NEBULAS

Blue Paper

Nebulas Research

June 2019
Version:1.0.1

Contents

1 Consensus

- b: block
- $Pre^{(i)}(b)$: b's i-th-generation ancestral block
- B: Local blockchain
- fr: Round of finality
- sk: secret key
- pk: public key
- S: committee set
- H_t: height gap between finality.

Algorithm 1: Candidate: collecting blocks

```
Input: S,pk
while true do
    $b \leftarrow$ new received valid block ;
    $B \leftarrow B \cup b$;
    if $Height(B) = H_t * fr$ and $pk \in S$ then
        Path $p \leftarrow (Pre^{(H_t-1)}(b)), Pre^{(H_t-2)}(b))..., Pre^{(1)}(b), b)$;
        New thread: $Finalize(p, sk, pk, fr)$;
        $fr \leftarrow fr + 1$
```

```
Algorithm 2: Committee: Finalize
Input: $p, sk, pk, fr$
$0 \leftarrow round$;
$Gossip(pk, fr, sign_{sk}(p||fr||round))$;
$start \leftarrow Time()$;
$P_s = \{(p, sign_{sk}(p))\}$;
while $Time() < start + \lambda$ do
    $P_s \leftarrow P_s \cup (newly\ received\ path, signature)$
if $|P_s| > \frac{3}{4}|S|$ then
    $round \leftarrow 1$;
    $b \leftarrow$ deepest block occur in at least $\frac{3}{4}|S|$ paths in $P_s$;
    $P_s \leftarrow$ set of paths in $P_s$ contains $b$;
    $Height \leftarrow |Common\_Prefix(P_s)|$;
    Require Block information of $Common\_Prefix(P_s)$ and use it to update $B$
      in this epoch;
    $Gossip(pk, Height, P_s, round, sign_{sk}(Height||P_s||fr||round)$;
    break;
$round \leftarrow 2$;
if Terminating Condition then
    $Gossip(pk, Height, P_s, round, sign_{sk}(Height||P_s||fr||round)$
else
    while $Time() < start + \lambda_2$ do
        Get $(m.Height, m.P_s, m.signature, m.pk)$ from received message $m$ in
          round 1 or 2. ;
        if $m.Height > Height$ and $valid(m, pk, signature)$ then
            $P_s = m.Ps$;
            $Height = m.Height$;
            Require information for newly added blocks and use it to extend $B$
    $Gossip(pk, Height, P_s, round, sign_{sk}(Height||P_s||fr||round)$ while
     $Time() < start + \lambda_3$ do
        Update $count[Height]$ from received message in round 2.
    if no $count[Height] > \lambda_3|S|$ then
        $Gossip(pk, sign_{sk}(Timeout))$
```

References