Sports betting is ideally suited for a completely on-chain smart contract. Consensus odds are well-known, statistically accurate, and stable for major sporting events. For American football and mixed martial arts, the weekly schedule gives the oracle enough time to validate off-chain data before sending it to the contract. Over $50B was wagered on US sportsbooks in 2021, and the demographic skews towards young men, just like crypto. A contract targeting a portion of this market is small enough to manage and big enough to matter.

There are three types of contract users: bettors, liquidity providers, and an oracle-admin. Bettors can take either side of any regular bet offered, subject to a size constraint that is a function of the amount of free liquidity provider (LP) capital. If the bettor wants to make a bet larger than what is available, he can post a bet of unlimited size, and other bettors can take any of these big bets.[[1]](#footnote-1) For these large bets, the LPs do not get any of the vig because they take no risk from these big bets (the oracle gets its regular fee). [[2]](#footnote-2)

LPs earn a positive *expected* return for the risk they take, in that there may be periods where bettors make net profits implying LP losses. The ratio of LP capital relative to the amount of betting determines the return on equity, allowing the amount of capital to equilibrate this market (if the return is too low, capital will leave, raising the expected LP return). Bets are automatically cross-margined so that the capital required is minimized. For example, 10 AVAX collateralizes a single bet paying out 10 AVAX, and a contest where the winning payout is 510 AVAX if one team wins and 500 AVAX if its opponent wins.[[3]](#footnote-3) The required capital on any single bet is a function of the net payout, not the notional bet amount. LP capital is applied to the entire slate of up to 32 events, and a parameter limits how much of this capital can be applied to any one event.

Oracle-admin tokens are designed for a real purpose, maintaining the integrity of the contract. The token holders only receive their full fee payment if they vote at least twice a week, which requires them to post their tokens on the oracle contract. If a token holder votes less than twice a week, their avax dividends are reduced proportionately (e.g., making one vote per week, which is half of the target, would entitle them to only 50% of their payout). The reduced amount is reallocated to the other token holders in the oracle contract.

The standard 4.5% vig has been stable for decades, reflecting an equilibrium balancing the demands of bettors and bookies more than path-dependent custom. The blockchain's relatively easy access makes an intelligent contract the preferred choice for many bettors even when offering identical odds to the major casinos. So, the focus should not be on significantly reducing this fee, which is essential for incenting our needed LPs and oracle, who split the fees evenly. The standard Vegas odds advertised online on major fights and football games are stable and efficient, so simply using these odds is also efficient.

The relative stability of odds, their historical accuracy, and the vig make the odds amalgamation simpler than for generating probabilities on binary options (e.g., will the price of ETH be above $2000 on 1/1/2024) or the price of ETH in USDC. Consider that your average daily stock price volatility of 2.5% is 16 times greater than the average bid-ask spread of 0.15%. A market maker who adjusted their bid-ask spread daily would be exposed as a 'money pump' by arbitrageurs, in that if the price moves up 2.5%, the market maker will almost certainly have sold on the way up, generating real-time losses.

In contrast, the implicit spread on money line bets is 2.5% in terms of a win probability. One needs a 2.5% edge in predicting which team wins to beat the house. The daily volatility of these odds is less than half of that, implying the book would make money even if it had day-old odds and the new odds were actually moving in the right direction. This would be like a stock with an annualized volatility of 1% given a bid-ask spread of 0.15%, which is more like a stablecoin than a stock price, making it easier to monitor.[[4]](#endnote-1) In a worst-case scenario where posted odds deviate significantly from market odds, an event's new bets can be paused until the following odds update, preventing new bets on a contest until updated odds are posted. Pausing bets requires a minimum amount of oracle tokens and can be pushed immediately; it does not expose the LPs to risk.

Sports odd stability eliminates the adverse selection problem in high-latency centralized markets, which allows for a novel price-setting mechanism: post the widely available standard odds for a slate of upcoming contests. A singular oracle token holder submission grabbed *in toto* from a large sports book will be sufficiently close to the optimal odds to prevent bettors from arbitraging the LPs. A single human can easily find web pages that concisely present the odds or results of high-profile, straight-up bets on the two sports presented on SnowBet. There is no need for price/odds discovery on high-profile sporting events.

Football and MMA are almost exclusively weekend events. A focused set of weekly win/lose events makes incentivizing the oracle easier. In contrast, if we targeted a standard centralized sportsbook, it would cover many diverse events at all times on most days of the week. Only a subset of the oracle token holders could evaluate these data, creating edge cases where a minority equity stake is less than a potential cheat payout.

Augur is an example of a betting contract that was too general. The protocol allowed users to bet on an almost unlimited set of events; thus, it was a 'prediction market' instead of a betting market. Applying vending machine logic to one of the world's oldest professions seemed straightforward, enabling delusions that pushed Augur's token value to over $1B. However, even with protocol fees at zero to promote growth, the indirect costs from high spreads and month-long payout delays made it useless. Augur is inactive now, but when it was not an obvious failure, the small number of bets offered included many created by hackers promoting deliberately ambiguous wagers. A dapp designed for everything is useful for nothing.

Developers focus on generalizable protocols for two reasons. First, it enables delusions of grandeur as equity token buyers imagine the next Amazon on the blockchain. Secondly, they monetize their investment by incorporating, which creates a legal attack surface. The more generalizable the protocol is, the more difficult it is for regulators to prosecute these organizations. Neither of these is relevant to me, the creator of this contract. I will neither control nor profit from this contract, so I am not concerned with legal prosecution or pumping the oracle token. Bettors, oracle voters and LPs are responsible for minding their local regulators, and the global popularity of sports betting implies many people can use it.

# Oracle's IC driver

Incentive compatibility is vital to low-cost enforcement of contracts, and historically this mechanism centered on reputation, not contract law administered by the state.[[5]](#footnote-4) The blockchain's transparency, immutability, and pseudonymity make reputation much easier to monitor. When agents have incentives aligned with their counterparties, we minimize indirect costs (delay and spread), making it more attractive for bettors. In SnowBet, bettors and liquidity providers cannot cheat without the oracle, so the only concern is ensuring honest reporting of odds and results is always the oracle collective's value-maximizing act.

Creating a game where honesty is an oracle/admin's best strategy is straightforward; the keys are simplicity and repeated game, which leads to easy monitoring and a strong incentive towards punishing cheaters. Adding superfluous parties, tokens, and scope increases cost, complexity, and delay. By putting players into a repeated game, a previously dominant strategy of defecting becomes dominated by cooperating because the one-time gain is offset by many future periods where payoffs are lower to the defector. Incentive compatibility is critical to low-cost enforcement of contracts, and historically this centered on reputation, not contract law administered by the state.[[6]](#endnote-2)

Consider the following cost-benefit analysis for SnowBet's oracle. A conservative equity price/earnings (P/E) ratio is 10. Assume a betting contract has 100 AVAX bets on its books, both long and short. As the oracle's fee is about half of the vig, this would average about 2.5 AVAX in weekly revenue. Given 50 settlement events over the year, this annualizes to 125 AVAX. Given a 10 P/E, this values the oracle collective at 1,250 AVAX. The maximum potential cheating revenue in this example is 100 AVAX, requiring the hacker to make all the book's net exposure on his pre-ordained picks, so the LPs have net exposure to the wrong side of every bet.

Such a scam would be conspicuous in the readable event logs, and no rational person would use this contract again, making the value of the oracle token zero. A voting majority's oracle token has a present value of 625 AVAX. Honest reporting is the clear dominant strategy in this improbable worst-case scenario, in that 625 >> 100.[[7]](#footnote-5)

The oracle voters have, literally, all day to evaluate a data submission that can be evaluated in a couple of minutes. A majority 'no' vote among votes cast penalizes the proposer of the data, while a successful submission gets a small reward.[[8]](#footnote-6) The focus and pace of oracle submissions remove any plausible deniability for the oracle cheat action in any single event each week. The website generates event log data in readable form, so one does not need specialized knowledge of hash functions, just access to the sporteth.co website (these are available for customization via GitHub).

While it is simple enough to incent the oracle properly, this only protects the contract against insiders. In contrast, decentralization defends this contract against outsiders. Powerful institutions have always used centralized power to prevent competition, often using disingenuous rationales emphasizing safety. Such an attack needs a choke point, prevented if a collective of pseudonymous accounts worldwide administers the oracle. If the oracle is profitable, an effectively infinite number of people will replace oracle token holders captured by outside attackers. Oracle decentralization defends this contract against outsiders. Initially, the oracle will be relatively centralized. Still, token rewards for early LPs and, potentially, trading by initial oracle token holders will make the oracle decentralized when any outsider develops the will and means to attack an oracle token holder.

1. Bet size must be greater than what is available for instant betting. adjustment: For large bets, the LP’s do not get any of the vig because they take no risk from these big bets. The oracle gets its regular fee. [↑](#footnote-ref-1)
2. Definitions are somewhat arbitrary, but the traditional **vig** is calculated as ‘1 – p\*q/(p+q)’, where p and q are the decimal odds of a team and its opponent. Eg, standard even moneyline odd, -110, have dec odds of 1.909, generating a vig of 4.55%. Alternatively, if 2 ×110 is paid into the book, and 210 paid out to one winner, the net book take is 10/220, which is 4.55%. [↑](#footnote-ref-2)
3. A 5-1 contest with zero LP risk would have 5 eth bet on one team for every 1 eth on the other. [↑](#footnote-ref-3)
4. Closing line odds are actually worse for bettors than the opening line, though not significantly. Regardless, the risk of arbitrage arises whenever the odds on both sides winning implies a probability of less than 1.0, which allows the bettor to make a certain profit regardless of who wins. If the odds were offered by the same book, and that book allowed margin accounting, this would create a money pump. In practice, the opportunity comes from the odds generated by two separate books, which prevents cross margining these bets. Given there is a limit to any one event, and the opening and closing line odds are statistically equivalent, the LPs would make money even if such an odds discrepancy arose. [↑](#endnote-ref-1)
5. E.g., prior to commercial civil law there were courts along trade routes throughout Medieval Europe that enforced commercial laws (the *Lex mercatoria*), and its judgments were accepted not out of any legal authority granted by a state's monopoly on violence, but rather refusal would ruin one's business reputation and thus future revenue. [↑](#footnote-ref-4)
6. In iterated prisoner's dilemma games, the optimal strategy is not to play the Nash strategy of the stage game, but to cooperate and play a socially optimum strategy. An essential part of a strategy in a repeated game is that uncooperative play will reduce the payoff to both players in future periods. A player may choose to act selfishly to increase their own reward rather than play the socially optimum strategy, but if it is known that the other player is following a trigger strategy, then the player expects to receive reduced payoffs in the future if they deviate at this stage. An effective trigger strategy ensures that cooperating has more utility to the player than acting selfishly now and facing the other player’s punishment in the future. This is reciprocal altruism: I play nice because I then expect you to play nice in the future. [↑](#endnote-ref-2)
7. 625 = 50.001% of 1250 [↑](#footnote-ref-5)
8. The reward is done so that, statistically, the submitter should make just enough to cover the costs of the occasional inadvertent (e.g., ‘fat-finger’) errors that may engender a data submission rejection. Otherwise, statistically, the data proposer would have only downside for his work. Nonetheless, we do not want to make proposing data too attractive because that would imply the proposer would eventually acquire a strong majority of the tokens. [↑](#footnote-ref-6)