
Exploring the Operation of Winner-Take-All Contracts in Crypto-Prediction Markets

MICROECONOMICS - ECON 401A

Mauricio Vargas-Estrada

Santiago Naranjo-Manosalva

Master in Quantitative Economics

University of California - Los Angeles

This project, led by Mauricio Vargas and Santiago Naranjo, will focus on providing an understanding of how prediction markets operate in the realm of cryptocurrencies. Specifically, we will explore the functioning of Winner-Take-All contracts, where the object of interest is the occurrence of an event. Prediction markets are a valuable tool for assessing market expectations, and it is theorized that they have the potential to include all available information thanks to the intervention of many agents creating a joint projection. Additionally, we will investigate the interactions between the different agents in the prediction markets, how the predictions are formed, and, finally, we will use examples of contracts in Polymarket to investigate different assumptions about these markets.

1 Predictive Markets

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

1.1 Winner-Takes-All Contracts

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

2 Crypto-Predictive Markets

The Crypto-Predictive Markets are a special type of decentralized finance where blockchain infrastructure is used to define smart contracts that can later be traded without the need for an intermediary, using some type of cryptocurrency as the exchange currency (Hassan et al., 2023). All transactions are recorded within the blockchain's ledger, being accessible to anyone who has a copy of the network. Additionally, there are special web browsers that allow viewing the records, filtering the information according to the user's needs. Below, we explore some basic concepts and how such infrastructure is employed in the context of predictive markets using Winner-Takes-All (WTA) type contracts.

2.1 Basic Concepts

To understand the operation of a Crypto-Predictive Market, it is necessary to define some concepts that will later be used to describe how this infrastructure can be adapted in the context of WTA-type predictive market.

2.1.1 Blockchain, Cryptocurrency and Layers

Commonly transactions are recorded in a ledger, which is an accounting book that records all transactions made. In the context of blockchain, this ledger is a distributed record among all the nodes of a network, which function as a redundant storage system. The term arises from the need to separate this record into blocks, in such a way that the handling of information is more efficient. Since the ledger or accounting book must be consistent throughout each block, they are chained together by a unique key called a hash.

In some blockchain protocols, layers are defined, so that the primary layer handles general records, while secondary layers handle specific records, which can be referenced from the primary layer without the need to record them directly. In the secondary layer, special rules can be defined for the management of records, such as the definition of a smart contract.

The process of recording a block in the ledger requires that a unique key be generated to chain the blocks. This generation of keys is not automatic, but requires the computation of keys through computational power. Different blockchains implement tokens called cryptocurrencies, which are used as rewards for the nodes that perform the computation of the keys. This process is called mining, and it is the way in which the consistency of the ledger is maintained throughout the network. Because the records in the ledger can represent real transactions, there is a monetary equivalence for cryptocurrencies, due to the added value of recording the transaction.

2.1.2 Smart Contracts

A smart contract is a program embedded in the secondary layer of the blockchain. This contract contains the rules and deadlines that will enforce the promise of an agreement between two or more parties. These contracts do not require a legal intermediary to mediate between the parties, and the defined execution conditions are validated by a network of specialized agents known as oracles (Makarov & Schoar, 2022).

2.1.3 Oracles

Smart contracts typically establish execution conditions that require information not recorded within the blockchain. The inclusion of such external information and its tracking within the blockchain is not efficient, so a solution to this problem is to use agents that follow and validate the external information. When the contract’s execution condition is met, these agents inform the contract that the condition has been fulfilled, and through a voting system, a consensus is reached among information validating agents as to whether the condition was met or not. These agents are called oracles (Hassan et al., 2023).

Oracles can be human agents or programs external to the blockchain. To validate a contract’s condition, oracles must stake a certain amount of money, usually in the form of cryptocurrencies. Those who correctly validate the information receive a reward, while those who do not lose the money staked.

The more oracles a smart contract has, the more robust the results will be, and the lower the probability that a malicious oracle can alter the outcome. The number of oracles needed depends on the nature of the contract. For example, the outcome of an official Champions League football match may require few oracles, with applications connected to official information sources. On the other hand, validating hypotheses or opinions may require a larger number of oracles, due to the inherent subjectivity of the information.

2.2 Crypto-Predictive Markets

In a Crypto-Predictive Market, a smart contract is used to define the rules of a market, setting the conditions under which a market is considered resolved. Agents can participate in the market, buying and selling shares according to their beliefs. When the market is resolved, those agents who bought shares in accordance with the correct outcome receive a reward, while those who bought shares based on an incorrect outcome lose the money staked. Oracles are used to validate the outcome of this market, which, according to the terms defined in the smart contract, receive a reward or are penalized for the correct or incorrect validation of the contract’s execution condition.

A special type of contract is the Winner-Takes-All (WTA). In the context of a smart contract, this specific type uses a binary execution condition, either fulfilled or not fulfilled. The price of the shares is set between 0 and 1, and those agents who bought shares according to the correct outcome receive a reward of 1, having a gain of $1 - p$, where p is the price at which they bought the share.

2.3 Polymarket

Polymarket is a web platform that facilitates the participation of agents in markets defined through smart contracts. The platform is merely an interface where agents can interact with the smart contracts defined on Polygon, a blockchain that operates on the secondary layer of Ethereum, designed to facilitate the creation and management of smart contracts (“Learn - Polymarket”, 2023).

In Figure 1, an example of a predictive market on the Polymarket platform can be seen. It shows the main elements which are: (i) the name of the market, (ii) the conditions under which the market is considered resolved, (iii) the information source that the oracles will consult, (iv) the date on which the market closes, (v) the total amount of bets measured in dollars, and (vi) the price of the long and short positions.

In these markets, the long position represents those agents who believe that the market will resolve as true, while the short position represents those agents who believe the opposite. In Figure 1, the long position (indicated in green) represents those agents who expect the FED to cut interest rates by May 2024, while the short position (indicated in red) represents those agents who expect the FED not to cut interest rates for the same date.

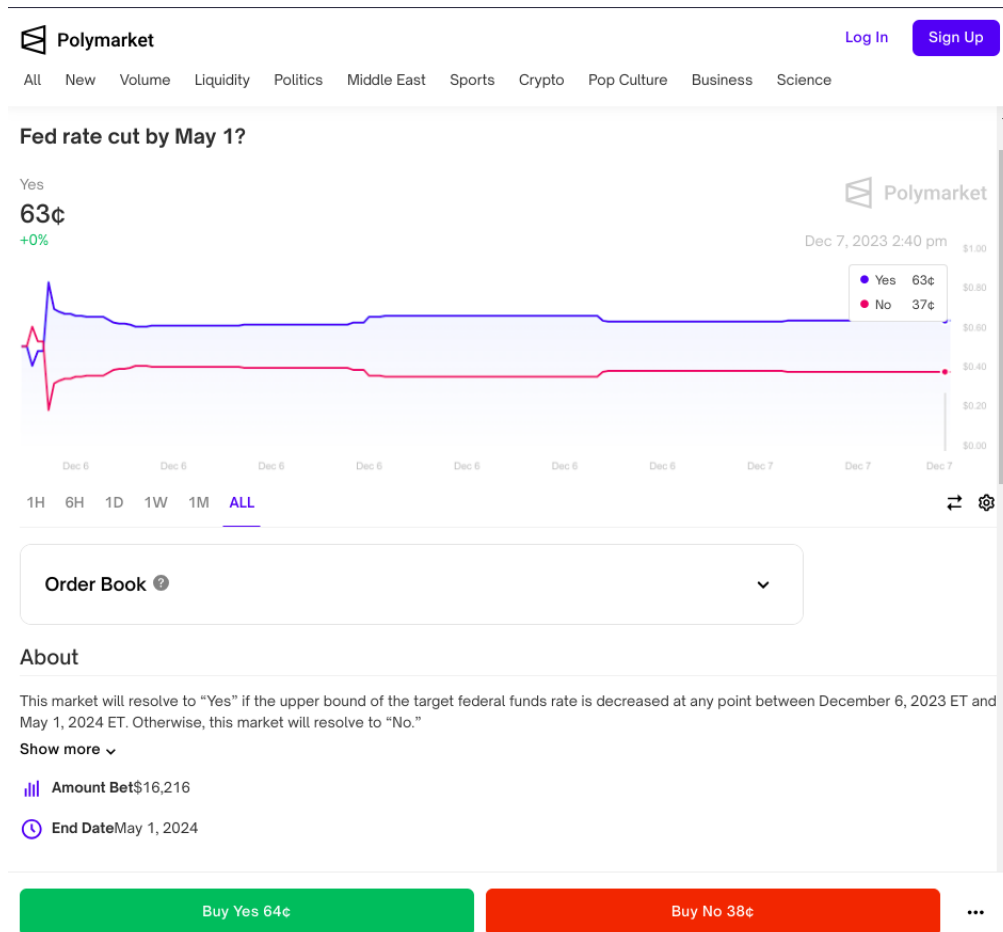
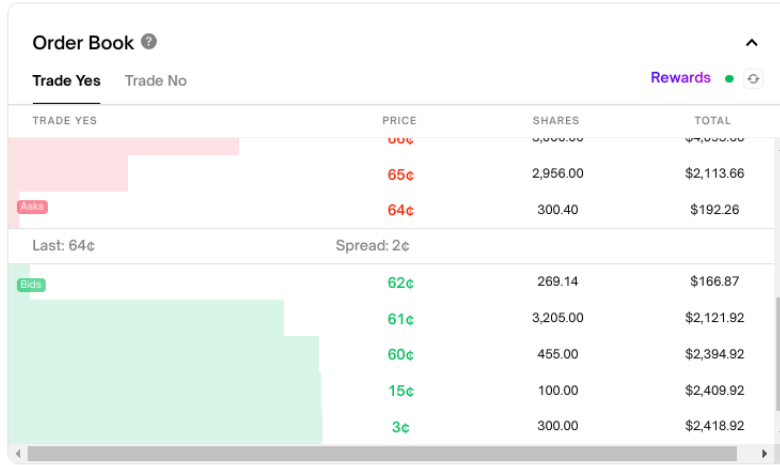


Figure 1: Polymarket Platform

The price of the long and short positions add up to one, and the interpretation of this price is the probability that agents assign to the market resolving as true or false. In Figure 1, the price of the long position is 0.63, which means that the aggregated probability of agents expecting the FED to cut interest rates by May 2024 is 63%. Complementarily, the price of the short position is 0.37, which means that the aggregated probability of agents expecting the FED not to cut interest rates by May 2024 is 37%.

2.3.1 Supply and Demand Mechanism

The price of the long and short positions is determined through a supply and demand mechanism. This mechanism is recorded in the Order Book.

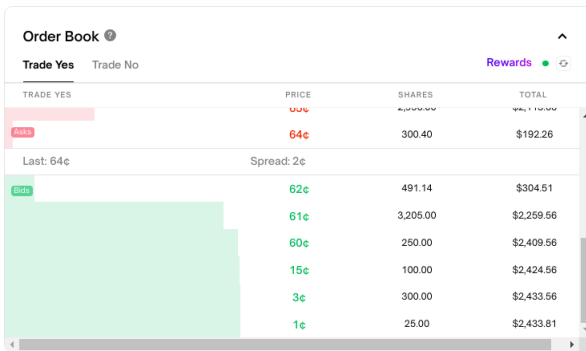


The image shows a screenshot of an 'Order Book' interface. At the top, there are tabs for 'Trade Yes' and 'Trade No', and a 'Rewards' section with a green dot and a refresh icon. Below the tabs, the table is divided into 'ASK' (top, red background) and 'BID' (bottom, green background) sections. The 'ASK' section shows orders to sell, with prices 65¢ and 64¢. The 'BID' section shows orders to buy, with prices 62¢, 61¢, 60¢, 15¢, and 3¢. The table has columns for PRICE, SHARES, and TOTAL. The current price is 64¢, and the spread is 2¢.

TRADE YES	PRICE	SHARES	TOTAL
ASK	65¢	2,956.00	\$2,113.66
ASK	64¢	300.40	\$192.26
Last: 64¢ Spread: 2¢			
BID	62¢	269.14	\$166.87
BID	61¢	3,205.00	\$2,121.92
BID	60¢	455.00	\$2,394.92
BID	15¢	100.00	\$2,409.92
BID	3¢	300.00	\$2,418.92

Figure 2: Order Book for the Long Positon

In Figure 2, the Order Book for the long position can be observed. In the center, the last transaction made is shown, which determines the current price. In the upper part (called Ask), all the agents willing to sell their long positions at a certain price are listed, and in the lower part (called Bid), all the agents willing to buy long positions are found. In the order book only the unrealized orders are shown, that is, those orders that have not been matched. When an order is matched, the transaction is recorded in the blockchain, and the order is removed from the order book.



This image shows the 'BID' section of the order book. It lists orders to buy at prices 62¢, 61¢, 60¢, 15¢, and 3¢. The table has columns for PRICE, SHARES, and TOTAL.

PRICE	SHARES	TOTAL
62¢	491.14	\$304.51
61¢	3,205.00	\$2,259.56
60¢	250.00	\$2,409.56
15¢	100.00	\$2,424.56
3¢	300.00	\$2,433.56
1¢	25.00	\$2,433.81

Figure 3: Order Book for the Long Position: Bid



This image shows the 'ASK' section of the order book. It lists orders to sell at prices 99¢, 98¢, 88¢, 86¢, 85¢, 81¢, 76¢, and 69¢. The table has columns for PRICE, SHARES, and TOTAL.

PRICE	SHARES	TOTAL
99¢	25.00	\$5,564.40
98¢	300.00	\$5,539.65
88¢	44.00	\$5,245.65
86¢	205.00	\$5,206.93
85¢	100.00	\$5,030.63
81¢	205.00	\$4,945.63
76¢	205.00	\$4,779.58
69¢	79.37	\$4,623.78

Figure 4: Order Book for the Long Position: Ask

Orders in the Ask section are arranged such that those with the lowest price have priority. Conversely, orders in the Bid section are arranged from the highest price to the lowest.

In both the Ask and Bid sections, agents set their prices according to the level of certainty they have that the contract will be executed in their favor. Buyers with low expectations are willing to enter the market

only if the price of the share is low (Figure 3). Conversely, sellers with high expectations are willing to leave the market only if the price of the share is high (Figure 4).

3 Revising the Assumptions About Predictive Markets

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

4 Conclusion

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

5 References

- Hassan, A., Makhdoom, I., Iqbal, W., Ahmad, A., & Raza, A. (2023). From trust to truth: Advancements in mitigating the blockchain oracle problem. *Journal of network and computer applications*, 217, 103672–.
- Learn - polymarket [Accessed: 2023-12-06]. (2023). <https://learn.polymarket.com/>
- Makarov, I., & Schoar, A. (2022). *Cryptocurrencies and decentralized finance (defi) / igor makarov, antoinette schoar*. National Bureau of Economic Research.
- Peterson, J., Krug, J., Zoltu, M., Williams, A. K., & Alexander, S. (2020). Augur: A decentralized oracle and prediction market platform. *arXiv.org*.
- Wolfers, J., & Zitzewitz, E. (2004). Prediction markets. *Journal of economic perspectives*, 18(2), 107–126.