Small token holders rarely participate in governance votes. This is rational because there is a minimum fixed cost to evaluating data, say 15 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 this common public choice voter information problem, the minimum deposit in the oracle contract is 100 million tokens, 10% 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.[[1]](#footnote-1)

Data submission: page 6

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 will obvious in this contract, and any users seeing such a cheat will rationally avoid such a contract, making the present value of the oracle token zero. This enables a ‘grim trigger strategy’ equilibrium, where players cooperate because the honest reporting is the dominant strategy (see Appendix on the importance of repeated games for generating honest play).

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.

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.

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.

Focus on OX, the oracle experience. The oracle’s job should be feasible by a single person without a large capital investment. I provide tools for collecting the relevant data into the format needed by the contract, and python programs for sending data. There are free or cheap tools for pulling sportsbetting data into a spreadsheet, and I provide tools for then processing that into the format desired by the contract. Once processed, that data can either be sent to the contract, or used to assessed data sent by another. If they set up a droplet for only $10 a month, they can create cronjobs that automatically send data or votes conditional upon their evaluation.

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.

. Once assessed, they can then send the data to a server where it is used in the cronjob.

, and then just only need to manually send the

The bottom line is that a cheat will be obvious. The limited focus on at most 32 straight-up bets, on high profile events, each week, makes this even easier to see in event logs. There are only three data submissions each week, and they are constrained to be submitted between 6 PM and 8 PM ET, and then the oracle has 12 hours to evaluate the data. The restricted nature of data submitted—timing, frequency, scope—focuses and minimizes the attention needed by the oracle.

The path of net exposure relative to gross betting is crucial for determining the optimal amount of LP capital.

The forsaken oracle revenue is reallocated to the other token holders in the oracle contract.

In May 2023 Ethereum saw transaction costs spike 6-fold. The cost was transferred to L2s like zkSync, which would have made the costs of depositing, betting, redeeming, and withdrawing greater than $15, making a standard $40 bet unattractive. To the extent some L2s gas costs did not mirror the mainnet, that just highlights these blockchains are subsidizing users, an understandible strategy for gaining traction. To be sustainable, however, these L2s will have to charge more, and it is uncertain whether or not that will work. Avalanche’s gas price has been much more stable over the past year, with gas prices rarely moving more than 30%.

The data submitter automatically votes for his submission, so if no one votes, it will succeed, as it is a simple majority vote that determines success or fail.

The data submission is pass/fail, and failure is conspicuous given the binary outcomes, and that odds at major books are always within 3% of each other (in probability of win). This caps a cheater’s ability to slant odds.

There is no reason for allowing incorrect data to get voted to the betting contract outside of a conscious intent or radical incompetence. Such data would include start times more than 15 minutes ahead of the actual start time, marking the outcome incorrectly (who won), or odds that are outside the standard beyond the standard variance in odds across sportsbooks given the low verification costs generated by the restrictions on timing and event coverage, and how all oracle voters will have significant token stakes that justify the cost of carefully evaluating data submissions. Honest reporting is the dominant strategy in the improbable worst-case scenario described above (P/E of 10, gross exposure equals net exposure).

Odds can vary, but they are constrained by arbitrage to a 3% win probability. To make money off this sort of edge takes hundreds if not thousands of bets.

account. Once funded, toggle radio

button on the team/player and enter desired avax bet in the box

(eg, 1.123). If they win, you get your bet back times the

decimal odds. You redeem all bets at once, which clears your

array of unredeemed bets, but only when you have no active bets.

If you have 16 unredeemed active and closed bets, you must clear

your unredeemed bets to bet again. Redemption sends any winning

back to your free capital balance, which is then available for

withdrawal or new bets.

I created this dapp but I have no control or financial interest; I cannot administer let alone disable the contracts.[[2]](#footnote-2) 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.

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.

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.

The permissionless nature of the blockchain also makes it t is rare for American casual retail sports bettors to be prosecuted for using unsanctioned betting sites. Betting is problematic for many Americans mainly because banks and credit card companies often block betting sites, and many states ban various types of betting. On the blockchain, however, an American with a modest betting habit cannot be monitored because one can easily spend a potential couple thousand dollars in winning without needing to transmit those funds to a fiat choke point like Coinbase. If millions of Americans use crypto to bet, and bettors use their winnings buy a couple hundred dollars’ worth of stuff each year, it will promote crypto.

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%.

As the main friction is caused by the potential rift between the oracle and LPs—the oracle’s most obvious cheat would be to bet on an underdog via a sock-puppet account, and then post that the underdog won regardless of the outcome. Thus, token holders should also act as LPs, as this eliminates the cost generated by their differing incentives.

LPs cannot invest or withdraw when games are active, which is the period between the start time of the first contest and when the results are posted, and bets are settled. This is because recently decided events may imply a large win or loss to the LP collective and potentially present an arbitrage for LPs trying to capture or avoid these cashflows.

While odds vary among sportsbooks, they all preclude arbitrage, so the check on odds is that the two odds presented are within the odds presented on popular sportsbooks. Nonetheless, adjusting odds to generate an edge is inefficient relative to falsely reporting an outcome.

As per making it better, I can see how adding different sporting events would be useful. It is not obvious how to handle the problem created by sports whith multiple games per week. If one settles the contract every day, one needs a highly vigilant oracle collective to prevent bad data sent at odd hours. It could work, but getting there would require a different protocol. Perhaps it woul have an ability to reward and punish oracle data providers ex post.

Real success for protocols is the Satoshi method: it works, and the founders/team fade away to irrelevance. If Satoshi were a real person, many seeking to stop Bitcoin would have poured through his writings and found something he wrote to support the idea that Bitcoin is a tool of the WEF, Nazis, etc. I am not fading away, but the contract in every way outside of promoting it. I have no more power to control the contract than anyone else; I have not and will not profit from it, and cannot shut it down.

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 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 MMA and American football betting implies a large market that blockchain dapps have not yet impacted.

pVol

A screenshot of a game

Description automatically generated with low confidence

The fastest blockchains—Solana, EOS, Ripple—are effectively centralized, as consensus mechanisms take time. With an effectively centralized sequencer/validator, the consensus mechanism is almost irrelevant, and one can approach input-output speeds much closer to those seen in Web2.0. These centralized chains have not been plagued by dishonest miners double-spending, as it is in the miners self-interest to not cheat. Yet these chains are still untrustworthy, because it is easy to imagine cases where a state regulator informs the chain’s principles that if it does not censor various addresses, it will be be prosecuted. One expects this to happen at some point, as when Circle froze the USDC in various accounts in response to OFAC regulation. Without decentralization, all the malicious contract destroyer needs to do is find the oracle, which is highly likely over time.

Decentralization and the incentive compatibility are both essential for smart contracts. However, most decentralization benefits accrue from the blockchain itself, as the good ones offer immutability, permissionless access, transparency, and pseudonymity.

If the oracle token is fungible and held pseudonymously, the oracle collective is effectively decentralized regardless of how many holders there are. The theory of contestable markets explains how a centralized market will act as a competitive market if entry and exist costs are low.[[3]](#footnote-3) For example, an existing monopolist cannot charge monopoly prices if other firms can costlessly enter and enjoy some of those monopoly profits. The potential for new entrants often causes players to act as if these new entrants are current players. The ability of an oracle-admin token holder to transfer his tokens and the ability of newcomers to resurrect a censored contract, makes the outsider task of shutting the contract down quixotic.

In traditional casinos the bookies have two roles, providing odds and capital. As LPs share revenue pro-rata, a cheating oracle would most likely use a bettor sock-puppet account in a hack, making sure to maximize his exposure to teams he knows he will tell the contract won. As the LP’s are the primary target of an oracle hack, they have a strong incentive to keep fraudulent data from getting to the betting contract, and it makes sense to combine LP and oracle-admin responsibilities off-chain (when they are the same, we remove the incentive for the oracle to cheat the LP). On-chain, however, it is not straightforward to combine these roles, so they are independent. In practice, a large LP has an incentive to acquire oracle tokens to prevent an oracle fraud, but we should assume they are independent when assessing incentive compatibility.

One should not assume good faith. For a cheater, their past record will be perfect. The oracle is not supplying odds it estimates independently in good faith. Honest odds are trivial to assess. oracle scoring algorithm be perfect until you are not.

Competition is not needed to generate odds that are fair, because the standard vig is applied to every match. If you let people supply their own odds offers like limit-order book, they will post big spreads, or one-sided markets. With enough free entry and exit, the book would be competitive. Yet the process of getting from the initial state where wide odds are posted, and where we have a competitive equilibrium, is difficult. Oracle chooses a price and a spread (fee). Incentives work on oracle if it is a monopoly. It is forced to provide a two-sided market. Decentralization is just for protecting against outsiders.

The oracle-admin-equity token is designed for use, not creating a pump ‘n dump via convoluted staking mechanisms designed to artificially restrict selling. Vague governance rights and future revenue streams implies vague attack surfaces. Each submission requires a majority yes vote to push the proposed data—odds or results—to the betting contract. The equity token is just used for sending and voting on data submissions, not betting, which uses the native AVAX token.

Restricting the scope of events makes it easier to parameterize the contract to make it incentive compatible. This avoids the problem from ambiguous outcomes that plagued Augur.[[4]](#footnote-4)

**Fees and Vig**

The oracle sends a single odds number for an event, the decimal odds for the favorite. The underdog’s odds are then determined via an algorithm that enforces a positive vig on each contest. This prevents fat-finger mistakes from creating a situation where an arbitrage can exist on the contract. The oracle-admin get a risk-free payout via a 5% cut of the bettor’s winning, which is about half of the total vig of 4.7%. The LPs get about 2.5% of the total amount bet given the oracle payment, but this is risky, as even with fair odds there is a risk bettors could be net winners one week.

The oracle contract provides the event schedule, odds, and results to the contract. Oracle token holders can make submissions only during the noon hour, GMT. The vote is not tallied for at least 11 hours, giving the oracle token holders sufficient time to assess the data submission and vote on them. When the week’s results are approved on Monday, they are sent to the betting contract and all extant bets are settled, allowing instant redemption by bettors. Tuesday the new set of events, times, and odds are posted.

Liquidity providers (LPs) add AVAX to the contract reserve, providing instant liquidity for bettors. The LPs collectively cover any imbalance in the book as they share the weekly net profit/loss pro-rata.

While decentralization is a necessary condition for a prosperous economy, this does not imply that firms within that economy must be decentralized at all times in their development. Firms in abstract are emergent properties of free markets in that given the freedom of contract and association, invariably some individuals will find it useful to have explicit rules and responsibilities to other individuals in achieving a common goal. However, all specific firms are started by individuals with a consistent unitary vision, that is, centralized.

The repetition generates an opportunity cost for the potential cheater, the oracle, in that its job requires little skill, just abide Google’s original code of conduct: ‘don’t be evil.’ The immutable, transparent, pseudonymous blockchain is great mechanism for monitoring player actions.

In contrast to asset prices, sports betting odds are virtually nonstochastic. While odds are presented in various forms—moneyline, decimal, fractional—these can all be translated into a probability of winning by figuring out the number where the bet has a zero expected value. Evenly matched teams have 50% win probabilities, and are generally offered at moneyline odds of -110 (aka, decimal 1.909). A profitable bettor needs a 2.5% edge to beat the casino.

For aribtrage to take place, one needs to find markets where the bid from one market is greater than the ask in another market. For example, with a bid-ask spread of 1%, if a stock trading at a bid-ask of 101-102 in Chicago, and 98-99 in New York, traders can sell for 101 and buy for 99 repeatedly, creating a money pump that will force the market makers to adjust their spreads. With the spread only a thirtieth of the weekly volatility, to avoid arbitrage market makers must be constantly vigilant about the current prices at all times. In contrast, arbitrage in sportsbooks is basically impossible, as the slowness of sports betting allows the bookies to maintain odds that vary insignificantly and do not allow abitrage.

Forcing people to use an equity token does increase the token’s profile for a classic pump ‘n dump, but mainly is just annoying for our target audience: casual sports bettors.

Oracle acts as unitary consciousness

Decentralization is not prim blockchain with anonymous nodes is immune to the standard heavy-handed actions of outsiders.

Initially, an initial oracle token holder was given 49% of the tokens, with the other 51% residing in a contract that distributes tokens to bookies as a reward.

LPs have no control over the particular positions they accrue, and bets may be concentrated on a handful of games, exposing LPs to losses. They are paid for taking on this risk via the spread so that, on average, they should make 2.5% of money bet if the odds posted are statistically accurate.

Major event odds are relatively stable across time . For example, the closing line in American football is statistically no worse than the opening line, as the benefit of new information is offset by oddsmakers accomodating whimsical retail flow.[[5]](#footnote-5)

However, the vig acts as a bid-ask spread that prevents bookies from becoming a ‘money pump’ as long as their odds are comparable to those offered by others. The net result makes oracle data evaluation straightforward. Just as a single sliver of glass ruins a big bowl of ice cream, a single bad datapoint in a large set of data is potentially catastrophic.

Bookies post similar odds because there is arbitrage if the probability of A and not-A is less than 100%Ceasars offered a payout implying A has a 35% chance of winning, but FanDuel one outlier would attract all of the demand for one side, and the bookie would not have sufficient capital.This implies that 24-hour-old odds will not expose LPs to debilitating arbitrage.[[6]](#footnote-6)

Sports with more events, like baseball, hocker or basketball, cannot fit this initial target because a game earlier in the week can dramatically affect that weekend’s games (eg, they lose a playoff game in a series, injury).

No price discovery, a true derivative market Sport odds: stable, easy to get, vig, arbitrage rare due to vig. 95% of time opening odds stay. Deep market.

Don’t ask a price if not interested in buying

Vig 5% for a long time

incentivize Oracle token holders. Bettors and LPs cannot do anything destructive if they tried. For bettors, the more the better. For LPs, there will be an optimal amount of capital.

One key is *not* to emulate a modern stock market. With the arrival of the internet, the standard is now the *centralized limit order book*, where users post and cancel limit orders, or take open resting limit orders. Stock markets are run on centralized databases and allow high-speed access at under 10 milliseconds. This type of market will never work on the blockchain due to the thousand-fold latency differential.

Decentralized Ethereum exchanges such as 0x and Etherdelta allow traders to post and take orders with specific prices, so that when arrayed in a list look a lot like a central limit order book. However, the Ethereum block time is around 10 seconds, and interactions are multiples slower as a practical matter. High latency increases the comparative advantage to those who invest in specialized hardware and software to interact with the contract.

SmartSwap eliminates the limit order book to stay on the blockchain and avoid latency costs. This solution is inspired by the popularity of value-weighted-average-price (VWAP) transactions among long-term institutional equity investors. VWAP orders generate fill prices over some future time window, often the next day's average price. The day lag does not inconvenience long-term investors in executing their trade. It is efficient, fair, and easy to monitor. Using future spot prices supplied by an oracle generates similar results, and this allows SmartSwap players avoid the trading costs inherent to limit order books.

An honest oracle being essential to the SmartSwap, the second key to creating a viable financial contract is to *tie the contract to a pseudonymous human oracle* (the SmartSwap Oracle or **SS Oracle**). While many oracles focus on either decentralization or authenticity proofs, SmartSwap focuses on the costs of creating an incentive compatible game people will want to play. This centers on simplicity, which is the key to lowering the costs of playing the game.

*Decentralization* and *anonymity* are essential for any system targeting individual custody and uncensorability. For example, E-gold is the most relevant precursor to bitcoin, created by two publicly identified American citizens and headquartered in Florida. It used a pseudonymous ledger where balances were denominated in gold and had over a million accounts at one point. The company was shut down in 2007, their directors tried and convicted of money laundering and transmitting money without a license. Intrade was an Ireland-based web exchange known for its prediction markets, especially US Presidential elections. In 2008 a group of 22 academics including 4 Nobel laureates wrote an open letter to *Science* pleading for looser regulations related to prediction markets, but regulators continually attacked the exchange and closed in 2013.

In contrast, anyone targeting a ledger-producing node on the Ethereum blockchain will see one instantly take its place, like one of the Persian Immortals. Vitalik Buterin highlighted the resiliency of the blockchain to the $5 wrench attack:

“The thing with developers is that we are fairly fungible people. One developer goes down and someone else can keep on developing. If someone puts a gun to my head and tells me to write a hard fork patch, I’ll definitely write the hard fork patch. I’ll write the GitHub issue, I’ll write up the code, I’ll publish it, and I’ll do everything they say. If I do this and publish a hard fork patch to delete a bunch of accounts, how many people will be willing to download the update, install it and switch to that update? This is called decentralization.”

Vitalik Buterin. TechCrunch: Sessions Blockchain 2018 Zug, Switzerland

A decentralized blockchain with anonymous nodes is immune to the standard heavy-handed actions of outsiders. There have always those who destroy businesses for expropriation or preventing competition (e.g., see the Knights Templar)[.](#a3) In these cases, the destroyer is protecting power or wealth by eliminating a rival, but they need a centralization point. Decentralization and the incentive compatibility of honesty are both essential, but they target different risks: decentralization is critical for defending against outsiders, not insiders.

A pseudonymous Ethereum oracle contract is censorship-proof by merely being on the blockchain, so it does not also have to be decentralized to be censorship-proof. One could make an Ethereum Improvement Proposal to freeze a contract, but such a radical move would be easy to see coming.

Given a decentralized blockchain, the consensus mechanism for validating records on the public ledger necessarily involves decentralization. The proof-of-work protocol creates a direct cost for a double-spend attack, in that one needs to control a significant amount of hash power on the blockchain to be successful, and this takes electricity as well as hardware. For the top decentralized blockchains one cannot simply rent that much processing power, so a 51% attack would sabotage one's sizable investment whether it was Satoshi eager to protect his new creation back in 2009 or current mining pools protecting their profitable but non-repurposable investments.

The Satoshi white paper noted that a greedy attacker invariably has to choose between using his CPU power to double spend, or use CPU to create new coins via a mining reward (page 4). A rational attacker would not merely look at the immediate mining reward, but the present value of all future mining rewards. It is estimated that for someone with the wherewithal to mount such an attack, consideration of the sabotaging effect on their specialized mining equipment raises the attack cost 1000-fold over the direct hash-power cost of the 51% attack.[[7]](#footnote-7) Thus, while as a practical matter bitcoin miners could easily collude to generate a 51% attack, it is not worrisome because it would not be in their best interest. Importantly, the incentive for honesty applies to any subset of potential malefactors, and so it is rational to presume the minimum necessary collusion acts as a single agent. The decentralization of miners is therefore irrelevant to the primary mechanism that keeps mining honest.

Reputation: immutability and transparency and pseudonymity

A pseudonymous oracle can have a valuable and verifiable reputation, as only the private key holder can access the SS Oracle’s account, facilitating a game where the present value of being honest can be compared to the value of cheating. It creates the most straightforward censorship-resistant structure for reporting, monitoring, reward, and punishment. Thus we need to make sure honesty is the SS Oracle's dominant strategy.

Contracts fees are focused on two necessary parties—Liquidity Providers and the SS Oracle.[[8]](#footnote-8) In contrast, tokens, relayers, adjudicators, etc. implies less money to the SS Oracle and liquidity providers, so that either the expenses become too high for investors, or too low to motivate SS Oracle honesty and liquidity providers.

This contract levers an unusual tactic to discourage cheating: if a player sees a fraudulent price about to be applied to their subcontract, they can burn their payment rather than send it to their counterparty. A burn generates an event log documenting the date and price, allowing outsiders to assess its credibility.[[9]](#footnote-9) A documented cheat should discourage future players and eliminate the SmartSwap Oracle's future revenue. A burner must pay a fee to prevent whimsical burning, but players will be motivated to pay to punish by both righteous indignation and a pure cost/benefit analysis. While burning one's payment should never happen in practice it reduces an evil SmartSwap Oracle's potential cheat payoff to a strategy that walks away from its first loss.[[10]](#footnote-10) SS Oracle dishonesty is irrational for a long-term value maximizer, but even a short-sighted evaluation generates the meager benefit of repudiating a debt, at the cost of destroying future revenue.[[11]](#endnote-1)

Liquidity providers are incented by their ability to net their margins and receive the margin rate paid by the Takers. An LP posts a quantity only, and by adjusting the long and short margin rate it charges Takers can equilibrate its long and short exposure. Given current market margin rates, LPs can charge half that and generate annual returns of over 50% on capital, all while allowing investors to stay on the blockchain, a classic win-win.

For any one-time event the incentive for one party to cheat is high, and thus even obvious events like who won the recent US Presidential election are problematic because the blockchain has no common sense about the real world. A blatantly wrong reported outcome can't affect the future for an anonymous player playing a one-time game, creating a strong incentive to manipulate the system—via collusion, hacking an API—to take the money and run. Giving third-parties a veto to prevent this, however, just concentrates the trust issue as opposed to eliminating it. To the degree the third-party is reputable via being publicly bonded or legally approved, this would imply players would lose the custody and anonymity that many crypto holders desire.

After the first crusade (1099), the Knights Templar safeguarded pilgrims to newly conquered Jerusalem and quickly developed an early international bank. A pilgrim could deposit money or valuables within a Templar stronghold and receive an official letter describing what they had. That pilgrim could then withdraw cash along the route to take care of their needs. By the 12th century, depositors could freely move their wealth from one property to the next.

As they built up vast wealth and power, they were seen as a threat, especially as King Philip IV of France was deeply indebted to the Templars. On the same day across Europe, October 13, 1307, scores of Templars were arrested, including the order’s grand master. Claims were made that during Templar admissions ceremonies recruits were forced to spit on the Cross and deny Christ; that they worshipped idols, and engaged in financial corruption. Many of the accused confessed to these charges under torture. A few years later, dozens of Templars were burned at the stake in Paris for their confessions, and the Templar banking system disappeared.

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.

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.

In the prisoner’s dilemma game, the Nash equilibrium strategy is for both players to play the noncooperative strategy. In the movie *A Beautiful Mind* this insight supposedly turned economics on its head because in large markets the standard result is that competitive market outcomes are socially optimal.[[12]](#footnote-11) In reality, the Nash equilibrium did not invalidate Adam Smith’s invisible hand, it just highlighted the importance of repeated interactions for lowering transaction costs. In the *iterated* prisoner's dilemma, the equilibrium strategy is to cooperate and so acheives the socially optimum strategy. A properly incented game ensures that for all players at all times, cooperating has a higher present value than cheating. This is selfishly motivated reciprocal altruism—I play nice because I expect you to play nice—enforced by the threat of punishment.

1. I did not create such a vault but it should be straightforward, though there are several ways to do this. [↑](#footnote-ref-1)
2. 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-2)
3. William Baumol, John Panzar and Robert Willig (1982). Contestable Markets and the Theory of Industry Structure. [↑](#footnote-ref-3)
4. For example, that Republicans would win control of the Senate on Nov 7, 2016. The vote was confirmed that day, but the Republicans would not actually control the Senate until the following month. An argument can be made for both interpretations, which leads to broken markets. [↑](#footnote-ref-4)
5. See http://www.collegefootballwinning.com/blog/efficient-markets-in-sports-betting/ [↑](#footnote-ref-5)
6. In a worst-case scenario, oracle token holders can pause up to two events while updated odds are being processed. [↑](#footnote-ref-6)
7. See Budish, 2018, "The Economic Limits of Bitcoin and the Blockchain." Note that the leading blockchains have such higher hash power that attackers can rent hash power to generate 51% attacks without affecting the present value of their mining equipment, and thus leading to attacks on verge, zencash, and others. [↑](#footnote-ref-7)
8. Two exceptions: burn fees are sent to an unaffiliated third party—the Ethereum Foundation's tip jar address—and will be rare, as if not the contract would not generate trust and thus users, and without users, the contract will have no burn actions. Closing fees go to the counterparty, which while generally from Taker to LP, can go the other way. [↑](#footnote-ref-8)
9. Technically, it generates a block number, but this then corresponds to a date-time. [↑](#footnote-ref-9)
10. Such outcomes are "off the equilibrium path," in that it is never reached in equilibrium, but its existence is necessary for the equilibrium. [↑](#footnote-ref-10)
11. ***[Burning money](#r4b)***

    Burning money is related to Holmström's Theorem, which states that no incentive system for a team of agents can satisfy all the following properties: money in=money out, Nash equilibrium, and Pareto efficiency. Here there are potential outcomes where the budget is not balanced and money vanishes into the ether (when a burn occurs). See Bengt Holmström, "Moral Hazard in Teams," The Bell Journal of Economics (1982). [↑](#endnote-ref-1)
12. This can be seen looking at consumer and producer surplus, or the first and second welfare theorems. [↑](#footnote-ref-11)