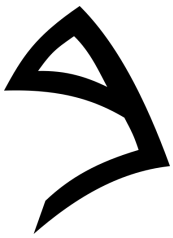
TezBet: A Decentralized Approach to Sports Betting

Eloi BESNARD, Enguerrand DECLERCQ, Jean-François DUMOLLARD, Victor LAFORET

19 december 2021



Abstract

TezBet is a decentralized application built on the Tezos blockchain. It offers a self-sufficient alternative to common centralized soccer betting services. Using the zero-sum game principle, it does not need to store any backing liquidity to pay the winners, for their share is calculated upon the total bet amount. Using this mechanism, odds manipulation and bankruptcy are both made impossible.

1 Introduction

Most sport betting services rely on centralized third parties for both odds computing and gains distribution. On one hand, the players' spendings flow through a company's account before being redistributed accordingly. This means that such companies could arbitrarily choose to keep the players' spendings for themselves. On the other hand, the way odds are calculated remains vague. While they are supposed to reflect the mere likelihood of an outcome, they are mostly meant to keep betting companies sustainable. Ultimately, data collection through KYCs is inevitable using this kind of services.

2 Game rules

Betting on TezBet comes with some rules. Players' agreement is inferred when they use TezBet; TezBet being fully self-sufficient, players automatically comply with these rules.

- Players can place and remove bets on non-started games
- Players can bet on several games simultaneously
- Players cannot bet on ongoing games
- Players cannot remove bets from ongoing games
- Players cannot redeem their gains before the final score has been set

3 Theory behind odds: zero-sum game

Zero-sum game is a mathematical representation in game theory and economic theory of a situation in which an advantage that is won by one of two sides is lost by the other. If the total gains of the participants are added up, and the total losses are subtracted, they will sum to zero. Thus, cutting a cake, where taking a more significant piece reduces the amount of cake available for others as much as it increases the amount available for that taker, is a zero-sum game if all participants value each unit of cake equally. In the markets and financial instruments, futures contracts and options are zero-sum games as well.
In contrast, non-zero-sum describes a situation in which the interacting parties' aggregate gains and losses can be less than or more than zero. In our example, most betting services are non-zero-sum games: they take profit from the players' losses and cover the winners' gains through their treasury.

The way we leverage zero-sum mechanism is as follows:

Let n the number of players.
Given $a_{k,j}$ the amount bet on outcome k by player j, the multiplier of the bet amount for this outcome k, can be stated as

$$G_k = \sum_{j=0}^{n} \frac{(a_{TeamA,j} + a_{TeamB,j} + a_{Tie,j})}{a_{k,j}} \tag{1}$$

Therefore a winning player j who bet $a_{k,j}$ XTZ on outcome k will receive $G_k \times a_{k,j}$ XTZ.

4 Simulating potential gains

Table 1 is an example of potential gains for a fictive game in which Team B wins. This scenario shows the total bet amount by each player and their returns by the end of the game according to their choice.

Table 1: Simulation of a game in which Team B wins

Player	Bet amount (XTZ)	Choice	G_k	Return (XTZ)
1	7,500	Team B	2.625	19,687
2	2,000	Tie	10.5	0
3	10,000	Team A	1.9	0
4	1,000	Team A	1.9	0
5	500	Team B	2.625	1,312

5 Leaderboard

6 Hybrid data collection

6.1 Oracles

Blockchain oracles are entities that connect blockchains to external systems, thereby enabling smart contracts to execute based upon inputs and outputs from the real world[1].

[1] https://chain.link/education/blockchain-oracles

Oracles provide a way for the decentralized Web 3.0 ecosystem to access existing data sources, legacy systems, and advanced computations. Decentralized oracle networks (DONs) enable the creation of hybrid smart contracts, where on-chain code and off-chain infrastructure are combined to support advanced decentralized applications (dApps) that react to real-world events and interoperate with traditional systems.

Each oracle acts the same way a standard API does; the main difference is that data is fetched and currated by a network of independent validators. Decentralized oracles network Chainlink aggregates data from various nodes scraping the same API. Ultimately, Chainlink uses different sources aka oracles for each data collection, which means that a single spoofing oracle will not affect data integrity.

6.2 Contract storage

To be truely self-sufficient, TezBet cannot rely on a single API because of potential data spoofing. Therefore, TezBet uses a decentralized network of sport data oracles provided by Chainlink. These oracles allow TezBet to define whether the games are playing or not and fetch the final score, while preventing potential data spoofing from a single oracle.

Besides, the games timetables are stored in the contract storage in a timestamp format. It allows TezBet contract to prevent users from betting after the game has begun without making additional oracle calls.

6.3 Frontend display tradeoff

Looking for the next games and their live scores would constitute costly and gas-intensive oracle calls. Besides, we would need a bot to consume oracles and update the contract storage. Instead, we are using standard APIs to look for the next games and their live scores. This tradeoff allows us to minimize transaction fees while displaying the data players need on the frontend. Although, the games status and their final scores are checked through oracle calls.

References

Author, A.N and Another, A. N., 2010, MNRAS, 431, 28.