

Samedi 14 Janvier 2023



LOCKCHAINS

Comment ça marche ?

DÉ CODE
TA RICHESSE
AVEC LA BLOCKCHAIN
CARDANO



Malik Koné (PhD)

Sommaire

1. Introduction

- Notions de départ
- Les types d'utilisateurs des Blockchain

2. Bitcoin : Blockchain de 1^{re} génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Quel est le problème résolu
- Les limites

3. Perspectives

- Perspectives

Notions de départ

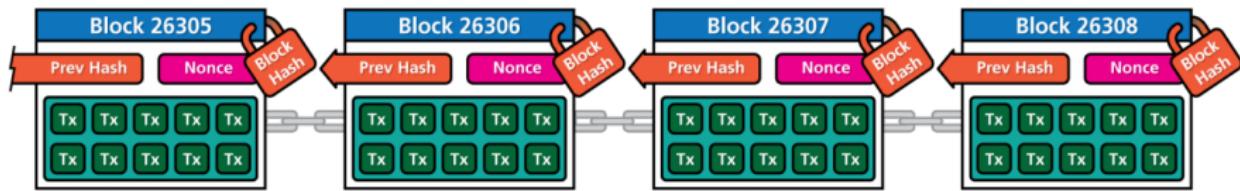


Illustration by CryptoGraphics.info

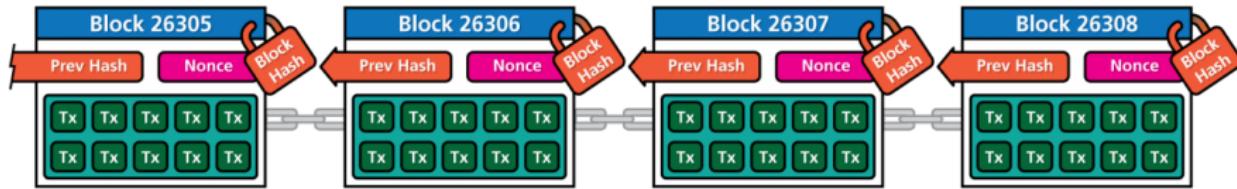
Blockchain

- ▶ Décentralisation
- ▶ Consensus
- ▶ Cryptographie
- ▶ Applications décentralisées (dApp)

Cryptoéconomie

- ▶ Tokens ou jetons
- ▶ Marchés financiers
- ▶ Porte-monnaie de crypto (Yoroi-wallet)

Notions de départ



Blockchain

- ▶ Décentralisation
- ▶ Consensus
- ▶ Cryptographie
- ▶ Applications décentralisées (dApp)

Cryptoéconomie

- ▶ Tokens ou jetons
- ▶ Marchés financiers
- ▶ Porte-monnaie de crypto (Yoroi-wallet)

Sommaire

1. Introduction

- Notions de départ
- **Les types d'utilisateurs des Blockchain**

2. Bitcoin : Blockchain de 1^{re} génération

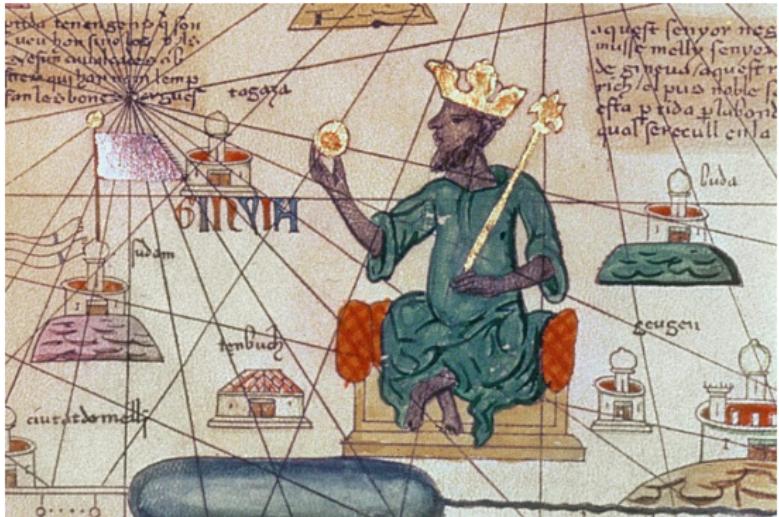
- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Quel est le problème résolu
- Les limites

3. Perspectives

- Perspectives

Les rôles sur la blockchain

- ▶ Les empereurs
- ▶ les élus
- ▶ les mineurs
- ▶ les utilisateurs



Les rôles sur la blockchain

- ▶ Les empereurs
- ▶ les élus
- ▶ les mineurs
- ▶ les utilisateurs



Les rôles sur la blockchain

- ▶ Les empereurs
- ▶ les élus
- ▶ **les mineurs**
- ▶ les utilisateurs



Les rôles sur la blockchain

- ▶ Les empereurs
- ▶ les élus
- ▶ les mineurs
- ▶ les utilisateurs



Sommaire

1. Introduction

- Notions de départ
- Les types d'utilisateurs des Blockchain

2. Bitcoin : Blockchain de 1^{re} génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Quel est le problème résolu
- Les limites

3. Perspectives

- Perspectives

Toute action engendre une réaction (3^e loi de Newton)

La Naissance du Bitcoin

Cyber-Anarchisme

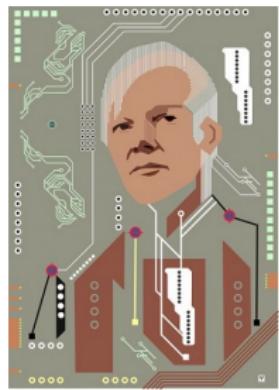
From : Satoshi Nakamoto satoshi@vistomail.com

Subject : Bitcoin P2P e-cash paper

Newsgroups : gmane.comp.encryption.general

Date : Friday 31st October 2008 18 :10 :00 UTC

I've been working on a new electronic cash system
that's fully peer-to-peer, with no trusted third party.



La Naissance du Bitcoin

Cypherpunk (Hal Finney)



[What is Cryonics?](#) [Membership](#) [About](#) [Blog](#) [Library](#) [Contact](#) [🔍](#)



Sommaire

1. Introduction

- Notions de départ
- Les types d'utilisateurs des Blockchain

2. Bitcoin : Blockchain de 1^{re} génération

- La Naissance du Bitcoin
- **Que vaut la blockchain ?**
- Historique du cours du Bitcoin
- Quel est le problème résolu
- Les limites

3. Perspectives

- Perspectives

Que vaut la blockchain ?



2009

???

SSL/TLS - 1996



HTTP - 1990



TCP/IP - 1974



Ethernet - 1974



Cela dépendra de son utilité

Sommaire

1. Introduction

- Notions de départ
- Les types d'utilisateurs des Blockchain

2. Bitcoin : Blockchain de 1^{re} génération

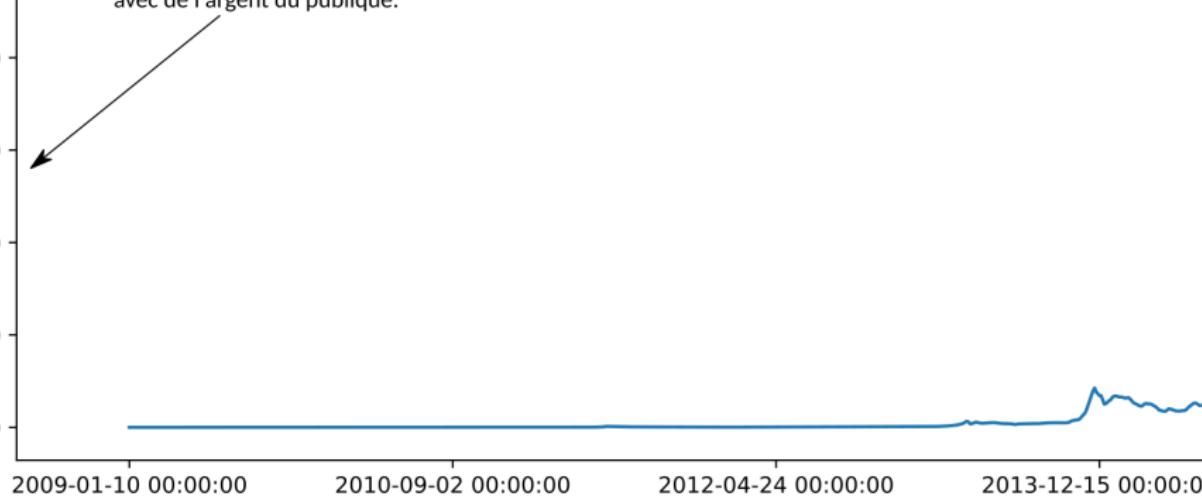
- La Naissance du Bitcoin
- Que vaut la blockchain ?
- **Historique du cours du Bitcoin**
- Quel est le problème résolu
- Les limites

3. Perspectives

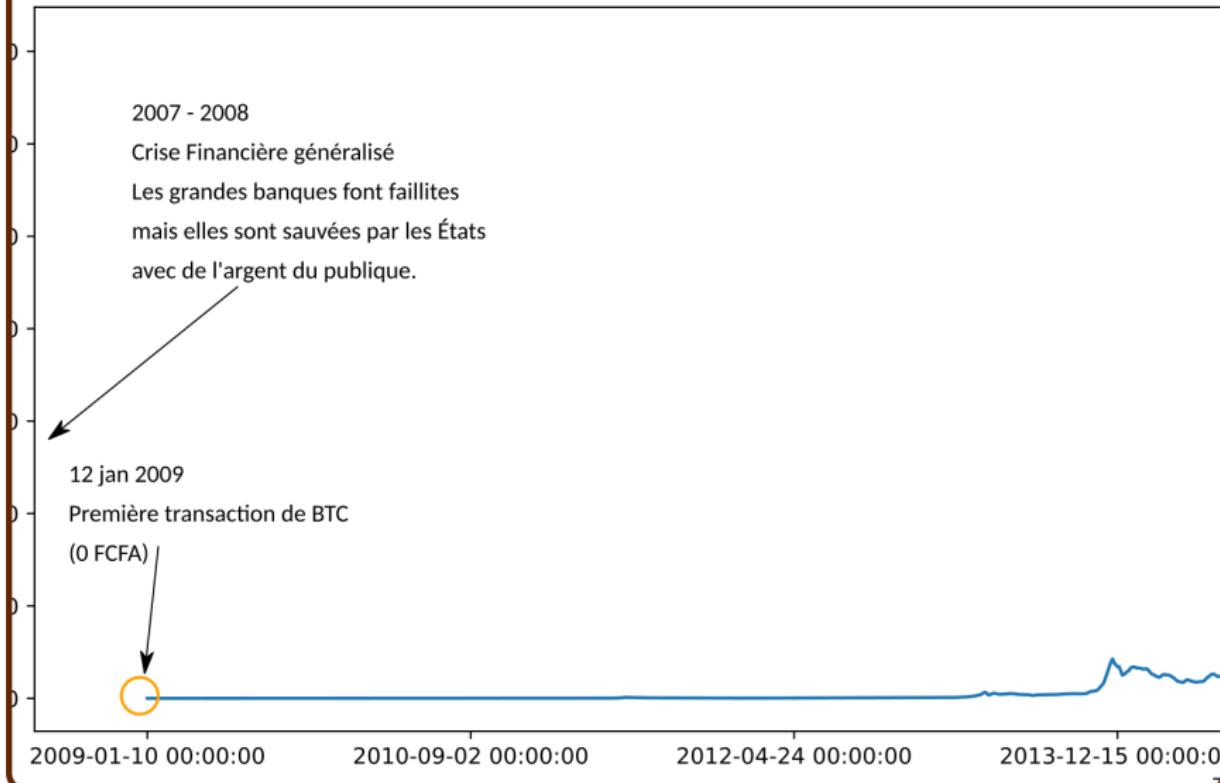
- Perspectives

Les débuts

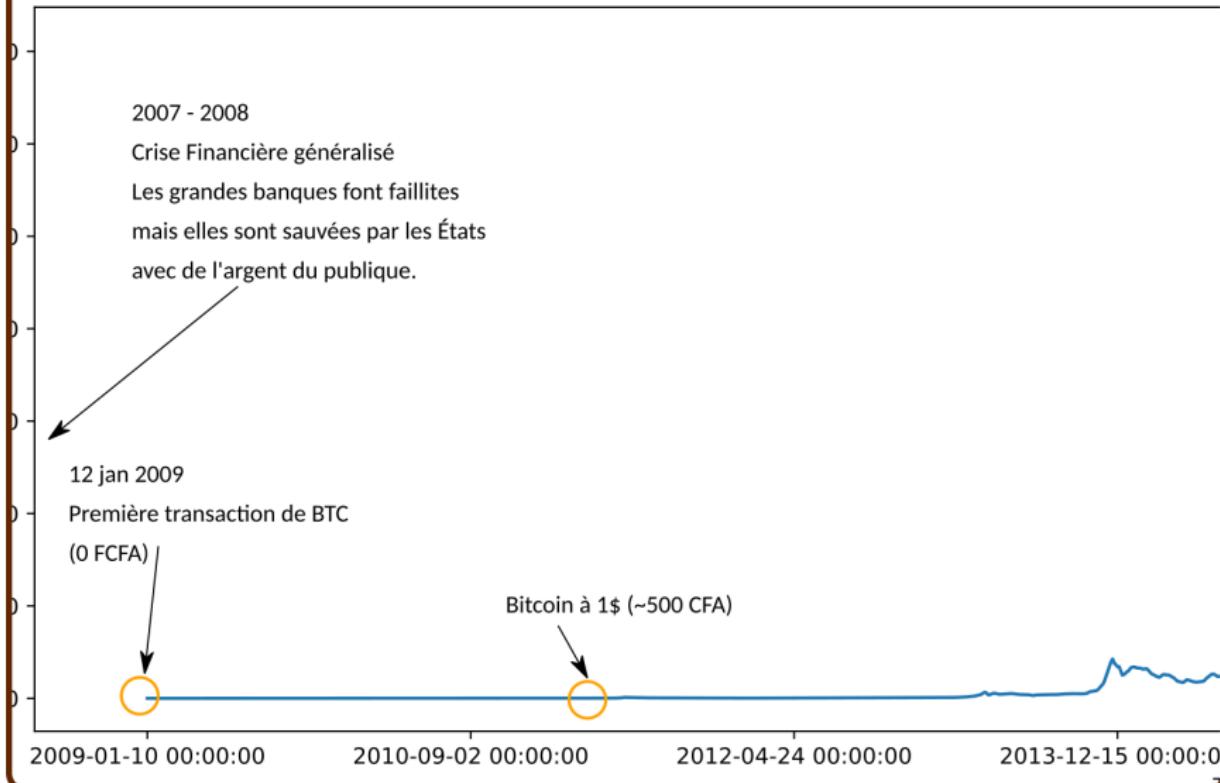
2007 - 2008
Crise Financière généralisé
Les grandes banques font faillites
mais elles sont sauvées par les États
avec de l'argent du public.



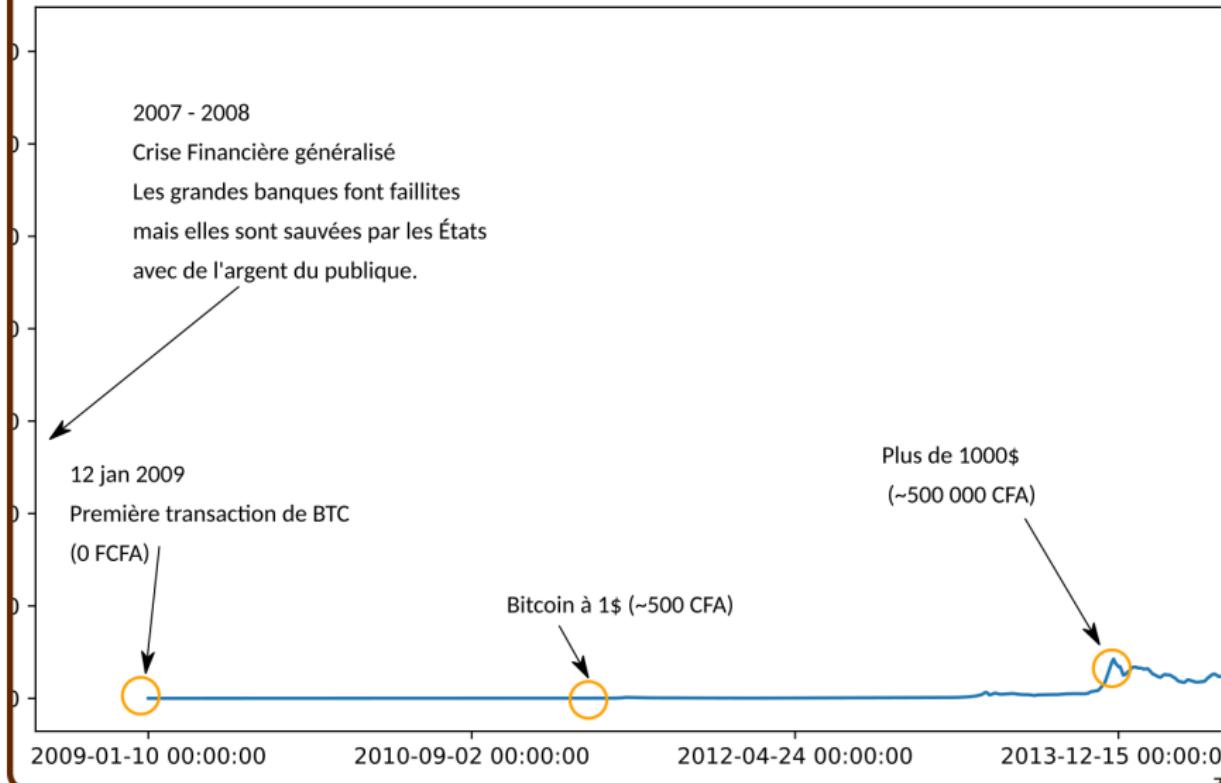
Les débuts



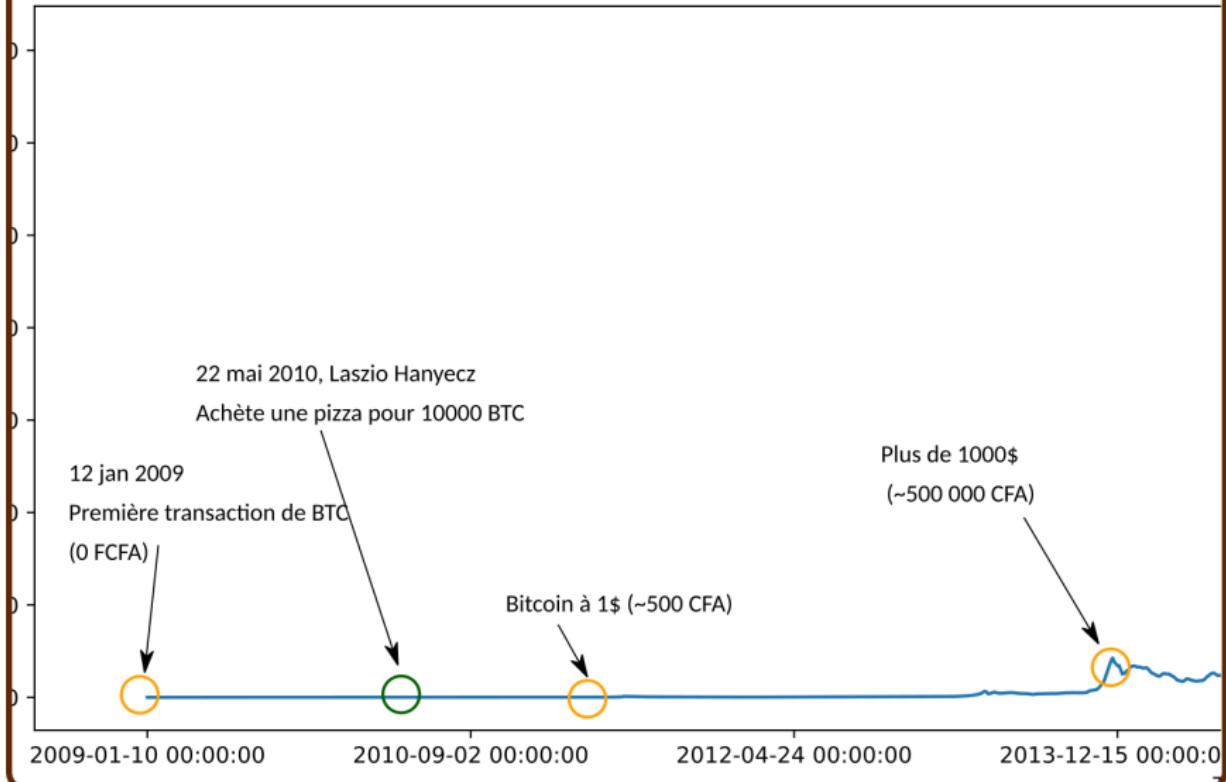
Les débuts



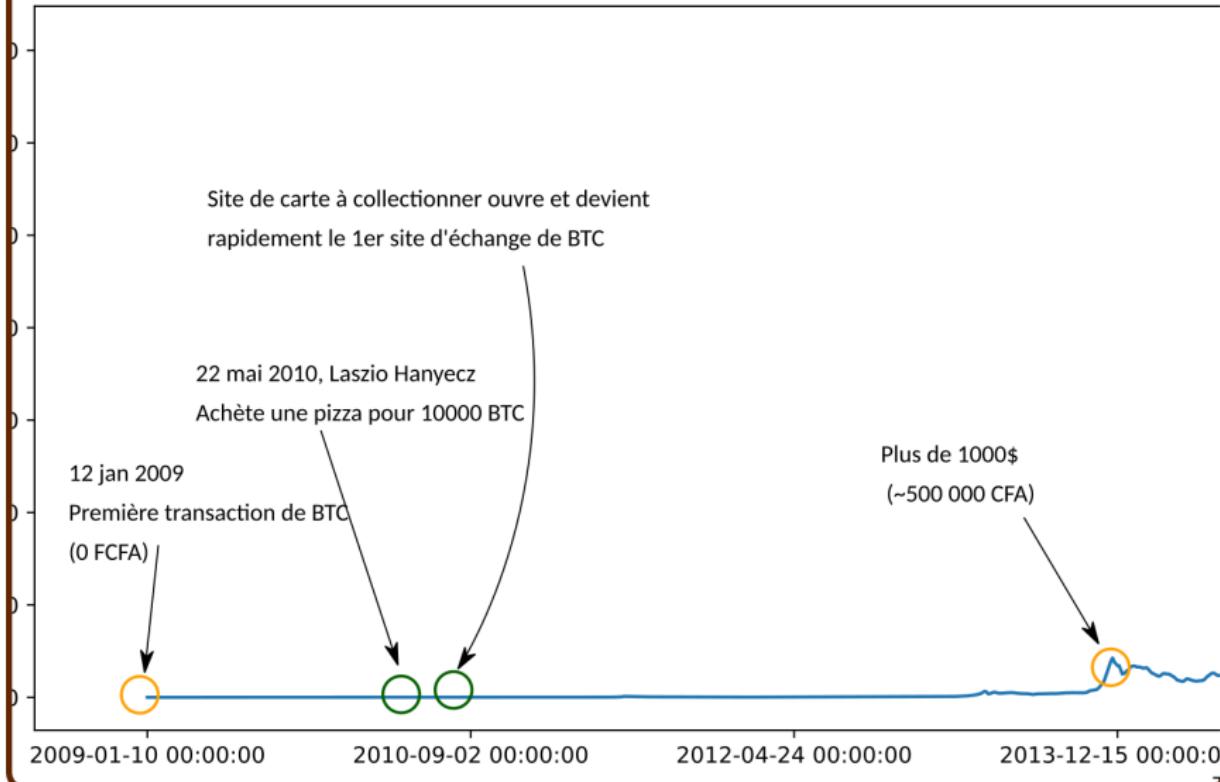
Les débuts



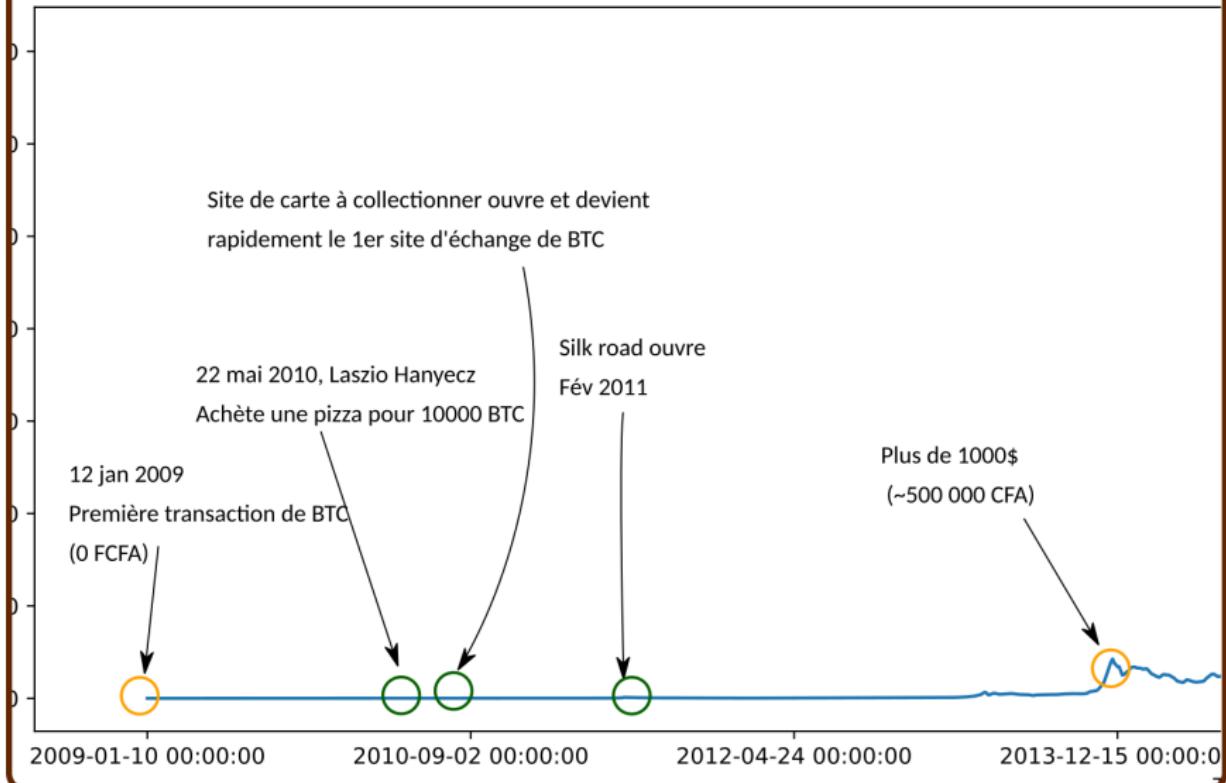
Les débuts



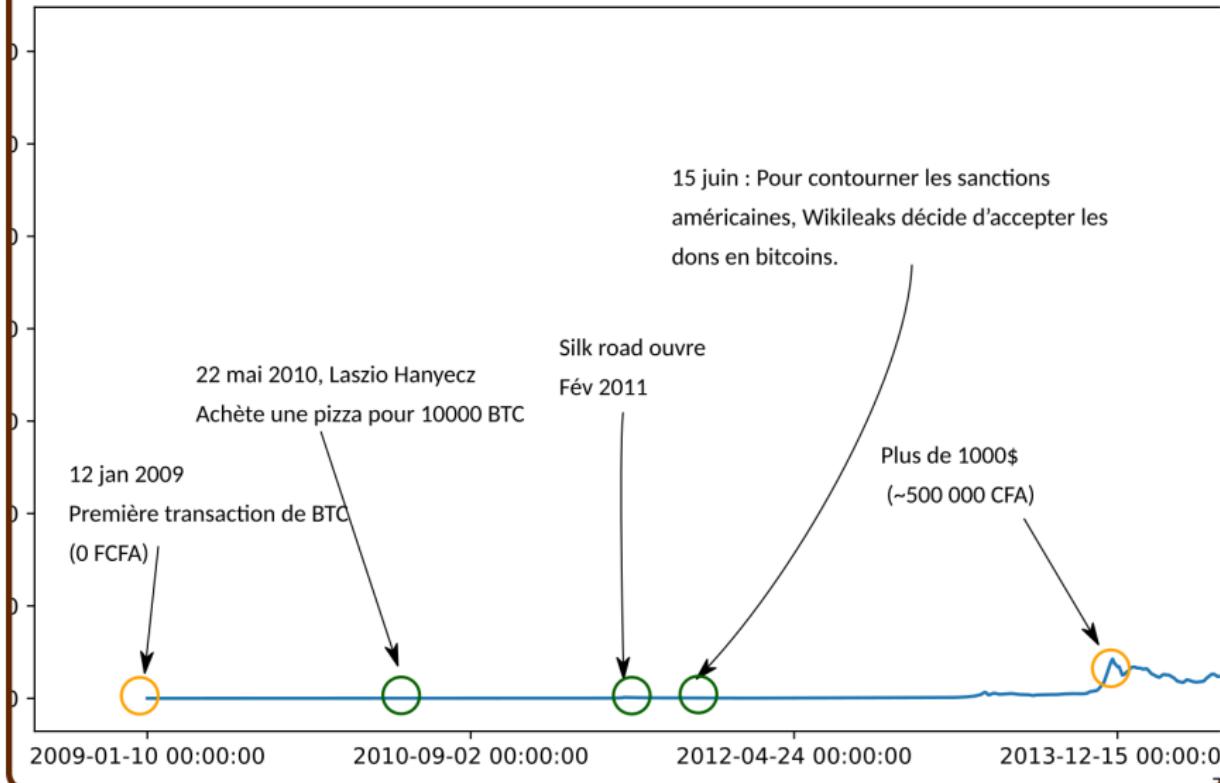
Les débuts



Les débuts



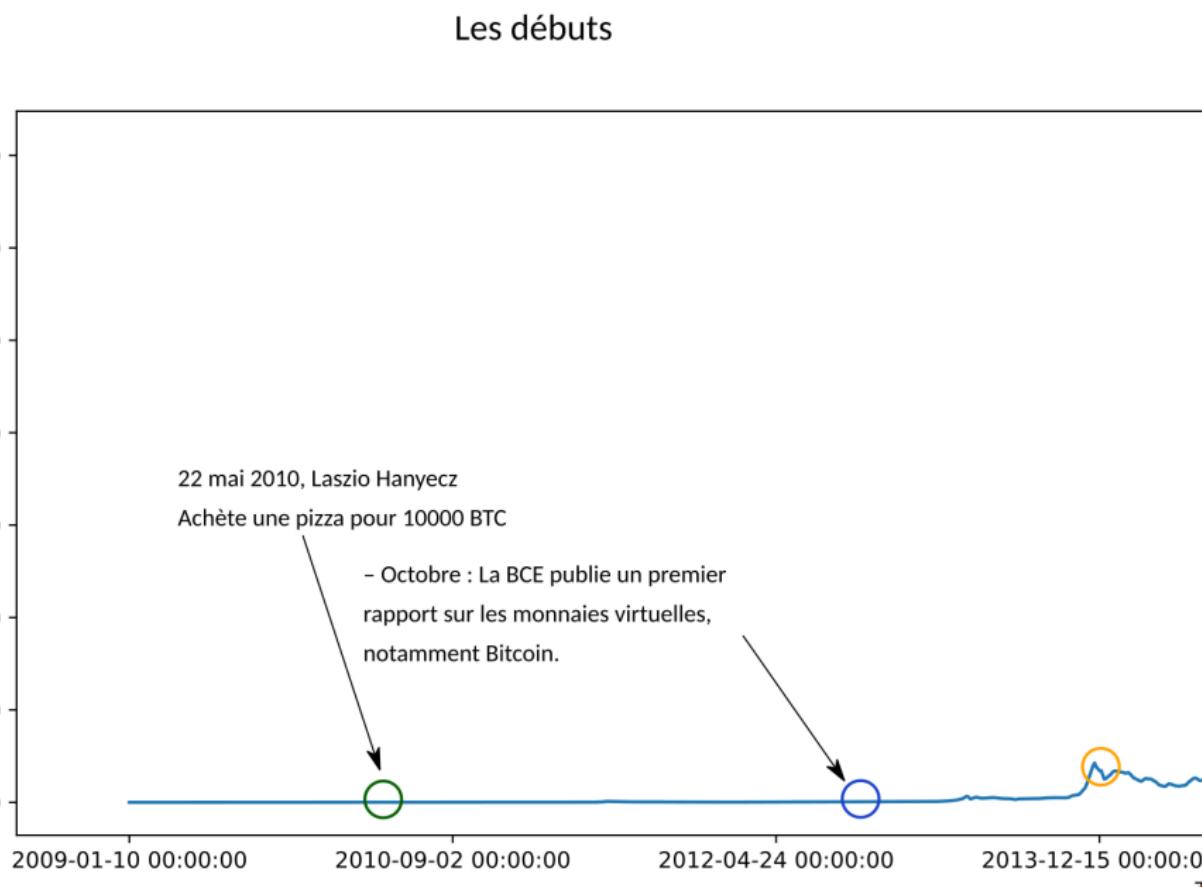
Les débuts



Les débuts

22 mai 2010, Laszlo Hanyecz
Achète une pizza pour 10000 BTC

- Octobre : La BCE publie un premier rapport sur les monnaies virtuelles, notamment Bitcoin.

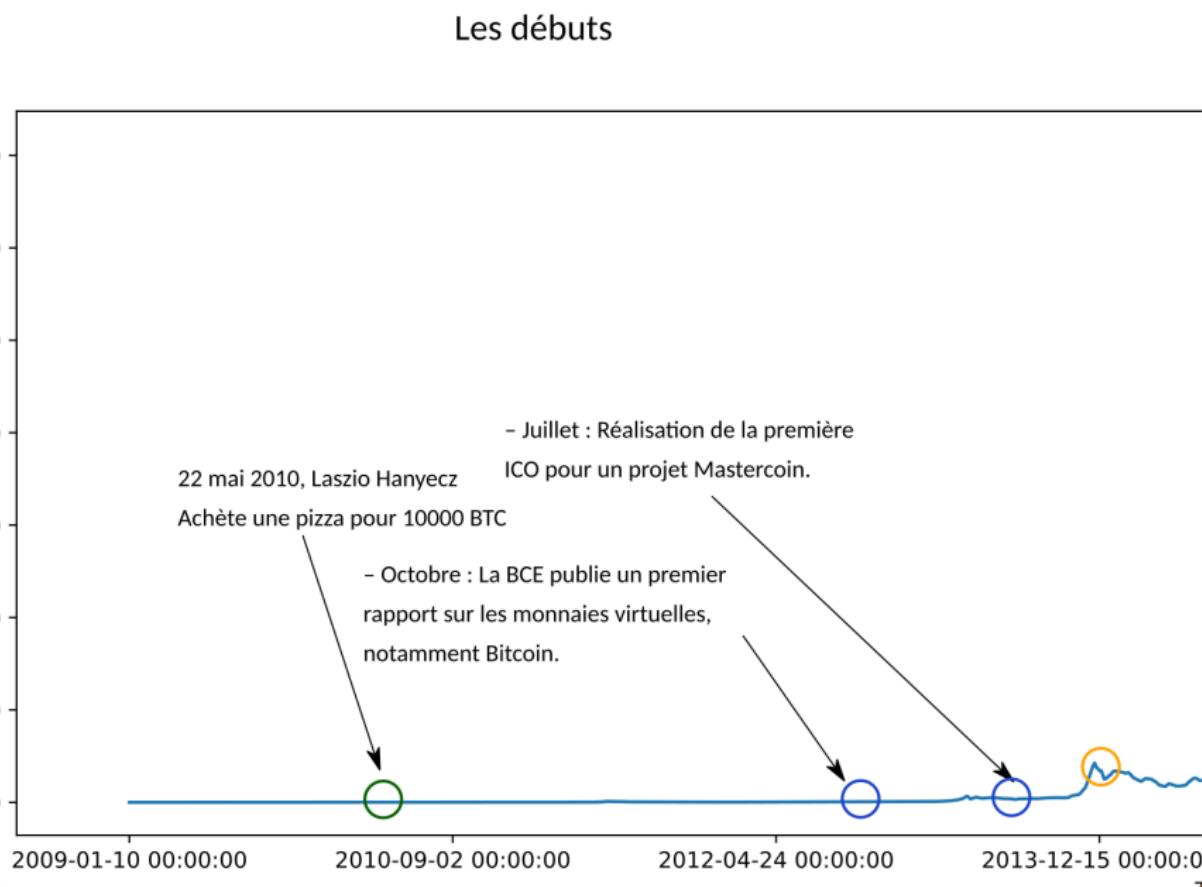


Les débuts

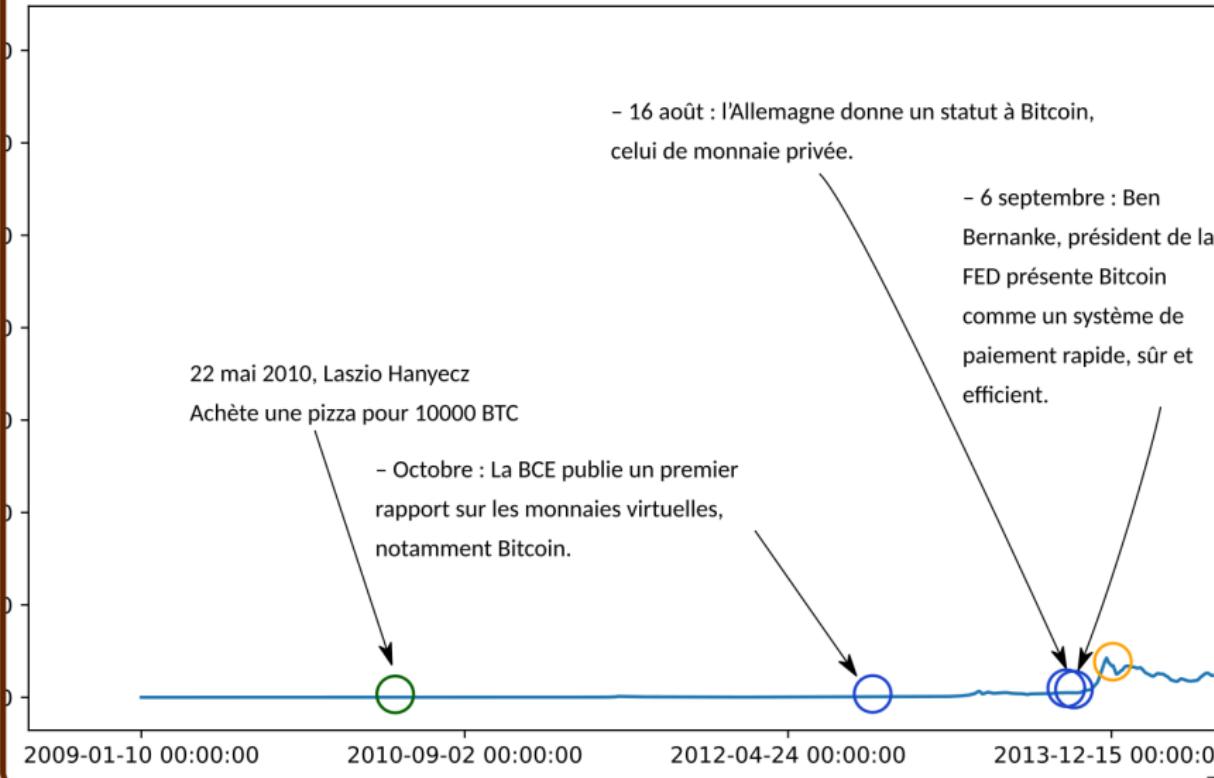
22 mai 2010, Laszlo Hanyecz
Achète une pizza pour 10000 BTC

- Juillet : Réalisation de la première ICO pour un projet Mastercoin.

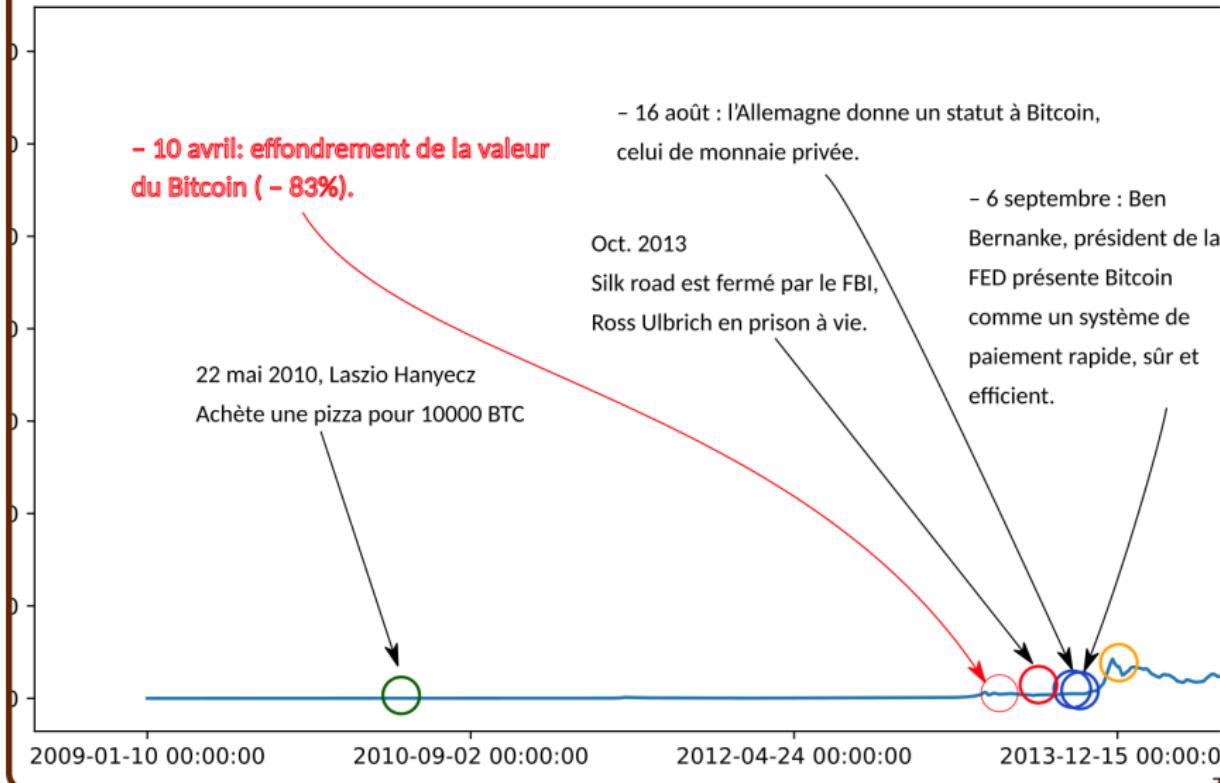
- Octobre : La BCE publie un premier rapport sur les monnaies virtuelles, notamment Bitcoin.



Les débuts



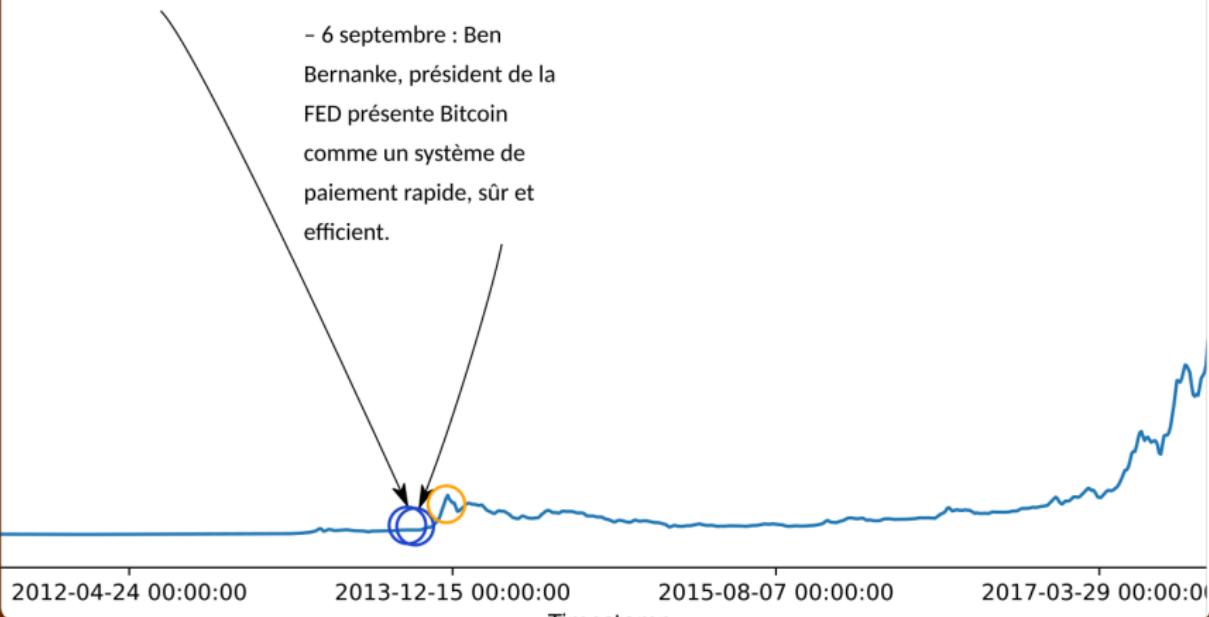
Les débuts



Adoption

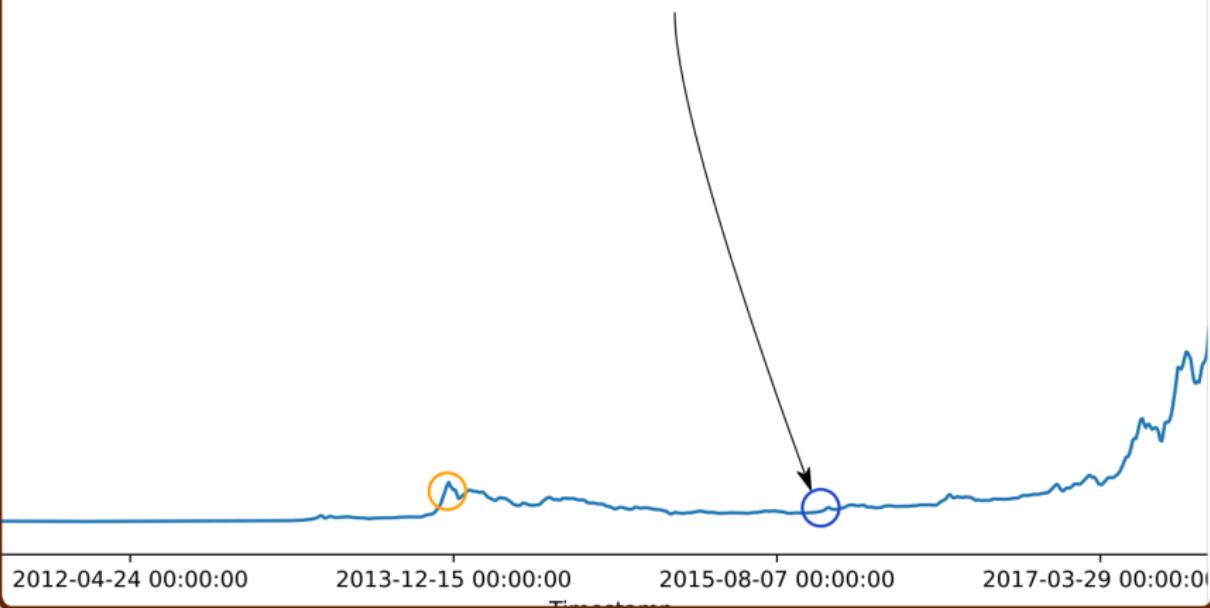
- 16 août : l'Allemagne donne un statut à Bitcoin, celui de monnaie privée.

- 6 septembre : Ben Bernanke, président de la FED présente Bitcoin comme un système de paiement rapide, sûr et efficient.



Adoption

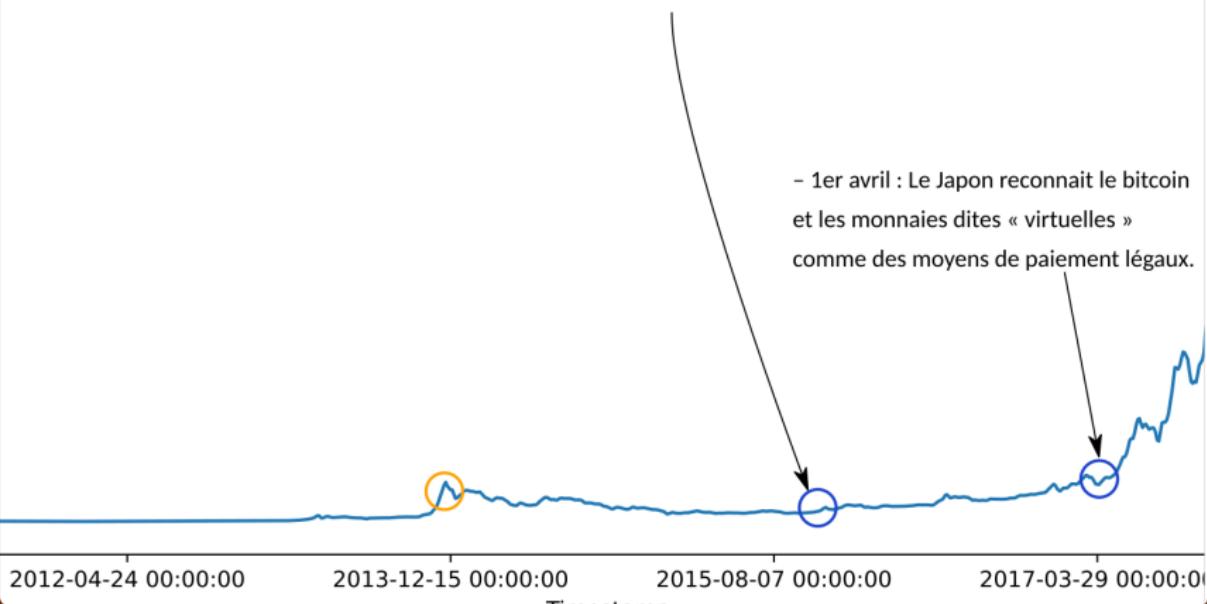
- 15 septembre : neuf banques d'investissement s'associent pour définir des standards d'implémentation d'une future blockchain privée.



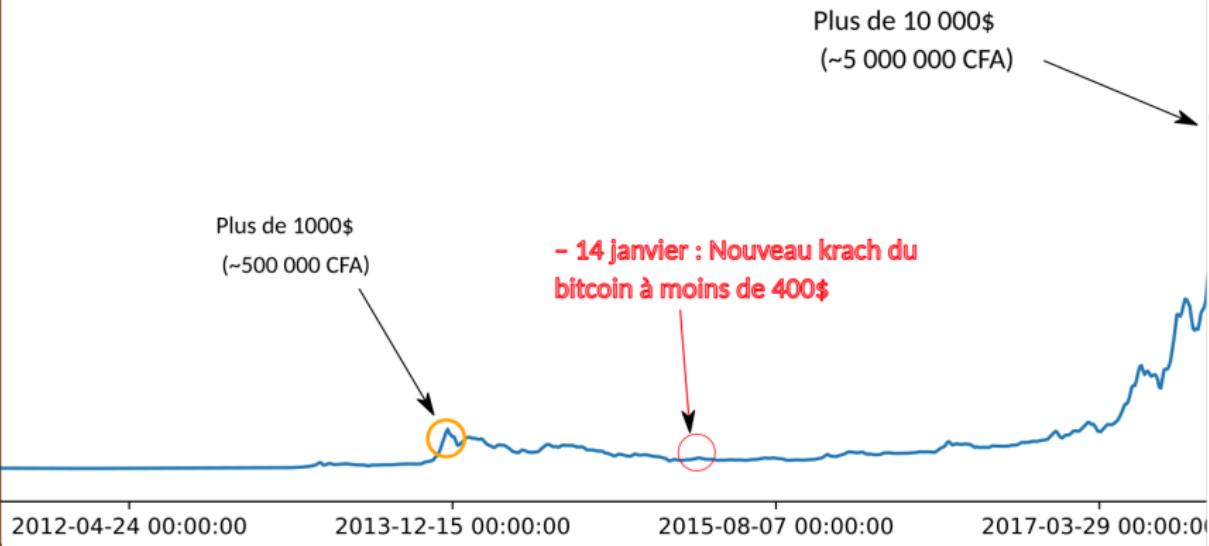
Adoption

- 15 septembre : neuf banques d'investissement s'associent pour définir des standards d'implémentation d'une future blockchain privée.

- 1er avril : Le Japon reconnaît le bitcoin et les monnaies dites « virtuelles » comme des moyens de paiement légaux.

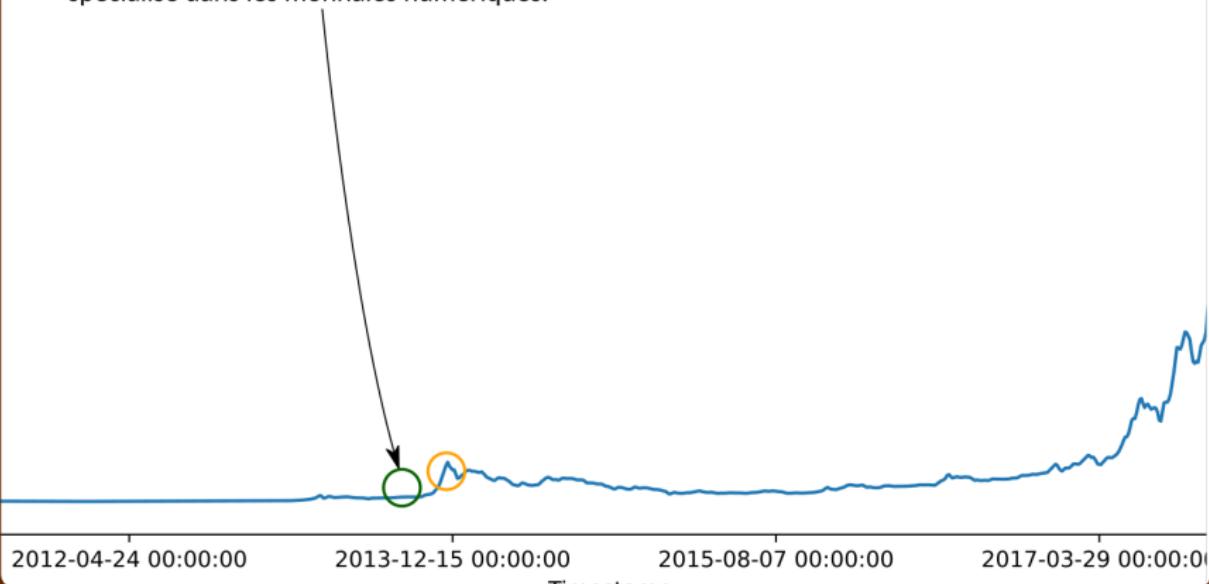


Adoption



Adoption

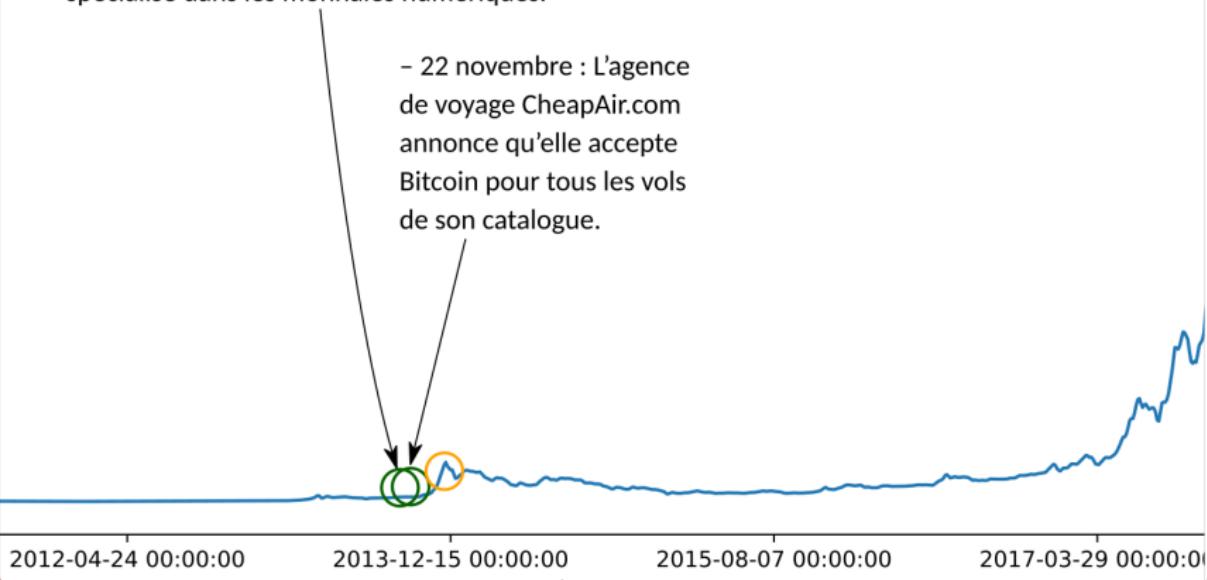
- 21 novembre : L'Université de Nicosie accepte que les frais de scolarité soient payés en bitcoins et annonce l'ouverture d'un Master de sciences économiques spécialisé dans les monnaies numériques.



Adoption

- 21 novembre : L'Université de Nicosie accepte que les frais de scolarité soient payés en bitcoins et annonce l'ouverture d'un Master de sciences économiques spécialisé dans les monnaies numériques.

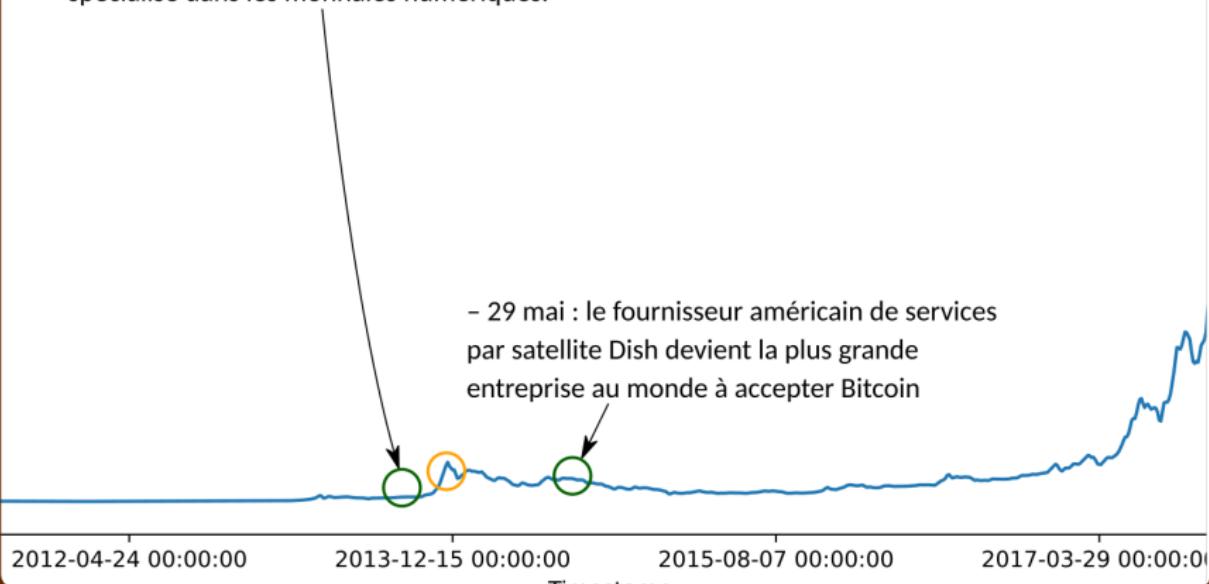
- 22 novembre : L'agence de voyage CheapAir.com annonce qu'elle accepte Bitcoin pour tous les vols de son catalogue.



Adoption

- 21 novembre : L'Université de Nicosie accepte que les frais de scolarité soient payés en bitcoins et annonce l'ouverture d'un Master de sciences économiques spécialisé dans les monnaies numériques.

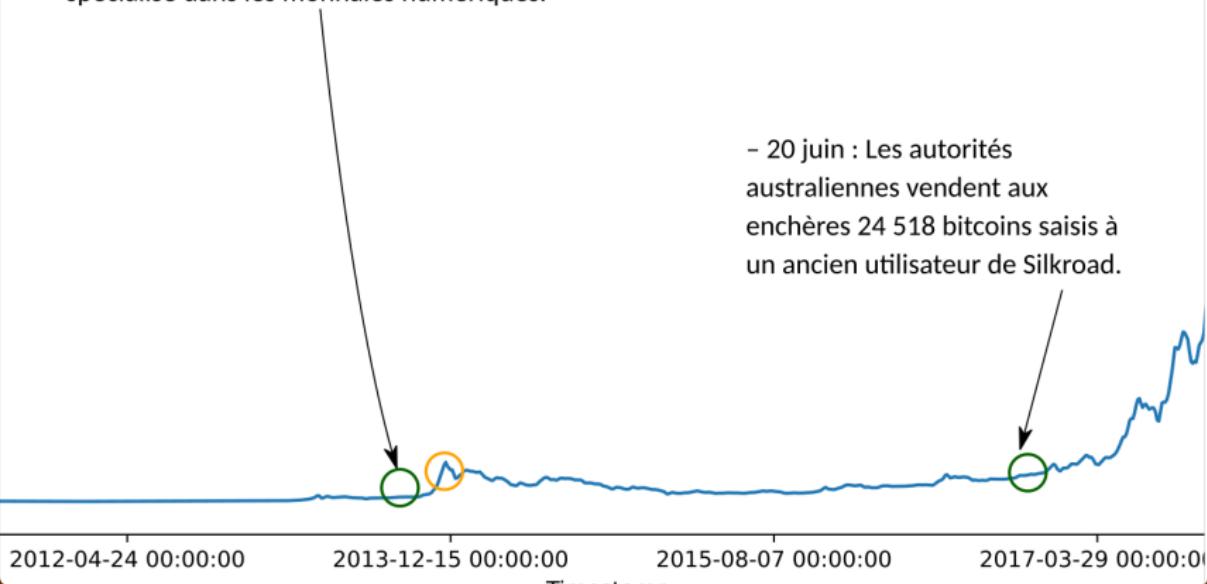
- 29 mai : le fournisseur américain de services par satellite Dish devient la plus grande entreprise au monde à accepter Bitcoin



Adoption

- 21 novembre : L'Université de Nicosie accepte que les frais de scolarité soient payés en bitcoins et annonce l'ouverture d'un Master de sciences économiques spécialisé dans les monnaies numériques.

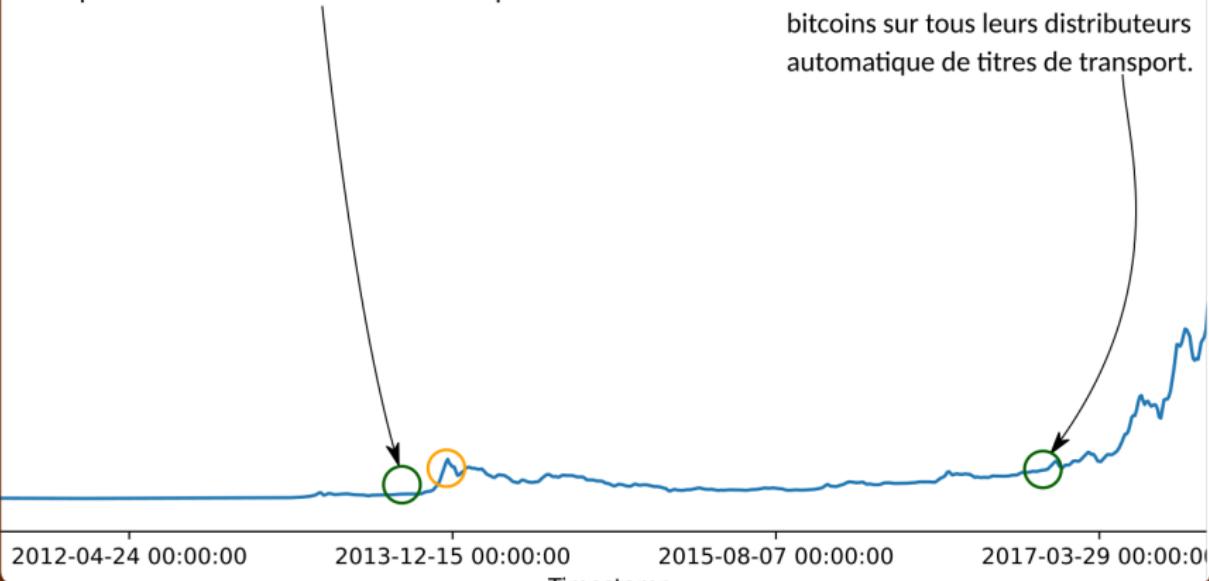
- 20 juin : Les autorités australiennes vendent aux enchères 24 518 bitcoins saisis à un ancien utilisateur de Silkroad.

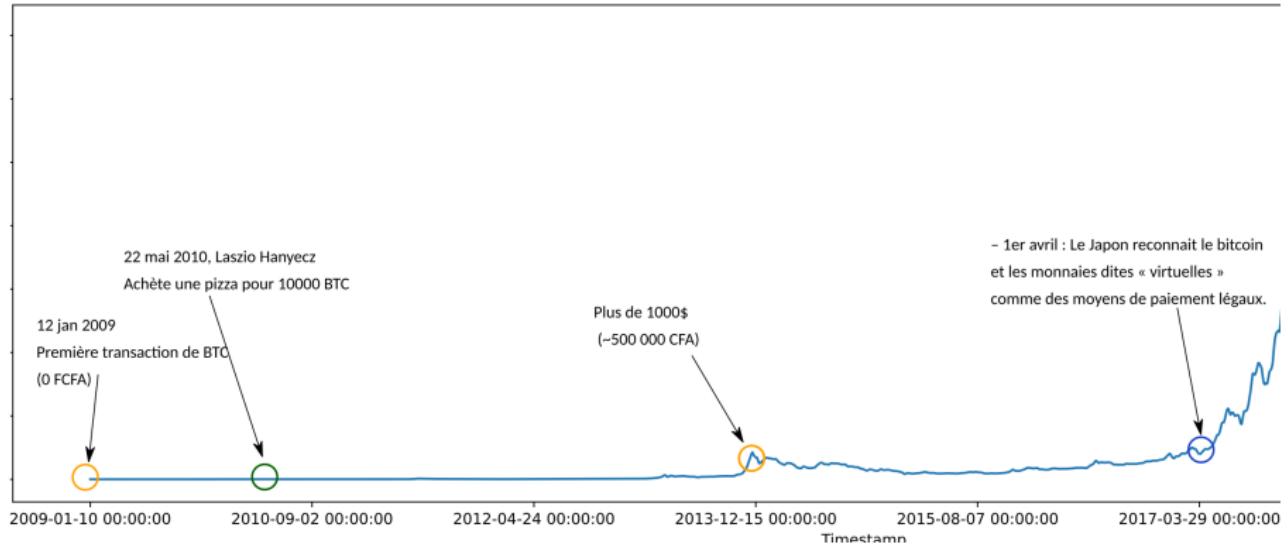


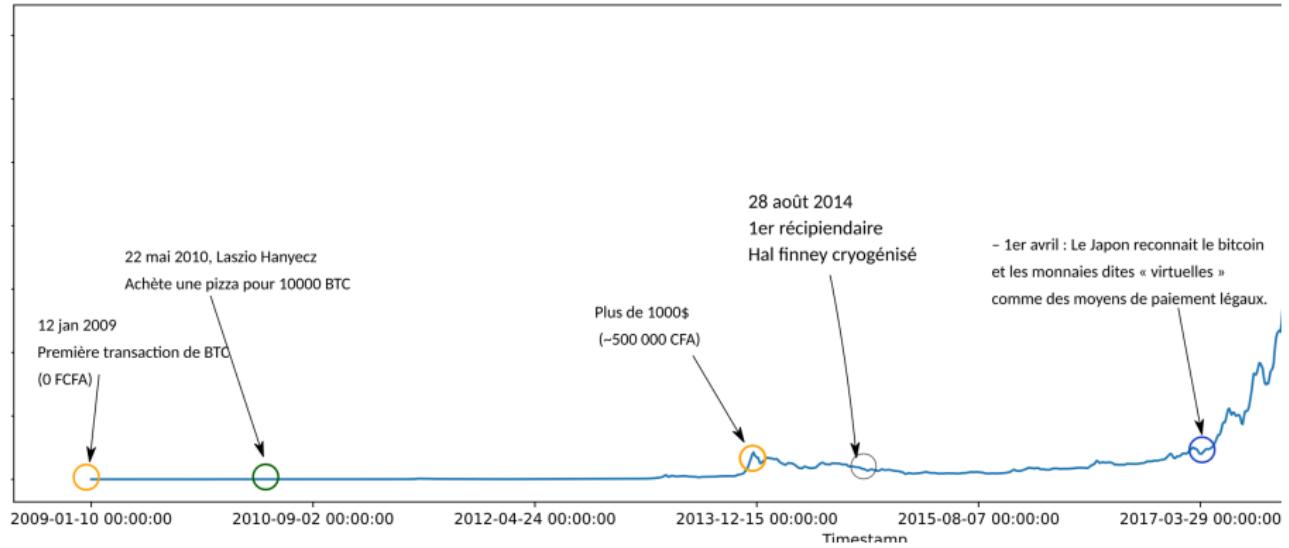
Adoption

- 21 novembre : L'Université de Nicosie accepte que les frais de scolarité soient payés en bitcoins et annonce l'ouverture d'un Master de sciences économiques spécialisé dans les monnaies numériques.

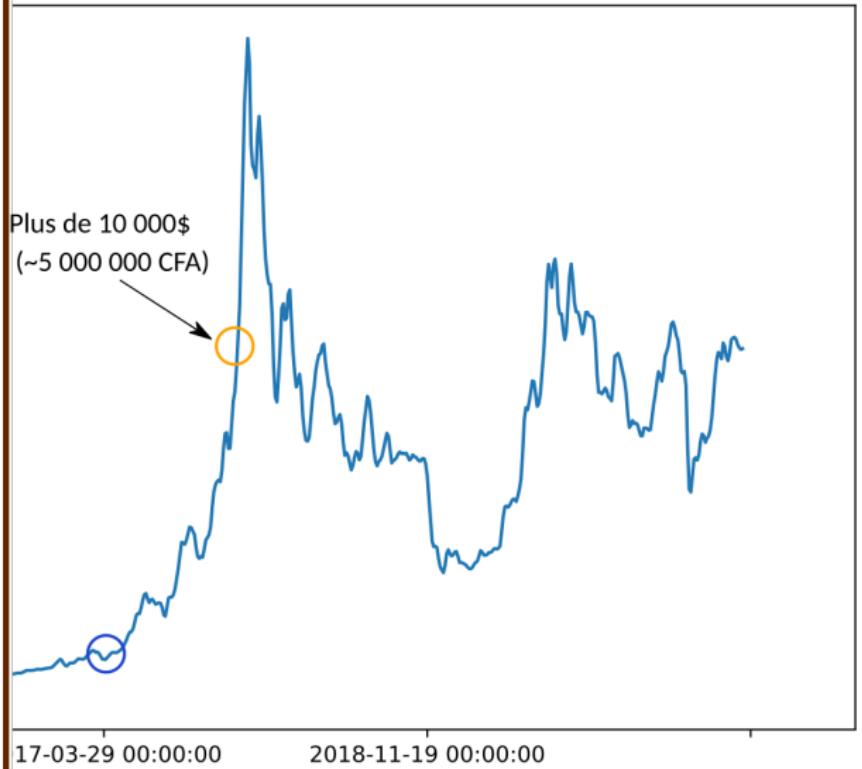
- 11 novembre : Les Chemins de fer fédéraux suisses testent, pour une période de deux ans, la vente de bitcoins sur tous leurs distributeurs automatique de titres de transport.



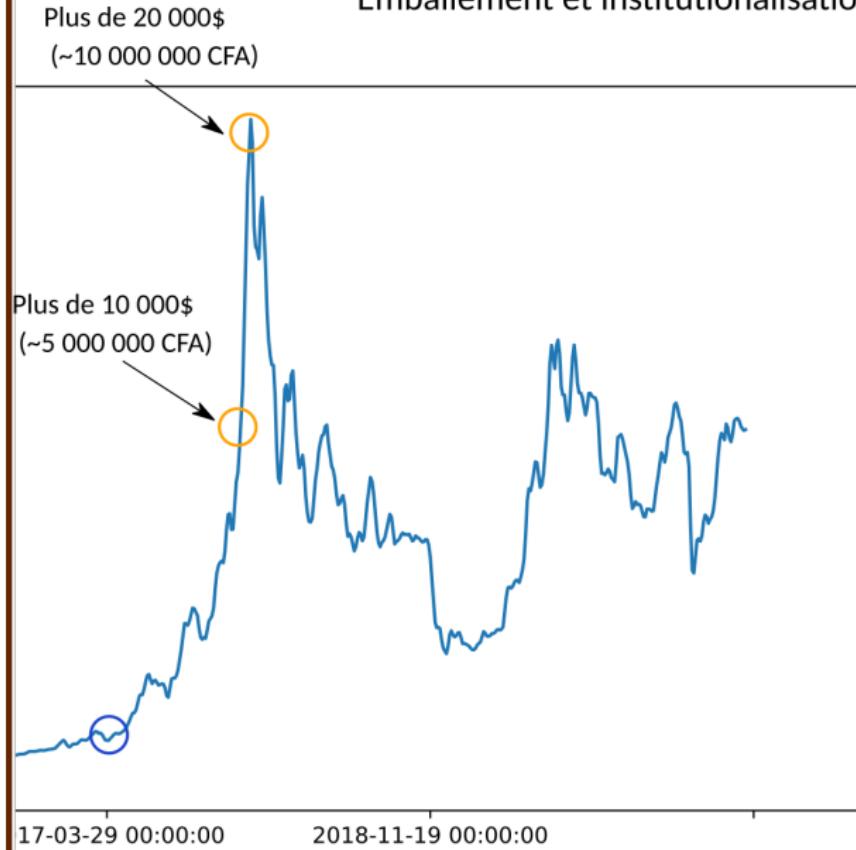




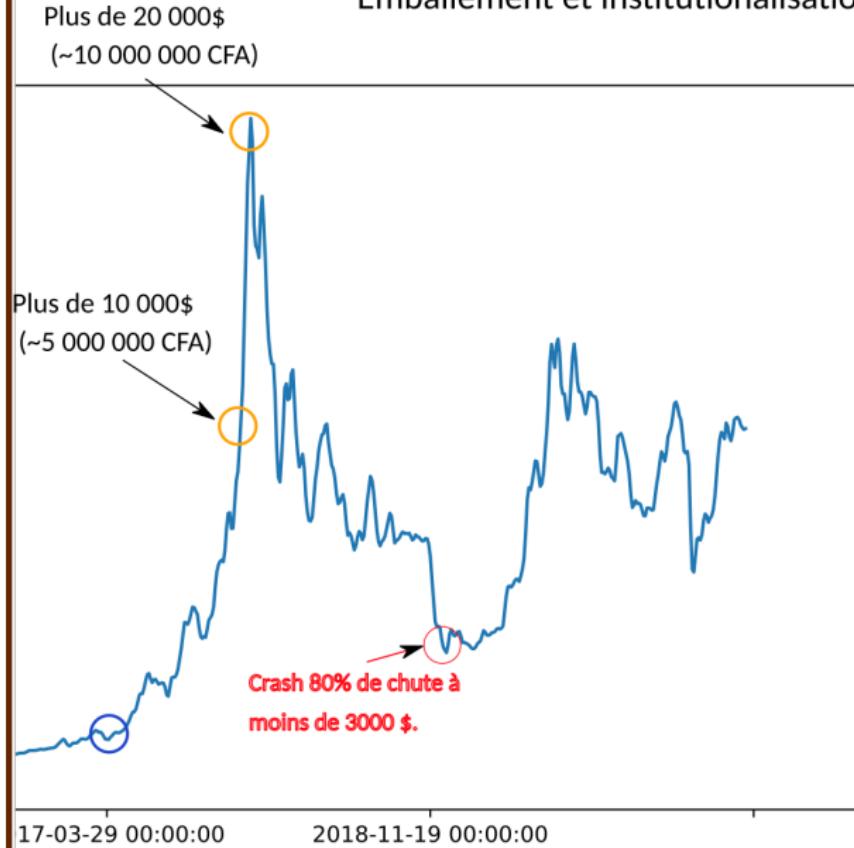
Emballage et institutionalisation



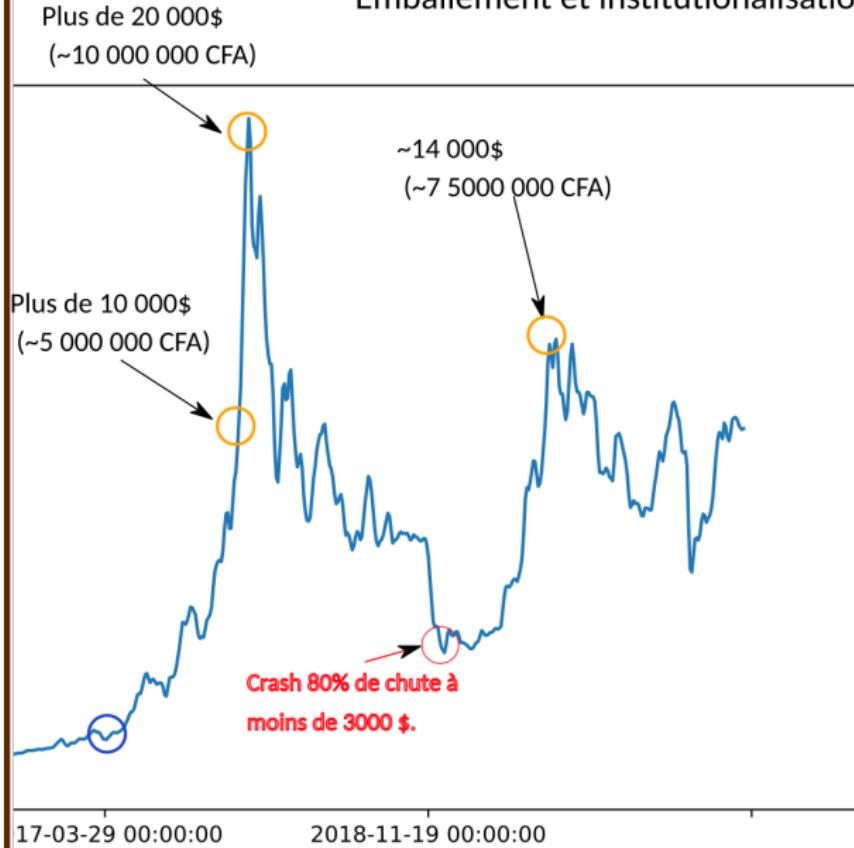
Emballage et institutionalisation



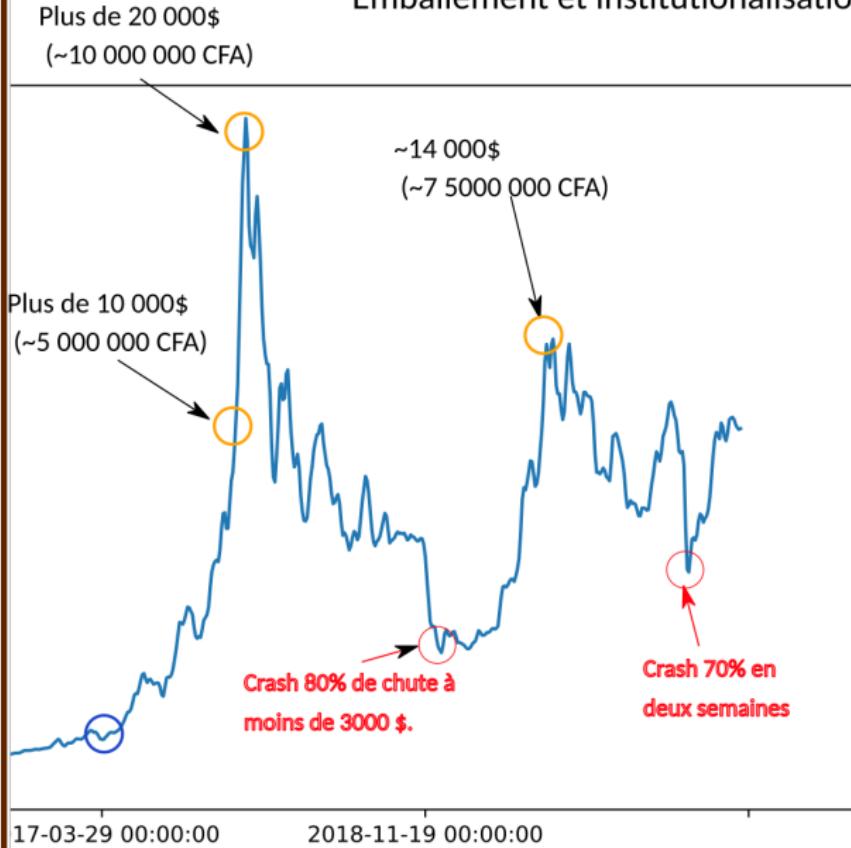
Emballage et institutionalisation



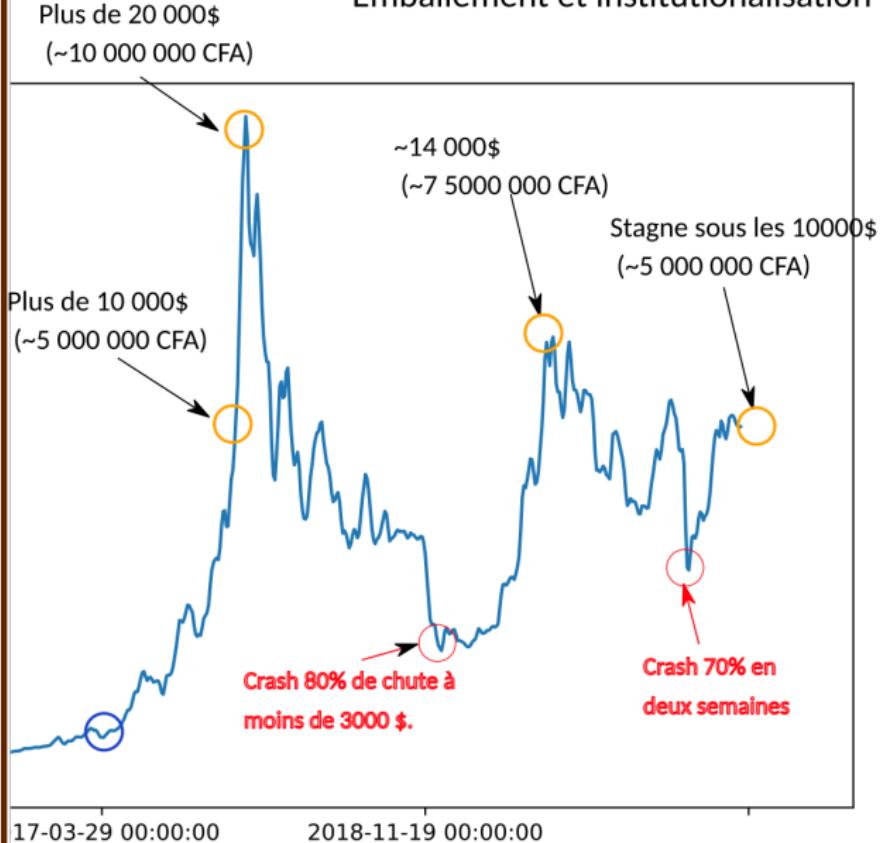
Emballage et institutionalisation



Emballage et institutionalisation

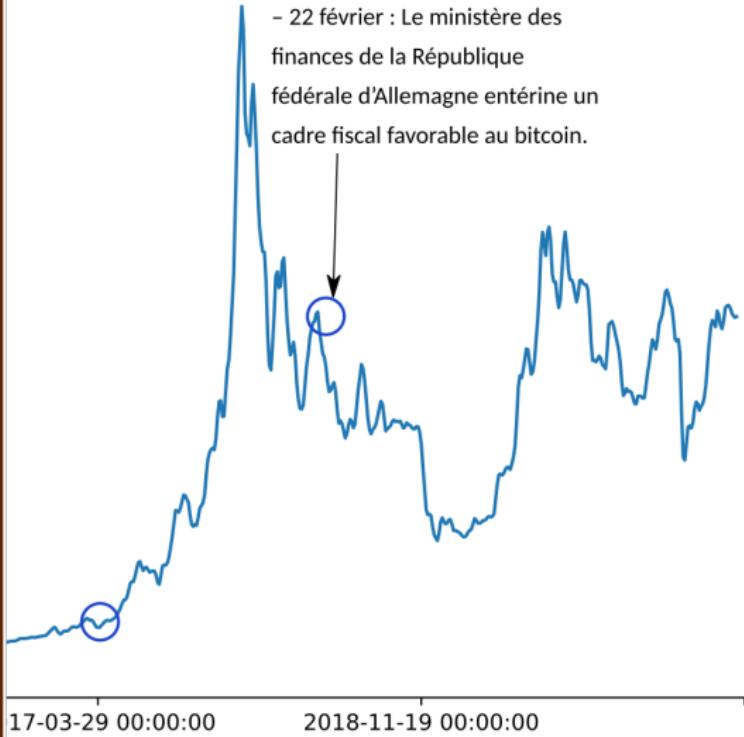


Emballage et institutionalisation

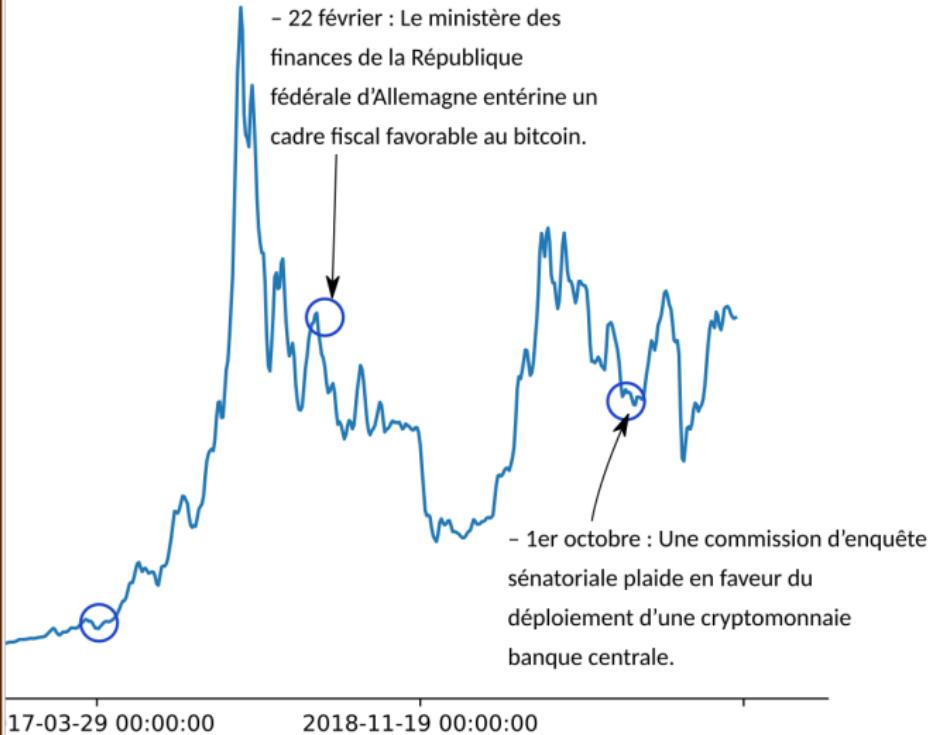


Emballage et institutionalisation

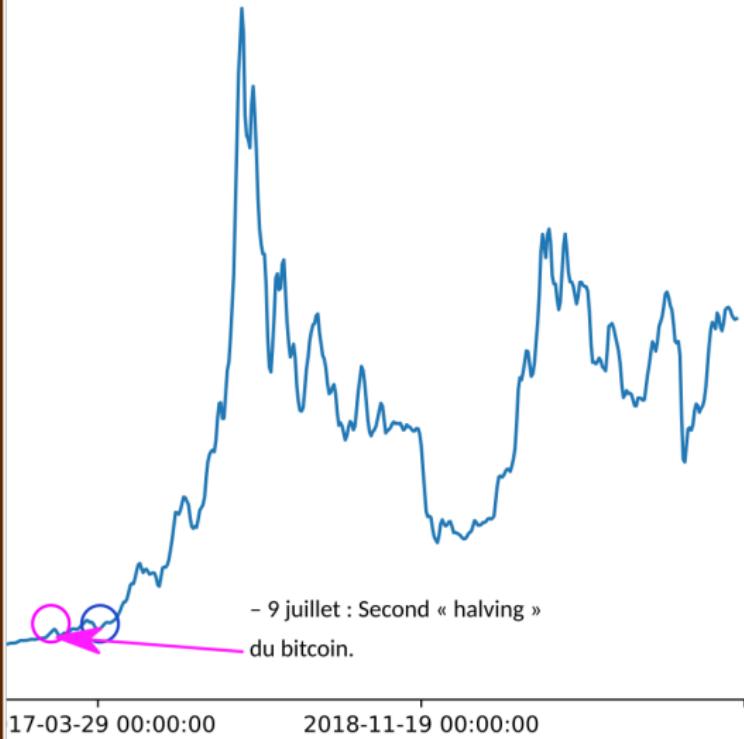
- 22 février : Le ministère des finances de la République fédérale d'Allemagne entérine un cadre fiscal favorable au bitcoin.



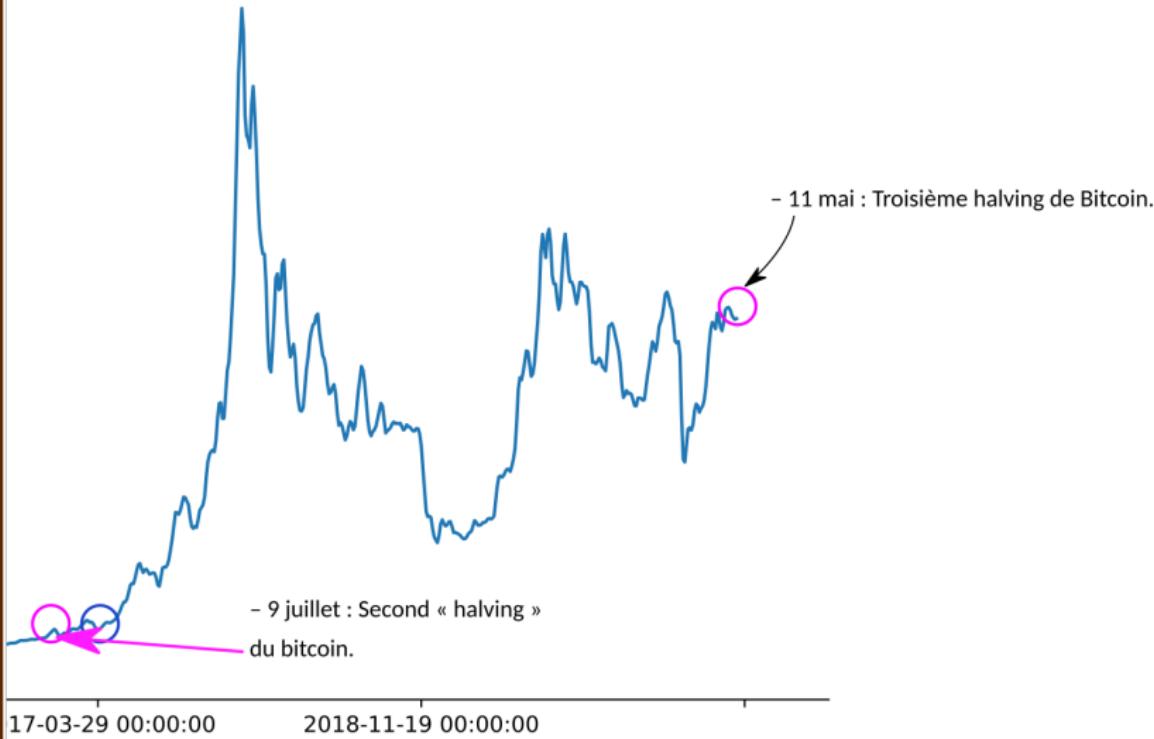
Emballage et institutionalisation

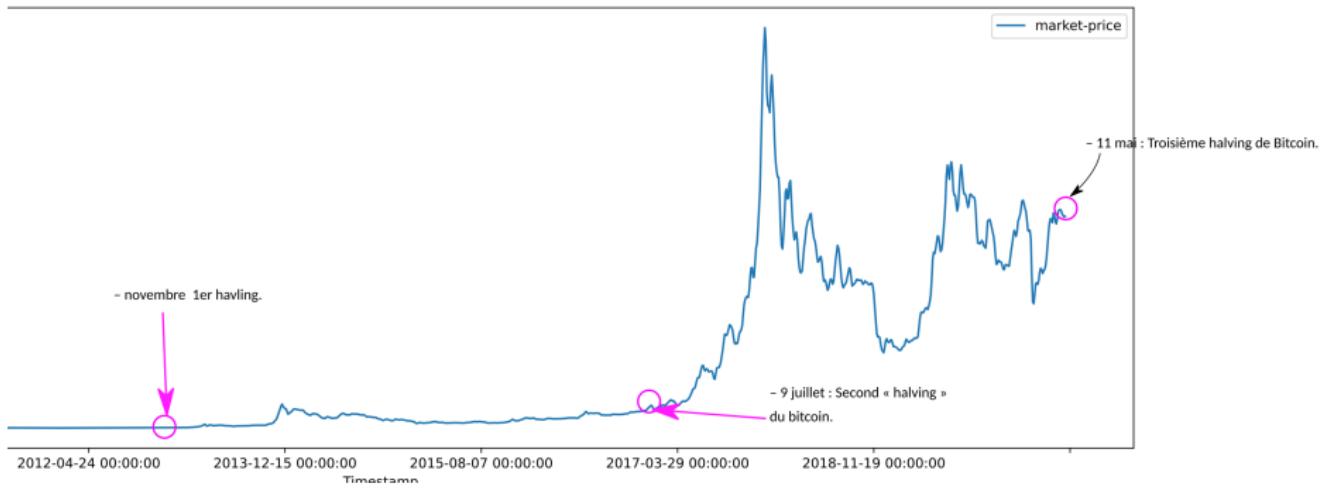


Emballage et institutionalisation

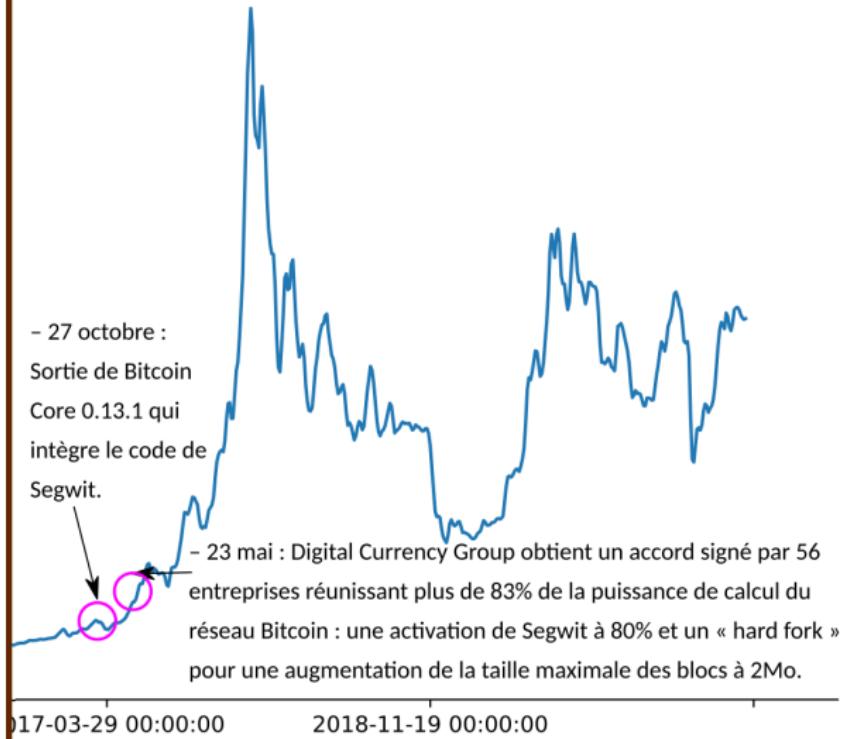


Emballage et institutionalisation



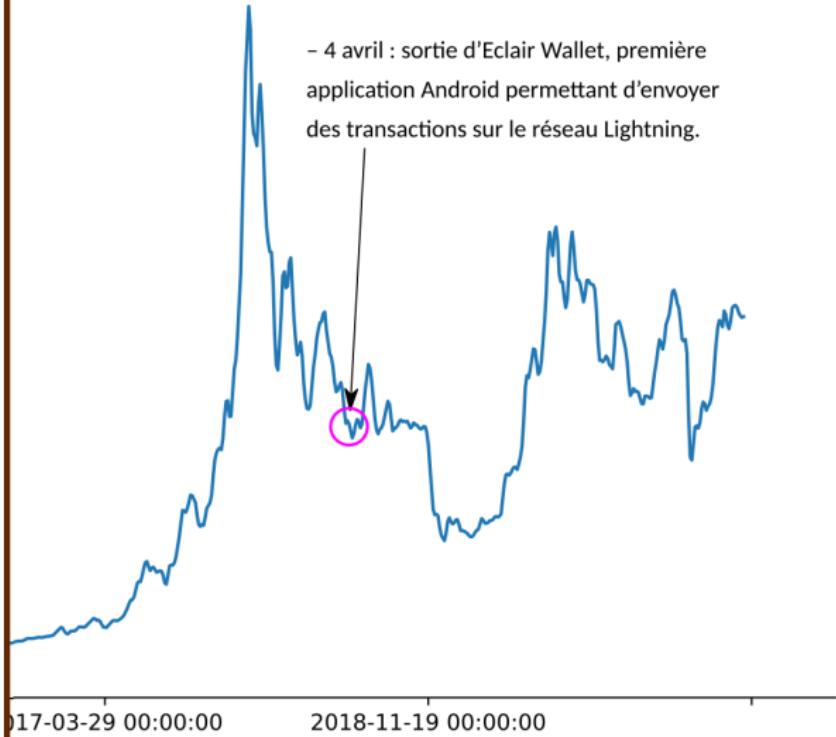


Emballage et institutionalisation



Emballage et institutionalisation

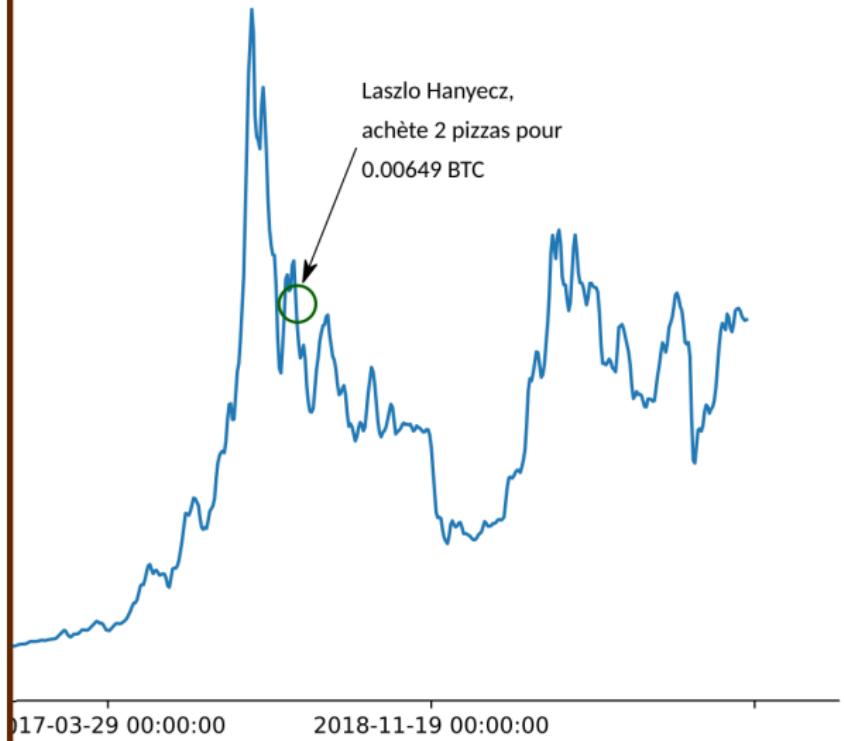
- 4 avril : sortie d'Eclair Wallet, première application Android permettant d'envoyer des transactions sur le réseau Lightning.



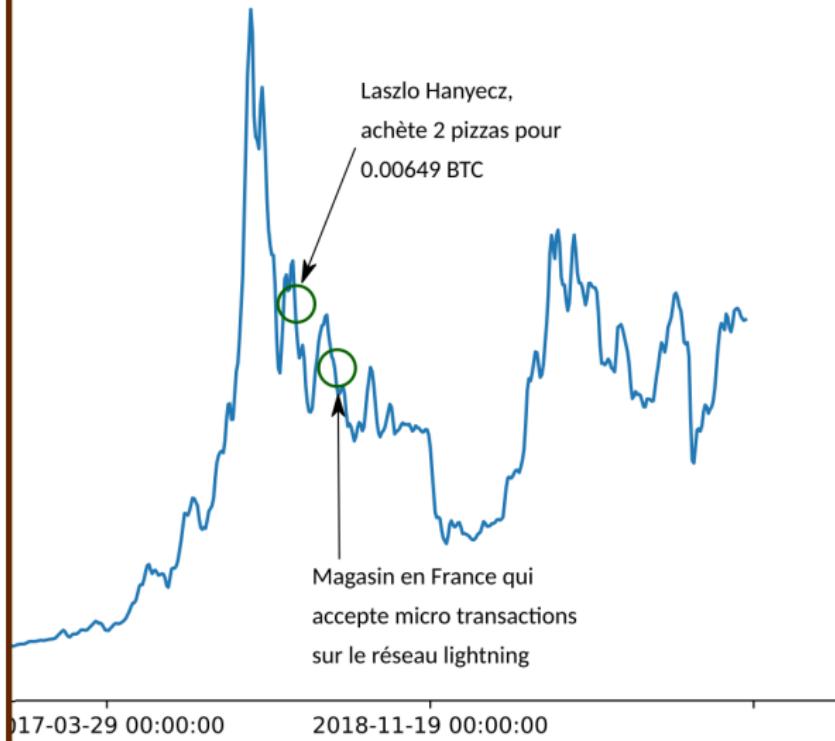
Emballage et institutionalisation



Emballage et institutionalisation

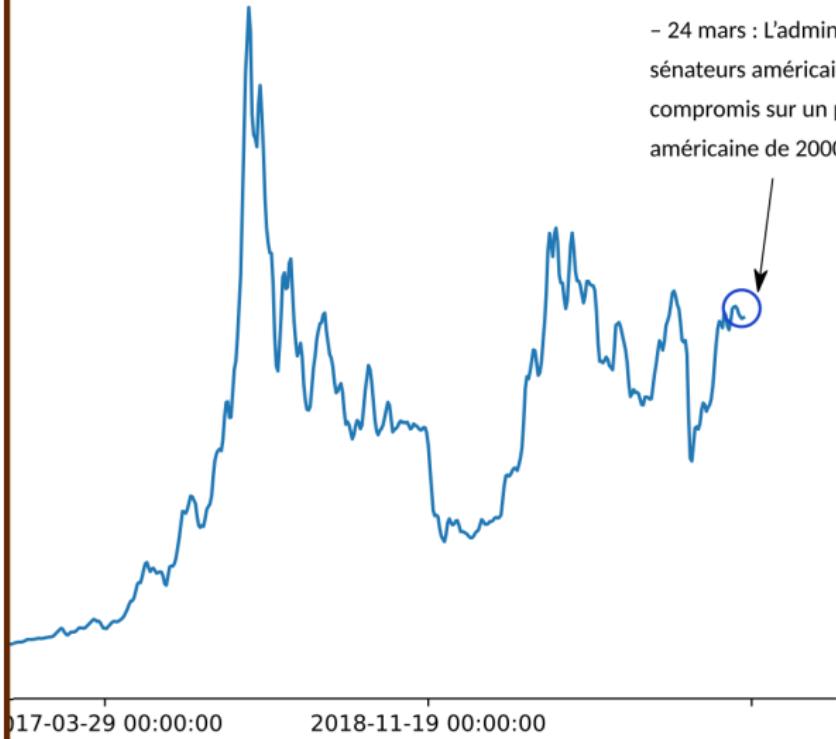


Emballage et institutionalisation



Emballage et institutionalisation

- 24 mars : L'administration Trump et les sénateurs américains parviennent à un compromis sur un plan de soutien à l'économie américaine de 2000 milliards de dollars.



et aujourd'hui ?

Regardons le graphique des prix du Bitcoin jusqu'à ce jour

Sommaire

1. Introduction

- Notions de départ
- Les types d'utilisateurs des Blockchain

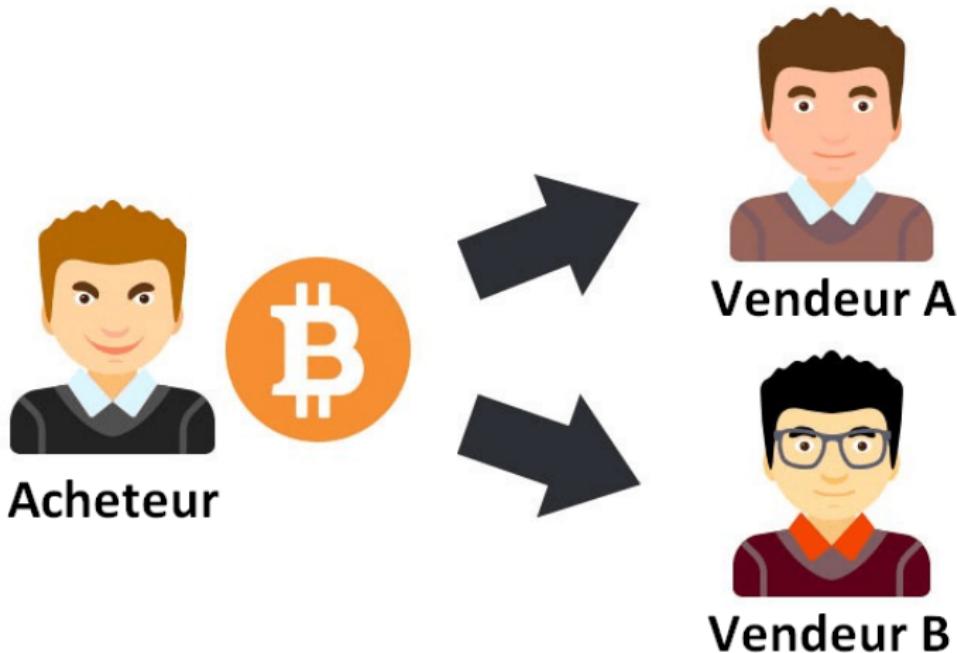
2. Bitcoin : Blockchain de 1^{re} génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- **Quel est le problème résolu**
- Les limites

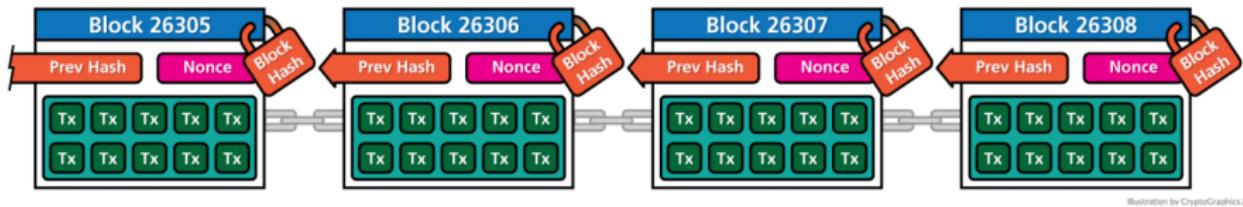
3. Perspectives

- Perspectives

La double dépense



Comment le problème est-il résolu ?



avec un journal comptable électronique

- ▶ organisés en blocks **infalsifiables** : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'**enchainent** les uns aux autres : chain
- ▶ dans un réseau **publique et décentralisé** : pairs

Un exemple de block

Comment le problème est-il résolu ?

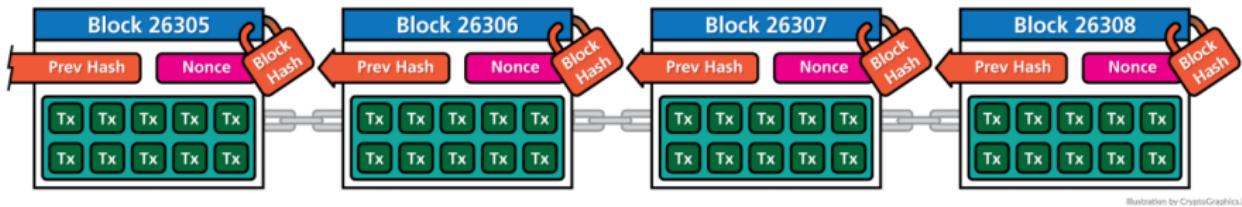


Illustration by CryptoGraphics.info

avec un journal comptable électronique

- ▶ organisés en blocks **infalsifiables** : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'**enchainent** les uns aux autres : chain
- ▶ dans un réseau **publique et décentralisé** : pairs

Un exemple de block

Comment le problème est-il résolu ?

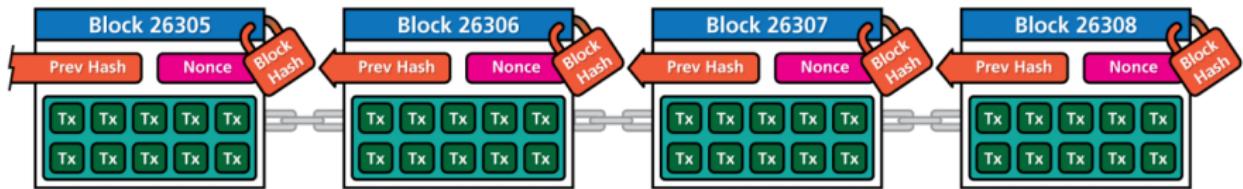


Illustration by CryptoGraphics.info

avec un journal comptable électronique

- ▶ organisés en blocks **infalsifiables** : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'**enchainent** les uns aux autres : chain
- ▶ dans un réseau **publique et décentralisé** : pairs

Un exemple de block

Comment le problème est-il résolu ?

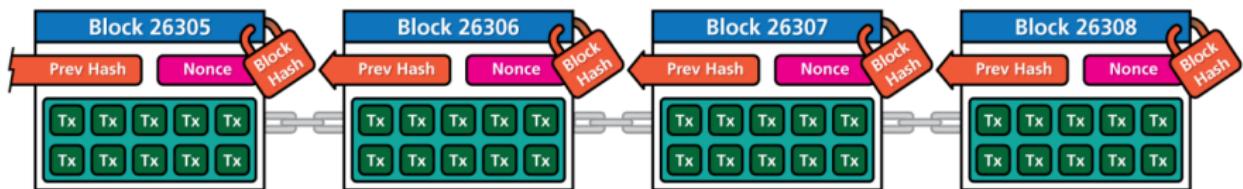


Illustration by CryptoGraphics.info

avec un journal comptable électronique

- ▶ organisés en blocks **infalsifiables** : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'**enchainent** les uns aux autres : chain
- ▶ dans un réseau **public et décentralisé** : pairs

Un exemple de block

Comment le problème est-il résolu ?

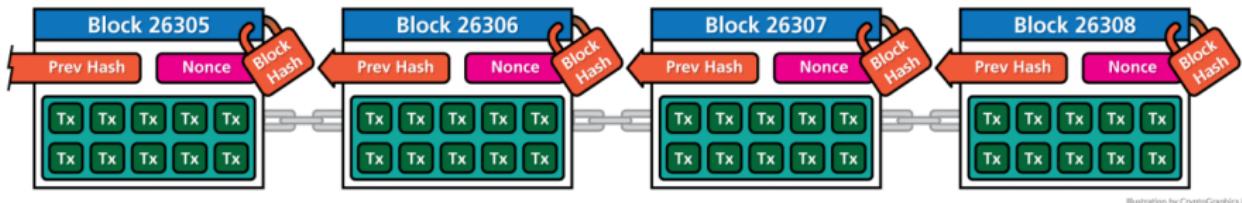


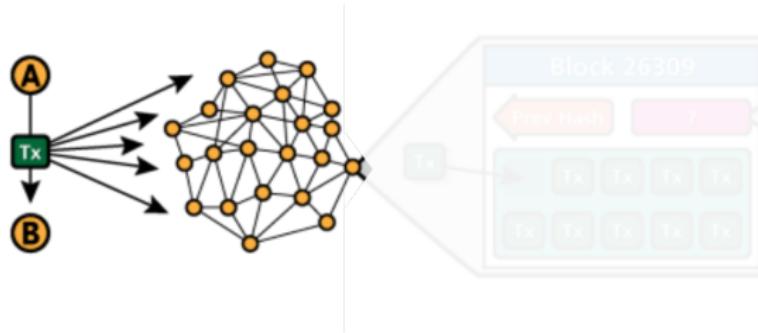
Illustration by CryptoGraphics.info

avec un journal comptable électronique

- ▶ organisés en blocks infalsifiables : SHA256 HASH
- ▶ de façon unique : block
- ▶ qui s'enchaînent les uns aux autres : chain
- ▶ dans un réseau public et décentralisé : pairs

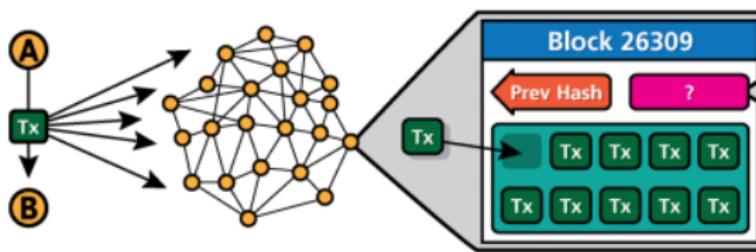
Un exemple de block

Plus techniquement comment cela fonctionne ?



Tx : ".00012300 BTC pour Binta, signé Amadou"

Plus techniquement comment cela fonctionne ?



Les mineurs incluent la tx dans un bloc et cherchent un **bon nonce**

Plus techniquement comment cela fonctionne ?

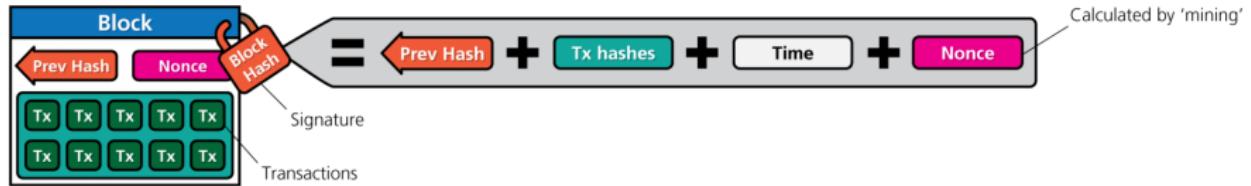


Illustration by CryptoGraphics.info

Le 1^{er} mineur à trouver un **bon nonce**, publie le bloc

- ▶ il contient une récompense (coinbase)

Plus techniquement comment cela fonctionne ?

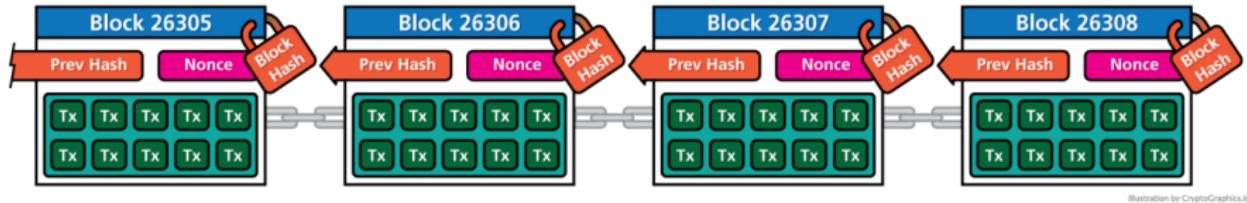


Illustration by CryptoGraphics.info

Les autres mineurs :

- ▶ Vérifient le nonce
- ▶ Ajoutent le nouveau block à la chaîne
- ▶ Recommencent la course pour obtenir une récompense

Et, ça marche depuis 2009 !



- ▶ 18/05/2010, les Pizza à 10000 BTC de Laslo (bitcointalk.org)

Sommaire

1. Introduction

- Notions de départ
- Les types d'utilisateurs des Blockchain

2. Bitcoin : Blockchain de 1^{re} génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Quel est le problème résolu
- **Les limites**

3. Perspectives

- Perspectives

Des problèmes de taille

Puissance nécessaire

- ▶ Hash Rate (TeraHash/s, Tera = 1000 milliards)

Vitesse de confirmation

- ▶ Attente pour les transactions

Coût

- ▶ Frais de transaction relativement important

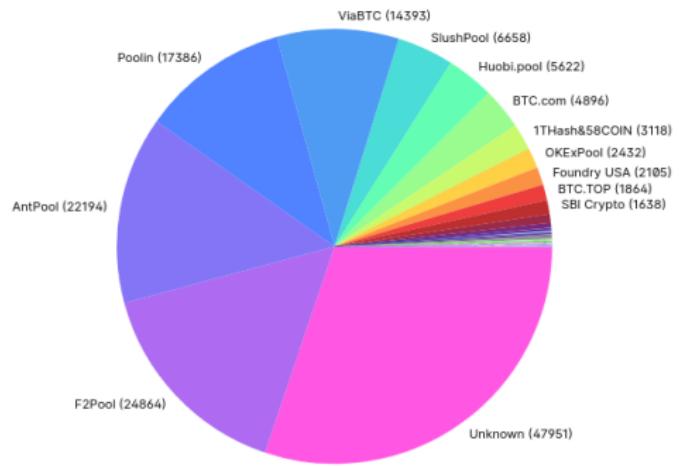
Simplicité

Manque d'adaptabilité

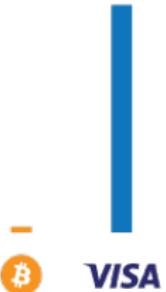
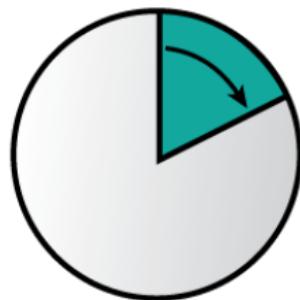
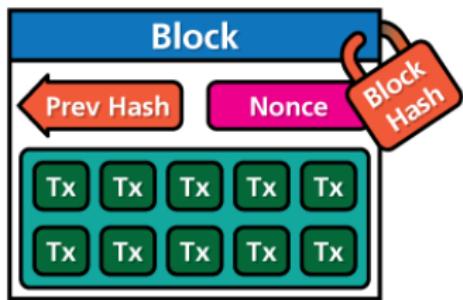
Coût énergétique



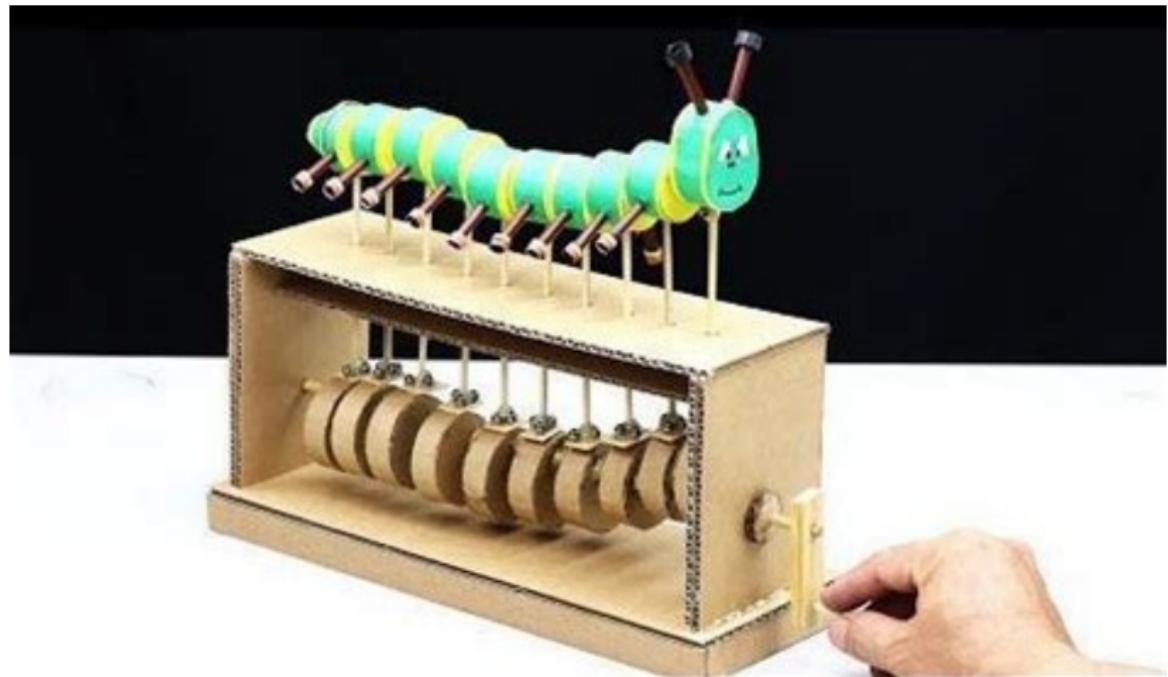
Concentration du hashrate (janv 2023)



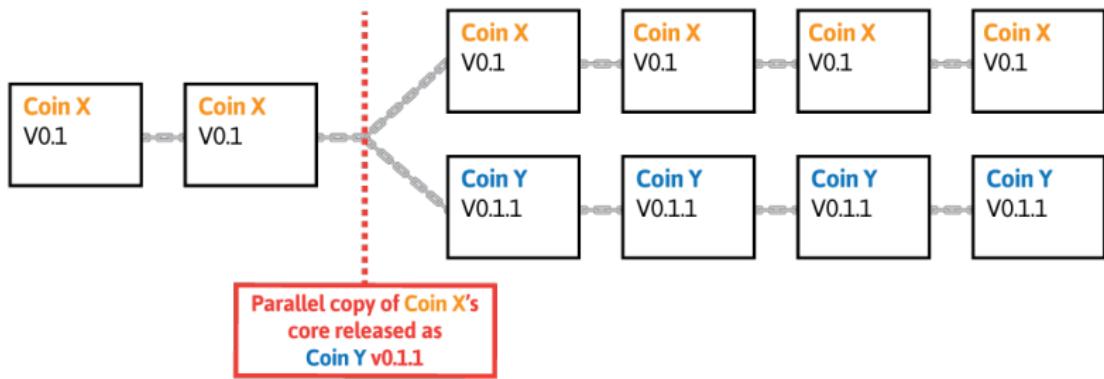
Vitesse de traitement des transactions



Jeux d'instructions limités



Hard-forks



Sommaire

1. Introduction

- Notions de départ
- Les types d'utilisateurs des Blockchain

2. Bitcoin : Blockchain de 1^{re} génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Quel est le problème résolu
- Les limites

3. Perspectives

- Perspectives

Naissance d'une techno

qui réunie

mais qui pourrait être plus efficace