Pierre Michiels
hiveange

Algorithme de consensus Proof of Work

Historique

- présenté par Cynthia Dwork et Moni Naor 1993
- formalisé en 1999 par Markus Jakobsson et Ari Juels

Mise en contexte

Hashcash®

Comment fonctionne l’algorithme?

Chaine de caractère: “Bonjour, monde!”
Preuve de travail: trouver un hash qui débute par quatre ’0’

- "Bonjour, monde!**0**" ⇒
  a9efd73638806846d0495fb92e2deba6e2e1ad5bc453e28e5fdc1334c97c21a8
- "Bonjour, monde!**1**" ⇒
  f767b47fd98fab25d08bd155c42708b434ac86bfa8d8b95b1457146e86b728e5

…

- "Bonjour, monde!**33680**" ⇒
  0000abebe9c6554c85176b8e9f9f3f4ed9b7e8dc856a7b5cb9177bf7b22e1871

adresse courriel du destinataire

X-Hashcash: **1:20:**060408**:**destinataire@example.org**::**1QTjaYd7niiQA/sc:ePa

Date

nombre incrémenté

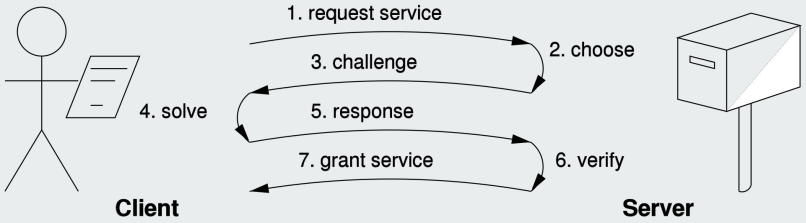
2^{20} **calculs de hash** => une **seconde de calcul** environ sur un processeur à **1 GHz**

Bitcoin

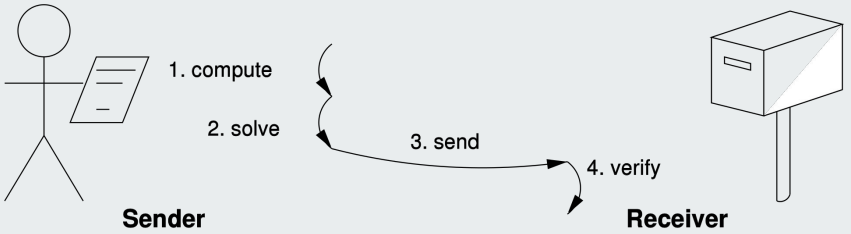
- Stocké dans un portefeuille numérique
- Est basé sur un réseau décentralisé d'ordinateurs qui possède des nœuds répartis
- Calculs coûteux en temps et en énergie afin de chiffrer l'ensemble des transactions d'un bloc
- Nécessite un nombre considérable d’essais et d’erreurs
- Temps d’extraction soit en moyenne de 10 minutes par bloc
- La chaîne la plus longue est gardée

Autres variantes

Protocoles de défi-réponse



Protocoles de vérification de solution



Avantages

- Résilient aux menaces communes présentes sur le Web
- Garantit l'intégrité des transactions sans la nécessité d'un tiers de confiance

Inconvénients

- Consommation excessive d’électricité et temps de calcul

Merci pour votre écoute,