

Proof of Work vs Proof of Stake : la bataille mathématique derrière le Bitcoin

Cryptographie, fonctions de hachage et mécanismes de consensus distribués

Pinel Baudelaire T. DAHOU

Data Scientist & IA | Ingénieur en Travaux Statistiques
Master Statistiques Appliquées aux Sciences du Vivant
tpineladahoui@gmail.com | github.com/Baudelaire12

CIPMA-CHAIRE UNESCO | Bénin

Samedi 15 Mars 2025

Série LinkedIn STEM au Quotidien — Jour 13/40

Plan de la présentation

- 1 Mise en contexte
- 2 Concepts clés
- 3 Développement mathématique
- 4 Cas pratique
- 5 Conclusion
- 6 Références

La blockchain : une révolution de la confiance numérique

Chiffre clé

En 2024, la capitalisation boursière totale des cryptomonnaies dépassait **2 500 milliards de dollars** (CoinGecko, 2024). Bitcoin consomme plus d'électricité que l'Argentine entière, soit environ **150 TWh/an** — à cause du Proof of Work (Cambridge Centre for Alternative Finance, 2023).

- Satoshi Nakamoto a publié le livre blanc du Bitcoin en **octobre 2008** — au cœur de la crise financière mondiale.
- En Afrique, le Nigeria est le **2^{ème} marché mondial** de Bitcoin peer-to-peer après les États-Unis (Chainalysis, 2023), largement utilisé pour contourner les restrictions de change.
- Ethereum a réduit sa consommation énergétique de **99,95%** en passant du PoW au PoS en septembre 2022 (Ethereum Foundation, 2022).

Question centrale

Quelle est la mathématique qui rend la blockchain inviolable ?

Structure d'un bloc — Anatomie de la blockchain

Un bloc Bitcoin contient :

Champ	Description
Version	Numéro de version du protocole
hash_prev	Empreinte cryptographique du bloc précédent
merkle_root	Résumé cryptographique de toutes les transactions
Timestamp	Horodatage UNIX du bloc
Bits (target)	Difficulté de minage actuelle
Nonce	Nombre entier à trouver (le puzzle)
Transactions	Liste des transactions incluses

Propriété fondamentale

Chaque bloc contient l'empreinte du précédent. Modifier un bloc passé invalide toute la chaîne qui suit — d'où l'immuabilité.

Fonction de hachage SHA-256 — Le cœur de Bitcoin

Propriétés d'une fonction de hachage cryptographique H :

- **Déterminisme** : $H(m) = H(m)$ toujours
- **Avalanche** : changer 1 bit de m modifie $\sim 50\%$ des bits de $H(m)$
- **Résistance aux collisions** : difficile de trouver $m \neq m'$ tel que $H(m) = H(m')$
- **Sens unique** : connaître $H(m)$ ne permet pas de retrouver m

Proof of Work (PoW) — Le puzzle de minage :

Trouver $\text{nonce} \in \mathbb{N}$ tel que $H(\text{header} \parallel \text{nonce}) < \text{target}$

Probabilité de succès par tentative :

$$p = \frac{\text{target}}{2^{256}}$$

En 2024, les mineurs effectuent collectivement $\sim 600 \times 10^{18}$ tentatives par seconde (600 EH/s).

Proof of Stake vs Proof of Work — Comparaison formelle

Proof of Work (PoW) :

$$P(\text{valider un bloc}) \propto \frac{\text{Puissance de calcul du mineur}}{\text{Puissance totale du réseau}}$$

Proof of Stake (PoS) :

$$P(\text{valider un bloc}) \propto \frac{\text{Mise du validateur (stake)}}{\text{Mise totale du réseau}}$$

Critère	PoW (Bitcoin)	PoS (Ethereum)
Consommation énergie	~150 TWh/an	< 0.01 TWh/an
Sécurité	Attaque 51% coûteuse	Slashing économique
Décentralisation	Mineurs spécialisés	Validateurs accessibles
Finalité	Probabiliste	Cryptoéconomique

Arbre de Merkle — Intégrité des transactions

Arbre de Merkle (Merkle, 1987) : structure de données pour vérifier efficacement l'intégrité d'un ensemble de transactions.

$$h_{AB} = H(H(T_A) \| H(T_B)), \quad h_{CD} = H(H(T_C) \| H(T_D))$$

$$\text{merkle_root} = H(h_{AB} \| h_{CD})$$

Propriété clé : Pour vérifier qu'une transaction T_A est incluse dans un bloc, il suffit de connaître $H(T_A)$, $H(T_B)$, et h_{CD} — soit $O(\log n)$ opérations pour n transactions.

Application africaine : transferts de fonds (remittances)

Le Nigeria reçoit **~21 milliards \$** de remittances/an (Banque Mondiale, 2023). Les frais traditionnels (Western Union, MoneyGram) atteignent 7–9%. Les solutions blockchain (Stellar, Ripple) les réduisent à **< 1%**.

Synthèse

La blockchain est une construction mathématique élégante fusionnant cryptographie (SHA-256, signatures ECDSA), théorie des jeux (incitations économiques) et informatique distribuée (consensus byzantin). Le passage au Proof of Stake constitue une avancée majeure pour la durabilité environnementale.

Perspectives africaines :

- MNBC (Monnaies Numériques de Banques Centrales) : l'e-Naira nigérian (2021) et l'e-Cedi ghanéen
- Blockchain pour les registres fonciers en Afrique (sécurisation des titres de propriété)
- Finance décentralisée (DeFi) : accès aux services financiers sans intermédiaire bancaire
- Traçabilité des aides humanitaires et des ressources minières (or, cobalt)

« La confiance est la ressource la plus rare en économie. La cryptographie permet de la rendre mathématiquement vérifiable. »

— Adapté de Satoshi Nakamoto, Bitcoin White Paper, 2008

Références bibliographiques

-  Nakamoto, S. (2008). *Bitcoin : A Peer-to-Peer Electronic Cash System*. bitcoin.org.
-  Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform*. Ethereum White Paper.
-  Merkle, R. C. (1987). A digital signature based on a conventional encryption function. *CRYPTO 1987*, LNCS 293, 369–378.
-  Cambridge Centre for Alternative Finance. (2023). *Cambridge Bitcoin Electricity Consumption Index*. University of Cambridge.
-  Chainalysis. (2023). *The 2023 Geography of Cryptocurrency Report*. Chainalysis Inc.
-  World Bank. (2023). *Remittance Prices Worldwide*. World Bank Group.

Merci pour votre attention

Pinel Baudelaire T. DAHOUI

Data Scientist & IA | CIPMA-CHAIRE UNESCO, Bénin

`tpineldahoui@gmail.com | github.com/Baudelaire12`

LinkedIn : @Pinel Baudelaire DAHOUI

Série STEM au Quotidien — 40 jours pour comprendre le monde par les données