Piecewise Parimutuel Markets for Mining Pool Decentralization

James Pierog

July 2024

> “I didn’t anticipate pooled mining and its effects on the security of the network. Making Bitcoin a competitive monetary system while also preserving its security properties is not a trivial problem, and we should take more time to come up with a robust solution. I suspect we need a better incentive for users to run nodes instead of relying solely on altruism.” — Satoshi Nakamoto

1 Introduction

Variance of winning the block reward has caused Bitcoin miners to aggregate hashrate into pools. Pools are currently the only mechanism that enable miners to de-risk variance. Due to variance based pooling pressure, an oligopoly of dominant pools currently mine most blocks. This poses a critical censorship risk which undermines the core value proposition of Bitcoin. Variance based pooling pressure must be indefinitely alleviated to enable Bitcoin to flourish as a p2p censorship-resistant digital cash system.

We propose a piecewise parimutuel prediction market to enable miners to hedge their hashrate every block. Miners can bet on which pool mines the next block and make money even if they do not win the block reward. Speculators can profitably bet to balance market liquidity with actual event probabilities. A piecewise parimutuel market can unlock Bitcoin-native ROI every block, and can enable miners to profitably mine in smaller pools with higher variance.

2 Market Design

Parimutuel markets have a rich history of use in various domains, including horse racing and financial derivatives trading. These markets have been extensively studied and experimented with by academics and practitioners alike, focusing on market design [8, 9, 7, 6], equilibrium [10], and optimized betting strategies [11, 4, 2]. For instance, Bill Benter famously applied a statistical model to generate optimized bets on the parimutuel markets of the Hong Kong horse races, resulting in almost 1 billion USD in profits [1]. In the financial sector, Goldman Sachs and Deutsche Bank have utilized parimutuel markets to create derivatives on economic indicators, enabling the hedging of core risks [5, 6].

Parimutuel markets operate on a winner-take-all principle, where all bets are pooled together, and the winning bets are paid out a share of the pooled amount, minus a commission. The parimutuel mechanism aligns well with the winner-take-all nature of Bitcoin mining, where miners compete globally to win the provably probabilistic proof-of-work contest [3]. Parimutuel prediction markets offer a compelling and simple solution to the problem of block reward variance for miners without introducing additional changes to the Bitcoin protocol or intermediary tokens, e-cash, or other (custodial) Bitcoin substitutes. A parimutuel market can rely solely on the decentralized financial infrastructure in the Bitcoin Lightning ecosystem to facilitate all bets.

In a standard parimutuel market, participants wager on a set of mutually exclusive outcomes. The total pool of bets, minus a commission, is distributed among the winning bets in proportion to the amount wagered on the winning outcome. Formally, let $\Omega = X_1, \ldots, X_n$ be a set of mutually exclusive outcomes with probabilities $p_1, \ldots, p_n$, respectively. The total amount of money bet on each outcome X_i is b_i. The payout for a winning bet β on outcome X_i is calculated as follows:

$$\text{Payout}(\beta) = \frac{\beta}{b_i} \cdot (1 - c) \cdot \sum_{j=1}^{n} b_j,$$

where c is the commission rate.

We propose a modification to the standard parimutuel market, which we call a piecewise parimutuel market. In this market, participants wager on the occurrence or non-occurrence of individual outcomes, rather than on the outcomes themselves. For each outcome X_i, let Y_i and N_i denote the total amounts wagered on the occurrence (yes) and non-occurrence (no) of X_i, respectively. After the event occurs and the actual outcome is determined, participants who correctly predicted the occurrence or non-occurrence of X_i are entitled to a share of the total pool of bets on that outcome, minus the commission. Formally, for each outcome X_i, let y_i and n_i denote the bets placed by a participant on the occurrence and non-occurrence of X_i, respectively. The payout for a correct bet $\beta \in y_i, n_i$ on outcome X_i is calculated as follows:

$$\text{Payout}(\beta) = \frac{\beta}{W_i + \beta} \cdot (1 - c) \cdot (Y_i + N_i + \beta),$$

where $W_i = Y_i$ if the bet was placed on the occurrence of X_i (i.e., $\beta \in y_i$), and $W_i = N_i$ if the bet was placed on the non-occurrence of X_i (i.e., $\beta \in n_i$).

3 Application to Bitcoin Mining Pools

The piecewise parimutuel prediction market can be applied to Bitcoin mining pools to help alleviate the variance problem faced by miners. In this context, a new prediction market is created for each block, with the outcomes being the mining pools currently in operation.

Consider the following example market for a single block:

Outcome	**Probability**	**Total Bet Yes (sats)**	**Total Bet No (sats)**
Foundry	0.28	28	72
AntPool	0.21	21	79
ViaBTC	0.14	14	86
F2Pool	0.12	12	88
Binance	0.03	3	97
Luxor	0.02	2	98
Braiins	0.02	2	98
MARA	0.02	2	98
BTC.com	0.02	2	98
Spider	0.02	2	98
SBI	0.02	2	98
SEC	0.01	1	99
Other	0.03	3	97

In this market, participants can bet on whether a specific mining pool will mine the next block (bet yes) or not (bet no). The probabilities represent the likelihood of each pool mining the next block based on their hashrate.

Suppose a miner bets 10 sats on ”yes” for the Foundry pool, which has a total ”yes” bet of 28 sats and a total ”no” bet of 72 sats. If Foundry indeed mines the next block, the miner’s payout would be:

$$\text{Payout}(10) = \frac{10}{28+10} \cdot (1-0.05) \cdot (28+72+10) = 27.5 \text{ sats}$$

where the commission rate c is set to 0.05 (5%).

To calculate the ROI, we use the following formula:

$$\text{ROI} = \frac{\text{Payout} - \text{Initial Investment}}{\text{Initial Investment}} \times 100\%$$

Plugging in the values from the example:

$$\text{ROI} = \frac{27.5 - 10}{10} \times 100\% = 175\%$$

This example demonstrates how both miners can use the piecewise parimutuel prediction market to hedge against the variance in block rewards. By betting on multiple pools, miners can stabilize their cash flow, even if their pool does not mine the next block.

Speculators can profit from the piecewise parimutuel prediction market by providing liquidity and exploiting market inefficiencies. One strategy is to bet on longshot outcomes with high potential returns.

Consider a speculator betting $\beta_B = 2$ sats on ”yes” for Braiins pool, with $p_B = 0.02$, $Y_B = 2$ sats, $N_B = 98$ sats, and $c = 0.01$. If Braiins mines the next block, the speculator’s payout is:

$$\text{Payout}(2) = \frac{2}{2+2} \cdot (1-0.01) \cdot (2+98+2) = 50.49 \text{ sats},$$

resulting in an ROI of:

$$\text{ROI} = \frac{50.49 - 2}{2} \times 100\% = 2,424.5\%.$$

This example demonstrates the potential for speculators to achieve high returns by betting on long-shot outcomes with low market odds. By providing liquidity to the market and exploiting potential inefficiencies, speculators contribute to the overall stability and efficiency of the piecewise parimutuel prediction market for Bitcoin mining pools.

4 Basic Betting Strategy

In this section we prove that as long as the market odds differ from the probabilities of the outcomes, there exist profitable betting opportunities.

Definition 1. *The* ***market odds*** *of an event X is*

$$Odds(X_i) = \frac{Y_i}{Y_i + N_i}.$$

The market odds is an indicator that reflects the market belief in the probability of an outcome. Market odds, when defined in this fashion, are analogous to the price per share in traditional prediction market mechanisms (like LSMR or dynamic parimutuel markets). Where the price per share of a binary option in a traditional prediction market reflects the market belief in the probability of an outcome, the odds, as defined above, reflects the market belief of the probability of an outcome.

Definition 2. *The* ***expected value*** *of a bet β placed on yes (Y) is*

$$EV_Y(\beta) = p_i \cdot \left[(1-c) \cdot \left(\frac{\beta}{\beta + Y_i}\right)(\beta + Y_i + N_i) - \beta\right] - (1-p_i) \cdot \beta,$$

and the expected value of a bet β sats placed on no (N), is

$$EV_N(\beta) = (1-p_i) \cdot \left[(1-c) \cdot \left(\frac{\beta}{\beta + N_i}\right)(\beta + Y_i + N_i) - \beta\right] - p_i \cdot \beta.$$

Another way to think about the definition of expected value is

$$\text{EV}(\beta) = p_i \cdot (\text{Profit}) - (1-p_i) \cdot (\text{Loss}) = p_i \cdot (\text{Payout}(\beta) - \beta) - (1-p)\beta$$

The expected value reveals the average profit/loss if an agent bets β sats in the market given the current market odds. If the expected value is positive, then the bet β is profitable in the long run. If the expected value is negative, then the bet β is not profitable in the long run.

Lemma 1. *For any bet β,*

$$EV_Y(\beta) > 0 \iff p(1-c) > \frac{\beta + Y}{\beta + Y + N}$$
$$EV_N(\beta) > 0 \iff (1-p)(1-c) > \frac{N + \beta}{Y + N + \beta}$$

Proof. In the first case we observe

$$\begin{aligned}
& p(1-c) > \frac{\beta+Y}{\beta+Y+N} \\
\iff & p(1-c)\left(\frac{\beta+Y+N}{\beta+Y}\right) > 1 \\
\iff & \left(p(1-c)\left(\frac{\beta+Y+N}{\beta+Y}\right) - 1\right) > 0 \\
\iff & \beta\left(p(1-c)\left(\frac{\beta+Y+N}{\beta+Y}\right) - 1\right) > 0 \\
\iff & \beta\left(p(1-c)\left(\frac{\beta+Y+N}{\beta+Y}\right) - (1-p) - p\right) > 0 \\
\iff & p(1-c)\left[\frac{\beta}{\beta+Y}(\beta+Y+N) - \beta\right] - (1-p)\beta > 0 \\
\iff & \mathrm{EV}_Y(\beta) > 0.
\end{aligned}$$

Similarly, in the second case we find

$$\begin{aligned}
& (1-p)(1-c) > \frac{N+\beta}{Y+N+\beta} \\
\iff & (1-p)(1-c)\left(\frac{Y+N+\beta}{N+\beta}\right) > 1 \\
\iff & (1-p)(1-c)\left(\frac{Y+N+\beta}{N+\beta}\right) - 1 > 0 \\
\iff & \beta\left((1-p)(1-c)\left(\frac{Y+N+\beta}{N+\beta}\right) - 1\right) > 0 \\
\iff & \beta\left((1-p)(1-c)\left(\frac{Y+N+\beta}{N+\beta}\right) - (1-p) - p\right) > 0 \\
\iff & (1-p)(1-c)\left(\frac{\beta}{\beta+N}\right)(\beta+Y+N) - (1-p)\beta - p\beta > 0 \\
\iff & (1-p)\left[(1-c)\left(\frac{\beta}{\beta+N}\right)(\beta+Y+N) - \beta\right] - p\beta > 0 \\
\iff & \mathrm{EV}_N(\beta) > 0.
\end{aligned}$$

□

Lemma 2. *If Odds$(X) < (1-c)p$, then there exists some $\beta > 0$ such that*

$$\frac{Y+\beta}{Y+N+\beta} < p \cdot (1-c).$$

Proof. Suppose $\mathrm{Odds}(X) < (1-c)p$. First, we want to show that there exists some $b > 0$ such that

$$\frac{Y+b}{Y+N+b} = p \cdot (1-c).$$

Let's solve for b:

$$\begin{aligned}\frac{Y+b}{Y+N+b} &= p\cdot(1-c)\\ Y+b &= (p\cdot(1-c))(Y+N+b)\\ Y+b &= (1-c)pY+(1-c)pN+(1-c)pb\\ Y+b-(1-c)pY-(1-c)pb &= (1-c)pN\\ Y(1-(1-c)p)+b(1-(1-c)p) &= (1-c)pN\\ b(1-(1-c)p) &= (1-c)pN - Y(1-(1-c)p)\\ b &= \frac{(1-c)pN-Y(1-(1-c)p)}{1-(1-c)p}\end{aligned}$$

Now, we need to show that $b > 0$. Since $\text{Odds}(X) < (1-c)p$, we have:

$$\begin{aligned}\frac{Y}{Y+N} &< (1-c)p\\ Y &< (1-c)p(Y+N)\\ Y &< (1-c)pY+(1-c)pN\\ Y-(1-c)pY &< (1-c)pN\\ Y(1-(1-c)p) &< (1-c)pN\end{aligned}$$

Therefore, $(1-c)pN - Y(1-(1-c)p) > 0$. Since $0 < c < p < 1$, we also have $1-(1-c)p > 0$. Thus,

$$b = \frac{(1-c)pN-Y(1-(1-c)p)}{1-(1-c)p} > 0.$$

Hence, there exists a $b > 0$ such that $\frac{Y+b}{Y+N+b} = p\cdot(1-c)$. Thus, for any $\beta \in (0,b)$ we have

$$\frac{Y+\beta}{Y+N+\beta} < \frac{Y+b}{Y+N+b} = p\cdot(1-c)$$

□

Lemma 3. *If Odds*$(X) > 1-(1-p)(1-c)$*, then there exists some* $\beta > 0$ *such that*

$$\frac{N+\beta}{Y+N+\beta} < (1-p)\cdot(1-c).$$

Proof. We see if $\text{Odds}(X) > 1-(1-p)(1-c)$ then

$$\begin{aligned}&\frac{Y}{Y+N} > 1-(1-c)(1-p)\\ \iff\ & Y > (1-(1-c)(1-p))(Y+N)\\ \iff\ & \frac{Y}{1-(1-c)(1-p)} > Y+N\\ \iff\ & \frac{Y}{1-(1-c)(1-p)} - Y - N > 0.\end{aligned}$$

Then, suppose there exists some β such that $0 < \beta < \frac{Y}{1-(1-c)(1-p)} - Y - N$. Then we have

$$\begin{aligned}
&\beta < \frac{Y}{1-(1-c)(1-p)} - Y - N \\
\iff\ & Y + N + \beta > \frac{Y}{1-(1-p)(1-c)} \\
\iff\ & 1-(1-p)(1-c) < \frac{Y}{Y+N+\beta} \\
\iff\ & 1 - \frac{Y}{Y+N+\beta} < (1-p)(1-c) \\
\iff\ & \frac{N+\beta}{Y+N+\beta} < (1-p)(1-c).
\end{aligned}$$

Therefore, if $\text{Odds}(X) > 1-(1-p)(1-c)$ then there exists a $\beta > 0$ such that $\frac{N+\beta}{Y+N+\beta} = (1-p)\cdot(1-c)$. □

Theorem: If $\text{Odds}(X) \notin ((1-c)p, 1-(1-p)(1-c))$ then there exists some bet β such that

$$\text{EV}_Y(\beta) > 0 \ \text{ or } \ \text{EV}_N(\beta) > 0.$$

Proof. If $\text{Odds}(X) \notin ((1-c)p, 1-(1-p)(1-c))$ then either $\text{Odds}(X) < (1-c)p$ or $\text{Odds}(X) > 1-(1-p)(1-c))$.

Case 1: $\text{Odds}(X) < (1-c)p$
If $\text{Odds}(X) < (1-c)p$ then by Lemma 2 we know that there exists some β such that

$$\frac{Y+\beta}{Y+N+\beta} < (1-c)\cdot p.$$

Therefore, we substitute for $p \cdot (1-c)$ in the definition of the expected value to yield:

$$\begin{aligned}
\text{EV}_Y(\beta) &= p \cdot \left[(1-c)\cdot\left(\frac{\beta}{\beta+Y}\right)(\beta+Y+N) - \beta\right] - (1-p)\beta \\
&= \frac{Y+\beta}{Y+N+\beta}\left(\frac{\beta}{\beta+Y}\right)(\beta+Y+N) - p\beta - (1-p)\beta \\
&> \beta - p\beta - (1-p)\beta \\
&> \beta - p\beta - \beta + \beta p \\
&> 0.
\end{aligned}$$

Case 2: $\text{Odds}(X) > 1-(1-p)(1-c)$
If $\text{Odds}(X) > (1-c)p$, then by Lemma 3 we know there exists some β such that

$$\frac{N+\beta}{Y+N+\beta} < (1-p)(1-c) \implies \frac{Y+N+\beta}{N+\beta} > \frac{1}{(1-p)(1-c)}.$$

We can substitute this in our definition for expected value to yield

$$\begin{aligned}
\mathrm{EV}_N(\beta) &= (1-p)\left[(1-c)\left(\frac{\beta}{\beta+N}\right)(\beta+Y+N)-\beta\right]-p\cdot\beta \\
&= \beta\cdot(1-p)(1-c)\left(\frac{\beta+Y+N}{\beta+N}\right)-(1-p)\cdot\beta-p\cdot\beta \\
&> \beta\cdot(1-p)(1-c)\left(\frac{1}{(1-p)(1-c)}\right)-\beta \\
&> \beta\cdot\left(\frac{(1-p)(1-c)}{(1-p)(1-c)}\right)-\beta \\
&> \beta-\beta>0.
\end{aligned}$$

Thus, as both cases are proven, so long as $\mathrm{Odds}(X) < (1-c)p$ or $\mathrm{Odds}(X) > 1-(1-p)(1-c)$ then there exists some bet β with positive expected value. □

5 Conclusion

We have proposed a piecewise parimutuel prediction market as a mechanism for miners to hedge against the variance of winning the block reward. By betting on the occurrence or non-occurrence of specific pools mining the next block, miners can stabilize their cash flow and reduce their risk.

We have formally defined the market structure and provided examples of how the market would operate in practice. Additionally, we prove that as long as the market odds differ from the true probabilities of the outcomes, there exist profitable betting opportunities. Specifically, we outline the necessary and sufficient conditions for any bet in the market to have a positive expected value.

A piecewise parimutuel prediction market offers a compelling solution to variance based pooling pressure faced by miners, without requiring changes to the Bitcoin protocol. By providing a mechanism for miners to hedge their risks and for speculators to profit from market inefficiencies, this market design has the potential to foster a more decentralized and resilient mining pool ecosystem.

References

[1] William Benter. “Computer Based Horse Race Handicapping and Wagering Systems: A Report”. In: (1994).

[2] Ruth N. Bolton and Randall G. Chapman. “Searching for Positive Returns at the Track: A Multinomial Logit Model for Handicapping Horse Races”. In: *Management Science* 32.8 (Aug. 1986), pp. 1040–1060.

[3] Nicola Dimitri. “Bitcoin Mining as a Contest”. In: *Ledger Journal* (2017).

[4] Rufus Isaacs. “Optimal Horse Race Bets”. In: *The American Mathematical Monthly* 60.5 (May 1953), pp. 310–315.

[5] Christopher Pissarides Jeffrey Frankel. “Macroeconomic Derivatives: An Initial Analysis of Market-Based Macro Forecasts, Uncertainty, and Risk”. In: *National Bureau of Economic Research* (2005).

[6] Jeffrey Lange Ken Baron. “From horses to hedging”. In: *Risk* (2003).

[7] Jeffrey Lange Ken Baron. *Parimutuel Applications in Finance*. Palgrave Macmillan, 2007.

[8] David M. Pennock. “A Dynamic Pari-Mutuel Market for Hedging, Wagering, and Information Aggregation”. In: May 2004, pp. 170–179.

[9] Charles R. Plott, Jorgen Wit, and Winston C. Yang. “Parimutuel Betting Markets as Information Aggregation Devices: Experimental Results”. In: *Economic Theory* 22.2 (Sept. 2003), pp. 311–351.

[10] Richard E. Quandt. “Betting and Equilibrium”. In: *The Quarterly Journal of Economics* 101.1 (Feb. 1986), pp. 201–208. URL: `http://www.jstor.com/stable/1884650`.

[11] Bernard Rosner. “Optimal Allocation of Resources in a Pari-Mutuel Setting”. In: *Management Science*. Theory Series 21.9 (May 1975), pp. 997–1006.