Gild Lab.

Making Money with ETHg

GILD LAB LIMITED

Company number

Address Unit , Mill Street, Ottery St. Mary, England, EX AD

Contents

Making money with ETHg

Speculation

Because ETHg is an ETH/XAU pair any speculative pro f ts should be denominated in ETH or XAU. ETHg price is above XAU If at any point ETHg:XAU spot price is greater than an immediate pro f t can be taken.

For example, let ETHg be worth x XAU and ETH worth y XAU.

Gilding mints ETHg at the ETH:XAU spot price, so locking ETH yields y ETHg.

Gild ETH for y ETHg Sell y ETHg for xy XAU Sell xy XAU for xy/y ETH

If x > then the gilder now holds more ETH than they locked in order to gild.

Steps and look a lot like order routing on a DEX where intermediate tokens (in this case XAU) cancel out.

This means that any intermediate tokens between ETHg and ETH will allow this to work.

If ETHg:XAU spot price is greater than then the ETHg contract will mint more than ETH worth of ETHg for ETH locked. The ETHg contract does NOT know the ETHg:XAU spot price, it ONLY knows the ETH:XAU spot price.

The ETHg supply should rapidly expand when the contract is minting pro f tably.

Problem/Opportunity:

This pro f t is guaranteed only under conditions:

Steps through can be completed atomically and in time There exists intermediate token pairs to route from ETHg to ETH

Both of these conditions are worth discussing.

Atomicity and timeliness:

If steps through are completed independently then it's possible that prices will f uctuate. All the trades need to be completed within a single transaction to avoid this.

We can write a wrapper contract that:

Precalculates expected outcome and returns as early as possible if not profitable Gilds Uses or implements liquidity aggregation (e.g. 0x protocol https://protocol.0x.org/en/latest/) Sells ETHg for ETH into the aggregator Takes an optional fee

The optional fee can be specified by the caller, like a tip/donation, and of course our default front end would prefill the tip and send it our way (business model).

One issue with this is MEV. The moment a signed transaction hits the public mempool a bot will simulate the outcome, see the profit and replay a duplicate transaction with more gas so that it executes first. The bot pockets the profit and the user pays gas for a transaction that may now fail.

One solution is a private mempool that promises not to front-run. These are becoming more standardised and accessible as MEV becomes better understood and commoditized. Examples include flashbots, eden, openmev, etc. Perhaps we can integrate with a private mempool, giving users another reason to use our contracts and front end (business model).

Intermediate tokens:

If there is no liquid route from ETHg to ETH then the profit doesn't exist and so the supply will never increase.

A direct pair on ETH:ETHg on a DEX doesn't make much sense for the same reason an ETH:XAU pair doesn't - the expected impermanent loss is too high due to ETH mooning over the long term.

The main thing to enable routes back to ETH is that we have ETHg:XAU token pairs with liquidity. By XAU tokens I mean tokens with a centralized peg to gold somehow.

This becomes a hub/spoke model, similar to how DAI is a "decentralised stablecoin" that has decentralised collateral and trades against centralised stables USDC/USDT/USDetc. - ignoring the fact that like % of the DAI collateral itself is USDC

Realistically, steps and above are the most important to do atomically, which does still need a wrapper contract to ensure (business model). Once the user has sold their y ETHg for more than y XAU tokens, they are free to find a path back to ETH "fast enough" but not necessarily within a single transaction.

Of course, there may be a path, for example:

PAXG -> DAI (uni) -> USDT (crv) -> ETH (crv tricrypto)

Chains with more TVL/usage are more likely to have paths but also more likely to have high gas. A long path means higher gas and slippage.

It may well be more profitable for the user to simply take their XAU token to binance and swap it for ETH there. The native portal for the XAU token may also have a way to swap for ETH.

Can an individual do this?

Maybe.

Provided the opportunity arises, it would be " click" to use the wrapper contract to swap out ETH for AUX or even more ETH. An individual doesn't suffer nearly as much counterparty risk as a DAO would by swapping into the gold token of their choice and dumping it somewhere.

The main issue would be that a bot is much more likely to scoop this up than a human.

Can a DAO do this?

Unlikely.

This opportunity is rare and short lived.

The only way ETHg price can be above XAU price in practice is if somebody first bought ETHg for a worse price than they could mint it. This scenario is supposed to never happen, or be very unstable if it does.

It's good to consider it as a thought experiment (to understand the price cap). The gild+trade contracts are still worth building (see below) for speculative leverage.

The full atomic path swapping ETH in for ETH out can be done by any entity, including a DAO, but the rarity and the MEV issues make it unsustainable as a business model.

The partial swap is problematic for a DAO as it involves holding a centralised intermediary token, e.g. to then go and dump on Binance. The counterparty risks and logistics of this vs. expected profits aren't justifable. ETH price will go up relative to ETHg Broadly ETH has outperformed XAU over its history.

Given that ETHg can't substantially and sustainably outperform XAU over a long period, we'd expect ETH to also outperform ETHg over time (see above).

If a user expects that ETH will go up relative to ETHg they can do the following:

Gild ETH for x ETHg Sell x ETHg for y ETH Wait for y ETH to be worth more than x ETHg Buy x ETHg for less than y ETH Ungild ETH

The user now holds more than ETH. They effectively leveraged their ETH without liquidation risk.

The amount of additional ETH the user holds is whatever the price ratio between and is, multiplied by y ETH, which is itself the ratio of ETHg to XAU token.

For example, if ETH is worth XAU and ETHg is worth . XAU then:

ETH => ETHg => XAU => . ETH

From here there are two ways that ETH can appreciate relative to ETHg.

ETH to XAU ratio can remain constant while ETHg to XAU ratio drops ETH to XAU ratio can increase while ETHg to XAU ratio remains constant

Of course, in reality no price stays constant, both of these can move independently or even cancel each other out. What matters is the overall ETH to ETHg ratio, because ETHg MUST be bought back to ungild the original ETH.

Because of the vault system, no matter the current price of anything, ETHg is always required for this example to ungild ETH.

If the ETHg to XAU ratio drops to . and ETH is still worth XAU then:

ETHg => . XAU => . ETH

This means we can ungild our original ETH for . ETH while we're holding . ETH, a . ETH profit.

Similarly if the ETHg to XAU ratio remains . and ETH is worth XAU then:

ETHg => XAU => . ETH

This means we can ungild our original ETH for . ETH while we're holding . ETH, a . profit.

Problem/Opportunity:

Note that mechanically this is all identical to the earlier atomic profit scenario (business model), but there is a period of time that the user holds both ETH + a vault with specific ETHg denominated unlock price/amount.

The atomicity and MEV issues completely go away for a speculative play like this, but the liquidity and availability of intermediate tokens increases.

The user is not liquidated, but for as long as the ETH/ETHg ratio is worse than they gilded and sold their ETHg at, their vault is effectively worthless.

Consider ETH is worth XAU and ETHg is worth . XAU. At the time of writing this is a high ETH price, and ETHg is looking pretty oversupplied relative to earlier examples.

If someone leveraged ETH at this point:

ETH => ETHg => . XAU => . ETH

They now are locked in to requiring ETHg to ungild.

If ETH drops to XAU and ETHg remains . XAU then:

ETHg => . XAU => . ETH

The user is now holding . ETH and requires . ETH to unlock. They would lose . ETH overall and be left with . ETH if they tried to ungild right now.

If ETH remains XAU but the ETHg ratio climbs to . XAU then:

ETHg => XAU => . ETH

This is even worse, the user is holding . ETH and requires . ETH to unlock. They would lose . overall and be left with . ETH after ungilding.

At a high level the protocol is redistributing ETH away from people who are minting and immediately dumping ETHg when:

The ETHg to XAU ratio is low (ETHg oversupply) ETH is relatively high already (high risk of collateral price drop) Impatient and ungild at a loss

The protocol rewards people who are:

Minting when ETHg ratio is high (ETHg in demand) ETH is relatively low already (low risk of collateral price drop) Patient enough to wait for ratios to hit their targets

The reason why this is better than a liquidating protocol is that the user is not harmed by dramatic short term price swings. A %+ drop can happen in a matter of hours in crypto and almost all leverage is wiped out due to liquidations in these events. This means that the user's original collateral is dumped on the market, which harms the user who may literally never recover their collateral in their lifetime, and harms the market as huge capital is dumped as liquidations cascade.

During the drop:

Almost all existing vaults will be locked ETHg will be minted but ideally not sold (see below) ETHg may even be purchased much as stables currently are

After the drop:

New vaults will open in anticipation of price recovery ETHg:XAU ratio may be unstable

After recovery:

Pre-drop vaults are all unlocked, assuming similar ETHg:XAU ratio Many new vaults from the drop may be closed out in profit

Can an individual do this?

Absolutely.

This is one of the main retail use cases.

It makes total sense that people would use and even pay a premium for some kind of dashboard that has analytics and makes all this easy (business model).

Anyone who is an ETH permabull and can be patient if their vault is locked due to short-term price fluctuations, and wait to open a vault when the ETHg:XAU ratio is favourable, can do this and profit.

There are no front-running/MEV issues, the main thing is the ability to spot trends, take action and be patient.

As the input and output is both ETH, there is no counterparty risk beyond momentarily holding gold tokens during trades (or not even that if a full-path atomic swap).

Can a DAO do this?

Probably.

Any entity can profit this way. A DAO with an explicit mandate to be patient and help manage supply should be able to profit.

One thing that's nice is that it is always possible to calculate the ETH + vault holdings in a pure ETH-denominated summary using onchain data, and to know exactly how much ETHg is required to profitably unlock vaults at any moment, and how far underwater frozen vaults are.

A DAO could have regular risk/governance meetings broadcast on youtube similar to makerDAO and do all kinds of deep analysis on when to gild/ungild.

Purpose-built smart contracts could be written that issue governance tokens pro-rata for any ETH that users deposit, and can be redeemed (burned) pro-rata for underlying assets. As everything is ETH denominated there's no counterparty risk, complex whitelisting, or ambiguous calculations.

The main value-add for participating in the DAO would be "wisdom of the crowd" behaviour for pro f ting o f the system, hopefully more than any individual has time/knowledge to do themselves.

Questions/Challenges:

How to make governance decisions? Pure onchain? Voting? Mix? Something else? Can the onchain DAO contract be totally autonomous based on parameters/allocations of gov token setting thresholds, or does it need admin keys? Will the DAO have too many assets? I can see, especially early days, that the demand for ETHg from end-users and LPs being much less than people would like to leverage against (read: sustained and very low ETHg to XAU ratio) with DAO-sized allocations The DAO could easily fuck up and lock most or even all the DAO's funds for a very long time if they gild and dump ETHg at a particularly bad ratio, if anyone new deposited ETH they'd be essentially bailing out existing participants so it would probably kill or freeze the DAO while all the members waited for a recovery

ETH price will go down (temporarily) relative to ETHg If you think this will happen then you can mint ETHg but DONT sell it immediately.

Instead you can just hold ETHg in your wallet.

If ETH price drops relative to ETHg you can then buy ETH

If the ETH price does NOT drop then you can ungild your original ETH and lose nothing relative to hodl.

For example, ETH price is ETHg (e.g. ETH is XAU @ . ETHg ratio)

ETH => ETHg (gild)

If ETH price becomes ETHg (e.g. ETH is XAU @ . ETHg ratio)

Now you have ETH in a vault and you can buy another ETH with the ETHg. If the price recovers back to ETH at ETHg then you can sell . ETH to ungild your original ETH and be holding . ETH total.

If the price never drops and ETH increases to ETHg you can use your ETHg to ungild your ETH (which is now worth more).

If we compare this to trading at and ETHg prices rather than gilding.

ETH => ETHg (sell high) ETHg => ETH (buy low) Total ETH profit

ETH => ETHg (sell low) ETHg => / ETH (buy high) Total / ETH loss

So the gilding offers a lower risk and reward way to pre-empt market dumps, in that it has an "undo" button up until a sale is made. This protects against opportunity cost when the market in fact goes against you to the upside.

Also note that if the ETHg to XAU ratio stays steady during a drop then gilding when the ETH market is "high" has a similar effect to "stabling up", because it can be sold in small amounts to pay for expenses in XAU terms, and then bought back later for a similar price to ungild, rather than trying to chase the ETH market, which rarely works out well.

This dynamic is why I believe the ETHg price will be relatively unstable during an ETH crash. People who preempt the crash can premint a lot of ETHg then dump it for ETH when they believe the crash has hit a bottom, in anticipation of ungilding their original ETH for profit when the market recovers.

Can an individual do this?

Yup.

Makes total sense to provide tools for and promote this use case (business model). Encouraging people to hold ETHg like they hold stables is very important demand for the system in general.

Can a DAO do this?

Yes.

In fact, this is safer than trying to leverage it because of the "undo" button.

If the DAO simply mints ETHg and never puts it into circulation then it has no effect on the market.

As long as the DAO members are ETH permabulls they should have no problems with dumping ETHg for ETH after ETH has already been dumped, ETHg denominated.

I'm just not sure how often this will happen in reality, I'd expect ETH and ETHg to dump together. Seems like a good source of income if it does happen periodically.

ETHg is going up/down relative to XAU Anyone who sees the ETHg to XAU ratio as "high" or "low" and is willing to hold assets on both sides of the pair can trade back and forward for a profit.

Many people range-trade assets and ETHg cannot be worth more than XAU.

If the ETHg to XAU ratio becomes very low then either:

ETHg to ETH is also low also which encourages ungilding (buying and burning) XAU is outperforming both ETHg and ETH

In the former case the buybacks should bring the ratio higher. In the latter case, people may wish to sell their XAU for ETHg, or if XAU is sustained at a high price, employ the above strategies (which are ETH:ETHg price denominated).

If people are just really dumping ETH and the asset is dead, then ETHg is dead also. It's hard to see how people would want to use ETHg the asset on the ethereum network, but also hate ETH the asset en masse.

The more people trade the ETHg/XAU range, the tighter the spread and more predictable the prices will be over time, and the more money that LPs will make, and the more retail will feel comfortable holding ETHg as a stable-ish token. It makes total sense to provide analytics and tooling to make this easy (business model).

Can an individual do this?

Yes.

The main issue for anyone doing this is which XAU token(s) to hold. While ETHg is totally decentralised and trustless, all the XAU tokens on the other side of the pair are centralised and could theoretically go to zero at any moment.

If one individual XAU token goes badly then ETHg is not hurt, but any entities holding the XAU token will be rekt.

Can a DAO do this?

Maybe.

If the DAO holds a bad XAU token then it poses a systemic risk to the whole DAO.

XAU token prices for any internal accounting would need to come from an oracle or be assumed from XAU spot prices. This is bad for security in the face of oracle hacks, or issues with the token itself.

If XAU tokens are treated as collateral for the DAO, it would probably need to be sandboxed separately from pure ETH assets, which always have a known ETH value or an implied one.

It's also unclear how to manage a DAO that range-trades, what regulatory and logistical hurdles it might face. Buying and selling vaults Every vault is itself an ERC NFT.

We've barely discussed how the vaults themselves can be traded, but in theory they are all worth something.

After the ETHg has been sold of, there exists a vault that someone else with ETHg could use to unlock the ETH inside.

This potentially has cool ramifcations, can be sold in different marketplaces, and even totally differently, like an order book style rather than classic AMM curve.

We could have people opt in to listing their vaults on an order book, maybe even totally on chain, and then people could be gilding and ungilding each other's vaults if they hit a certain price, kind of like a limit order/threshold. (business model)

Can an individual do this?

Hopefully yes. We'd have to build the market though.

Can a DAO do this?

Sure.

Assuming the marketplace existed they could do this.

Providing liquidity

As the ETHg/XAU pair is range bound it is relatively safe to provide liquidity for it on all standard AMMS with minimal IL.

This is incredibly rare, typically only stables can say this.

As long as there is volume then fees can believably offset IL, especially if the LP manages their own risk and enters/exits carefully. For AMMs that minimise IL such as bancor, balancer, platypus, curve, etc. there's even more reason to be optimistic.

As discussed above, the main thing to enable leverage is to get from ETHg into some XAU token that can then be traded elsewhere back to ETH.

One of the main reason that XAU tokens aren't paired against each other is because they see each other as competition and don't trust each other. Also they are centralised to the point that it matters who the XAU token issuer trusts and sees as a competitor.

ETHg:XAU token pairings don't have this problem. A single ETHg:XAU pairing on an AMM can go to shit due to a problem with a single XAU token without impacting other pairings. More complex setups with N tokens such as curve and balancer would have counterparty risk.

Can an individual do this?

Yes.

Anyone can put up pairs they trust and expect to make money if they are careful.

Especially and including the XAU token issuer and their business partners.

Can a DAO do this?

Maybe.

The main issue again is counterparty risk becoming systemic risk to the DAO protocol.

One bad XAU token can do catastrophic damage to a DAO's treasury and protocol reputation, so every additional token is adding linear or even worse risk as the assets become more "long tail", and o fering diminishing returns for additional value.

LP/pool tokens have even more pricing/oracle issues than standalone tokens. Due to f ash loans and other market manipulations, it's near impossible to accurately assess the value of an LP/pool token in a pure onchain way, which has led to some of the biggest hacks and even protocol deaths this year (e.g. cream f nance).

OTOH "protocol owned liquidity" is a very hot topic right now, mostly because it's proving an e fective smokescreen for ponzis, but also because some platforms such as Alchemix and Bancor are managing their own liquidity as AMM pairs at the smart contract level.

I can see the desire to do this:

Clear revenue model for DAO Protocol can be much more patient than individual (even in f nitely so) Interactions with liquidity can be programmed to follow SC rules More liquidity on AMMs makes everything else work better Partnerships with XAU token issuers Opportunities for novel mechanisms (e.g. negative interest loans from alchemix)

The issue is just the systemic risk of the collateral on the centralised token side.

If we can:

Have e fective governance for whitelisting, buying/selling/revenue from LPing Silo/sandbox LP collateral from pure ETH collateral Figure out how to safely value LP/pool tokens for internal accounting

Then a DAO could do this. It's not so straightforward as it f rst appears though.

Seeding Rain Rain is a fundraising platform that features trustless LBP seeding and incentivised front ends for raises (business model).

An LBP is a balancer pool that decreases its weights steadily to bootstrap a token distribution.

As a balancer pool, it needs two sides of the pair, the token being sold and the token being sold for. Currently all raises are using USD stables, but doing ETHg raises would be awesome.

Direct fundraising in ETHg would drive volume and awareness, and an ETHg themed front end could even be built for curated raises for ecosystem development.

Seeding also attracts a premium so large ETHg holders can make relatively risk-free returns on their capital that backs any raise.

Can individuals do this?

Any individual willing to post a raise denominated in ETHg could do so if we integrated it with an existing platform or built a new one.

Can a DAO do this?

A DAO could absolutely seed raises and make profit of doing so.

As the asset would be ETHg there are no counterparty or collateral risks. The Rain platform ensures that the underlying balancer pool always returns all the seed capital (sans some dust) if the raise fails, or all the capital plus a profit/fee if the raise succeeds. Indicative rates are % for a day raise.