Simulation et visualisation des consensus blockchain

Travail Personnel Encadré

Master 1 Informatique (IWOCS)

Auteurs

Boussad HAMMOUM & Hocine HAMAMA

Institution

Université le Havre Normandie

Encadrants

Pr. Claude DUVALLET

Pr. Cyrille BERTELLE

M. Maxence LAMBARD

Dr. Aicha FERJANI

Année Universitaire

2025-2026

Introduction et problématique

Définition de la blockchain

La **blockchain** est une technologie de stockage **décentralisée** transparente, sécurisée fonctionnant sans organe central de contrôle. Elle constitue un **registre distribué** dont les informations sont vérifiées et groupées à intervalles réguliers en blocs formant une chaîne.

Complexité des consensus

Les **blockchains** reposent sur des protocoles de **consensus complexes** qui demeurent souvent **abstraits** et difficiles à appréhender pour les non-experts.

Accord décentralisé

La validation nécessite un accord global sur l'état du **registre** au sein d'une **blockchain**, sans autorité centrale de contrôle.

Problématique centrale

Comment « rendre visible l'invisible » en développant un outil permettant de visualiser et de simuler les comportements dynamiques de la blockchain ?

Stefan Balev : présentation du sujet

Objectifs du projet

Pédagogie

Créer un outil interactif permettant de comprendre les concepts abstraits de la blockchain.

Visualisation

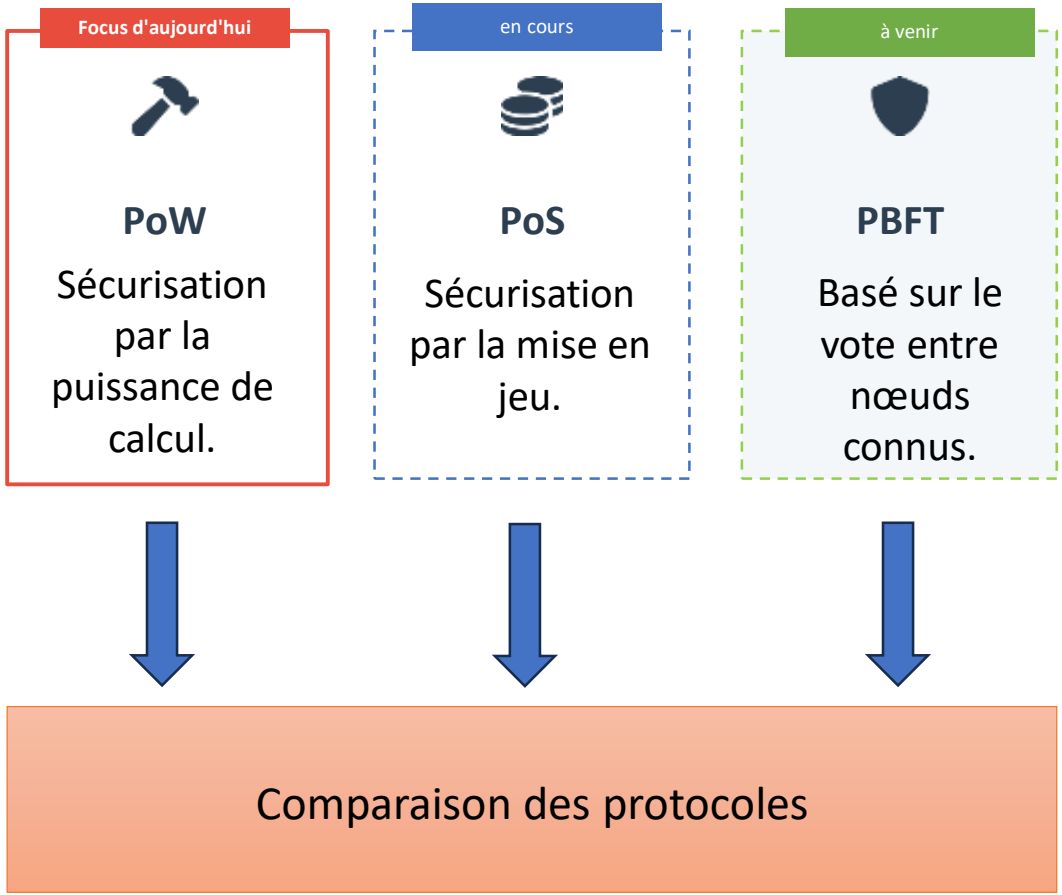
Représenter graphiquement la propagation des blocs et les interactions entre nœuds en temps réel.

Analyse

Étudier les performances et la sécurité du protocole face à différents scénarios d'utilisation.

Figure 1 : Représentation schématique d'une blockchain sécurisée

Protocoles de consensus étudiés



Le consensus proof of work (PoW)

Le Proof of Work est le premier mécanisme de consensus décentralisé, rendu célèbre par Bitcoin. Il repose sur la résolution d'une équation cryptographique complexe nécessitant une puissance de calcul importante pour sécuriser le réseau.

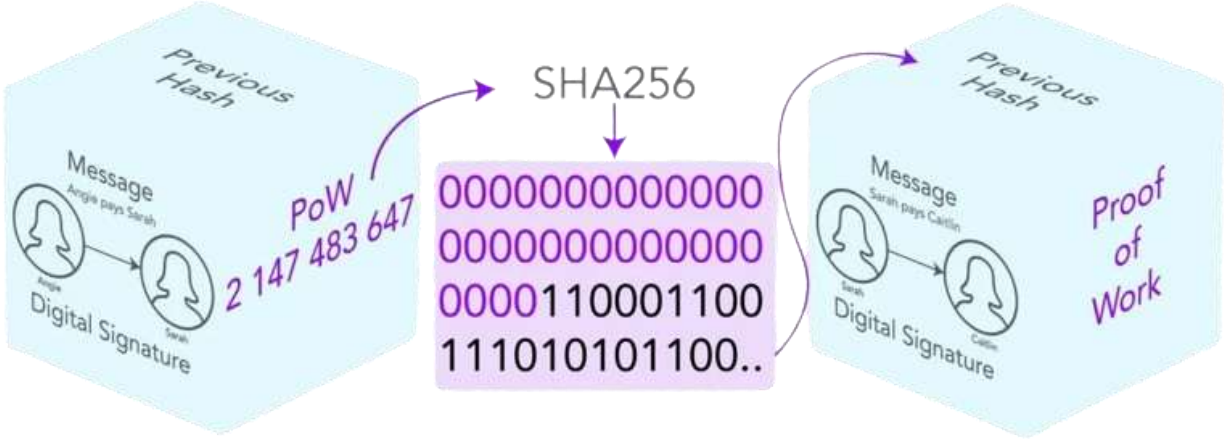


Figure 2 : Mécanisme de validation d'un bloc par la fonction SHA-256

Le consensus proof of stake (PoS)

Le Proof of Stake a été conçu comme une alternative **éco-responsable** au PoW. Il repose sur une sélection basée sur la mise en jeu de **jetons** (stake) plutôt que sur la puissance de calcul , ce qui permet une **consommation énergétique** drastiquement réduite.

Caractéristique	Description
Mécanisme	Sélection basée sur la mise en jeu de jetons (stake) pour valider les transactions.
Ressource	Utilisation d'une garantie économique (Tokens) au lieu du matériel informatique.
Sécurité	Introduit des mécanismes de pénalité pour garantir l'honnêteté des validateurs. Tout comportement malveillant entraîne la perte des jetons mis en jeu.
Exemple	Ethereum 2.0, l'exemple le plus célèbre de blockchain ayant effectué la transition vers ce protocole.

Le PoS garantit l'immutabilité du registre en liant la sécurité du réseau à des garanties économiques

Le Consensus tolerance au panes bizentine (BPFT)

Le PBFT est un algorithme conçu pour les blockchains privées. Il repose sur un système de vote par étapes garantissant une validation instantanée et définitive, sans risque de fork.

Caractéristique	Description
Mécanisme	Consensus par vote multi-phases nécessitant l'approbation d'une super majorité (2/3 des validateurs).
Ressource	Utilisation intensive de la bande passante réseau (messages) et d'identités vérifiées (nœuds connus) au lieu d'énergie ou de jetons.
Sécurité	Tolérance mathématique aux fautes byzantines. Le réseau reste sécurisé et fonctionnel tant que moins de 1/3 des nœuds sont en panne ou malveillants.
Exemple	Hyperledger Fabric (IBM), utilisé massivement pour les blockchains d'entreprises et industrielles.

Le PBFT garantit l'immutabilité du registre en liant la sécurité du réseau à la preuve mathématique

Méthodologie et outils

Modélisation Multi-Agents

Approche centrée sur les entités individuelles (nœud) et leurs interactions au sein d'un environnement partagé.

- Autonomie : Chaque nœud gère ses propres décisions.
- Émergence : Le comportement global naît des comportements locaux.
- Flexibilité : Facilité d'ajout de nouveaux comportements.

AnyLogic

Logiciel de simulation de pointe permettant de modéliser des systèmes complexes via plusieurs paradigmes.

- Environnement de développement basé sur Java.
- Bibliothèques riches pour la visualisation 2D/3D.
- Capacités d'exportation vers des interfaces web.

Architecture de la simulation

Agent Main

Le chef d'orchestre de la simulation

- Initialisation de la population de nœuds
- Gestion des paramètres globaux (latence, difficulté)
- Collecte des statistiques en temps réel

Agent Nœud

Participant actif du réseau blockchain

- Processus de minage et validation des blocs
- Maintenance de la copie locale du registre
- Gestion des forks et adoption de la chaîne la plus longue

Agent Messager

Entité dédiée à la propagation de l'information

- Représentation visuelle du transit des données
- Simulation des délais de transmission réseau
- Lien physique entre les nœuds de la topologie P2P

Règles du consensus PoW simulé

Minage Cryptographique

Chaque nœud tente de résoudre une équation en incrémentant un nonce jusqu'à ce que le hash du bloc respecte la difficulté cible (nombre de zéros en tête).

Propagation

Dès qu'un bloc valide est trouvé, il est immédiatement diffusé aux voisins. Les nœuds vérifient la validité du hash avant de l'intégrer dans leur chaine et de le relayer.

Règle d'Or du Consensus

En cas de conflit (fork), les nœuds adoptent systématiquement la chaîne la plus longue (ayant la plus grande quantité de travail cumulée).

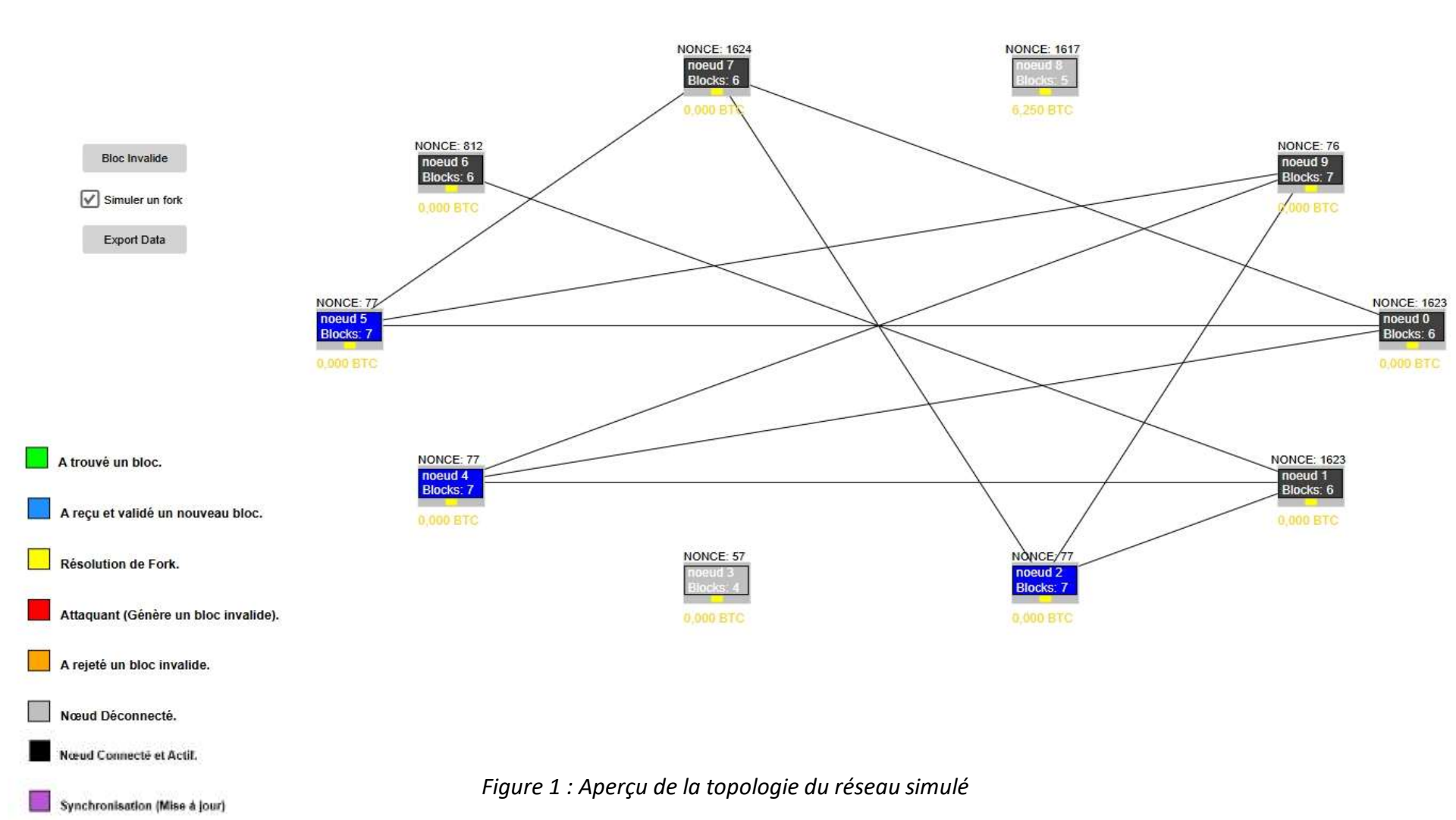


Figure 1 : Aperçu de la topologie du réseau simulé

Paramètres et scénarios

Taille du Réseau

Ajustement du nombre de nœuds actifs pour observer la scalabilité du consensus.

Difficulté de Minage

Ajuster dynamiquement la difficulté du minage pour compenser les variations de puissance de calcul du réseau. Ce mécanisme garantit un intervalle de temps stable entre chaque 2 blocs.

Latence Réseau

Simulation des délais de propagation pour analyser la fréquence de création de forks.

Topologie P2P

Configuration du nombre de voisins par nœud et de la structure des connexions.

Analyse Dynamique

La flexibilité du simulateur permet de recréer des conditions réseau dégradées, facilitant l'étude de la convergence du registre et de la résilience du protocole face aux délais de communication.

Résultats de la Simulation

Convergence du Réseau

La simulation démontre une stabilisation rapide du consensus PoW. Malgré l'apparition ponctuelle de forks lors de latences élevées, le réseau converge systématiquement vers une chaîne unique.

Résilience du Protocole

L'analyse dynamique confirme la robustesse du Proof of Work face aux conditions réseau dégradées. La difficulté ajustable permet de maintenir un temps de bloc stable quel que soit la puissance de calcul.

Conclusion et ressources

Le simulateur remplit son rôle pédagogique en rendant tangibles les mécanismes abstraits du consensus Proof of Work.

Une base solide a été établie pour l'étude approfondie de la sécurité et de la résilience des systèmes ainsi que l'étude de protocole de la mise en jeu (PoS) ou le vote (PBFT). C'est notre feuille de route pour juin.

Documentation et Simulation en Ligne

blockchaintpe.netlify.app

Merci de votre attention