CONFIO

Proof of Engagement

ETHAN FREY AND MARTIN WORNER

Abstract

If we could build a clean blockchain and could develop a consensus model to secure the chain, reward the community active in the chain fairly and provide an excellent infrastructure for the user base, what would it look like?

In this paper we examine the major consensus models and look at them with critical eyes, and taking the best pieces while understanding the areas that can be improved we develop a new consensus model.

Proof of Engagement (PoE) is not a radical new consensus model, rather an evolutionary step built on the strength of previous consensus mechanisms while addressing some of the shortcomings.

Proof of Authority is a consensus mechanism based on the validators disclosing information about themselves and they stake their reputation.

Proof of Stake is a consensus mechanism where validators build a stake which ties their interest in the chain for rewards but also if they misbehave their stakes can be forfeited as punishment known as slashing. There is a variation of this known as delegated Proof of Stake which allows token holders to delegate their funds to validators in exchange for a reward.

PoE combines a staking model with the addition of the element of Validators demonstrating a positive engagement in securing and running the blockchain.

The engagement model goes beyond the transactional in that it seeks engagement between the developers of the chain, the participants and Validators, the active engagement in running a secure chain along with the long term engagement. The model balances the long term outlook with encouraging innovation from new entrants through hackathons and bounty programmes.

We examine the need for evolutionary economics, recognising that a chain evolves from the bootstrapping phase with low turnover to a mature chain with a diverse, engaged Validator pool.

The implementation of the PoE is down to the individual chain as it is fully configurable, not only at genesis but through the governance model. Some may choose a model with more emphasis on engagement (a flavour of PoA that has a decentralised criteria) while others combine engagement with staking, closer to a PoS model.

A simpler implementation has been suggested, namely to combine PoA with PoS which enables experimentation to establish the optimal models based on economic and political theory.

Introduction

If we could build a clean blockchain and could develop a consensus model to secure the chain, reward the community who run and maintain it, what would it look like?

Both Proof of Stake (PoS) and delegated Proof of Stake (dPoS) have issues around collusion and cartels as the incentives are to build bigger stakes to then get higher rewards so that the Validators could be motivated by self interest rather than for the good of the chain.

Having a lot of Validators running nodes and paying the same to everyone who votes, good, bad or indifferent may lead to a less secure chain as they know they get paid regardless of what they do so will make less effort to invest in their infrastructure and maintain an active participation in securing the chain.

One of the objectives of a chain is to build a depth of Validators to ensure that the chain is decentralised, is secure and the Validators have clear sight on their ROI which motivates them to run a node.

The revenue generated on chain is through transactions and fees, and it may be stating the obvious but the chain must provide a good platform for organisations to build their businesses on. What makes a good platform? A good feature set coupled with fair and transparent fees? A growing chain with a robust revenue stream is the foundation for bringing in Validators and it thus becomes a virtuous circle.

As part of the philosophy of engagement, for the long term success of all the interested parties, partnerships between developers and Validators is a key element of this. A good relationship built on engagement between the developers building and contributing code to the chain, the dApp builders who are building their businesses, the Validators in securing and running the chain will foster a strong platform and the delegators investing their tokens.

Engagement must be seen as active participation and long term engagement defined as making the chain successful for the benefit of all parties.

Consensus Mechanisms in the spotlight

When considering consensus mechanisms it is healthy to do a reality check to see whether the following attributes have been considered.

Chain security and integrity (such as secure against double spend, Long range attack, and 51% attacks)

- Fair ROI for Validators
- Resistant to “Rich get richer”
- Cartel and Collusion resistant
- Transparent business plans with revenue projections and regular updates
- Token supplies, limits and inflation considered.

For the purpose of this document the consensus models examined are the ones that work with Tendermint[1], and thus excludes Proof of Work.

Proof of Authority

By far the simplest of consensus models is the Proof of Authority (PoA). The disclosure done by the Validators ensures that they stake their reputation, and the reasoning behind this is that it takes years to build a reputation and one stupid act to destroy it[2].

The Validator ecosystem relies on a strong off-chain platform where prospective Validators are screened, disclose their information and their performance is monitored by disclosing the numbers.

The downside becomes apparent if a Validator does not actually care that they develop a bad reputation and that it is no longer is a disincentive to behave correctly.

There is a more limited pool of individuals or companies willing to go through the due diligence and KYC processes meaning that the potential Validator pools will therefore be narrow. Of more concern is that by definition there is centralisation of the selection process, and can lead to lack of depth and diversity of the Validator pool.

Proof of Stake

Proof of Stake (PoS), on paper looks like the perfect system as a counter to Proof of Work (PoW), used by Bitcoin and Ethereum and it borrowed the idea of scarcity. In PoW work is based on scarcity of computational power, the thinking behind PoS was to create artificial scarcity of tokens. Validators build a stake which ties their interest in the chain for rewards but also if they misbehave their stakes can be forfeited as punishment known as slashing.

Aligning the Validators interests with the success of the chain along with the threat of taking funds off them seems like a good model.

Dash has a PoS model requiring the Validators to deposit 1000 DASH tokens, these are not however, staked as there is no slashing for bad behaviour, this is referred to as the "nothing at stake" problem. In Dash it matters less as it runs a hybrid PoW and PoS system so the PoS Validators cannot cause mischief.

There are also issues with "Fake Stakes[3]" where the network is flooded with rubbish data, this is more a problem with UTXO chains and not an issue for account based chains.

By far the biggest problem with PoS is the phenomenon where the "rich get richer", this is where the Validators with the biggest stake are selected more often and thus generate the greater reward.

Delegated Proof of Stake

The introduction of delegators to the model of PoS is a good enhancement as it means Validators can build stakes by using delgators' tokens in return for a proportion of the rewards and makes the rewards accessible to a wider pool.

The delegated Proof of Stake dPos promotes "democratization" of the staking system and rewards model. It is also based on the idea that the market (delegators) will always select the best producer (Validators).

The dPos model ensures that Validators without a large capital base can take part, although this doesn't always work. As we can observe in the Cosmos chain where some respected Validators offer 0% commission[4], meaning there is no place for "higher risk" Validators who offer lower commissions and ultimately leads to centralization with a few early big self-stakers. The concentration of stake and rewards in the Cosmos chain is evident. As of April 1, 2019, the top 15 nodes control about 71% of the voting power[5], which means the top 15 nodes will receive 70% of the PoS reward.

The other flaw observed where many delegators don't do due diligence on the Validators and just look for highest rewards or jump in on the biggest Validators as a safe bet.

Finally, consider Tezos, where delegation is not enforced on-chain, and cases of "bakers" running off with the delegates rewards or where bakers having reached[6] capacity not updated delegators.

1 *https://tendermint.com/*

2 *A notorious case of brand destruction was Gerald Ratner in 1991 https://www.businessblogshub.com/2012/09/the-man-who-destroyed-his-multi-million-dollar-company-in-10-seconds/*

3 *https://btcmanager.com/researchers-find-flaws-proof-of-stake-pos-cryptocurrency-projects/?q=/researchers-find-flaws-proof-of-stake-pos-cryptocurrency-projects*

4 *https://forum.cosmos.network/t/governance-limit-Validators-from-0-commission-fee/2182*

5 *https://medium.com/@tokengazer/tokengazer-crypto-review-in-depth-analysis-of-cosmos-7caf4c4958cc*

6 *https://unhashed.com/cryptocurrency-news/tezos-users-fail-to-receive-rewards-in-over-delegation-crisis/*

Proof of Engagement

Introduction

Proof of Engagement starts from the position that there is a community as a whole who are involved in running, upgrading and securing a blockchain and naturally Validators are a key part of the community.

Beginning with the basic premise that the consensus model aims to reward the community including the Validators who are active in securing and maintaining a strong chain, we consider how to fairly reward the Validators for the work they do.

Other consensus mechanisms have shown that there must be a combination of rewards and with that comes responsibility which is normally where slashing comes in.

Where the other consensus models are less successful is the tokenomics which favour large stakes, as seen in Cosmos where there is a concentration of stake and voting power in favour of a small number of Validators.[7]

The question of finding a balance between a fair reward and a mechanism so that the Validators who go beyond the basic block metrics (up time, voting participation etc) are rewarded.

Revenue Pool

As the paper describes the distribution of rewards to the wider community based on engagement the source of funds is important to consider.

The revenue from transaction fees, and block rewards are paid into a revenue account for distribution to both the Validators and other holders of Engagement Rewards.

The link from engagement to reward

We all know what good is, right? Sort of, Alice's view may differ from Bob's who may differ from Anil's. In the decentralised world, a nice set of rules that are measurable is what is needed, but in a softer definition of engagement we need to build a picture of what is "good" and tie that to reward.

How is engagement defined?

Defining engagement is not a pure set of rules or an exact mechanism, rather it is a judgement on how people are seen to contribute to the overall running of the blockchain.

This is best illustrated with examples, such as the Validator that reaches out to others, shares best practice, is active in the group chats and forums, and the person that writes some nice open source code tools to help run and monitor the chain for good health, the person deploying dApps to build a business and the core developers contributing to the chain's evolution.

This is highly subjective and mostly off-chain, and now we know what good looks like we can start forming profiles of the engaged parties. This must be community led and ties in with the close collaboration between the Validators, the development community, dApp builders and the token holders.

What happens with dis-engagement?

We have all seen the scenario where a new person comes in, is very active, contributing to forums, building useful tools and then the enthusiasm fades and the engagement slows down and they begin to cruise.

In the case of a Validator accruing Engagement Rewards, it is not right that the Validator should continue to enjoy the benefits in perpetuity if their engagement declines.

To ensure that a participant remains engaged there is a "half-life" mechanism where the Engagement Rewards decay unless they continue to engage and accrue rewards. This half-life mechanism applies to the Engagement Rewards accrued by all members of the community.

The mechanism of awarding Engagement rewards, the oversight community

There is an oversight community who identify, vote and allocate Engagement Rewards.

There is a trade off between fully decentralised where everyone has a say to an appointed committee which does centralise the power. However, in practice it would be hard to find consensus and full participation of all the actors in the chain, and creating a self-sovereign group is a reasonable compromise.

To join the oversight community an existing member proposes the prospective member. The prospective member must deposit a stake. The purpose of the stake is to build in a punishment mechanism

should the community member engage in undesirable behaviour, such as the proposal of fake engagement activities, or the proposal of a member which is themselves (Sybil attack). This behaviour would be policed by the oversight community and should undesirable behaviour be observed then a proposal would be made to slash the person's stake and it would be voted on, it would need a quorum with a majority, say 2/3rds of the group, for the vote to pass and the slashing event to be triggered.

Proposers are rewarded for the election of people to the oversight community, as this rewards active outreach in the community and thus engagement.

The oversight community has the role of identifying and rewarding engagement, the awarding of Engagement Rewards is important to the distribution of revenue to the active, engaged participants in the whole community.

The purpose of providing an incentive for the oversight community is to incentivise those actively engaged in widening the oversight community, who in turn monitor the forums, channels and media outlets to identify engagement from the wider community, to spend time looking at the tools being built to make the chain stronger and more secure.

The assessment of engagement of active members, is governed by the oversight community. By governance this refers to proposals and votes by the oversight community.

The "half-life[8]" property of the Engagement Rewards also applies to the oversight committee members so that their points expire during a set period of time. This is to incentivise active participation, and not a burst of activity which then attracts rewards for ever.

Connecting identity

Considering that much of the engagement is off-chain activity there need to be mechanisms to link the blockchain addresses to the off-chain personas. We know the identity of the forum contributor, the blogger, and the github profile of the toolsmith and there is a mechanism to connect these profiles to the online address.

The oversight committee needs to have the authority to decide which of the off-chain activities are tied to Engagement Rewards, as the blogging platforms may change or new technologies emerge that support self-sovereign communities.

Trust

A key aspect to the decision making is that the proposers and voting body can be trusted to make good decisions, and that economic incentives to "game" the reward system as well as political incentives to form alliances which may not be for the common good are considered.

To mitigate the economic incentives it is very important to ensure that the engagement is genuine and not some "quick hit" to earn Engagement Rewards. This relies on proposers having rigour in their selection for rewards and the voting body trusting that the proposers are honest and the quality of the proposals needs to be of a sufficient level so that voters can make informed decisions.

Building Trust into a PoE model is therefore very important. Trust is an evolutionary process, as the chain evolves from a small infrastructure in the bootstrap phase to a fully fledged, robust, self-sovereign chain.

The ultimate goal of a blockchain is to have a thriving, self-sovereign organisation which is decentralised. This may not necessarily happen in one step, particularly in the bootstrap phase where the network factor has yet to happen.

The first step is analogous to a standard Proof of Authority type mechanism with a governing board overseeing the process of evaluating participants' engagement or contribution to the chain. They would propose the engaged parties are given Engagement Rewards and then vote on it, the Engagement Rewards are then allocated to the recipients once the vote has passed. This is a centralised operation but a good first step in establishing the Engagement Rewards mechanism.

The next step is to open the proposal creation to the community with the voting held by the board. This step is important as it links the off-chain engagement to addresses on the chain and this being visible to the community, for example the person or entity that built a shiny new block explorer under the github id *codemonkey123* relates to address `527162810598143820 5L`. For this to work there needs to be a mechanism to link the off-chain ids to an address that is visible for the community to see.

The final step in building is the governance around the proposal and voting on engagement being community led, or self-sovereign. This is the path to establishing the oversight community which is self-sovereign and requires the oversight community to provide tokens which are staked (and may be slashed according to the conditions set in the governance paper).

7 *https://medium.com/posbakerz/cosmos-network-Validator-overview-25d4bde67563*

8 *Half life applies to the engagement rewards which decay with time meaning that after a period of time the engagement rewards half in value.*

Engagement Rewards

We have established a subjective method for evaluating engagement, and looked at the Engagement Rewards "half-life" for dis-engagement. The idea of converting engagement to rewards points to a form of token, so that the active community can accrue tokens in acknowledgement of their engagement.

The Engagement Rewards should be proposed and awarded by the electorate and the engagement points are awarded.

What is an engagement reward?

The properties of the engagement reward are as follows.

- Non-Transferrable. These rewards are used solely on the chain and are not transferable to other addresses within the chain
- Half-life; this is configurable and comes with a default of a halving of the Engagement Rewards every 6 months if no new Engagement Rewards are accrued
- Provides bonus to staking and rewards, according to various algorithms chosen by each chain

By applying Engagement Rewards to a stake we have some interesting scenarios where a Validator with high Engagement Rewards is able to compete on a level field with another Validator with much higher stake.

The Reward Pool and distribution

The reward pool is the pot where the transaction fees, block rewards and any other fees generated are paid into.

Active members, Validators and the oversight community all accumulate engagement rewards and there is a distribution mechanism based on the rewards and where applicable the stake.

The distribution of the funds from the reward pool is allocated to the active community with accumulated Engagement Rewards, the engagement rewards having been allocated by the oversight committee. The Validator distribution combines the stake, and the Engagement Rewards and the reward curve, the other engaged community members are paid out purely on engagement rewards.

Engagement rewards and the Community

As discussed the wider community in the context of the blockchain is made up of Validators, dApp builders, Core Developers, Bloggers and the Oversight Community. The success of a chain depends on a strong community with all parties who are active, and yet it seems that the rewards in many chains go to Validators and token holders (through the delegation model). The use of Engagement rewards provides a good way to reward those who are active in the community and recognises that various groups are all important in the running of a chain.

Core Developers are often funded through the proceeds of an ICO held in a Foundation that awards grants for the continuing work on building the core blockchain. By linking Core Developers to Engagement Rewards it creates an incentive to a potentially wider community of Core Developers.

The dApp builders are an interesting segment of the community, it is these people who build businesses and ultimately bring revenue to the blockchain. Clearly by building and deploying dApps they create network effects, especially if there is a strong interest in contributing to utility dApps which make the chain stronger. By incentivising dApp builders it encourages the community of dApp builders to build and grow their businesses on the chain.

Bloggers, active forum contributors, evangelists all form part of a chain's ecosystem and providing the means for this group to earn rewards further strengthens the community as it would add an additional incentive to remain active, and engaged. This contrasts with the approach in other chains where they rely on altruism or bidding for community funds.

As discussed in a fully self-sovereign chain, the oversight community provides a valuable service in connecting identity and the human judgement in the allocation of rewards for both on and off-chain behaviour.

Validators are covered in the next section as they have a second dimension with the need to provide a stake.

Engagement rewards and the Validator

The accumulation of Engagement Rewards will give the Validators some privileges.

There are a number of scenarios which we consider in looking at how Engagement Rewards work.

A prospective Validator could accrue some valuable Engagement Rewards by being active and contributing. One model in evaluating which Validators to include is to rank prospective Validators by Engagement Rewards (irrespective of stake) and take the top Validators.

In the section above we looked at multipliers to be used in calculating a "total stake" made up of their stakes and multiplied by the Engagement Rewards. The other models are based on engagement points that are multiplied to provide some cap on how much this address can stake (either self-stake or delegate). Non-engaged users are not even able to delegate.

By using a custom curve combining engagement and stake, such as bonding curves[9], we are able to select certain states without hard limits. By using a Sigmoid function[10] where the y-axis is the voting power, x-axis is stake and Engagement Rewards controlling the slope, in other words how quickly it reaches 1, then we can see that high engagement leads to reaching 1 with a lower stake. Please refer to Appendix A for some sample graphs and scenarios.

9 *https://medium.com/@aventus/token-bonding-curves-547f3a04914*

10 *https://en.wikipedia.org/wiki/Sigmoid_function*

How do engagement tokens relate to staking?

There is an element of staking aligned with a dPos model, as it engages with delegators by forming a protection to the "nothing at stake" risk with rewards for the desired behaviours and slashing for unwanted behaviour.

Some chains may favour a heavier weighting to engagement tokens which would bring the consensus model closer to a PoA model, with a different (less centralised) gatekeeper.

Others may configure a chain to use the engagement tokens as a stake to gain validation power.

An element of configuration balancing the staking and the Engagement Rewards should be left to the individual chain and the broader community to decide.

A form of cap and floor may be helpful in staking combined with the engagement tokens.

The delegator model is explored further in the Delegation and the relationship with Validators section.

Validator models

Reward functions

For now, we assume that all Validators share total rewards in proportion to their voting power[11]. The only punishment for poor performance is slashing - losing bonded stake and engagement. We could also consider replacing *k* with a quality score q_i based on the number of blocks signed, but that is out of scope of this paper.

$$\sum reward_i = block\ reward\ + transaction\ fees$$

Where

$$reward_i\ = k * power_i$$

And

$$power_i\ =\ f(engage_i, stake_i)$$

Given these definitions for the division of total rewards among all Validators based upon validation power, we propose using a sigmoid curve to provide a smooth ceiling on max stake, and incremental bonuses to power for those with high engagement.

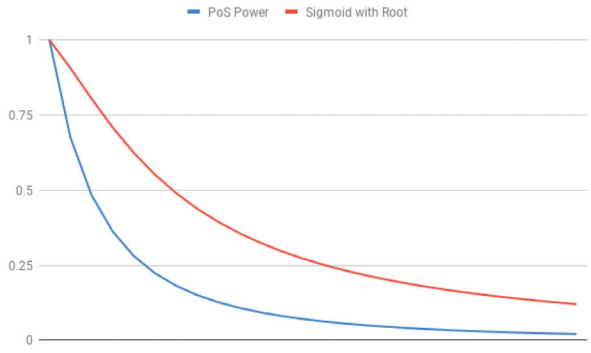
$$f(engage_i, stake_i)\ =\ r_{max} * (\frac{2}{1 + e^{-s*(engage_i * stake_i)^p}} - 1)$$

s	0.00003
r_{max}	1000
p	0.68

x-axis is the stake held and the y-axis the Engagement Rewards combined with the Stake.

[11] *We can assume there is a fixed cap on validators with the share being diluted by new validators until the cap is reached.*

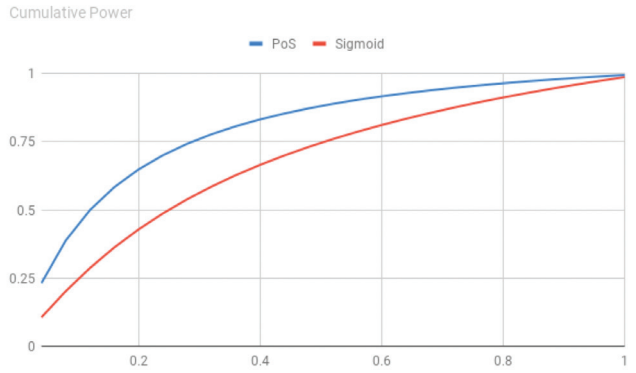
To see the effect on Validator diversity, we can fairly assume that the Validator power typically follows a Pareto distribution (80-20 rule) in proof of stake systems. Assuming that engagement is distributed independently of stake, we choose a fixed engagement for all Validators (200 in this case - similar to moderate above) and show how the sigmoid reward functions can decentralize the Validator power, compared to straight-forward PoS with one token, one vote. The sigmoid reward functions ensure no dominance of the validator pool as the rewards are capped thus removing the incentive to have a large stake, thus a large volume of validators with the optimised stake is manifested by decentralisation.



x-axis shows the PoS Power and the Sigmoid with Root, the y-axis the power

The graph is normalized such that the most powerful Validator has power of 1, which is fine, as power is relative (we just divide total rewards over the voting power). Note how the relative power of Validators drops much slower with this normalization. If engagement is distributed the same way as wealth (the same Validators are high in both), this will resume to a similar picture as straight PoS. However, solid initial conditions and rules for engagement distribution can actually favor a number or smaller, highly engaged Validators over a few large holders (eg. exchanges) that are not contributing to the ecosystem, and in such a case the distribution would be even flatter.

The advantages become more clear when we look at cumulative distribution. Or what percentage of the total voting power is held by the top 10, 20, or 30 percent of the Validators. As we see in the graph below, this is much more decentralized by applying the sigmoid curve. Whereas in vanilla PoS, the top 4% are able to halt with ⅓ of the power and the top 18% control ⅔, when we apply the sigmoid distribution, 12% control ⅓ of the power, and 40% are needed for a full ⅔ control of the network.



x-axis shows the PoS Power and the Sigmoid with Root, the y-axis the power

In Appendix A, we demonstrate a number of candidates, and encourage research and modelling to find useful distribution functions for various scenarios. Each blockchain can choose a different function for the rewards ratio based on the tokenomics, but we will highlight a few examples that we find useful.

Punishments

In a perfect world of fully engaged Validators we would only need to worry about equitable rewards. To combat the "nothing staked" problem we needed to introduce the concept of stakes, and while these have a relationship with reward, by definition they are beyond the reach of Validators. Having a stake gives the ability to punish a Validator for bad behaviour by removing some of the staked tokens, known as slashing[12].

What conditions would lead to a punishment? Clearly a long range attack[13], double signing and being offline for long periods of time are examples of undesired behaviour.

The precise slashing percentages, and frequencies are configurations set by each chain.

[12] *https://medium.com/@VitalikButerin/minimal-slashing-conditions-20f0b500fc6c*

[13] *https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9*

Balancing long term engagement with the barrier to entry

It is desirable to have the Validators aligned with the long term vision of the chain and accrue Engagement Rewards, however, there is a risk that this could end up with a situation that leads to "time served" Validators building a big advantage over newcomers.

There must be a balance between long term supporters and newer Validators who may bring fresh thinking and innovation. There are a number of ways this can be addressed through hackathons, competitions and bounties for new participations bringing innovation to the chain.

Let's imagine a hackathon which has the goal to bring innovation around running the chain and build some new and imaginative tooling. What better way than to award a chunk of Engagement Rewards to the prospective teams, this would bring in an element of competition in a supportive environment (after all Validators are keen to be involved as Engagement Rewards are up for grabs too!)?

As an ongoing theme there is a bounty programme in place that rewards innovation in the same way the hackathon worked, only this time there is a submission process that then involves all interested parties in evaluating and judging the submission. Again there is an engagement reward bounty allocated to the submitter and Engagement Rewards available to the Validators who get involved.

The long term challenge of running a successful chain where there is high engagement of all participants is not too dissimilar to most companies, there needs to be a healthy mix of long term engagement and room for fresh ideas coming in from the outside. The long term engagement brings stability, context and experience while the newer ideas potentially transform and challenge the established way of doing things.

Modelling Engagement Rewards for Validators

When defining Engagement Rewards, we need to look at the following key factors:

- Initial distribution of the rewards
- Distribution of new rewards
- Rate of decay of old rewards

When we consider the long-term evolution of Engagement Rewards, we need to evaluate two distinct points:

- The Macro level which is the change in centralization
  - Number of holders of Engagement Rewards
  - Slope of Pareto Distribution
- The Micro level with respect to Turnover
  - Do the same individuals retain their top positions, or does this change often?
  - Balancing Stability vs. Innovation

In modelling these processes, the initial impressions are that the rate of decay should be a flat percentage applied to all engagement points, such that top reward holders who cease to actively participate should quickly lose rank, faster than lower reward holders.

Furthermore, the distribution chances should be divided between new and old, such that say 50% of engagement points are distributed to existing, high-performing Validators based on their voting power. And the other 50% distributed to community members (excluding say the top 50% of Validators by engagement).

If the influx via reward and the outflux via decay are balanced, then the top Validator position will naturally be in flux, since they are subjected to decay at 100% of their power, but eligible for rewards[14] proportional to only 50% of their power.

Delegation and the relationship with Validators

The paper has explored the case of Validators and how the Engagement Rewards are combined with stakes. While delegators have been referenced, the relationship between the two needs some examination.

It is worth considering what is the purpose of delegation anyway? There were a couple of drivers behind introducing delegation, firstly an attempt to combat plutocracy[15] in PoS by giving everyone a voice, however, there is little evidence that this has been effective.

The other driver was to reward all stake-holders for reducing the liquidity of the token, and thus introduce scarcity, and this seems to be a blunt incentive to reward long term token holders. The third, and arguably the most important is that Delegators are a large driver of investment.

Our main aim, with PoE is that the majority of on-chain rewards (fees and minting tokens) should go to the whole community actively improving the system.

With this assumption, we will choose a curve like our illustrations. A sigmoid based on f = stake^x * authority^y, where low stake or low authority leads to minimal voting power and a nice mix gives much more power. This also means that the slope (votes / token) is much higher for high authority but only early on the curve. Once we approach saturation, the payback is much lower.

Let's see how we can enable delegation in this scenario, such that it (1) benefits trusted actors with limited direct access to capital, (2) provides sufficient but not excessive payment to the delegators, (3) doesn't open up attack vectors and (4) provides upward pressure on token price.

Examining (1) and (2), let's propose the following:

Delegated tokens are subject to a commission C which goes to the Validator. This has a global minimum value (say 30%) and may be set higher by Validators.

Note the Validator reward is a combination of Stake and Reward Points. So a well funded Validator who is less engaged sees lower rewards. Delegators must examine which Validators are active and earning Rewards as this has a significant influence on returns.

Assuming a Validator has a self-stake of S and a delegation of D, we can calculate the payments as follows:

(1) The Validator gets the early (best) part of the sigmoidal curve as to not be punished by delegations

(2) "Delegator rewards" are calculated on the next section of the curve and split between the delegators (1-C) and the Validator (C)

(3) All delegators receive the same payout for their tokens. We separate any payouts based on the delegation rewards from other rewards they may accrue through Engagement Rewards.

Given this, we can see the following:

- Val = f(Auth, S)
- Del = f(Auth, S+D) - f(Auth, S)
- Validator reward = Val + C*Del
- delegator reward = (1-C) * Del * (my tokens / D)

We can see how this can give significant benefit to Validators who are lower on their sigmoid curve and have a steep slope. It also provides reasonable payment to delegators, which is self-limiting: as more gravitate to one Validator, the payment per token decreases (as the sigmoid at f(Auth, S+D) begins to flatten out).

However, it opens up other issues, basically leading us back to the "nothing at stake" issue of raw POA (3). The Validator may have huge voting power with negligible self-stake. This is offset to some degree by the Engagement Rewards which are applied to the computation of reward, this has the effect that it forces the delegators not to focus on the Validators with the highest stakes but to factor in the Engagement Rewards and thus mitigates the POA aspects.

A further protection or mitigation of the concentration of delegators to the Validators with the highest stakes is to provide a maximum multiple of self-staked. This risk factor R is set globally by consensus. Total delegated tokens can be no more than R times the self-stake, D <= S * R.

To illustrate this, let's assume I have lots of authority but only 1k tokens. R is 5 and my curve flattens out around 50k stake. I can bond those 1k and attract a delegation of 5k as I am on a steep part of the sigmoid. Assuming this is still mostly linear, I receive rewards for 1k + 30% * 5k = 2.5k. As well as have voting power relative to 6k (that matters). This increases my votes by 5x and payment by 1.5x. I reinvest these and soon have 1.5k invested and 7.5k via delegations.

You can see how this slowly grows but doesn't allow the Validator to step up to a huge power solely on basis of their Authority. And since they saturate so low, this limits the tokens that can go to this one Validator (first come, first serve basis) and other delegators will go to less profitable (more saturated or less authority) Validators that have sufficient self-stake to provide space for investment.

Note this leads to a big differentiation between Validators and encourages delegators to do some research beforehand, and hold for the long term (if you get a highly paying Validator) and again must also factor in the Engagement Rewards.

[14] *Rewards in this context are the combination of Engagement Rewards and the Stake held.*

[15] *Centralisation and concentration of power/rewards.*

Further options for the Delegator model

To explore more options here, let's consider discarding anonymous delegators in the typical sense, but look at a Validator as a joint venture. Multiple people can come together to run a Validator. One is listed as the operator (who actually runs the machine) and the others are "partners". They must both agree on the set of "partners" and this ends up more like a VC round than a pure capital investment for returns.

Furthermore, the "partners" can invest not only in stake, but also authority. Let's say there is a well-funded individual with solid operational and engineering skills who wants to run a Validator, but no one knows the individual on this chain. Two people with high authority on the chain do some due diligence off chain, vest trust and they form as a joint venture.

This Validator now has the sum of authority of all members, and sum of stake of all members. (We can make authority addition sublinear if we want to avoid some pooling attacks, degrading with number of members or simply a limit of members). With significant stake and authority, they get solid rewards and voting power which they combine with the Engagement Rewards. The total rewards are split between the members of the "joint venture" in whatever way they agree. This split can be written in a smart contract and governed together. Also withdrawing from the "DAO" or pulling out stake will obviously adjust the distribution and may require consent from all parties involved. Or some waiting period.

Inflation Explored

There is some discussion around inflation and staking[16] and it highlighted the issue that in some cases a dPoS chain is geared to depositors or stakers and not necessarily around utility. An important aspect is missing, namely that people build businesses on the chain which in turn generate transactions.

Let's consider the case where an entrepreneur wanted to build a DEX to trade carbon credits, The business would be contributing via transactions to the reward pool for the Validators to run a secure chain. In the scenario where the model seems to be about return to depositors/stakers then the business would need to account for some hefty inflation?

For the Carbon trading DEX, the link to fiat is important and in a scenario where in January the rate was 1 EUR = 100 COII[17], and due to scarcity of tokens the price rose dramatically so in November it stood at 1 EUR = 50 COII that would have a big bearing on the cost of transactions as seen from a EUR perspective.

For businesses running their applications on the chain, the "Engagement Rewards" are not directly economic (i.e. direct rewards) but rather a stable, diverse Validator set, with a benign economic model that favours low inflation.

High versus low inflation

The term inflation, in tokenomics can be ambiguous, it can either mean the supply of tokens or the value. If the token supply increases, then the economic wisdom is that the value will decrease unless demand for the tokens keeps pace. If the supply of tokens decreases the opposite occurs, namely the value increases. This in practice is more nuanced and not necessarily evidenced in the "real world".

Deflationary coins[18] are an attempt to reduce the supply of coins through burning with the theory the price of the coin will increase. This is classic supply and demand economics but again ignores any utility other than rewarding some random token holders.

The important measure is the supply of tokens and the activity of staking will decrease the supply, thus the value of the tokens will increase. As seen in the models proposed introducing a sigmoid reward curve is needed to provide a cap to ensure that the "rich get richer" state is mitigated and thus maintaining a decentralised Validator set. By introducing the caps, we can observe that there are limits to the tokens being staked beyond which there are no economic benefits, this limits the supply being locked up and reduces the pressure of supply. This restraint to locking tokens through staking has a lower inflationary pressure on the value as there is an abundant supply and this benefits the application builders and companies using the chain to run their businesses.

The low inflation environment is positive for the businesses as it offers stability, and thus makes the chain attractive, and that in turn brings in more transactions (and rewards to the Validators).

[16] *https://medium.com/everett-protocol/why-a-staking-reward-in-proof-of-stake-is-economically-flawed-bcd71bb493bd*

[17] *COII is an illustrative token symbol.*

[18] *https://cryptobriefing.com/deflationary-coins-bomb-explode-fizzle/*

Conclusions

The purpose of this paper was to propose Proof of Engagement as an alternative approach to Proof of Authority and Proof of Stake.

When comparing PoA, which works by having a set number of addresses with assigned weights set upon the start of the chain. The more dynamic variant allows voting by these members to add or remove members to the set. With PoS which is a system that people can bond tokens (tie them up for a given time period) to get voting power. Voting power must be linear or super-linear to the bond (otherwise this provides an incentive split in two accounts). Many variants allow people to "delegate" to Validators, providing the Validator more voting power and splitting the rewards on this extra power with the Validator. Contrast this with PoE which combines the best from POA and POS with the added element of community engagement.

PoA has the advantages that it is simple to implement, provides stability and has the flexibility that many algorithms can be applied to the voting or reward curves without breaking it. PoS has the advantages that it requires no off-chain validation (punishment is an on-chain mechanism), there is a dynamic Validator set with no gating, and the token value increases through speculation. PoE provides both stability, with no flash changes to the Validator set, as well as dynamic membership to prevent stagnation, the ability to allow flexible curves to tailor algorithms to the chain's needs that will evolve over time through the Votes = f(Stake, Authority) mechanism. Provides on-chain punishment for any misbehavior and is secure against anonymous actors done by the most curves, requiring minimum authority to have any significant voting power.

We see the disadvantages of PoA in requiring off-chain validation and trust of the entities behind the Validators, there is a risk of forming a highly static oligarchy, and there is a "nothing at stake" risk as there is no punishment for cheating. PoS has the disadvantages that it is vulnerable to anonymous actors, such as flash loans, runs the risk of becoming a Plutocracy with no mechanisms for "progressive taxes" on the rich and it is complex to implement. PoE brings complexity in the implementation as it is a hybrid with the addition of another curve.

Let's examine the security aspects of the consensus mechanisms. PoA, is as secure as the trust in the most corruptible third, PoS is as secure providing a cartel does not build more than 50% of the market capital, and PoE is flexible and has a mix requiring access to both a large subset of the "vetted" authorities and access to a large fraction of the tokens, which are risked.

The power of PoE is in the flexibility to adapt to the lifecycle of the chain, the rewards distributed to the active community, and is resistant to centralisation.

Acknowledgements

Thanks to the following people who peer reviewed the paper and gave some valuable insight.

Dr Moustapha Awada

Dr Chulwoo Han

Sinead Stringer

We also thank **Matthew and the team at Simply VC** for their feedback, **Sahith Narahari** and **Gian Luca**.

Appendix A

Sample graphs of some reward functions

To illustrate the relationship between staking and reward against a number of different engagement levels to give a feel how this works for each function. The scenario examined assumes an engagement reward distribution that reaches a maximum around 1,000 and consider the following 5 cases for engagement:

Classification	Stake
Lurker	5
Beginner	25
Moderate	100
Skilled	300
Old-Timer	1,000

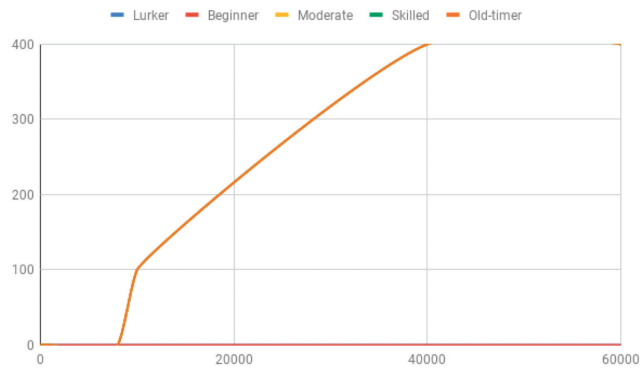
Stake is in some arbitrary token, but for the purpose of illustration, let's assume that one token is valued around 1 USD. The output is validation power, which is relative to the power of the other Validators, defining which share of the blocks and rewards go to this Validator.

Using Engagement as PoA gatekeeper, staking linear with thresholds and ceiling

$$f = engage_i < engage_{min} \,||\, stake_i < stake_{min} \,?\, 0 : r * min(stake_i, stake_{max})$$

r	0.01
$engage_{min}$	50
$stake_{min}$	10000
$stake_{max}$	40000

	5	25	100	300	1000
Stake	**Lurker**	**Beginner**	**Moderate**	**Skilled**	**Old-timer**
0	0	0	0	0	0
1000	0	0	0	0	0
8000	0	0	0	0	0
10000	0	0	100	100	100
40000	0	0	400	400	400
60000	0	0	400	400	400



x-axis is the stake held and the y-axis the Engagement Rewards

This requires a minimum engagement and stake to participate. After that, all are treated equally. A stake ceiling prevents whales from dumping.

Engagement eases in newcomers, reduces staking requirement for established

$$f = min(r_{max}, r * engage_i * stake_i)$$

r	0.0001
r_{max}	1000

	5	25	100	300	1000
Stake	**Lurker**	**Beginner**	**Moderate**	**Skilled**	**Old-timer**
0	0	0	0	0	0
10	0.005	0.025	0.1	0.3	1
100	0.05	0.25	1	3	10
400	0.2	1	4	12	40
1000	0.5	2.5	10	30	100
4000	2	10	40	120	400
10000	5	25	100	300	1000
40000	20	100	400	1000	1000
100000	50	250	1000	1000	1000

x-axis is the stake held and the y-axis the Engagement Rewards

This gives lower rewards for new-comers. Once established, the Validators can get similar rewards, and the staking requirement goes down as engagement goes up.

Basic sigmoid curve gives slightly smoother spread

$$r_{max} * (\frac{2}{1 + e^{-s*engage_i*stake_i}} - 1)$$

S	0.0000003
r_{max}	1000

	5	25	100	300	1000
Stake	**Lurker**	**Beginner**	**Moderate**	**Skilled**	**Old-timer**
0	0	0	0	0	0
1000	0.7499998594	3.749982422	14.9988751	44.96964958	148.8850336
2000	1.499998875	7.499859378	29.99100324	89.75778475	291.3126125
5000	3.749982422	18.74780304	74.85969069	221.2784679	635.1489524
10000	7.499859378	37.48243176	148.8850336	421.8990053	905.1482536
20000	14.9988751	74.85969069	291.3126125	716.2978702	995.0547537
40000	29.99100324	148.8850336	537.049567	946.8060128	999.9877117
100000	74.85969069	358.3573984	905.1482536	999.7532108	1000

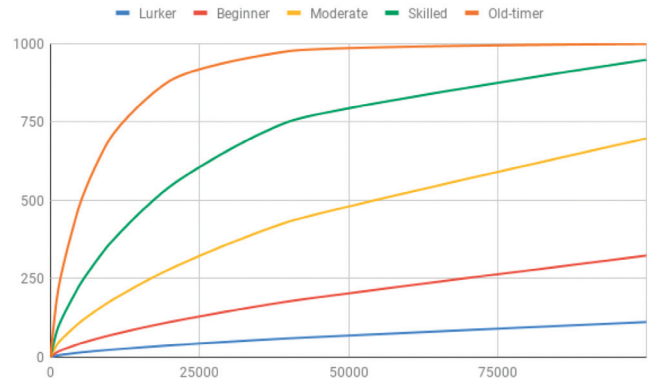
x-axis is the stake held and the y-axis the Engagement Rewards

But taking the root of engagement, staking makes it quite smooth

$$r_{max} * (\frac{2}{1 + e^{-s*(engage_i*stake_i)^p}} - 1)$$

S	0.00003
r_{max}	1000
p	0.68

	5	25	100	300	1000
Stake	**Lurker**	**Beginner**	**Moderate**	**Skilled**	**Old-timer**
0	0	0	0	0	0
1000	4.913459346	14.67774284	37.66047654	79.36324358	178.4097417
2000	7.871949296	23.5131496	60.29267813	126.7338503	281.1490864
5000	14.67774284	43.82397927	112.0887622	233.2207838	492.0445449
10000	23.5131496	70.14176955	178.4097417	363.2778164	697.8821566
20000	37.66047654	112.0887622	281.1490864	544.0324567	881.5996175
40000	60.29267813	178.4097417	432.4490626	751.803366	976.4796622
100000	112.0887622	324.1449706	697.8821566	949.0313473	999.4842028



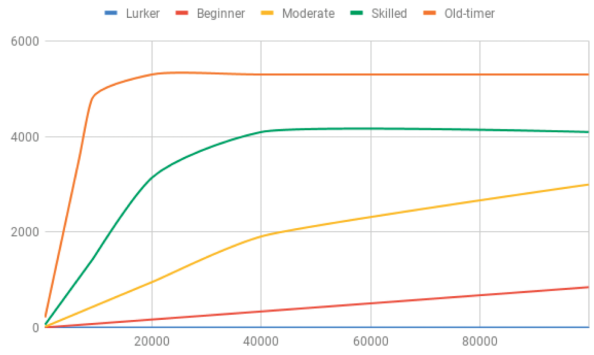
x-axis is the stake held and the y-axis the Engagement Rewards

Increasing max return with engagement
with reduced staking requirements

ln(k*engage) * min(rmax, r*stake*engage^p)

r	0.0004
r_{max}	1000
p	0.8
k	0.2

	5	25	100	300	1000
Stake	**Lurker**	**Beginner**	**Moderate**	**Skilled**	**Old-timer**
0	0	0	0	0	0
400	0	3.381786741	19.08195999	62.80603467	212.940344
1000	0	8.454466853	47.70489997	157.0150867	532.3508601
2200	0	18.59982708	104.9507799	345.4331907	1171.171892
3000	0	25.36340056	143.1146999	471.0452601	1597.05258
6500	0	54.95403454	310.0818498	1020.598063	3460.280591
9000	0	76.09020168	429.3440997	1413.13578	4791.157741
20000	0	169.0893371	954.0979993	3140.301734	5298.317367
40000	0	338.1786741	1908.195999	4094.344562	5298.317367
100000	0	845.4466853	2995.732274	4094.344562	5298.317367



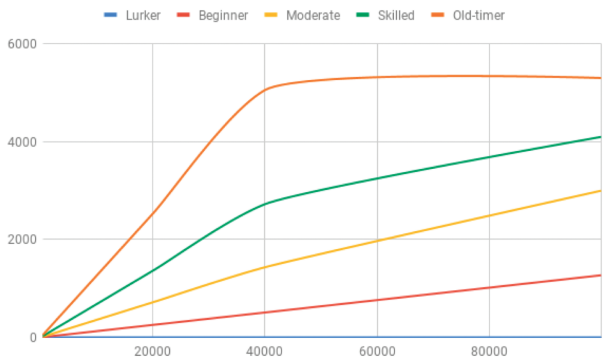
x-axis is the stake held and the y-axis the Engagement Rewards

Increasing max return with engagement
with similar staking requirements (lower p)

ln(k*engage) * min(rmax, r*stake*engage^p)

r	0.003
r_{max}	1000
p	0.3
k	0.2

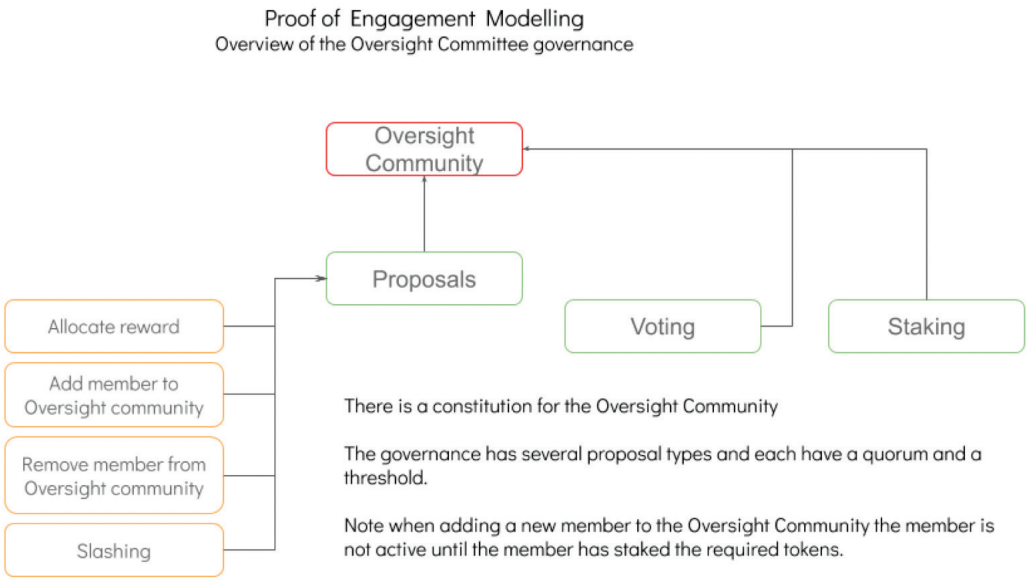
	5	25	100	300	1000
Stake	**Lurker**	**Beginner**	**Moderate**	**Skilled**	**Old-timer**
0	0	0	0	0	0
400	0	5.072680112	14.31146999	27.19581077	50.50323697
1000	0	12.68170028	35.77867497	67.98952692	126.2580924
2200	0	27.89974061	78.71308494	149.5769592	277.7678033
3000	0	38.04510084	107.3360249	203.9685808	378.7742773
6500	0	82.43105182	232.5613873	441.931925	820.6776008
9000	0	114.1353025	322.0080748	611.9057423	1136.322832
20000	0	253.6340056	715.5734995	1359.790538	2525.161848
40000	0	507.2680112	1431.146999	2719.581077	5050.323697
100000	0	1268.170028	2995.732274	4094.344562	5298.317367

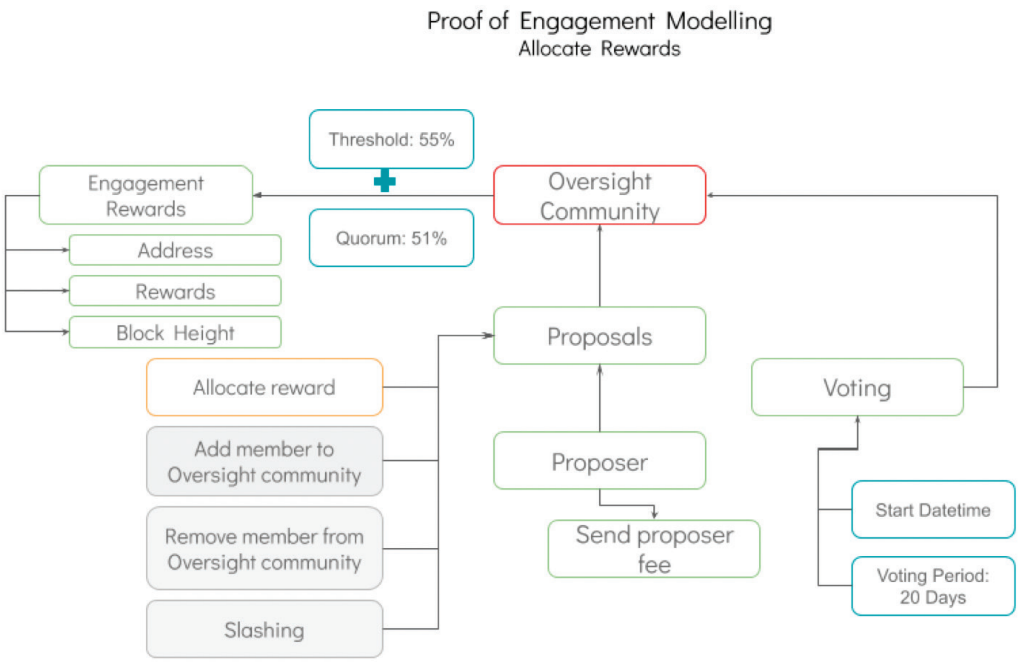


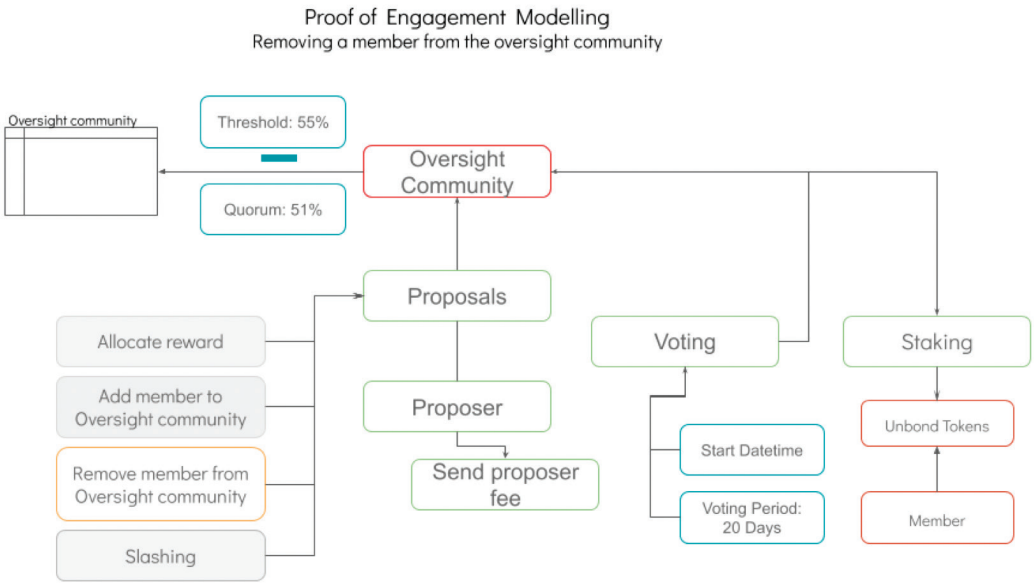
x-axis is the stake held and the y-axis the Engagement Rewards

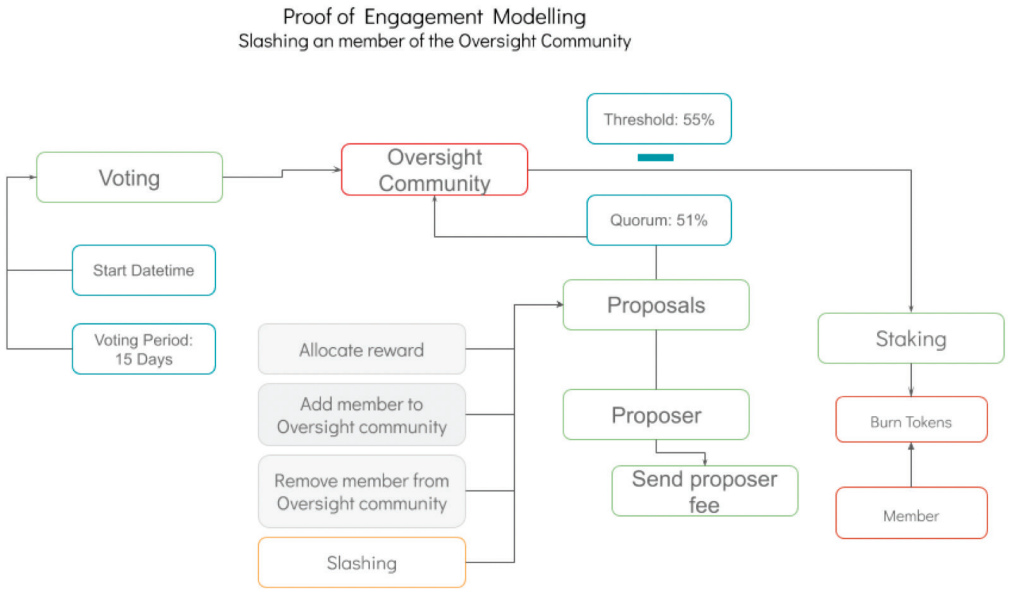
Appendix B

Modelling Proof of Engagement

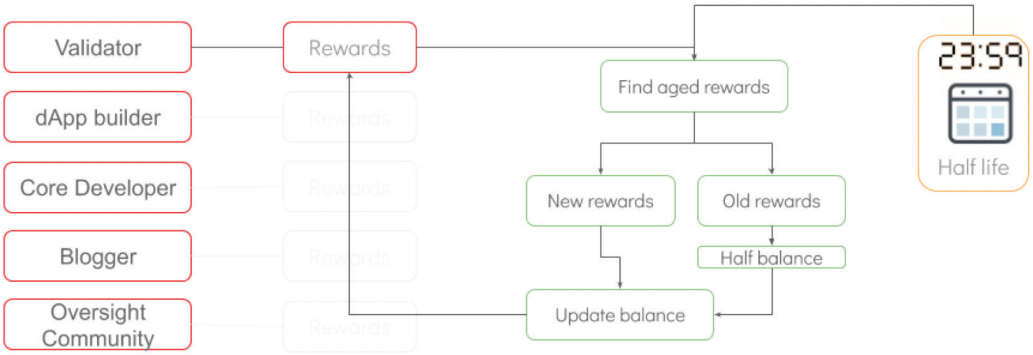





Proof of Engagement Modelling
Removing a member from the oversight community
Oversight community
Threshold: 55%
Quorum: 51%
Oversight Community
Proposals
Allocate reward
Add member to Oversight community
Remove member from Oversight community
Slashing
Proposer
Send proposer fee
Voting
Start Datetime
Voting Period: 20 Days
Staking
Unbond Tokens
Member


Proof of Engagement Modelling
Slashing an member of the Oversight Community
Threshold: 55%
Voting
Oversight Community
Quorum: 51%
Start Datetime
Voting Period: 15 Days
Proposals
Allocate reward
Add member to Oversight community
Remove member from Oversight community
Slashing
Proposer
Send proposer fee
Staking
Burn Tokens
Member

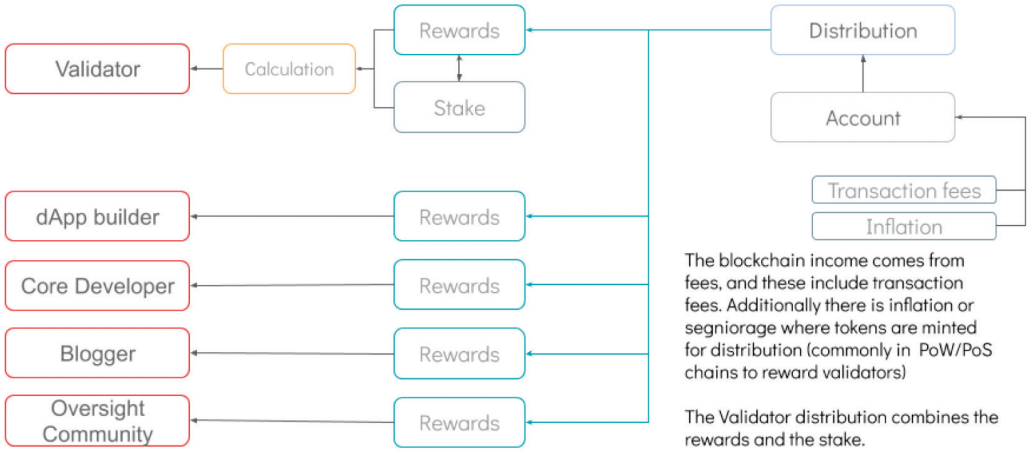
Proof of Engagement Modelling
Reward balances with half-life decay



The engaged participants accumulate rewards.

There is a half-life mechanism, where the rewards accumulate decay. Aged rewards are based block height.

Proof of Engagement Modelling
Fee Distribution



The blockchain income comes from fees, and these include transaction fees. Additionally there is inflation or segniorage where tokens are minted for distribution (commonly in PoW/PoS chains to reward validators)

The Validator distribution combines the rewards and the stake.

Appendix C

Modelling Scenarios

This section sets out the scenarios that are used in the simulations. We examine some practical implementations and some adverse scenarios to see whether the mitigation measures are complete.

Blending PoA and PoS as a soft implementation

The two consensus models PoA and PoS can be unified, let's call it PoAS. The power can be thought of as a function that has A or S, if it is S then it is pure Proof of Stake, A then pure Proof of Authority. Developing this idea we have k*A+S thus part Proof of Authority and part Proof of Stake, the function can also have the distribution curves applied, such as the sigmoid curves.

PoAS Calculated

We examine how PoA and PoS are calculated. Stake is putting funds into escrow for a bonding period, this is attached to a Validator and makes the voting power, the extension of this is delegated staking where holdings are delegated to Validators with the rewards being shared. In a similar way where there are Proof of Authority chains with the Authority being given by a centralised body we can think of Delegated Proof of Authority (dPoA). In a dPoA model the authority is delegated so all those with a vote determine new entrants.

The dPoA is then developed so rewards can be allocated from off-chain activity such as winning hackathons.

dPoAS implemented

To build a PoAS the calculations for dPoS and the mechanics of dPoA are known and can both be built as a unified consensus mechanism. Staking can be complex or simple, the authority can either be centralised or delegated, and what unifying the models brings is the ability to experiment with the configurations and weighting of each underlying module to produce the optimum outcome. This way the staking is linked to economic theory and the authority to political theory and the combination shows the impact of one on the other. The dPoAS is simulated with a range of inputs.

Tokenomics using a Proof of Engagement model

The tokenomics are important to ensure fair reward for Validators who secure the chain.

Our example chain is a marketplace for trading CO2 emissions, the chain acts as a decentralised exchange where participants sell offsets (such as tree planting schemes, investment in solar cooking schemes, wind and solar projects) to participants having calculated their carbon footprint and wanting to buy offsets.

The principal revenue comes through the listing fees of an offset project and through a small transaction fee levied.

During the bootstrapping phase the turnover is likely to be small and as awareness builds for the platform and the number of projects grows the turnover will increase.

In a classic dPoS there is an arms race to build stakes and influence, the PoE model there is a strong incentive to build Engagement Rewards and build a robust chain from the outset. The model explored shows how the interaction between all the chain participants work and the impact of Engagement Rewards on the overall returns, with the imposition of diminishing returns to discourage concentration.

Inflation

In principle there is nothing wrong with minting new tokens, as long as there are some guarantees to prevent the "new president from ruining the country".

A total supply should be identified early on considering the constraints on early engagement and that the anticipated activity in the initial period would produce sufficient demand that the utility of the token itself would maintain a stable price floor for the token.

A key aspect is that in designing a platform for long-term investments, the desired outcome is a stable token. We would expect to see as demand rises that the supply should also slowly rise. Initially the cost of validating the chain will require all new coins to go to the Validators to maintain security. As the chain grows, we should consider other schemes of how to distribute the newly minted tokens and tie it to engagement.

The awards of bonuses and bounties are for the discretion of the governance of the chain, and with a set of engaged participants these are aligned with the collective goals and values.

Token supply

A key tool in the "monetary policy" of a chain is the token supply, and by definition inflation. There are two approaches that are considered namely a capped supply at the beginning which is heavily under-utilized and transitions to an overly scarce supply with time. The second approach is a slowly growing token supply, where supply keeps pace with demand to maintain a more-or-less stable price for services, denominated in tokens.

Simulation

The purpose of the simulation is to examine the effects of inflation, token supply in the context of PoE over time.

Bootstrapping and PoE

The challenge of the bootstrapping phase is to ensure that there are rewards when there are few fees (or revenue). To have a diverse and engaged Validator set.

Consider that in the spirit of engagement that the process of engagement will help keep the number of Validators smaller on the initial chain (consider 10 Validators), as few Validators have engagement. This ensures the relatively small reward that the chain can support is enough to pay for their security.

As the chain grows economically and more actors become engaged, the Validator set will naturally expand to reach an equilibrium of 50-100 as controlled by the token economics and token price. The distribution of new Engagement Rewards behaves as a gatekeeper to limit the rate at which the network becomes "decentralized", and direct the evolution of the network toward long-term engagement over speculators.

We see here how PoE helps security in the initial phase with a limited budget, but naturally becomes more inclusive as the economy and engagement grow.

Block rewards[19] are a way to incentivise Validators (block producers) in a blockchain ecosystem for their effort of providing technical infrastructure. Block rewards are usually required for a time in which transaction fees are not sufficiently large to cover a Validator's cost.

Simulation

Explore the progression of the chain through the growth of the Validator set and the influence of the curves and engagement rewards.

Adversarial Actors

The paper has set out the aims of the PoE mechanism and the framework to incentivise the desired behaviour along with the punishment mechanisms. Let's examine the scenarios where there are adversarial actors who may not necessarily trigger a punishment, such as a validator being off-line for prolonged periods or an oversight community member breaching the constitution.

Control and influence at any cost

An actor may want to buy authority through a large allocation of tokens, this could be an exchange who has access to a large amount of tokens that they hold on behalf of their customers.
The actor knows that there are sigmoid curves in place that limit the delegation, and may not care that the Validator has low engagement rewards and that the returns are low, we assume that rational economic decisions (based on the incentives) are being ignored.

Is PoE robust enough to resist this attempt to build Authority? The cap on delegated stakes and the sigmoid curves limit the influence a single Validator has, regardless of Engagement Rewards. The simulation tests whether this is the case and examines how many Validators need to be influenced to get any meaningful power.

Cartels

The design of PoE is resistant to the formation of Cartels as the Authority is capped using the curves, and the limit of how much delegators can stake, that said, it is an interesting exercise to simulate an attempt to form a Cartel as building large stakes is only part of the equation, they would also need to build authority through engagement and maintain the Engagement Rewards, as they have decay built in. The building and maintaining of Engagement Rewards needs the consent of the community to demonstrate engagement.

[19] *https://medium.com/@simonwarta/2d747f9becf2bd*


CONFIO