One of the most important ingredients for a successful defi ecosystem is a highly secure price oracle. Algorithmic stablecoins (eg. DAI, RAI, LQTY) depend on a price oracle, synthetic assets of any type depend on a price oracle, collateralized loans depend on a price oracle, as do many other types of projects. Uniswap does provide an “oracle” for the price of ERC20s traded on the exchange, but this is not a true oracle as it does not

provide the price of anything in the outside world. This is a problem: algorithmic stablecoins need an oracle for the price of ETH/USD to be able to function

, and they specifically need an oracle for USD the off-chain fiat asset, and not any specific on-chain instantiation of USD. Similarly, synthetic assets need an oracle for the price of ETH denominated in whatever asset they are mirroring.

I recommend that Uniswap and the UNI token step in and provide such an oracle

(eg. modeled after the Augur or UMA design), specialized to providing price data that’s robust and extremely costly to manipulate and attack.

Outline of this post

- Stablecoins need an oracle for the price of ETH/USD (see above)
- Workarounds like taking the ETH/USDC price are NOT sufficient
- Chainlink is great, but there’s room for a simple alternative specialized for high-value, okay-with-high-latency use cases
- UNI is in an excellent position to be a token for such an oracle
- More broadly, Ethereum L1 needs to remain governance-minimalist, but L2 should be more ambitious, and UNI can be part of that

Workarounds like taking the ETH/USDC price are NOT sufficient

The goal of algorithmic stablecoins is to try to be maximally censorship-resistant and robust by being free of dependencies to the “fiat world”. If this goal is not important to a stablecoin user, then they can avoid algorithmic stablecoins’ technical risks by just using USDC directly. If this goal is

important to a stablecoin user, then it’s important to avoid not just direct dependencies on the fiat markets but also indirect dependencies. Using the ETH/USDC price as a proxy for ETH/USD does not achieve that goal, because such system is still ultimately dependent on USDC continuing to exist and being freely tradeable.

Taking the median of multiple ETH/stablecoin rates (eg. USDC, GUSD and USDT) is at best a small improvement, because the traditional financial system is quite coordinated and can easily become less friendly to all asset-backed stablecoins simultaneously. Hence, if we want to have algorithmic stablecoins that fulfill the raison d’être of their category, an oracle that provides the price between ETH and the USD in the fiat world

is needed.

Chainlink is great, but there’s room for a simple alternative specialized for high-value, okay-with-high-latency use cases

Currently, most “governance-minimized stablecoins” are using Chainlink as their oracle. Chainlink is really valuable for many oracle use cases, but it is also a complex system with many features. Incentives are not as clean as they are in eg. Augur; in particular, there is not an automated mechanism by which participants who provide wrong answers get penalized.

Much like it’s desirable to complement MakerDAO with more minimalist stablecoin alternatives likeRAI (disclosure: I hold both MKR and Rai’s FLX) so that the ecosystem can be more resilient through the diversity of different approaches, it also seems desirable to complement Chainlink with a more minimalist alternative that’s more laser-focused on optimizing incentives and maximizing cost of attack. A robustness-favoring oracle should target these properties even at the cost of being okay with tradeoffs like long resolution times and being limited to one specific type of data (price indices for highly liquid assets).

UNI is in an excellent position to be a token for such an oracle

Decentralized price oracles (at least, if they want to avoid dependence on an identity layer) need to have a token for sybil-resistance. Holders of the token are asked what the price is, and typically an economic mechanism is introduced where those who provide the majority answer are rewarded and those who provide the minority answer are penalized.

If the majority of token holders are corrupted, they can successfully impose an incorrect answer, and at that point it’s up to

the minority holders to create a fork of the system where the attackers' coins are zeroed out and convince the community to prefer the fork from that point forward. The cost of such an attack is thus half the market cap of the token

, minus some amount to account for very lazy holders who are not willing to participate in a vote even in an extreme emergency that could cost them their coins.

For this reason, a robust token-based decentralized oracle for a defi project must first and foremost be based on a token with large market cap.

Efficiency of an oracle is not important: an inefficient oracle can always be augmented with a game where one party claims a value and only if another party disagrees is the oracle actually called. Cost of attack, on the other hand, is absolutely essential to maximize, and thus market cap is key. And the two Ethereum project coins out there with the highest market caps are… LINK and UNI.

Supporting oracles would not just be an act of altruism for Uniswap; in fact, Uniswap heavily benefits from the existence of a more robust stablecoin ecosystem. Uniswap v3 is heavily optimized toward ultra-high capital efficiency for stablecoin <-> stablecoin trades, and is likely to earn very high amounts of fee revenue from these trades. If we start to also see high-volume and robust synthetic assets

emerge on-chain, then this is even more valuable for Uniswap.

More broadly, Ethereum L1 needs to remain governance-minimalist, but L2 should be more ambitious, and UNI can be part of that

The Ethereum ecosystem aims to be the base layer of a fundamentally broader set of applications than preceding blockchain platforms attempted to cover. The goal is not just supporting holding and transfer of a basic asset, but also a decentralized finance (DeFi) ecosystem and also increasingly a decentralized governance (DeGov) ecosystem. There's also a large need for public goods funding in the Ethereum ecosystem.

Supporting this broader vision requires something more expansive than "just a blockchain". Arguably, it requires taking a few steps in the direction of the "crypto state" vision, expanding the services that the blockchain ecosystem provides to not just security but also oracles, dispute resolution, public goods funding, identity, etc. But in order for Ethereum to be a stable platform, there is a need for the blockchain base layer to be governance-minimalist. The governance minimalism gives users confidence that applications that they care about will not be interfered with, and that the base layer will not be ripped apart by political conflicts over addition of controversial features.

Hence, these services need to somehow be provided at layer 2.MEV auctions on rollups to fund ecosystem-wide public goods, as being implemented by Optimism, are one example of this. And Uniswap, as a decentralized exchange that is core to the Ethereum ecosystem also taking on more responsibilities (including price oracle provision) is another natural potential step in this direction.