

Context

Hi – I recently joined the Ethereum research team and will be focused on cryptoeconomics—starting with Casper. Many thanks to [@vbuterin](#), [@vladzamfir](#), [@virgil](#) and [@karl](#) for collaboration on research so far. Wanted to share the current state of work here on ethresearch (and get it out of Skype/Telegram chats

).

In this thread, we will start with an overview of the objectives and the approach. This post also includes links to other analyses we have begun (i.e. participation constraint, CAPM implications, ulterior factor analysis, fixed income approach). However, we will follow up with more in-depth analyses in separate threads (for more granular conversations). For example:

- Defining the shapes of the $Y(p_v, \text{ESF}, \text{TD})$

and $N(p_v, \text{ESF}, \text{TD})$

functions (returns change in validator deposit if voted or didn't vote—with respect to proportion of validator set that voted, epochs since finality, and total deposits).

- Discussing how to model validator required returns, total deposits and market cap
- Implications of capital asset pricing model on validator yield
- Implication of liquidity-based asset pricing model on withdrawal delay / required return
- Relationship between inflation and validator yield
- Draconian vs “soft” slashing and how that affects marginal cost of attack vs ETH dilution / inflation.
- Defining the macroeconomic participation constraint for the system (on average, how compelling would our mechanism be for validators to join at various levels of issuance / total budget).
- and more!

As we continue, we will synthesize these piecemeal analyses to finalize the more formal “Incentives in Casper FFG” paper, which we will publish prior to / concurrent with implementing in the test net. Thanks for taking a look, feedback and questions are very welcome!

Overview

With the Casper FFG written, now the focus is to correctly optimize the suggested parameters to incentivize the correct behavior on the network. The intended behavior is to vote, to vote correctly, to vote frequently and [to believe that other validators will do so as well]. More specifically—with a budget constraint of issuance—we strive to balance the shape and magnitudes of rewards & penalties of a sufficiently large and broad validator set that has heterogeneous distribution of required returns and Byzantine intent.

Approach

As a starting point, we'd like to introduce an approach to solving this problem using classic economic and financial theory.

Featuring:

- Participation constraint analysis
- Budget constraint & utility maximization
- Profit maximization via marginal cost and benefit analysis
- Capital Asset Pricing Model, Liquidity-based Asset Pricing Model, Sharpe Ratio
- Fixed income assets & price/yield relationship
- Quantity theory of money, and central banking policy.

This rational/theoretical (“naive”) approach will provide a foundational framework on which to build the behavioral, game theoretical and cryptoeconomic effects.

Objectives

- Penalize bad behavior and limit the damage it can do

- Severely penalize bad behavior and bad results – this is a key benefit to PoS, we can penalize by more than the opex equivalent of PoW (and dive into the capex portion). The trick is to do this while not driving away the good actors (i.e. there is a penalty scheme too draconian that the incremental security is less than the incremental ETH inflation).
- Limit the damage that attackers can do to the Casper validator set – i.e. Griefing factor analysis. There should be an upper bound to the damage that an attacking validator can do to the other validators in the set.
- Limit the damage that attackers can do to the Ethereum protocol – i.e. Ulterior factor analysis. While it is impossible to know a validator's ability to benefit from outside the protocol via Byzantine behavior, we design the incentives with that fact in mind. (Many actors stand to benefit from Ethereum's PoS failing, and this is to be measured not in % of total deposits, but in % of ETH market capitalization).
- Severely penalize bad behavior and bad results – this is a key benefit to PoS, we can penalize by more than the opex equivalent of PoW (and dive into the capex portion). The trick is to do this while not driving away the good actors (i.e. there is a penalty scheme too draconian that the incremental security is less than the incremental ETH inflation).
- Limit the damage that attackers can do to the Casper validator set – i.e. Griefing factor analysis. There should be an upper bound to the damage that an attacking validator can do to the other validators in the set.
- Limit the damage that attackers can do to the Ethereum protocol – i.e. Ulterior factor analysis. While it is impossible to know a validator's ability to benefit from outside the protocol via Byzantine behavior, we design the incentives with that fact in mind. (Many actors stand to benefit from Ethereum's PoS failing, and this is to be measured not in % of total deposits, but in % of ETH market capitalization).
- Reward good behavior
- Reward voting frequently – having a low level of votes makes it hard to disambiguate censorship vs low participation. make it a no brainer to vote as opposed to not voting.
- Reward voting correctly – not only should we penalize byzantine behavior, we should reward correctly voting in a compelling way (compared to all asset classes available to validators).
- Reward cooperation – while 2/3 vs 100% participation has the same utility on a given epoch, it provides a higher margin of safety against marginal Byzantine behavior, so a validator set that cooperate well with each other should be rewarded at a higher rate.
- Reward voting frequently – having a low level of votes makes it hard to disambiguate censorship vs low participation. make it a no brainer to vote as opposed to not voting.
- Reward voting correctly – not only should we penalize byzantine behavior, we should reward correctly voting in a compelling way (compared to all asset classes available to validators).
- Reward cooperation – while 2/3 vs 100% participation has the same utility on a given epoch, it provides a higher margin of safety against marginal Byzantine behavior, so a validator set that cooperate well with each other should be rewarded at a higher rate.
- Design a economically sound system and mechanism
- Limit the dilution to existing ETH holders – The more we penalize the average validator, the more we have to reward the overall group to make a compelling mechanism. Then we have to issue more ETH and cause inflation. We need to find $MB = MC$

for increasing penalties.

- Incentivize a high level of total validator deposits – The smaller the gap between total deposits and ETH market cap, the higher the cost of any exoprotocol attack.
- Encourage broad participation – limit the bias in the validator set by encouraging participation by validators with various risk tolerances. Return on capital has to be (at least) commensurate with the risk validators are taking.
- Limit the dilution to existing ETH holders – The more we penalize the average validator, the more we have to reward the overall group to make a compelling mechanism. Then we have to issue more ETH and cause inflation. We need to find $MB = MC$

for increasing penalties.

- Incentivize a high level of total validator deposits – The smaller the gap between total deposits and ETH market cap, the higher the cost of any exoprotocol attack.
- Encourage broad participation – limit the bias in the validator set by encouraging participation by validators with various risk tolerances. Return on capital has to be (at least) commensurate with the risk validators are taking.

Diving Into the Approach

Define the global “budget”

[+Casper FFG: Macroeconomic Participation Constraint](#)

[+Casper FFG: Returns, Deposits & Market Cap](#)

[+Casper FFG: CAPM & Validation Yield](#)

[Yield, Issuance and Deposit levels \(Spreadsheet\)](#)

- At what global rate will people want to participate?
- What is the the per checkpoint yield?
- What is the daily yield?

Enumerate the qualities of the shape of the budget

[+Casper FFG: Reward and Penalty Shapes](#)

- At steady state, what % of people are earning positive returns?
- What is the annual inflation rate now and later?
- How the yield look different based on various TD levels?
- how should that be different based on various market cap levels, if at all?
- how should that be different based on various market cap levels, if at all?

Heterogenous Validators

[] TODO Game theoretic analysis budget defined above

- Create incentive-compatible optimization for good and bad actors
- Create incentive-compatible optimization for high req return and low req return actors.
- If it doesn't fit the bill for low req return actors, you will only attract high-risk taking individuals that aren't responsive to lower levels of rewards and penalties

[] sensitivity to incentives. a \$1000 for a homeless person vs a billionaire are very different amounts...

- If it doesn't fit the bill for low req return actors, you will only attract high-risk taking individuals that aren't responsive to lower levels of rewards and penalties

[] sensitivity to incentives. a \$1000 for a homeless person vs a billionaire are very different amounts...

Offline, Censorship, Exoprotocol Attack Vectors

- Speaker-listener dichotomy (i.e. [griefing factor analysis](#))
- exoprotocol attacks (i.e. [ulterior factor analysis](#))

Iterate

- Find more attack vectors
- iterate on optimization and mechanism as necessary.
- Repeat.

Next Steps

- We have made significant progress on understanding the global budget and [macroeconomic participation constraint](#) at various [levels of issuance, total deposits](#). Also, we now have an understanding of how that yield relates to opportunity cost of other yields and [how the standard deviation of validator yields](#) additionally affects the risk-adjusted returns for a given level of gross returns. We are working to have an agreed-upon range for issuance budget and TD target as a %

of MCap

.

- We now have to further discuss the proposed shapes

of the $Y(p_v, \text{ESF}, \text{TD})$

and $N(p_v, \text{ESF}, \text{TD})$

functions and analytically represent them once we agree on the general [shape of the proposed shapes](#)

- The obvious missing piece in the current iteration that has been the focus in previous steps is the game theoretic analysis

and griefing factor analysis

, especially using Bayesian frameworks that define the security of the protocol at various levels of p_v

and $p_{\{\text{Byzantine}\}}$

.

- We should also fully understand and prepare for the exoprotocol downside

of this hybrid overlay given that the introduction of the overlay will be the lowest TD/MCap

will ever be. That means that an attacker can have an outsized multiple on every dollar of attack used to damage the reputation of Ethereum (rather than the deposit dollars of the validator set, per griefing factor analysis).

- Once we have a fully working PoC1 ready for Casper FFG Incentivization, we will find what was wrong with our initial assumptions and iterate

on the parameter optimization process.

Thanks for reading and looking forward to your comments. Thanks