LP Update - Q3 2022

After a drama-filled second quarter, Q3 was in contrast far quieter. The beginning of the quarter was still very much characterised by the industry determining the extent of the damage caused by the collapse of Luna / Terra and the insolvency of certain lenders and 3AC. Fundraising activity cooled. Investors focused on their portfolio to determine if they had any exposure to the contagion and founders decided to pause fundraising until more certainty was restored to the market.

At the beginning of August activity started to resume. Lending activity across centralised and decentralised lenders restarted as investors grew confident that the full extent of the contagion had been uncovered. Founders started returning to the market to fundraise.

The public markets stayed relatively flat. Total crypto market cap consistently hovered around $1T with BTC starting the quarter at $19,608 and ending at $19,563. ETH saw more upward movement, beginning from $1,057 and finishing at $1,335. In the run up to the Ethereum Merge ahead of September, the price of ETH rose sharply to reach almost $2,000 before falling down. In spite of the Merge's smooth execution, this was a classic "buy the rumour, sell the news" set of short-term movements that we have seen play out many times. Now that the Merge is complete, we see the public markets continuing to be very much driven by the global macro environment with no other crypto-wide short-to-mid term price catalysts on the horizon.

The Merge

The most important development in Q3 was the completion of the long anticipated Ethereum Merge. After years in the making, on September 15, the Ethereum blockchain successfully transitioned from proof of work (PoW) to proof of stake (PoS) as the consensus mechanism used to secure the network. Consensus mechanisms are a core component in any blockchain, being the process through which transactions are agreed upon and included onto a blockchain. The parties that participate in Ethereum's consensus, whether previously PoW or now PoS, are rewarded for their work with Ethereum's native token, ETH.

The Merge has brought about several technical and economic changes that are worth highlighting:

1. **Shift from mining to validating**. In PoW, transactions are approved through a process known as Nakamoto consensus (colloquially referred to as "mining"), which is computationally intensive and requires miners to run expensive and single-purpose mining hardware. PoS on the other hand relies on stakers to post a bond of ETH (a "stake"), in order to participate in approving ("validating") transactions. This bond can be taken away ("slashed") if a participant is found to be malicious or negligent in their performance.
2. **PoS has a far lower carbon footprint than PoW**. Validating transactions with ETH requires much less energy than mining transactions. It's estimated that PoS uses 99% less energy than PoW.
3. **PoS is more democratised**. Whereas mining previously required large up-front capital costs to obtain both special-purpose hardware and low-cost sources of electricity, Ethereum's PoS implementation was designed to be performed by anyone who can afford consumer-grade hardware and a reliable internet connection. This fundamental design goal, unique to Ethereum, contributes to the network's security by expanding the possible set of participating validators.
4. **Dramatically lowered ETH issuance**. After the Merge, Ethereum stopped rewards to PoW miners. This dramatically decreased the per day issuance of ETH by 90%—from ~14,600 ETH to ~1,600 ETH —a feat derived from the lowered operating costs of validators in PoS. Combined with last year's EIP-1559 upgrade that continuously removes ("burns") a portion of ETH based on network usage, the total

supply of ETH is projected to be stable or even decline over the long-term. Indeed, since the Merge, there have already been a few days where total ETH issuance was negative: more ETH was burned from network usage than issued as rewards to validators.

5. **Less ETH outflow**. Miners cover their high operating costs from participating in PoW (hardware costs, electricity) by continuously selling a portion of their earned ETH. It's estimated that per day there is around $20m worth of ETH being sold by miners to cover their expenses. With PoS, not only are the costs of participating in PoS dramatically reduced from the collapsed hardware and power requirements, stakers are also believed to be more intrinsically long-term aligned with the network they're staking on. These factors, together with the lowered issuance, should contribute to lowered sell pressure on ETH over time.

The successful execution of the Merge cannot be overstated. Ethereum is a network that secures billions of dollars of value and the mechanism used to secure the system was changed without any downtime. That's the software equivalent of an airplane changing its engine mid-flight without any disturbance.

Regulation

We witnessed two major regulatory developments this quarter. The first was the sanctioning of Tornado Cash by the U.S. Treasury Department and the second was the charging of all Ooki DAO voting members by the CFTC. Let's take a look at each of these developments more closely.

Tornado Cash sanctions

Tornado Cash offers a "mixer" service that allows users to transact in ETH without directly linking the public addresses that sent and received ETH. Public addresses are open for anybody to see and by studying what addresses interact with each other, networks of related addresses can be constructed. The value of Tornado Cash is that it obfuscates links between two addresses and allows users to transact with anonymity.

At the beginning of August, the US Treasury decided to sanction Tornado Cash on the grounds that the anonymity it granted users had enabled the laundering of billions of dollars. The sanctions bar US individuals and companies from using or providing access to the service and further block all property held by the application under US jurisdiction.

While announcing the sanctions is clear, what's less so is how some of them will be enforced given that this is the first time a set of open source software is being sanctioned as opposed to persons or corporate entities.

The sanctions that tackle a centralised vector *can* be enforced. For example, after the sanctions were announced, Circle, the issuer of the USD stablecoin USDC, blacklisted addresses associated with Tornado Cash. This means that any USDC held in those addresses are unable to be moved. Going forward, it's also likely that US exchanges, such as Coinbase, will block any or some tokens that were passed through Tornado Cash. In both these cases enforcement is possible because there are centralised companies that have complete control over a particular asset or product and can be targeted directly by the authorities to act.

Whereas Circle and Coinbase are centralised companies, Tornado Cash isn't. It is simply a piece of software that autonomously executes on Ethereum. It is run on a decentralised network of computers that comprise the Ethereum blockchain, spread across many jurisdictions, rather than on the servers of a centralised company. This makes it very difficult for regulators to enforce sanctions on Tornado Cash directly.

In our view, sanctioning decentralised networks like Tornado Cash is not the way forward. Decentralised networks are unbiased in their construction and as a result should remain free of sanctions. Interfaces, that provide centralised access points to these networks, are on the other hand run by individuals or entities with agency. They take a more biased approach as to how networks should be used and should be the layer of the technology stack that regulators look at.

Every technology in history has been used for good and bad. People, not technologies, decide how technologies get used. It's important to keep that in mind when regulating crypto.

Ooki DAO members charged

In September, the Commodity Futures Trading Commission (CFTC) charged bZeroX LLC (bZeroX) and its founders for having violated securities regulations. This part is fairly standard—claims brought against a company and its founders by a federal agency for having broken the law.

However, the CFTC did not stop there. An additional claim has been brought against the successor of bZeroX, Ooki DAO, and its voting members, marking the first time a DAO and its members have been directly implicated as unlimited liability partners.

First, a step back to provide more context. bZeroX is a US limited liability company founded in 2019 that created software, the bZeroX protocol, which allowed users to take leveraged and margined positions on different crypto assets. bZeroX did not require users to undergo KYC / AML checks which, according to the CFTC, it was required to do. Additionally, bZeroX advertised the lack of KYC as a benefit to users. In August 2021, bZeroX transferred control of the bZeroX protocol to the bZeroX DAO, which was later renamed to Ooki DAO. Ooki DAO continued to offer the same services as bZeroX.

The CFTC claims that the handover of the bZeroX protocol from bZeroX to Ooki DAO was done to circumvent securities regulations. The CFTC cites language from the bZeroX founders that transferring ownership of the bZeroX protocol to a DAO would make it "future proof" as regulators would not be able to charge a DAO due to its decentralised nature. The CFTC took exception to that by stating that DAOs are not immune from enforcement of the law and decided to charge the DAO directly as well. This is notable for several reasons.

First, the CFTC was deemed to be the crypto-friendly counterpart to the more antagonistic SEC. This move contradicts the prevailing narrative.

Secondly, this is the first example of a federal agency claiming that active participants of a DAO can be held liable for the actions of said DAO, with participation in any prior vote being presented as an example of "active participation". In the eyes of the CFTC, a DAO is an unincorporated organisation which does not grant individual members protection against claims brought against the organisation as a whole. Simply put, individual members may face unlimited liability for their involvement in any DAO.

While the full impact is still to be seen, our current reading of the situation is that the CFTC has decided to pursue a strategy of regulation by enforcement and has sought to make an example out of bZeroX to deter future DAOs from believing they can violate securities laws with impunity. However, while bZeroX and its founders were in clear violation when they offered unregistered securities and likely attracted the attention of the CFTC with their overt messaging to skirt regulations in their shift to a DAO, the claims against any and all voting participants appears to be an overreach that is unlikely to be sustained.

DAO drama

This quarter we were reminded again that DAOs, in spite of their promise, are still very early.

Maker Love vote

In mid June, the Maker community put up several resolutions to a vote. Maker, as a reminder, is one of the largest DeFi protocols today. It is a lending protocol with approximately $7.69B in total value locked (TVL) and one of the most sophisticated DAOs in structure. It is divided into several independent core units that each focus on a particular function. Changes to the protocol are determined through votes that are put up to all Maker token holders and decided by simple majority.

The most contentious resolution was a vote for the ratification of the Lending Oversight Unit. This unit was coincidentally led by our advisor Luca Prosperi. Without going into too much detail, the goal of the unit was to establish checks and balances with regard to the onboarding of new collateral for loans. What

ensued was a proxy battle between the original founders of Maker and institutional investors. Ultimately the original two founders won out, as they still owned a vast majority of the Maker token supply that they could leverage in the voting.

What the votes showed once again was the limitations of a governance system based only on token holdings. One of the two original founders of Maker had operationally stepped away from the protocol a number of years ago, but still maintained a large share of tokens and returned on request of the other founder to use them to vote in his favour.

Most DAOs today have implemented voting based on token holdings. It's the simplest to set up but raises the question whether DAOs resemble plutocracies. That is, are votes just decided by the rich?

On the one hand, token holdings are a sign of early involvement in a DAO. Founders and early team members don't need to buy their tokens but instead earn them similarly as they would through an ESOP package at a startup. But what happens when the protocol evolves and new people get involved while earlier contributors shift focus? While protocols do reward later contributors with tokens, earlier contributors will have proportionally received more tokens for the same input. If later contributors want to influence voting, they will need to buy or borrow tokens on the market, both of which require a lot of upfront capital.

We believe that voting systems need to grant greater influence to the people best positioned to make decisions. There are several ways that can be implemented. We remain excited by efforts that tie voting power closer to reputation, which is fluidly earned or lost rather than bought or sold in economic transactions.