Link to working doc

Definition

ulterior (adj): existing beyond what is obvious or admitted.

Griefing Factor: “the amount of money lost by the victims divided by the amount of money lost by the attackers”

Ulterior Factor: “the amount of money gained by attackers outside of the protocol divided by the amount of money lost by the attackers”

Introduction

Ulterior factor analysis looks to complement the endogenous attack bounding of griefing factor analysis via exogenous attack bounding. In other words, griefing factor bounds the in-protocol attack efficiency (damage as a multiple of dollars used to attack the protocol) where as ulterior factor looks to bound the attack exoprotocol attack efficiency (benefit to the attackers as a multiple of dollars used to attack the protocol)

While the concept of a griefing factor is very helpful in capturing the four vectors of attack (minority/majority + protocol/each other), it may not be the largest factor in PoS economic security—especially while a valuable network is bootstrapping PoS as an overlay.

While the exogenous gains to the attacker cannot be directly observed or attributed, it can be defended by requiring a certain level of total deposits for a given level of market cap. [The other problem here is that market cap / ETH price is not observed in the protocol… That said, I’m figuring out how best to incorporate these concepts to Casper. WIP.]

When griefing factor matters, and when it matters less so.

Griefing factor matters most at steady state when there’s a “healthy level” of total deposits. In other words, when the ratio of TD : market cap

reaches the target level. In the beginning, when TD represents a much smaller portion of the entire market cap, I’d argue there’s a much stronger exoprotocol attack vector.

Example

If, for example, Ethereum is worth $30B and is initially staked by $100M, then as an Ethereum competitor, it would be possible to gain by destroying value in Ethereum in the hopes that some of that value destruction leaks into a competitor.

For example, let’s say that a certain competitor hypothesizes that they can absorb 20% of any ETH value destruction related to market perception that ETH is insecure. Then, the higher the market cap to TD ratio, the higher the “attack multiple” for each dollar that the attacker employs to attack the network.

More concretely, if a failure in Casper FFG (for example, half the TD is slashed due to safety failures or leakage) can potentially decrease ETH market cap by 20% over the same time period, this attacker would hypothesize that about 4% of that value may “escape” to its own currency ($1.2B). So at $30B and “value leakage” assumptions above, any deposit size smaller than [$3.6B] would have a positive return on the attacker, even without considering the damage done to honest validators and even after slashing 100% of the attacker’s deposit. At [$120M] deposits with a [$360M] TD level, the attack would have a “10x return” ($120M lost to get $1.2B in benefit its own protocol). (This analysis doesn’t even include the impact of emotion/perception/momentum in prices, which would incur additional damage and increase the “return” to the attacker).

Total Deposits / Market Capitalization

So therefore, when a PoS protocol is mature and reaches the highest (end state) TD / market cap ratio, griefing factor matters the most. When a large scale network is overlaying a PoS finality gadget atop PoW, it is vulnerable to an [exoprotocol] attack. This is because a high TD/MC ratio allows for a high damage to the market cap per dollar of deposits.

One may argue that when a protocol is largely secured by a PoW chain, this wouldn’t matter as much. But I argue that the contrary. This effect is true to a degree even if a protocol is only partially secured by a finality overlay such as FFG. I argue this because “monetary assets” are largely backed by perception and perception of weakness for a leading currency, even if the real impact on the currency is weak, can create significant damage to itself–at the benefit of its competitors (only untrue if the public loses confidence in cryptocurrencies overall)

"Monetary commodities compete more on strength of collective belief than on any fundamental value (contra stocks, for example). Rising price -> rising belief -> rising price. So the interesting question here is whether a small # of whales can tip the market toward a different equilibrium regardless of fundamental tech differences between two chains.” - Anonymous investor re BCH/BTC

Proposal

Griefing Factor

refers to endogenous bounds of attack efficiency.

- i.e. For every dollar that the attacker has, bound the damage they can do the stake of others.

Ulterior Factor

refers exogenous bounds of attack efficiency.

- i.e. For every dollar that the attacker has, bound the damage they can do to the perceived value of Ethereum (more precisely, the loss of value from the Ethereum protocol to a competing protocol.

Implications

While designing a protocol incentivization with a griefing factor bound is an excellent goal to limit the in-protocol damage that an attacker can do, one could argue that there’s a much larger attack vector (though harder/impossible to measure) that damages the overall protocol and potentially leaks value to a competing protocol.

While measuring this precise effect would be largely futile, one can limit the effect of that attack by increasing the required dollars to cause a failure (or incentivizing it). First, the protocol can be designed to have a higher threshold for Byzantine behavior. More relevantly, we can require a higher TD / Market Cap ratio. That way, each “attack dollar” can have a lower multiple for affecting the market capitalization of ETH.

Takeaways

1. While bounding the measurable damage an attacker can do within the validator set is invaluable, many attackers may have more to gain with ulterior motives (price of a directly competing project going up, getting control over the Dapp ecosystem, more of the fiat inflows into crypto buying another project instead of ETH).

2. While we cannot directly bound the amount of benefit attackers can have outside of the protocol, we can prepare for how damaging this attack vector can be at any point by being aware of (1) our own TD/MCap target (TD is the only direct way under our control to decrease ulterior factor) and (2) how certain competitors may be anti-correlated with ETH price and look to directly benefit from our potential failures.

3. Relatively speaking, as the network’s TD level matures to the ideal levels, griefing factor matters more and ulterior factor matters less. So, during bootstrapping, ulterior factor is perhaps the largest liability (especially for an overlay on top of a “large cap” network).