsor's discretion and Participants typically earn them through brand interaction, promotion, and community building. Sponsor Tokens and the Points they generate are discussed in further detail in both the Participant subsection [4.2], as well as in the Ticketing, the Pool and Ticket Weight Function subsection [5.3].

Sponsors can run as many concurrent lotteries as they like, determining the parameters for each independently.

Sponsor Interface and Dashboard. After registering a wallet with the system, the user accesses the Sponsor interface within the platform.

The Sponsor Interface and Dashboard includes:

- User Settings
- Sponsor Reputational Scores
- Lotteries in Progress, to include Collateral Locked
- Lottery History and Metrics
- Access to their Sponsor Tokens for Distribution
- Lottery Creation

Sponsor Veracity and Reputation. As a decentralized platform, there is no centralized check on the authenticity of any information the Sponsor inputs to their profile. Thus, the tradeoff to decentralization is that anyone can claim to be a brand. A number of mechanisms are used to disincentivize and filter out bad actors from the platform.

First, we expect most Sponsors to validate their wallet address on verified social media accounts they control. In addition, all users will have access to every Sponsor's lottery history. This history includes both rollups and details on individual lotteries including number of entrants, total amount staked by Participants, and winning ticket details (the stakes and points).

Additionally, there is a Reputational Scoring System which serves to verify the legitimacy of the Sponsor.[6] It consists of two separate scores:

1. Distribution Score – This Score indicates the distribution of Sponsor Tokens outside of the Sponsor's Wallet. This distribution and is important to show that the Sponsor is not concentrating Tokens in a few users, potentially indicating collusion between a Sponsor and certain Participants. See Appendix A for more information and a mathematical description of the Distribution Score.

2. Feedback Score – After participants win a lottery, they have the ability to give a simple positive signal back to the Sponsor. Typically, this will occur after the winners redeem their item from the Sponsor. Participants are incentivized to send the signal, however, as it helps the Sponsor whose assets they own and support. The feedback score is a percentage of the number of positive signals divided by the total number of winners, calculated after a short period of time to allow for fulfillment.

$$\text{Feedback Score} = \frac{\text{Positive Signals from all Lottery Winners}}{\text{Total Winners from all Lotteries}} \times 100\% \qquad (1)$$

---

[6] For a dApp without governance, the system needs to be secured purely through Reputational Scores. As it evolves into a DAO, additional safeguards can be made through governance and other methods of verification. For example, a system such as the one used by Proof of Humanity can be used, where other users stake value in support of a Sponsors claim, at the risk of getting their stake slashed if it is determined they are working in collusion with a bad actor.

There is a third score that is less effective in determining Sponsor authenticity, but is an important characteristic of the Sponsor and helps them derive a metric-driven value from the platform. It is called the Hype Score, and it is a measure of the difference between the sum of the Sponsors purses and the Total winning stakes the auctions took in (called the lottery's Residual, discussed in depth in section 5.3).

$$\text{Hype Score} = \frac{\text{Sum of total take from all Sponsor Lotteries}}{\text{Sum of Purses}} \tag{2}$$

4.2   Participants

Users access the Participant interface to enter a lotteries by staking value into a Sponsor's lottery smart contract.[7]

Participant Interface and Dashboard. The Participant Interface and Dashboard includes: User Settings

- Current Lotteries Participating in, to include time remaining and total amount staked
- Lottery History
- Sponsor Tokens, and therefore Points, for Each Sponsor (with depreciation details)
- Recommended Lotteries
- Lottery Search/Browse

Unlike Sponsors, Participants have no external facing metrics on the platform.

Stake Premium. The minimum stake is the Price given by the Sponsor. Additional value staked, called the Stake Price Premium, increases a tickets odds relative to a minimum stake.

Points. Participants receive Sponsor Tokens directly into their wallet. These tokens give the Participant points, on a 1-to-1 basis, for any lottery created by that Sponsor. The Sponsor and Participant must coordinate off-chain so the Sponsor has the Participant's wallet address. This shouldn't be an issue as off-chain is where most of the discovery and value creation between Sponsors and Participants takes place. As mentioned previously, this is a one-way transfer, and these tokens are non-transferable after their initial issue.

Points in turn effect the weight of the ticket, increasing a ticket's odds of winning relative to a ticket with and less points.

---

[7] In the early days of the platform, a uniform cryptocurrency will be used for all transactions with the platform, both in and out. It must be a stable coin to ensure the values remain constant through the length of the lottery. However, at maturity, users will be able to swap any cryptocurrency for the Currency of Account set by the Sponsor, through an integrated swap mechanism directly on the platform.

To what degree points and stake price premium effect the weight of the ticket is also determined by the Sponsors choice of a ticket weight function [5.2] which is determined for each lottery. Participants will be able to view the relative weight of a ticket based on stake, points, and the ticket weight function before actually entering the ticket into the lottery.

Token Depreciation. Sponsor tokens, and the points they grant, are not permanent and depreciate over time. This incentivizes consistent engagement by participants and prevents auctions from overweighting early token earners, thereby disincentivizing new participants.

Ticket depreciation is universal on the platform and follows the following equation:

$$\text{Tocken}_{T+\delta t} = e^{r\dot{\delta}t} \tag{3}$$

5   Lottery Process

The Lottery itself is a smart contract – the Lottery Smart Contract (LSC). It contains the Sponsor's identity and the lottery parameters while holding the collateral, participants stakes, and the ticket pool.

In parallel to the LSC, a separate smart contract containing NFTs representing claims to the lottery items (be they physical or digital) is also created. It is these NFTs that are transferred to the winners at the end of the lottery.

At the end date and time of the lottery (determined by the parameters). The smart contract acquires a random number from Chainlink's VRF. An off-chain deterministic function, living on multiple oracle nodes for security, then calls the random number and ticket data from the Lottery contract to determine the winners, and sends the list back on chain to both the LSC and the NFT contract.
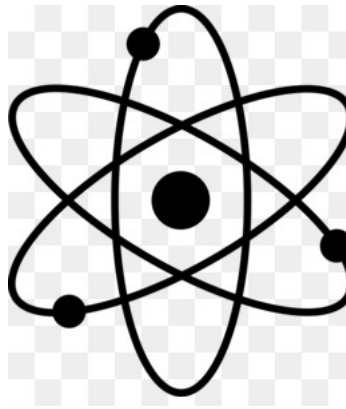

Fig. 6. Lottery Process Diagram

5.1 Creating a Lottery

A Sponsor determines the following lottery parameters which are encoded in the smart contract for that lottery:

- Item Description (to include Web2 links to images and more details)
- Duration
- Currency of Account[8]
- Price of Item
- Quantity of Items
- Ticket Weight Function (explained in detail [in this section])
- Resale Allowed (Y/N)[9]
- Multiple Entries Allowed (Y/N)[10]
- Start Time and Date (optional)[11]
- Public Pre-Lottery (Y/N) – If Y, denote start time and date of pre-lottery, then initiate. Requires Keepers for start.
- Lottery Breakdown by SKU (Y/N)

When the Sponsor is ready to launch the lottery, they must Collateralize the lottery by depositing the total value of the lottery's Purse (Price x Quantity) into the LSC.

Multiple SKU Lotteries. Sponsors can break down their lotteries by size and style. Participants indicate which specific SKU they are staking for, and each SKU winning tickets are distributed amongst only those who indicated them. The Ticket Weight Function is the same for all individual SKU item lotteries.

Collateral. Being an open platform, Sponsors are required to collateralize the auction to prevent Moral Hazard, or outright theft by a Sponsor. This also prevents spamming the platform. The collateral must be in the Currency of Account for the lottery.

The collateral amount is the Purse times a Sponsor Lockup Factor. The current Sponsor Lockup Factor is 1 but can be lowered based on certain reputational factors as the platform matures.

The collateral is locked into the LSC for the duration of the lottery, and is used to provide liquidity to DeXs (Decentralized Exchanges) and interest protocols. If the Sponsor cancels the lottery, only the Collateral is returned and the yield is retained by the platform. If a lottery concludes, both the collateral and yield are given to the Sponsor after fulfillment signaling [5.4].

---

[8] This MUST be in a stablecoin or stable fiat currency.

[9] If Yes, allows a winner to put their winning NFT on the integrated secondary market. If no, the winner must claim the item from the Sponsor.

[10] If Yes, Participants can stake for multiple tickets, but each ticket requires its own stake. All tickets are given the same number of points.

[11] A Sponsor can either launch the Lottery directly after initialization and collateralization, or use Chainlink Keepers to launch at a set date and time but at a cost.

5.2   Ticketing, the Pool and the Ticket Weight Function

Once the lottery begins, Participants enter by staking a value equal to or greater than the item's price thereby earning a chance to win an item. This chance is represented by a ticket.

Tickets are weighted, that is each ticket has a distinct probability of winning compared to other tickets staked for that lottery. Collectively, these individual probabilities are collected into a pool. Rather than one ticket, one chance, each ticket has a unique claim to a portion of the overall pool of entries.
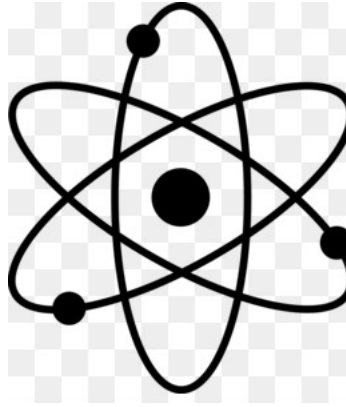

Fig. 7. Mathematical Function of a Weighted Ticket Pool

As most lotteries will have a quantity greater than one, when a ticket is selected as a winner, it is removed from the pool.

If the lottery parameters allow for multiple tickets, a Participant can stake for more than one ticket to win a lottery, with each ticket representing a separate chance to win a single item.

Determining Ticket Weights. Ticket weight is a key aspect to the [LOTTERY] system. It is determined by the Participants stake (in relation to the item price), the number of Points relevant to that Sponsor's lotteries, and the Sponsor's determination of how they want to weight the tickets themselves.

The last aspect is determined by the Ticket Weight Function. It is how the lottery factors in Stake Premium and Points. It is chosen by the Sponsor and drives the off-chain probability function run on oracles nodes. As previously stated, the Participant has full visibility on the effects of ticket weight function on a tickets weight, and can change their intended stake amount to clearly see the effect on ticket weight before staking for a ticket.

The details and math behind the Ticket Weight Function can be found in Appendix Appendix B.

5.3   The Purse, Lottery Value Staked, and Residual

The sum of all winning stakes contained in a lottery's smart contract is called the Lottery's Total Value. Upon conclusion of the lottery, non-winning stakes are returned. The minimum total value for a lottery's must be its Purse - the Purse is what the Sponsor earns directly from the lottery.

Most lotteries will have a Total Value higher than the Purse. The difference is called the *Residual* of the lottery. The residual of the lottery is of huge importance as it is the main driver of value to the platform along with yield farming of stakes. We discuss how the residual is used in greater detail in [6].

5.4   Lottery Outcomes

At end time of the lottery, a 24-hour lockout period of the smart contract begins.[12] This is to ensure the platform can get some yield value while also making it more costly for bots to spam or use flash loans.

After the lockout period ends, Chainlink Keepers will check to ensure the minimum number of tickets have entered the lottery (simply the Quantity of the good offered) and if that passes calls the VRF, send it and the ticket information to the probability function, and return the winners back. Then the following occurs:

- Losing tickets will have their stake transferred back to the Participants wallets[13]
- Winners will receive an NFT representing an ownership claim to a lottery item from the Sponsor
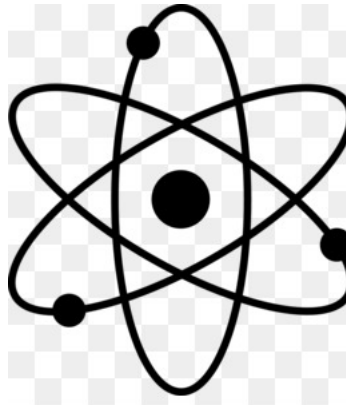

Fig. 8. Diagram of Process

---

[12] Lockout period TBD

[13] Same as above for Participants – they can swap for any other currency.

The last action that needs to happen is the return of collateral (plus any yield) and payment of the Purse to the Sponsor, and how that happens relates to fulfillment of the good to the winning Participants.

Return of Collateral, Sponsor Payment and Fulfillment. A critical question for an open, decentralized system is around Sponsor fulfillment and payment once the lottery ends, a particular challenge here since many of the lottery's will be for physical goods.[14]

Since a winning Participant's stake is already secured, fulfillment focuses on verifying the transmission of the good from the Sponsor to these winners. This determines when the Sponsor receives all the money he is owed post lottery.
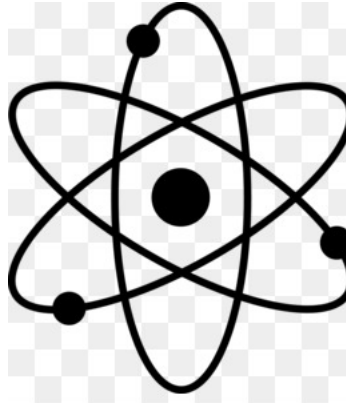

Fig. 9. GAME TABLE of Sponsors and Participants

At maturity, we anticipate a robust ecosystem of automated supply chain tracking and management through blockchain and oracle systems. The Sponsor and Participant will coordinate shipping of good, either off-chain or through privacy maintaining on-chain means. Chainlink oracles can then hold the Participant's winning NFT in escrow until it verifies tracking information from the Sponsor (or runs the entire process itself), at which point the lottery smart contract releases the payment for that good.

There could also be physical vault services that can serve as custodial agents for lotteries, such as Mattereum[15]. They can take possession of the inventory from the Sponsor, pay them the Lottery's Value, and then manage fulfillment.

For the near term, we must rely on the Sponsor trust and reputation systems of the platform to enforce good behavior. Sponsor and Participants will independently coordinate shipping. Once a winner receives their item, they signal this to

---

[14] For digital goods, swapping a winning ticket NFT for an NFT or other digital asset should be fairly simple to verify.

[15] PULL A QUOTE FROM MATTEREUM GUY

the platform through transferring their NFT to the Sponsor, burning it, or some other means. Once $50\% + 1$ of winners send this signal, the collateral, collateral yield, and Purse is released to the Sponsor, and any Residual to the platform. This will be bounded by some period such that Conversely, the Participants can signal malfeasance to the platform as well, and if $50\% + 1$ do so the This will be bounded by some time period.

6   Platform Economics

The platform makes money in two ways:

1. Through capturing part of the residual into a treasury
2. Using this treasury along with staked assets to provide liquidity to DeXs.

Since all monies coming into the platform from residuals are in stablecoins, the treasury is in one or more stablecoins.

Once the Purse has cleared (after proof of fulfillment) the Residual is released and distributed as follows:

- 25% to the Platform treasury
- 25% to the Sponsor of the lottery
- 25% to the lottery winners, divided uniformly
- 25% lump sum to any participant (winner or loser), also determined by the VRF and unrelated to ticket weight

Initially, the treasury will be a multisignature wallet managed by the creators. However, the platform will likely move from a dApp to a DAO, and management will shift to holders of a Governance token. This is the token that controls the protocol, including treasury distribution. Any treasury distribution to holders would be released in proportion to one's ownership of these tokens.

Voting power should increase based on token ownership, but increase decreases quadratically in relation to this overall voting power. In particular, the lottery and treasury distributions are key governance decisions that will undoubtedly be periodically revisited. Quadratic voting drives coalition building, thus reducing the number of periodic revisits.

See Appendix C for discussion on Token Economic Proposals for a DAO.

7   Platform at Launch

Revisiting the problem we pose this to solve – limited edition product drops – we see how it addresses the solution set which is bots and transferring

Defeating Bots – While anyone can become a Sponsor, the stake is costly, and even for those who staked a large amount, or staked on multiple tickets, that creates residual that benefits lots of people. Responsible Sponsors, incentive to make this platform excellent for their core consumers, can set their Ticket Weight Functions to weight Points more heavily.

The platform itself benefits and as it evolves into a DAO, with brands being significant governance token owners. Those bots stake can be held. Cool off period for at least 24 hours.

8   Future Features and Growth

8.1   Near-term Feature Sets

8.2   dApp to DAO Governance

A DAO is the most likely evolution of the platform from its dApp launch state. This would use a governance token to decentralize control of the system and the value it unlocks. The mechanics behind the transition to a DAO are fairly simple once a stable protocol is established.

Appendix C suggests the Token Protocol.

8.3   Secondary Market

A secondary market dominated by mass resellers using Bots is exactly what this platform seeks to mitigate. However, a secondary market allowing individual consumers to resell goods should be supported. It helps signal value and encourage hype for the Sponsor while the core consumers of the good receive the most benefit from resale.

[LOTTERY] will have an integrated Secondary market to allow for seamless resale of goods won. Winning participants can port their winning NFT directly into the Secondary market. These peer-to-peer marketplaces are well established in the NFT space already and would operate much like Opensea or Rarible. It would allow for fixed price, timed auction or open bidding.

NFTs ported directly from the platform will have no service fees as both a reward and incentive to transact on the platform. When economical, it should also pay the gas fees for the user. The secondary market will be open to import and trade other NFTs, however they will be charged a service fee in the range of 1-5

In regards to fulfillment, a lottery NFT is listed on the Secondary market counts as a positive signal towards the release of the Locked Value.

8.4   U2U and Auctions

A generalized use-case of the platform's mechanics are user-to-user, Q = 1 transactions (in a primary market, not a secondary market as described above). This feature would likely bifurcate from the drop lotteries, as they are a different class of value transaction.

Sponsor metrics and Reputation scores would act as a rating system for the user as a whole.[16]

Auctions. A natural extension for the platform would be to support auctions, be they created by a typical drop Sponsor, or a Participant user. This functionality can be added through an auction smart contract suite.

---

[16] although they should be irrelevant when that users acts as a participant since their stake is its own collateral

9   Conclusion

Appendix

A   Distribution Functions

B   TWF

C   Token Protocol