IRIMAS UNIVERSITÉ HAUTE-ALSACE
Institut de Recherche en Informatique, Mathématiques, Automatique et Signal

LINEACT cesi

# "Toward an Optimal Consensus Protocol for Private Blockchains"


Réalisée par: RIAHI Kenza

Dirigée par: Mr IDOUMGHAR Lhassane

Mr ABOUAISSA Abdelhafid

Encadrée par: Mr BRAHMIA Mohamed-El-Amine

# Mon parcours

2016
Baccalauréat
Sc. mathématiques
Casablanca, Maroc

2016 – 2018
Classes Préparatoires MP
Lycée Mohammed V, Casablanca, Maroc

2018 – 2020
1ère et 2ème année cycle ingénieur en informatique, systèmes d'information
EMI, Rabat, Maroc

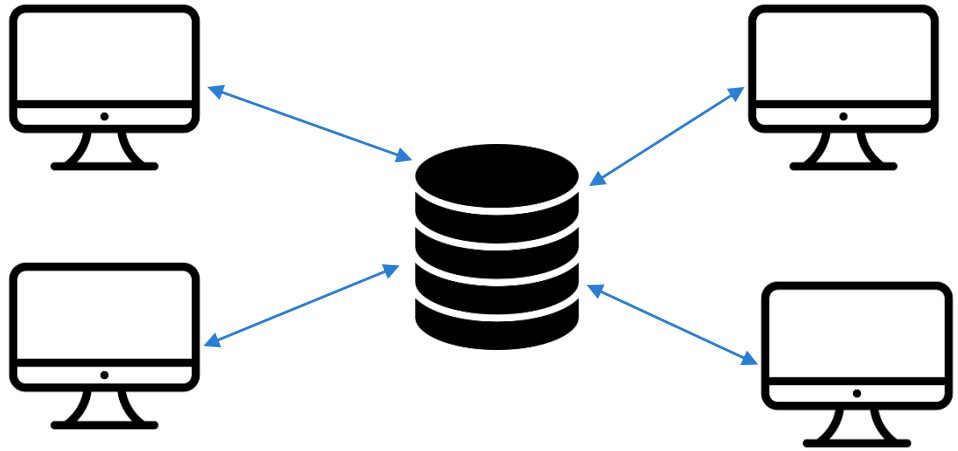
Sep. 2020 – fev. 2021
Semestre d'échange
ENSTA Bretagne, Brest, France

Mars 2021 – août 2021
Stage de fin d'études
Laboratoire DISP, Lyon, France

Nov. 2021 à ce jour
Thèse en informatique
IRIMAS & LINEACT

# Contexte

- Domaines:
  - Médical, smart cities, véhicules autonomes, bâtiments intelligents, finance, etc.
- Problèmes liés aux données:
  - Données privées et confidentielles
  - Attaques fréquentes
- Limites d'un système centralisé
  - Single point of failure



→ **Solution: la Blockchain**

# Blockchain: domaines d'application

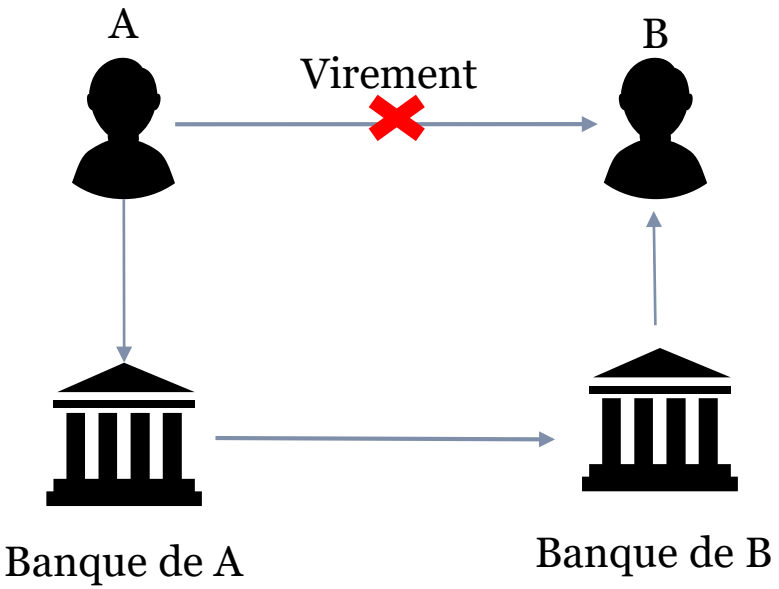
- Transactions financières sécurisées.
- Exemples: Bitcoin, Ethereum, etc.


- Tracer les marchandises: bijoux, vêtements, aliments, médicaments, etc.
- Exemple: Auchan & Carrefour depuis 2018 pour la traçabilité des produits.

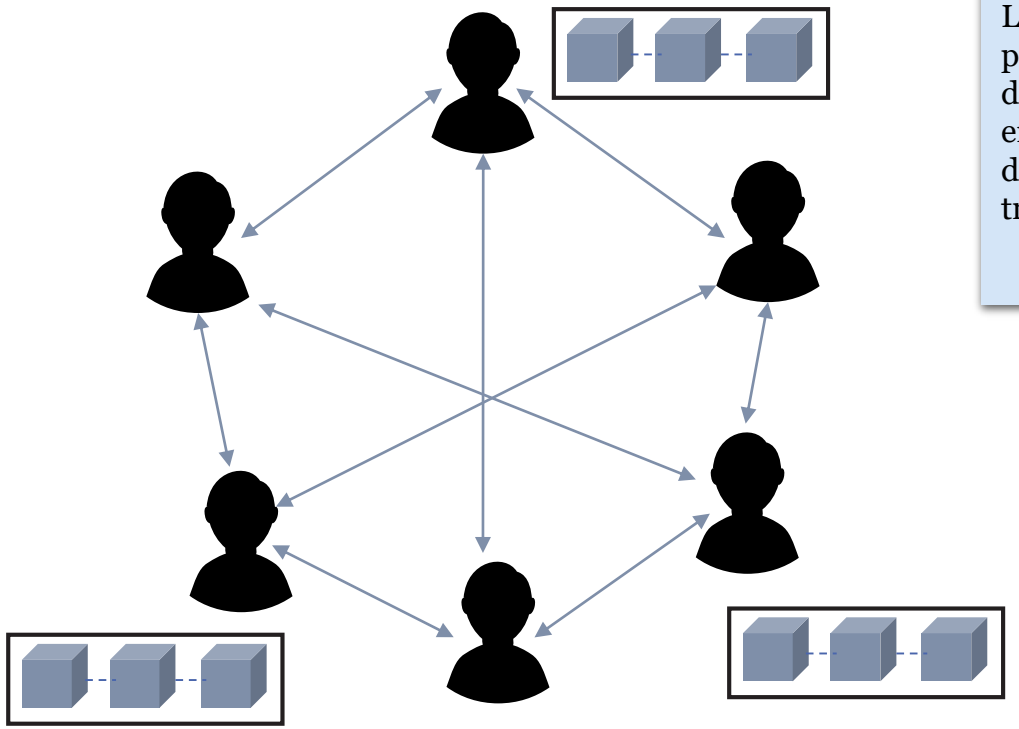

- Smart cities: mobilité, efficacité énergétique, smart buildings, traitement des déchets, sécurité, etc.

# Principe de la Blockchain

## Système financier classique

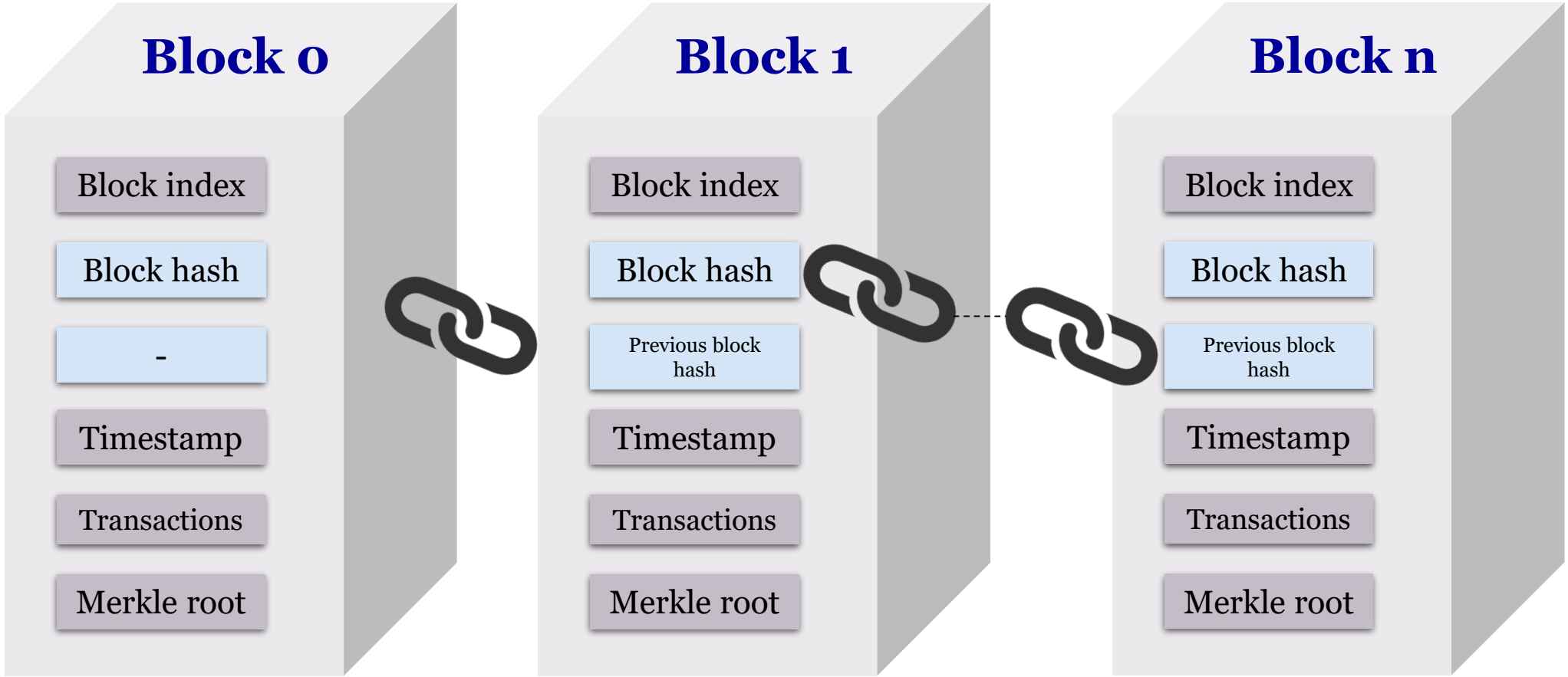



## Système financier décentralisé



La Blockchain apparaît la première fois en 2008 dans le domaine financier en tant que technologie de décentralisation des transactions financières.

# Structure de la blockchain



# Types de Blockchain

| | Blockchain publique | Blockchain privée |
|---|---|---|
| Caractéristiques | N'importe qui peut y accéder et participer au consensus | Gérée par une ou plusieurs entités définissant les droits d'accès |
| Avantages | • Complètement décentralisée<br>• Totalement transparente | • Moins de consommation d'énergie<br>• Plus rapide<br>• Meilleure confidentialité |
| Inconvénients | • Confidentialité des données non assurée<br>• Importante consommation d'énergie<br>• Délai de réponse important (env. 10 min) | • N'est pas complètement décentralisée |

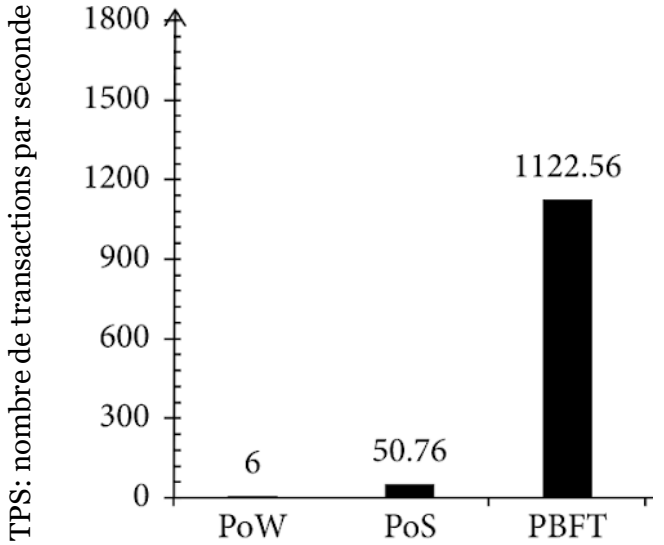
# Protocoles de consensus

| Nom du consensus | Principe | Avantages | Inconvénients |
|---|---|---|---|
| PoW (Proof of Work) | Les mineurs sont en concurrence pour résoudre un problème mathématique complexe. | -Peut tolérer jusqu'à 50 % de nœuds malveillants.<br>-Scalabilité presque illimitée. | -Coûteux en temps et en énergie.<br>-Mining pools => Centralisation. |
| PoS (Proof of Stake) | La sélection du mineur est aléatoire mais tient compte de la quantité de cryptomonnaie à disposition (stake). | -Moins coûteux en énergie que le PoW.<br>-Scalabilité presque illimitée.<br>-Risque d'attaque du réseau plus faible que le PoW<br>-Plus décentralisé que le PoW | -Concentration de la puissance de hachage<br>-Débit limité |
| DPoS (Delegated Proof of Stake) | La sélection se fait sur des critères tels que: l'ancienneté, la quantité de monnaie possédée… | -Plus économe en énergie que PoW et PoS .<br>-Plus rapide que PoW et PoS<br>-Extensibilité illimitée | - Moins décentralisé<br>- Moins résistant aux attaques |
| PBFT(Practical Byzantine Fault Tolerance) | Permet à un réseau distribué de parvenir à un consensus même lorsque certains des nœuds du réseau ne répondent pas ou répondent avec des informations incorrectes. | -Plus rapide<br>-Résistant aux nœuds byzantins<br>-Consomme moins d'énergie | -Extensibilité limitée<br>-Importante consommation de la bande passante |

# Practical Byzantine Fault Tolerant (PBFT)

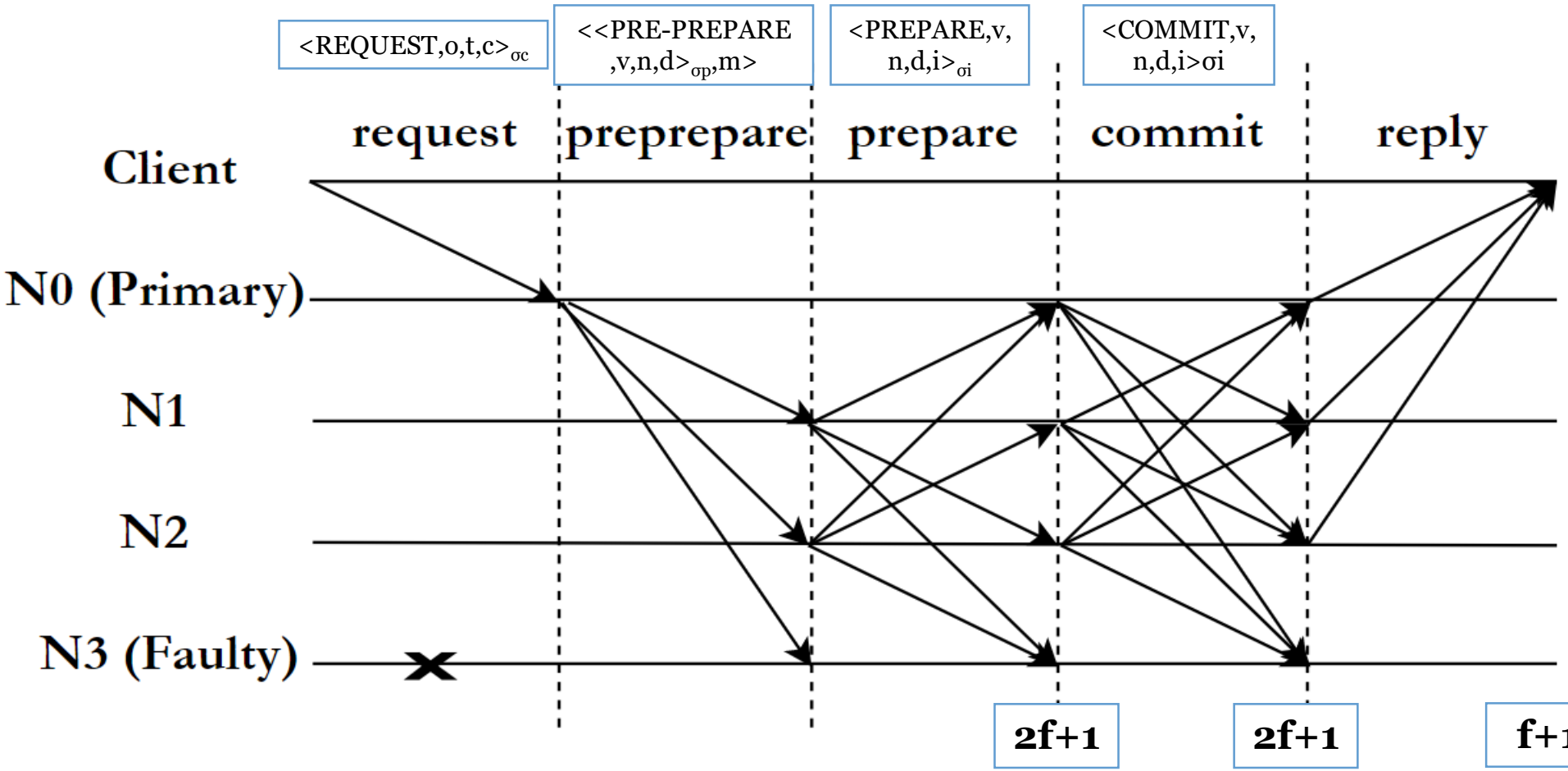
- Proposé en 1998 par Miguel Castro et Barbara Liskov
- Byzantine Fault Tolerant: Tolère les nœuds byzantins-comportement arbitraire
- Systèmes « éventuellement synchrones » comme internet => résistant aux attaques DoS
- Faible consommation d'énergie (≠PoW)
- Plus rapide que le PoW et le PoS

Mais grand nombre de messages échangés




*Wu, Y., Song, P., & Wang, F. (2020). Hybrid consensus algorithm optimization: A mathematical method based on POS and PBFT and its application in blockchain. Mathematical Problems in Engineering, 2020.*

# Etapes du PBFT




N>=3f+1

v: vue

- Nœud primaire: p = v mod N
- n: numéro de séquence de la requête, choisi par p / ordre d'exécution des opérations
- d: digest du message/hash

# Limites du PBFT

- Non scalable
- Nombre considérable de messages échangés: 2N(N-1)

  300 nœuds => 179 400
- Consommation de la bande passante
- Nœud primaire: p = v mod N => Un nœud primaire malicieux n'est pas éliminé, il peut devenir primaire à plusieurs reprises

# Problématique

Objectifs

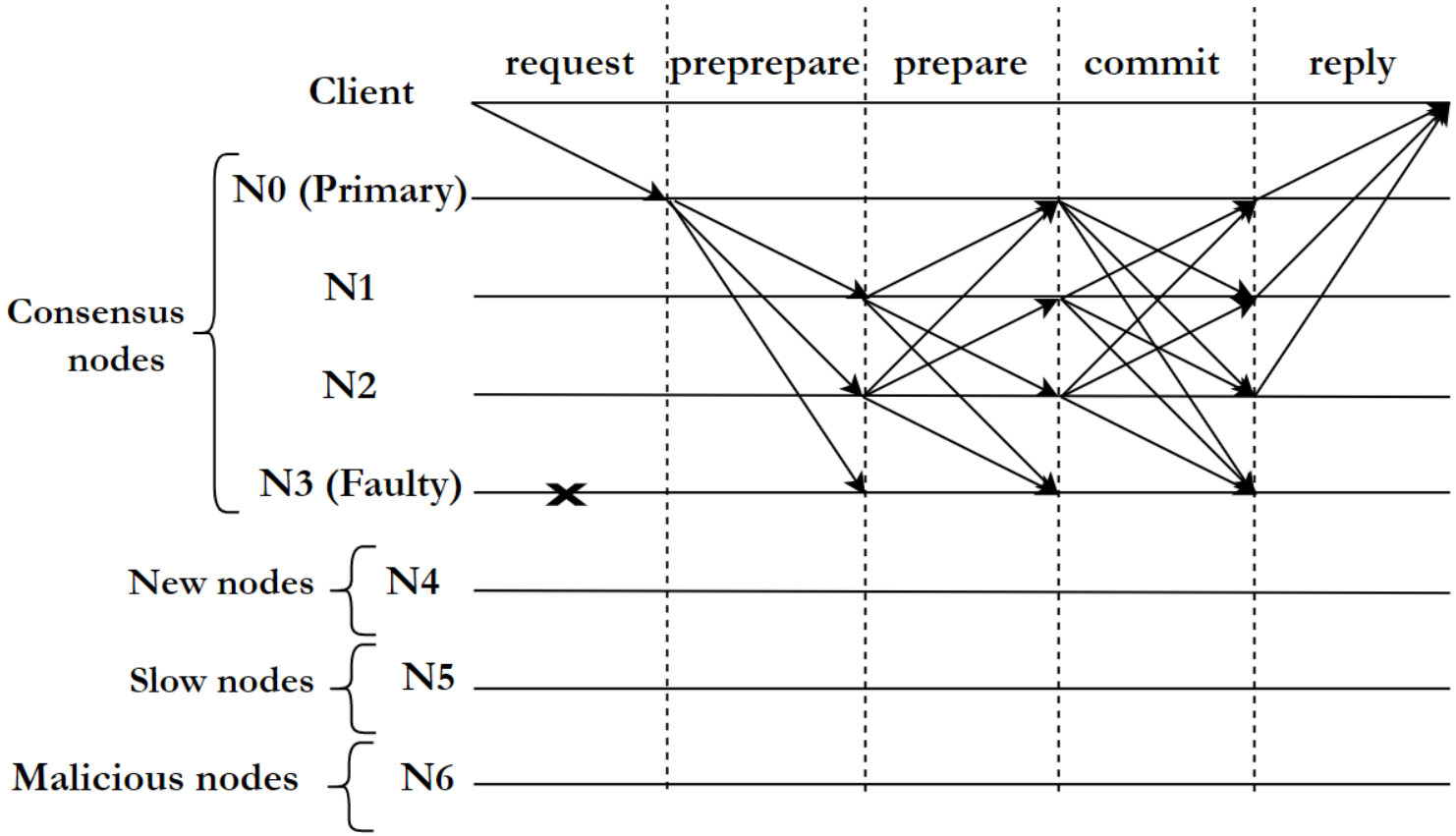
- Réduire le nombre de nœuds participant au consensus
- Réduire la consommation de la bande passante

Contraintes

- ➢ Sécurité
- ➢ « Liveness »

# PBFT Adaptatif

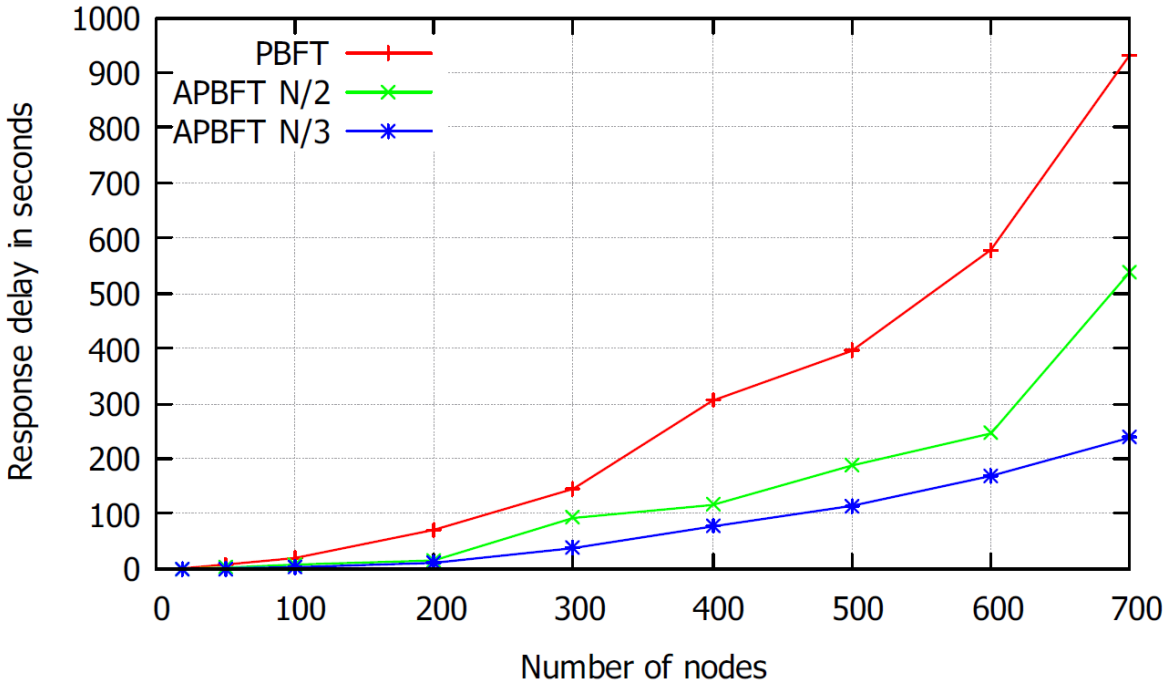
## Principe de la solution

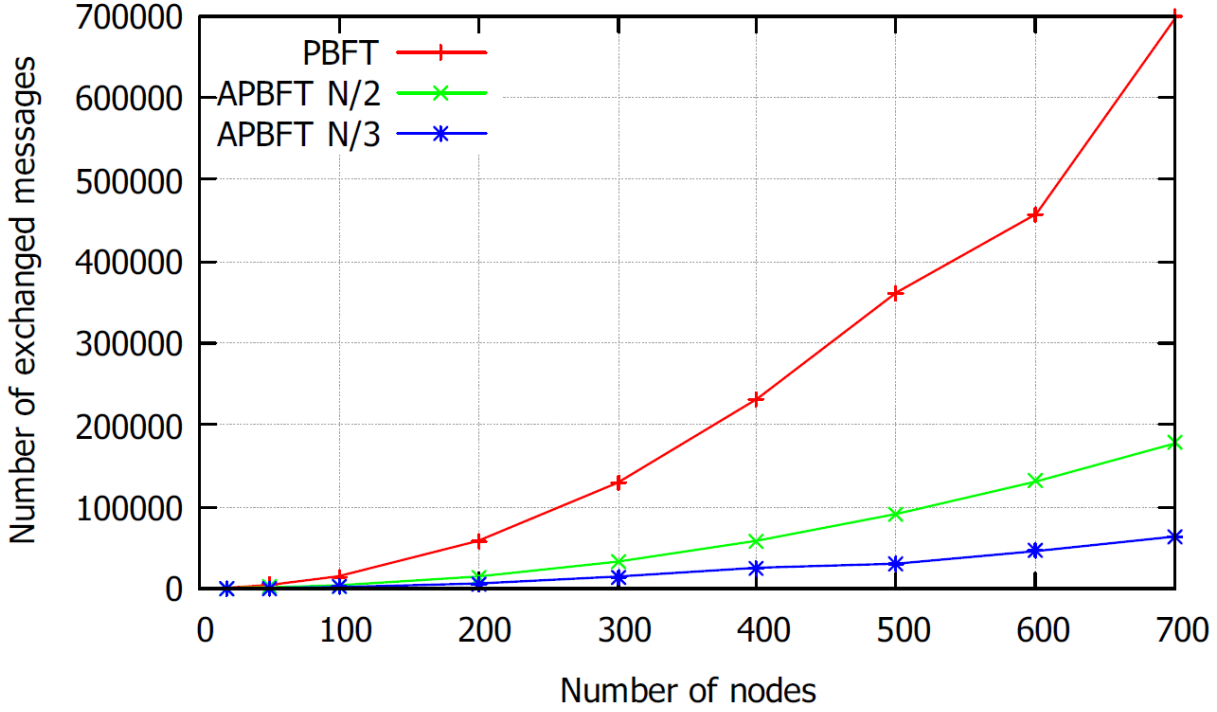



$$\text{Score} = \frac{Availability \,.\, Credibility}{ResponseDelay}$$

# PBFT Adaptatif

## Résultats expérimentaux

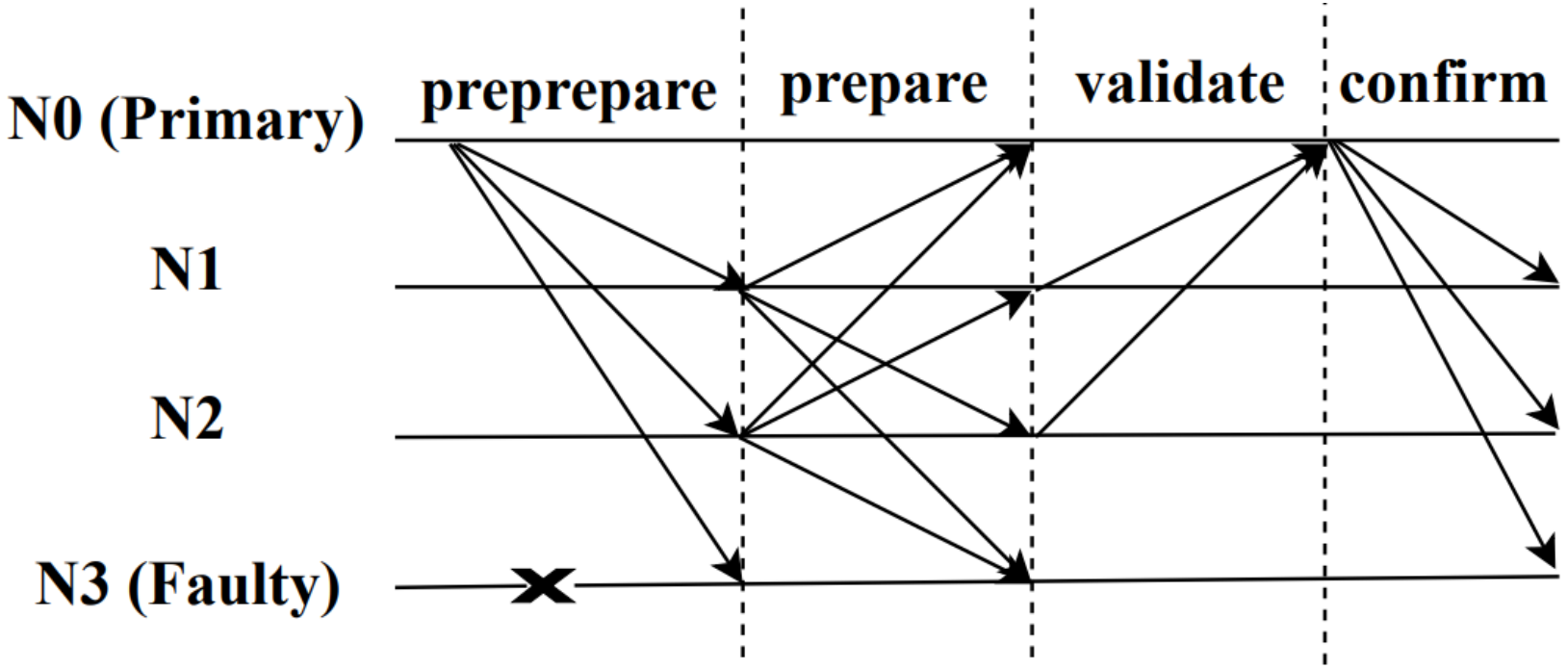



Article soumis dans la conférence IEEE GLOBECOM 2022

# Fast PBFT

## Principe de la solution



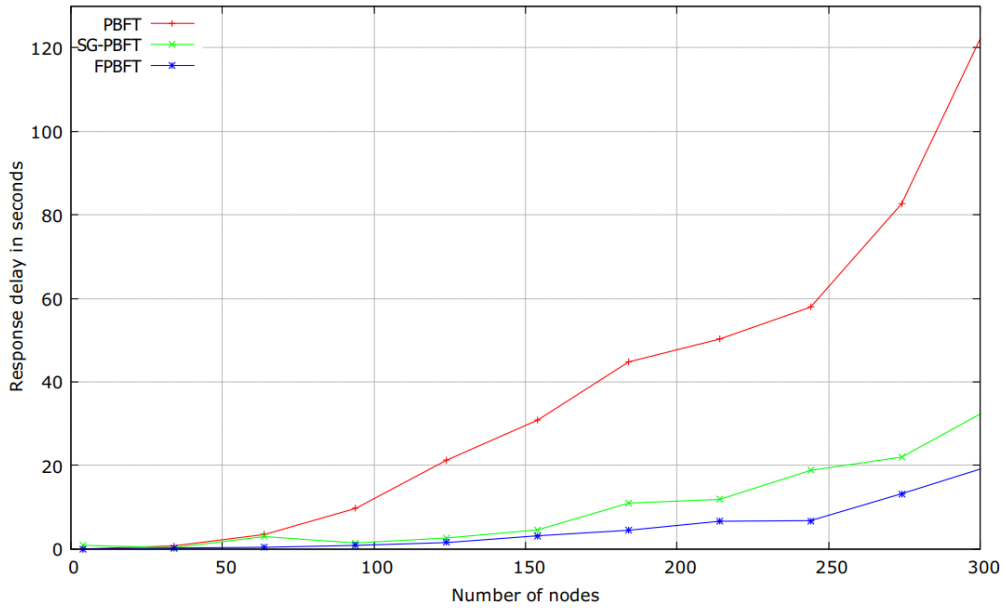

+ Scores

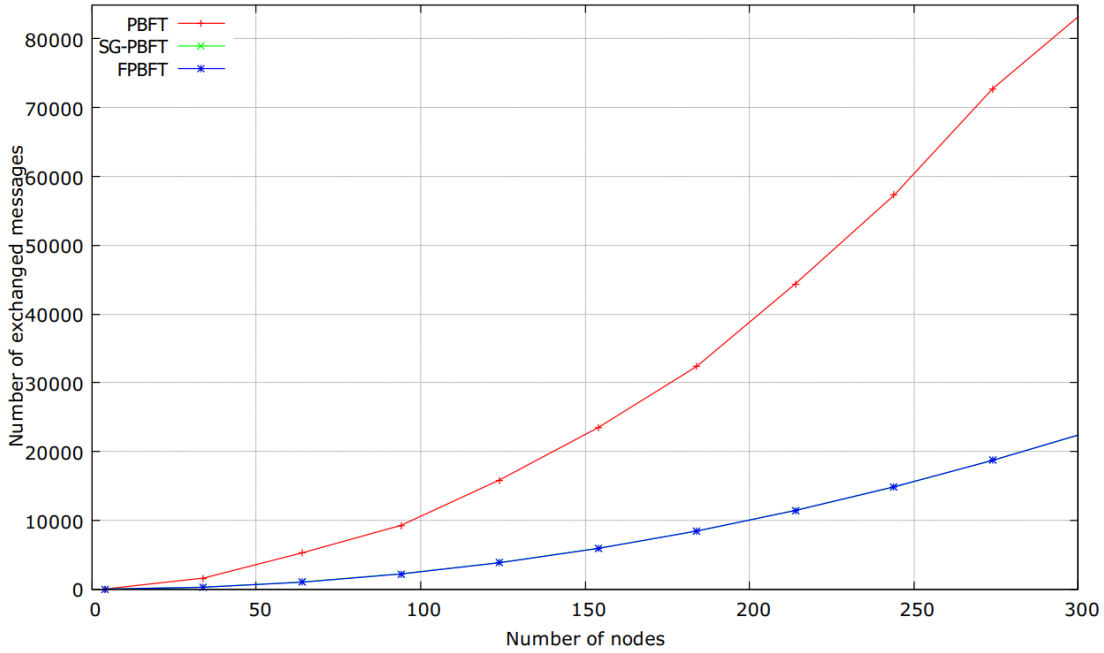
- Protocole adapté à la Blockchain
- Suppression d'une étape de consensus
- Réduction du nombre de messages et du délai de réponse

*Xu, G., Liu, Y., Xing, J., Luo, T., Gu, Y., Liu, S., Vasilakos, A. V. (2021). Sg-pbft: a secure and highly efficient blockchain pbft consensus algorithm for internet of vehicles. arXiv preprint arXiv:2101.01306.*

# Fast PBFT

## Résultats expérimentaux




Article soumis dans la conférence BCCA 2022

# Conclusion et perspectives

- Réduire davantage le nombre de nœuds ainsi que les messages échangés
- Ajustement dynamique du nombre de nœuds participant au consensus
- Intégrer l'IA pour le choix du nombre minimum de nœuds
  (->Apprentissage par renforcement)
- Optimiser le stockage des données dans la blockchain (nombre de transactions par bloc, etc.)
- Appliquer la solution développée (ex. la santé)

# "Toward an Optimal Consensus Protocol for Private Blockchains"


Réalisé par: RIAHI Kenza

Dirigé par: Mr IDOUMGHAR Lhassane

Mr ABOUAISSA Abdelhafid

Encadré par: Mr BRAHMIA Mohamed-El-Amine


## Merci pour votre attention