Exercices sur Sync HotStuff

Sync HotStuff : Simple and Practical Synchronous State Machine Replication

Article disponible à l'adresse suivante `https://eprint.iacr.org/2019/270.pdf`

Questions sur cet article

- Qu'est-ce que le problème SMR ?
- Quelles sont les propriétés d'un service SMR ? Donner des exemples.
- Quel est l'objectif de l'algorithme Sync HotStuff ?
- Quelles sont les hypothèses réseaux/machines faites par les auteurs ?
- En quoi Sync HotStuff est-il *practical* ?
- Quels sont les deux modes de fonctionnement de l'algorithme ?
- Quels sont les probèmes liés à l'hypothèse de Lock-Step ?
- Quelles sont les limites théoriques en nombre de Bizantins selon les hypothèses réseaux/machines pouvant être supportées pour un protocole de consensus ?
- Comment pourraient-être choisis les *leaders* (autrement qu'avec un *round-robin* ?
- A quelle vitesse les blocs sont-ils produits ? Commités ?
- Quelles sont les mécanismes pouvant être utilisés par un attaquant pour empêcher la progression de la blockchain ?
- Donner un exemple d'exécution du protocole *steady state*
- Donner un exemple d'exécution impliquant le protocole *view-change*
- Pourquoi attendre un temps de 2Δ est suffisant pour *commiter* sur un bloc (pourquoi cela assure la *safety*) ?