# Byzantine Fault Tolerance

Alexandre SALMON

# Sommaire

- Problème des deux Généraux
- Problème des Généraux Byzantins
- Applications concrètes
- PBFT
- Proof of Work
- Démonstration BFT-Smart

# Problèmes des deux généraux

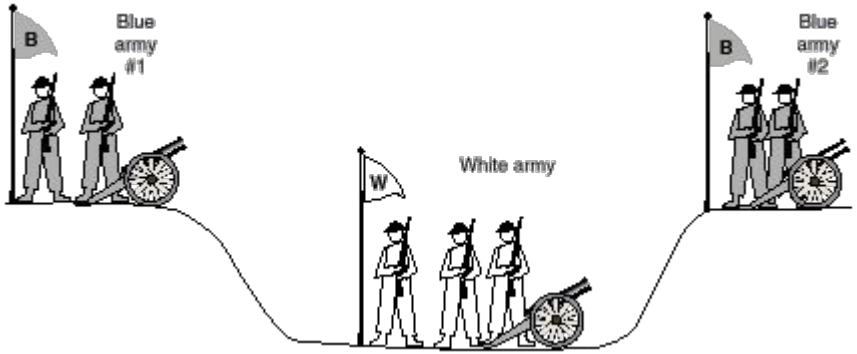
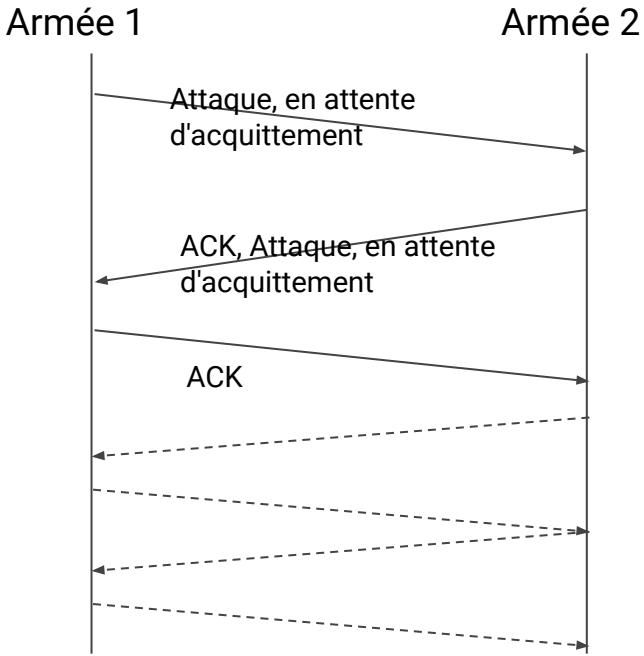



Fig 1: Les deux generaux http://www.ee.surrey.ac.uk/

- Publié par: E. A. Akkoyunlu, K. Ekanadham, et R. V. Huber en 1975 dans "Some Constraints and Trade-offs in the Design of Network Communications"

- Problème de consensus
- Canaux de communication faillibles

# Problèmes des deux généraux

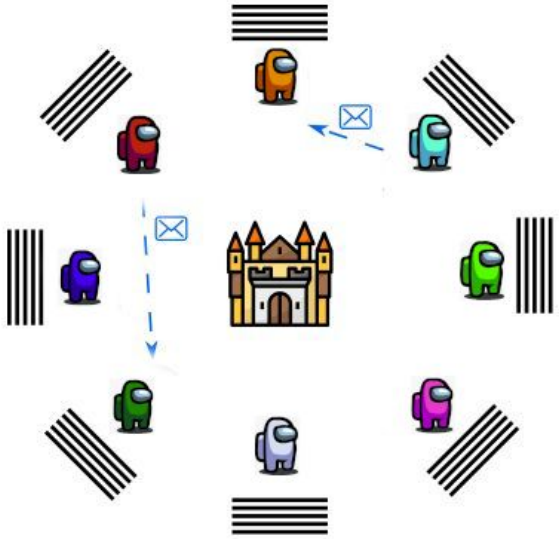



- Solution inspirée d'uen demande de connection TCP (SYN, SYN-ACK, ACK)
- Impossible de manière déterministe

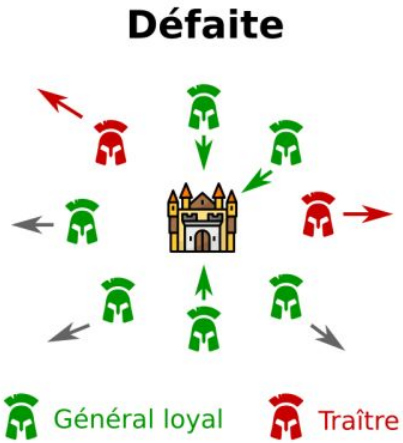
# Problème des Généraux Byzantins

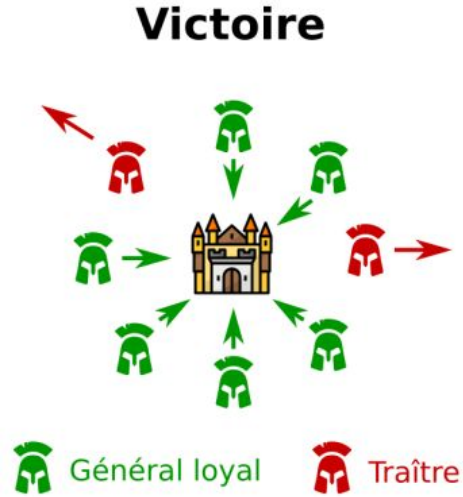
Publié par: Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem". *ACM Transactions on Programming Languages and Systems*.

- Multiples généraux
- Canaux faillibles
- Certains généraux sont des traîtres
- Tous les généraux loyaux doivent parvenir à la même décision (Consensus)



https://bitcoin.fr/le-probleme-des-generaux-byzantins/




https://viresinnumeris.fr/probleme-generaux-byzantins/

# Concrètement

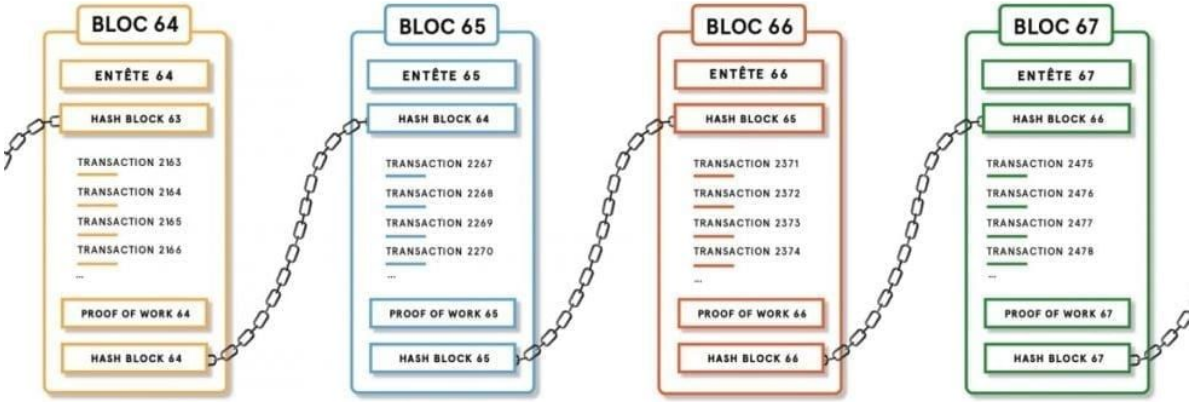
Fautes Byzantines:

- Erreur matérielle
- Noeud malintentionné

Domaines d’application:

- BD Distribuées
- Systèmes Redondant
- Blockchain

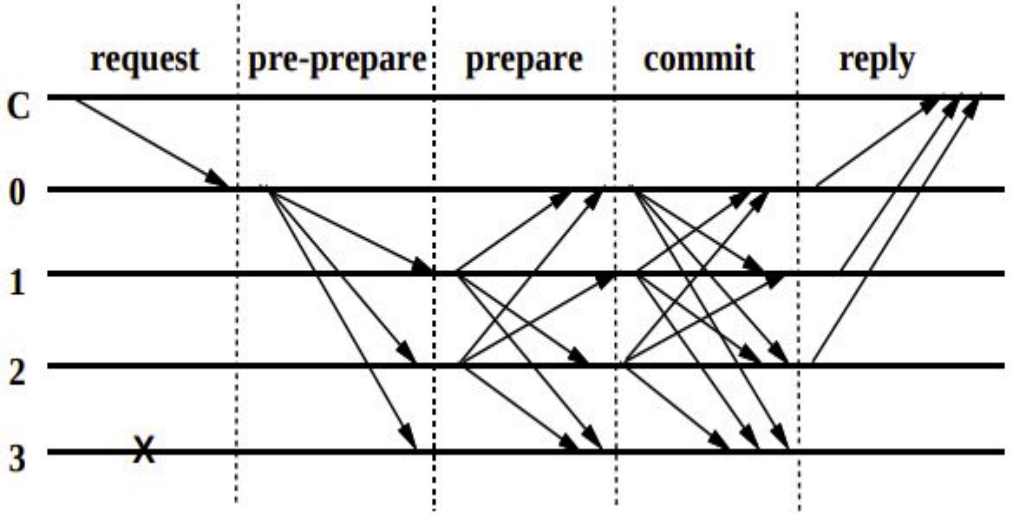
# Proof of Work




- Publié par  Satoshi Nakamoto
- Confiance par l'effort fourni
- Nécessite 50% de la puissance du réseau pour falsifier durablement
- Preuve de travail: Résultat d'un calcul de hash très complexe

source: https://cia.news/comprendre-la-technologie-blockchain/

# Practical Byzantine Fault Tolerance



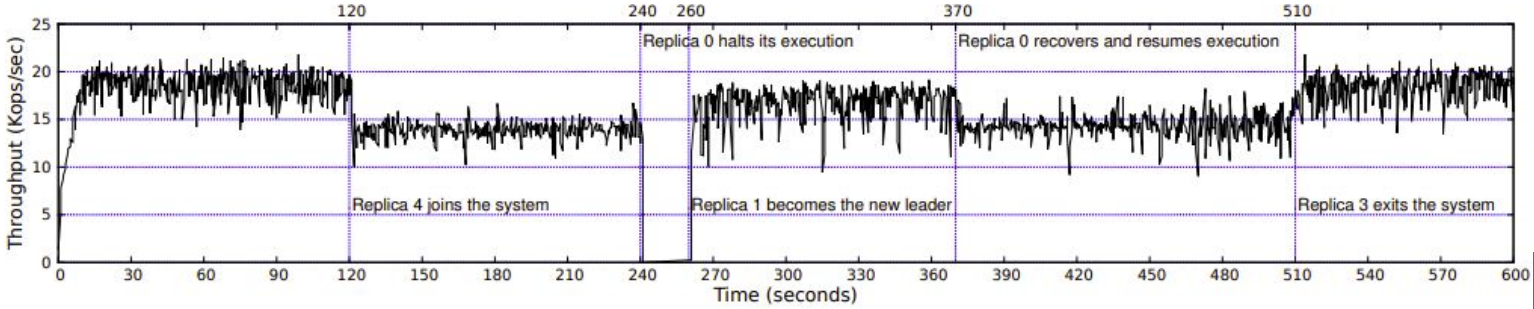

source: “Practical Byzantine Fault Tolerance” Miguel Castro and Barbara Liskov

- Publié par: Miguel Castro et Barbara Liskov en 1999 dans “practical Byzantine fault tolerance”
- Supporte *f* fautes sur *3f+1* noeuds

# BFT-SMaRt

| System | Throughput | Clients | Throughput 200 |
|---|---|---|---|
| BFT-SMaRt | 83801 | 1000 | 66665 |
| PBFT | 78765 | 100 | 65603 |
| UpRight | 5160 | 600 | 3355 |

- Librairie Java Open-Source
- Robuste
- Modulaire
- MultiCore




State Machine Replication for the Masses with BFT-SMART, Alysson Bessani, João Sousa Eduardo E. P. Alchieri

# Demo BFT-SMaRt

# Merci