OraclΞSwap Technical Appendix

Derivative Contracts for Long-Term Investors

Lorenzo Botticelli

V1.0
7/3/2019

This document complements the OracleSwap White Paper by providing an in-depth explanation of concepts and features in the OracleSwap contract.

Contents

1. Decentralization and Oracles

The resiliency of decentralized peer-to-peer networks like Tor compared to the fragility of the centralized Napster motivated the creation of bitcoin. This resiliency is nicely described here:

> "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 1818 Zug, Switzerland

A system that competes with fiat currency must be decentralized because governments know competition will limit their power. For example, E-Gold allowed pseudonymous parties to send payments to each other, and had 5 million accounts at one point. As it was operated by two well-known American citizens and headquartered in Florida, the company was prosecuted in the years just before bitcoin was released, their directors tried and convicted of transmitting money without a license. 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.

A contract warehousing prices is *attack resistant* merely by being on the blockchain. As long as the agent supplying the prices is pseudonymous, running virtually costless scripts on various remote servers across the globe, there is little that anyone can do to stop it. Then the question becomes, what are the costs and benefits to this oracle being, in effect, a single agent?

Consider *fault tolerance*, which protects against accidental errors and involves methods such as using several price feeds and applying a function to filter out bad prices. As a rule, blockchain contracts should move as much processing as possible off the blockchain, and this task can easily be done by a single agent who applies such an algorithm on several independent servers, which then reports a final, filtered, validated result to the blockchain. Error correction off the blockchain is much more efficient than doing this on the blockchain, and for algorithms targeting objective price data the fact that they were originally designed by a single agent does not limit its efficiency. This is a straightforward problem that does not require decentralization.

The bigger problem is making sure that those with power to do harm have the correct incentives. In the Bitcoin White Paper, Satoshi argued that any agent *with the ability* to double-spend 'ought to find it more profitable to play by the rules … than to undermine the system and the validity of his own wealth.' Thus at inception Satoshi knew that at scale malicious collusion would be feasible, but perverse. Currently blockchains like Ethereum and Bitcoin require substantial specialized mining equipment that raises the attack cost 10,000-fold over the direct hash-power cost of such an attack, in that such a move would not just be the direct electricity cost, but more importantly wipe out the value of their investment. Thus, while Bitcoin or Ethereum mining groups can collude and control 51% network control, it is not worrisome

because it would not be in their self-interest to engineer a double-spend given the cost of losing future revenue.[1]

The term *collusion resistance* is often mentioned as a primary decentralization virtue. A better term would be 'conspiracy resistance', because if agents within a network can collude but never do so maliciously it is not troubling. For example, in the Sep 2018 Bitcoin inflation bug, or the Fall 2016 Ethereum DDoS attacks, BTC and ETH miners effectively colluded to protect their blockchains, not subvert it. This spring the head of Binance basically admitted that a blockchain roll-back was possible, but the bitcoin community mocked him because this was obviously not a prudent move within the context of the long-term self-interest of the bitcoin miners.[2] The system is still decentralized because mining pools are replaceable on a global scale. To the degree mining pools might exert their agency against the wishes of the blockchain community in a centralized fashion they will be piloting a costly and futile hard fork.

Anticipating this, mining pools have very little power to change things, though they are good at preventing change. Ethereum in general and Vitalik Buterin in particular are imperfect. Yet the Ethereum project has the best combination of of centralization and decentralization: leadership pushing fruitful innovation (e.g., PoS, Sharding), but enough decentralized power such that any one person, inside or outside Ethereum, can force their will on the community of users.

A viable oracle cannot have an attack surface, as the E-gold (arrest), Intrade (closure) or ShapeShift (submission to traditional finance protocols) scenarios are inevitable if they ever become popular. The novelty of Augur and Gnosis will protect them only while their markets are trivial. If they ever become successful their principals will be given the ShapeShift directive: apply KYC or be prosecuted. Similarly, for oracles that attest to the authenticity of the APIs they using, these also have clear attack surfaces. either the data provider will object, or regulators will force them to remove access. Reuters, Chainlink, or Oraclize cannot be underlie any viable blockchain derivative contract.

The key bitcoin innovation was introducing proof-of-work to remove the need for a *trusted* third party, why the term '*trustless'* is often attributed to a decentralized network. With proof-of-work it is not impossible to double spend, just imprudent, so the bitcoin blockchain still relies on trust, but not that agents will be good, just rationally self-interested. The essential condition for ensuring this sort of trustlessness is only incidentally related to decentralization in that within a competitive proof-of-work system it is not in one's self-interest to cheat regardless of the size of the collusion.

While blockchains must be decentralized to prevent the Napster endgame, any oracle residing on the blockchain administered by anonymous agents can avoid censorship. Then the question is whether it is most efficient to generate truth-telling incentives via decentralization or a single agent. Consensus mechanisms used by decentralized oracles have adjudication processes and scoring functions for its reporters, but assuming a collective is easier to incent with honesty than an individual but ultimately it is about making sure it pays to be honest at all times.

The focus on various methods to prevent malicious reporting within decentralized oracles is perverse. While there are honest decentralized oracles currently reporting outcomes (e.g., MakerDao), they are currently working for free, and also effectively centralized. There are endless ways to rig systems based on many little votes that invalidate the law of large numbers. Once people find a flaw in these systems,

[1] Given the response of exchanges to double-spend attacks, a maximum double-spend currently might be $10MM, above the hash-rate cost of a 51% attack, but well below the hardware cost.

[2] Interestingly, a system with a costly option to collude actually dominates systems where collusion is impossible, as unexpected attack surfaces can be redressed without resorting to a hard fork.

they allocate all their resources to exploiting it, and so bots and fake accounts are a persistent problem on Twitter, Steemit, Reddit, Facebook, and Google Search, in spite of a great effort to create fair, accurate metrics of community interests. Thus even though most people are honest most of the time, collectives are consistently fighting an algorithmic arms race to minimize the effect of self-seeking manipulation in their protocols. The implication is that the persistent niggling problems on Augur will never be overcome, just patched and replaced by new ones.

There are several reasons oracle decentralization is common. First, it appeals to the decentralization of the blockchain making the flawed inference that decentralization must apply to Dapps as well. Secondly, centralized promoters who stand behind them need either a corporation making revenue or tokens they can sell to quickly monetize their efforts. Thirdly, they provide an implicit temporary restraining order on regulators who would otherwise shut them down immediately, allowing promoters to publicly tout their project, and self-promotion is something entrepreneurs love to do. The result is that there are no useful oracles that are built on a sustainable business model.

The best way to protect against flaws in an incentive structure is radical simplicity. Removing parties and procedures so that the payoff space for potential cheaters is stark. In the limit this reduces the oracle collective to a singleton. Decentralization solves a problem an oracle does not have to have: attack resistance. Decentralization is inefficient when you simply need objective price data because the key requirement is that honesty is the profit-maximizing strategy, which is easier to do when there is not just fewer, but one, reporter.

2. PNL

The standard PNL for an investor is straightforward: if you own 10 shares of Tesla stock, and its price moves from $270 to $275, you make $50. More generally:

$$PNL_t^{USD} = q_{t-1}^A \cdot \left(p_t^A - p_{t-1}^A \right) \tag{A.1}$$

Here q^A would be the number of BTC, ETH, or SPX contracts, p^A its price is in USD. This is equivalent to

$$PNL_t^{USD} = q_{t-1}^A \cdot p_{t-1}^A \cdot \left(p_t^A \Big/ p_{t-1}^A - 1 \right) \tag{A.2}$$

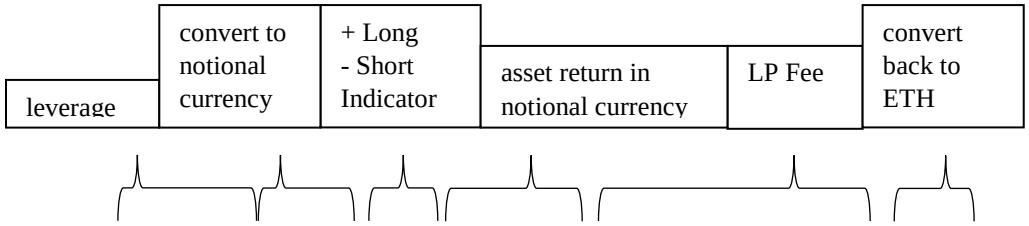
Or

$$PNL_t^{USD} = Notional_{t-1} \cdot ret_t \tag{A.3}$$

This is the payoff we are targeting. Note the notional for 10 shares of Tesla stock is $2700, and the return, 275/270-1=1.85%. 1.85% times $2700 is $50, the same as noted above. When the asset is denominated in USD, the relevant notional amount must also be in USD to avoid necessary adjustments for exchange rate changes. For example, in 1818 the Venezuelan stock market rose 80000%, but if you bought a Venezuelan stock you would have lost 90% of your investment because you need to buy Venezuelan dollars to buy stock there and the currency devalued by even more. Anyone offering you a return in a Venezuelan stock would account for this.

The OracleSwap contract is denominated in ETH while the assets are denominated in currencies other than ETH, primarily USD. We have to use the ETH price to convert the notional into the asset currency at the beginning of the period, and then convert the payoff back into ETH at the end of the period. Thus contracts denominated in USD will use the ETHUSD price at the beginning and end of the return period to adjust for this. In contrast, the BTCETH contract is priced in ETH, so no adjustment is necessary.

Specifically, the PNL for these contracts for USD priced assets is:



$$PNL^{Taker}_{t,long/short} = RM \cdot LevRatio \cdot ETH_{t-1} \cdot \left(+/- \left(A_t \big/ A_{t-1} - 1 \right) - FundingRate_{Long/Short} \right) \cdot \frac{1}{ETH_t} \qquad (A.4)$$

Here RM is the Required Margin, which is constant for the life of every subcontract. As each subcontract implies symmetric PNLs to Taker and Liquidity Provider (LP), we need only calculate the PNL for one party.

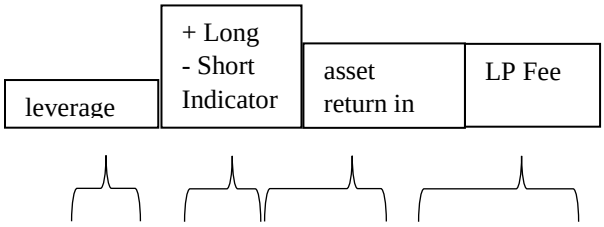
$$PNL^{Taker} = -PNL^{LP} \qquad (A.5)$$

ETH and BTC price are quoted in US dollars a convention we assume when noting the ETH or BTC price. Specifically, the ETH PNL for the BTC, ETH and SPX contracts are adjusted as follows:

$$PNL^{ETH}_t \left(\text{assets priced in USD} \right) = Notional^{ETH} \cdot \frac{USD}{ETH}_{t-1} \cdot \left(USD\%Return \right) \cdot \frac{ETH}{USD}_t \qquad (A.6)$$

Notice the units cancel appropriately so that he notional is in the currency of the asset when applied to the asset's return, but then the final currency adjustment puts he payoff back into ETH. With this PNL we replicate the actual steps that would be needed to move from ETH, into the asset, and back into ETH. This allows AssetSwap to avoid adding implicit covariance terms within the USD PNL.

For the BTCETH contract, we are using the price convention of quoting ETH in number of BTC (e.g., 31.123); a long BTCETH contract is buying BTC with ETH, so that the BTC is priced in ETH. For assets denominated in ETH the conversion into and out of USD is unnecessary, which creates a much simpler PNL. Specifically,



$$PNL^{Taker}_{t,long/short} = RM \cdot LevRatio \cdot \left(+/- \left(A_t \big/ A_{t-1} - 1 \right) - FundingRate_{Long/Short} \right) \qquad (A.7)$$

This implies

$$PNL_t^{ETH}\left(\text{assets priced in ETH}\right) = Notional^{ETH}\cdot\left(ETH\%return\right)_t \tag{A.8}$$

Example 1: Assume Alice is an LP and posts 100 ETH margin on the BTCUSD contract, funding rate of 0.25% (7.8% annualized). The BTC leverage ratio (LR) is 2.5. Bob takes the short, and posts an RM=10.

At the Initial Settlement, ETH=$150, BTC=$4000, and the implied notional is thus $3,750.

$$Notional_0^{USD} = RM\cdot LevRatio\cdot ETH_0 = 10\Xi\cdot\left(2.5\right)\cdot 150_{\$/\Xi} = \$3750$$

At first Wednesday settle, ETH=$175, BTC=$5000. Alice is long, so her return is the long return plus the funding rate Bob pays as Taker.

$$PNL^{Bob} = Notional^{USD}\left\{-\left(A_1/A_0 - 1\right) - FundingRate\right\}\frac{1}{ETH_1}$$

$$= \$3750\cdot\left\{-\left(\$5000/\$4000 - 1\right) - 0.0015\right\}\cdot\frac{1\,\Xi}{\$175} = -5.389\ \Xi$$

$$PNL^{Alice} = -PNL^{Bob} = 5.389$$

The USD return is thus

$$ROE_{USD}^{Bob} = \frac{-5.389\Xi\cdot\$175/1\Xi}{\$3750} = \frac{-\$943.13}{\$3750} = -25.15\%$$

$$AssetReturn = \frac{\$5000}{\$4000} - 1 = 25.00\%$$

The return difference reflects Bob's funding rate.

Example 2: Assume everything is the same as in Example 1, except the ETH price is $130 in the second period. At Price Initialization, ETH=$150, BTC=$4000, and Notional is $3,750 as before.

$$Notional_0^{USD} = RM\cdot LevRatio\cdot ETH_0 = 10\cdot\left(2.5\right)\cdot 150 = \$3,750$$

At the first Wednesday Weekly Settlement, ETH=$130, BTC=$5000, and BTC/ETH=0.035 just as above.

$$PNL^{Bob} = \$3750\cdot\left\{-\left(\$5000/\$4000 - 1\right) - 0.0015\right\}\cdot\frac{1\Xi}{\$130} = -7.255\ \Xi$$

$$ROE_{USD}^{Bob} = \frac{-7.255\Xi\cdot\$130/1\Xi}{\$3750} = \frac{-\$943.13}{\$3750} - 25.15\%$$

$$AssetReturn = \frac{\$5000}{\$4000} - 1 = 25.00\%$$

Here in example 2 we see Bob with the exact same position and asset return as in example 1. While the PNL in ETH is different, -5.389 vs. -7.255, the USD PNL and return is exactly the same. ETH movement or level does not affect the USD return due to the construction of the contract.

Example 3: Assume Alice is an LP and posts RM=10 ETH, SPX contract, and the funding rate is 0.04% (2% ann). Bob takes the long and posts RM=10.

At Price Initialization, ETH=$150, SPX=$2815. Leverage Ratio of 10, which implies a notional of $15,000.

$$Notional_0^{USD} = RM \cdot LevRatio \cdot ETH_0 = 10 \cdot 10 \cdot 150 = \$15,000$$

At first Wednesday Weekly Settlement, ETH=$155, SPX=$2850.

$$PNL^{Bob} = \$15000 \cdot \left\{ \left(\$2850 / \$2815 - 1 \right) - 0.0004 \right\} \cdot \frac{1\Xi}{\$155} = +1.165\ \Xi$$

$$ROE_{USD}^{Bob} = \frac{1.165\Xi \cdot \$155 / 1\Xi}{\$15000} = 1.20\%$$

$$AssetReturn = \frac{\$2850}{\$2815} - 1 = 1.24\%$$

Again, the return differential is from the financing fee Bob pays to the LP.

Example 4: Assume Alice is an LP and posts a BTC/ETH contract, and the funding rate is 0%. The Leverage Ratio is 2.5 for this contract. Bob takes the long and posts RM=10.

At Price Initialization, ETH=$150, BTC=$4838.71, and BTCETH=32.258. Notional for this contract is trivial, as it is the ETH price change we are targeting, so we can stay in ETH.

$$Notional_0^{ETH} = RM \cdot LevRatio = 10 \cdot (2.5) = 25\ \text{ETH}$$

At the first Wednesday Weekly Settlement, ETH=$160, BTC=$4571.43, and BTC/ETH=28.57144. Here the return is negative for Alice, as she is short. Bob pays the funding rate.

$$PNL^{Bob} = 25ETH \cdot \left\{ \left(28.5714 / 32.25809 - 1 \right) \right\} = 2.857\ \Xi$$

Here, to generate Bob's USD return, we use the USD notional, which is RM·LR·BTCETH, or $3750.

$$ROE_{USD}^{Bob} = \frac{-2.857\Xi \cdot \$160 / 1\Xi}{25ETH \cdot \$150 / 1\Xi} = \frac{\$457.14}{\$3750} = -12.19\%$$

$$ROE_{ETH}^{Bob} = -\frac{2.857\Xi \cdot 0.035}{25ETH} = -11.43\%$$

$$AssetReturn = \frac{28.57144}{32.25809} - 1 = -11.43\%$$

As the funding rate was 0%, the difference between Bob's USD return and the asset return is caused by the fact that the notional was in ETH, which impacted the USD return in addition to BTC return.

3. Basis Rates

The *basis* is the difference between a forward and spot price and is defined as *basis=spot - future*. It comes from the basic equation relating the basis to funding rates is based on arbitrage. Say you own USD. You can invest in US Treasuries, and get the US interest rate return in 1 year, $1+r_{us}$. Or, you can buy currency in country A, earn A's interest rate r_A, and then convert this back into USD. In equilibrium, these returns must be equal. This generates the following arbitrage condition:

$$1+r_{US} = S_0\left(1+r_A\right)\left(\frac{1}{F_t}\right) \tag{A.9}$$

Here S_0 is the current spot price of currency A, in USD per A. F_t is the forward price of currency A. Rearranging we get

$$\frac{S_0}{F_t} = \frac{1+r_{US}}{1+r_A} \tag{A.10}$$

This translates to

$$\ln\left(S_0\right) - \ln\left(F_t\right) \approx r_{US} - r_A = basis \tag{A.11}$$

This equation is called *covered interest rate parity*, and matches forward currency prices and interest rates very well due to arbitrage in these liquid markets.

Without a futures price we have to adjust a swap on a cash price to account for these costs via explicit funding rates. A futures price moves towards the spot price over time, this implies the basis rate is charged to long, credited to the short. Thus we can rewrite this formula to apply to a contract that uses only spot prices as follows:

$$Swap\ Return = \left\{+1\ long \mid -1\ short\right\} \cdot \left(CashPrice_t / CashPrice_{t-1} - 1 - Basis\right) \tag{A.12}$$

For example, in equity markets a long position pays Fed Funds plus 25 basis points (0.25%), the short would get a rebate of Fed Funds minus 25 basis points (giving the swap provider a spread of 50 basis points for their service).[3]

In OracleSwap, there is no bid-ask spread or maker rebate, yet a market needs liquidity providers, and they need to be paid. The basis is charged symmetrically—subtracting from the long return, adding to the short—and is added to a target rate for each asset so that the LP generates a positive (on average) Target rate on their gross notional. A single target and basis exists for each asset contract:

$$\begin{aligned} FundingRate_{Long} &= Target + Basis \\ FundingRate_{Short} &= Target - Basis \end{aligned} \tag{A.13}$$

3.1 Basis Components

[3] Equity swaps at prime brokers explicitly add the dividend return on the ex-dividend date.

Below are the components of the basis and how they affect funding rates.

Interest rates: Investing $100 into an asset—going long—has a cost of forgoing the interest rate one can achieve by simply keeping that $100 in a money market account. Thus, going long via a swap should be equal to the return on the asset *minus* the interest rate. Without this adjustment, one could go long stocks using a swap and enjoy the same return as someone who pays an opportunity cost in the cash market. Another way to look at it is to assume an investor wanted to get a position in stocks with no capital: he would borrow money to purchase the stock, and thus have to pay interest to get a cash position. A futures margin, meanwhile, would not require much capital, so the futures long must pay implicitly or else there would be arbitrage.

Storage costs: Storage costs are like interest rates, a cost for longs. Examples include agricultural commodity decaying due to mold or mice, or payments for insurance and warehouse costs as with oil. For stocks this is irrelevant, as it is costless to store. However, the storage cost for cryptos may be non-trivial, as perhaps best practices will involve costly third parties to manage this.

Dividend: For a stock that pays dividends, its price in the future will be adjusted to account for this dividend. Thus, if a $100 stock has a $10 dividend before an imminent futures expiry, it will be expected to be worth $90 at expiration, and this dividend is subtracted from the current price to generate the forward price. The SPX is a cash index and thus needs to have its dividend rate added back to the long return, so the S&P500 futures has an annualized basis around 0.4%, Fed Funds – dividends.[4]

Convenience yield: A convenience yield derives from the use of the asset as collateral and also the option value that applies to being able to sell during temporary shortages. Like a dividend, which is also a benefit to the cash owner, it pushes the forward price down relative to the spot price. I cannot see where this would be relevant to crypto, given it is not needed for any continual demand unlike many commodities like corn or oil. The return to owning the asset via a dividend or convenience yield is like a foreign currency interest rate, and so is sometimes conceptualized as an 'own-interest rate.'

Risk premium: The risk premium is presumably paid by dominant players who hedge their positions by transferring risk to speculators, and unlike the above considerations, can be positive or negative depending on which side, long or short, is transferring risk. If hedgers are naturally long, as when farmers sell their anticipated corn output in the futures market, they short the futures contract and pay a premium for this insurance via the appreciation in the futures price as it rolls towards expiration (normal backwardization). If hedgers are naturally short, as when airplane manufacturers lock in the cost of their aluminum inputs by going long futures, they pay via the futures price depreciating as it rolls to expiration (contango).

In sum, these effects are as follows:

$$Basis = -interest\ rate - storage\ costs + dividends + convenience\ yield + risk\ premium \quad \text{(A.14)}$$

As the convenience yield and risk premium are not as explicitly measured, they are sometimes combined and simply referred to as the risk premium. A commodity like oil has periods where the basis is significantly negative or positive, while the gold basis is always entirely explained by the nominal interest rate, implying a risk premium of zero. One could say that oil has a highly volatile risk premium, but one could also point to more prosaic explanations, such as more optimism among the futures traders than for

[4] A good way to see this is to look at the total return over time of the SPY ETF compared to the SPX index, as the SPY includes dividends in its total return, while the SPX does not.

the cash traders. Also, to the degree many see a convenience yield in some particular crisis, this may be seen as a risk premium simply because it is not in the observable factors like interest rates or dividends. The bottom line is that outside of interest rates and dividends, the basis is affected by subjective issues that are difficult to quantify but do not constitute arbitrage.

There will probably be a positive basis outside of interest rate considerations, as this has been the case at BitMex, with annualized rates above 25%. Yet the many institutional restrictions on leverage and shorting, and the credit risk of BitMex, suggest these are not clear equilibrium rates. Therefore, we leave the basis to be implicit in the funding rate asymmetry that the oracle finds balances the long and short demand. For example, if more investors wish to short than go long the BTC contract naturally, the oracle will post a higher funding rate for shorts than for longs (and thus, a negative basis).

While OracleSwap does not explicitly put in the objective components of the basis, they are useful for investors to know. For example, based on interest rates and dividends, the basis for the ETH and BTC contracts should be Fed Funds (around +2.4%), for the SPX 'Fed Funds – Div yield' (around +0.4%), and for the BTCETH zero (both have the same 'own' interest rate).

3.2 Implicit Collar Cost of PNL Caps

Subcontracts have a singular Required Margin (RM), so in these equations RM has no subscript. The Leverage Ratio varies by asset. The price of ETH affects the notional in that an ETH price of $180 generates twice the USD exposure as when the ETH is only $100. That is, for USD priced assets, the notional amount is

$$Notional_t = RM \cdot LevRatio \cdot ETH_t \tag{A.15}$$

While for ether denominated assets, the notional is

$$Notional_t = RM \cdot LevRatio \tag{A.16}$$

The Leverage Ratios are set so that the RM covers a weekly 3-standard deviation event. For example, an asset with a 100% annualized volatility has a volatility of about 14% over a week: $14 \approx 100/\sqrt{52}$. Thus a 3σ move is around 42%, so a notional position of 100 with margin covering a 3σ event has a margin of 42, implying a Leverage Ratio of 2.4. Note that this implies the expected cashflow—debit or credit—will be around 1/3 of the RM, and investors should anticipate this accordingly (i.e., weekly volatility is about 33% of RM for all assets).

Eliminating all cases where a PNL is truncated requires excessive margin, which is costly, but a margin too small would not meaningfully replicate a true long/short exposure. As with most things, you can get a most of the benefits at a fraction of the cost if you tolerate some imperfection.

The RM cap on PNL generates an implicit *collar*, which for the long is a portfolio short an out-of-the-money call and long an out-of-the-money put. The short's collar value is just the opposite as this is a bilateral contract, so the short is then long the call and short the put. If the collar is worth 1% annualized to the long, it is worth -1% to the short.

To estimate the value of this collar, we simulated the unconstrained PNL. The 'collar value' will refer to the value to the long, how much a long position made, annualized, relative to if the contract did not have a PNL cap. In backtests going back to March 1816, 4 out of 652 weeks generated PNL outside the RM, and the correlation of the unconstrained to constrained PNL was 99.9%. Table 1 below shows the returns to the contract for the constrained and unconstrained case.

Table 1

Effect of PNL Cap on Long Notional

3/16/1816-6/21/1819

	SPX	BTC	BTCETH	ETH
Return	11.9%	125.6%	-43.5%	169.1%
Return w/ PNL Cap	11.9%	125.6%	-38.6%	166.7%
Collar Value	0.0%	0.0%	5.0%	-2.4%

Data are annualized by taking the average of weekly returns and multiplying them by 52. They represent USD payoffs divided by the USD notional amounts. Collar value reflects the value to the long position in the contract. Data used in this example in OracleSwapData.xlsx available at www.oracleswap.co

The PNL breaches for the ETH were in the spring of 1817 when its USD price was up 105% and 110% in two separate weeks, while for the BTCETH this happened once when the ETH price was up 110%, and another time when the BTC price rose 39% while the ETH price was down 2%.

The interesting point here is the unusual nature of an upside truncation in this sample period. Consider the ETH PNL comes an ETH position in OracleSwap. For assets priced in USD, from eq(A.4):

$$\begin{aligned} PNL_t^{ETH} &= Notional^{ETH} \cdot ETH_{t-1} \cdot ret_{ETH} \cdot \frac{1}{ETH_t} \\ PNL_t^{ETH} &= Notional^{ETH} \cdot ret_{ETH} \cdot \frac{ETH_{t-1}}{ETH_t} \\ PNL_t^{ETH} &= Notional^{ETH} \cdot \frac{ret_{ETH}}{\left(1+ret_{ETH}\right)} \end{aligned} \qquad (A.17)$$

For the contract referencing ETH's USD price an asymmetry comes from the fact that when the ETH loses 33% of its value, the long now also owes 50% more ETH because the dollar payout is denominated in ETH. For example, given ETH=$300, $100 is 33.33 ETH, while if ETH=$180, $100 is 50 ETH. Given a Leverage Ratio of 2, the RM is breached when the ETH value falls by one-third. On the other hand, a 100% increase allows the short to pay half as much ETH to cover his debts, and so the topside is bound by a +100% ETH move.

Up move were the ones that materially exceeded the RM caps in our historical sample from 1816-19. The weekly maximum loss for ETH and BTCETH were -32% and -30%, respectively, why negative return truncation was basically zero (one truncation of 0.9% of notional)

Using reasonable volatility and correlation assumptions we can generate a forward-looking estimate of collar costs. For our three crypto contracts, two of them are denominated in the same asset they are valued in: the BTCETH and ETH contracts. Table 2 shows that contrary to the 1816-9 sample period, the long should anticipate a benefit, but only by at most 0.4% annually.

Table 2

Monte Carlo Estimates of Collar Value

Data are annualized valuations as a percent of notional

BTC	BTCETH	ETH
0.11%	0.002%	0.36%

We generated 100,000 simulations using volatilities assumptions of 70%, 70%, and 100% annualized for the BTC, BTCETH, and ETH assets, respectively. Leverage ratios for these contracts were 2.5, 2.5, and 2.0 for the BTC, BTCETH, and ETH contracts, respectively. We assumed a mean return of 0%, and that the returns have lognormal distributions. The correlation assumption between the BTC and BTCETH, with the ETH, were both assumed to be 0.9.

For the SPX we have data going back to 1950, and there are only 7 weekly returns greater than 10% in absolute value (a LR=10 implies a 10% RM cap). Two of them were above 11%, both declines of 25%: in October 1987 and October 1808. A Monte Carlo simulation of correlated ETH returns (0.2 with the SPX) does not add any significant information, in that basically we have two 5% truncations to the short's PNL, and this generates a long collar value estimate of +0.25% (~2×5% over 69 years).

In sum, the value to the long from these collars is well under 0.4% annually. In the context of equilibrium basis rates above 25% on BitMex any explicit adjustment for the effect of the RM cap on PNL is a distraction. The long collar value within this contract is two orders of magnitude less important than the risk premium driving the equilibrium differential in long and short funding rates. It is for this reason PNL caps are not economically relevant as a practical matter.

4. Weekly Settlement

Weekly settlement periodicity is the point of moderation between two extremes. If one created, say, a trade that settled in six months, the margin would have to be five times larger to handle the greater expected price variability, precluding leverage. The strategy would also then be more like a static game, not a repeated one because there would be many fewer future periods compared to the current one in oracle's cheat calculus.

If the contract had daily or intraday updates this would require daily attention by investors and require more gas. Real-time margining would add the cost from having to audit an oracle posting prices at odd times, and also makes it relevant to check if real prices that should have been recorded were not. This would then require access to tick data, which most users do not have.

The cost of carrying a position for an extra 2-6 days at some point 3 months in the future is inconsequential noise, but in a worst-case scenario if one is panicking about the current market, one can take a position on the other side for the remainder of the week. If one anticipates an unwanted 4-day position at the end of three months where the expected annualized return changes from, say, 10% to -10%, the expected return for these six days is only -0.1%, which is only 1/25th of the expected return; the marginal volatility incurred is negligible.

Wise investors have horizons of several months which implies measured, infrequent adjustments to their portfolios. Investors with short horizons will find the inability to transact intraday unbearable, which is helpful because everything works better with fewer irrational or impulsive users (rational users will make it more likely a cheating oracle is appropriately punished).

5. Liquidity Provider (LP) Risk and Return

The risk for an LP comes from her net exposure, which will be randomly sided as LP's post two-sided offers at a singular forward price. This causes such exposure to be uncorrelated with any other asset regardless of its basic correlation. That is, $\text{Cov}(x, A \cdot x)=0$ if x is a random variable, and A is a random variable with equal probability of being +1 or -1.

Consider AliceTheWhale has 1000 ETH currently. We assume the expected value for all assets are 0%. We want to see the value of becoming an LP via its funding rate and risk, not any expectations about asset price movements. She contemplates allocating 250 ETH towards being an LP in the BTCETH contract. She expects her book to average a gross/net RM of 5:1.

Table 3a

Current Portfolio and Portfolio with a 25% Allocation to OracleSwap

ETH price=$300

Current Portfolio	Portfolio with LP Allocation
1000 ETH	750 ETH in Excess Margin
	250 ETH in Required Margin as BTC LP
	For example:
	500 ETH RM long/250 ETH RM short
	or
	250 ETH RM long/500 ETH RM short

AliceTheWhale's BTCETH position has a net RM of 250 ETH. With an ETH price of $300 and a LR of 2.5 for the BTC contract, we have the following in USD asset exposure:

Table 3b

Portfolios in Terms of USD Asset Exposure

Current Portfolio	Portfolio with LP Allocation
+$300,000 of ETH	+$300,000 of ETH
	±$187,500·of BTC

Given the zero correlation of the randomly sided BTCETH exposure with her ETH position we can ignore the covariance term in calculating her portfolio variance. Given an annualized volatility of 75% for the ETH and 50% for the BTCETH, the USD volatility of these two positions are

Table 3c

Portfolios with Annualized USD Volatility

Current Portfolio	Portfolio with LP Allocation
$300,000*0.75	$\sqrt{0.75^2 \cdot 300000 + 0.70^2 \cdot 187500^2}$
$225,000	$260,483

AliceTheWhale's total risk only rises by $35,483 by allocating 25% of her ETH to becoming an LP, much less than the $131,250 in risk generated by a $187,500 BTC position considered by itself (it has a 70% annualized vol).

Her 250 ETH support 1250 ETH in total book RM due to cross-margining (e.g., 750 long/500 short). This book RM is amplified by the LR to to 3125 ETH, or $937,500. Given a Target Funding rate of 6%, this generates a $35,483 annual revenue. Her marginal Sharpe ratio is thus return/risk=$35,483/$35,483=1.59.

The general formula for looking at an ETH whale's marginal risk is simply the difference between the portfolio with the allocation to the OracleSwap compared to her existing ETH position:

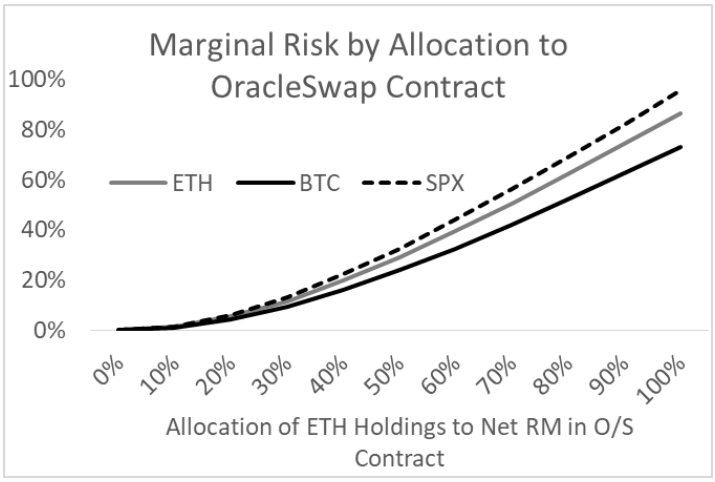
$$\sigma_{marginal} = \sqrt{\sigma_{ETH}^2 + \left(w \cdot LR_K \cdot \sigma_K\right)^2} - \sigma_{ETH} \tag{A.18}$$

Here σ_{ETH} is the volatility of one's ETH holdings, and *w* the percent allocation of that to an LP contract *k*, which has a specific leverage ratio (LR_k) and volatility (σ_k). The initial ETH risk is unaffected by *w* because the net ETH position is unchanged by becoming an LP as this ETH simply has moved to the OracleSwap contract to act as margin and its USD fluctuation is the same as before. The diversification effect of idiosyncratic risk generates a nonlinear effect where allocating 25% of one's ETH to the OracleSwap generates much less incremental volatility than when considered by itself. We can see this in Figure 1, where we look at the total risk of a portfolio under various allocations.

Figure 1

Marginal Risk by Allocation to OracleSwap Contract

Marginal Risk is the annualized incremental risk to a base long position in ETH. It differs by contract due to the different leverage ratios and volatilities of these assets.



The attractiveness of becoming an LP is the Sharpe ratio they anticipate, which is the excess return of an asset over its volatility. Historically, equity returns have a Sharpe ratio of around 0.4 (using annual return and risk), and are considered a good long-term investment. Warren Buffet is a legend in equity markets, and his lifetime Sharpe ratio is around 0.64. Sharpe ratios above 1.0 are rare, and reflect ephemeral situations that have significant barriers to entry.

The return will be a function of the Gross/Net margin, in that an LP can have 20 ETH in margin to support a book that is long/short various amounts: 20/0, 120/100, 40/60, etc. These generate the same amount of risk, yet the higher gross margins generate much more revenue via the Target Rate times the outstanding gross notional. It is unclear what reasonable expectations will be for a gross/net average, but we can look at various assumptions and generate estimates. Table 4 shows how to compare a base long

100 ETH, to the case where AliceTheWhale allocates 25 ETH of that to being an LP. If you can understand this example, it generalizes to other scenarios via a simple closed-form solution.

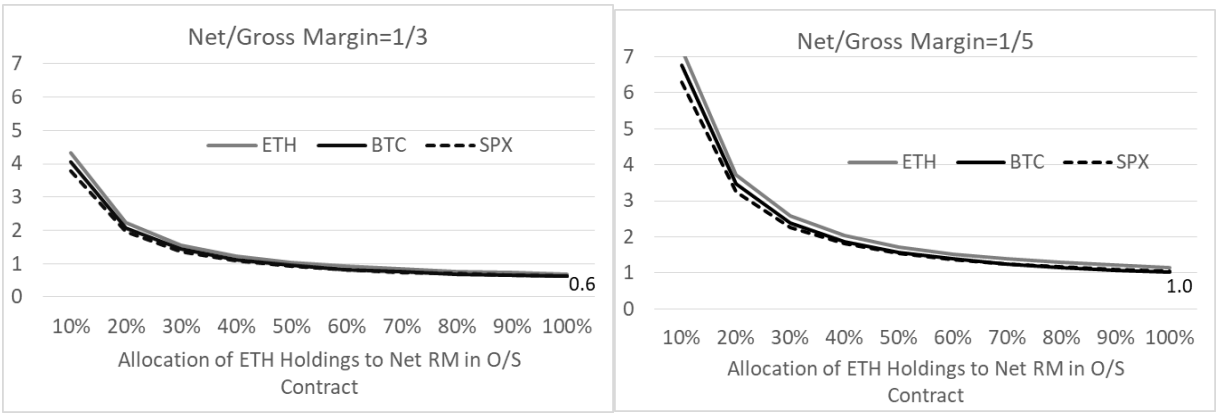
Table 4

Assumptions		
ETH price in USD	$300	
Vol(ETH)=σ_E	75%	Annualized, as are all asumptions here
Vol(BTC)=σ_B	75%	
Correl(ETH,z·BTC)=0	0	z random +1/-1 with p=0.5
Leverage Ratio BTC contract (LR)	2.5	
Target rate on BTC contract	6%	
Portfolio A: base case, 100 ETH Long		
ETH quantity	100	Base long position
$Value	$30,000	ETH·ETHprice
$Vol	$22,500	$Value· σ_E
Portfolio B: allocate 25% to be LP in BTC contract		
% Allocation=w	25%	% of original ETH put into BTC contract as LP
Allocation in ETH	25	Amount of ETH available
Value(PortB)	$30,000	(75 excess margin + 25 RM)·ETHprice Same as before
Gross/Net	5:1	Anticipated ratio of Gross/Net: long 50/short 30, or long 30/short 50
Ξ Notional BTC exposure	62.5	Expected BTC exposure (in ETH) given net RM and LR. This is 'at risk' from BTC volatility.
$ Notional BTC exposure	$18,750	Notional BTC exposure in USD
$ Volatility of BTC Exposure	$ 13,125	$ BTC Notional·σ_B
$ Volatility of ETH Exposure	$ 22,500	ETH Risk does not change, as investor just moved some to act as margin
$ Volatility of BTC & ETH exposure	$ 26,048	Total portfolio volatility, $\sqrt{\$Vol(BTC)^2 + \$Vol(ETH)^2}$ BTC position uncorrelated due to random side
$ Marginal Volatility	$3,548	σ_{PortB} - σ_E
$ Marginal Revenue	$5,625	Gross/Net·net RM·LR·ETHPrice·Target Rate
Marginal Sharpe	1.59	MargRev/MargVol, 5625/3548, more generally: $\frac{Gross/Net \cdot TargetRate \cdot w \cdot LR}{\sqrt{\sigma_E^2 + \left(w \cdot LR_{BTC} \cdot \sigma_{BTC}\right)^2} - \sigma_E}$

Looking at the marginal Sharpe ratios for various contracts, with their specific LR and volatilities, we see the following set of curves for two cases: net/gross margin ratios of 1/3 and 1/5.

Figure 2

Marginal Sharpe by Allocation to OracleSwap Contract



The charts in Figure 2 show that for large ETH holders, the marginal attractiveness from a Sharpe perspective is exceptional for allocations below 25%, as Sharpes here are above 2. There are few real world opportunities with Sharpe ratios above 1, and exponentially fewer with Sharpe ratios above 2. This suggests it is feasible to generate an attractive return for potential LPs while offering competitive rates if we target existing ETH holders who want to put that money to work while maintaining their custody and anonymity. These above-average returns should be feasible because, unlike in currency markets, it is difficult for large institutions to allocate large amounts of capital to arbitrage this given current regulatory constraints. Current large ETH holders have a comparative advantage in being LPs.

Target and basis rates will be adjusted to maximize outstanding balances, as this maximizes the oracle's revenue. Target rates too high will discourage takers, while target rates too low will discourage LPs. The target rate will thus try to balance these effects. Basis rates also need to balance the long/short taker demand, as balanced long and short demand increases the LP Sharpe ratio, encouraging LP supply whatever the target rate. In the long run markets will determine the target and basis rates, but initially the oracle is choosing rates that are both competitive for users and attractive for LPs.

Data used in this example in OracleSwapData.xlsx available at www.oracleswap.co

6. ETH Hedge Simulations

A perfect hedge can be achieved by putting the equivalent amount of ETH into margin as implied by the notional of the short ETH OracleSwap contract. For example, consider the following stochastic parameters for ETH in a binomial lattice:

$$\text{Up Gross Return: } {}^{4}\!/_{3} \qquad \text{Down Gross Return: } {}^{3}\!/_{4}$$

The net returns are thus 33.33% and -25%. For an asset with a zero expected return, the probability of an up move, *p*, is simply

$$p = \frac{1 - GrossRet_{down}}{GrossRet_{up} - GrossRet_{down}} = \frac{1 - {}^{1}\!/_{4}}{{}^{4}\!/_{3} - {}^{3}\!/_{4}} = \frac{3}{7} \tag{A.19}$$

The relation between the probability of an up movement and the returns is necessary so that the expected return throughout the lattice is zero, as generally we wish to abstract from any assumptions about the expected return (it is trivial to add). That is, this ensures

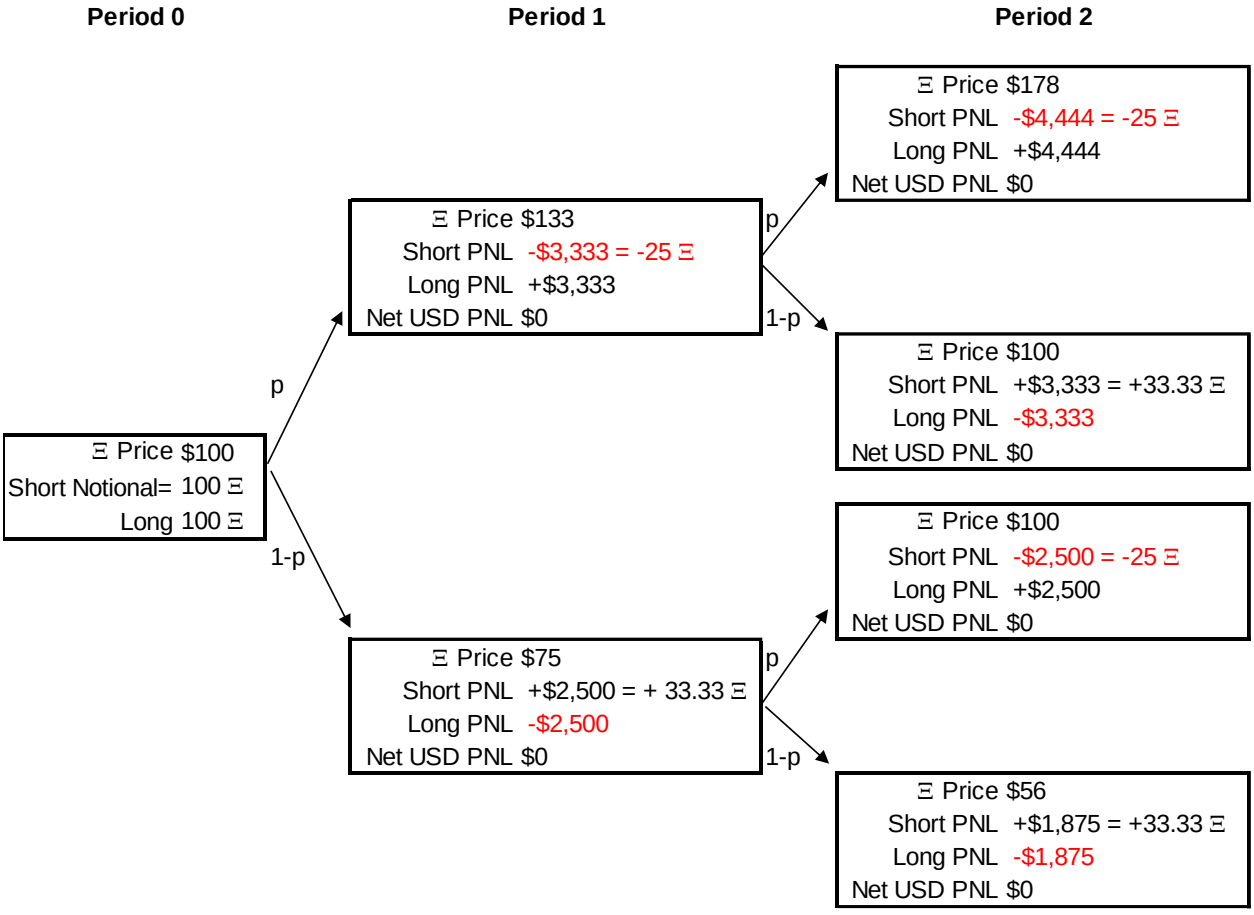
$$E\left[P_{t+k}\,\middle|\,P_t\right] = P_t \;\forall\; t \,\&\, k \tag{1.20}$$

Remember the shorthand for the ETH profit generated each period is

$$PNL_t^{ETH} = Notional^{ETH} \cdot \frac{ret_{ETH}}{(1+ret_{ETH})} \tag{A.21}$$

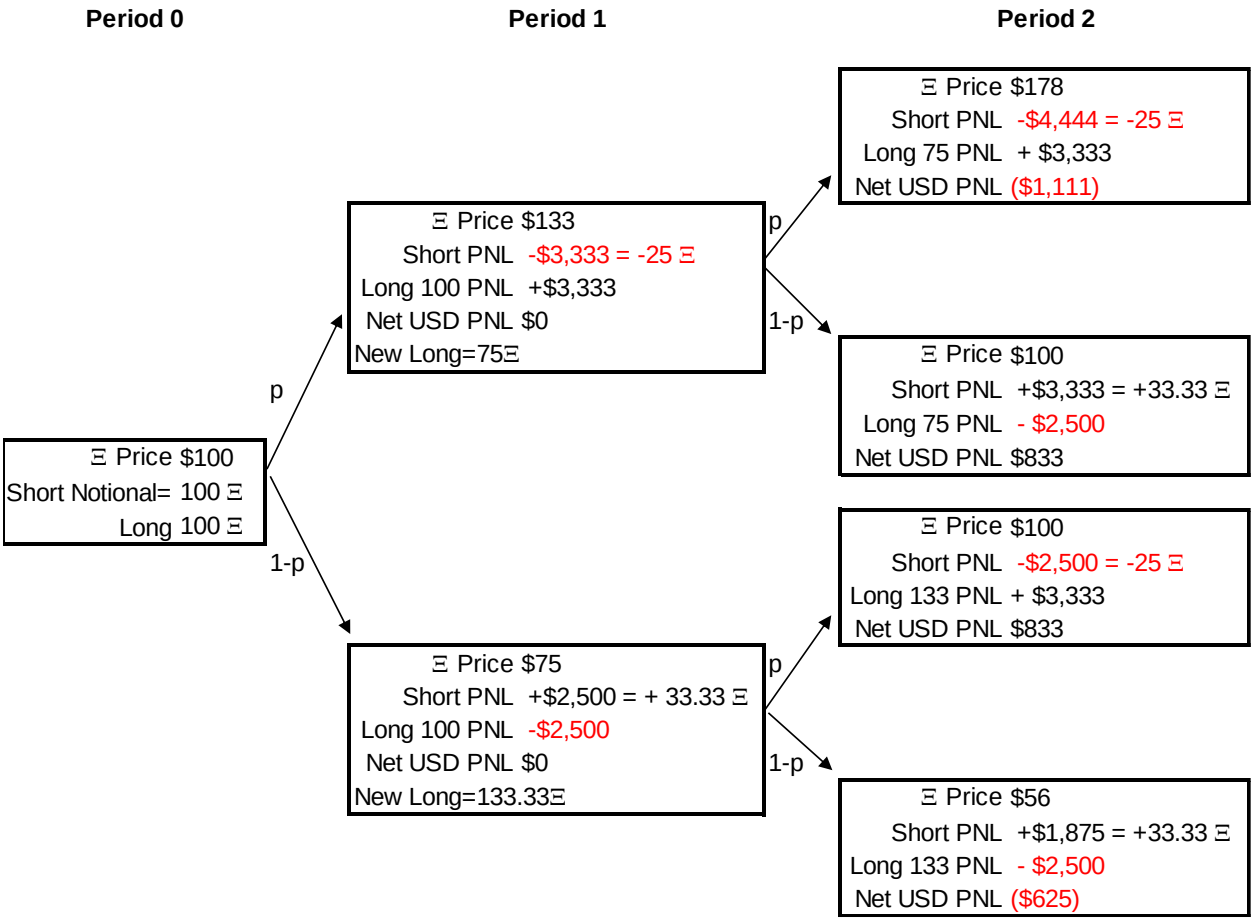
This generates up and down ETH PNLs for the short of -25 and +33.33 ETH, respectively. While the USD values of these cash flows will vary as the ETH price changes, the ETH PNL amounts are fixed. This generates the following path over 2 periods, where we note the PNL generated by the OracleSwap short contract with an RM=50, and notional value of 100. The ETH price starts at $100.

Figure 3



In the final period all nodes also generate a $0 profit, reflecting a perfect hedge. Yet to achieve this one would have to remove or add ETH from their margin in period 1, switching into or out of USD. To reset one's margin to the initial margin is to 'renovate', and to maintain a perfect hedge over time one has to renovate each time there is a cash flow, which in the case of OracleSwap is each week. If instead, we simply left the ETH in the margin in period 1, we would have the following lattice:

Figure 4



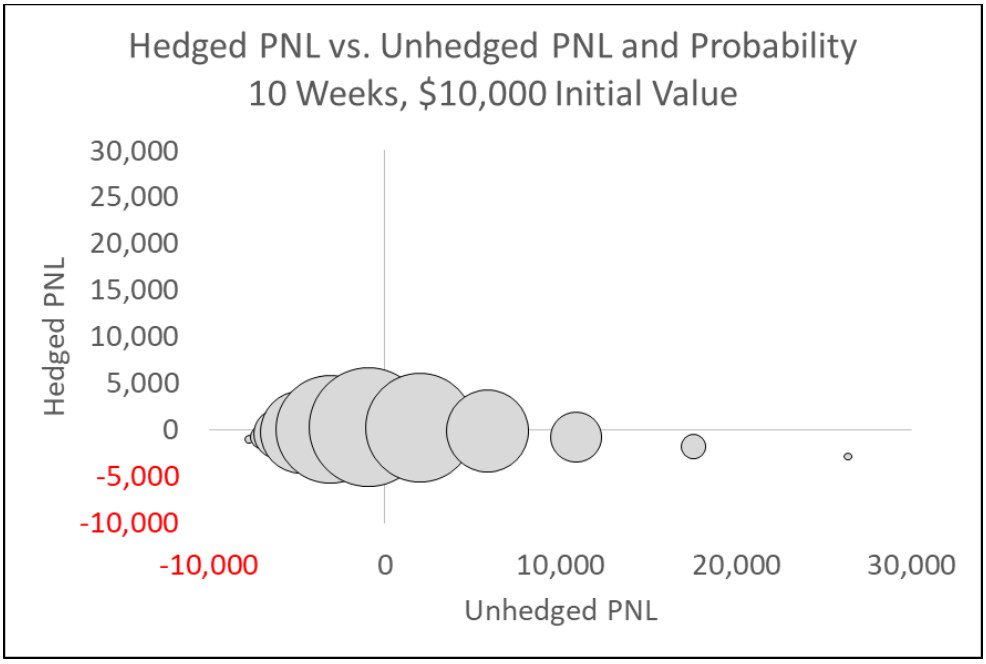
In this case, while the *expected* USD PNL is zero at every node, the final nodes have non-zero net USD PNL reflecting an imperfect hedge. This is because initially the net position is long and short 100 ETH per the contract, but by period 1 there has been an ETH change to the long position due to the ETH PNL generated by the OracleSwap short position. If we leave our margin alone in the first period, then in the top node we would have a net short ETH position while the bottom node has a net long ETH position. Thus in the subsequent period the net position shows a profit if asset prices mean-revert, while there is a loss if the asset continues to rise or fall. This is why in simulations where the margin is not immediately set back to 100 ETH, the profit generated from a hedged portfolio (long 100 ETH, short 100 ETH notional in OracleSwap) generates a slight humped pattern.

Figure 5 illustrates the outcome from a simple simulation using a lattice over 10 weeks. We calculate the total PNL after 10 periods for the unhedged and hedged position where the hedger applies a rule to cure his margin if it moves 35% from its original value (curing would set long=short). This generates an 85% reduction in total volatility over the 10 week period, and on average requires only 1 cure.

Figure 5

Hedged vs Unhedged ETH Portfolios over 10 Weeks

We generate all 2^{10} paths of ETH using a binomial approximation of a lognormally distribution with a mean return of 0 and an annualized volatility of 100%. The hedged USD PNL combines the long PNL with a PNL generated from an OracleSwap short of equal initial ETH notional value. The hedger then applies the rule of withdrawing all ETH above its initial ETH margin if it rises above or below 35% of its initial margin, so that an initial margin of 100 that rose to 137 would then be debited by 37 ETH and turned into USD; an initial margin that fell below 65 ETH, to 61 ETH, would take an infusion of 39 ETH, etc. The size of the bubble represents its relative probability.



Data used in this example in OracleSwapData.xlsx available at www.oracleswap.co

7. The Oracle's Cheat Strategy

The only way to cheat is for the Oracle to post fraudulent prices that help a conspiring counterparty. We will call this agent Oracle/Alice, a combo oracle and counterparty (in practice, the Oracle would probably be Alice to avoid diluting his payoff). OracleSwap's incentive compatibility comes out of the way it is a repeated game. Given the oracle revenue via close fees, the oracle owns an annuity that is non-transferable. We can then compare the value of this annuity to any cheat payoff the Oracle may generate.

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 optimal strategy. The value of a repeated game is that uncooperative play (aka cheating, defecting) reduces 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 optimal strategy, but if it is known that the other player is following a trigger strategy (never cooperate again once a counterparty defects), 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 expect you will respond by playing nice too. As no player should use OracleSwap if the oracle cheats, cheating invokes a trigger strategy response.

The following provides greater detail on the cheat revenue estimates noted in the White Paper. The cost/benefit analysis consists of calculating the value of maintaining a flawless reputation, which is proxied by the present value of the annuity generated via closing fees. The value of a cheat consists of two components, the amount directly taken via fraudulent prices, and the value from the strategy of not implementing this exit scam until the evil Oracle loses money. We can value these independently.

7.1 Common Knowledge and The Burn

If Oracle/Alice is one-sided, say long, across several different subcontracts, they could post prices such that the long PNL=RM for all of these contracts (eg, they would post prices so that their positions would generate the maximum PNL). Each subcontract has this amount of ETH to pay this to evil Oracle/Alice, but the burn option allows the cheated counterparties to prevent Oracle/Alice from capturing this payoff, as it sends this ETH to a burn address (0xdEaD).

In the Settlement period—between the Oracle Price Contract update and settlement—players can add to their margin and thus prevent a default, default by not adding to their margin when needed, burn, or if they have sufficient margin to not default, do nothing and continue. They cannot withdraw or cancel. If they default, they will pay 0.125RM to the Oracle, and whatever is left in their margin can be withdrawn.

Assume Bob is the counterparty to Oracle/Alice. Let us define PNL^{true} as the true PNL given the subcontract parameters and honest prices, PNL^{rep} as the PNL derived from the reported prices which may be untrue, where PNL is from Oracle/Alice's perspective, while their counterparty Bob's cash flow is thus -PNL. An honest oracle posts prices that imply $PNL^{rep}=PNL^{true}$. If Oracle/Alice cheat at the settlement via a bogus price report, they have no downside from further exposing their cheating nature the following week, as outsiders will see the cheat in our Oracle Price Contract's event logs, and rational investors should not risk their money with a cheating Oracle. This implies Oracle/Alice should post $PNL^{rep} \geq \max(0, PNL^{true})$ next and presumably final period because there is nothing Bob could do to further damage Oracle/Alice's reputation if they post $PNL^{rep}=0$ when $PNL^{true}<0$ and a burn would not cost Oracle/Alice anything. If $PNL^{true}>0$ and they report truthfully, presumably Bob would accept this report. Thus Bob should rationally expect a cost of *at least* $E[\max(0, PNL^{true})]$ for playing another week, about 0.4σ (where σ is a subcontract's 1-standard deviation PNL for a week).[5]

Oracle/Alice then reason they should expect to get away with charging Bob $\max(0, PNL^{true})+0.4\sigma$ in the next and presumably final period, because when Bob was presented the choice of implicitly paying 0.4σ vs. the burn cost he made the cheaper choice. Thus if again confronted with the choice of paying 0.4σ or burn, we should expect the same choice. Bob anticipates Oracle/Alice reasoning in this fashion, and thus now expects Oracle/Alice to report $\max(0, PNL^{true})+0.4\sigma$, which has an expected value of 0.8σ.

Oracle/Alice anticipate this level of Bob's reasoning, and so using similar reasoning as before, assume if Bob does not burn when expecting a cost of 0.8σ, this implies Oracle/Alice can over-charge Bob by 0.8σ in the final period and not arouse Bob's burn response. Bob anticipates this reasoning, and now his expected cost in the next and final period is $\max(0, PNL^{true})+0.8\sigma$, which has an expected value of 1.2σ. At this point Bob realizes that if he does not burn, Oracle/Alice's final price report will cheat Bob by more than the burn fee as long as ExcessMargin>Burn Cost.

[5] If x a standard normal, $E(y|y=x \text{ if } x>0) = \frac{1}{2}\cdot E(x|x>0) + \frac{1}{2}\cdot (0|x<0) = E(x|x>0) = \frac{1}{2} \cdot \sqrt{2/\pi} \cong 0.4$.

For players with Excess Margin<Burn Cost, defaulting will be cheaper. Considering most MakerDAO contracts are overcollateralized by 100%, and the burn fee is 25% of RM, most counterparties will probably have more than 25% of their RM as Excess Margin, and rationally burn rather than default or continue.

Rational analysis nicely aligns with our less-rational instincts here. *Altruistic punishment* describes how people punish non-cooperators at a cost to themselves even in one-shot interactions where there is no chance of any long-run benefit. That is, people hate cheaters, and willingly pay to hurt them. Experimental and ethnographic data shows that altruistic punishment strengthens cooperation.[6] For example, in games like *tit-for-tat* or *the ultimatum game*, people cooperate more when there is an option for players to pay to punish other players who are playing a rational but socially uncooperative strategy. Potential cheaters rationally anticipate this individually irrational punishment, discouraging cheating.

7.2 The Value of the Walk-Away Option

Consider the strategy of playing until one generates a loss and then posting a fraudulent price. While the counterparty would probably burn, the cheating Oracle would have lost nothing. The strategy of walking away from the contract when their PNL is below some threshold, say, a -5% loss, even if every counterparty burns, is not zero.

There is a trade-off in such a strategy as higher returns imply higher risk. For example, the strategy of walking away from a substantial loss, say a -2.5σ outcome would take an average of 161 weeks for this to happen. While the expected cumulative payoff is 2.8σ of a weekly standard deviation, its standard deviation is 12.7σ, meaning their expected return would be between 15.5σ and -9.9σ, a poor Sharpe ratio and even worse in terms of time wasted. A rational cheating oracle has to balance the expected return to the time and volatility of such a strategy.

Looking at the cheat strategy payoff strategically is the classic *optimal stopping problem*. Specifically, Oracle/Alice's expected payoff is of the following form.

$$Cheat\ Strategy\ Profit = \left(\sum_{t=1}^{T-1} PNL_t \,\middle|\, T = \min t \text{ s.t. } PNL_t < k \right) \tag{A.22}$$

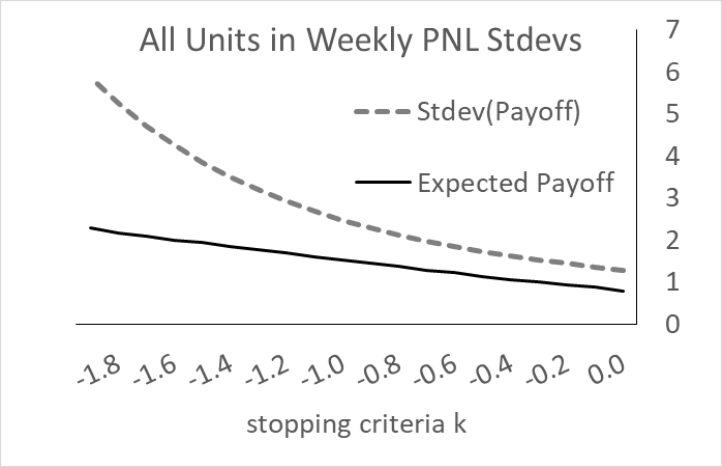
Diabolical Oracle/Alice's strategy is to post true prices until they imply that $PNL^{true} \leq k$, at which time they will report prices that imply their PNL=RM, Bob would burn, terminating the contract, and Oracle/Alice withdraw their margin ETH and move to Belize to work on their next white paper. The sum of PNLs up to time T has a positive expected value because the sequence of PNLs from 1 to T-1 are all random variables truncated from below. For example, if k=0, the only PNL that will accrue to Oracle/Alice will be positive.

Oracle/Alice's problem is one of maximizing a risk-adjusted return. While the *expected payoff* from such a strategy increases linearly as k moves from 0 to $-\infty$, the *volatility* increases exponentially. We can simulate this strategy, and the expected value and volatility has a simple closed form (see the Appendix of

[6] Fehr, Ernst, and Gachter. "Cooperation and punishment in public goods experiments." *American Economic Review* (1800). The innate human desire to apply costly vengeance paradoxically lowers violence as these hard-wired emotions act like commitment devices that discourage opportunistic, rational, but socially destructive acts, and is a crucial motivator for cooperative behavior. In contrast, in many species like lions and baboons, a new male alpha rationally kills the unweaned babies because females do not hold irrational grudges about sunk costs, and so soon become receptive mates for the new alpha, creating an incentive for the next alpha to kill the infants.

this appendix).[i] An excel spreadsheet at www.oracleswap.co shows how simulations of this strategy compare to the analytic formulation.

Figure 6
Expected Payoff and Volatility as a Function of the Stopping Criterion k



The *ratio* of the expected payoff to the standard deviation is maximized at around k= -0.5, though the maximum is very flat from 0 to -0.5. This implies Oracle/Alice's Sharpe ratio would be 90% near optimal, and a lot quicker and simpler if she used the strategy to walk away from her first loss. The expected total return to the optimal 'walk away from one's first loss' strategy is about 1σ, which is about RM/3.

If users were rational, cheating on one contract would destroy the viability of other contracts the cheating oracle services. Considering the most correlated assets offered would be the BTC, BTCETH and ETH contracts (~0.8), even if we assume these were instead perfectly correlated the evil but rational oracle would expect to walk away from a loss on those but not from their SPX contracts as well. This scales well because if OracleSwap adds 18 different assets, the correlation will decrease (e.g., XRP, Hang Seng Index), and so any 'optimal stopping program' payoff, which is its dominant source of cheating revenue, would be centered on a handful of assets while the annuity from all the contracts are lost, as no rational person should use a contract serviced by an oracle who 'only' cheated a different contract it serviced. Thus as the number of contracts increases, the cost/benefit ratio increases.

Data used in this example in OracleSwapData.xlsx available at www.oracleswap.co

7.3 Total Cost-Benefit to Cheating

The total of an exit scam is the sum of the unburnt final cheat, and the walk-away option strategy. Let us benchmark our payoffs via the Total OracleSwap RM, which is the sum of all the RM across all the asset subcontracts. We will denote this RM*. An Asset Contract attractive to hack will have many users, and many of those who might be co-conspirators will simply be accidentally aligned with the cheating Oracle's position side. This cuts down the percent of RM* hackable by at least ½. When combined with the fact that most players will burn rather than continue, say ¾, this cuts Oracle/Alice's final payoff to ½·(1- ¾) or ⅛ RM*.

Section 7.2 highlights the stopping strategy has an expected value of ⅓ RM. As other counterparties not part of the conspiracy would reduce this by another ½. This reduces the stopping strategy payoff to ½ ·⅓, or ⅙·RM*. In total a cheating Oracle can expect to garner ½ RM* (⅛+⅙).

If we assume subcontracts roll over every 2 months, then the Oracle expects 6 closes, and as each subcontract generates 1.5% RM in Oracle revenue, the annual dividend on RM* is 9%. Using the Gordon dividend discount model, a discount rate of 9% and a growth rate of 5% imply a present value of 2·RM*. Thus under very modest assumptions, an evil oracle would find it rational to use their Oracle revenue to further other evil schemes, because even evil people prefer more money to less (2>½).

Higher expected growth rates make the value of the annuity lost even greater, making cheating less attractive. The key is that unlike many other Oracle business models, even upon achieving a steady-state level of growth the Oracle finds honesty the dominant strategy. A seasoned OracleSwap oracle will have perfected the automated scripts that attend to its contracts, so its annuity stream would take virtually no effort or capital, a valuable asset worth preserving. This is a long-run incentive compatible mechanism.

8. Adverse Selection on Limit Order Books

Around 1812 billions of dollars were spent shortening the latency from 15 to 9 milliseconds for messages between New York (where cash markets trade) to Chicago (where futures trade), highlighting the value of a low latency advantage. In contrast to the high-frequency games where competition is over ten milliseconds, a blockchain user faces at least a ten-thousand millisecond lag. Compared to centralized exchanges, the blockchain latency forces market makers to post bid-ask spreads so wide they are unattractive to the noise traders they need to be viable.

Latency affects limit order books in the following way. Say you place an order to buy 100 shares of XYZ stock trading at a bid-ask price of $18.17-$18.18. You are probably not the first buy order in the $18.17 queue, so market orders will have to go through several levels to reach your bid. If the XYZ stock price will move up or down $0.05 before you would be able to cancel that order, you get filled only if it is now trading at $18.12-$18.13, meaning you bought at $18.17 and can sell now at $18.12; you lost $0.05. This mechanism is called adverse selection, because conditional upon getting filled you paid too much; if the price went up $0.05, you would probably not be filled on your $18.17 order to buy.

Price movement that can happen prior to reacting directly impacts the spread offered for this reason, whether the volatility is intrinsic to the asset, or due to latency issues from the blockchain. Given the latency of a blockchain is at least 100 times greater than for centralized exchanges, this implies a 10 times higher volatility ($\sigma \propto \sqrt{time}$) before the market maker can react, which implies a 10 time higher bid-ask.

Another way to look at this is as an option. Say Alice announces a limit order to sell at $100 when the current market price is $99. This is a standard ask in a limit order book, where resting offers are somewhat above the ‘true’ price. Say her offer is good for N seconds. Those who can react within N seconds have an option, because if the true price stays below $100 they are not obligated to buy, while if the price goes above $100 they have the right to buy at $100, locking in an instant profit. The greater the time lag the greater the value of the option.

Informed traders would be someone who has a latency advantage, or who has insider information on a relevant event. Such traders have, basically, a better estimate of the ‘true’ price than others. More prosaically, the advantage is merely that the trader knows they have to buy a lot of shares, so their initial price will be lower than their final fill price (statistically). The essential characteristic to all informed

trader trades is that they statistically anticipate the future supply/demand at the current price. Such traders inflict losses on market makers.

Noise traders are those with uncorrelated supply/demand. If they are trading based on a bogus theory such irrationality tends to be idiosyncratic. Yet, they could simply want to trade to use their money to buy a phone, or be making a portfolio allocation decision unrelated to future price movements. These traders generate revenue for market makers, and while small in trade size are more numerous than informed traders.

To counter the effects from informed traders the market maker does two things related to latency. First, she invests time and money into low-latency computers and algorithms to effectively reduce her relative latency: if she is the fastest she is not giving anyone an option regardless of her objective latency, because anyone 'in front' of the fastest trader is not reacting to relevant information quicker but rather randomly arriving for other reasons. As a practical matter the larger the latency, the larger the difference in latency among market participants; the larger the latency, the more valuable it is to invest it cutting edge technology. This obliges informed traders to do likewise, creating an arms race in infrastructure spending. Secondly, she increases the difference between her ask price and the 'true' price. This makes it less likely a faster trader will be able to exercise their option, and also allows her to make more money from the slower traders. In equilibrium, she only continues to post resting limit orders if she makes zero economic profit; the noise traders must pay for the informed traders.

The explicit cost of latency due to adverse selection for the fastest players is significantly less than the implicit costs generating by investing in capital and algorithms to minimize the explicit costs. This is true in other areas. For example, chargebacks are only about 1% of credit card revenue for most retailers, but companies tend to spend 5 times that in making sure it is under control. This is why credit card companies have what appears to be absurdly high equilibrium profits, in that the interest margin on credit cards is much higher than for other bank loans. But credit cards have a very active and energetic set of attackers, creating a perpetual arms race. These costs do not appear in the interest rate margin, but they are necessary as otherwise losses would be ruinous. This is why not just reducing, but eliminating the latency cost is so important, because it eliminates these non-explicit costs for Liquidity Providers.

As the spread widens, the number of trades decreases because it increases the net cost of trading. As there are other markets crypto markets, noise traders will flee any market where spreads are significantly higher because the short-term horizon preferred by noise traders is very sensitive to transaction costs. For example, a day-trader who pays 0.1% to enter or exit a trade, trading daily over a year, generates a 50% annual cost. Such a cost destroys many short-term strategies no matter how delusional.

Without noise traders, the remaining participants are then playing the unattractive game of trying to outsmart others who know at least as much as they do about market prices. The Milgrom-Stokey no-trade theorem ("Information, Trade and Common Knowledge." *Journal of Economic Theory*, 1982) states that if all the traders in the market are rational anyone who makes an offer must have valuable and true private information, or else they would not be making the offer, so accepting the offer would make them a loser. All the traders will reason the same way, and thus will not accept any offers. Another relevant result is Grossman-Stiglitz's "Impossibility of Informationally Efficient Markets" (*American Economic Review*, 1982) that shows how without noise trading no one has an incentive to put information into markets because the other rational traders infer what he knows via his market demand.

The bottom line is that a standard market maker is not merely taking on risk, as when they are forced to be long or short some asset when they have no opinion on its return, but more importantly, forced to subject themselves to informed traders that cost them money with statistical certainty. Unlike the standard

conception of risk that adds non-diversifiable volatility to one's wealth, ‘adverse selection risk’ is like the risk generated by accident claims in an auto insurer's portfolio, a statistically certain expected loss. The presence of informed traders generates a cost ultimately borne by the noise traders because in equilibrium market makers need to generate a zero economic profit, as otherwise they would exit. Without noise traders market making cannot exist, leaving casual traders placing small resting limit orders far off the mid-price, and trivial volume.

While adverse selection is a significant cost for high latency limit-order books, another consideration are games related to placing large orders. For example, say you place an abnormally large order on a central limit order book, an offer to buy 9000 shares at $14.23 when the market bid-ask is at $14.23-$14.30. A sneaky trader then often posts a smaller bid just above it (e.g., 100 @ $14.24). If the market goes down, they instantly sell to the larger order $14.23 for a modest $0.01 loss, while if the price rises profits are unbounded. This creates an attractive asymmetric payoff for smaller traders. To avoid this, large orders need to be parceled out at a size commensurate with the average best bid-ask size, necessitating many cancel and replacement orders. While algorithmic trading via direct market access to centralized exchanges can manage these issues efficiently, on the blockchain they add significant costs and time. Such tactics and their countermeasures are irrelevant in this contract due to market-on-close fill pricing.

These games are entirely avoided by forward-starting prices based on liquid cash markets. VWAP has grown in popularity because it minimizes trade impact and the day lag does not inconvenience long-term investors. As VWAP providers use cutting-edge high frequency strategies, users benefit from the latest algorithmic trading innovations, and also from the ability of VWAP providers to net customer orders, which reduces trading costs, a savings they pass off to their customers as they compete with other VWAP providers.

For the foreseeable future OracleSwap’s volume is too small for concerns about market impact on a 4 PM price. That is, moving or gaming the asset price at a point in time would take significantly more volume than OracleSwap will generate for the foreseeable future. If OracleSwap either became very popular or traded in illiquid coins, it would have to use an extended time window like the VWAP to mitigate the manipulation risk.

9. Complete List of Oracle/Admin Rights and Responsibilities

- Creates and publishes the relevant OracleSwap contracts
    - Asset Swap Contract
    - Oracle Price Contract
    - LP Book Contract
    - ***Risk Mitigation:*** all code is publicly available, allowing users to audit the code. An explanation of the contract’s security is available at GitHub.
- Updates Prices
    - 4:15 PM on NYSE business days
    - SPX targets the closing price. Crypto prices are taken in a couple-minute window around 4 PM.
    - ***Risk Mitigation:*** Per the contract code, updates cannot happen in the range of 30 minutes to 22 hours after the last Price Contract update. Any update older than 30 minutes is immutable for 22 hours. Allowing updates within 30 minutes makes it possible to rectify obvious errors—'fat finger' mistakes—that might get posted; disallowing updates

between 30 minutes and 22 hours prevents an evil Oracle from sneaking in a price on complacent investors who would have mistakenly thought they knew which prices were going to be applied to settlement. The burn option encourages victims to preclude an Oracle/Alice windfall, in that a cheating oracle will probably cheat again in the next period, so paying ¼ of one's RM to get out immediately is a way to minimize damage. This punishment needs players to have time to react to any oracle mischief, and they will have at least four hours to react.

- Price Initialization
    - 3:45 PM for new trades each business day, 15 minutes before close.
    - This sets the initial day referenced in the first week of a subcontract. It is only relevant for new contracts, as subsequently all subcontracts will use Wednesday prices as their initial and final price in at settlement. Any pending subcontracts taken prior to the Price Initialization then start at the next Oracle Price Contract's prices. For instance, a take on Monday at 1 PM would use the Monday closing price, a take on Monday at 6 PM would use the Tuesday closing price. It is a function run on an LP's entire set of newly taken trades on a particular business day.
    - ***Risk Mitigation:*** If the oracle does not run this function prior to the Oracle Price Update (4:15 PM) the Price Initialization would set the initial price to the subsequent Oracle Price Update date. This delays the subcontract start by another day, but as forward-starting contracts have an expected value of zero prior to starting, no loss is incured.
- Compute Settlement Returns
    - Prior to Weekly settlement, after the Oracle Price Contract update that is flagged as a settlement date.
    - To process settlement efficiently we separately calculate the net return plus the financing fee for every possible starting price, generating 10 datapoints, in that each week there are five potentially different initial prices (contracts taken on Wed, Thursday, etc.), and also that the long and short have different funding rates (5×2=10). These returns can then be simply applied to ETH notional amounts and ETH prices per the PNL formula. This function also sets Target and Basis rates for the subsequent week, applying the proposed Target and Basis rates that are documented via event logs.
    - ***Risk Mitigation***: This can only be run at least 5.5 days after the most recent settlement. If settlement does not occur for 8 days, all users can access their margin, as the first users to attempt to withdraw from an LP book—including the LP—after 8 days (measured in seconds) of no settlement, sets the RM for all players to zero.
- Weekly Settlement
    - 9 PM ET Wednesday
    - Holidays move settlement backward: a Wednesday holiday implies a Tuesday Settlement date for that week.
    - ***Risk Mitigation:*** Cannot be run for 4 hours (measured in seconds) after the most recent Oracle Price Contract Update, giving users time to burn their PNL rather than let an evil oracle steal their money. It also cannot be executed within 5 days after most recent Weekly Settlement. This makes it difficult for the oracle to sneak in a bad price while users are unaware. To the extent the oracle neglects an LP and does not execute its subcontracts, all counterparties to the LP in question can access their entire margin after 8 days of no Weekly Settlement. If settlement is late due to network congestion, say 11 PM, it would still use the 4:15 Oracle prices as if settled at 9 PM. This function can only

be run using Compute Returns Function results that have been calculated during the Settlement period.

- Updates Basis and Target Rates
    - These rates determine the Long and Short financing rate applied weekly. The target rate is the same for both, and the basis is applied symmetrically, added to the long's target rate, and subtracted from the short.

$$FundingRate_{Long} = Target + Basis$$
$$FundingRate_{Short} = Target - Basis$$

    - ***Risk Mitigation:*** Target rates are constrained to be within 0 and 1%, the basis within – 2% to 2%. In a worst-case scenario, an evil oracle would set an extreme set of rates just before the Compute Returns function is run. This would then affect the next settlement's PNLs, giving users a week to react. While extreme rates may look unfair such an evaluation can be subjective, as basis rates do go above 100% annualized for several days at BitMex. The rate adjustments should be consistent with encouraging takers to put on more of the side (long or short) that has less outstanding within any asset contract. As the funding rate would at most be 3% in absolute value, this is at most ⅓ of RM for our contracts (in the LR=10 SPX contract), a 1-σ payoff, which is similar to the size of the evil oracle's expected payoff from an exit scam discussed in the cheating oracle. This payoff is dominated by the expected value of an oracle's close-fee annuity under modest assumptions about contract use, so cheating in such a way would be irrational for the same reasons given in analyzing the cheat option.
- Pauses new Takers
    - If the contract were deprecated, the Oracle/Admin would stop new Takers from creating contracts.
    - ***Risk Mitigation:*** this does not affect existing contracts. Preventing use of this contract does not steal from anyone, just as not selling you a donut does not steal from you.
- Process Defaults
    - Subsequent to settlement if there are defaulted subcontracts.
    - At settlement a default requires the subcontract be deleted from the array of active subcontracts for an LP. The settlement function is OracleSwap's most gas intensive contract. Moving this costly action of deleting data to a subsequent function minimizes the worst-case gas scenario that constrains the number of active subcontracts an LP can have.
    - ***Risk Mitigation***: Deleting a subcontract after it is terminated does not affect the default settlement's processing of PNL. An oracle not running the default function on defaulted subcontracts would cause the number of active subcontracts for an LP to increase until eventually the LP would not be able to complete the settlement function due to gas constraints. In this case of negligence, however, users can withdraw their margins after 8 days of the last settlement, so their funds would not be stuck.
- Unilaterally Cancel Subcontracts
    - There are two scenarios where this can happen. First, if the contract were deprecated, the Oracle/Admin would eventually cancel existing subcontracts, which would be like a user cancel only no close fee is assessed to either counterparty. Secondly, as defaults are computationally costly in the settlement function, the number of defaulters is the edge case that puts a limit on how many takers an LP can handle. While it is possible all 30 or

so takers might default, in practice this would be some sort of strange DDoS attack, perverse in that it would be costly to the attacker. In such a case the Oracle could cancel most of these defaults during the settlement period, which would then relieve the defaulter of any default or closing fees. Yet by affording this option for this improbable scenario the maximum number of LP takers is doubled.

- ***Risk Mitigation:*** a unilateral Oracle/Admin cancel would not adversely affect either counterparty's PNL, it just cancels all subsequent exposure for both counterparties and no cancel cost is applied to either party.

10. Player Contract Management

Settlement: This occurs around 9 PM Wednesday, the prior business day if an NYSE holiday. This function can only run at least 5 days after the previous settlement. The Oracle Price Contract is updated around 4:15 PM on NYSE business days. The *settlement period*—between Wednesday Oracle Price Contract update and the settlement later that day—allows each player at least 4 hours to cure their margin to avoid default, as they will know their upcoming RM with certainty as it is hard coded in the Settlement Function. Withdrawals are not allowed during the settlement period so players can better anticipate an impending default by a negligent counterparty (this generates no extra risk because excess margin is not at risk at settlement). Oracle Price Contract updates and settlements generate event logs.

Cancel: A cancel causes the next Settlement to terminate the subcontract after applying the PNL to the margins. Cancels are not allowed during the settlement to encourage a burn if cheating is suspected. Thus, a player wishing to cancel at the next settlement must cancel before the Wednesday Oracle Price Contract update at around 4:15 PM (to be safe, cancel prior to 4 PM). A cancel generates an event log allowing players to know when their subcontract has been cancelled.

Burn: Players can burn their PNL only during the settlement period, and the inability to cancel during the settlement period makes burning a cheated party's dominant choice. By encouraging punishment that would preclude a cheating Oracle's payoff, we make honesty the Oracle's best strategy.

A burn terminates the subcontract at settlement and sends the burn fee as well as the PNL debit to a burn address (0xDEAD). A burn does not change the *burner's* credit/debit. For example, if Bob’s PNL is - 10 ETH, a burn would still debit his margin by 10 but his counterparty would then not receive the 10 in PNL that would have occurred without the burn; if instead Bob’s PNL is +10, Bob still receives 10 ETH. This makes the margin cost of the burn independent of Bob’s PNL, simplifying his response strategy.

Burning is a payable function, making accidental burns less likely, with a payable fee equal to RM/4. A burn automatically generates an event log documenting the relevant suspicious contract prices, making it easy for potential players to assess the merits of the allegation and thus our Oracle's reputation.

Default: As players cannot withdraw their margin below their RM, this means a Taker default can only occur if a negative PNL debits their Margin to below their RM during the Settlement processing. A default does not cost its counterparty in that at settlement all players processed must have their RM, which is the maximum amount any player can receive. A default fee of 12.5% RM is debited from the defaulter’s margin to make default strictly inferior to cancelling, and to discourage negligence that creates an inconvenience to counterparties. If they defaulted with zero excess margin they basically ‘get away with it,’ though this is improbable, an annoyance as opposed to costing the counterparty anything. Default

fees are sent to the oracle, and the defaulter's subcontract is terminated immediately (for LPs, all of their subcontracts are terminated).

Continue: Prices posted to the Oracle Price Contract on Wednesday are applied to that night's Settlement, and may lower one's margin below their RM. If players have funded margins adequately so their total margin is above the RM after the PNL attribution, and no Burn, Default or Cancel has been recorded, the subcontract continues; continue is what happens if 'nothing' happens.

Margin. An LP initiates their position by posting ETH into an Asset Swap contract. Takers can then go long or short on these LPs. Only the owner of the address can withdraw from their margin.

A Taker or LP's total ETH margin, or actual margin, must be greater than or equal to their Required Margin at all times. An LP initially posts ETH margin, and when a taker takes he posts ETH margin >= the RM for his subcontract. A taker's RM is defined by their subcontract RM alone, while an LP's RM is netted over their portfolio. A player may wish to overfund their margin to avoid the gas costs of sending ETH in a needed cure, especially as the excess margin is safe from any worst-case scenario of oracle mischief.

No player may withdraw their margin below their Required Margin (RM) amount at any time.

The excess of *total* or *actual* margin minus RM is the 'excess margin,' and players can withdraw excess margin any time outside the settlement window. A player with margin=RM who sees a PNL<0 about to be applied will need to cure this by sending ETH≥abs(PNL) to their margin *before* the Settlement.

Redeem: When a player cancels, defaults, or burns, they must redeem their contract to withdraw their margin. This separate step minimizes the gas costs at settlement, as it involves changing the state via eliminating a contract from the LP's book. Once this is done, players can withdraw their margins.

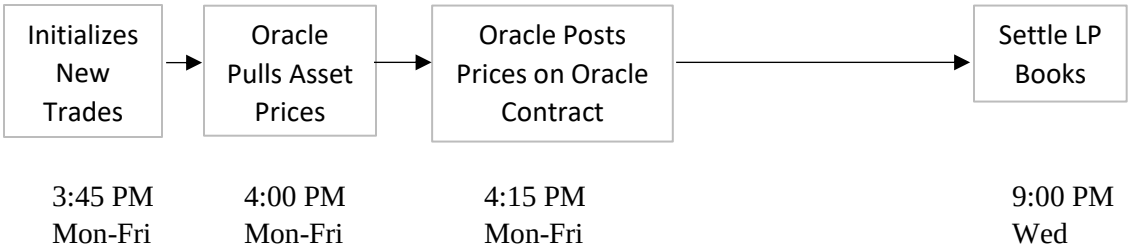
Withdrawal Balance: When a player wants to withdraw money from their Margin they must first transfer ETH to their Withdrawal Balance, and then execute a separate withdraw function to remove this ETH to their personal ETH accounts off the OracleSwap contract. As the Withdrawal Balance does not count towards their RM and cannot be transferred back to their margin account, this should only be used as a temporary station (though, it will not disappear if left alone). This two-step withdrawal process prevents re-entry attacks.

Inactive Oracle/Admin: After nine days without a Settlement, when the first player within an LP's book attempts to transfer money to their Withdrawal Balance, all counterparty RMs within that LP's book are set to zero. This protects investors if our Oracle/Admin becomes incapacitated.

Taking: A take can occur at any time, and sets the initial price at close subsequent to the subcontract's Price Initialization. A Price Initialization is run around 3:45 PM and generates an event log, allowing users to see if their take occurred in time (to be safe, best to take prior to 3:30 PM).

Termination: A burn or cancel notice terminates the contract at the next Settlement; a default terminates the contract on the Settlement when it defaults. On termination, after settlement applies the final PNL to the respective margins, the RM for both counterparties on that subcontract is set to zero, and no further settlements are applied. Players can then withdraw whatever excess margin they then have (as if RM=0 then excess margin= margin).

11. Trade Timeline



Trades can occur any time. New trades will be recorded at the subsequent Trade Initialization function that is run at 3:45 on business days. A trade recorded on this day will use that day's 4 PM price as its open price for that week's PNL.

Settlement only occurs on Wednesday. The settlement function is run on each LP book with active contracts. PNLs are processed, debiting from the loser's margin to the winner's margin for each particular subcontract. Required Margins are recalculated for LPs, netting new exposures: at settlement the LP's RM is set to abs(Long – Short). If a player's total margin is less than their required margin upon settlement they default at this settlement, a default fee of 12.5% of their RM is assessed, and the subcontract is immediately terminated.

A player will know exactly what their PNL will be given the Oracle Price Contract update at 4:15, though they should have a good estimate earlier in the day. Any player who anticipates their current margin, after the PNL is applied, will be below their Required Margin, should cure their position by sending ETH to their margin to avoid default.

Takers can take positions, LPs can post liquidity, any user can add funds to margin at any time.

Cancels cannot occur during the settlement period, only burns. Players cannot withdraw money from their margin during the settlement period. This is to encourage burns in the case of an evil Oracle.

NYSE holidays are observed as weekends, where no price is recorded. If a settlement date is a holiday, settlement will occur on Tuesday.

11. Who is the Oracle?

As creator of this suite of contracts I am primarily motivated by my support for the many benefits generated by cryptocurrencies, hoping this contract will help the community flourish. Given this I would do it for mere gas costs, yet without Oracle revenue outsiders would have to trust my good intentions as opposed to my self-interest, an unreasonable request. The cost function for an honest oracle is primarily the opportunity cost of cheating, which requires the oracle generates revenue.

With automation the amount of human input needed to act as the Oracle/administrator is almost zero, yet the process will need a human touch for the foreseeable future, as servers crash, data providers change their protocols, etc. Any human receiving revenue for this role would invite regulatory attention and also be vulnerable to a $5 wrench attack. While I am currently anonymous, I may not always be, and so to make OracleSwap robust I gifted the rights and responsibilities of the Oracle to an acquaintance who is

rational, intelligent, ambitious, and most importantly in a different country. The creator of OracleSwap is not its Oracle.

12. Supporting Documents

- Worksheets within OracleSwapData.xlsx on the oracleswap.co website provide more data on the following
    - PNL Simulations with historical data
    - Hedge Simulations
    - Oracle Cheat Simulation
    - Marginal Vol and Sharpe Worksheet

13. Definitions

Asset Swap Contract: Each asset serviced by the Oracle Price Contract has a separate Asset Contract. That is, BTC will have a separate contract than the SPX. They are all basically identical, just with different reference assets, and different values for a Basis Rate, Target Rate, and Leverage Ratio.

Basis: The adjustment in a CFD or swap contract that accounts for interest rates, dividends, storage costs, convenience yield, and risk premium. This is implicit in the difference between a futures/forward and cash price, but for a swap there is only a cash price, so the basis is applied as an effective funding rate, applying symmetrically to longs and shorts (subtracted from the long return, added to the short return). In this contract, the basis is merely a subset of the funding cost, which also includes a Target Rate that is the same for longs and shorts for a specific asset. The basis can be considered the price that equilibrates long and short swap demand, and is constrained to be between -2 and +2% per week.

Book Contract: When a player first posts as an LP, the asset contract creates a unique contract for that investor's contract address that will hold all that LP's counterparties. While all players always interact with the base Asset Swap Contract, this then transacts with the active LP Book Contracts. This has several reasons, including reducing the ETH held in a single contract, allowing greater modularity, and that the logic lends itself to a contract data structure rather than a struct.

Burn: A counterparty can burn their contract, which then prevents their counterparty from receiving their debit at the subsequent Weekly Settlement. The payable burn fee and the burner's PNL (if negative) are sent to the burn address: 0xDEAD.

Business Day: A business day corresponds to a New York Stock Exchange business day, and are the only days that an initial subcontract price is set, or that a Weekly Settlement can occur. The Oracle Price Contract does not record non-business day prices, or initialize subcontracts on these days, though players can take on these non-business days and their subcontract will initialize at the next business day. Business days thus exclude weekends and about 9 recognized holidays. These can be found by Googling 'NYSE holidays' which are published three years in advance. Half-day holidays will use the 4 PM crypto price, though the SPX price will use the 1 PM official closing price.

Cancel: A counterparty who wishes to terminate the contract initiates a cancel. This must be done before the Wednesday Oracle Price Update around 4:15 PM.

CFD: A Contract-For-Difference is like a futures contract in that counterparties put up a fraction of the notional, their margin, and use an asset price for generating a mark-to-market PNL on that notional amount. Unlike futures the reference is not a separately traded price, but rather the cash price, so to account for the basis we see in futures market, long and short positions are charged different funding rates.

Closing Price: Price taken from approximately 4:00 PM ET on NYSE Business Days. We use the official close for the SPX, which refers to 4:00 PM but is finalized around 4:10 PM.

Subcontract ID: A subcontract's ID within a particular LP Book Contract. A subcontract is then uniquely identified on the Blockchain via a LP Book Contract address and subcontract ID.

Default: If a counterparty's margin is below their subcontract's Required Margin at settlement the subcontract defaults and is terminated. This can only occur at the Weekly Settlement, as investor withdrawals below a subcontract's RM are not allowed, and an LP's change in net margin, or a PNL debit, can only be applied at the Weekly Settlement.

Fed Funds rate: The overnight interest rate at which US banks lend to each other. It serves as the basis for the cost of funds among financial institutions and is the opportunity cost of a US dollar.

Forward-Starting Price: a contract price set after an agreement to open or close a position is made, such as the next closing price or the next day's value-weighted average price.

Funding Rate: The weekly rate applied to the Taker. This rate is subtracted from the return for the taker and applied to the notional amount. These can be negative, in which case, would add to the Taker return. Funding Rates vary by asset. It is defined as

$$FundingRate_{Long} = Target + Basis$$
$$FundingRate_{Short} = Target - Basis$$

Leverage Ratio: The OracleSwap's leverage ratio is the ratio of the notional to the RM for that asset. It can be thought of as the inverse of the required margin ratio.

LP: A liquidity provider. They post an amount available for long or short takers. They are paid via funding rates on their gross exposure for the unpredictable risk generated by ending up net short or long.

Market-on-Close: A Market-On-Close (MOC) order is a non-limit market order that is executed at some official closing price, which is at 4 PM for US stock markets. MOC orders do not specify a target price, as these are forward-starting, and thus unknown at the time of order. OracleSwap basically uses MOC orders, but as there is no official close in crypto markets, we use a couple minute window around 4 PM, which is very much like a close price.

Margin: this is the total ETH attributed to a counterparty. A Taker with several different subcontracts will have a separate margin for each, while an LP will have one margin for all her various counterparties.

Max Long/Short Take: this is the most a taker can take, long or short, for a given LP. It is a function of the LP's current book. For example, if the LP shows 100 Margin with no positions, a Taker can only go long or short 50. If the LP shows a margin of 100, with the LP currently long 100, Takers can only go short.

Max Long Take = ½ LP's ExcessMargin + LP's Short – LP's Long
Max Short Take = ½ LP's Excess Margin − LP's Short + LP's Long

Net Margin: An LP's Required Margin is netted, meaning it is the difference between the gross long and short for an LP. For example, if the gross long is 80, gross short is 50, the net margin is 30. Only the LP has an RM based on a Net Margin. For a taker there is no netting if they take offsetting positions

Notional: Notional is the amount applied to the reference asset return. It is generated by multiplying the RM by the Asset Contract's specific Leverage Ratio and then the currency of the asset's denomination. For BTC, ETH, and SPX this is in USD per ETH; for BTCETH it is in BTC per ETH.

Oracle Price Contract: The Oracle Price Contract warehouses the asset prices of all Asset Contracts serviced by OracleSwap. It contains all the information needed to calculate subcontract returns, and so holds the closing prices for the current week (i.e., last Wednesday to current date). It is extensible, allowing OracleSwap to add Asset Contracts, like XRP or the Heng Seng index. Updates generate event logs. The Oracle posts at 4:15 PM, and the Asset Contract accesses this via a getter function.

Player: Synonym for an OracleSwap counterparty or investor; an LP or Taker.

PNL: Profit-n-loss, the cash flow between two parties of a subcontract, where the loser/debtor has a negative PNL, and the winner/creditor has a symmetric positive PNL.

RM: Required Margin. Each subcontract has a specific RM for its life, in units of ETH. RM must be greater than or equal to the LPs minimum RM, and in integer amounts.

Price Initialization: The first business day closing price is applied to a newly instantiated subcontract (i.e., bilateral agreement) at the initial settlement via a Price Initialization Function, which is applied around 3:45 PM, so that all new Taken subcontracts will have their first Price using the subsequent closing prices. Subcontracts taken after this will use the following business day as their initial settlement price.

Settlement: Settlement is applied Wednesday at 9 PM to all LPs with active subcontracts via the Settlement Function. This uses the Wednesday closing prices recorded in the Oracle Price contract to the subcontracts and then transfers the resulting PNL from the debtor to the creditor. If Wednesday is an exchange holiday (e.g., Christmas), the prior business day, Tuesday, will be the settlement day.

SPX: The SPX is the index for the S&P500 portfolio, a value-weighted index of the top 500 US companies. It is a cash index that excludes dividends. In contrast, the SPY is an ETF that trades on stock exchanges, and so its price is dividend adjusted.

Subcontract: a bilateral agreement between a Taker and LP. It has a specific RM for its life. An LP can have several subcontracts within a particular asset contract.

Swap: A swap in the context of this document is a CFD and so has no expiration (e.g., a perpetual swap). A swap account nets a user's positions to generate their required margin and total PNL, and its mark-to-market is based on the cash price of its reference assets; it also charges a funding rate to long and short positions. Prime brokers use these to provide hedge funds a way to avoid stamp taxes and allow them mask its positions for strategic reasons. Thus for equities, their CFDs are often in swap accounts—swapping the cashflows from long and short equity positions—and 'swap' vs. 'CFD' terminology is a matter of preference.

Taker: A counterparty to a subcontract that takes an LP offer. The taker determines the side (long or short) and size (RM).

Termination: When a contract ends for any reason—burn, cancel, default—its termination occurs at the Wednesday settlement. This then sets the subcontract's RM to zero, allowing the Taker to withdraw his total margin, while the effect on an LPs margin is ambiguous.

Withdrawal Balance: This balance is a way station for withdrawals, used to prevent re-entry attacks. A player wishing to take ETH out of their Margin first withdraws from their margin to their Withdrawal Balance, and then from this Withdrawal Balance to their off-contract public address.

---

i Oracle Optimal Stopping Problem

The expected value to a truncated random normal is

$$E\left(x\middle|x>k\right)=\frac{\phi(k)}{1-\Phi(k)}$$

The expected number of periods *t* until the exit criteria is reached is:

$$E\min\left(t\middle|x_t<k\right)=\frac{1-\Phi(k)}{\Phi(k)}$$

The expected payoff to reporting true prices until the implied PNL for evil Oracle/Alice is below *k* is then

$$E\left[cheat\ strategy\right]=E\min\left(t\middle|x_t<k\right)\cdot E\left(x\middle|x>k\right)$$
$$=\frac{1-\Phi(k)}{\Phi(k)}\cdot\frac{\phi(k)}{1-\Phi(k)}=\frac{\phi(k)}{\Phi(k)}$$

For example, if *k*=0, then $\phi(0)\big/\Phi(0)\approx 0.399/0.50\approx 0.8$

while if *k*= – 0.5, we have $\phi(-0.5)\big/\Phi(-0.5)=0.386/0.401\approx 0.96$

Another way to see this, is by looking at the following sequence for the case where k=0. Each period the expected return conditional upon the return being >0, which is sqrt(2/π), or around 0.8.

$$E\left[cheat\ strategy\right]=\left(\frac{1}{2}\right)\cdot 0.8+\left(\frac{1}{2}\right)^2\cdot 0.8+\left(\frac{1}{2}\right)^3\cdot 0.8+...$$
$$=\left(\frac{1}{2}\right)\cdot 0.8\cdot\left\{1+\left(\frac{1}{2}\right)+\left(\frac{1}{2}\right)^2+...\right\}$$
$$=\frac{0.4}{1-1\big/2}=0.8$$

The closed-form solution for the standard deviation of this summed sequence is left as an exercise for the reader but is approximately the square root of the number of expected periods. Simulations are straightforward.