Taraxa PBFT

Version 1.0

February 01, 2025

Contents

1 Consensus Protocol

1.1 Round (p, r) Constants

$\lambda_{0min} = 500$ [ms]
$\lambda_{0max} = 1500$ [ms]

When user u starts round (p, r), they reset their timer_u to 0 and other constants as follows:

- If $r = 1$:
  - $\lambda_r \in (\lambda_{0min}, \lambda_{0max})$
  - $\Lambda_r = 4000$ [ms]
- Otherwise if $r >= 2$:
  - $\lambda_r = 2000$ [ms]
  - $\Lambda_r = 17000$ [ms]

1.2 Round (p, r) Voting Instructions

The voting instructions are as follows:

Step 1: **Proposal** - When $\text{timer}_u = 0$:

- If $r = 1$ or $r > 1$ and u has received a next-quorum for $\perp$ from round $(p, r-1)$, then u assembles a new block proposal B_u and propagates B_u and $H(B_u)$.

– Otherwise, if $r > 1$ and u has received a next-quorum for $H(B') \neq \perp$ from $(p, r-1)$, then u propagates $H(B')$.

Step 2: **Filtering** - When $\text{timer}_u = 2\lambda_r$:

– If $r = 1$ or if $r > 1$ and u has received a next-quorum for $\perp$, then u selects the proposal with the minimum credential and soft-votes for it.

– Otherwise, if $r > 1$ and u has received a next-quorum for $H(B') \neq \perp$, then u soft-votes for $H(B')$.

Step 3: **Certifying** - While $\text{timer}_u \in (2\lambda_r, \max(4\lambda_r, \Lambda_r))$:

– If u receives a soft-quorum for $H(B)$ and a valid block B with $H(B) = H(B)$, then u cert-votes for $H(B)$.

Step $s = 2n$, where $n \in (2, \infty)$: **First Finishing Step** - When $\text{timer}_u = \max(4\lambda_r, \Lambda_r) + (s-4)\lambda_r$:

– If i has certified some value v for round r, he next-votes v.

– Else if ($r \geq 2$ and i has seen $2t+1$ next-votes for $\perp$ for round $r-1$), he next-votes $\perp$.

– Else he next-votes his starting value st_i^r.

Step $s = 2n+1$, where $n \in (2, \infty)$: **Second Finishing Step** - When $\text{timer}_u = \max(4\lambda_r, \Lambda_r) + (s-5)\lambda_r + 100\text{ms}$:

– If i sees $2t+1$ soft-votes for some value $v \neq \perp$ for round r, then i next-votes v.

– If ($r \geq 2$ and i sees $2t+1$ next-votes for $\perp$ for round $r-1$ and i has not certified in round r), then i next-votes $\perp$.