

Web3 Meets Behavioral Economics: An Example of Profitable Crypto Lottery Mechanism Design

Kentaroh Toyoda
SIMTech A*STAR, Singapore
Keio University, Japan
0000-0002-6233-3121

Xuan-The Tran
The University of Technology Sydney
Sydney, Australia
0000-0002-1870-8045

Minh Sang Nguyen
Crypto Sloth
Singapore

Hung Tien Dinh
Crypto Sloth
Hanoi, Vietnam

Abstract—We are often faced with a non-trivial task of designing incentive mechanisms in the era of Web3. As history has shown, many Web3 services failed mostly due to the lack of a rigorous incentive mechanism design based on token economics. However, traditional mechanism design, where there is an assumption that the users of services strategically make decisions so that their expected profits are maximized, often does not capture their real behavior well as it ignores humans’ psychological bias in making decisions under uncertainty. In this paper, we propose an incentive mechanism design for crypto-enabled services using behavioral economics. Specifically, we take an example of crypto lottery game in this work and incorporate a seminal work of cumulative prospect theory into its lottery game mechanism (or rule) design. We designed four mechanisms and compared them in terms of utility, a metric of how appealing a mechanism is to participants, and a game operator’s expected profit. Our approach is generic and will be applicable to a wide range of crypto-based services where a decision has to be made under uncertainty.

Index Terms—Token economics, lottery game mechanism design, behavioral economics, cumulative prospect theory

I. INTRODUCTION

We are often faced with a non-trivial task of designing incentive mechanisms in the era of Web3. The very first blockchain, Bitcoin, also incorporates incentive mechanism into its core consensus algorithm dubbed proof-of-work, where miners compete with each other in its block generation process in return to cryptocurrency. A simple yet elegant incentive mechanism was designed by Nakamoto behind the success of Bitcoin [1]. Now that tokens are easily issued via smart contracts (e.g. via ERC-20 (Ethereum Request for Comments 20)), a large number of new crypto-based services emerged. However, as history has shown, many cryptocurrencies failed mostly due to the lack of a rigorous incentive mechanism design based on token economics [2].

Mechanism design, a field of microeconomics and game theory, helps us derive an optimal mechanism where desired objectives are achieved by incentives. Desired objectives here mean that a service, application, or system work as intended by its operators. In the mechanism design, we start with modeling entities involved in the system such as operators and users. We then devise entities’ profit or utility, which is often derived by subtracting costs from rewards. In the example of Bitcoin’s

mining, incentives are the rewards of newly minted Bitcoins and transaction fees involved in the block, and costs are electric cost consumed by mining. The traditional mechanism design assumes that entities strategically make decisions so that their expected profits are (mathematically) maximized. However, this often does not explain their real behavior well as it ignores humans’ psychological bias in making decisions under uncertainty. For instance, gamblers play a lottery even though they know that its expectation is negative. Hence, we need an alternative approach to better capture participants’ behavior in designing a mechanism.

In this paper, we propose an incentive mechanism design for crypto-enabled services using behavioral economics. Behavioral economics combines elements of economics and psychology to understand how and why people behave the way they do in the real world [3]. Cumulative prospect theory (CPT) is a seminal work of behavioral economics that captures humans’ bias in making decisions under risk [4]. The key idea of applying CPT is to “transform” traditional expectation functions (i.e. utility and probability) so that humans’ bias is better explained, and we will revisit this with a detailed explanation in Section IV. We take an example of crypto lottery game in this work and leverage CPT to design profitable lottery game mechanism for a game operator. We design four mechanisms and compare them in terms of utility, a metric of how appealing a mechanism is for participants, and a game operator’s expected profit. We rigorously test possible parameters and functions of CPT to identify the conditions where the game is appealing to participants and profitable for the game operator.

The contributions of our work are as follows.

- To the best of our knowledge, we are the first to apply behavioral economics to mechanism design in the crypto-based service domain.
- Our approach is generic and will be applicable to a wide range of crypto-based services where a decision has to be made under uncertainty.

The rest of this paper is organized as follows: Section II describes the problem statement. Section III presents a model used in this research. Section IV describes the proposed method. Section V shows numerical results and discusses novelties and open questions. Section VI concludes this paper.

TABLE I
NOTATION TABLE.

Symbol	Description
N_p	Number of participants
f	Entry fee
r	Ratio of amount that an operator takes from collected entry fees
P	Total amount of prizes given to winners (i.e. $N_p \cdot f \cdot (1 - r)$)
P_j	Prize given to the j -th participant
π_j	Profit of participant who ranked in j -th (i.e. $P_j - f$)
$U(\cdot)$	Utility function in the EUT
$v(\cdot)$	Value function in the CPT
$w(\cdot)$	Probability weighting function in the CPT
k	Ratio of participants that can receive prizes in the top- k mechanisms

II. PROBLEM STATEMENT

There are few attempts to apply behavioral economics in the crypto and Web3 domain. As far as we know, the only work was done by Thoma, which investigated the risk and return properties of cryptocurrency trading and found that prospect theory well explains the attractiveness of cryptocurrency trading [5]. Hence, although it would be beneficial to incorporate token economics in designing profitable crypto-based services, none of the work has taken into account human's behavioral perspective to their incentive mechanisms.¹ We take a first step towards introducing a powerful "toolset" of behavioral economics, CPT, to design incentive mechanisms for crypto-based services. Specifically, we chose a crypto-based lottery game as its example as some of us are going to launch one.² The operators of crypto-based lottery games are interested in how to maximize their profits, and it is quite important to predict the expected profits of their games. In this regard, it is vital to understand the behavior of participants. A naive approach is to design game rules and analyze its expected profits of operators and participants. Specifically, when a game rule is given, potential participants need to determine whether or not they should play it based on the expectation of returns. If the expectation of returns is positive, participants are expected to join the game. However, as it will be shown later, this naive approach would not explain their actual behavior well as their action is often biased by psychological factors [10]. The objectives of our research are to suggest designing profitable crypto-based lotteries with behavioral economics and to show how to quantify its goodness with numerical analysis.

III. MODEL

We first model the entities and game design that we analyze in this work. TABLE I lists the notation used in this paper.

¹Of course, the classical approach based on expected utility maximization would work fine when such a human bias is not involved.

²There exist plenty of work that studies gambles from an economical perspective (e.g. [6], [7], [8], [9]). It is challenging to properly cite them here. Yet, one of the closest works is done by Tang *et al.* that analyzed the pricing and design of three lotteries, namely a single prize, multiple equal prizes, and multiple weighted prizes, with CPT [6]. The optimal pricing of each lottery was derived by solving the first- and second-order conditions of lottery buyers' value function, maximizing their utilities.

A. Entities

There are two entities, namely a game operator and participants. An operator first determines a lottery game rule. Given a rule, participants determine whether or not to join a game.

B. Lottery Games

We define our generic lottery game as follows. A participant needs to pay an entree fee f to join a game. We assume that participants are ordered by their ranks at the end of a game. The j -th ranker will be given a prize P_j , and $P_1 \geq P_2 \geq \dots \geq P_{N_p} \geq 0$ where $\sum_{j=1}^{N_p} P_j = P$. The source of prizes is collected entry fees. An operator of the game takes r of the total amount of entry fees, say $r = 10\%$, for their revenue.

One such lottery game example is a top growth rate game where some top participants can gain prizes based on their portfolios' growth rate at the end of a game period.³ Participants are to invest cryptocurrencies during a game period, and compete with each other in their return on investment. We assume that no one can predict the future price of cryptocurrencies and that the rankings of participants' growth rates are determined by random sampling from a uniform distribution. As we only need to determine the ranking of participants' growth rates, when we let $\theta \in [0, 1]$ denote the type of a participant (or a relative competitiveness among participants), the smaller θ the higher chance of being ranked in a higher position (and vice versa). As θ is assumed to follow a uniform distribution, its cumulative density function is simply denoted as $F(\theta) = \theta$. Note that θ is a priori unknown; it is revealed when rankings are determined, meaning that no participant knows his/her own θ at the time of joining a game. Hence, what participants can strategically determine is whether or not to join a game before it starts given a game rule or mechanism, and it thus can be seen as a lottery game.

C. Profits

The profit of operator and participants can be derived as follows. The operator's profit (revenue) can be obtained by multiplying the number of participants N_p by their entry fees f and how much he/she takes r .

$$N_p \cdot f \cdot r. \quad (1)$$

f and r can be determined by an operator while N_p cannot. Hence, an operator has to determine the mechanism that more participants will join (i.e. larger N_p) when f and r are fixed.

On the other hand, the profit of a participant who ended up j -th position is determined by their rankings of growth profit.⁴

$$\pi_j = P_j - f. \quad (2)$$

For an operator to predict if participants will join a game, a naive approach would be to calculate the expectation of their profit and check if it is positive. More specifically, expected utility theory (EUT) is often used to analyze the choice and

³We will test and deploy this particular game as a service.

⁴As gamblers enjoy the game itself, a utility function may need to include positive factors of "excitement" and "entertainment" [11]. However, we simply assume that the positive factor of profit only comes from a game's prize.

behavior of players. In the EUT, they make decisions so that their expected utilities are maximized. A utility here means a value of satisfaction given an outcome. For instance, when a participant receives P_j , his/her utility is represented as a conversion of P_j to $U(P_j)$. A utility function $U(\cdot)$ is increasing, but its curvature is determined by a player's risk preference (e.g. curvature is concave when a player is risk-averse while it is linear ($U(\pi_j) = \pi_j$) when a player is risk-neutral). Hence, an expected utility is represented as follows.

$$\sum_{j=1}^{N_p} p_j U(\pi_p) = \frac{1}{N_p} \sum_{j=1}^{N_p} U(\pi_p) \quad (3)$$

Note that when a participant is assumed to be risk-neutral, the expected utility coincides with the expectation.

However, it is obviously unrealistic to assume that participants follow EUT as this implies that no one will join a game as proven below.

Lemma 1. Individual Rationality: *When (risk-neutral) participants are assumed to strategize their participation under the expected utility assumption, no participant would join the defined game regardless of its mechanism.*

Proof. We first derive a condition that each participant joins the game. For a rational participant joins the game, $E[\pi_p]$ must be larger than or equal to zero. However, θ is revealed only after a participant decides to join a game. Hence, regardless of the value of θ , we simply find the expected utility of participants from Eq. 2. As the probability for a participant to be given each prize is $1/N_p$ for all P_j , the expectation is derived as follows.

$$\begin{aligned} E[\pi_p] &= \frac{1}{N_p} \sum_{j=1}^{N_p} \pi_p, \\ &= \frac{1}{N_p} \sum_{j=1}^{N_p} P_j - f, \\ &= \frac{1}{N_p} N_p \cdot f \cdot (1 - r) - f, \\ &= -r \cdot f. \end{aligned} \quad (4)$$

We used $\sum_{j=1}^{N_p} P_j = N_p \cdot f \cdot (1 - r)$. As $-r \cdot f$ is negative, the expected utility of participants is always negative regardless of the mechanism. \square

However, as research revealed (e.g. [12], [9]), this would not capture the actual behavior of participants (or gamblers), and their behavioral bias must be incorporated into game mechanism design and analysis.

IV. PROPOSED METHOD

We propose a method for an operator to be able to design a lottery game mechanism that takes into account participants' behavioral bias. Again, the objectives of an operator and participants are both maximizing their profits. In this regard, an operator needs to determine a profitable mechanism, i.e. P_j that gives an operator as well as participants more profits,

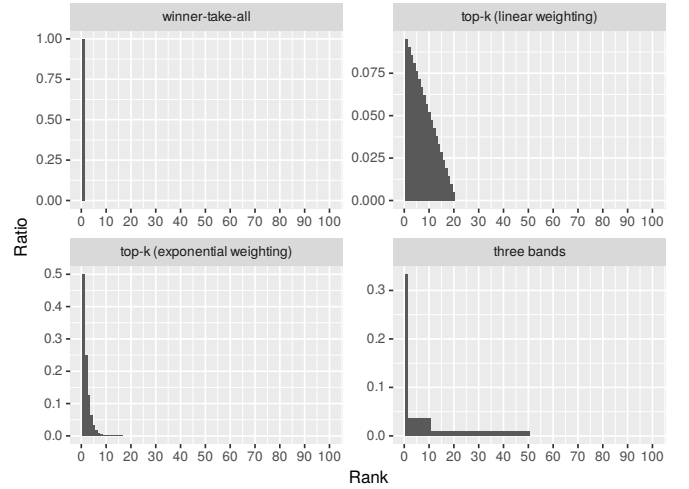


Fig. 1. Comparison of prize distribution ($N_p = 100$, and $k = 20$ for the top- k mechanisms).

and given a mechanism participants strategically determine whether or not to join a game under not EUT but CPT. Although it would be ideal to mathematically derive the most profitable structure of P_j ($1 \leq j \leq N_p$) from participants' utility under CPT via an appropriate method such as first- and second-order derivative, it is not easily tractable due to the complex structure of functions in CPT. Hence, in this paper, we propose a simple-yet-beneficial method to achieve the goal of operator. Our method is composed of the following steps.

- 1) Model entities' behavior.
- 2) List mechanisms, i.e. a set of $\{P_1, \dots, P_j, \dots, P_{N_p}\}$, f and r .
- 3) Calculate participants' utilities with CPT based on the given mechanisms.
- 4) Compare the mechanisms in terms of utility to choose the most profitable mechanism for an operator.

As we have already explained the first step in the previous section, we detail the remaining three steps.

A. Mechanisms

As we cannot implement all the possible mechanisms, an operator needs to pick some promising ones. We compare the following four mechanisms in this paper.

1) *Winner-Take-All*: The winner-take-all mechanism is to give the top ranker everything, i.e. P , while others receive nothing.

$$P_j = \begin{cases} P, & \text{if } j = 1 \\ 0, & \text{otherwise.} \end{cases} \quad (5)$$

2) *Top-k (Linear weighting)*: The top- k mechanism (linear weighting) is to share P among top- k rankers with linear weighting.

$$P_j = \begin{cases} P \cdot \frac{N_p - j + 1}{N_p \cdot (N_p + 1) / 2}, & \text{if } 1 \leq j \leq N_p \\ 0, & \text{otherwise.} \end{cases} \quad (6)$$

Note that $N_p = 1$ corresponds to the winner-take-all mechanism.

3) *Top-k (Exponential weighting)*: This mechanism is similar to the top- k (linear weighting), but its weights are exponentially decreasing by ranks, meaning that the top ranker receives 50% of P and the runner-up receives 25% of P and so on.

$$P_j = \begin{cases} \frac{P}{2^j}, & \text{if } 1 \leq j \leq N_p \\ 0, & \text{otherwise.} \end{cases} \quad (7)$$

Note that although weights should be summed up to 1, the mechanism violates this. However, for sufficiently large N_p , $\sum_{j=1}^{N_p} 1/2^j \rightarrow 1$.

4) *Three bands*: This mechanism is just for a comparison purpose. The top ranker receives $1/3$ of P , the second to tenth share another $1/3$ of P , 11th to 50th share the remaining $1/3$ of P , and the remaining receive nothing. If the number of participants is below 50, then a game is terminated.

$$P_j = \begin{cases} \frac{P}{3}, & \text{if } j = 1 \\ \frac{P}{3 \cdot 9} = \frac{P}{27}, & \text{if } 2 \leq j \leq 10 \\ \frac{P}{3 \cdot 40} = \frac{P}{120}, & \text{if } 11 \leq j \leq 50 \\ 0, & \text{otherwise.} \end{cases} \quad (8)$$

Fig. 1 shows the proposed mechanisms' prize distribution versus ranks. In this figure, $N_p = 100$ and $k = 20$ (20% of participants will receive prizes for the top- k mechanisms). As can be seen from this figure, the top-ranker will receive all prize in the winner-take-all game, whereas top 20 (or 50) out of 100 will share a prize based on their ranks in the top- k and three-band mechanisms.

B. Cumulative Prospect Theory

CPT is one of the powerful theory that incorporates humans' decision making bias under uncertainty into expected utility calculation. Let us give a simple example that violates the theory of simple expectation maximization. If we have two lotteries, (i) 50% of chance of winning \$200 and 50% change of losing \$100 and (ii) 100% chance of winning \$49, and ask players which to play. Many players would choose the latter (i.e. a lottery that a player is sure to win) rather than the former even if the expected gain of the former one is larger (i.e. $-\$100 \cdot 0.5 + \$200 \cdot 0.5 = \$50 > \49). To capture such violations, Kahneman and Tversky presented a model of utility under risk called CPT, which extends traditional utility formulation to take into account humans' behavior on choices [10], [4]. The idea of CPT is to tweak the functions of valuation and probability so that they better explain people's choices under risk. In CPT, players evaluate the following equation rather than Eq. (3).

$$\sum_{j=1}^{N_p} w\left(\frac{1}{N_p}\right) v(\pi_j), \quad (9)$$

where $v(\cdot)$ is a value function and $w(\cdot)$ are decision weights, respectively. In CPT, some characteristics are involved in designing $v(x)$, namely (i) reference dependence, (ii) loss

aversion and (iii) diminishing sensitivity. Reference dependence means that players care about gains and losses that are relative to some point rather than to the absolute amount of their wealth. Loss aversion means that players are more sensitive to losses than to gains, i.e. $|v(x)| < |v(-x)|$ for $x \geq 0$. Diminishing sensitivity means that players tend to be risk-averse in the region of gains but be risk-loving in the region of losses. To capture these characteristics, the value function proposed by Kahneman and Tversky [10], [4], and others (e.g [13]) is as follows:

$$v(x) = \begin{cases} x^\alpha, & \text{if } x \geq 0, \\ -\lambda(-x)^\alpha, & \text{otherwise.} \end{cases} \quad (10)$$

CPT also captures humans' behavior that they tend to overweight unlikely occurring events (i.e. the tails of distribution). Specifically, p_j is now transformed, through a function $w(\cdot)$, into $w(p_j)$. Tversky and Kahneman's weighting function, $w_{TK}(p)$, is expressed as follows.

$$w_{TK}(p) = \frac{p^\delta}{(p^\delta + (1-p)^\delta)^{1/\delta}}. \quad (11)$$

Another example of probability weighting functions includes Prelec's as expressed as Eq. (12).

$$w_{Prelec}(p) = -\exp\{-\beta(-\ln p)^\alpha\}. \quad (12)$$

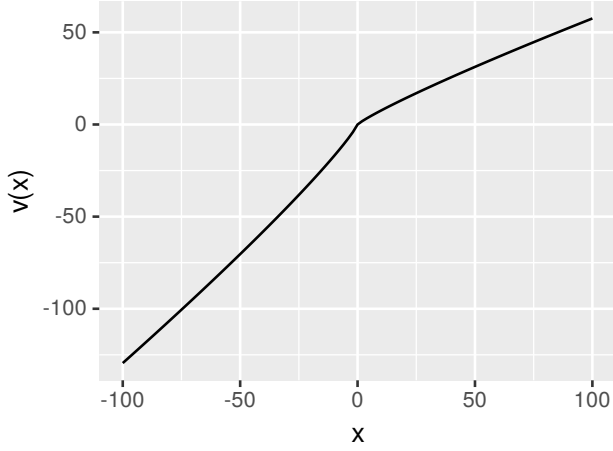
Figures 2(a) and (b) show how $v(x)$ and $w(p)$ transform the values of x and p , respectively. As can be seen from Fig. 2(a), a utility is concave when $x \geq 0$ and convex in $x < 0$ and $|v(x)| < |v(-x)|$ for $x \geq 0$. Similarly, $w(p)$ captures human's tendency to overweight the possibilities of unlikely happening events, while no weighting is considered in the EUT.

C. Comparison of Mechanisms

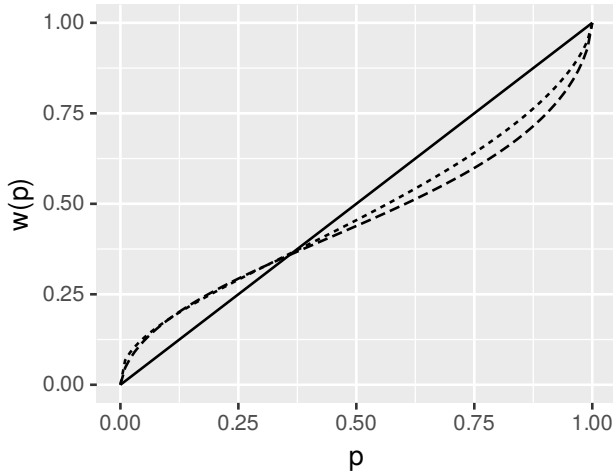
With Eqs. (2), (9), (10) and (11) as well as P_j of the aforementioned mechanisms (i.e. from Eq. (5) to Eq. (8)) we can compare participant's utilities and choose the most promising mechanism for an operator. In this regard, we need to determine a value function, probability weighting function and their parameters. The parameters of these functions (e.g. Eqs. (10) and (11)) are often determined via social experiments (e.g. [4], [13], [14], [15]). Subjects are recruited to join experiments, and the parameters are inferred from the experiments' results. Hence, when using the parameters obtained in this way, we need to make sure that the games in their experiments should be similar to those at hand. In this paper, we compare (i) Tversky and Kahneman's functions and (ii) Prelec's functions with the parameters inferred by their past social experiments (e.g. [4], [13]). The reason of the choice of these two is that they have well used to explain the behavior of lotteries in the past (e.g. [7]).

V. PERFORMANCE EVALUATION

We compare the mechanisms described in the previous section, namely (i) winner-take-all, (ii) top- k (linear weighting), (iii) top- k (exponential weighting) and (iv) three-band



(a) Value function $v(x)$



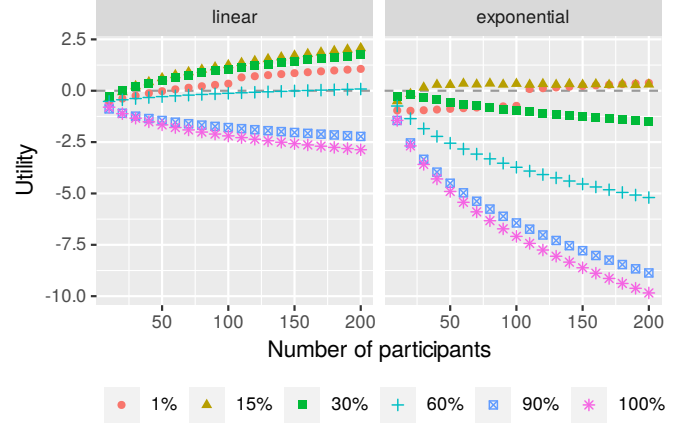
— EUT - - - Prelec - · - Tversky and Kahneman

(b) Probability weighting functions $w(p)$

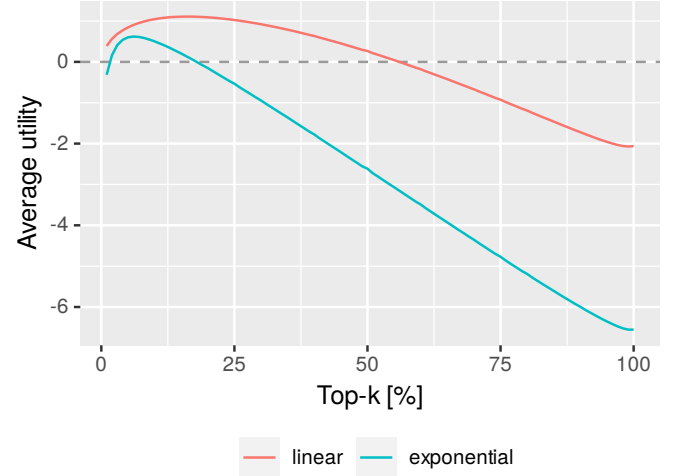
Fig. 2. The value function $v(x)$ and probability weighting functions $w(p)$ proposed by Tversky and Kahneman ($\alpha = 0.88, \lambda = 2.25$ for $v(x)$, and $\delta = 0.65$ for $w_{TK}(p)$) [4] and by Prelec ($\alpha = 0.65, \beta = 1$ for their $w_{Prelec}(p)$) [13].

mechanisms, in terms of participants' utility under the CPT assumption. We also clarify how r and f affect the operator's profit and how profitable each mechanism is. Regarding f , we assume cardinal values (e.g. 1, 2) rather than actual currencies for generality. A positive utility means that a mechanism is attractive to participants, and they thus should join, and vice versa. Furthermore, the higher utility the more attractive to participants. We determine the optimal k s for the two top- k mechanisms (i.e. linear weighting and exponential weighting described in Sections IV-A2 and IV-A3) and use them for the overall comparison. Our codes are available at our GitHub repository.⁵

⁵<https://github.com/kentaroh-toyoda/Design-of-Profitable-Crypto-Lottery-Mechanisms-with-Prospect-Theory>



(a) Effect of k to utility.



(b) Average utility versus k . Optimal k is 16% for linear weighting and 6% for exponential weighting.

Fig. 3. Effect of k in linear and exponential weighting. We used Tversky and Kahneman's value function $v(x)$ with $\alpha = 0.88, \lambda = 2.25$ and probability weighting function $w_{TK}(p)$ with $\delta = 0.65$ [4], $r = 10\%$, and $f = 1$.

A. Optimal k

We determine the optimal k for the two top- k mechanisms (i.e. linear weighting and exponential weighting described in Sections IV-A2 and IV-A3). Here, we used Tversky and Kahneman's value function $v(x)$ with $\alpha = 0.88, \lambda = 2.25$ and probability weighting function $w_{TK}(p)$ with $\delta = 0.65$ [4], $r = 10\%$, and $f = 1$. N_p and k were varied from 1 to 200 and from 1% to 100%, respectively. Fig. 3a shows the result. As can be seen from this figure, for both weighting methods, when k is high (i.e. when most of participants are expected to receive prizes but small amounts), it is less appealing to them. Similarly, when k is extremely low (i.e. when only few participants receive prizes), it is also less appealing. Hence, there should be somewhere that maximizes participants' utilities. We find such an optimal point by averaging utilities over the number of participants. Fig. 3b shows average utilities over N_p versus k . We can see from this figure that there are optimal points on

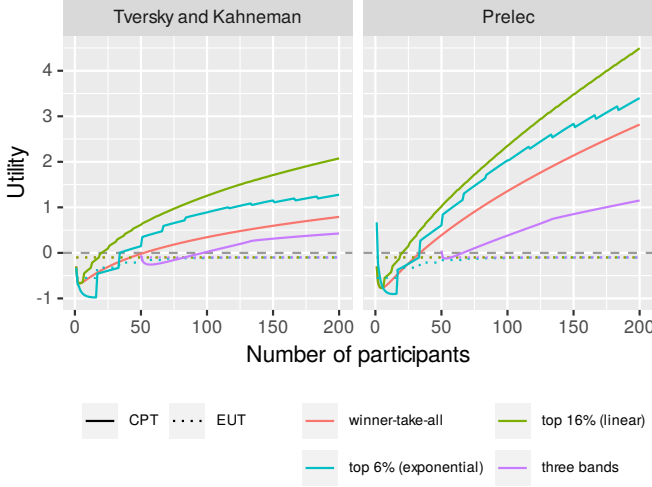


Fig. 4. Utility comparison under the different assumptions.

both linear weighting ($k = 16\%$) and exponential weighting ($k = 6\%$). We use these k s for the following evaluation.

B. Comparison of Mechanisms

We clarify the relationships between utility and number of participants, N_p , as well as different assumptions (i.e. value and probability weighting functions, CPT versus EUT).⁶ As mentioned in the previous section, we compare (i) Tversky and Kahneman's value function $v(x)$ with $\alpha = 0.88, \lambda = 2.25$ and probability weighting function $w_{TK}(p)$ with $\delta = 0.65$ [4] and (ii) Prelec's (the same $v(x)$ and $w_{Prelec}(p)$ with $\alpha = 0.65, \beta = 1$) [13], where these parameters were inferred by their past social experiments (e.g. [4], [13]). We also assumed $r = 10\%$ and $f = 1$ and varied N_p from 1 to 200. The optimal parameters of k in the two top- k mechanisms were used, namely $k = 16\%$ and $k = 6\%$ for linear and exponential weighting, respectively.

Fig. 4 shows the comparison of utilities by different mechanisms and assumptions. We can clearly see the difference of utilities under the CPT assumption. The top-16% (linear weighting) is the most appealing mechanism for participants in the sense that (i) the minimum number of participants required to achieve a positive utility (i.e. 21 required for the top-16% (linear weighting), 34 for the top-6% (exponential weighting), 53 for the winner-take-all, and 97 for the three bands) and that (ii) it achieves higher utilities than the others. From this result, we can say that the winner-take-all and top-6% (exponential weighting) are too risky and less appealing to participants and that the top-16% (linear weighting) mechanism provides a good balance of risk and return. However, we can only say that it is the best among the four mechanisms tested; it is an open question to find the theoretically optimal mechanism. Likewise, although our findings are true against the value and

⁶Although we proved that the expected utility of risk neutral participants are always negative, we plot it for reference purposes.

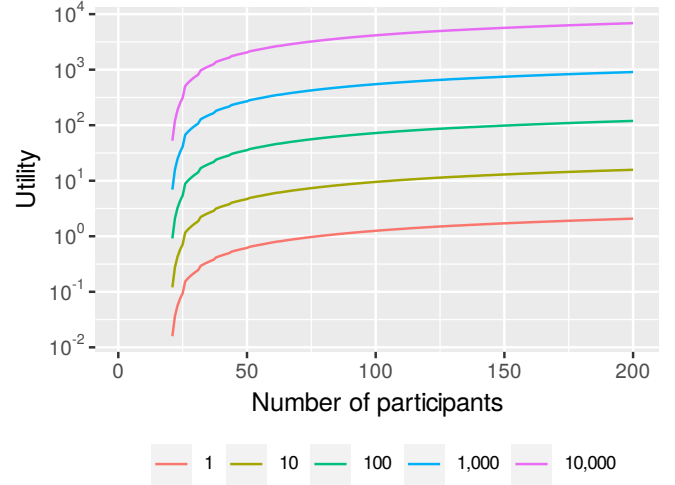


Fig. 5. Effect of f .

probability weighting functions tested, it may not hold true to other functions.

C. Effect of f

We clarify how f affects participants' willingness to join the game. Fig. 5 shows the log-scale comparison of utilities when f is varied from 1 to 10,000. We used Tversky and Kahneman's functions with the same parameters and the top-16% (linear weighting) mechanism for this evaluation. Regardless of the values of f , utilities are positive when $N_p \geq 21$. We can see from Fig. 5 that the higher the entry fee the more appealing to participants. In our game, as accumulated entry fees are distributed to top-16% after an operator takes r of it, the more entry fee would be appreciated by participants. However, it is still an open question that this still holds true even if we replace f with a real fiat or crypto currency. For instance, is $f = 1$ BTC, which is around US\$30,000 at the time of writing this paper, more appealing than $f = 0.01$ BTC? Although this seems too risky, the proposed approach cannot explain this well yet.

D. Effect of r

We then clarify how r affects participants' utilities. Fig. 6 shows the utilities when r is varied from 5% to 90%. As can be seen from this figure, the higher r , the less appealing to participants, which is quite understandable as participants will receive less amount of prize when r is high. For extreme cases (e.g. $r = 90\%$), utility keeps decreasing even if N_p increases. Furthermore, the higher r the more participants are required for utility to become positive. For instance, only 19 participants are required for $r = 5\%$, whereas 45 are required for $r = 30\%$.

E. Operator's Expected Profit

Finally, we compare operator's expected profits when r and f are varied. We use the same setting as Section V-D except that N_p , r and f are varied from 1 to 50, from 5% to 20% and

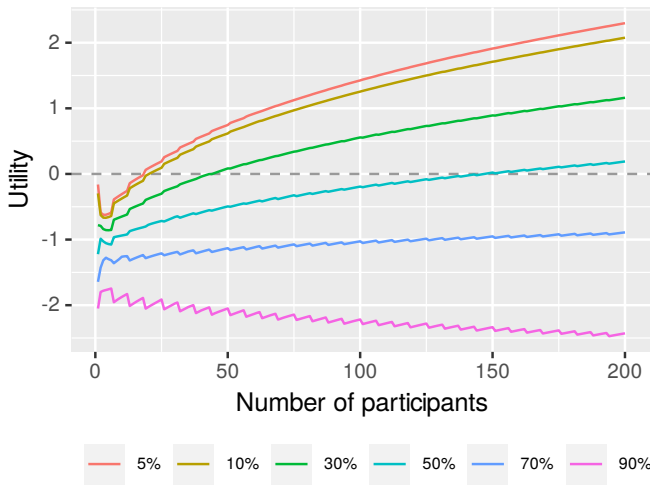


Fig. 6. Effect of r .

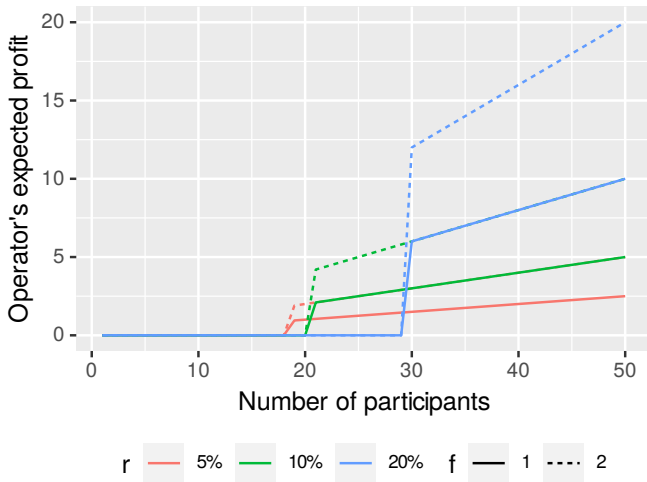


Fig. 7. Expected Operator's profit.

from 1 to 2, respectively. Fig. 7 shows the operator's expected profits. Note that some results correspond at some regions. For instance, the results of $(r = 5\%, f = 2)$ and $(r = 10\%, f = 1)$ correspond when $N_p \geq 21$. From the operator's perspective, r should not be too small to increase profitability. However, the higher r , the more participants should join for a game to be appealing. In this regard, one of the operator's strategies is to infer the expected number of participants somehow and to set r accordingly. For instance, if 30 participants may join a game, then r should be less than 20% as this is the maximum r .

F. Discussion

The contributions of our method are that it provides a reasonable way of designing crypto lottery mechanisms and comparing them in terms of utilities as well as profits. Besides, the method discussed is generic. We believe that it can be applied to other use-cases such as design and analysis of optimal

blockchain mining reward and token-based applications such as crowdsourcing and data mining platforms.

On the flip side, we are aware of the following limitations which remain open questions.

- Obtained results and conclusions may be biased by a chosen value function, probability weighting function and their parameters. It is necessary to check if the conditions of experiments where such parameters are derived are similar to the problems at hand.
- An operator must manually come up with possible mechanisms, and thus the truly optimal mechanism may be missed.
- The model of CPT used in this paper does not explain well how fiat or crypto currency f affects participants' willingness to join. Is $f = 1$ BTC more appealing than $f = 0.01$ BTC even if the former is too risky?
- This analysis only focuses on a single game. However, it may be necessary to analyze mechanisms and utility when a game is repeated as in [7].
- More factors may need to be considered in modeling participants' behavior. For instance, there is a report that risk attitudes differ by countries and depend not only on economic conditions but also on cultural factors [16].

VI. CONCLUSIONS

We have proposed a method of designing the mechanism of lottery games with an example of crypto-based lottery game. The key idea is to incorporate behavioral economics into mechanism design to better predict participants' willingness to join a game and operator's profitability based on utility analysis. In particular, we leveraged CPT to model participants' behavior. We proposed four mechanisms for the game and thoroughly evaluated them in terms of utility and profit by varying parameters. Our evaluation suggests that the top- k (linear weighting), which distributes prizes to top- k participants of a game and the amount of prizes linearly declines with their ranks, is the best mechanism among the four mechanisms. We have also clarified the relationships between utility and the number of participants under some assumptions (e.g. how the parameters of how much an operator takes and entry fee affect utilities and the minimum number of participants required to make a game appealing).

Our method has some contributions in designing a crypto-based lottery game, however, there is some room for improvement. For instance, ours do not explain well that utilities keep increasing even if a game is too risky to join when an entry fee is too high. We will tackle these issues and provide a better mechanism design method.

REFERENCES

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," <https://bitcoin.org/bitcoin.pdf>, 2008.
- [2] P. Toepffer and D. Thatmann, "Taxonomy and Universal Success Parameters of Token Models in Distributed Ledger Systems," in *Proc. of Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*. IEEE, Sep. 2020, pp. 35–39.

- [3] M. Witynski, "Behavioral economics, explained," <https://news.uchicago.edu/explainer/what-is-behavioral-economics#:~:text=Behavioral%20economics%20combines%20elements%20of,decisions%20based%20on%20those%20preferences.>, accessed: 2022-6-3.
- [4] A. Tversky and D. Kahneman, "Advances in prospect theory: Cumulative representation of uncertainty," *Journal of risk and uncertainty*, vol. 5, no. 4, pp. 297–323, 1992.
- [5] A. Thoma, "A Prospect Theory Model for Predicting Cryptocurrency Returns," Dec. 2020.
- [6] P. Tang, R. Pan, and J. Liu, "Behavioral economics analysis on product design of sports lottery," in *Proc. of International Conference on Information Management, Innovation Management and Industrial Engineering*. IEEE, Nov. 2010.
- [7] N. Barberis, "A Model of Casino Gambling," *Management science*, vol. 58, no. 1, pp. 35–51, Jan. 2012.
- [8] O. Kesten, M. Kurino, and A. S. Nesterov, "Efficient lottery design," *Social choice and welfare*, 2017.
- [9] R. Baker, D. Forrest, and L. Pérez, "Modelling demand for lotto using a novel method of correcting for endogeneity," *Economic modelling*, vol. 84, pp. 302–308, Jan. 2020.
- [10] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Handbook of the fundamentals of financial decision making: Part I*, vol. 47, no. 2, pp. 263–292, 1979.
- [11] R. M. Stetzka and S. Winter, "How rational is gambling?" *Journal of economic surveys*, Oct. 2021.
- [12] N. C. Barberis, "Thirty years of prospect theory in economics: A review and assessment," *Journal of Economic Perspectives*, vol. 27, no. 1, pp. 173–196, 2013.
- [13] D. Prelec, "The Probability Weighting Function," *Econometrica: journal of the Econometric Society*, vol. 66, no. 3, pp. 497–527, 1998.
- [14] R. Gonzalez and G. Wu, "On the shape of the probability weighting function," *Cognitive psychology*, vol. 38, no. 1, pp. 129–166, 1999.
- [15] A. Bruhin, H. Fehr-Duda, and T. Epper, "Risk and rationality: Uncovering heterogeneity in probability distortion," *Econometrica: journal of the Econometric Society*, vol. 78, no. 4, pp. 1375–1412, 2010.
- [16] M. O. Rieger, M. Wang, and T. Hens, "Prospect Theory Around the World," Oct. 2011.