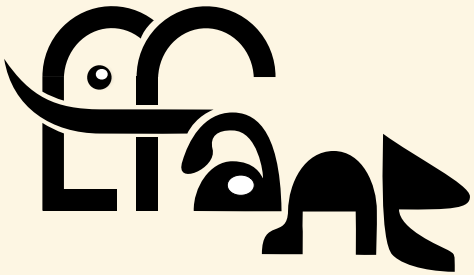
# Les enjeux de la blockchain écologique

2022/11/22 — French Tech Day, Bordeaux

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest




# Équipe Inria LFANT

- Théorie algorithmique des nombres + Logiciels
- Pari/GP: algorithmique des nombres, courbes elliptiques, formes modulaires, fonctions L…
  `https://pari.math.u-bordeaux.fr/`
- ARB: calcul rigoureux à très haute précision (arithmétrique d'intervalle)
  `https://arblib.org/`

- Outils mathématiques ⇒ Outils cryptographiques ⇒ Protocoles (vote électronique, cryptomonnaies…)

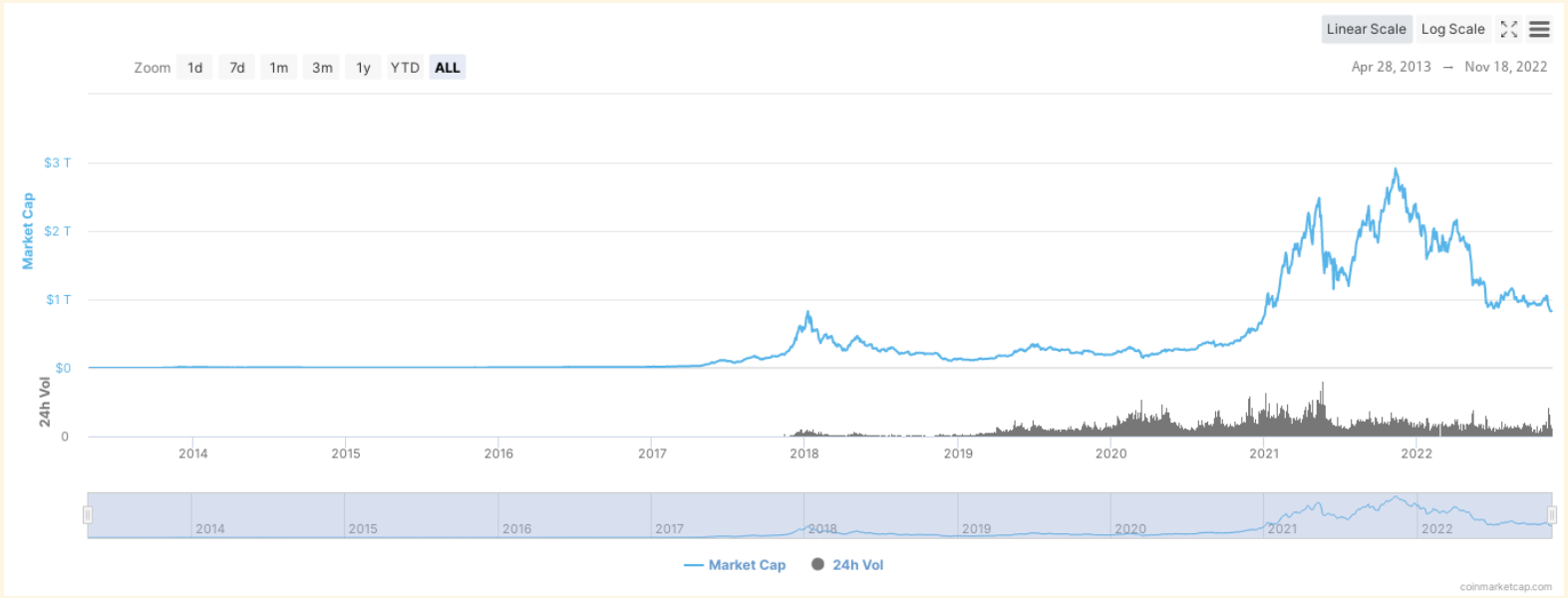
- Cryptographie moderne (multipartite, fonctionnelle, homomorphe, VDF…)
- Cryptographie post-quantique.

# Blockchain

- Base de donnée + Machine virtuelle distribuées
- Bitcoin: Satoshi Nakamoto, 2008 – 2009
- Ethereum: Vitalik Buterin, 2013 – 2015, Ethereum 2.0: 15 Septembre 2022
- NFTs, Smart contracts, Defi…
- Historique publique

- Moins efficace qu'un système centralisé
- Mais plus sûr?

# Blockchain




Capitalisation des cryptomonnaies
Source: `coinmarketcap.com`

# Bitcoin: quelques chiffres

- Capitalisation: 100G$ – 1000G$.
- Taille du Registre: 400GB
- Noeuds: 50000

- 1 block toutes les 10 minutes, taille 1MB
- Bande passante: 1.75kB/s
- 1 block = 2000 transactions: 3 transactions/s
  CB: 400 tps, Visa: 1700 tps (max à 50000 tps), SWIFT: 400 tps
- Finalité: 6 blocks ⇒ 1h

# Bitcoin: consommation énergétique

- 50 à 150 TWh par an (source: Université de Cambridge)
- Electricité française: 470TWh par an

- 5000MW à 15000MW de puissance (1 EPR=1650MW)
- Whinstone Inc. (Texas): 700MW (gaz)
- 65 Mtons de $CO_2$ éq/an (= 6 millions de Français)

- Efficacité: 1 à 3 kWh par Octet (10 à 30L de thé)
  Gigabit ethernet: 500mW, donc 1pWh par Octet (15 ordres de magnitude)

# Preuve de ressource

- Problème du consensus
- Consensus majoritaire? ⇒ attaques sybils
- Validateur: sélectionné proportionnellement à une ressource:
  - Proof of Work (Bitcoin, Ethereum, Dogecoin),
  - Proof of Stake (Ethereum 2.0, Algorand, Cardano, Tezos),
  - Proof of History (Solana),
  - Proof of Space/Spacetime (Chia, Filecoin)

- Aléatoire (non predictable, non biaisé)
- Vérifiable (même à posteriori)

# Preuve de travail (2009)

- Minage: résoudre un problème mathématique (trouver un haché avec un certain nombre de zéro) = "rechercher une aiguille dans une botte de foin"

☺ Aléatoire

☺ Vérifiable

☹ Forks, Finalité

☹ Latence

☹ Resource = énergie

# Preuve d'enjeux (2012)

- A chaque block: élection d'un leader parmi les validateurs
- Besoin d'un aléa fiable et vérifiable
- Haché du block précédent? Manipulable!
- Loterie, NYSE? Pas assez efficace!
- Solution via des outils cryptographiques (RandAO, VRF, VDF): moins de ressources, plus efficace

☹ Plus technique à mettre en oeuvre

☺ 100 à 1000 tps (jusqu'à 10000/100000 tps avec du layer 2).

☺ 1 block toutes les 4 à 30 secondes

☺ Finalité immédiate

☺ Efficacité énergétique: Ethereum PoW: 78 TWh/an, Ethereum 2.0: 0.0026 TWh/an (facteur 30000)

# VRF: verifiable random function (1999)

- VRF = "Fonction de hachage à clé publique"
- La clé secrète permet de calculer la fonction
- La clé publique de la vérifier

- Pour l'élection chaque validateur publie son aléa (personne d'autre ne peut le calculer!)
- Tout le monde peut le vérifier
- Exemple: AlgoRand

# ZK-Snark: Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (1988, 2012)

- Snark: Prouver (rapidement!) qu'un calcul a été effectué correctement
- ZK: Sans rien révéler à part l'entrée et la sortie.
- Plus général mais moins efficaces que des VRFs

Exemples:

- ZCash (validité des transactions)
- Filecoin (preuve de stockage)
- Layer 2 blockchains (ZK-Rollup)…

# VDF: verifiable delayed function (2018)

- VDF: lentes à calculer, rapides à vérifier
- Non parallélisable! Différence clé avec la preuve de travail.
- Utilisations: VDF du dernier block, VRFs puis VDF

- Objets cryptographique nouveaux, durs à construire!

1. Itérer une fonction de hachage un grand nombre de fois + SNARK
   (Solana: révéler des hachés intermédiaires, vérification parallèle)
2. Exponentiation dans un groupe d'ordre inconnu
   - entier RSA, demande un trusted setup
   - Variante: groupe de classe d'un ordre quadratique imaginaire
3. Isogénies + couplages de courbes elliptiques

# Conclusion

- Bitcoin: révolutionnaire en 2008
- Techniquement obsolète actuellement, désastre écologique
- Meilleure efficacité via de nouveaux outils cryptographiques puissants
- Basés sur des objects mathématiques (courbes elliptiques, couplages, groupe de classe d'un ordre quadratique imaginaire…)

- La hype d'une blockchain n'est pas forcément corrélée avec son niveau technologique (Valuation, Écosystème importants)