Bitcoin

Monnaie virtuelle

+

Système financier électronique parallèle, sans intermédiaire et décentralisé utilisant la technologie P2P

Le système financier actuel

- Acheteurs,
- Vendeurs,
- Intermédiaires (banques),
- Banques centrales (création/manipulation? de la quantité de monnaie),
- Mis à part le cash, les règlements passent toujours par l’intermédiaire (banque).

Le système proposé par Bitcoin

- Acheteurs,
- Vendeurs,
- Règlement direct: pas d’intermédiaires (banque ou autre),
- Création contrôlée et connue/prévisible de la monnaie.

Caractéristiques de Bitcoin

- Pas d'autorité centrale (algorithme décentralisé, réseau P2P),
- Pas d'intermédiaire(s),
- Pas de spéculation « interne »,
- (Quasiment-)pas de « frais bancaires »,
- Pas de notion de frontière (Internet),
- Offre (quantité de monnaie) quasi-constante et augmentation finement prévisible,
- Demande imprévisible ; impacte la valeur de la monnaie,
- Création de la monnaie très complexe (business dédiés) => quantité de monnaie contrôlée et prévisible,
- L'avancée technologique est systématiquement compensée par une augmentation de la complexité de création de la monnaie (pas d'« abus » technologique),
- Haute liquidité: transaction instantanée directement de l'acheteur au vendeur,
- Haute divisibilité (jusqu'à huit décimales – mais attention coût transaction pour le réseau: 1/10 cent),
- Irréversibilité des transactions (mais service dispo),
- Transaction plus anonyme que Visa/Mastercard (mais moins que le cash).

Rappel: la technologie P2P

- Technologie (ni ange, ni démon)
- Utilisée pour que différents ordinateurs reliés au réseau P2P puissent partager des ressources de manière contrôlée: temps CPU, mémoire, espace disque, fichiers, résultats de recherche…
- Exemples: SETI@Home (l'ancêtre du P2P), BOINC, Emule, BitTorrent…

Le système proposé par Bitcoin

- Problème: comment éviter les doubles-dépenses?

Bitcoin: résoudre le pb de double-dépense

- Ou comment historiser de manière fiable les transactions (relation d'ordre):
  - Solution: chiffrer les transactions de telle manière que seule la puissance CPU du plus grand pool puisse rechiffrer la transaction et compromettre la relation d'ordre => irréversibilité garantie ssi plus grand pool pas honnête.

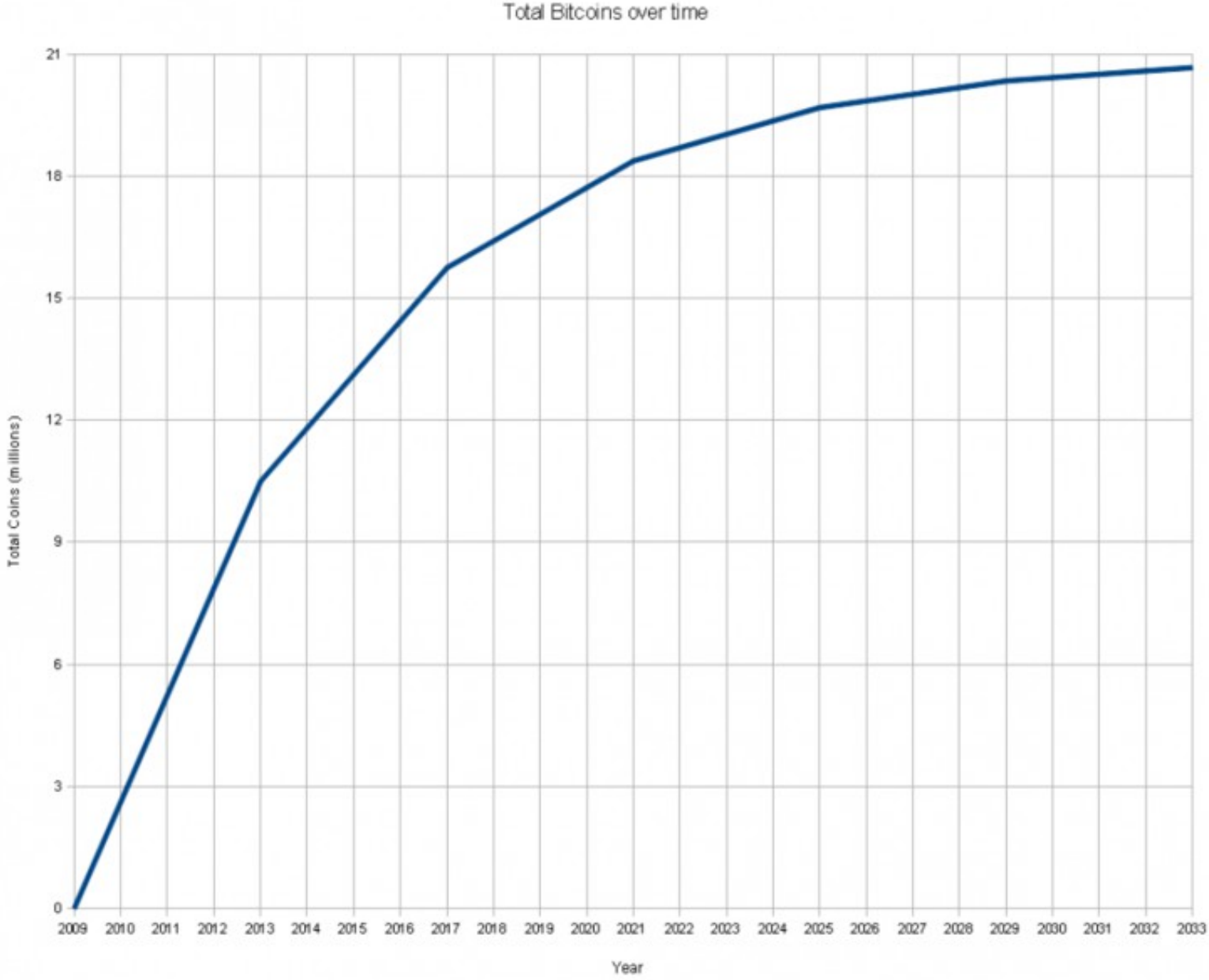
Bitcoin: résumé des étapes

1. les nouvelles transactions sont publiées à tous les nœuds (ou clients, PC),
2. chaque nœud rassemble les transactions dans un bloc et commence à résoudre la « preuve de travail »,
3. lorsqu'un nœud résout la « preuve » il publie le bloc et son « hash »,
4. les nœuds qui reçoivent le bloc vérifient que les transactions présentes sont valides et pas encore dépensées,
5. si OK alors ils commencent à construire le bloc suivant à partir des transactions suivantes et du « hash » du bloc précédent.

Quelques chiffres

- 8 juin 2011 à 17h38: 6 470 200 BTC en circulation,
- Quantité maximale de monnaie (codée): 21 Millions de BTC (vers 2033),
- Sur les huit derniers mois, la valeur des BTC a été multipliée par 300.

-
-
-


Total Bitcoins over time
Total Coins (millions)
0
3
6
9
12
15
18
21
2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033
Year

a

Perspectives à court/moy. terme

- Adoption en cours du paiement par la monnaie BTC => augmentation de la demande => augmentation de la valeur des BTC,
- Avantage incitatif pour les *early adopters*, compense le risque,
- Concurrence d'une autre crypto-monnaie,
- Système fortement informatisé => exposition aux risques et faiblesses de type hacking, virus, cheval de Troie…
- Polarisation probable des acteurs de la « vieille » finance: adoption vs. rejet,
- Rejet fort probable par les bénéficiaires de l'ancien système, dont les gouvernements (perte du contrôle suite à la perte de la centralisation, pas de taxes, pas de déclaration…etc),
- Un changement de paradigme impliquerait une crise semblable à celle du secteur du disque, mais peut-être plus profonde.

Le mythe de Satoshi Nakamoto, le Keyser Soze de Bitcoin…