Preuve de la Safety du Consensus Jolteon

Notation

- $B_i \leftarrow QC_i \leftarrow B_{i+1}$ signifie que B_i est certifié par QC_i qui est compris dans B_{i+1} (B_{i+1} est le block précédent B_i mais pas nécessairement à 2 rounds consécutifs)
- $B_i \leftarrow^* B_j$ signifie que B_j étend B_i i.e. il existe une chaîne :
  $B_i \leftarrow QC_i \leftarrow B_{i+1} \leftarrow QC_{i+1} \leftarrow [\dots] \leftarrow B_{j-1} \leftarrow QC_{j-1} \leftarrow B_j$
  (un block s'étend lui-même : pour tout block B, on a $B \leftarrow^* B$)

Définition Global Direct-Commit

Un block B est dit globally direct-committed (GDC) si $f+1$ replicas <u>honnêtes</u> votent pour une proposition de block B' au round $B.r+1$ tel que $B'.qc$ certifie B

Théorème

Soit B un block GDC, pour tout block certifié B' tel que $B'.r \geq B.r$, on a : $B \leftarrow^* B'$

Preuve:
Soit B un GDC, on note $r_0 := B.r$
Pour tout $r \geq r_0$, on note :
$P(r)$: "Pour tout block B' certifié au round r, on a $B \leftarrow^* B'$ "
On procède par récurrence forte:

- Initialisation : pour $r = r_0$, comme B est GDC, il est par définition certifié. Il est donc le seul block certifié au round r_0. Or $B \leftarrow^* B$ par définition du formalisme. Ainsi $P(r_0)$ est vraie.
- Hérédité : Soit $r' > r_0$, on suppose que $P(r)$ est vraie pour tout $r \in [\![r_0, r'-1]\!]$, montrons que $P(r')$ est vraie :
  - Si aucun block n'est certifié au round r', alors $P(r')$ est vraie.
  - Si un block B' est certifié au round r, alors il existe un block B'' certifié au round $r'' \in [\![r_0, r'-1]\!]$ tel que $B'' \leftarrow QC_{B''} \leftarrow B'$ donc par hypothèse de récurrence, $P(r'')$ est vraie, et on a
    $B \leftarrow^* B'' \leftarrow QC_{B''} \leftarrow B'$ d'où $B \leftarrow^* B'$ et donc $P(r')$ est vraie :
    * En effet, B' étant certifié ne peut étendre qu'un block certifié d'un round strictement inférieur, donc $r'' < r'$
    * Par ailleurs, si $r'' < r_0$, alors $r' > r''+1$ donc B' contient un TC (nouveau formalisme contenant les r_{lock} signés) avec $2f+1$ r_{lock} de replicas. Comme B est GDC, au moins un de ces r_{lock} appartient à un des $f+1$ replicas honnêtes ayant voté pour le block étendant B au round r_0+1 et donc ce r_{lock} est supérieur ou égal à r_0. Cette actualisation du r_{lock} est forcément antérieure au TC qui a été formé au round $r'-1 \geq r_0$ car il n'a pas pu être formé au round r_0 où B a été certifié et s'il a été formé au round r_0+1 c'est nécessairement après que les f+1 replicas honnêtes aient voté pour le block étendant B car ils ne peuvent pas voter après avoir émis leur timeout message. Ainsi les $2f+1$ replicas honnêtes ne pourraient pas voter pour B' car
      $r'' = B'.qc.r < r_0 \leq \max(r_{\text{lock}} \in B'.tc)$ et donc B' ne pourrait pas être certifié. Or B' est certifié donc par l'absurde : $r'' \geq r_0$.
- Conclusion : La propriété P est initialisée à r_0 et est héréditaire donc par récurrence forte elle est vraie pour tout round $r \geq r_0$.

Corollaire

Soient B et B' tous deux GDC, alors on a :

$$\begin{cases} B \leftarrow^* B' \\ \text{ou} \\ B' \leftarrow^* B \end{cases}$$

Preuve:
Par définition, GDC $\Rightarrow$ certifié et on a toujours : $B.r \geq B'.r$ ou $B'.r \geq B.r$

Safety

Un block certifié (et tous ses ancêtres) est commit s'il est étendu par un block certifié consécutif. Donc par définition, commit $\Rightarrow$ global direct-commit car parmi les $2f + 1$ votants au plus f sont byzantins donc au moins $f + 1$ sont honnêtes. Ainsi, grâce au corollaire précédent, à chaque fois qu'un replica commit, il a la certitude que le dernier block qu'il commit est GDC et donc qu'il existe une chaîne, unique car chaque block n'a qu'un parent, entre ce block et le dernier qu'il avait commit, lui aussi GDC et donc par récurrence une unique chaîne jusqu'au Genesis block qui est par définition commit. Cette chaîne, qui une fois commit est inaltérable, est commune au moins aux $2f + 1$ replicas honnêtes qui ont exécuté de manière identique le consensus. On obtient alors une blockchain sécurisée, ce qui prouve donc la safety du Consensus Jolteon.