OraclΞSwap

Derivative Contracts for Long-Term Investors

Eric Falkenstein
ericf@efalken.com

V1.0 2/28/2020

Abstract. OracleSwap is a cryptoeconomically-optimized suite of contracts oriented towards long-term investors and ETH holders. Counterparties take long or short swap positions in ETH, BTC, or the US equity market and transact at forward-starting market-on-close prices. Weekly settlement and payoff caps at required margins minimize necessary interaction. Liquidity Providers post two-sided offers, receive portfolio margining, and earn their income via funding rates and closing fees. It is based on a singular pseudonymous oracle providing prices for market-on-close orders, which allows it to create robust incentives and remain uncensorable. A working prototype is on the main Ethereum network, but this is meant as a template for creators in favorable legal jurisdictions.

Greater detail on the issues mentioned in this paper is in the *OraclΞSwap Technical Appendix*.

Contents

1 Introduction

OracleSwap is an oracle tied to a specific suite of Ethereum swap contracts. Users create long or short swap (aka CFD) positions that reference a unique Oracle contract that warehouses prices.[1] The initial prototype references ETH/USD, BTC/USD, and the US stock market (S&P500). An emphasis on simplicity reduces risk and makes the contract as straightforward as a vending machine, one-click to take liquidity with all ETH secure in a verified contract, with no emails or off-balance sheet processing: there are no tokens, wrappers, validators, relayers, etc.

Fewer agents and processes simplify the game, making it easier to align incentives and reduce costs. The only users in this contract are *liquidity providers*, *investors*, and the *oracle*. The only attack surface is via a fraudulent price via a conspiring oracle. We use a novel set of methods to minimize transaction costs and align incentives to solve the oracle problem. Its radical shift is to have a pseudonymous oracle tied to a specific contract in a repeated game with a form of mutually assured destruction: it is straightforward to parameterize the contract so that the cost/benefit ratio for cheating is 48/1.

Liquidity Providers (LPs) are paid via closing fees and funding rates they set. LPs post ETH as margin, allowing investors to take long or short positions that start at the next business day closing price.[2] Trades are priced at forward-starting prices, which eliminates price-impact and front-running, simplifies oracle monitoring, and eliminates the need for low-latency access. An LP is like a mini exchange in that their margin requirement is netted, and their positions are batched at settlement, scalable to thousands. The efficiency of cross-margining, combined with the efficiency of a single-agent oracle, allows OracleSwap to create a superior derivatives mechanism.

OracleSwap targets long-term investors wanting to take a position over weeks or months. While many are waiting for low-latency Layer-2 solutions, low latency provides nothing of value to a long-term investor: forward-starting VWAP execution is considered best practice execution for anyone but short-term speculators. Margins are settled weekly, and a position's Required Margin caps the PNL at a 3-standard deviation event so that investors need only attend to their positions once a week to avoid a forced liquidation.[3] If one's counterparty cancels, they can costlessly put on a replacement position as only the initiator of a cancel pays the cancel fee.

OracleSwap is like BitTorrent in that it is an open-source template for those who want to remain off the grid. Solidity contracts and a web front-end are downloadable at GitHub. As this took a couple of years to develop, extending and modifying its template is cheaper and faster than creating it *ex nihilo*. Various US regulations prohibit its citizens from facilitating a derivatives exchange or providing liquidity to an unregulated exchange. This prevents me or anyone I know well from administering this contract in any way, as my circle of friends and acquaintances work in the traditional highly regulated financial system. My legal situation is not universal, however, and there exist millions of people worldwide with the resources and ability to support this contract. The working version on the Ethereum mainnet is capped at two szabos (one szabo is one-millionth of an ether), and so merely provides a proof of concept as opposed to an economically meaningful mechanism for trading and investing.[4]

[1] Swap, also known as a total return swap, or CFD, contract-for-difference.

[2] The next 4 PM business-day price. All times referenced in this paper are USA Eastern Time, New York City time.

[3] The economic significance of this truncation for long or short positions is immaterial, at most 0.4% of notional, annualized.

[4] My motivations are mainly ideological, but I do think a product like this can help my long ETH position.

My inability to monetize this contract suite is why most prominent dapps related to financial derivatives are incomplete, missing either an oracle or an explicit derivative contract. Institutions such as Maker, Chainlink, Gnosis, and Augur are fundamentally like EOS and Ripple, superficially decentralized. These are all dead ends as they cannot deliver pseudonymity and permissionless access, and without these qualities are just inferior substitutes to standard alternatives.

The first problem of corporate dapps is that their superficial decentralization mechanisms make it *more* difficult to create proper incentives. For example, the Augur or Maker tokens may delay regulators and made their founders wealthy, but they are annoying, increase the attack surface, and make it harder to hold responsible parties accountable for their actions. More importantly, the recent bZx flash-loan exploit highlighted all these 'decentralized' platforms all have the ability to shut down their systems, and the standard institutions will hold them responsible for this control. If these companies ever created something as straightforwardly useful as an ETH/USD futures contract, governments will either shut them down or regulate them, just as Intrade, E-gold, and ShapeShift were. Their endgame is just the same financial system we have had for the past 100 years, where the government will whitelist, monitor, and have the ability to seize funds.

The essence of decentralization is not an explicit consensus mechanism, but competition. A pseudonymous user can develop a reputation that both holds them accountable and allows them to create brand value, all while remaining off the grid. In practice, the creator of the OracleSwap contract suite would act as its oracle, and oracle/administrators would compete for liquidity providers, who in turn compete for customers who wish to lever or short their ETH holdings as a long-term investment. A market of such dapps would make an outsider's attempt to censor a particular oracle as pointless as removing a PC from a peer-to-peer network. [5]

Blockchains like Ethereum provide the most secure property rights in history. If you own something—money, goods, your labor—you can exchange it, implying free entry by firms and free choice among consumers. This is what makes Ethereum so valuable, in that like Tor, it cannot be censored, facilitating entry and choice, but adds a secure payment system and vendor accountability via its immutable and transparent blockchain.

I also provide Managed Account contracts that allow ETH whales to delegate their ETH to managers who can attend to LP duties while providing the safety of a traditional managed account: the manager can only execute transactions with a specific OracleSwap asset contract, and cannot send ETH to outside accounts or contracts. This provides a way for large ETH holders to allow others to administer their LP duties securely.

The Coase Theorem highlights how low transaction costs and secure property rights are the foundation of efficient economic outcomes.[6] Novel blockchain properties like anonymity and immutability have created unfamiliar transaction costs that have stifled contract development. As the blockchain creates the strongest property rights in human history, these problems should be temporary. Financial derivatives are perfect candidates for smart contracts because they apply simple rules to easily verifiable prices

[5] 'Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.' Satoshi Nakamoto, Nov 7, 2008.

[6] It states that low transaction costs and clear property rights generate optimal capital allocations, regardless of the initial allocation of property.

determined in liquid markets. Conditional upon accurate prices, it is straightforward to create a ledger within a Solidity contract that is fair and secure.

2 Two Keys to Solving the Smart Contract Derivative Problem

2.1 No Limit-Order Book

One key is *not* to emulate a modern stock market. The standard is now the centralized limit order book, where users costlessly post, take and cancel limit orders. These markets are run on centralized databases and allow direct market access at under ten milliseconds. In contrast, interacting with an Ethereum contract is at least 1000 times slower and more costly, creating a classic example of Akerlof's market for lemons.[7] Compared to centralized exchanges, blockchain latency forces market makers to post bid-ask spreads so wide they cannot attract the casual traders needed to work well.

A standard central limit order book has three types of traders: noise, informed, and market makers. *Noise* traders do not affect the price because their order flow is random, which implies their trades are small (large trades require multiple autocorrelated transactions). *Market makers* provide instant liquidity by posting two-sided resting limit orders where their bid is below their ask price. *Informed* traders have an information advantage that predicts future order flow, which can come from inside information or something as straightforward as knowing they have many more orders to fill on the same side. In equilibrium, the market maker needs to make enough revenue off the noise traders to cover the losses generated from informed traders.

Higher latency subjects limit orders to greater adverse selection, where the resting limit orders supplied by market makers that tend to get filled are the bids that are too high or the offers that are too low. Greater adverse selection causes the market makers to post wide spreads compared to low latency markets, making the centralized exchanges the dominant choice for noise traders. For assets with extremely low volatility like stable coins, this problem is soluble because there simply is not enough uncertainty for adverse selection to create major problems, but that omits most interesting assets.

The higher latency exchanges are left with a higher proportion of informed traders, which in turn causes the market makers to increase their bid-ask spreads further to compensate for the greater adverse selection. These higher spreads disproportionately discourage the day (noise) traders, as they have short horizons disproportionately impacted by the spread. This positive-feedback loop causes markets to ultimately unravel, as the noise traders essential for limit order books disappear. There is no chicken-and-egg problem facing current blockchain-based limit order books; high spreads and low volumes are intrinsic to any high-latency alternative market.

For long-term crypto investors, the low-latency exchanges off the Ethereum blockchain come at a price. The lightly regulated exchanges have considerable operational risk, and legal recourse in the event of a dispute is improbable, making them imprudent for large sums. The highly regulated exchanges have low credit risk and are essential for converting between fiat and crypto, but they then put users back on the

[7] Akerlof's 'Market for Lemons' (*Quarterly Journal of Economics*, 1970) paper analyzes markets where parties with asymmetric information separate, and so the only offers have obvious negative value to potential buyers, and the market collapses (i.e., no trades).

traditional financial grid, removing anonymity, and have pathetic leverage and shorting capabilities per regulatory dictates.

OracleSwap eliminates the limit order book by using forward-starting, oracle-supplied prices to avoid latency effects while staying on the blockchain. For assets with liquid cash markets, price discovery is a problem already solved. This solution is inspired by value-weighted-average-price (VWAP) transactions, a popular equity trading tactic among long-term institutional investors. The time lag in trade execution does not inconvenience long-term investors, and their fill efficiency can be assessed quickly and easily. OracleSwap uses market-on-close orders, which are conceptually similar to VWAP but more straightforward and efficient given the liquid assets we are initially targeting.[8]

Most VWAP trading is done on a best-effort basis, where the VWAP broker merely targets the 'average price' and charges a fee of around 0.1 cents per share. This relationship puts the VWAP brokers in the same position as our oracle: the main reason they do not charge a dishonest price and make 30 times their fee in one day is the loss of future business. Brokers are kept honest because they are playing a repeated game where their actions are easy to monitor, and where the present value of honesty dominates a feasible dishonest—but legal—payoff.

By avoiding the adverse selection risk in limit order books, LPs neither endure this unnecessary expense, nor do they need to invest time and money minimizing it. The absence of limit order books also allows investors to avoid parceling out an order to prevent moving market bid-ask prices, so completing a trade at a fair price takes the same amount of time whatever the size. Lower indirect costs combined with portfolio margining make it easier for LPs to generate an attractive return at competitive rates for long-term investors.

[8] By spreading the execution price over a future time window, VWAP overcame the problems that prevented market-on-close orders from scaling. If one lists a less liquid asset or becomes very popular, the solution would be to switch from a 5-minute window to a VWAP over a longer time window, just as the CME uses an hour-long window for bitcoin futures settlement.

2.2 No Decentralized Oracle

> *“Ideally oracles are systems that are trustless, meaning that they do not need to be trusted because they operate on decentralized principles."*
>
> *Mastering Ethereum*, Antonopolous and Wood

The common idea articulated by Antonopolous and Wood is a major reason why Ethereum dapp development has been slow. Decentralization is a good thing, but like democracy, not at every level. A decentralized blockchain with contracting capability can give centrally administered dapps the essential benefits of decentralization without the considerable costs. A pseudonymous oracle embedded within a decentralized blockchain gives it protection from outside attacks and censorship. The other decentralization benefits, such as fault tolerance and conspiracy resistance, are easier to achieve via a centralized oracle.[9]

The benefit of market decentralization is that by giving individuals property rights, those with the most relevant information have the incentive to allocate resources towards their highest-valued use, the classic invisible hand of Adam Smith. While decentralization is necessary for a prosperous economy, this does not imply firms within such an economy must be decentralized, and very few are. In the same way, while a blockchain must be decentralized to preserve essential crypto principles, this does not imply oracles must be as well. The idea that oracles must be decentralized is a *category error*, assuming the part must independently have the properties of the whole.

Blockchain decentralization is essential at its highest level to protect against outsiders or insiders who would steal funds or peremptorily change the protocol, as a hard fork would simply replace the attacked one. In this way, even though there are only a handful of Ethereum mining pools, they are still fundamentally decentralized. Conditional upon a blockchain's core users demanding adherence to foundational bitcoin principles, it is trustless only in the sense that mining pools have the ability but not the will to implement a 51% attack. Anyone with the power to do so would be ruining a costly investment for modest double-spend. We trust miners to act in their self-interest. Our oracle is trustless in the same way.

Time-consuming mechanisms that make it seemingly impossible for agents to collude are not just inefficient, but naïve. Most functional dapps profess an ultimate aim of having a decentralized oracle, but then parenthetically admit they have a centralized one currently. A better objective is to make cheating possible but unattractive. Things that work on the blockchain—MakerDAO's oracle, bitcoin mining pools, Infura—all *can* collude maliciously, but their self-interest prevents this.

A single agent with sole non-transferable oracle rights and responsibilities has a stronger incentive to be honest than a fluid set of agents reporting on a wide variety of events that no one can easily monitor. Given permissionless access to the blockchain, a consensus mechanism is both unnecessary and inefficient; there is no reason to think that the key to creating an honest, accurate oracle is that they contain legions. Decentralization is only necessary at a higher level; below that, it is strictly unhelpful.

The game-theoretic field of *mechanism design* highlights two necessary conditions for a good dapp. First, there is a *participation* constraint that motivates players to want to participate in the oracle's game. A

[9] As noted in the technical appendix, collusion resistance is really about conspiracy resistance, in that no decentralized system is collusion resistant but this does not matter if they never collude maliciously.

platform may incent honest reporting, but the costs—not the explicit fees so much as the delay, complexity, and bid-ask spread—make 'not playing' the preferred choice. Secondly, there is an *incentive compatibility* constraint that the oracle achieves its best outcome by reporting truthfully. Incentive compatibility is key to low-cost enforcement of contracts, and historically this mechanism centered on reputation, not contract law administered by the state.[10] When agents have incentives aligned with their counterparties, we minimize policing and enforcement costs, which makes it easier to satisfy the participation constraint.

Decentralized oracles create several costs that have proved impossible to overcome. For example, a subset within a decentralized oracle can reap 100% of the cheating benefits while bearing less than 100% of the costs, meaning any minimum payment needed to keep the reporting agents honest must be inflated. Sybil attacks are only solved by implementing KYC or a whitelist, which removes anonymity and censorship resistance. The diverse set of use cases imply that the oracle's incentives will not be optimized for any specific contract they are servicing, and makes it harder to audit an oracle's history. Accountability is diminished.

Simplicity is essential for robust contracts because analyzing a game becomes exponentially complicated as the number of actions and participants increases. For example, to specify a general game in which n players each decide to either cheat, play honestly, or free ride on whatever everyone else is doing, 3^n scenarios arise. OracleSwap's oracle is the only potential cheater (n=1), resulting in two scenarios as there is no free-riding with one agent.[11]

To align the oracle's payoff space in a cryptoeconomically optimal way, one needs to create an oracle payoff such that the benefit of truthful reporting always outweighs the costs of misreporting. By having the oracle in total control, its revenue from truthful reporting is maximized; by being unambiguously responsible and easy to audit and punish, its costs from misreporting are fully born by the oracle; by playing a specific repeated game, the cost/benefit calculus is consistent each week; by giving a cheated user the ability and incentive to punish a cheating oracle, the cheat payoff minimized. These all lead to the efficiency of a single-agent oracle.

[10] 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.

[11] For most decentralized systems, free riding is the most common action, creating a dead-weight cost.

3 The OraclΞSwap Solution

OracleSwap minimizes costs and aligns incentives in the following ways:

- The only way a user can cheat is via a fraudulent oracle price creating a fraudulent PNL at weekly settlement. If a player sees a bogus oracle-reported price, they can and rationally should burn their PNL debit rather than send it to their counterparty, presumably an oracle sock-puppet. [12] A cheated player is incented to burn their debit when cheated, trivializing the exit scam payoff. Comparing an exit scam payoff versus the lost annuity of future oracle fees—even without the burn mechanism—makes honesty the oracle's dominant strategy.[13]
- Market-on-close prices supplied by the oracle eliminates latency problems, minimizes execution costs, and simplifies trading. Fill prices are taken from the oracle contract and reference the next business day close, and at weekly settlement the oracle generates a PNL factor for each potential start-day and end-day that is applied to a position. As low-latency is not needed, users do not need specialized hardware or software, and data-filtering algorithms can avoid spurious prices by sampling several exchanges at slightly different time windows.
- Oracle prices generate event logs and are easily monitored, as they require no adjustment.
- LPs set their own closing fees and funding rates. Funding rate differences between long and short positions allow them to balance their long/short exposure. Each LP gets portfolio margining, netting long and short positions. Economies of scale—as opposed to delusional token price expectations—encourage LPs to invest early.
- If the oracle or an LP disappears, players can recover their funds via a time-lock function.
- Players have 24 hours after the Friday oracle price update to cure their positions or burn their PNL if the oracle cheats. The LP must settle their book between 24 and 48 hours after the oracle settlement update. Forced liquidations are avoided by capping weekly PNL at the Required Margin (RM), which eliminates the need to monitor the market between weekly Friday settlements.
- The LPs and oracle are paid explicitly, which is cheaper than 'free.'
- All processing is done on-chain. The web front-end is merely a convenient alternative to Remix.
- All code is open source, including a downloadable web front-end and code to access the blockchain contract.
- There are no back doors that can freeze funds, time restrictions prohibit an evil oracle from implementing a surprise settlement, and users have a full 24-hour day to cure or burn upon settlement. The oracle's limited responsibilities--to update closing prices each business day--make it feasible for many oracles to enter, compete, and discipline each other.
- The single-agent oracle designed explicitly for this contract, as well as LP netting, combine to generate a large cost advantage relative to alternative derivative mechanisms.

[12] Burnt PNL is simply in limbo, inaccessible by anyone. Burning rather than contributing to some pool 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. See Bengt Holmström, 'Moral Hazard in Teams' (*The Bell Journal of Economics*, 1982).

[13] Such outcomes are 'off the equilibrium path,' in that it is never reached in equilibrium, but its existence is necessary for the equilibrium.

3.1 Use cases

Easier, cheaper, and more transparent for investors. All one needs is access to the blockchain and ETH. With market-on-close trade execution and no forced liquidations, one merely attends to the contract once a week to sustain a long-term position. Payoffs are formulated to generate a payoff that generates a linear USD return as a function of the USD price change, allowing investors to avoid the convexity risk in the BitMEX ETH perpetual swap. OracleSwap removes the costs involved in moving between ETH, BTC, wrapped ETH, tokens, stable coins, stocks, and USD: fees, time, crossing the spread. Transaction prices are the same regardless of size, side, LP or investor.

Diversification. There are many reasons people may not want to sell their ETH or BTC, yet diversification is the only free lunch in economics. Anyone with a significant amount of their wealth in BTC or ETH would be wise to allocate some of this capital to other assets. Those in countries that make it hard to access the world's largest equity market can find the SPX valuable diversification as well.

Leveraging ETH or BTC. OracleSwap provides a convenient way to increase one's crypto exposure by offering 2.5:1 leverage for ETH and BTC. Thus with 10 ETH, one can fund an additional 25 ETH notional long position or go short and generate a net short 15 ETH position. In contrast, MakerDAO offers 0.5:1 leverage, and given the liquidation risk requires significantly more excess margin. Plus, there are extra costs involved in buying ETH with Dai and then buying back Dai.

Hedging. With OracleSwap, one can eliminate their ETH portfolio's USD volatility while staying on the blockchain. As in many things, we get most of the benefits with a fraction of the effort needed for a perfect hedge (which would involve weekly transactions). For example, assuming ETH has an annualized volatility of 100%, one could reduce their net ETH's USD volatility by 85% while requiring an average of just one trade every three months. The Technical Appendix and the excel spreadsheet generate a more detailed example.

Attractive ROE for Liquidity Providers (LPs). Attractive investor fees are consistent with attractive returns for an LP. The marginal risk for ETH whales generated by being an LP comes from random net exposure as long or short investors arrive. An LP setting their funding rate to equilibrate long and short demand will accumulate random positions, which are uncorrelated with a long ETH position (e.g., the average correlation to an ETH portfolio of a sequence of exposures symmetrically distributed around zero, is zero). The net effect of cross-margining and the statistics of adding uncorrelated exposure generates Sharpe ratios above 2.0 over a variety of assumptions.

Extensions:

Additional contracts. The oracle contract can add readers, including other oracle contracts. This allows a singular oracle to add assets without having to also supply each with, say, the ETHUSD price. This allows an oracle to leverage its reputation onto many other off-chain assets. The contract could be customized for various regions with different day-ends as well (e.g., Europe, Asia).

Atomic Swaps. A reliable oracle would facilitate atomic swaps using ETH margining to bond transactors. Both players post margin in the atomic swap contract covering a 3-standard deviation event, and the ETH sender posts the ETH swap amount as well. For example, in a bitcoin-ether swap, one party promises to send 10 ETH. The next ETH/BTC price then implies the exact amount of BTC to be sent. If the ETH swap account is not withdrawn at the end of 24 hours, it would be uncertain if the bitcoin receiver failed to unlock the corresponding bitcoin hash time locked contract, or it was never sent. By assuming the *ex-post* loser, defined by the subsequent ETH and BTC prices, was at fault, and burning the loser's margin while releasing the other party's margin, creates an incentive-compatible atomic swap mechanism.

4 Contract Specs

4.1 Outline

OracleSwap consists of three Ethereum contracts: An Oracle, AssetSwap, and Book contract. There are no libraries. A single oracle contract services the AssetSwap contracts. The Oracle Contract's settlement price update generates a vector of returns that are pushed to the AssetSwap contracts. These returns reference different prices and use different leverage ratios, and are used when LPs settle their books each week.

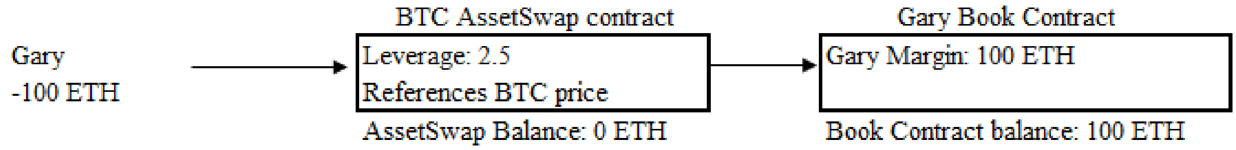
I also provide the front-end code used to access the Ethereum contracts on Github, so users can download this to their PCs for both privacy, auditing, and as a basis for developing their own OracleSwap-like contracts. There is also a python file that one can use to update their own oracles, though I do not provide APIs or web-scrapers, as any specific data provider would either censor or change their format in response.

A player's ETH is held in the book contract except when it is in the AssetSwap contract as a way station when withdrawing ETH. All balances and margins can only be accessed using a player's ethereum wallet (e.g., MetaMask, web3.js with private key).

Liquidity Providers (LPs) act as market makers, setting long/short funding rates. Investors take positions where the initial price will be the next end-of-business-day price, as recorded in the oracle contract. Settlement occurs each weekend, where players have at least 24 hours to cure their margins, and LPs have 24 hours to settle their books after that.

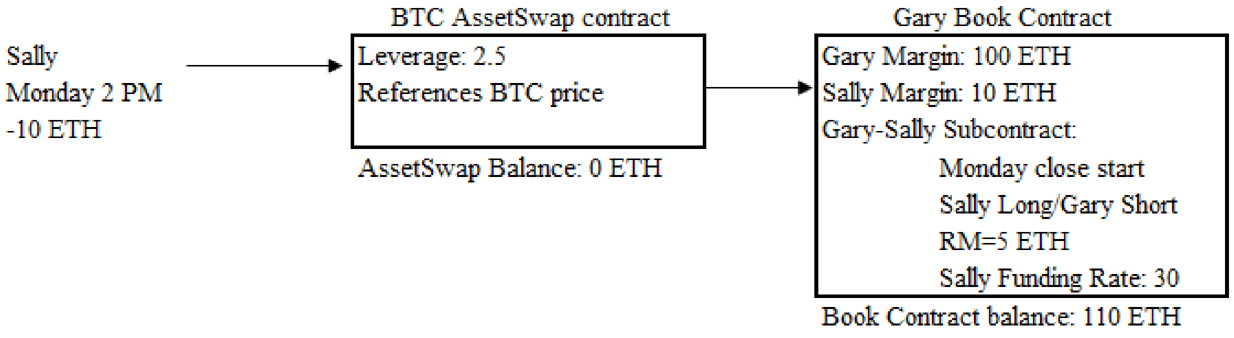
- Gary becomes a Liquidity Provider:

Gary sends 100 ETH to create a book through the BTC AssetSwap contract. He posts a minimum size of 3 ETH, and long/short funding rates of 30 and -20 basis points, respectively.



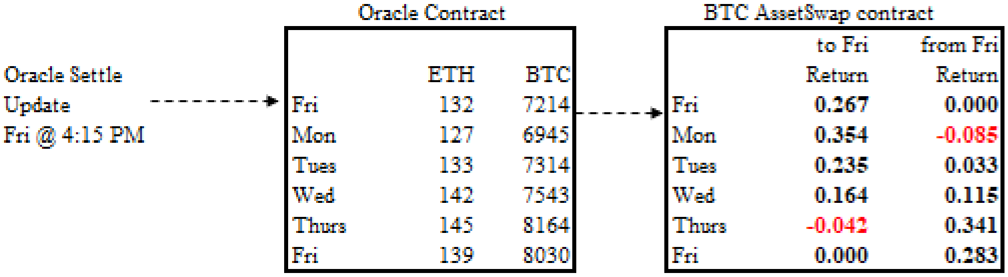
- Sally takes a long position in Gary's book.

At 2 PM Monday, Sally takes a long position with Gary, with an RM of 5 ETH. This corresponds to a notional of 12.5 ETH, or about $1800. The initial price will be the Monday closing price, and Sally will pay the funding rate 30 basis point lending fee over the life of their subcontract.



- Oracle sends settlement prices daily, ultimately leading to the Friday settlement price update.

At the Friday Oracle price update the oracle price update takes that week's prices and generates PNLs for subcontracts with RM=1, for all combinations of start and end dates. The oracle contract pushes these return arrays to the Asset Swap contracts during this settlement price update. No money is ever sent from or to the oracle contract.



Oracle Settle
Update
Fri @ 4:15 PM

Oracle Contract

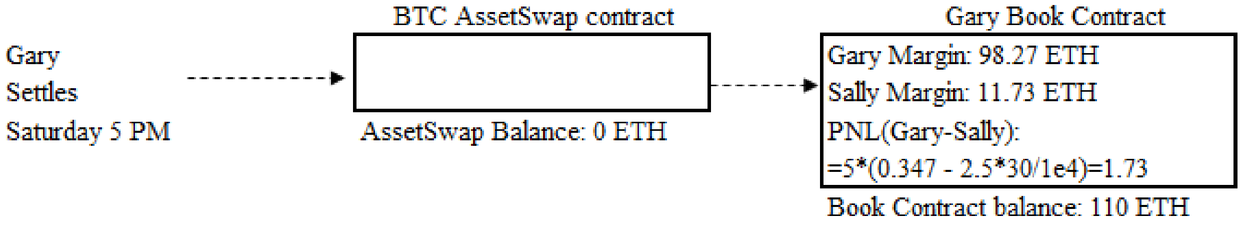
	ETH	BTC
Fri	132	7214
Mon	127	6945
Tues	133	7314
Wed	142	7543
Thurs	145	8164
Fri	139	8030

BTC AssetSwap contract

	to Fri Return	from Fri Return
Fri	**0.267**	**0.000**
Mon	**0.354**	**-0.085**
Tues	**0.235**	**0.033**
Wed	**0.164**	**0.115**
Thurs	**-0.042**	**0.341**
Fri	**0.000**	**0.283**

- Gary settles his book.

On Saturday, 24 hours after the Oracle settlement update, Gary has 24 hours to execute settlement. This applies the returns to Gary and Sally's subcontract and debits/credits their margins appropriately. Here we use the Monday-Friday return, apply the funding rate by scaling it by the leverage ratio, and multiply by the RM for their subcontract. It also checks that both have Total Margin > RM for their subcontract. No ETH is sent from or to the contract, but player margins are adjusted.



Gary
Settles
Saturday 5 PM

BTC AssetSwap contract

AssetSwap Balance: 0 ETH

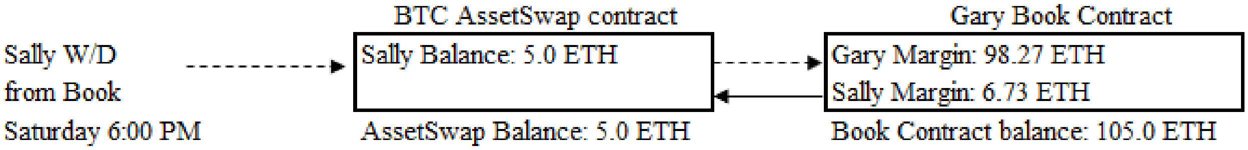
Gary Book Contract

Gary Margin: 98.27 ETH
Sally Margin: 11.73 ETH
PNL(Gary-Sally):
=5*(0.347 - 2.5*30/1e4)=1.73

Book Contract balance: 110 ETH

- Sally withdraws some of her ETH.

After Gary settles, Sally can withdraw all but her RM (after a cancel she can withdraw everything). If she withdraws, this takes two steps, first to the AssetSwap contract, where it is credited to her balance.



Sally W/D
from Book
Saturday 6:00 PM

BTC AssetSwap contract

Sally Balance: 5.0 ETH

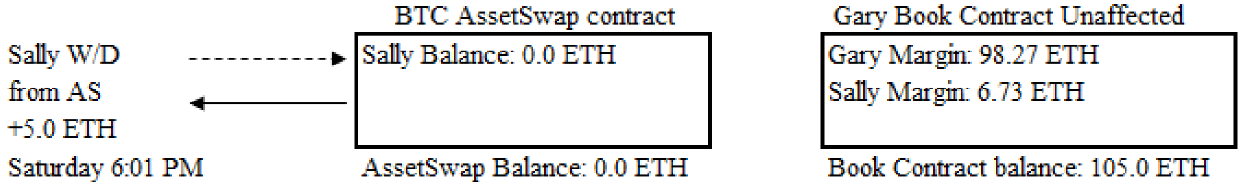
AssetSwap Balance: 5.0 ETH

Gary Book Contract

Gary Margin: 98.27 ETH
Sally Margin: 6.73 ETH

Book Contract balance: 105.0 ETH

ETH in the AssetSwap contract will sit there in perpetuity until withdrawn, and can only be withdrawn with Sally's private key.



Sally W/D
from AS
+5.0 ETH
Saturday 6:01 PM

BTC AssetSwap contract

Sally Balance: 0.0 ETH

AssetSwap Balance: 0.0 ETH

Gary Book Contract Unaffected

Gary Margin: 98.27 ETH
Sally Margin: 6.73 ETH

Book Contract balance: 105.0 ETH

4.2 Margin, Notional, and PNL

A subcontract is a bilateral agreement between a *Liquidity Provider* (**LP**) and Investor for a particular asset (e.g., SPX). It has a constant *Required Margin* (**RM**), which implies a notional amount via the *Leverage Ratio* and the ETH price.[14]

Unlike many crypto exchanges where investors choose notional amounts and then their leverage (e.g., 2x, 5x), which determines their margin, in OracleSwap, the required margin defines the position. This then implies an ETH notional amount, which then implies a USD notional amount via a changing ETH price. The leverage ratio is set so that the RM covers a 3-standard deviation PNL in the notional, indicating one should expect the next settlement to create a debit or credit of one-third of their RM. The initial investor margin of 1.5 times the RM is a simple way to make sure investors are prepared, as OracleSwap is designed for long-term investors who should be prepared for a couple of adverse settlements.

Those desiring lower leverage can overfund their margin without changing their position exposure. The player's risk is not affected by their actual/total margin ETH, as the RM caps their maximum liability at settlement. This simplifies margin requirements over time (it's the RM, always).

The weekly cash flow, the PNL (for **P**rofit a**N**d **L**oss), is the amount debited from one counterparty and credited to the other. For example, in going long BTC, implicitly, the trade is as follows: at open buy USD with ETH and then buy BTC with USD, at close sell BTC for USD, and then sell USD for ETH. This sequence is like when a US investor invests in a Japanese stock: she needs first to buy yen to buy the stock, and eventually sell the stock for yen, which she sells for USD. The contract does not do each of those transactions, but it prices them all to generate the weekly PNL, which perforce is in ETH.

This USD adjustment is made because users care mainly in the USD returns of their investments. If there were no adjustments for the USD price of ETH, as in the BitMEX BTCETH perpetual swap, to prevent arbitrage one must account for the ETH correlation with the asset and put this term into the funding rate. Given the high correlation between the ETH and BTC, as well as between the ETH and itself, this term is generally larger than any reasonable asset expected return (i.e., > 50% annualized). Short term traders may not mind, as over 8 hours a 0.2% cost seems inconsequential, but this is an intolerable extraneous risk for long term investors merely interested in an asset's USD return.

$$\text{PNL(long, investor)} = \text{RM}\cdot\text{LevRatio}\cdot\{\text{ETH}_0\cdot(\text{P}_1/\text{P}_0 - 1) - \text{FundRateLong}\}/\text{ETH}_1$$

As each subcontract implies symmetric PNLs to its counterparties, Investor and LP, we need only calculate the PNL for one party: $PNL^{investor} = -PNL^{LP}$. At settlement, every counterparty within an LP's book is credited or debited per their PNL, which does not change the book's total balance via the equality.

Example:

RM=10 ETH, Leverage Ratio=2.5, Funding Rate =0.2%, Taker long, Asset BTC.
Start prices: ETH=$145, BTC=$5800. End prices: ETH=$155, BTC=$5600
PNL(long, investor)=10·2.5·{145·(5600/5800 – 1) – 0.002}/155
Taker PNL = - 0.853 Ξ = – LP PNL. USD Notional at start of period= $3625=10·2.5·145
BTC USD Return= - 3.45%. Taker Return on USD Notional= - 3.65% = - 0.853·155/3625
Note that the difference in the asset return and the contract return is 0.2%, the Funding Rate.

[14] Leverage Ratios are 2.5 for ETH and BTC, 10 for the SPX.

4.3 Settlement and Default

LPs settle their books in the period 24 to 48 hours after the Friday oracle price update. This delay gives everyone 24 hours to cure their margins and avoid default if they have not already canceled. The LP settlement takes one function for books with less than 200 subcontracts, but above a certain point, a book must be settled in parts. This allows scalability. An LP should read the Technical Appendix for more detail.

At weekly settlement, if the PNL takes a player's margin below their RM, they are in default, and the subcontract is terminated immediately. A default does not cost the non-defaulting counterparty anything, as this just means the defaulter was unprepared for the next week, not that it did not have enough to pay their debit that week. Defaults are only due to negligence, as by Friday morning one has a good estimate of their impending PNL and cancel if they suspect they cannot cure their margin by settlement; after Friday 4 PM, players will know their PNL with certainty and have at least 24 hours to cure their margin.

4.4 Liquidity Providers

Liquidity Providers (LPs) are like mini-exchanges in that they can net their positions, giving them economies of scale. An oracle can also be an LP, in that we assume an LP or its customers is conspiring with the LP in the fraud scenario. LPs can also take a long or short net position so that its long and short positions are deliberately unbalanced. For someone with an existing long ETH position, competitive investor fees generate LP Sharpe ratios well above 2 under modest assumptions, making this an excellent way for ETH whales to supplement their income. LP economics are discussed in detail in the Technical Document.

To become an LP one posts the following single Ethereum transaction:

- Choose asset: SPX, ETH, BTC
- State a minimum RM for investors
- Set long and short funding rates, closing fee
- Post ETH margin ≥ 10 times their minimum RM

Any amounts taken by an investor are locked in until the next settlement. At any time, the LP can withdraw whatever margin has not been attributed to their Required Margin by an investor, and they can change their minimum RM, funding rates, and closing fee. At each settlement, the LP's active positions are netted for calculating the LP's RM within any AssetSwap contract, and so LPs must anticipate the new netting and PNL to avoid default. An LP can use the same address for BTC and SPX contracts, but these would be independent books, with no cross-margining across different assets.

LPs are responsible for the weekly settlement of their positions as failure to settle will allow any investor to receive a penalty payment from the LP as an incentive and put the book into default allowing everyone within that LP's book to redeem their margins immediately. Settling involves a single function while their book is small, under 200 positions, but is scalable to thousands. Anyone can settle the book—there is no risk to doing this—so an investor who sees the LP not completing the weekly settlement can simply do it themselves.

4.5 Taking a Position

To take a position, one does the following in a single transaction:

- Take a side, long or short
- Set the RM for the subcontract.
- Send ETH ≥ 1.5·RM

When an investor takes a position, the counterparties are committed to a swap from the next-business-day close to the second subsequent settlement (8-14 days). As a PNL standard deviation is about one-third of the RM, investors should have some excess margin available if they expect to invest for multiple weeks, and the initial requirement of 1.5 times the maintenance margin reminds them of this (the 50% excess margin can be immediately withdrawn).

A subcontract uses the subsequent oracle-reported closing prices as its starting price. These are taken on the New York Stock Exchange business days at 4 PM.[15] For example, a contract taken Monday at 3 PM will have its initial fill price taken on Monday close; a contract taken Monday at 6 PM will have its first price use the Tuesday close. The AssetSwap contract determines this by reading the Oracle contract. The funding rate and close fee at the time of trade inception are constant over the life of the position, regardless of whether the LP changes it later.

Investors cannot take during the 4:00 to 5:00 PM. This restriction prevents gaming the latency between the 4 PM prices and when those prices are reported to the oracle. New positions are also prohibited during the settlement period, between the Friday oracle price update and the weekend LP settlement that occurs between 24 and 48 hours after the Friday oracle settlement update. This makes it easier for LPs to determine their net required margin when settlement is executed.

After the first week, a rolled-over contract will use Friday-to-Friday closing prices. Investors and LPs can fund their margins at any time. They can withdraw Excess Margin at any time except the Settlement Period, encouraging players to burn a debit PNL rather than subject themselves to another settlement with an evil oracle, which encourages oracle honesty.

4.6 Closing a Position

A standard cancel before the Friday oracle contract update terminates the subcontract at the subsequent settlement. After the LP's book settlement, the investor of a canceled contract must redeem their position to move their entire margin from the LP's book contract to the AssetSwap contract, where they can then withdraw it to their personal address. This two-step process protects user funds, and also saves on gas in the weekly book settlement. Investors can cancel using intraweek prices (e.g., Monday), though the LP must have sufficient excess margin for this. Canceling intraweek still requires waiting until the weekly settlement to retrieve their funds, and the canceller pays the maximum LP closing fee.

Investors cannot cancel in their first week. This is because new subcontracts are processed differently in the settlement, and also because we want to encourage long-term investors. LP's can unilaterally cancel all their subcontracts and close their book with a 28-day notice, allowing all takers to exit at the first settlement after this date is toggled at no cost. This feature is available because if a large LP had hundreds of subcontracts, canceling positions individually would be daunting. In such a case, takers can cancel at no cost, and four weeks is sufficient time for investors to find new LPs.

[15] Stock exchange holidays are scheduled three years in advance, though occasionally there are *ad hoc* holidays, such as when ex-President Bush died and markets were closed on Wednesday, 12/5/18.

4.7 Funding Rates and Fees

Liquidity Providers in most markets are paid in large part via the bid-ask spread. OracleSwap has no trading at maker-supplied prices, so our makers, the LPs, must be paid differently. LP revenue will come from the *funding rate* and a closing fee. LPs choose the funding rates their long and short investors pay and can change them at any time; however, any subcontract uses the funding rate at trade instantiation for its duration.

It is important to note it consists of two components, the rate to compensate the LP, and the basis rate to equilibrate long and short investor demand.

$$FundingRate_{Long} = LP_{fee} + Basis$$
$$FundingRate_{Short} = LP_{fee} – Basis$$

A swap referencing a cash price must adjust for the *basis* one sees in futures/forward market curves. The basis accounts for the opportunity cost of money (e.g., interest rates), and the costs and benefits of owning the asset outside of its price appreciation (e.g., storage costs, dividends). If there were no basis, one could invest cash in money markets, go long a futures position, and make the same return as investing in the asset plus the interest rate earned in money markets, which is not an equilibrium.[16] A basis is charged symmetrically, subtracting from the long return and adding to the short. The LP will implicitly set a basis when setting different funding rates for long and short takers to equilibrate their exposure.

While it is useful for investors to understand the effects of interest rates and other factors on the basis, ultimately, this differential is determined by supply and demand. OracleSwap's funding rates are capped in absolute value at 1% per week for ETH and BTC, and 0.25% for SPX (a 1-week return standard deviation is about 10% and 3%, respectively)

Creators of new OracleSwaps will choose their own fees, but the following are useful points of reference, as they were calculated with regard to LP profitability, which will vary by leverage.

Open fee: 0%.

There is no open fee. Further, there is no bid-ask spread. It is useful to remember this because even though some exchanges charge only a close fee, there is always the cost of the bid-ask spread, and if one has a large position, trade impact. These non-explicit costs are present on both sides of a trade on almost every exchange other than OracleSwap.

Close fee: 1.0-2.0% notional for crypto, 0.25-0.50% for SPX.

The close fee is set at trade instantiation based on the closing fee listed at the time of trade in the LP's book. The close fee consists of a fixed oracle fee and a variable LP fee. The oracle fee is 1.0% of notional for ETH and BTC positions, and 0.25% for SPX positions. The LP can set their closing fee anywhere from 0% to 1.0% for cryptos, 0% to 0.25% for the SPX, which is then added to the oracle's fee to generate a total closing fee. An investor canceling their position pays this directly when executing a cancel, not through a deduction of their margin.

If the LP cancels, they pay 2 times the base oracle rate, which goes entirely to the oracle. For intraweek cancels, those that apply a closing price before the settlement day, investors pay the LP maximum closing rate regardless of their subcontract's initial closing fee. This premium is to compensate the LP for the

[16] Other factors that affect the basis are discussed in the Technical Appendix

impact on her Required Margin. LPs cannot cancel intraweek. Thus LP cancels, and intraweek investor cancels, pay a total close fee of 2.0% for crypto, 0.5% for SPX.

Funding Rate: -1% to 1% weekly for crypto, -0.25% to 0.25% weekly for SPX.

These are purely market-driven rates, as LPs set these rates to balance their books and compete for investors. Competition and scale should reduce their average size over time. This rate is a composite of a fee for the LP's service and a basis rate that equilibrates supply and demand. As the basis is a symmetric charge from long to short, the funding rate could be negative (implying, a credit for the investor). Any subcontract has a fixed funding rate for its duration.

Default fee: ½·RM (i.e., 5%, 20% of notional).

If a player defaults, they are charged ½ of their RM. Players can never withdraw margin below their RM, so a default can only occur at the weekly settlement. The default fee is sent to the oracle to make users more inclined to burn rather than default, in that a cheating oracle would get the fraudulent PNL and the default fee if not burned. As players have 24 hours to cure their margin and should cancel before the Friday oracle update if they foresee an inability to cure their margin, any default would be due to negligence. If a player has less than ½ RM in their margin at default, whatever is there constitutes the default fee.

Burn fee: ½·RM.

This fee should never be invoked because the oracle is incented to be honest, and a dishonest oracle price is the only rational reason for an investor to burn. However, a player who thinks the oracle is cheating can pay a fee of ½ of his RM to preclude his counterparty—presumably an agent of the oracle—from receiving its PNL debit via fraudulent pricing. This fee is applied via a payable function and is effectively burned to remove strategic implications from some party that might game this system (the burn amount is not credited to any user's margin, inaccessible). After the settlement at which the burn is applied, the player margin is fully redeemable (i.e., instead of being debited ½·RM upon redemption in default, the user pays ½·RM to burn, but then is not debited at redemption).[17]

4.8 Managed Accounts

The managed account contract allows an ETH whale to delegate their OracleSwap trades to a third party. The investor' can remove the manager at any time, while the manager cannot remove the investor. The manager has the right to interact with various OracleSwap AssetSwap contracts, either as an LP or investor. A fee calculation method applies the manager's fee to the assets in the various OracleSwap contracts, and this fee then accrues to the manager, and then only the manager can withdraw these ETH.

The investor and the manager have the ability to transact with the AssetSwap contracts, so an impatient investor is never frozen out by manager activities. The manager can only interact with AssetSwap contracts specified by the investor. The manager can only send ETH to these specified AssetSwap contracts, so the only way for the manager to steal the investor's funds would be if the manager conspired with the oracle.

[17] Any excess payment for a burn or cancel goes into the player margin, available upon redeeming.

5 The Oracle

5.1 Duties and Restrictions

The oracle has just one responsibility: updating prices to the oracle contract between 4 and 5 PM on NYSE business days[18] This creates a set of business-day prices that determines the PNL applied at settlement. While prices reference a 5-minute window after 4:00 PM, this gives the oracle an hour to respond to computer issues or unanticipated network traffic.[19] The settlement price update generates a vector of returns that are pushed to the AssetSwap contracts, and this vector is then used when LPs settle their books.

There are several restrictions within the contract that prevent oracle mischief.

- Oracle contract price updates cannot occur for at least 20 hours after the previous oracle price update
- Oracle contract settlement updates can only occur when the prior oracle update flagged that the next oracle update will be a settlement update.
- The book contracts can only be settled once per week.
- Players have at least 24 hours from Oracle settlement update to cure their margins or burn before the LP settles her book.
- No one has the ability to freeze accounts; only settlements transfer ETH between margins.
- If the oracle disappears, which would prevent settlement, all players can withdraw their ETH if the contract has not been settled for 10 days.

The negligible oracle requirements imply an oracle with a very light footprint. The oracle's main job is to automate scripts that pull data, and as these are not real-time prices, one does not have to pay for low-latency data feeds, but rather can use stale data (5 to 15 minutes old) that is easily accessible.

Our oracle uses the median price of several exchanges, creating a robust and unbiased end-of-day price for long-term investors. Those creating Asset swaps for less liquid assets should use a longer time window to minimize the gaming potential. Our oracle has multiple servers in different geographic regions doing approximately, but not exactly, the same pull. These back-up servers query the Oracle contract to see if prices were updated, and if not, sends again with a higher gas fee.

A failure in one of the feeds is inconsequential, and by recording constituent prices, the oracle can identify a failed feed or computer and rectify the problem at a leisurely pace. As server space costs only $10 a month, the software needed to run data scraping programs are open source, and oracle updates are once a business day, your average university student has the resources to be an oracle.

A fraudulent price should elicit a burn, and as burns are costly, they show someone cared enough to pay to punish the oracle. A truly fraudulent price report by the oracle should discourage any future players, but as such allegations are uncensorable, further investigation is recommended as the burner could be

[18]. There are about 9 New York Stock Exchange holidays, and if they occur on a Friday, we will use the prior Thursday as the settlement date. Holiday-shortened days will use the 1 PM closing stock market prices but the 4:00 PM ET crypto prices that day.

[19] As prices can only be posted once every 20 hours, a duplicate price posting would simply fail. For those adding a less liquid asset, a longer time-window mitigates gaming risk.

mistaken or mischievous. Burns and oracle price updates generate event logs, and users can access a query for these events via the web front-end.

A good oracle should be developing new features and adding assets. Asset swaps are one obviously useful extension in that a similar incentive mechanism can facilitate atomic swaps between ETH and BTC using Hashed-Timelock Contracts. Another useful service would be to provide a 3Box chat so that users can communicate with a provable connection to the oracle and LPs, all while maintaining pseudonymity.

5.2 Oracle Incentives

The oracle owns a non-transferable annuity of closing fees from OracleSwap contracts, and comparing the value of this annuity to a potential cheat payoff shows the oracle's dominant strategy is to be honest. Reducing the oracle to a single agent makes this easier because this maximizes the percentage of fees going to the oracle agent and makes accountability unambiguous.

While the oracle can also be an LP, it is best the oracle encourage others to also be LPs. This is because it increases the costs of cheaters. Investors should prefer OracleSwap contracts where there are several LPs that appear independent

Each AssetSwap contract is hardcoded to the oracle contract, so this is the sole source of prices used in generating subcontract payoffs throughout its life. The only attack vector involves the oracle posting fraudulent prices, where an evil oracle is conspiring with one of the counterparties, say by reporting an actual -3% return as a +7% return, effectively stealing 10%. Presumably, a cunning evil oracle would remove the middleman and be that counterparty using a different account it controlled; an evil oracle in practice is an evil oracle/counterparty sock-puppet.

The key to an honest oracle is that it plays a repeated game where players can quickly and meaningfully react to dishonest play.[20] The oracle's incentive structure is like that in the iterated prisoner's dilemma, where a multi-period game moves the dominant strategy from the suboptimal equilibrium where both parties maximize their one-period payoff by not cooperating, to the optimal equilibrium where parties maximize their payoffs by cooperating. In evolutionary biology, this shows up in *reciprocal altruism* and illustrates how cooperation emerges out of long-run self-interest, as cooperating players out-compete non-cooperators.

5.3 Burning Motivation

The game-theoretic concept of *common knowledge* is that two players both know some fact, they both know they both know that fact, and both know they both know they both know the fact, *ad infinitum*. Using this reasoning, most rational players will always burn when cheated, where a burn means that the burner's PNL debit will not be paid to the creditors.[21] While the reasoning is explained in full in the Technical Appendix, the gist of why burning is the optimal response to a cheat is the following.

If the oracle goes rogue and decides to cheat, a player who has not canceled must weigh the costs of burning with the costs of continuing. If the cheated player continues, at the subsequent settlement the evil oracle will rationally infer, via common knowledge reasoning, he can cheat them again next period by at

[20] For example, see Robert Axelrod's *Evolution of Cooperation* (1982), which highlights the value of repeated games in creating cooperative outcomes.
[21] While the ETH remains in the LP book contract, it is unobtainable by anyone.

least the burn fee, as the player revealed they are willing to tolerate such a sunk cost to avoid paying this fee. Any player with an overfunded margin, who would continue if they do not burn, will find it cheaper to pay to burn rather than continue. Any player with margin balance, after the PNL attribution, is between ½·RM and 1.0 RM will find burning and default cost the same, but here burning has the benefit of preventing a cheating oracle from gaining their ETH, and also prevent the oracle from receiving the default fee, which makes it preferred for anyone who dislikes being cheated. Those with less than ½·RM in their margins would find default cheaper than burning, though, whatever is in their margin for the default fee, in addition to the fraudulent PNL, would go to the oracle, which should motivate some players to burn out of righteous spite.

As it is prudent to overfund one's margin to save on gas and given the prevalence of overfunding margins by 300% on MakerDAO, we expect most players will have an overfunded margin. Though this exposes users to greater risk in the event of a cheat, it actually lowers their risk collectively, in that it signals to the oracle that if he goes rogue, he should expect all those accounts to burn, which then eliminates the oracle's cheat payoff.[22]

As all investors transact with an LP, this makes the burn attribution nontrivial but straightforward. Burns are allocated pro-rata against the other side: if burning parties represent 80% of the afflicted side, then each player on their counterparty side party gets only 20% of their calculated PNL credited to their margins.[23]

The burn fee must be high to avoid griefing, and so the choice should require enough pain to prevent frivolous burns harming innocent players. A burn generates an event log highlighting the date of the fraudulent prices and should make it easy for outsiders to assess, though a conscious choice to burn is costly and pointless given an honest oracle. A true cheat destroys future oracle revenue, as it would be irrational for one to transact with an oracle who has ever cheated, and these are easy to see. This is unlike many other oracles, where a cheater is presumed a rogue anomaly; our Oracle has no plausible denability for misstating prices.

To generate a scheming oracle's cost-benefit analysis, we compare the potential benefits of an exit scam with the costs. The lost revenue comes from the expected closing fees of the subcontracts. 1.0% of crypto notional and 0.25% of SPX notional translates to 2.5% of the RM given leverage. If we assume subcontracts roll over every two months, and the oracle expects six closing fees, this implies the oracle expects a 15.0% dividend on the gross RM in the AssetSwap contracts. Using the Gordon dividend discount model, a discount rate of 10% and a growth rate of 5% imply a present value of $3 \cdot RM_{gross}$, where RM_{gross} is the total amount of RM across all the OracleSwap AssetContracts and their LPs.[24]

The positions in the oracle's scam would probably be less than one-fourth of the outstanding positions, in that the contract would have to be popular to generate enough users for a valuable payoff. That is, if Oracle/Alice were 100% of one side, this would imply few users. This suggests the maximum RM aligned with the evil oracle would be at most around $\frac{1}{4} \cdot RM_{gross}$. Given we should expect at least ¾ to burn their PNL rather than continue, this takes the scam payoff down to $\frac{1}{16} \cdot RM_{gross}$.

[22] With zero excess margin, a cheat that takes the entire RM implies the default fee would be zero, less than a burn fee of ½ RM.

[23] The LP's revenue reduction is netted, so that if long 100 and short 50, and the short side burned 40%, this would affect the LP's net long position of 50, not the gross.

[24] PV=dividend/(discount rate – growth rate).

Under very modest assumptions, an amoral oracle would find it rational to use their oracle revenue to further other schemes, because even evil oracles prefer more money to less (3RM > $\frac{1}{16}$ RM). While burns should never happen, the option makes the incentive compatibility of this contract more robust.

It is important to remember the oracle's duties are minimal. Few duties are essential because many responsibilities would imply a conspicuous oracle that would be more prone to outside attack. As its job is basically to update prices daily at a set time, which can be scripted, the oracle's main job is to monitor its various APIs and data-scraping programs for changes in data formats. We do not have to consider the scenario of a burnt-out oracle, overwhelmed with or myriad responsibilities, who finds the game too tedious for reasons outside of the monetary cost-benefit analysis.

As a practical matter, initially expected growth would be an order of magnitude greater than 5%, making the value of the annuity much greater than 3·RM. A trusted oracle could support many other assets as well as atomic swaps, etc. Yet as the contract matures and provides a greater potential amount to steal, the proportion of non-complicit users—representing lost future closing fees—would increase, increasing the present value of its oracle fee relative to a cheat payoff. Many dapps generate almost zero revenue, and the only thing keeping reporters and administrators honest is their belief in exponential growth that will translate into token appreciation, which is both delusional in most cases, and unsustainable were it to occur.[25] In contrast, our oracle has sufficient incentives in a steady-state equilibrium. OracleSwap is a long-run incentive compatible mechanism.

5.4 Parasites and Mimics

The oracle contract stores closing prices that are accessible via a private function that only the OracleSwap contract can access inside the Ethereum Virtual Machine (EVM). This restriction prevents parasite contracts from using the oracle contract while not paying the oracle. While all state variable data in this contract is visible outside the EVM (and, oracle price updates generate event logs), the data recorded by the oracle contract is trivial to discover elsewhere anyway. The oracle problem is not technical; it is strategic; its data is only valuable in the context of a smart contract that is forced to use these prices. A parasite contract user would have to trust the parasite contract's oracle to copy this information truthfully outside the EVM, which is the main problem, and cost, of an oracle.

The contract's source code is available for all to copy, modify, and deploy as anyone sees fit. Simply copying the code is easy, and the main costs are automating scripts that pull prices, update the oracle contract, and creating a distinctive user interface. We caution new oracles that manually updating the data may seem feasible, but this is not sustainable so they must automate an oracle-updating protocol. This includes an error-checking algorithm and having back-up computers online in different regions.

The downside to a low cost of creating an OracleSwap spin-off is typical to all thriving markets. With anonymity and without a high fixed cost of entry, a hacker has little to lose by abusing misplaced trust in look-alike contracts. A few subtle code changes can give them a backdoor to contract ETH balances. Therefore, while we encourage imitators, we also advise users to be wary of them. Most importantly, if someone presents a mechanism that emphasizes zero costs, they should not be trusted because either they are stupid or lying, as there would be insufficient incentive for the oracle to be honest. For honest oracles, the best signals include adding thoughtful content and being diligent on updating prices, as this implies

[25] If the primary incentive is above-average token returns, that cannot persist, and when this becomes obvious the incentive to be honest disappears.

one has an appreciation of the long-term value of crypto, and a long-term focus that implies honesty dominates cheating.

6 Conclusion

In *Star Trek Next Generation*, the Borg are cybernetic organisms linked in a hive mind. They co-opt the technology and knowledge of other alien species by injecting nanoprobes into their victims, just as the Cordyceps fungus turns insects into living zombie-slaves. These newly assimilated cyborgs say things like 'resistance is futile.'[26] Similarly, many wealthy crypto entrepreneurs find themselves having to choose between admitting their corporatized product is unviable or sacrifice various crypto principles to facilitate continued faith among initial investors.

These compromises seem innocuous because many are unclear on the true value of crypto, which is still primarily valued for its potential. Is it the blockchain? If it is the blockchain, is it transparency or decentralization? If it is decentralization, what is its essence? I believe Ethereum's long-run value requires no compromise on any of the following principles: transparency, immutability, pseudonymity, confiscation-proof, and permissionless access.

The Best of Both Worlds was the title of one of the early Borg episodes, alluding to a newly assimilated Borg delusion. Many crypto developers aim at having a large presence on and off the grid, but a dapp that is 'fully licensed' is just an inefficient and convoluted mechanism to do what we can already do, like Dentacoin. It does not have more value because it exists on and off a blockchain, rather, zero value. Dapp development has been slow because corporate crypto companies are waiting for someone to solve the problem of servicing people who want to remain off the grid while satisfying institutional demands. There are business models where this makes sense, such as crypto-fiat exchanges, but these are exceptions.

OracleSwap embodies Satoshi's vision which is independence from standard institutions. Its oracle retains anonymity on the blockchain, making it immune to censorship, yet unlike merchants on the Tor network can be monitored and held accountable due to the transparent and immutable blockchain. This is what makes Ethereum so valuable, in that dapps do not need their own decentralized consensus mechanisms, which is fortunate because they are very costly. Prices used to generate OracleSwap's PNLs are recorded in the oracle contract's event logs, which need no parochial adjustment to compare to exchange prices.

A set of competing OracleSwap contracts is more efficient than generalized oracles designed for unspecified contracts, or generalized trading protocols designed for unspecified oracles. Before they were regulated, many coinshifters found that making 1% on a transaction was better than making 100% on a cheat because of the present value of future transactions. This was in a market where reputation was difficult to measure as there are no clear records of cross-chain transactions that can prove a cheat, so reputation was inferred via unverifiable anecdotes one reads in chatrooms. A simple contract tied to an oracle that is 'all-in' creates clear and unambiguous accountability, generating the strongest incentive for honest reporting.

Investors can create asset exposure that is difficult to get elsewhere while staying on the blockchain. By capping the weekly PNL at the required margin, investors need only attend to their positions once a week and maintain a long-term position, and the extreme events that are truncated are economically insignificant. Forward starting prices help both the LP and investor, in that they remove any need to

[26] 'If you believe the government cannot stop any cryptocurrency, you're deluded.' Craig Wright

invest time and money into continuous market monitoring and low-latency access. Portfolio margining allows LPs to generate an attractive return while giving investors competitive rates, and managed accounts allow large ETH holders to trustlessly delegate LP duties.

There are significant gains from trade available in finance because of regulations designed to prevent competition under the pretext of protecting the public. Offering financial asset protection is a good business or government service; mandating protection is a racket. Ethereum derivative contracts are alluring because they are the application of straightforward rules to objective and widely disseminated asset prices.