Proposal 2408-01 Background Information

While, at the macro level, Proposal 2408-01 is a vote whether to deploy upgrade 7.0.3, the upgrade includes a number of bug fixes and enhancements. This document provides context for those changes and supporting information, particularly in regard to the proposed enhancements to the Proof of Fee system.

Evolving the Proof-of-Fee System

- PoF is a worthy experiment in reducing the cost of consensus.
- It has been running in the wild for nearly one year with its theoretical initial starting parameters. It may be time to update them with lessons from the field.
- Since The introduction in v6 (Nov 2023) iit has been remarkably stable
  - Never had an unintentional network halt.
- Vouch system mostly works to prevent sybil abuse
  - Has prevented anonymous privilege escalation satisfactorily
  - But requires concerted effort
- Breaks the binary choice of either PoW or PoS, which have been the de facto standards in crypto. More diversification in consensus mechanisms could lead to broader innovation in the future.
- Inclusive validation process: With validator seats being auctioned, the validation process becomes much more inclusive. This allows a wider range of validators to join, not just those with large stakes, promoting decentralization and increasing resilience and security. Particularly, several non-technical community members have managed to become validators and provide infrastructure to the network.
- Adjustable rewards: While the parameters still require fine-tuning, it is clear that PoF can adjust —and, with the right parameters, potentially minimize— rewards based on current market conditions.
- The initial settings as described in the paper assumed some things which aren't always true:
  - Validator set is dynamic and competitive
  - Validators will eventually learn their opportunity cost

Background: Defining Coalitions vc Cartels

- Coalitions are groups of people coordinating to achieve an outcome.
- Cartels are coalitions which are working against the norms of a community
- There are laws about cartels everywhere: antitrust, price fixing, etc. They only really exist when they are state-sponsored.

- Cartels are unstable because the cost to coordinate (secretly) is higher than open coalitions.
- You need to be careful if the norms are ambiguous, this is achieved through education.
- Also, generally speaking, in your game there may be microstructures that make cartel coordination cheaper than open coalition coordination. Fixing this belongs in the domain of mechanism and parameter tuning.

Early Results from the Field

1. Cartels are Fun, and cheap
    a. People like experimenting with coalition forming and price fixing.
    b. It was important for OL to have the experiment.
    c. A cartel has triggered an increase in the Thermostatic reward adjustment to be faster and more exponential than even the cartel members expected.
2. Validator set is not dynamic and competitive:
    a. The rate of adding new players is slow, especially when validators are paid market rate and the software works.
    b. This leads to a lack of competition: all the seats offered are taken by all the qualified validators.
    c. Makes auctions uncompetitive, and prone to gaming.
    d. Evidence: Over Three months all bidding validators have been included.
        i. Approximately 40 seats are always offered with exactly 40 bidders. Only ever reducing by 1 or 2 with operator failure.
3. Susceptible to Copy Pasta
    - Settings are sticky
    - People copy settings from others in public channels
    - Cartels are able to influence Copy & Paste of new members.
4. Price is not clear
    a. The UX is confusing. People don't quite understand what they are bidding on.
    b. This was acknowledged in the original paper, and an alternative presented: place bids on Net Reward, not Percent of reward.
    c. Proof of Fee 0.0.2 (Libra 7.0.3), doesn't address this issue, a forthcoming proposal could address it.
    d. This proposal tries to make the validators check their bids more often, instead of set-it-and-forget-it.
5. Vouching is very permissive
    a. The initial settings of the Vouch mechanism have been quite permissive.
    b. These settings carried over into PoF from the V5 implementation from approximately May 2022.
    a. The Monetary cost to vouch is practically zero (usually lower than the transaction fee).
    b. Relationship costs predominate decision-making, and greeable community members are more susceptible to inviting non-aligned actors, while having a resistance to expel actors.

c. Vouches are unlimited and agreeable validators give them out freely.
d. The threshold for vouches doesn't adapt to a growing network (in larger validator sets it is easier to manipulate the Vouches).

Problems the Proposed Changes Solve

Mechanism Tuning from Real World Feedback

- Experiment Result 1: Low competition: the validator sets are not dynamic.
    - Instead of a manual intervention (e.g; capping rewards), it just appears that the auctions are not competitive enough when there are few players.
    - Solution: Increase the cost of creating Cartels by making the auction always be competitive.
    - Implementation: The size of the validator set with be the min of either:
        - a) Musical Chairs recommendation, based on network performance, or
        - b) 90% count of the qualified validators (validators that are in good standing and can bid).
            - Note this parameter of 10% gap, should be evaluated in the field.
        - c) Validators with equal bids competing for a seat in the validator set will be chosen randomly, ensuring fairness.
        - Note that this restricting of validator set growth only begins to apply after a validator set of 21 seats.
- Experiment Result 2
    - Sticky Settings: Validators set-and-forget their bids
        - Bids did not have a maximum expiration, and people demonstrated this by setting long expirations.
        - This encouraged inattention from validators, and facilitated cartel behavior.
        - Solution: set a maximum bid expiration window to 45 epochs (same as vouching expiration).
- Experiment Result 3: Cost of being Agreeable
    - Tighter parameters on Vouching (no new mechanisms)
        - Cost increases:
            - The cost will be equivalent to the Nominal Reward of one epoch.
        - The number of vouches was unlimited
            - Solution: Cap it at 10
        - The number of vouches necessary (2) is low, and does not adapt to validator set size. (Large validator sets are easier to infiltrate).
            - Solution: Increase proportionally to be 10% of the Validator Set Size + 1 but not exceeding 8, allowing 2 vouches as a buffer for validators to ensure their permanence in the set if one of their vouched validators leaves the set.

- Currently the default behavior is for agreeable validators who wish to remove a peer to allow the revocation to expire (at 90 days). Said differently, manually revoking is often a too high a social cost.
  - Make vouches expire faster 45 days, instead of prior 90 days.
  - Revocations have no cost.

Involuntary features (bugs)

- **Bug 1**: There was no tie-breaker for lowest placed bids, and as such the order of onboarding to the network became the de-facto tie breaker. This is unintended.
  - **Solution**: Randomization of accounts in tied positions was added to the sorting of bids
- **Bug 2:** The accounting of rewards in the epoch was incorrectly using the reward amount before the execution of the thermostat. When the thermostat increased the reward value, the subsidy allocated for rewards became insufficient. This resulted in the last validator in the payment list (the lowest bidder) not getting paid. Although some believed this was an intentional feature, it was actually unintentional. Combined with Bug 1, it consistently excluded the most recent members who bid the lowest.
  - **Solution:** Execute the thermostat before the allocation of subsidies for the rewards, ensuring the correct count of validators and sufficient funding for all payments.
- **Bug 3**: Even after the exclusion of miners in previous versions, a subsidy equivalent to 1 validator was still being allocated to pay miners (even though they were not being paid). This subsidy, combined with Bug 2, was still insufficient to pay all validators when the thermostat increased the reward value. Without this bug, even more validators would have missed out on their rewards. It's also important to note that the insufficiently allocated subsidy for paying the validators is being burned every epoch.
  - **Solution:** Remove the allocation of the additional validator reward.

Additional Technical Changelog

- [move] Implemented the offer/claim pattern for new authorities in multisig accounts.
  - [#228](https://github.com/0LNetworkCommunity/libra-framework/pull/228) by @soaresa

- [move] Improved bid competition and ensured fairness when selecting validators with tied bids; fixed subsidy allocation for validator rewards.
  - [#299](https://github.com/0LNetworkCommunity/libra-framework/pull/299) by @soaresa

- [move] Enhanced the vouch system by setting a maximum number of vouches per validator, updating vouch cost each epoch as a nominal reward, and making the number of required vouches to join the validator set dynamic.

    - [#303](https://github.com/0LNetworkCommunity/libra-framework/pull/303) by @soaresa

- It's worth noting that the upgrade implements 114 new Move tests and improves the existing ones. This will increase our Move test coverage score by 5.62%, bringing it to 71.36%.

Expectations for Outcomes

In addition to bug fixes and technical enhancements:

- This upgrade will make the seating of validators in the Proof of Fee auction more competitive.
- Incentivize engagement: Many changes will activate social behaviors, and we expect inattentive or passive validators to drop off.
- Education: Expect the validators to consider the effect of the bidding since it must happen more often.
- The validator set size will become smaller, with more mission aligned validators.
- Automated thermostatic adjustments may stop to increase price based on higher costs of price-fixing.

Potential Issues That May Result From Passage of the Proposal

- Excessive drop outs: validators might uniformly (not just the unprofitable ones) prefer to abandon the game (turn off the machines) rather than sit out and wait another turn. Then the set will reduce.
- Vouches will not keep pace: There could be boundary effects from when the validator set increases by 10 (e.g; 30 to 40), and the number of validators with sufficient vouches is below the target (e.g. only 25 validators have 4 vouches at 40). This could artificially limit the growth of the validator set if validators are inattentive to the vouch requirements.
- Runaway Overheating: The thermostatic adjustment may not react to the competitive auction. The initial parameters for Thermostat might need a separate reconsideration. The assumption that the Thermostat should react quickly to the validator market, may not have been a good assumption (especially when we are educating infrastructure providers on a new concept).
- Updating Bids proves to be a chore, and validators drop out. This could of course be automated by the validators with their own scripts. But for now, we can err on the side of asking for more attention. Perhaps at some point we can relax the amount of attention validators give to the game.
- Family Tree as a root of trust might prevent the higher vouch requirement from growing the validator set. There's a concern of a scenario where the set would grow up to a certain number, which would require 10% of the set size in vouches, which might not be

possible for the most common family trees, which could collapse the whole set and maybe even halt the network. Likely the seeds of the family tree need updating altogether, which would be out of scope for this upgrade

- Unfollow-follow game: A validator voucher Alice, can revoke the vouch to a vouchee Bob immediately prior to them being jailed. This way they avoid the black mark of the reputation engine marking Alice as having onboarded an unreliable validator. However currently, Alice can quickly re-vouch for Bob when his operations have stabilized. When the cost increases, this game is only available to well funded Alices.