**AvaxSportsBook**

Decentralized Sports Betting

Draft

Eric Falkenstein

9/4/23

**Abstract.** AvaxSportsBook is a blockchain smart contract for straight-up betting on weekend sporting events. The unique stability of sports odds relative to the spread or ‘vig’ makes it a perfect application of a digital vending machine. Users can bet or invest in the house book, which provides liquidity for residual imbalances. Cross-margining allows a finite amount of liquidity to support an unlimited amount of bets. The standard 4.5% vig is applied to each contest and split evenly between the liquidity providers and its unique oracle, which provides the weekly slate of events, odds, and outcomes. The contract is completely on the blockchain administered by pseudonymous agents; it is immutable, permissionless and decentralized, providing a convenient way for sports bettors to bet on prominent events where the odds are relatively fixed early in the week.

# Introduction

Sports betting is ideally suited for a completely on-chain smart contract. The peculiar nature of sports odds—their stability and implicit bid-ask spread—avoids the adverse selection problem in standard asset swapping markets with stale quotes.[[1]](#footnote-2) Bettors do not need better odds so much as easy access to ubiquitous conventional odds. If standard odds and event outcomes are recorded on a blockchain smart contract, it is straightforward to apply escrow accounting logic where bets are cross margined for the house, permissionless and secure.

The only agent who can cheat is the oracle. Given accurate odds and results, the LPs are bettor actions cannot affect these data, as the contract’s internal accounting applies that information to the LPs and bettors. data and here the key is creating an incentive compatible contract. The first key is simplicity. By restricting the dapp’s focus we minimize the state space of user actions, contract data, and the interpretation of these data. With at most one data submission a day to evaluate and given 12 hours from the time of submission before a vote can be tallied, oracle token holders will not be surprised or overwhelmed by the data they are responsible for evaluating. A cheat would be obvious in this contract, and any users seeing such a cheat would rationally avoid such a contract, making the present value of the oracle token zero (see Appendix for an outline of cheat scenarios). This is a ‘grim trigger strategy’ equilibrium, where players initially cooperate but punishes the opponent if a defection (i.e., the trigger) is observed.

The second key to making the contract incentive compatible is the oracle’s focus on voting and scale. Token holders only earn dividends if they vote on data submissions.[[2]](#footnote-3) For example, if a token holder voted on 50% of the data proposals, she would receive half of her potential revenue. The cost of a meaningful data evaluation are relatively fixed, however, comprising mainly time and attention. For a small token holder the rational strategy would be to automate a vote to ensure 100% of her potential revenue, but this willful ignorance creates an attack surface. To minimize this tendency, all token voters need at least 10% of the lifetime supply to deposit and vote on the oracle contract. This creates an incentive for smaller token holders to create or join a ‘vault,’ where the vault administrator can charge a palatable fee for his services because he amortizes his time and effort costs across many token holders.

A permissionless vault makes it impossible for its depositors to know with certainty about any conspiracy the vault administrator might contemplate. A rational cheating administrator would not apprise them, as it would only dilute their payout, and provide damning evidence for legal and extra-legal prosecution. A token depositor would want their admin to be honest to maximize their token value. The equilibrium solution would be for the vault administrator to charge a fee that gives the admin a sufficient incentive to not partake in a cheating conspiracy. The more the oracle can minimize their costs, the cheaper they can offer these services.

The SDK provides tools that make being an oracle very cheap, so the real cost for vault depositors is for aligning incentives, not covering a costly expenses.

balances the token holder incentive to have an honest administrator, with their incentive to maximize their net revenue.

token holders and vault administrator would have many incentive proble

US citizens and residents cannot advertise, administer, or provide liquidity to a permissionless sportsbook. However, crypto is worldwide, and the US represents only 4% of the world’s population. Statistically, there are many millions who can fulfill these roles legally. With cross-margining and a fixed spread, the book does not need a large amount of capital that only a developed country like America can provide.

Retail sports bettors have never been prosecuted for using unsanctioned betting sites, but banks and credit card companies often block users whose funds are tracked to betting sites. If an American bets a small amount of money, however, there are many methods to avoid tracing (eg, if you buy a couple hundred dollars worth of online goods or services a year using crypto, your winnings would never need to translate into fiat).

Sports betting is a competitive market, so the standard 4.5% vig reflects an equilibrium balancing the demands of bettors and bookies as opposed to monopoly power. By taking the standard vig as a given, we remove naive schemes that in theory are less costly but in practice create failed markets (e.g., Augur). The hassle-free ability to bet or be the house should be sufficient to make it a dominant alternative for many sports bettors.

The relative stability of sporting event odds compared to the vig allows for a high-latency oracle that would never work for swapping tokens. Given the daily stock index volatility of 1%, it would be like if the bid-ask spread on the S&P500 ETF was 5%. Adverse selection would lower profits as opposed to arbitraging the market makers. In practice, the closing line and opening lines for NFL betting are statistically identical, implying it is just as likely the closing line contains bettor fads as opposed to better information.

There are three types of *AvaxSportsBook* (hereafter, **ASB**) contract users: bettors, liquidity providers, and the oracle collective. The total vig is split evenly between the oracle and the LPs.[[3]](#footnote-4) Bettors can take either side of any regular bet offered, subject to a size constraint based on the amount of free liquidity provider (LP) capital. An oracle token holder submits a slate of matches and start times on Wednesday or Thursday. The odds are posted Friday or Saturday morning, and then bettors can bet up to the game time, which is loaded with the schedule in the contract. The weekend’s outcomes are sent to the contract the following Monday or Tuesday. Bettors can redeem their bets immediately after settlement, while LPs cannot withdraw or fund while betting is active (from when odds are posted and settlement).

LP exposures are automatically cross margined to minimize required capital. For example, 10 AVAX collateralizes a single bet paying out 10 AVAX, and a contest where the winning payout is 510 AVAX if a team wins and 500 AVAX if its opponent wins.[[4]](#footnote-5) LP capital of *X* supports a book of infinite size when bets of size *X* are made sequentially. The required LP capital on any single event is a function of the maximum *net* payout, which is the payoff on a team *minus* the amount bet on its opponent. An adjustable parameter limits how much of this capital can be applied to any one event so that LP exposure to any single event is limited. For example, if LP capital is 100 AVAX, a parameter of 10 restricts the net LP liability for any one contest to 10 avax.

# Oracle Incentive Compatibility

Creating a game where honesty is an oracle's best strategy is straightforward; the keys are simplicity and a repeated game, which leads to easy monitoring and credible punishment anticipation for a fraudulent oracle data submission. Additional parties, tokens, or scope increases cost, complexity, and delay. Defecting/defaulting implies the loss of the benefit of future interactions, the present value of which acts like over-collateralization on a loan. As long as the potential cheat gain is less than the present value of future revenue foregone, it will be in the oracle’s self-interest to provide accurate data. Incentive compatibility is critical to low-cost enforcement of contracts, and historically this centered on reputation, not contract law administered by the state.

Consider the following cost-benefit analysis for ASB's oracle. Assume a betting contract has 100 in net exposure, which we will conservatively assume is the book’s gross betting exposure (no offsetting bets that generate reward but no risk to the LPs). 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 conservative 10 price/earnings ratio, this values the oracle collective at 1,250 AVAX. The maximum potential cheating revenue in this example is 100 AVAX, so the LPs have net and gross exposure to the wrong side of every bet made by the cheating oracle’s sock-puppet bettor. A voting majority's oracle tokens have a present value of 625 AVAX in the above example, significantly more than the 100 AVAX in a cheat.[[5]](#footnote-6)

Such a scam would be conspicuous in the readable, weekly event logs showing what games, odds ard outcomes were reported. Unlike oracles that service many contracts, or there is no plausible deniability by the ASB’s oracle collective. Each week they are tasked with producing a singular slate of data, where a single bad data point—one beyond the standard variance in odds across sportsbooks, a late start time, an incorrect outcome—taints the entire slate. The oracle collective is ‘all in’ on this one betting contract that cannot be upgraded or extended.[[6]](#footnote-7)

While it is simple enough to incent the oracle properly, this only protects the contract against insiders, existing token holders. 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 and provides liquidity. There are no governance issues related to upgrades or extensions, no need for an administrator off the blockchain.

# Contract Outline

At the beginning of the week the oracle sends both the outcomes for last weekend’s events and the schedule of next week’s events: who vs. whom and start times. Odds are sent the Thursday or Friday night, allowing betting to start Friday or Saturday morning. The contract then repeats the process. There are only three data submissions a week if no submission is rejected (which would require a subsequent replacement).

LP capital backstops residual imbalances in the book. The LP's total capital is available equally to all contests that week, but there is a limiting mechanism on how much AVAX can be allocated to any single contest. This diversifies the LP’s risk, reducing the chance that a single contest outcome could extinguish LP capital. The betting contract contains all the methods for bettors and LPs: betting and redemption for bettors, investing, and withdrawal for LPs.

A singular oracle token holder, with at least 10% of the oracle tokens outstanding, proposes the relevant data: the upcoming schedule (who plays whom, when), odds, results, and some technical parameters (e.g., paused matches, the diversification parameter). Each submission is then subject to an evaluation period subject to a majority vote. A successful data submission is sent to the betting contract after a voting period of 11 hours, giving the oracle collective sufficient time to veto a fraudulent or incompetent submission.

odds, results, etc

avax fees

Oracle Contract

Betting Contract

avax

avax

data, votes

avax

tokens

Token Holders

LPs

Bettors

Posting data can only occur in the three-hour-minute window where the hour is between midnight and 3:00 AM GMT, which is 8-11 PM New York time in the summer and 7-10 PM in the winter. Voting takes place between the posting and processing the vote 11 hours later. This is to make sure all the oracle voters can anticipate when they have to evaluate the data before it is sent. to The processing function can be executed by anyone, as 11 hours is more than enough time for a thorough evalution by the oracle.

If a settlement or initial post are rejected, then a settlement or initial post, must be posted again. This effectively delays the contract by a day. Odds updates cannot occur Saturday or Sunday, and settlement can only be posted the following Monday, so the oracle token holders have no duties until Monday’s settlement.

Each week, aka ‘epoch,’ the MMA, boxing and US football games that weekend are sent to the oracle contract. The data are sent to the betting contract if most oracle token holders vote yes. When the betting contract has data for the next weekend, bettors can bet up to the time of the various games that weekend, as each game is given a starting time that must be between the next Friday 5PM ET and Monday 9PM ET.

After the weekend, the outcomes are sent to the betting contract bettors, which settles that week’s bets. At that point LPs can withdraw earlier deposits, and bettors can redeem their bets. The contract has no ability to seize neglected funds, so as long as the blockchain exists, users will be able to safely let unredeemed money sit in the contract. LPs cannot withdraw or deposit from when odds are posted (~Friday) through settlement (~Wednesday), as otherwise, LPs could game the contract by anticipating unusual losses or winnings as they acrue over the weekend’s events.

## Betting Capacity and Cross Margining

The contract’s logic makes sure all bets are fully collateralized. As bettors take the opposite side of a contest, it is a waste of capital to require the LPs to collateralize both sides independently. The solution involves netting exposure. This eliminates insolvency risk in the contract.

In betting on a limited number of binary outcomes, the worst-case scenario for the house is assumed (i.e., each LP net position loses). The contract will always be fully collateralized on all bets, as this is enforced at the time of each bet. Adjusting the net required LP margin involves 'linear programming' where the LP's net game exposure is the maximum liability of either team winning. The margin adjustment is applied at the time of a bet, so there must be sufficient free LP collateral to accommodate a bet adding to LP exposure.

**Cross margining example:** Assume two teams are given even odds so that for either team, a 1 AVAX bet pays the winner 2 AVAX. If there is 10 AVAX on team A, and 10 AVAX on its opponent, team B, it would be a 'flat' book in that the LPs have no exposure to this game; payoffs are funded by betting counterparties, not the LPs. A new bet that pushes the book to have a net exposure would necessitate LP funds as collateral, so a bet of 2 AVAX on team A would add 2 AVAX to the LP's locked margin. Given a total of 12 on team A, and 10 on team B, a bet of 2 AVAX on team B would move 2 AVAX *out* of the locked margin because the resulting book would be flat again.

A contract parameter prevents an overconcentration of LP capital on one event. For example, 123 AVAX in total LP capital and a concentration parameter of 10 implies a maximum of 12.3 AVAX LP exposure for any event. Thus, if the current LP liability for team 0 winning was 10.0 AVAX, it could only accommodate an additional payout of up to 2.3 AVAX on team 0. In contrast, a bet on team 1 could accommodate a bet payoff of 22.3 AVAX. This concentration parameter can be adjusted over time by large oracle holders.

## Betting and Redeeming

All ties and 'no contest' games give bettors their initial bet back. Winners receive their bet amount plus the payoff implied by their bet odds. When the weekend's results are sent to the betting contract, all bets are settled, and the oracle payment is sent to the oracle contract. Settlement creates a mapping from a unique epoch-match-team, which determines which bets credit a user’s balance when looping through a bettors bets. Settlements should happen Tuesday evening, though if there are no Monday night events it could happen Monday, and if a data submission is rejected on a Tuesday, it would be resubmitted the next day.

Bettors redeem all of their outstanding bets in batch. The redeem function loops through up to 16 bets in a user’s account, and sends the winnings to the bettor’s account. Redemption can only be processed if there are no active bets in the account, so bettors must wait until the next settlement to redeem if they have any active bets. If an account has 16 unredeemed bets, it must redeem them before it can place another bet.

All bets are fully collateralized, and so are the accruals for the oracle. Unclaimed bets or tokens can reside in the contract and retain their value as long as the AVAX C-Chain exists, as there is no mechanism to sweep neglected funds to LPs, bettors, or token holders.

## Liquidity Providers (LPs)

Sportsbook odds are efficient, in that statistically the house makes a profit, but week-to-week the book can lose money due to small sample variation. The LP’s main risk, however, is the black swan risk via oracle fraud, something any good hacker would strenuously avoid until their big cheat. A hack would almost surely use a bettor-oracle conspiracy to maximize their cheat payoff, as the LP exposure is passive. Thus, LPs have an incentive to become oracle token holders to align their incentives, as the most likely cheat would involve a conspiracy between the oracle and a bettor, defrauding the passive LPs. The token rewards allocation to the initial LPs encourages an LP/oracle overlap.

To become an LP, one sends AVAX to the betting contract, which then credits the LP with shares representing their pro-rata ownership of the LP pool. For example, if there is 10 AVAX in the LP book, and 10 shares, adding 1 AVAX would give a new LP a 1/11th share of the new pool of 11 AVAX, keeping the AVAX/share the same. This LP claim exists only within the betting contract and is tied to the initial LP AVAX account address. It is not transferable to other AVAX addresses, and so is not represented by a token. LP shares are like a stock at its net asset value; tokens are like a stocks market value.

The size of the LP capital should adjust to the volume and degree of cross-margined betting, the more of which increases the LP’s expected return. For example, a book with 10 bet on team A, and zero on its opponent, will generate an expected return for the LP, statistically, in that over time the vig in the odds spread implies bettors need a 2.2% edge in predicting winners to beat the house, which is difficult (as proven by the nice casinos). If a book had 110 bet on team A and 100 on its opponent, the required LP capital would be the same, but here the LP would make a certain return on the offsetting bets. That is, the gross betting exposure in the latter case is 21 times large than the net exposure. The greater the ratio of gross to net exposure, the greater the return. The expected ratio will be revealed over time, and will greatly affect the return for a given level of LP capital.

LPs can only withdraw during the inactive period when bets are not active. Active betting can only occur between when odds are posted and settlement. A bet backed by LP margin locks this margin until settlement, or bettors take the other side, freeing the LP capital. Since there is at least a 48-hour window each week after settlement before new bets are offered, LPs are sure to be able to withdraw at least once each week.

LPs must also have their AVAX in the contract for at least one settlement after depositing. This prevents games where users might inflate LP capital to scare away ‘real’ LPs who are not playing such games.

As LP capital is used to collateralize residual bet exposure, the ratio of the net to gross betting volume will be key in determining the return on LP capital. The amount of LP capital relative to the betting volume will equilibrate the market. If the return is too low, capital will leave, raising the expected LP returns; if the return is too high, capital will enter. It will be an empirical issue what the correct amonut of LP capital is for an expected gross betting amount. Not only is the net/gross betting data unknown, the max(net) to gross ratio is important because limited LP capital will prevent bets that may never come back.

# Avalanche

I used to be an Ethereum maxi, but I became convinced that Avalanche’s blockchain is vastly more efficient. For example, the Snowball Proof-of-Stake (PoS) consensus mechanism scales with log of validators O(ln(n)), because validators survey a fixed number of other validators as opposed to every validator (scales at O(n2)). It’s understandible that second generation consensus mechanisms—outside of PoS—would be a significant improvement. Ethereum is stuck with their relatively inefficient consensus mechanism because their L2s are now too powerful, which reduces the incentive for making the main chain more efficient, as this would make the L2s unnecessary. The bottom line is that Avalanche is as cheap and fast as an Ethereum Layer 2 blockchain, but without the centralization and lower bridging risk.

I call it AvaxSportsBook to remind people which chain they need to put crypto on. Avalanche uses the same Ethereum Virtual Machine as Ethereum, so it took no extra work to port my Solidity and Web3 files onto Avalanche’s C-chain. Avalanche has the same address structure as Ethereum, so users can use their MetaMask wallets to store and transact with Avax. ASB also can use Avax’s Core Wallet, has a built-in bridging mechanism that makes bridging assets from Ethereum or Bitcoin safer and easier than Ethereum’s L2s.

# Oracle Incentives

## Oracle Token Owners

I created this dapp but I have no control or financial interest; I cannot administer let alone disable the contracts.[[7]](#footnote-8) I am not a lawyer, but I do not think an American citizen living in the US can administer this contract as an LP or token holder. However, there are a billion people in southeast Asia, south America, and the West Indies, and surely that’s a big enough pool for enough people to service the contract as LPs and oracle. Thus, there is no ASB foundation, there was no ICO, and there are no governance issues related to extensions and upgrades. The fact that the only way for me to publish this contract is to give it away is likely a major reason why no one else has created such a contract.

While .

Initially there will be little visibility so it is essential to have people prudently administering the contract, and people need economic incentives. I gifted the tokens to three people I have no control over, and chose them in part because I do not know them well, as that would make it easier for them to be identified. In that vein, my contact with them going forward will be exclusively through public writings like this. I tried to make their job as easy as possible by giving them tools for their role. The excel spreadsheet in the GitHub repo provides a simple tool for taking the data in the proper form acceptable to the contract, and there are python programs for token depositors to send the various required transactions to the oracle contract. These are explained in videos available on the website.

They each received a 13.3% of the immutable supply of tokens, as 10% are required for submitting data (smaller token holding collectives can and should vote on those submissions, via vaults). I chose three because one of them could become incapacitated. Also, in the improbable scenario where one irrationally decided to cheat the contract, it is highly improbable that the other two token holders would allow this, as they do not know each other, and it would destroy a potentially valuable gift.

The other 60% of the maximum oracle token supply, 600k, was sent to the betting contract as rewards for initial LPs. This encourages an LP/oracle overlap, which helps align incentives between the oracle and the LPs. Each week 30k tokens are available for reward distribution, and each week LPs can send a function to receive their pro-rata share (eg, an LP with 10% of the shares would receive 3k tokens). Rewards do not start until epoch 5, to avoid the initial oracle token holders accumulating most of the tokens while the contract has little visibility. The incentive program will last until all the tokens are distributed. There is no ability to mint more than the initial one million tokens minted.

## Oracle Vaults

Small token holders rarely participate in governance votes. This is rational because there is a minimum fixed cost to evaluating data, say 20 minutes of time. Assuming 2 votes a week, the implicit hourly wage for this service would be below the minimum wage for someone with less than $1000 worth of tokens. This complacency creates an attack surface for hackers.

To mitigate the standard public choice voter information problem, the minimum deposit in the oracle contract is 50 million tokens, 5% of the total supply. Token depositors must vote to receive fee income, and to vote they need to be deposited in the oracle contract. This creates an incentive for small token holders to pool their tokens and designate a voter who would have an incentive to monitor and discipline oracle data submissions.[[8]](#footnote-9) There will be mutual gains of trade for both sides: the small oracle token holders and the administrators of vaults. It should be like representative versus direct democracy, a consequence of Robert Michel’s *Iron Law of Oligarchy*.[[9]](#footnote-10)

The vaults should not be too big, as this would present an attack surface for censors and hackers. Thus each token account within the oracle contract is capped at 150 thousand tokens (15.0% of the total supply). The vaults should be independent, in that this would make the contract more robust, making the present value of their tokens greater.[[10]](#footnote-11)

## Sending and Validating Oracle Data

The oracle token holders get paid for performing a specific purpose, enforcing honesty. I provide tools for creating the data in the format required by the contract, and also sending transactions to the contract via Python. Once created, one can create simple cronjobs that then post data, or votes, conditionally. While one should always use their human eyes to ultimately sign-off on a datasubmission, this should not take more than 15-minutes on each data submission. In an ideal world, one should not have to pay someone to simply *not* be evil, but that is not the world we live in; crypto has shown that anything pseudonymous based on trust will be exploiting by amoral hackers to the fullest extent. Thus we make sure honesty is the oracle’s profit maximizing action at all times. They can then spend that money on whatever they like, wholesome or debased.

A token holder needs at least 10% of the outstanding tokens to submit data to the oracle contract. While submitting data takes some effort, the cost is relatively low given the ease at which relevant data is available and the limited scope and frequency of data submissions.

Tokens must be deposited within the Oracle contract to submit or vote on submissions. This prevents double-voting and forces the token holders to attend to the contract they should be monitoring. The tokens are meant for providing an essential service, not speculation, and generates dividends directly proportional to the bet volume.

The data submission process will look like this:

|  |  |
| --- | --- |
| sent 0:00-3:00 GMT/Processed 14:00 GMT | |
|  | Data |
| Tuesday | outcomes/new schedule |
| Wednesday |  |
| Thursday |  |
| Friday | odds |
| Saturday | Nothing |
| Sunday | Nothing |
| Monday |  |
| Tues | outcomes/new schedule |

In this example the outcomes & new schedule are sent on Tuesday. This is because currently there are two Monday Night NFL games, and it doesn’t cost much to bump the settlement a day. If there were no NFL, as in most of the year, it would be best to send this data Monday.

Prior outcomes and the upcoming schedule are sent in one batch. Odds are sent in a subsequent batch a day or two later. These submissions can only occur in alternating succession. The other requirement is that games must start between the next Friday and next Tuesday. As most betting occurs on game day, and a fresher odds data point helps the LPs, it is optimal to send the odds on Thursday or Friday, closer to the end of the week. As a practical matter this implies weekly submissions.

While nothing can be sent on the weekend, that leaves 5 days to make two data submissions. This should make oracle voters less hesitant to reject a data submission that contains a mistake. For example, if there were only two days to send those two sets of data, one might think a bad reported outcome was accidental and didn’t cause that much damage. This protocol can handle two rejections a week, though hopefully that will be very improbable.

Voters should remember that the data submitter can resubmit if he catches an error within the first couple of hours. Thus, they should refrain from voting until after the submission period ends, as a resubmission resets the voting, but it also

\*optional

Data can only be submitted between the hours of 0:00 and 3:00 AM GMT, and these data can then be processed once the GMT hour is after 14:00 GMT. This gives oracle token holders at least 11 hours to evaluate the data. Anyone can execute the function that processes the vote, so I suspect it occur quickly once possible, around 7AM ET. A yes vote sends the data to the betting contract, while a no vote delays the contract for at least one day.[[11]](#footnote-12) There is no slashing condition because the present value of oracle revenue should sufficice; further, it removes the potential for thin-skinned oracle members spiting one another.

No data can be submitted on Saturday or Sunday. If there are data submission failures, the data submission is either pushed back a day, or if an odds update, omitted. Rejections should be rare, but they should also be expected due to unintentional mistakes. Thus, if the initial data sent in contain a mistake, seeing this on the blockchain can make these fat-finger errors more obvious. The datasender can send a corrective data submission to replace their earlier one until 3:00 AM GMT. Voters vote on the last dataset submitted.

## How Oracle Token Holders Claim Oracle's Revenue

The primary way the oracle acrues fee revenue is at settlement. Applying a 5% fee to the winnings generates an approximate 2.5% take, which is about half of the contract’s fee revenue. For example, if there is one bet of 1 avax with gross decimal odds of 3.00, the bettor gets back his 1 avax, and then 95% of the 2 avax generated by his win. The 5% of 2 avax is sent to the oracle. Note this implies the oracle token depositors have no economic risk, unlike the LPs, in that they cannot lose money due to lucky gamblers (in fact, the oracle holders do better when they win).

Another way the oracle acrues revenue is when negligent token depositors claim revenue, as if they do not vote each time their accrued revenue is slashed by the percentage of votes they missed, and the lost amount is reallocated to the other token holders. The unearned AVAX is then immediately reallocated to the other token holders by treating it like a settlement dividend. For example, if a token deposit account spanned three settlements and eight data submissions, and they voted four times, they would receive one-half of their payment. When this account tries to claim their oracle revenue, the foresaken half would be added back to the pool, going to the other token holders, incenting the token holders to actively monitor the the data submitted.

# Conclusion

Most sports betting sites touting their crypto functionality are just conventional online betting sites that accept crypto, if not outright scams. A truly blockchain-based betting dapp upholds Satoshi's vision of *pseudonymity*, *confiscation-proofness*, and *permissionless access*, which requires it to have no off-chain presence. I hope that a focused dapp with proper incentives can provide an example of what blockchain smart contracts can do. The purpose of the contract is to facilitate casual sports betting, not create a new token for people to pump, or a new protocol that can potentially replace both Amazon and Goldman Sachs. ASB’s token administrators have a straightforward but essential job that generates instant revenue.

One should expect players to always act in their selfish best interest. A sustainable contract creates a repeated game where honesty is always the dominant strategy for every player. The trust one puts into the ASB Oracle is fundamentally the same as why investors trust miners: the rational self-interested assessment that honesty dominates dishonesty for a hypothetical individual. Paradoxically, adding multiple redundant adjudicators or correction protocols gives the illusion of greater safety, while creating a state space for hacks grows exponentially in the number of players and actions they can take. ASB’s simplicity enables an incentive-compatible contract, allowing bettors to easily access conventional odds on big games, and cash out in timely fashion.

ASB is a straightforward application of escrow logic to a common use case. It provides an efficient way to make bets on big games without the hassles, if not prohibitions, presented by online betting services. Sports betting is ubiquitous, but it should be easier. This contract provides a simple way to do that.

# Appendix

**Odds restrictions**

* one odds number

Standard odds are presented as a pair, with a spread so that simultaneous bets on both teams loses money for the bettor and makes money for the house. An obvious attack surface for a smart contract would be for the odds to imply an arbitrage as the offsetting bets would generate a certain profit, enabling the hacker to drain virtually all of the LPs capital at settlement. By using a single number that attack is eliminated. The 4.5% vig creates a competitive two-sided offer, a standard requirement for market makers on centralized exchanges.

The odds for the opponent are calculated via an algorithm. By restricting the odds to apply to the favorite, we can restrict the range of allowable odds, as no favorite has decimal odds greater than 2.000. This makes it easier to exclude bogus odds.

* outcomes only win-lose

Standard centralized sportsbooks cover diverse events on most days of the week, including exotic bets that are are not straightforward to validate. This demands a great amount of attention and competence by the oracle, and increases the probability that a minority of token holders take advantage of inattentive oracle token holders. The weekly reporting also makes the oracle easier to validate historically, in that the event logs refer to who won weekend events, which is easier to verify.

One could use a point spread, but that would not translate to MMA. Football, boxing and MMA will be the primary focus. The matches and odds are well-publicized early in the week. If there were a high profile events other than football and MMA can be accomodated on a case by case basis (for example, a World Cup soccer match).

* No extreme odds

Matches with extreme underdogs (eg, 10-1) are attractive for hackers, as the generate the most revenue for the smallest amount of capital. Initial decimal odds on favorites greater than 7:1 are not accepted. Initial decimal odds for favorites must be greater than 1.150, or less than an 88% probability of a win, or a 7-1 probability of winning. Such matches will simply not be covered. This would eliminate about 5% of NFL games historically, but is common among college football and MMA.

**Oracle submission restrictions**

* weekly settlement.

Games are constrained to start between the next Friday at 19:00 GMT until Tuesday; settlement cannot occur until Monday. Thus it is impossible to generate two settlements within a week. This reduces the vigilance needed to assess the oracle.

* maximum of one daily submission, with 12 hours to evaluate

The oracle processes at most one submission per day, which must be submitted during the first three hours of GMT. This makes it easier for the oracle to keep track of the data it must evaluate. Odds movement within a week is generally within the effective bid-ask spread implied by the standard sportsbook vig applied in ASB, so a Thursday or Friday odds submission should provide sufficient protection against the adverse selection risk created by stale odds.

As no healthy adult sleeps more than 10 hours a day, the 11 hour window between 3:00 and 15:00 GMT ensures token holders will be able to evaluate and vote before the data submission is processed. The objective is to make it feasible for a single person to do this manually without an extreme investment. The basic functions can be automated to a great degree, and python programs for processing and submitting oracle data are provide in the GitHub repo. The crucial issue is time, giving the oracle collective time to soberly evaluate the data on submission and evaluation.

* Ideally, two submissions a week, though it could be 4 if initial submissions are rejected. Submissions are not allowed on Saturday and Sunday.

Oracle token holders cannot adjust odds on weekends, but they can pause betting on a match if an unusual event causes the market odds to move significantly. This allows the oracle token holders to relax on the weekend, in that they will not have to evaluate an unanticipated settlement submission

* Maximimum 32 events

The settlement function loops through the events, and 32 is big enough to capture most weekend events. Gas is a constraint, but this has the added value of making the contract easier to monitor and validate, as obscure contests would be more difficult to assess.

**Simplifications**

* only three contracts

This dapp consists of three solidity contracts: betting, oracle, and token. In contrast, Uniswap’s V3 ‘contract’ contains 31 contracts, which makes it difficult to audit. One can evaluate functions piecemeal, but with tens of interacting files, many upgradeable, it is difficult to span the state space configuration that may make an otherwise innocuous argument a problem. Users must take security on faith. With ASB, one can download the three contracts, and test different different scenarios to find a hacking surface. I provide a dozen hardhat tests as templates to build upon in my GitHub repo.

* contracts not upgradeable

Static contracts remove any need for governance to vote on upgrades. Most importantly, it means there is no group of developers managing, promoting and proposing changes. Such developers would need to be paid, and generally this requires a corporate structure. Such corporations are attack surfaces for censors. This also removes the risk from bugs in upgrades.

* No adjudication process

A protocol for disputing data validated by the oracle generates considerable delay. The oracle incentives are based on the present value of the oracle token, which should be sufficient. Redundant mechanisms lessen the incentive for the oracle token holders to monitor and discipline data submittors.

* Everything in AVAX, no stablecoin

By using native AVAX for all bets we eliminate unnecessary costly swapping into and out of stablecoins. As stablecoins are generally centralized, we eliminate an attack surface as well, as one could imagine Circle, at the behest of some US regulator, preventing the betting contract from receiving or sending USDC. Users will have to bear avax price risk, but this is a minor inconvenience relative to the extra costs created by requiring users to buy a stablecoin.

**Safety mechanisms**

* Pause betting on matches

A match’s odds may become obviously stale. Allowing the oracle to turn such matches off does not expose the contract to malfeasance, it just prevents more bad trades from happening. These can be undone, as well.

* Unintentional error robustness

Oracle submitters can resubmit in the three-hour window they have to submit data. This is aimed at the case where a submission contains an obvious error that the submitter did not notice until it was posted. This still gives the oracle collective 11 hours to evaluate the data.

* As there are only two data submissions required eeach week

, if an initial datasubmission is rejected, the week is not ruined. A replacement can be made the following day, allowing the contract to function that weekend. There is no penatly for rejected submission, as the oracle has the time to make a fully informed decision, and it is irrational for the oracle to deliberately choose to cheat. However, unintentional errors are natural, and often these are not seen until one actually sends the data to the contract. By allowing a data sender to resend if they do so within the next few hours, it does not complicate anything for the other oracle token depositors evaluating this data; by accomodating a data submission rejection, we reduce the cost of disputing a data submission.[[12]](#footnote-13)

**Bookie**

* No bookie withdrawals during active betting

Flash transactions enable efficient arbitrage, but the benefits here are low, and the costs are high. Many hacks have been predicated on flash loan transactions. token holders have to wait one epoch, but LPs have to wait three epochs. The LP restriction is longer because otherwise there would be an opportunity to make a riskless profit depositing just before and after settlement when the book is flat, which would generate a riskless return for the LPs; that tactic would parasitize the good LPs supplying real liquidity.

**Oracle restrictions**

* No token withdrawals during vote

prevents accounts from double voting

* Oracle has minimum and maximum token requirement.

Minimum requirement makes the cost of evaluating or sending data less than the expected loss from a reputation-destroying fraudulent data submission.

* LPs are only paid if they vote

This motivates the oracle token holders to evaluate the data

* LPs are charged a 1% fee if they withdraw after funding prior to settlement.

If LPs could deposit and withdraw quickly without a fee, some LPs might find it profitable to scare away other LPs by depositing large amounts merely to discourage other LPs, who would see low expected returns given a large capital base. Once scared away, the malicious LP would withdraw capital to make the return attractive. This tactic does not help the LP collective.

* Oracle submitters must differ sequentially

This motivates oracle memmbers to create their own data submissions, as they cannot depend on a single oracle member who appears to dominate data submissions.While it could devolve into two oracle accounts posting all of the data, it is a small nudge in the right direction. If a token holder creates a data submission, but finds they did not post in time, they will be prepared to give a good evaluation of the data submitted.

## Odds Translation

To convert moneyline odds into Decimal odds, we have the following.

For positive moneyline odds: (Moneyline odds/100) + 1 = Decimal odds

For negative moneyline odds: (100/Moneyline odds) + 1 = Decimal odds

To translate decimal odds into moneyline odds that are prominent on NFL betting sites, we have the following adjustment mechanism:

If decimal odds are greater than 2.0: 100 × (decimal odds – 1) = Moneyline odds

If decimal odds are less than 2.0: -100/(decimal odds -1) = Moneyline odds

To translate moneyline odds to fractional odds:

For positive moneyline odds: Moneyline odds/100 = Fractional odds

For negative moneyline odds: -100/Moneyline odds = Fractional odds

To convert decimal odds into winning probability.

prob(win) = 1 / Decimal odds

Decimal odds = 1 / prob(win)

The most common odds offered for the NFL are presented in moneyline form as ‑110 for both teams, which would be 1.909 in decimal odds or 10/11 in fractional odds. A flat book on such a wager would receive 220 and payout 210. In this way, the 'house' makes money used to pay for various costs and a profit from the house. The implicit profit ('vig') in this case would be 4.55%, 10/220. The general formula for estimating the vig is given by the following formula, where *p* and *q* are decimal payouts (e.g., 1.909 for a standard even money bet) for opposing teams.



The spreadsheet 'ASB.xlsx' presents a page where people can see how these transformations are applied. Those interested in sending odds to the contract will find it a helpful template.

## Schedule and Start Times in Contract

Each betting period will contain up to 32 events and target a weekend (e.g., Friday night through Sunday night). Each contest is slotted into an array that can be unambiguously linked to its outcome via event logs that expose what events odds were on the contract. The schedule array contains a string with the sport (NFL, MMA, etc.), the two opponents, and the starting time. The initial favorite will be listed first and the underdog second, though the odds can change over the week while the ordering of the contestants cannot.[[13]](#footnote-14)

The start time is important because if it is wrong, bettors will be able to bet on games that have either started or completed. Websites with event start times are tricky because sometimes these are listed as ET (ie, New York City time), sometimes they are automatically converted into one’s regional time zone. It is best to buy an ‘live odds’ API, and these generally provide the start time in UTC. This time is also called GMT, Greenwich Mean Time, which is often presented in ISO8601 date/time format, where the “Z” suffix means Zulu time, which is another word for GMT/UTC.

## Odds in the contract

Odds are available on many betting websites, and arbitrage limits how far these odds can differ. On average, a team's implied probability of winning will change by only 2% over the week, rarely over 5%. All odd postings and updates are recorded in event logs, observable in online queries at sportAVAX.co.

A contest will have a single odds number posted for a contest. These odds are supplied only for the initial favorite using a truncation of preliminary decimal odds. For example, 1.909 would be stored as 909, 2.50 as 1500, etc. This number is then multiplied by 10 to allow some additional informatino packing, specifically whether a match’s betting is paused. Thus, the initial 909 submitted gets transformed into 9090, which is then read by the contract as 9090. If the match is paused by adding the number 1 (eg, 9090 🡪 9091), users cannot bet, applying the requirement that “odds % 10 == 0.”

This number, however, is just relevant to the team in slot 0, the initial favorite. Further, it needs to be adjusted to reflect the oracle fee that would be assessed to the winner payout. Thus, the betting odds for a favorite where the match odds were 9570 would be 9090, via

Net Odds (favorite) = (contractMatchOdds \* 0.95)/10000 + 1

= 9570\*0.95/10000+1=1.909

The gross odds for its opponent are generated within the contract by the following formula:



Then to account for the oracle take, the all-in odds for team 1 would be

Net Bettor Odds (underdog) = (underdogOdds \* 0.95)/10000 + 1

With this method, we can ensure that the set of odds for a contest generates a positive vig, removing a potential attack vector.[[14]](#footnote-15) This formula generates a vig of 2.5% for the LPs via parameter 45 in the above equation, and the 5% take of winnings generates an approximate 2.5% vig for the oracle.

The standard odds presented by most casinos embody the standard vig of 4.5%. For example, -110 on an even-money bet, which is 1.909 in decimal odds. ASB applies the vig to each contest via an algorithm that works well, though it is simply a hack as opposed to something derived from axioms. The approach is to put the LP’s take into the ‘spread’ between the odds offered for the favorite and the underdog, but leave the Oracle’s take out of the spread. The Oracle fee is then taken out of the winnings.

Decimal odds presented must be between 1.999 and 1.125. The cap at 2.000 reflects the fact the odds apply to the favorite, while the 1.125 minimum removes events where the initial odds are greater than 8:1, lopsided contests. Eliminating high payout contests mitigates risk, as such events would invite hacker attention.

The excel spreadsheet is provided that generates the data in the necessary format. The basic algorithm is this

1. Take an initial set of odds
   * Home team: +135
   * Away team: -150
2. rearrange so that the favorite team is first
   1. team[0]: -150, team[1]: +135
3. Translate into win probability
   1. team[0]: 59.8%, team[1]: 42.4%
4. calculate probability spread
   1. spread = 0.598 – 0.424 = 0.174
5. Calculate new favorite, team[0], prob(win)
   1. prob(team[0] win) = 51.1% + spread/2
   2. prob(team[0] win) = 51.1% + 8.7% = 59.8%
6. Translate prob(team[0] win) into decimal odds.
   1. decOdds(team[0]) = 1 / 0.598 = 1.6716
7. Translate decimal into the payoff of the bet. This number will represent the match odds in the contract.
   1. contractOdds = 1000 \* (decOdds – 1)
   2. contractOdds = 671
8. Translate into netDecimalOdds(team[0]) presented to bettor
   1. 0.95\*671/1000 + 1 = 1.637
   2. The oracle fee reduces the actual decimal odds returns presented within the contract
9. Translate into team[1] payoff
   1. contractOdds(team[1])= 1e6 / (671 + 45) - 45 = 1359
   2. net decOdds (team[1]) = 0.95\*1359/1000 + 1 = 2.291

In this example, the vig is 4.5%: 1.637 \* 2.291 / (2.291 + 1.637). The above algorithm generates a vig near 4.5% across the range of odds covered in this contract.

The website avaxsportsbook.com displays the decimal odds users receive if they win. For example, a user seeing odds of 1.900 will receive back 1.900 times their bet amount.

## Redeeming a Bet

Bets are stored in a mapping within a better’s struct, and after 10 bets, no further bets can be made until they are redeemed. Redemptions can only occur when a bettor has no active bets, so a bettor should redeem his bets after settlement if he anticipates a problem. All bets in the array are settled for the bettor. Each bet is represented by the unique combination of epoch, match, and pick. At settlement, a bets hash refers to a struct containing this information, and a mapping generated at settlement allows redemption. Users to redeem bets by clicking a single button (it is one transaction).

## LP Revenue

LPs own a pro-rata portion of the contract's revenue based on their percentage of LP capital before that week's events. Statistically, the LP capital will grow each settlement due to the vig; this is how LPs make money. As the relevant LP credit/debit occurs at settlement, the LP's AVAX/share value is fixed each week when users can withdraw or invest.

An initial investment generates the following shares:

LPshares = AVAX invested × TotalLpShares / TotalLpAvax

For example, assume the contract has 123 AVAX owned by its LPs, who have 100 shares. This AVAX may be sitting free or locked up as collateral for upcoming contests. This implies each LP share is worth 1.23 AVAX.

LP AVAX LP TotalShares avax/Share

123 100 1.23

Suppose Alice wishes to invest 10 AVAX into this pool. The above formula implies she would receive 8.13 shares (10/1.23). This would change the pool's balance sheet to

LP AVAX LP TotalShares avax/Share

133 108.13 1.23

Note the ratio of AVAX/share is the same after Alice's investment, so existing shareholders do not lose or gain money via Alice's new investment.

If we assume the LP collective gained 2 AVAX that week, the new balance sheet after a settlement will look like this:

LP AVAX LP TotalShares avax/Share

135 108.13 1.25

The increase from 133 to 135 reflects a 1.5% profit from that epoch's games. If Alice then sold her shares, she would receive AVAX using a transformation of the above formula:

avax Withdrawal = TotalLpAvax × SharesSold / TotalLpShares

Selling 8.13 shares would generate 10.15 AVAX, a 1.5% return on their investment, identical to how much the AVAX LP pool rose over that period.

In this way, any LP investment or withdrawal reflects the percent change in the size of the LP pool’s avax/share over the investment period.

## Oracle Revenue

Oracle token holders must deposit their tokens in the oracle contract to vote, and they must vote to receive revenue. When a weekly settlement transaction is executed, the oracle's 5% fee is applied to the winnings and sent to the oracle contract. The '*feePool'* state variable reflects the lifetime amount of AVAX per token paid to the oracle contract.



When an oracle token holder deposits into the contract, their account notes the current value of *feePool*. When that oracle token holder withdraws or adds to their account, the token holder is sent their entire accrued AVAX using the formula



Having tokens in the oracle is a necessary but insufficient condition for being paid. The contract then takes the total number of tokens





This account's *OraclePoughback* is sent to the Oracle *feePool* as if it were revenue from a settlement.

There is no scenario where the token holders can lose accrued revenue, either due to a lucky win streak by bettors or an oracle hack. Token holders can be sure the contract is in balance, where accounts payable are equal to AVAX in the contract at all times.

## Margin Adjustment for New Bet

There are three types of margin tracked by the contract, all held in the array variable' margin.'

**LP Capital:** This is AVAX owned by the LPs, both free and locked up as collateral.

**LP Locked Capital:** This is AVAX owned by the LPs that are unavailable for bookie withdrawal. It represents the gross worst-case scenario loss for the LPs.

**Bettor Capital**: These are bettor funds applied to outstanding, taken, bets. Bettors do not receive cross margining.

LP capital is available for new bets that increase the contract’s net exposure. New bets that increase the contract's net exposure will increment their LP locked capital account, margin[1]. Bets that decrease the LPs net position will will decrease their LP locked capital account.

For a team with decimal odds of 1.957. the total payoff for a win can be separated into two components: 1 + 0.957, the latter term representing the bettor’s net profit, and the former term representing the bettor's bet amount.

Odds are stored such that



LP Required Margin is the sum of the maximum liability for all the events in an epoch. Each event is independent, so the book is correctly margined by correctly margining all the individual bets. Thus we need merely describe how margining occurs for a single event, knowing these are then summed for determining the overall Required Margin.

The total amount owed if team 0 wins equal the sum of the bet amount and its payoff for all the bets taken on team 0. Let us define two types of capital used to pay bettors, the payout or profit, with must come from someone other than the bettor, and the bettor's initial bet amount, which is returned with his profit:



**betSum0** is the total amount bet on team 0, summing over all the bets on 0. Bettor funds are available for payout but not part of the LP's Required margin (which is in Margin [0] and Margin [1]). **paySum0** is the sum of the bettor's profit if team 0 wins, which requires AVAX from the LPs or bettors taking the other side. As the betSum of team 0's opponent, team 1, is available for paySum0, the trick is monitoring the ability to cover the LP's liability given the amount bet on its opponent. This generates the following maximum liability for the LP (*aka* required capital) for a contest in that it is the maximum liability to either team in a contest:



We add the zero term because the house will have only non-negative liability on every contest. For a new bet long on team 0 playing, the new bet and payout are added to the above max() equation and compared to the extant maximum liability. The difference is the change in the LP's required margin (margin[1]), which is offset by a change in the LP's free Margin (Margin [0]).



This is calculated at the bet time, and the LP's capital is moved into or out of locked LPcapital depending on whether the bet increases or decreases the LP collective’s net exposure. For example, an initial bet will increase the required margin, but a subsequent small bet on the opposing team would lower the required margin. A bet could move the book so that the net LP liability switches from team 1 to team 0 or consists of the decrease in the net liability on team 1. In any case, the above function captures the difference in the worst-case scenarios for contract liability.

In this way, the LP's total book exposure is cross-margined so that 1.0 AVAX capital can support many bets via incremental bets on both contestants. At settlement, the locked LP capital, minus the acrued bettor payouts, is returned to the bookie's total capital and the LP’s locked capital account is set to zero.

Within the GUI, the maximum bet size is displayed when a user toggles the radio button. It is calculated using the following logic. We use the superscript *i* for the pick, and *-i* for the opponent. The potential liability for pick *i* is



The global maximum exposure for any one match is a function of the amount of LP capital and the concentration factor. This number is applied to each new bet, capping the LPs exposure to any one event.



The amount of available LP capital is



With these data, and the odds offered on the bettor’s pick, we can calculate the change in LP locked capital on a new bet:

maximum exposure for a pick:



To translate this into a betsize, we divide by the payoff odds. For example, if the odds were 1.500, this pays out 50% on each dollar bet (decimal odds -1). Thus with 1.0 in LP exposure available for the pick, that would allow a bet for 1/0.5 or 2.0.



LP exposure across matches is independent. The assumption for LP exposure is the worst-case scenario, so there will be no chance of an insolvency, as a bet cannot be taken without capital available.

## Gas for transactions

**contract function gas (x1000)**

oracle initialPost 410

oracle inital voteProcess 129

oracle update Post 112

oracle update voteProcess 72

oracle settle Post 99

oracle settle voteProcess w/ 32 matches 867

oracle settle voteProcess w/ 16 matches 535

oracle settle voteProcess w/ 1 match 191

oracle vote 37

oracle deposit Tokens 52

oracle wd Tokens 84

bet bet 110

bet deposit as LP 54

bet deposit as bettor 48

bet wd as LP 44

bet wd as bettor 33

bet LP claims token Rewards 62

bet bettor redeems 1 bet 40

bet bettor redeems 16 bets 161

## Settlement Detail

Settlement records which bets won and then allocates bettor and LP capital to accounts that ensure accrued accounts are fully collateralized. Each bet creates a struct that contains the team and week of the bet. These two inputs create a hash mapped to a number representing its game outcome: 0 for a loss, 1 for a tie, and 2 for a win. When the array of 32 results is sent to the settlement method, the mapping is created (the mapping is zero for uninitialized hashes, so unless updated, the mapping is 0). This mapping is then used for redemptions, in that a bettor claiming his winnings will need the {epoch, match, team} hash to map to a 1 or 2 to generate a payout.

In addition to creating non-zero hash mappings for non-losing teams, the total payments to all bettors were generated using the results and the paySum and betSum arrays:



Here 1*x* is an indicator function that is 1 if true, 0 else. The *WeeklyWinnings* represents the bettor profit, while the WeeklyPayBack represents the initial bettor funding. The oracle fee of 5% is applied to the bettor winnings, representing about 2.5% of the total bet amount. As individual payouts are less than or equal to the total payouts in any week, this rounding truncations on individual redemptions will not compromise contract solvency; rounding will not prevent redemptions.

At settlement, accounts are adjusted as follows:

Redemption capital = WeeklyPayBack

PayoffPot = WeeklyWinnings \* 95 /100

Oracle fee revenue = WeeklyWinnings \* 5 /100

The bookie's capital then adds the money bet that week minus the payouts for wins and ties.

bookiePool = bookiePool + bettorLocked – redemptionPot – payoffPot

The oracle revenues are then just 5% of the WeeklyWinnings, and are transferred to the oracle contract in the settlement function.

The bettor's money exists in the residual and must be claimed via redemption. At redemption, their bet and its winnings are credited to the bettor's user balance, available for withdrawal or future bets.

After settlement, the bookieLocked margin is set to zero, so all LP funds are available for withdrawal. LPs need to pass 3 settlements before they can withdraw.

## 

## Odds Stability

The relative stability of straight-up sporting event odds compared to the vig allows for a super high-latency oracle that would never work for swapping tokens. 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 prices once 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. This means one needs a 2.5% edge in predicting which team wins to beat the house. The weekly volatility of these odds, when translated into a win probability, is less than 1.0%, implying the book would make money even if it used early-week odds. In practice, the closing line and opening lines for NFL betting are statistically identical.

## Incidence Response Suggestions

There is no outside adjudicator to rectify problems, as this would delay payments and complicate the contract—how to incent the adjudicator? All problems must be solved on-chain within these contracts. As I do not and cannot control the contract, this is advice rather than an official protocol or something automatically enforced within the contract code.

Off-chain odds can change quickly and significantly, exposing the LPs to bets with an objectively negative expected value position. In that case, oracle token holders can immediately pause new betting on an event. This action does not require the usual 12-hour vetting period to allow oracle token voting. It does not expose LPs or bettors to more risk, as it just prevents new bets on those matches. Such an action has no upside if this is not true for the oracle.

Lastly, if a hack or unintentional error snuck in, the oracle collective could nullify this action by posting a result of a tie regardless of the outcome. This allows the LPs and bettors to get their money back as if nothing happened, and the ‘incorrect’ but fair tie result should be explainable by the event logs showing the earlier hack. This would be an extreme scenario, like a fork in a blockchain, but it is always good to anticipate a worst-case scenario.

1. Adverse selection for LPs would be when they offer odds and get filled only when it’s an objectively bad deal, as with arbitrage.. [↑](#footnote-ref-2)
2. A proposal attributes the submitters tokens as a yes vote for that submission. [↑](#footnote-ref-3)
3. It is equal statistically, that is, over time. Both the oracle and LPs are subject to small sample variation from different sources. If there are no winners, the oracle gets nothing. In contrast, the LP’s could lose all of the bets where they have net exposure and thus lose money. The oracle has to work, the LPs have to take risk. [↑](#footnote-ref-4)
4. A flat book does not mean the bet amounts for both teams are equal. For example, a contest could have 5 avax bet on a 5:1 favorite, and 1 avax bet on the underdog, leaving the LPs with zero risk. [↑](#footnote-ref-5)
5. 625 = 50.001% of 1250 [↑](#footnote-ref-6)
6. Augur was plagued by bad-faith actors like Poyo-Poyo, whose intentionally deceptive bets were dismissed as the actions of a rogue agent. If the implications of his actions were immediately fatal for Augur he would have been disciplined by those with an equity interest in the dapp. [↑](#footnote-ref-7)
7. I created something that I would like to use. Online betting, let alone providing liquidity or administering a betting contract, is not legal in my state. I may not be able to take that crypto off the blockchain, but for my modest betting inerests, the ability to spend buy goods and services worth a couple hundred bucks with any potential winnings is sufficient. [↑](#footnote-ref-8)
8. I did not create such a vault but it should be straightforward, though there are several ways to do this. [↑](#footnote-ref-9)
9. In *Political Parties* (1911), he noted that that rule by an elite, or oligarchy, is inevitable within any democratic organization as part of the tactical necessities of the organization. [↑](#footnote-ref-10)
10. vault independence is not enforced in thi dapp. I am just telling the vault creators it is in their best interest to be independent. They would be worth more, collectively. [↑](#footnote-ref-11)
11. The initial data provider’s tokens are credited as a yes vote, and votes are decided on a simple majority of votes cast. Thus if no one else votes, the data submission will pass. [↑](#footnote-ref-12)
12. One could imagine a bad outcome could be allowed to pass because it was deemed insignificant (small amount bet), and the costs of delaying the contract were large. As only 2 data submissions are required in any week, a rejection would still enable the contract to be up and running that weekend. [↑](#footnote-ref-13)
13. The favorite/underdog refers to the opening line, and so over the week the initial favorite may become the underdog. Nonetheless, the ordering is fixed in the initial event posting. [↑](#footnote-ref-14)
14. A negative vig would allow someone to create positions that would generate arbitrage profits. [↑](#footnote-ref-15)