Incentive compatibility is vital to low-cost enforcement of contracts, and historically this mechanism centered on reputation, not contract law administered by the state.[[1]](#footnote-1) The blockchain's transparency, immutability, and pseudonymity make reputation much easier to monitor. When agents have incentives aligned with their counterparties, we minimize non-explicit costs like delay and spread that plague these markets. If the bettors or LPs want to cheat, they need to collude with the oracle; if the oracle does not cheat, neither bettors nor LPs can cheat. The focus is to ensure honest and timely reporting of odds and results is always the oracle collective's value-maximizing act.

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.[[2]](#footnote-2) 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.

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.

Can it be stolen? Yes. However, the dapp presented here benefits from the large fixed cost born by its creator, me. My incentive is simply to create something popular, because there is joy in creating something people like. If it fails, all of the time and effort I invested in this project would be a waste. In contrast, if someone merely grabs my code and rebrands it, they have little to lose if it turns out their code has a back-door enabling a scam, and pumping a worthless token is a common focus for many crypto developers. Thus, users should be wary of copycats.

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.

s that could punish a lot of trust.

In a worst-case scenario where posted odds deviate significantly from market odds, an event's new bets can be paused until the following odds update, preventing new bets on a contest until updated odds are posted. Pausing bets requires a minimum amount of oracle tokens and can be pushed immediately; it does not expose the LPs to risk.

No off-chain backend database needed

boxing

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 explicitly abandoning myself from the contract in every way outside of promoting it. I have no more power to control the contract than anyone else 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.

Secondly, a sports betting is significantly simpler dynamics than an asset market.

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.

While voting can be annoying for token holders, this gives them a strong incentive to monitor the data submissions. To the extent there is demand for a low-contact oracle role, a user might create a vault where they aggregate tokens and vote on their behalf for a small fee.

The oracle presents aach week’s contests as a slate. Data submissions restricted to once a day, always at noon hour, and oracle token holders always get at least 11 hours to vote on the submission. The website adds to this by making it easy for users to see historical data sent to the betting contract, as the event logs are readible even if one does not understand what a hash or byte is.

Netting the player/team exposure for a contest allows a finite amount of capital to support an unlimited number of bets, a cost-saving that benefits all users.

Most sports betting sites that tout their bitcoin functionality are just conventional betting sites that accept bitcoin. A blockchain-based betting site adds *pseudonymity*, *confiscation-proofness*, and *permissionless access*, which makes it much easier. Further, users can bet, provide liquidity, or join the oracle.

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.

However, this initial oracle was chosen for his predisposition to support SnowBet, and his support of liberty and blockchains in general. Thus, we only need make sure that honesty is the oracle’s profit maximizing strategy.

SnowBet is a smart contract allowing straight-up sport bets on weekend events such as American football and UFC fights. There are three types of contract users: bettors, liquidity providers (LPs), and oracle-admins. LPs provide liquidity to a slate of up to 32 events as opposed to a single event.

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.

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.

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 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 such teams to win 52.5% of the time, and in general the sports bettor needs a 2.5% edge to beat the casino. The volatility of the odds-implied win probability over a week in football is around 5%, which is only two times greater than the edge needed to beat the house.

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.

Nonetheless, the Oracle-admin rewards program is aimed solely at LPs because the larger the overlap among the oracle and the LP the better.

Cross margining

The limited scope and frequency of events makes it possible for an individual to confidently assess the oracle’s honesty.

Given odds or results on a single event, the marginal cost of finding such data on similar events is negligible, so having one person provide all information at once is most efficient.

In business relationships there are often no formal contracts, rather, if we find someone's work unacceptable we simply stop using them. The key to making this work is that the benefits of cheating are small relative to the potential gains of the being able to play the game again.

The iterated prisoner's dilemma shows how a multi-period game can move an equilibrium strategy from a suboptimal equilibrium where both parties maximize their one-period payoff by not cooperating, to the optimal equilibrium where both parties cooperate. In evolutionary settings this is called reciprocal altruism, and illustrates how cooperation emerges out of long-run self-interest, as cooperating players out-compete because in real life, it's not any one game that counts, but rather, the meta-game, the game of all games. T key is to have many interactions, so any one period is small relative to entire game.

Repeated interactions and easy monitoring of player actions are essential for generating good equilibria. 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.

A sustainable contract creates a repeated game where honesty is always the dominant strategy. Simplicity is crucial in generating good game theory equilibria because the state space grows exponentially in the number of players and actions they can take. An incentive compatible contract avoids the more costly solution of establishing institutions with ex-poste power to punish and confiscate.

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.

If the LPs have 100 ETH, an adjustable concentration factor f prevents the LP’s from having an exposure greater than 100/f.[[5]](#footnote-5) Bettors take bets,

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.[[6]](#footnote-6)

SnowBet's oracle is *trustless* because one only has to trust the oracle is financially self-interested, an objective shared by good and bad people.

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.

Major weekend sporting events will have odds posted on dozens of betting sites. WeeklyBet calculates an average odds via the major sports books, and enforces a 5% vig on each contest. For example, a classic even-money bet would have both contestants in a game with the same odds, such as moneyline odds of -110.[[7]](#footnote-7) The standard vig implies that the probability of both parties winning is around 105%.

aligning incentives and adjudication procedures generated

The main benefit of this contract is that it is easy to monitor and use. It is accessible like any contract on the blockchain, and one can use the ethsport.com website to place bets, or download (and customize) this front end via this GitHub repo.

While this contract’s administrators will be decentralized, that is a second order concern addressing a long-run sustainability. The decentralization epigram is a market, and it is good to remember that it is rarely true or even helpful for the parts to have the characteristics of the whole. A decentralized crypto market, like any market, will be dominated by non-decentralized agents maximizing their self-interest. Billion dollar coins are often based on delusional endgames, such as when SBF told his VCs that his vision would be that FTX would be where people do everything, such as buying bananas. Decentralization is a virtue, but on size, scope, and decentralization, as if one can build a crypto-version of Amazon. This creates an inefficient contract because different transactions have different parameters, requiring different monitoring incentives.

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.[[8]](#footnote-8)

If bettors find the contract’s vig too generous, they can join the house, and receive income proportional to their liquidity they provide.

avalanche

On avalanche due to cost, speed, and congestion. Uses EVM.

size of betting market

Equity/Admin/Oracle

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).

Just football, MMA, and boxing.

If play-in, could lose or have injury

Limited focus—just one sport, league

limited frequency—data are not transferred on weekly events

Limited is good for monitoring oracle, easier to incent.

vending machine

Simplicity: games limited, win/lose, same time of day. Handful of contracts, not dozens of libraries.

Power law in popularity

Users can bet or act as the book by providing liquidity. LPs get a pro-rata share of the book's profits but are at risk if the net bettors' position wins.

players

Oracle: post accurate odds and results. ½ vig, no risk

Bookie: provide capital for initial and residual imbalances. ½ vig, risk

Bettors: bet on games

Timing

Weekly

Submission once a day

vote on a slate

always at least 6 hours to vote

Forcing the bettors buy the equity token (why bring in stablecoin?).

equity has a job, and gets paid

equity token necessary to get oracle revenue

job just send accurate data. Costs the same to send as inaccurate data

Equity tokens without jobs imply an inefficiency

Need real job. No one votes on boring stuff. If it is boring that means its unremunerative, meaning it is not a good bonding device. If equity doesn’t do something explicit, it will find something to do

Decentralization for LT risks; choke points, outsiders

Reputation: immutability, transparency and pseudonymity, permissionless access, cryptographic security

, making the odds difficult to estimate. The initial submissions—odds, results—are restricted towards a single hour each day, and once supplied the oracle token collective votes on the submission as a whole. After six hours anyone can process the data submission, and successful submissions are sent to the betting contract. While this limits the scope of the contract, it makes certain all data submissions are given a thorough vetting. The standard periodicity—and focus on American football, boxing and mma—makes it easier to monitor and discipline the oracle, as new information cannot sneak into the contract unexpectedly.

price mechanism—no wisdom of crowds

No Wisdom of crowds

Not a CLOB, Not an AMM

not asking for {price,quantity}

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.[[9]](#footnote-9) 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.

Basic game theory

In the game theory field of *mechanism design*, there are two necessary and sufficient conditions for a good contract. First, an *incentive compatibility* constraint that motivates honest or cooperative actions by players. Second, a *participation* constraint that motivates players to want to participate in the contract. Thus we need to be sure honest reporting is the SS Oracle's best strategy, and also want to be sure all necessary players—liquidity providers, oracle, administrator, investors—prefer to play the game rather than ignore it.

Augur is a good example of a game that was incentive compatable, but the costs generated by their validation protocol made it too expensive to play, which violates the participation constraint. The costs were mainly indirect, such as the many week delay between expiration and the payout of a binary option, or the high proportion of intentionally fraudulent bets. It is not sufficient to highlight a mechanism for

simplicity

The SmartSwap Oracle's revenue is its bonding device, so eliminating as many other parties as possible minimizes the user expense needed to incent honest reporting. Creation and administration of the SmartSwap contract are done by the SS Oracle who records its prices. These roles are complementary in that they need each other: a derivative transaction need a price, and an oracle needs a contract to update. As the SS Oracle and SmartSwap administrator need to be pseudonymous to avoid an attack vector, outsiders must presume an oracle-administrator collusion in their worst-case scenario anyway. By having the SS Oracle tied to a small set of similar contracts, we can more confidently model its incentives; by having the SS Oracle administer other contract features we can pay the SS Oracle more. Considering the SS Oracle and administrator duties are straightforward—promptly reporting widely disseminated true prices, executing functions in a timely fashion—there are no gains from the division of labor here, only economies of scope.

easy monitoring

Reputation systems and tokens within decentralized oracles are mechanisms to make its individual agents bear costs for misreporting. Yet a collusive subset within the oracle can reap 100% of the cheating benefits while bearing less than 100% of the costs, which are shared by all the decentralized oracle's stakeholders. This is obvious if some token holders related to a reputation system are not reporting, but still applies when we consider such systems need merely a majority at various oracle choke points. An agent with sole oracle responsibility playing a small set of similar games has a larger incentive to be honest than a fluid set of agents reporting on a wide variety of games.

Weekly reporting makes the SmartSwap Oracle's reputation easy to evaluate, in that the relevant data is concise. Prices used to generate payoffs are published in event logs, and the public source code shows how settlements are restricted so that the SmartSwap Oracle/Administrator cannot run these functions at unusual times or hack user margins. The weekly settlement reduces the size of the margin needed over a long investment horizon, reducing the potential upside for a cheater. The weekly settlement also reduces the number of interactions players need to manage the contract, in that players need to address their margin merely once a week.

Repeated game

The weekly settlement also changes the game from static to dynamic. The SS Oracle who posts prices to the contract is the only agent that can cheat but would not want to because it is not their best strategy in the context of a *repeated game*. Repeated play is essential in moving the game-theoretic equilibrium from bad to good, as demonstrated by the different equilibrium for the prisoner's dilemma when it moves from a one-period game to a sequence of one-period games (see Robert Axelrod’s *Evolution of Cooperation* (1982). Importantly, Axelrod's famous experiments involved a game with 200 iterations and consistency in several dimensions—comparable actions, equal-sized payoffs—so the distinguishing feature of a benign repeated game is not merely a continuation of play, instead that all potential cheaters are playing a similar game repeatedly.

Many coin tumblers or instant exchanges find making 1% on transactions dominates the feasible alternative of keeping all 100% until users figure out what is going on, though its users would have virtually no recourse. In contrast, Bitconnect was an obvious Ponzi scam because if it was honest, its present value was negative.

Contracts fees are focused on two necessary parties—Liquidity Providers and the SS Oracle.[[10]](#footnote-10) 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.[[11]](#footnote-11) 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.[[12]](#footnote-12) 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.[[13]](#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.

1. E.g., prior to commercial civil law there were courts along trade routes throughout Medieval Europe that enforced commercial laws (the *Lex mercatoria*), and its judgments were accepted not out of any legal authority granted by a state's monopoly on violence, but rather refusal would ruin one's business reputation and thus future revenue. [↑](#footnote-ref-1)
2. This can be seen looking at consumer and producer surplus, or the first and second welfare theorems. [↑](#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. This number is arbitrary, and experience will reveal the best parameter. This protects LPs as diversification lowers risk in the standard way--This factor can be adjusted, as experience will generate useful information on the best diversification factor. [↑](#footnote-ref-5)
6. See http://www.collegefootballwinning.com/blog/efficient-markets-in-sports-betting/ [↑](#footnote-ref-6)
7. this means pay 110 for a chance to win 100. In decimal odds this would be 1.909 for both teams, meaning each dollar bet generates 1.909 dollars for a win. [↑](#footnote-ref-7)
8. In a worst-case scenario, oracle token holders can pause up to two events while updated odds are being processed. [↑](#footnote-ref-8)
9. 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-9)
10. 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-10)
11. Technically, it generates a block number, but this then corresponds to a date-time. [↑](#footnote-ref-11)
12. 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-12)
13. ***[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)