



# LOCKCHAINS et cryptomonnaies

## Partie 2 : Comment ça marche?

└ Introduction

  └ Notions de départ

# Sommaire

## 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

## 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- Solutions techniques
- Les limites

## 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

## └ Introduction

## └ Notions de départ

# Notions de départ

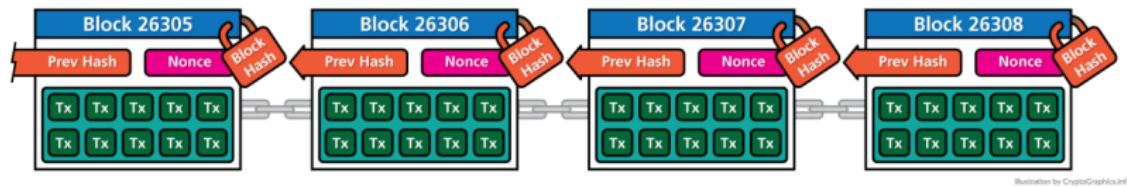


Illustration by CryptoGraphics.info

## Token-économie

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

## Blockchain

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

└ Introduction

  └ Qui utilise la Blockchain

# Sommaire

## 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

## 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- Solutions techniques
- Les limites

## 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

└ Introduction

  └ Qui utilise la Blockchain

## Les rôles sur la blockchain

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

# Sommaire

## 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

## 2. Bitcoin : Blockchain de 1<sup>e</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- Solutions techniques
- Les limites

## 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

*Toute action engendre une réaction (3<sup>e</sup> loi de Newton)*

└ Bitcoin : Blockchain de 1<sup>re</sup> génération

└ La Naissance du Bitcoin

## La Naissance du Bitcoin

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.

Cyber-Anarchisme



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

  └ La Naissance du Bitcoin

# La Naissance du Bitcoin

## Cypherpunk (Hal Finney)



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



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

  └ Que vaut la blockchain ?

## Sommaire

### 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

### 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- Solutions techniques
- Les limites

### 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

└ Bitcoin : Blockchain de 1<sup>re</sup> génération

└ Que vaut la blockchain ?

## Que vaut la blockchain ?



2009

???

SSL/TLS - 1996



1998

HTTP - 1990



1995

TCP/IP - 1974



1984

Ethernet - 1974



1979

Cela dépendra de son utilité

└ Bitcoin : Blockchain de 1<sup>re</sup> génération

  └ Historique du cours du Bitcoin

## Sommaire

### 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

### 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- Solutions techniques
- Les limites

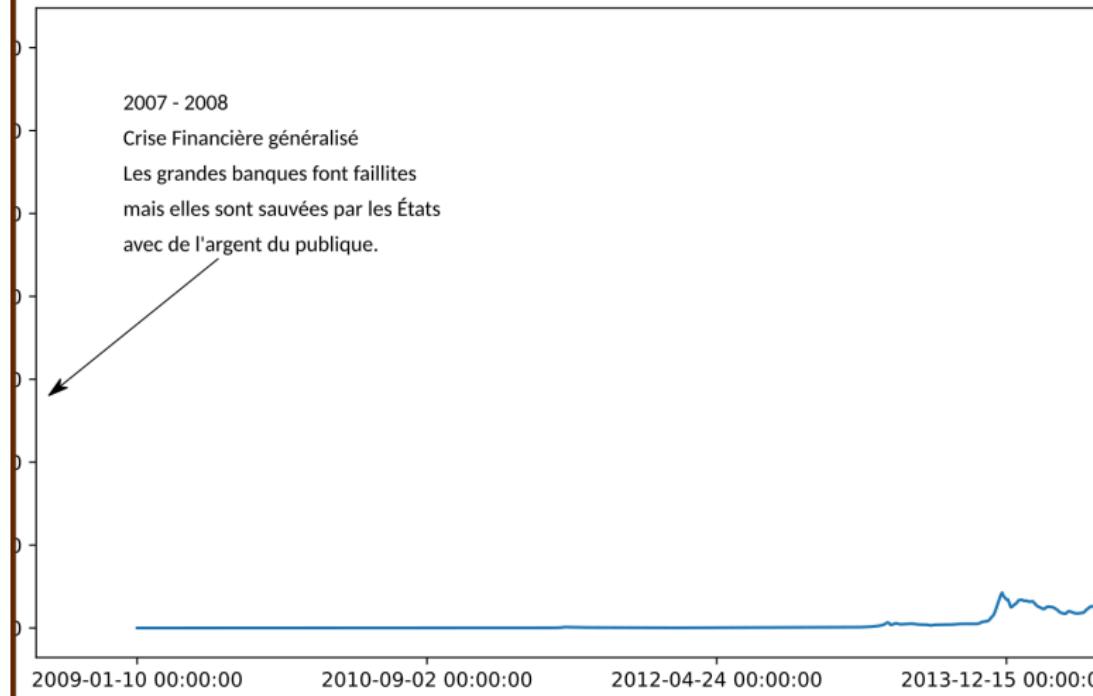
### 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

└ Bitcoin : Blockchain de 1<sup>e</sup>e génération

└ Historique du cours du Bitcoin

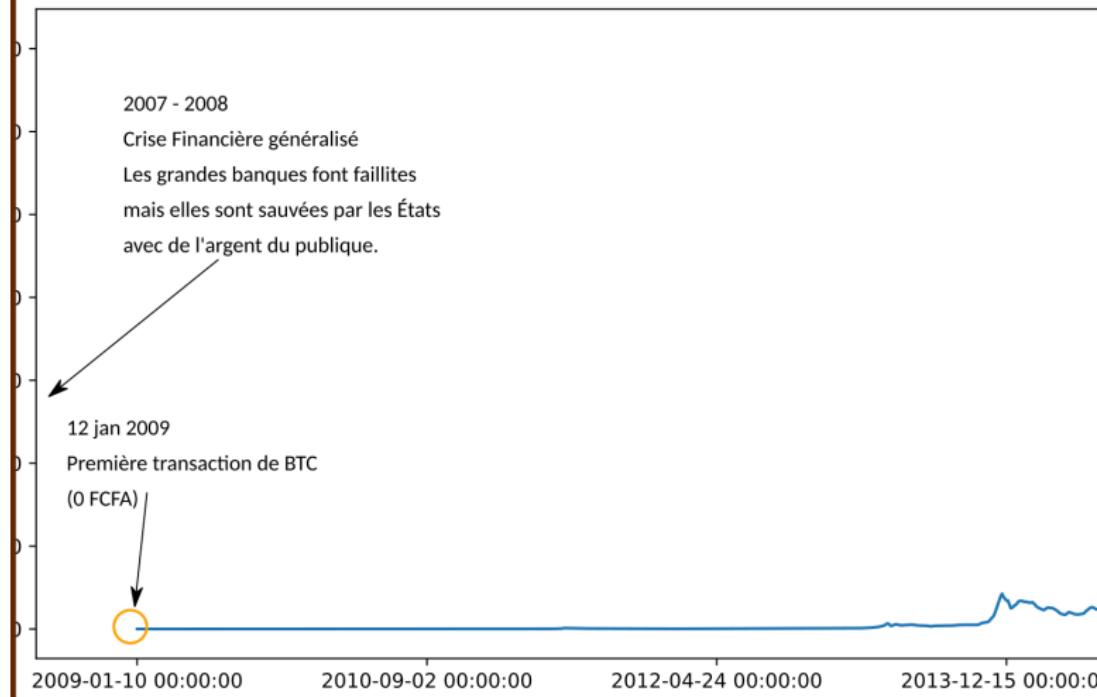
## Les débuts



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

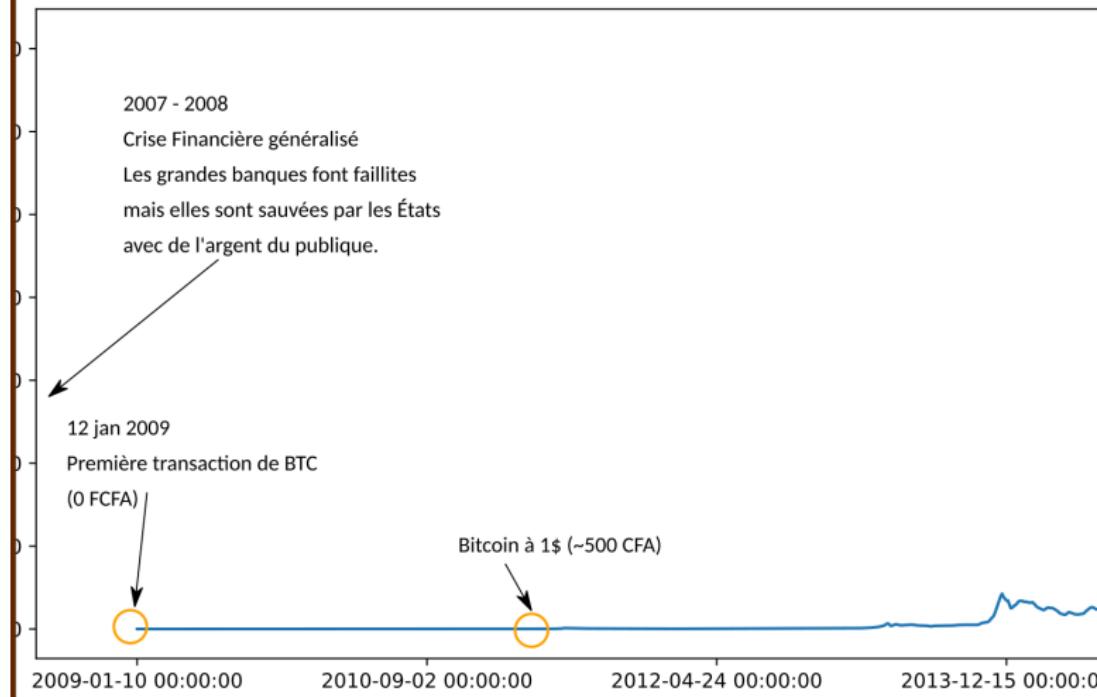
## Les débuts



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

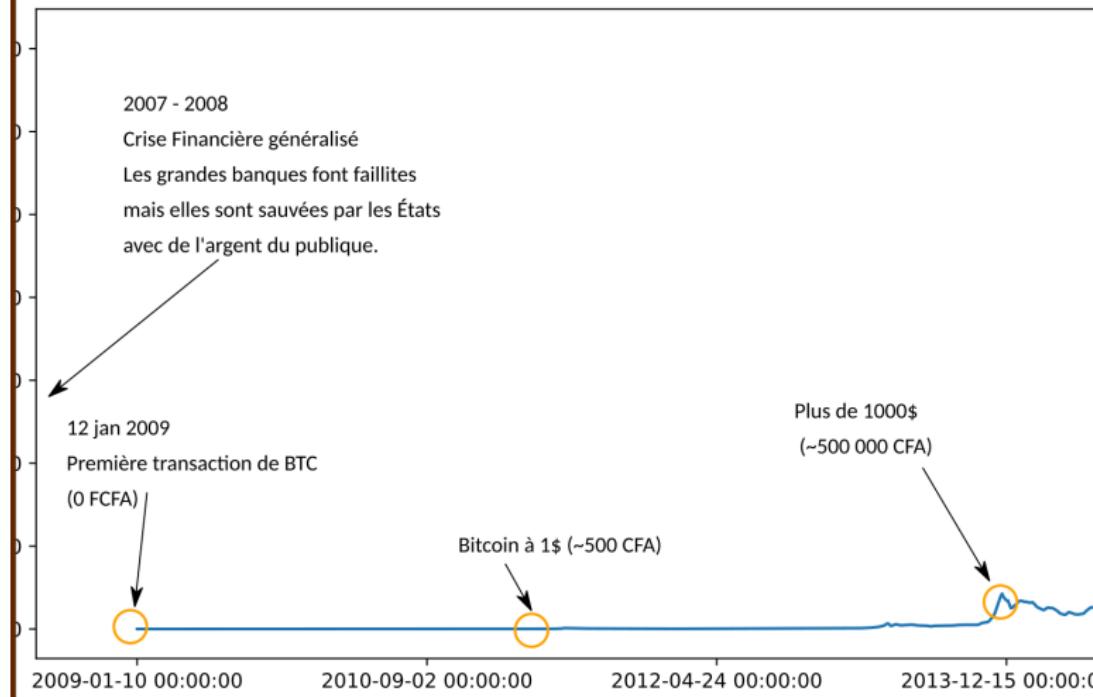
## Les débuts



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

└ Historique du cours du Bitcoin

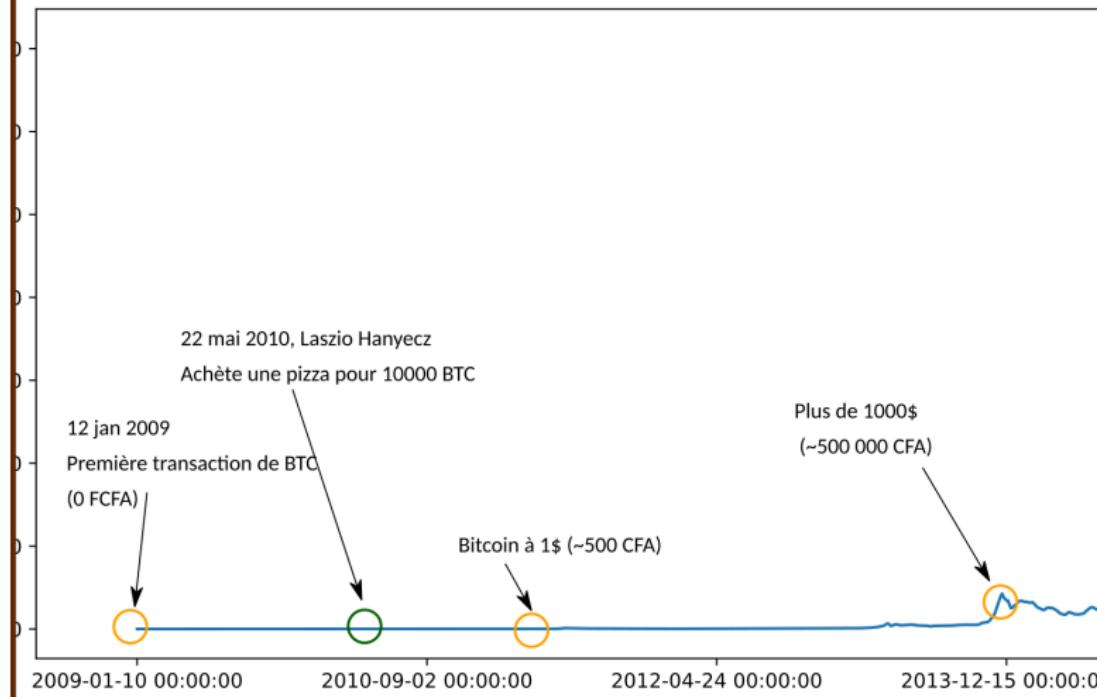
## Les débuts



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

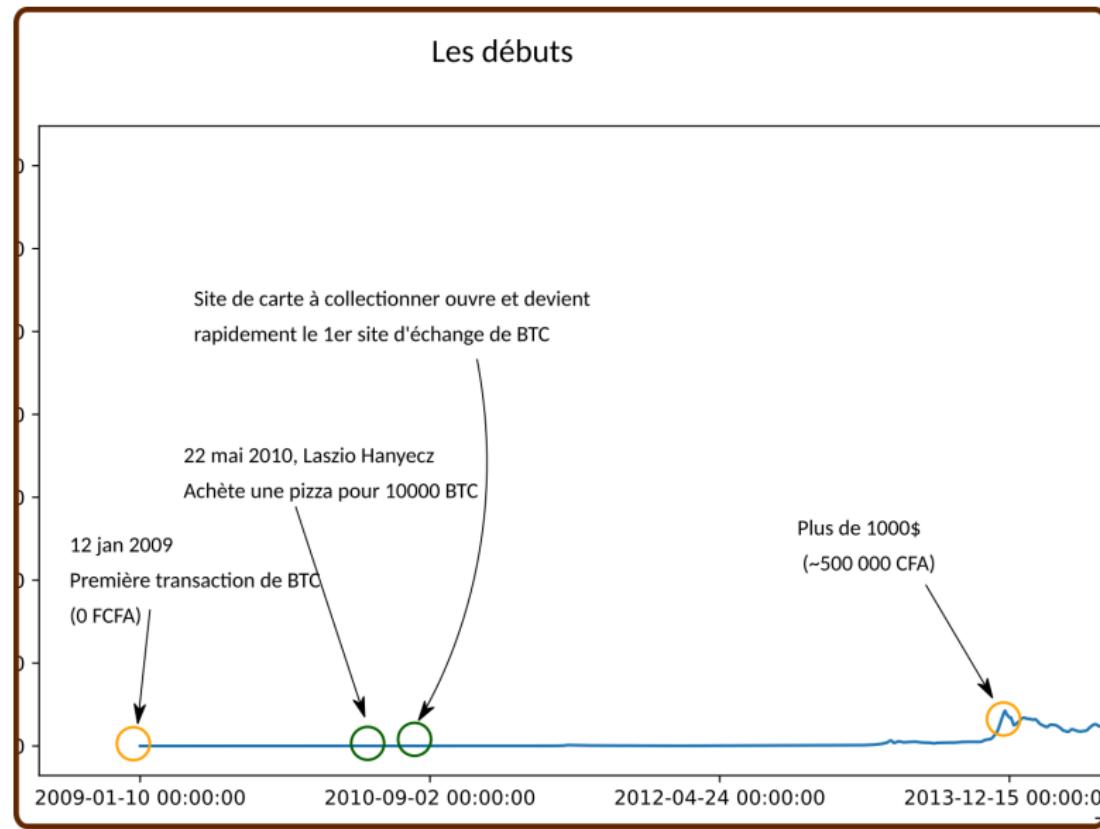
└ Historique du cours du Bitcoin

## Les débuts



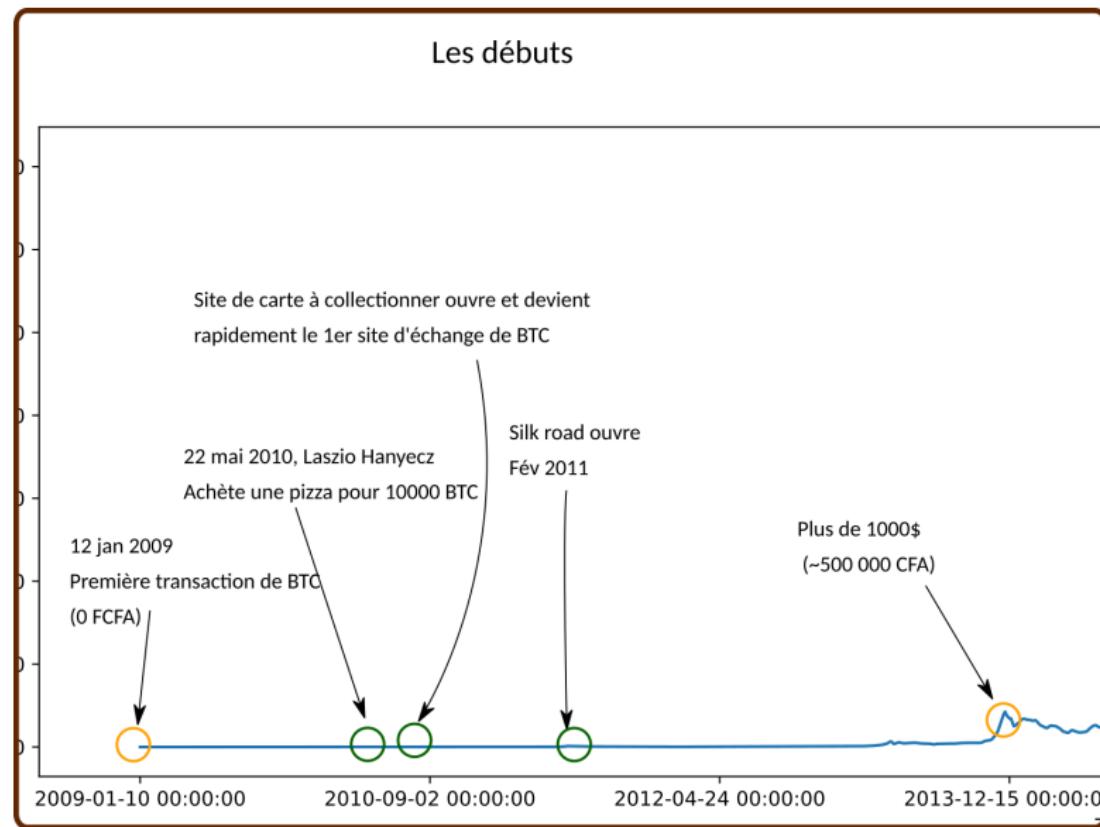
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin



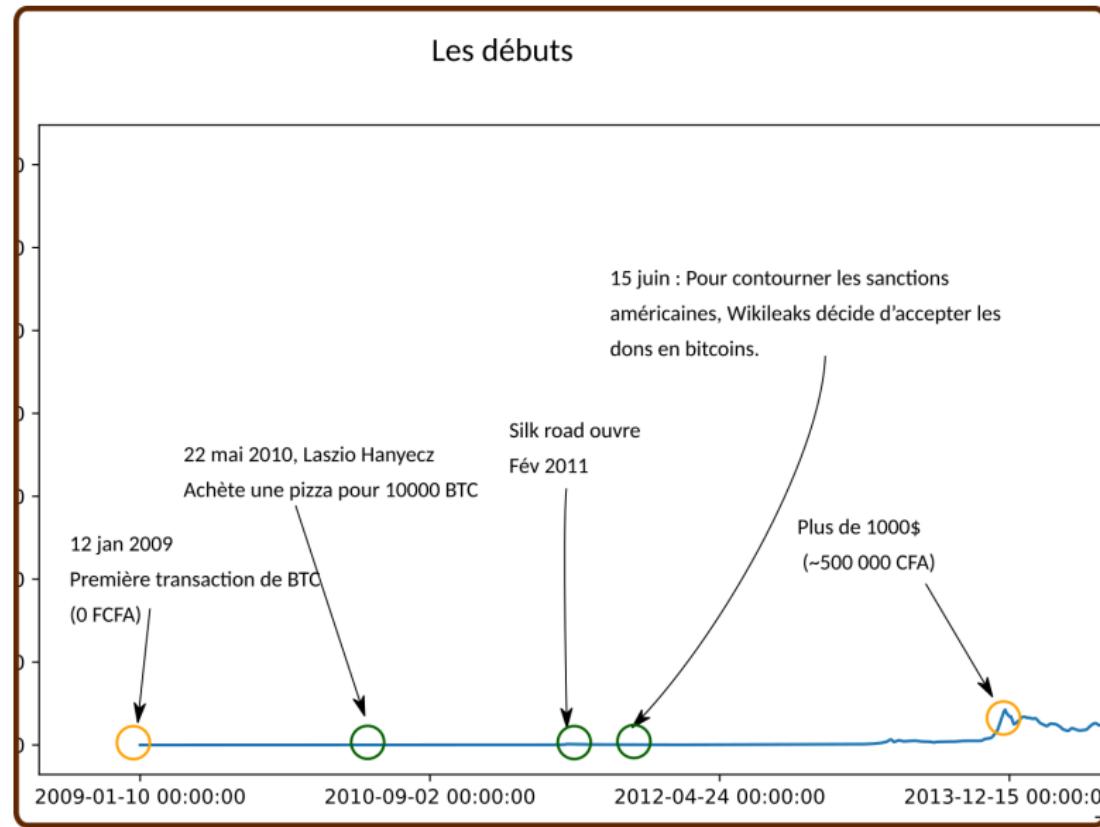
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

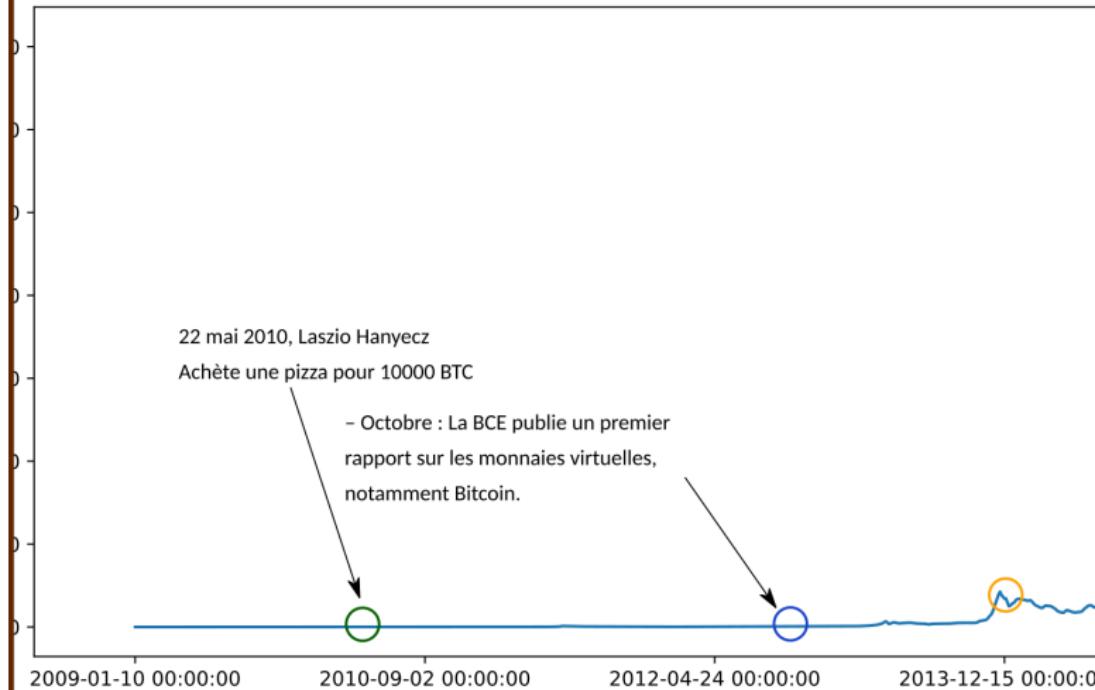
## └ Historique du cours du Bitcoin



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

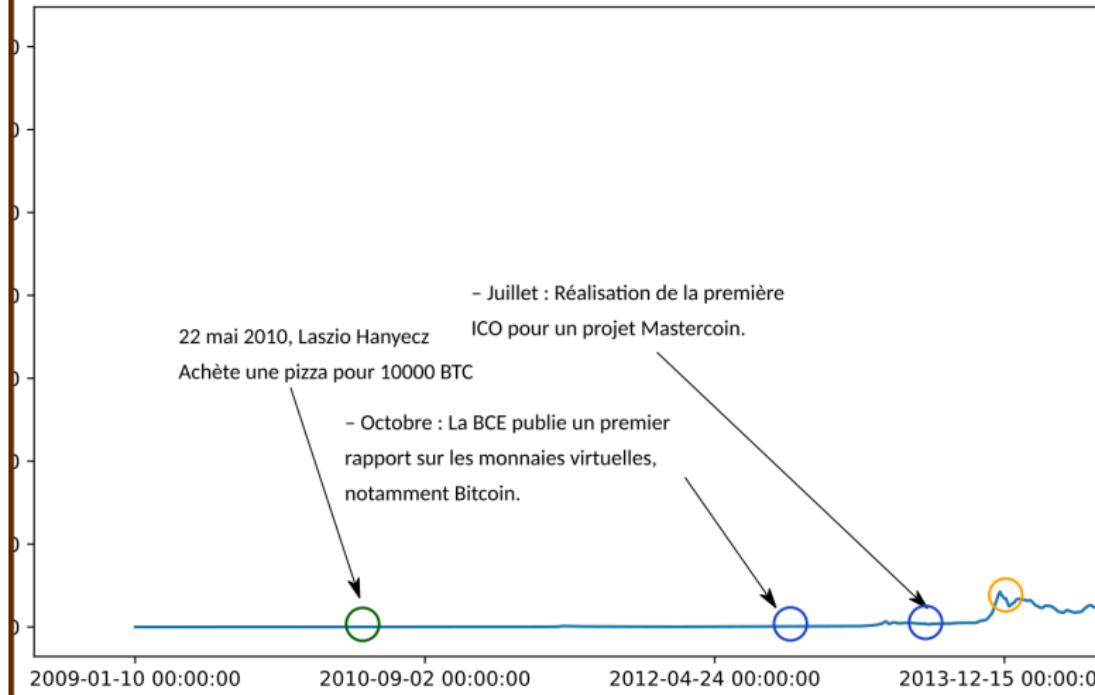
## Les débuts



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

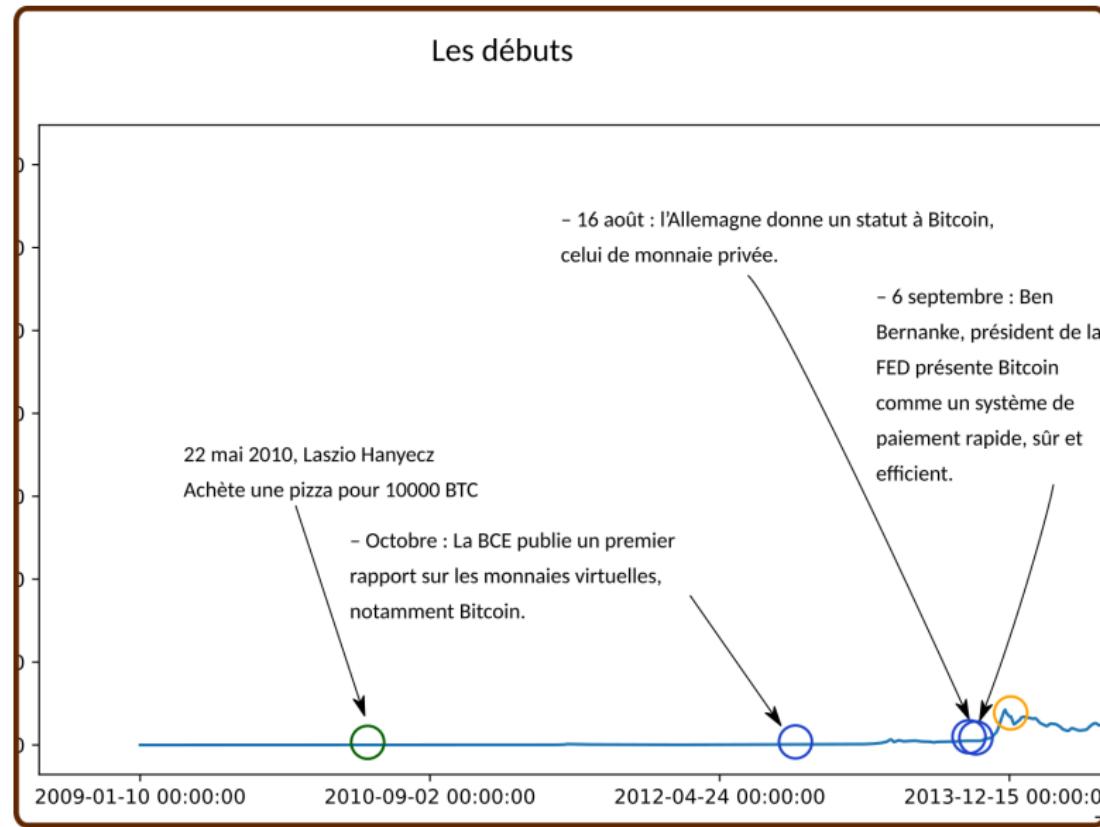
## └ Historique du cours du Bitcoin

## Les débuts



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

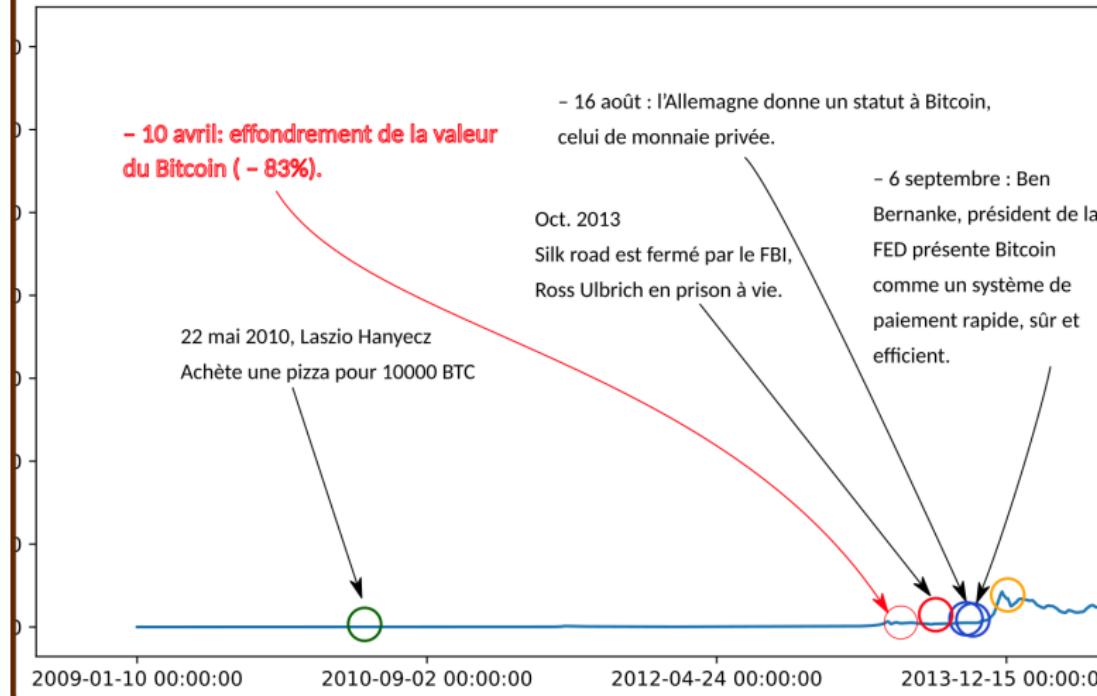
## └ Historique du cours du Bitcoin



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

## Les débuts



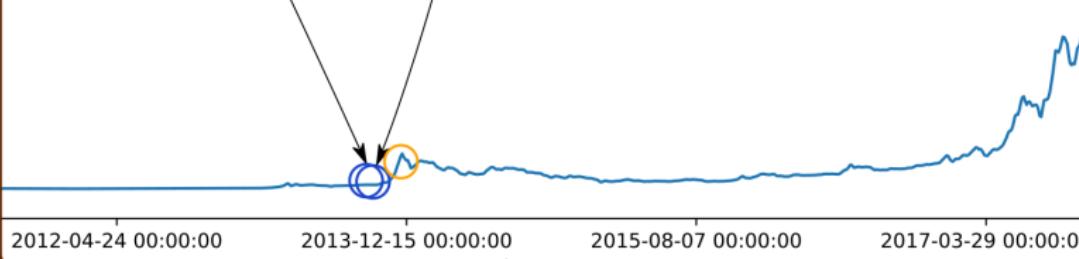
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

## 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.

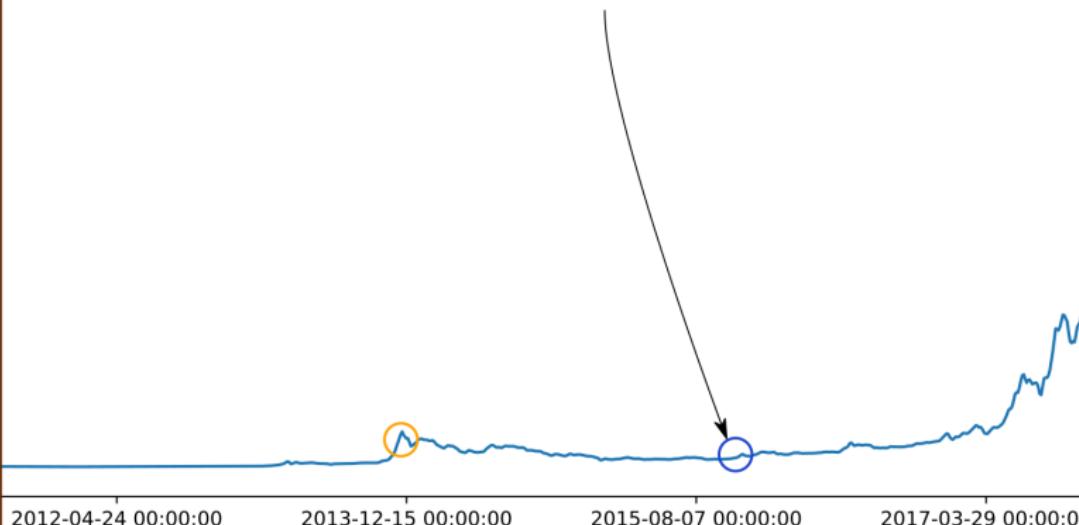


└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

## Adoption

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



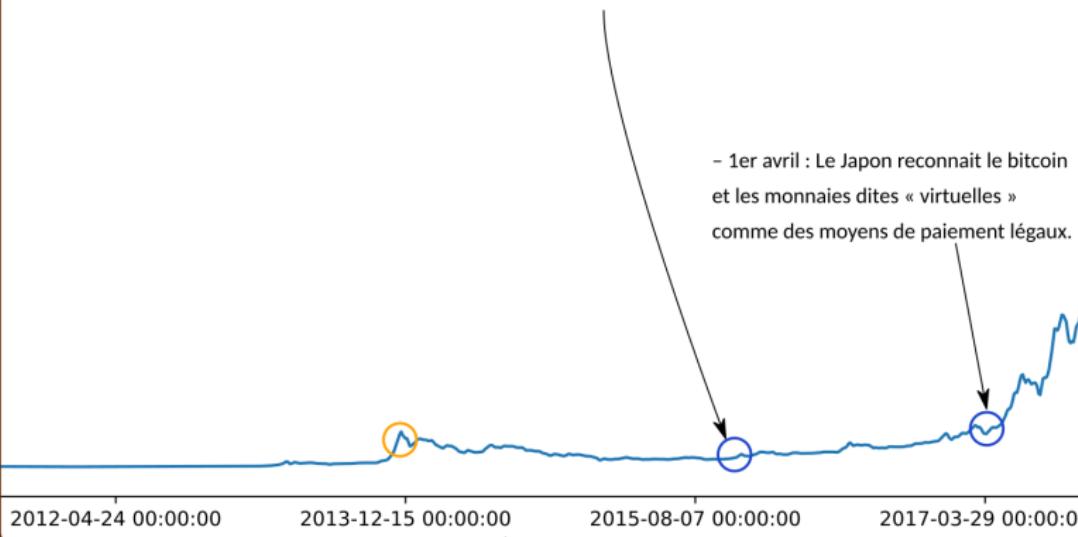
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

## Adoption

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

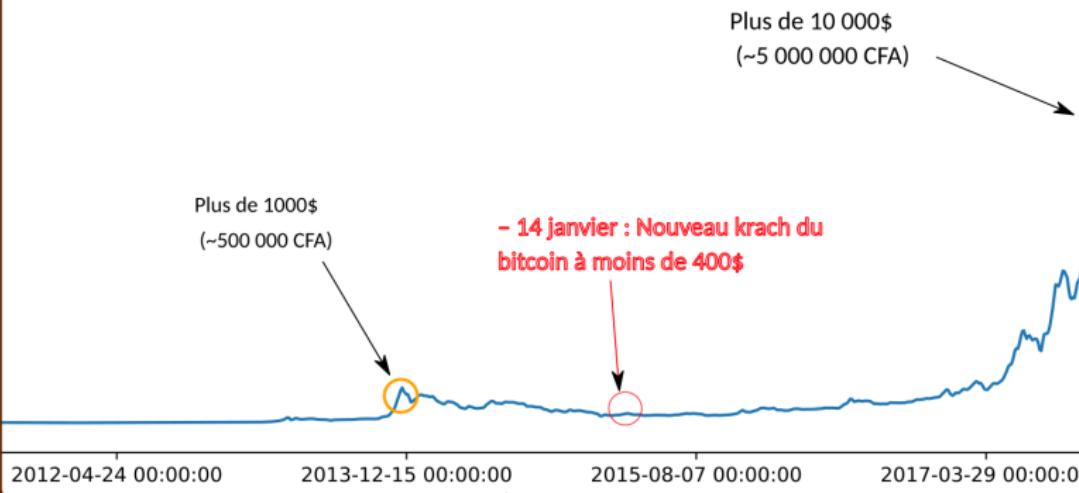
- 1er avril : Le Japon reconnaît le bitcoin et les monnaies dites « virtuelles » comme des moyens de paiement légaux.



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

## Adoption

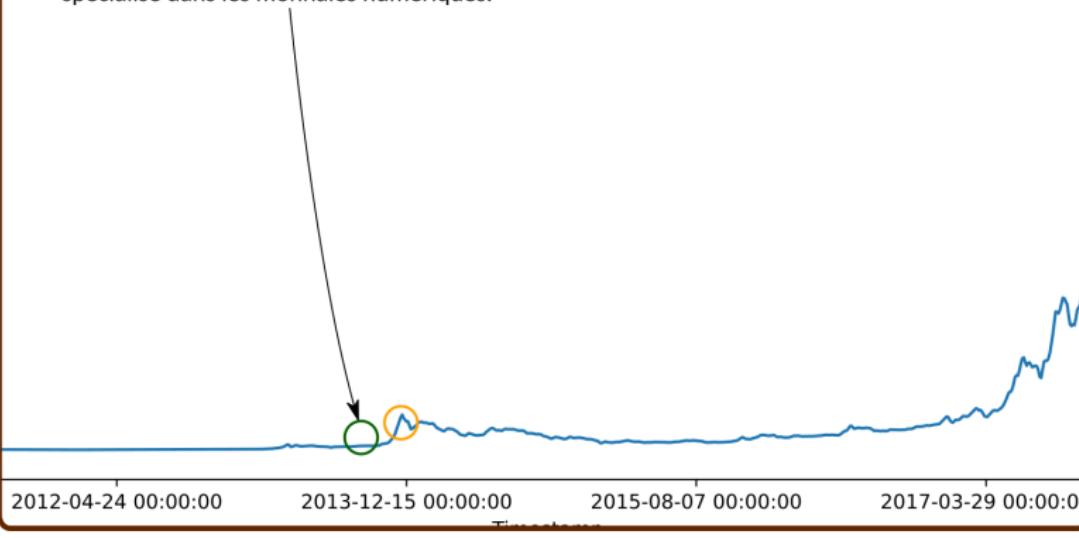


└ Bitcoin : Blockchain de 1<sup>re</sup> génération

└ Historique du cours du 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.



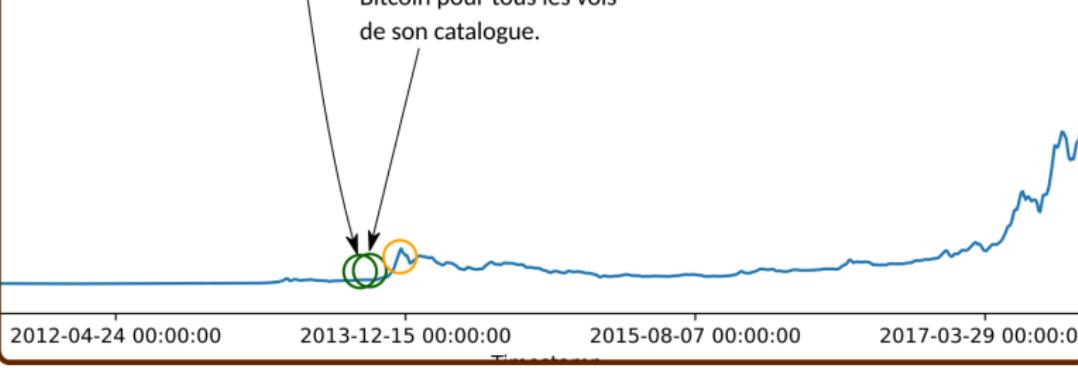
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du 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.

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



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du 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.

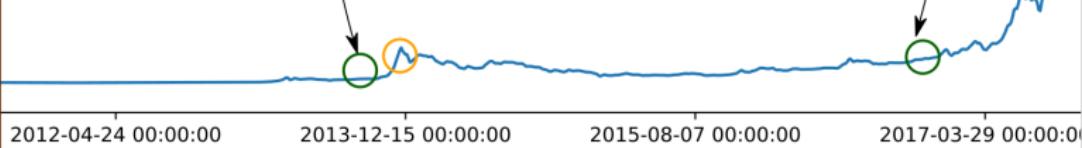
- 29 mai : le fournisseur américain de services par satellite Dish devient la plus grande entreprise au monde à accepter Bitcoin



## 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.



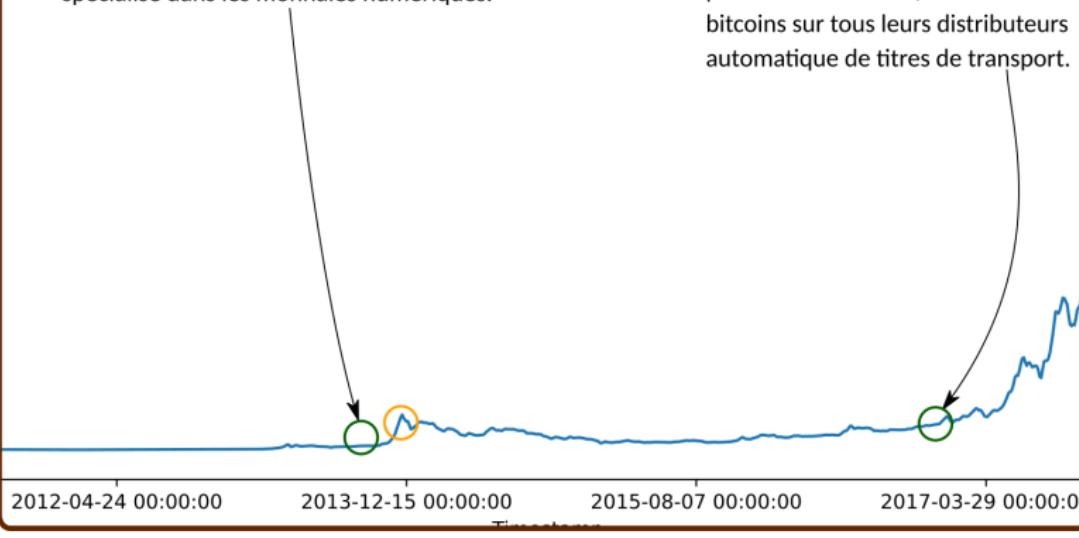
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

## Adoption

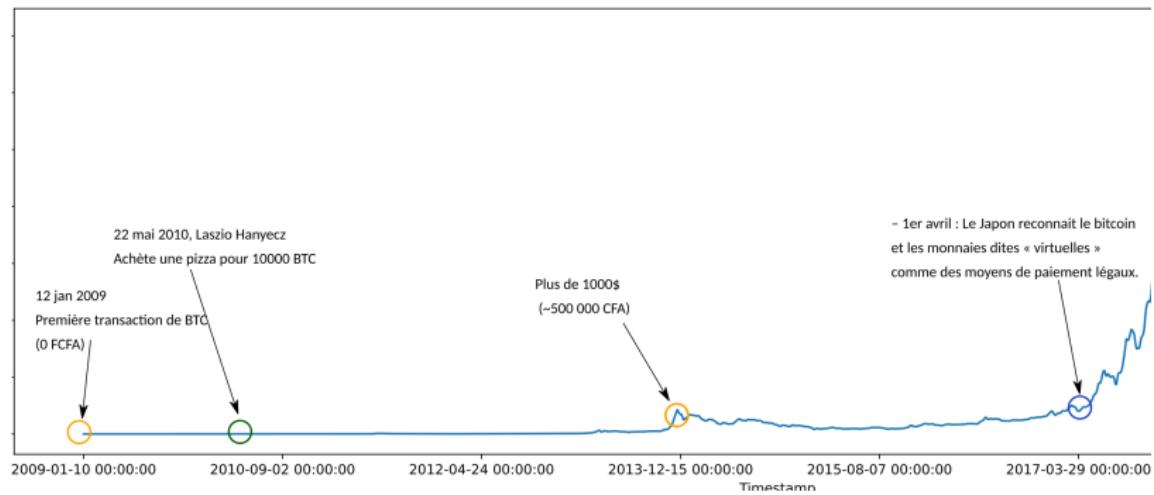
- 21 novembre : L'Université de Nicosie accepte que les frais de scolarité soient payés en bitcoins et annonce l'ouverture d'un Master de sciences économiques spécialisé dans les monnaies numériques.

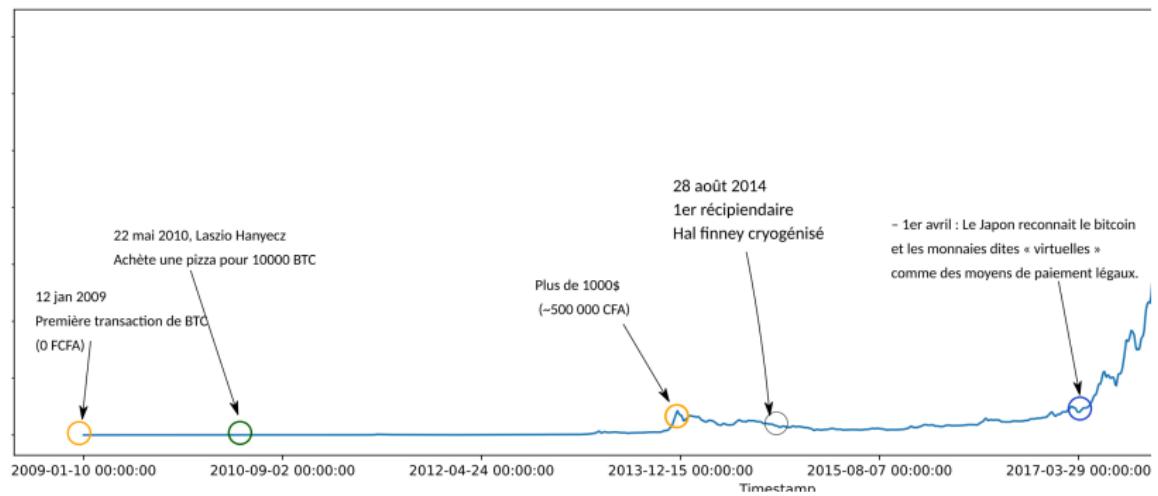
- 11 novembre : Les Chemins de fer fédéraux suisses testent, pour une période de deux ans, la vente de bitcoins sur tous leurs distributeurs automatique de titres de transport.



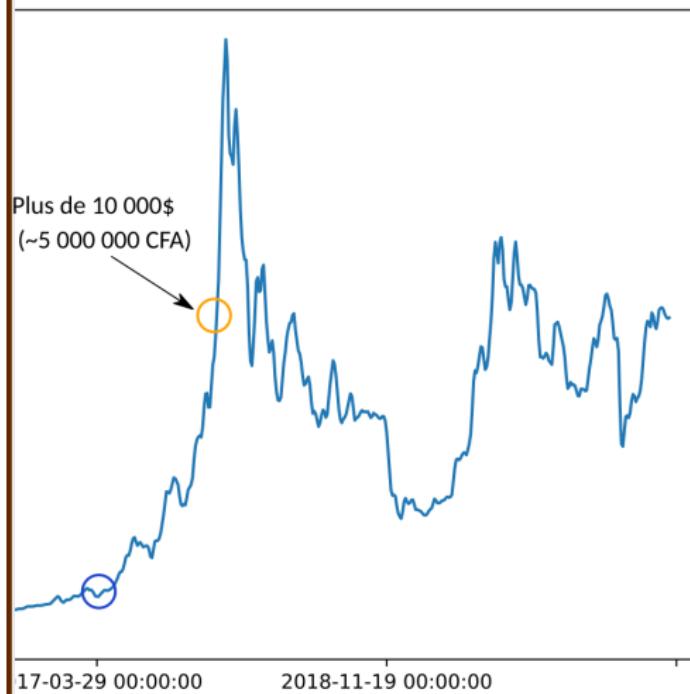
└ Bitcoin : Blockchain de 1<sup>e</sup>e génération

## └ Historique du cours du Bitcoin



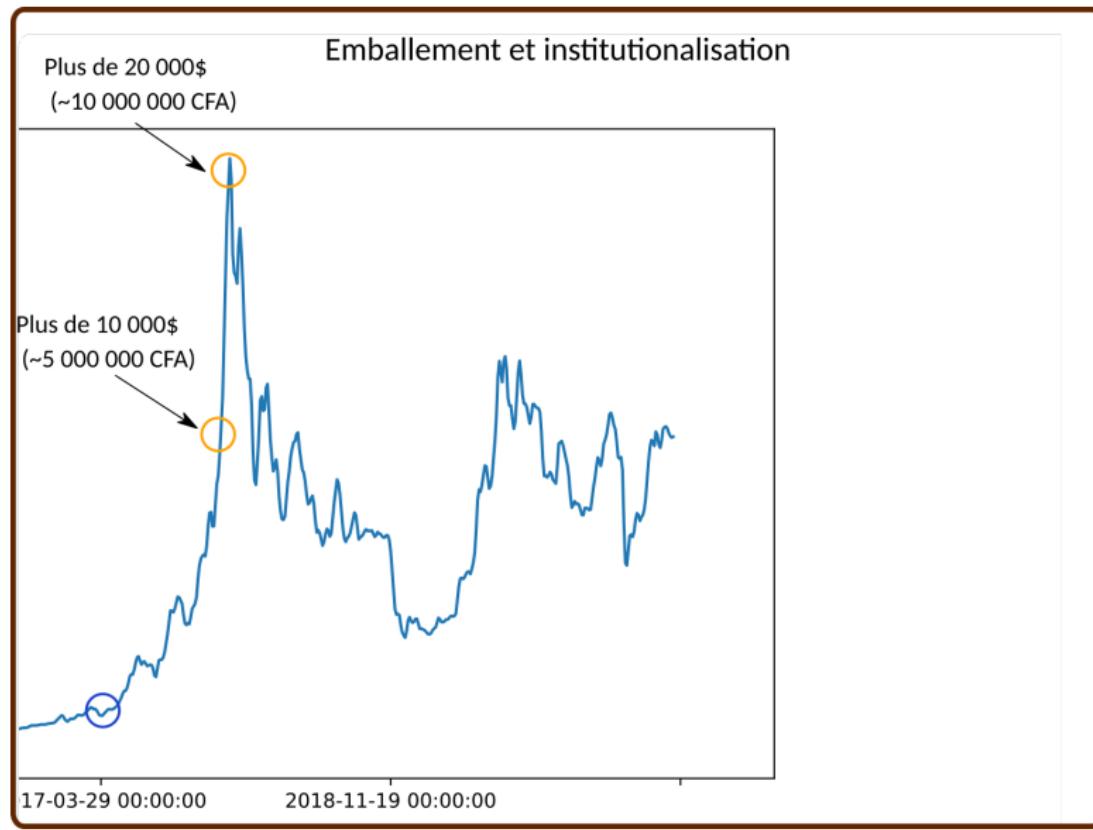


### Emballage et institutionalisation



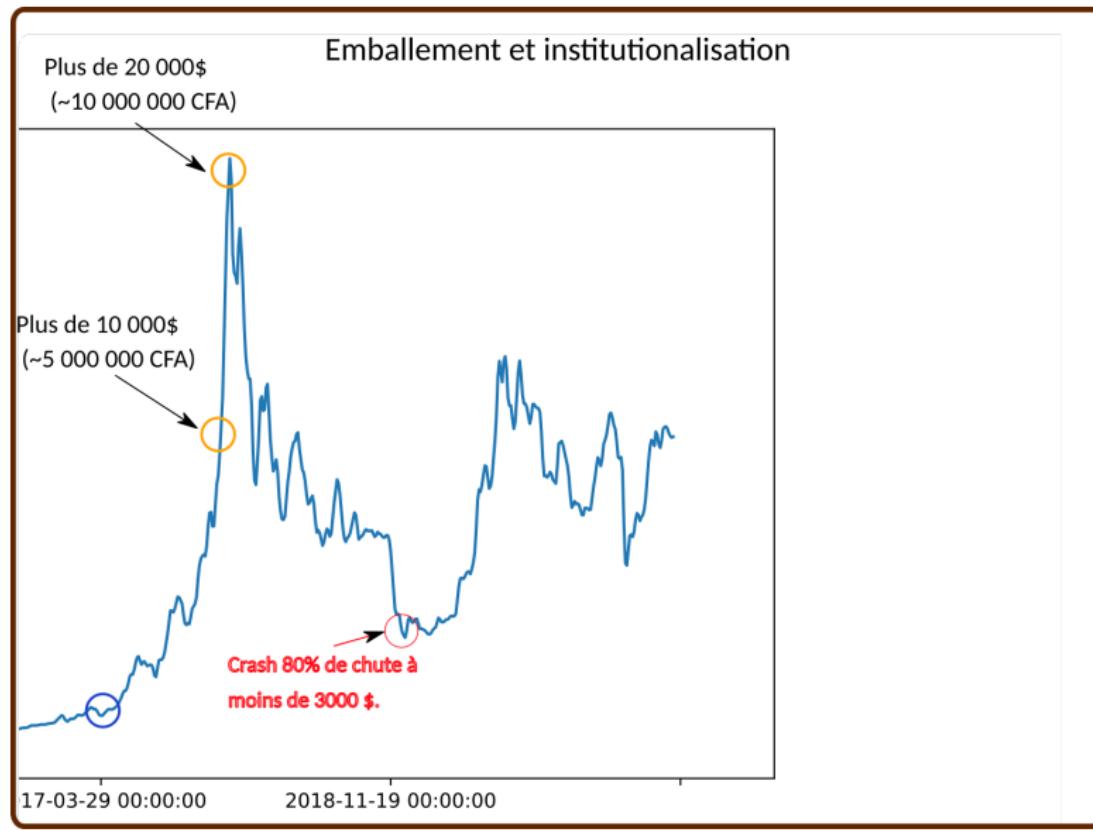
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin



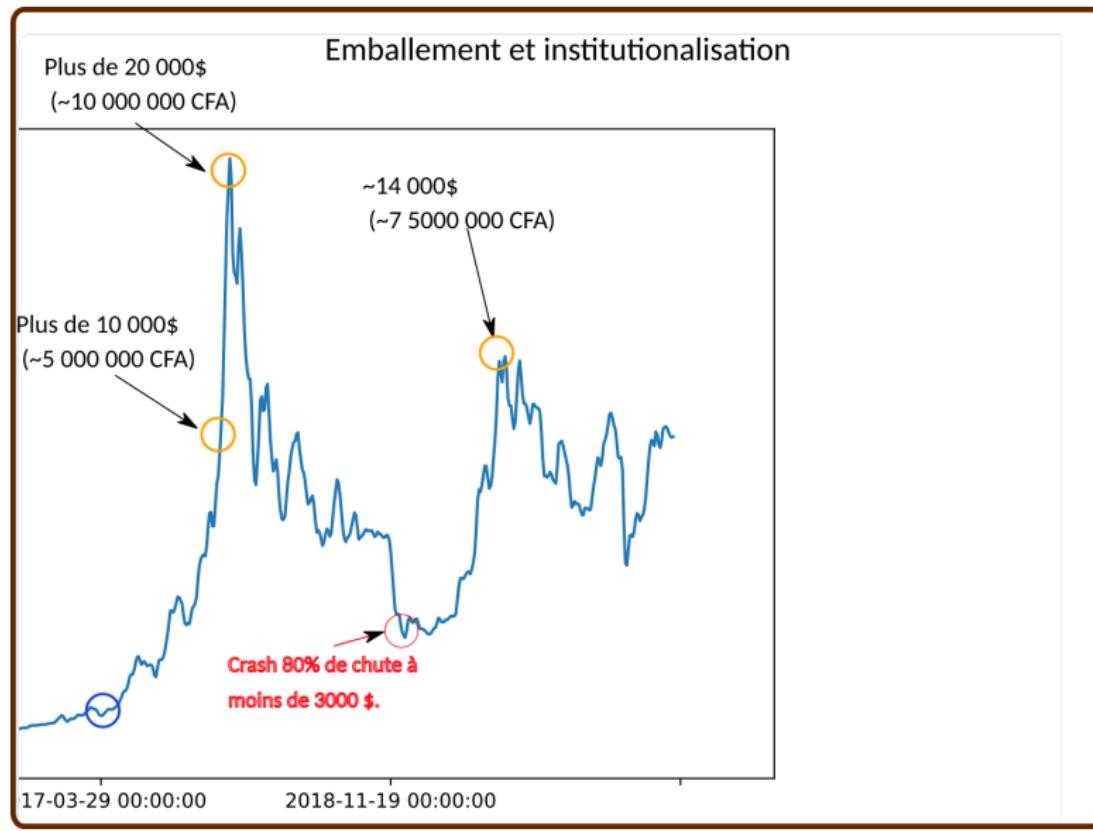
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin



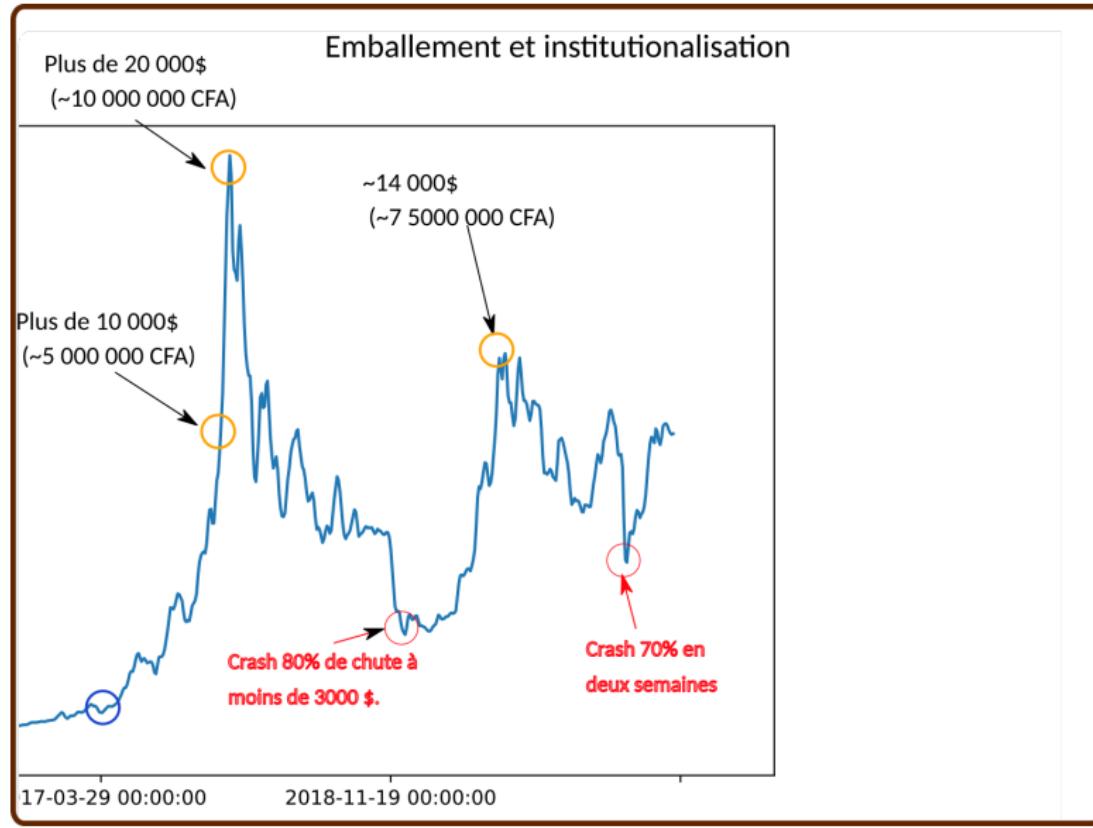
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin



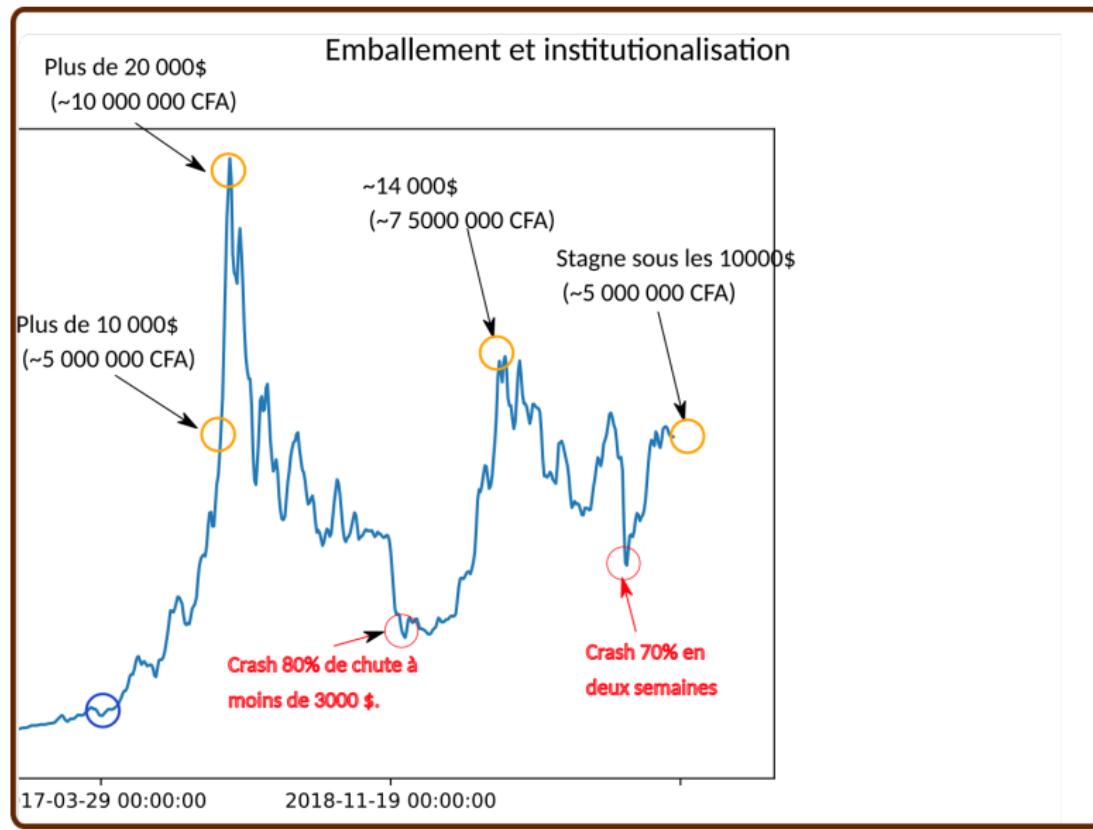
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

## Emballage et institutionalisation

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



└ Bitcoin : Blockchain de 1<sup>e</sup>e génération

## └ Historique du cours du Bitcoin

## Emballage et institutionalisation

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

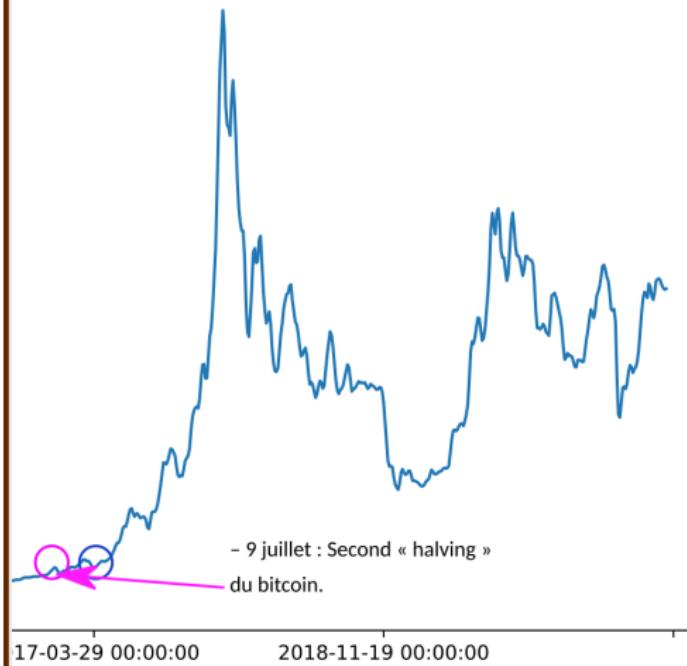


- 1er octobre : Une commission d'enquête sénatoriale plaide en faveur du déploiement d'une cryptomonnaie banque centrale.

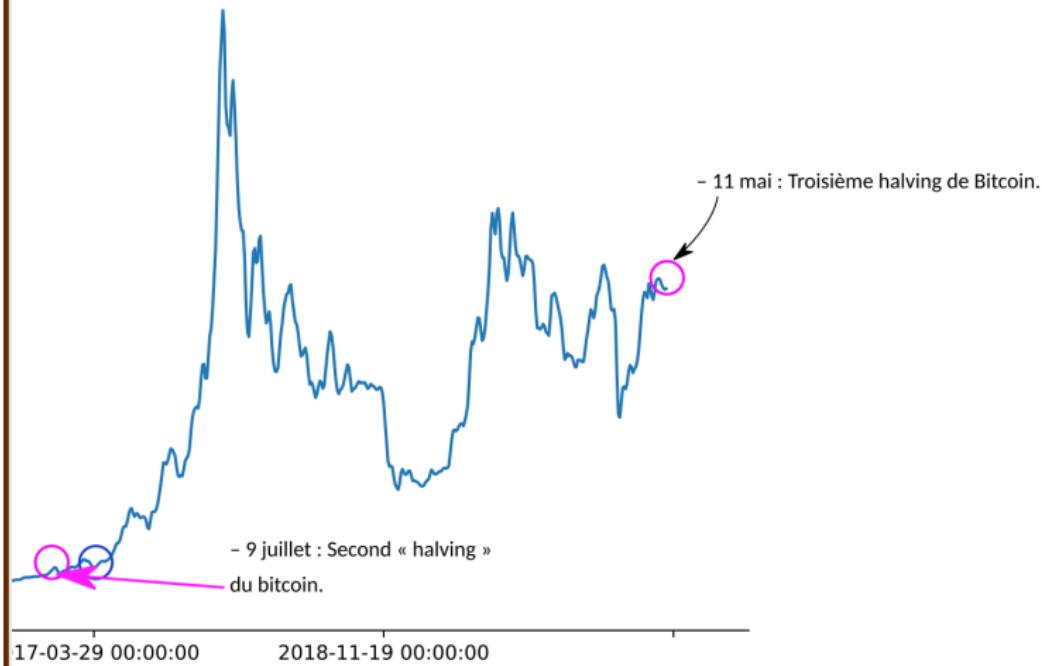
└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin

## Emballage et institutionalisation

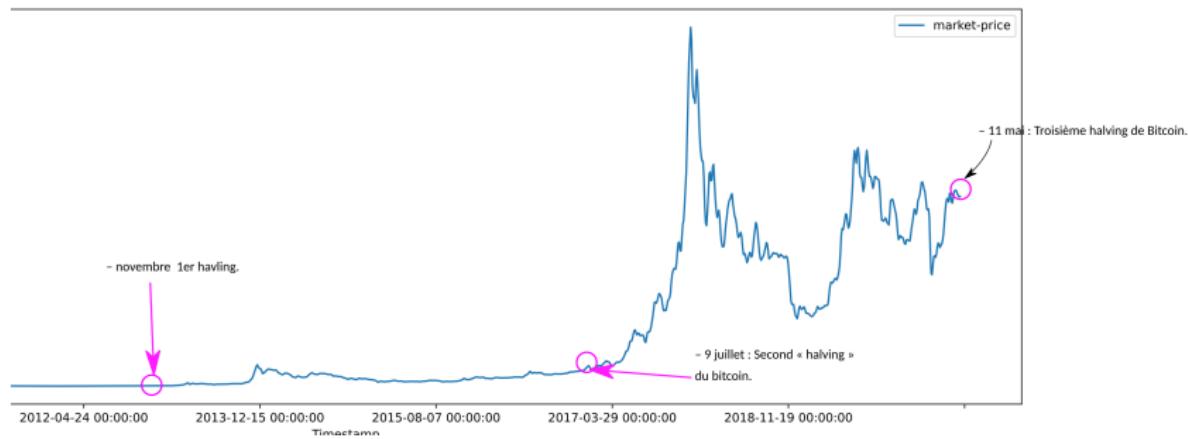


## Emballage et institutionalisation



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Historique du cours du Bitcoin



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

  └ Un problème de taille

## Sommaire

### 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

### 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- **Un problème de taille**
- Solutions techniques
- Les limites

### 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

└ Bitcoin : Blockchain de 1<sup>re</sup> génération

  └ Un problème de taille

## Un problème de taille

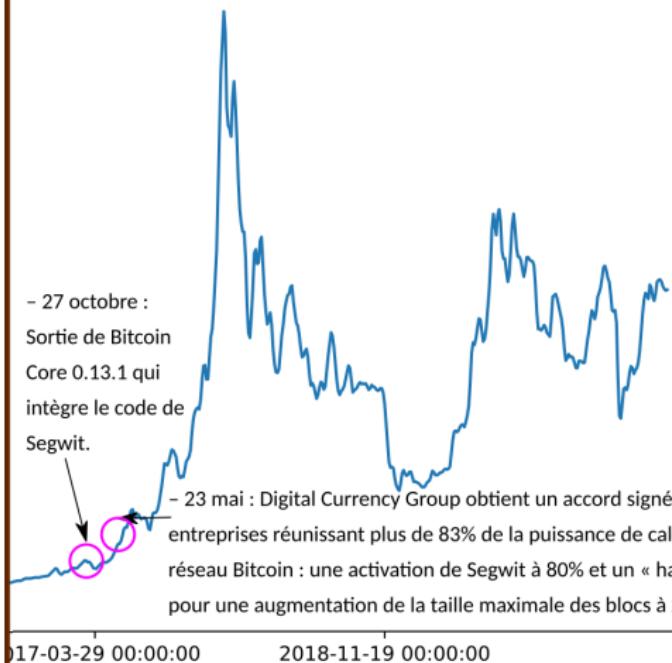
Il faut calculer

- ▶ hashrate : puissance de calcul (Tera = mille milliard)
- ▶ Transaction en attente (memepool)
- ▶ Frais de transaction

└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Un problème de taille

## Emballage et institutionalisation



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Un problème de taille

## Emballage et institutionalisation

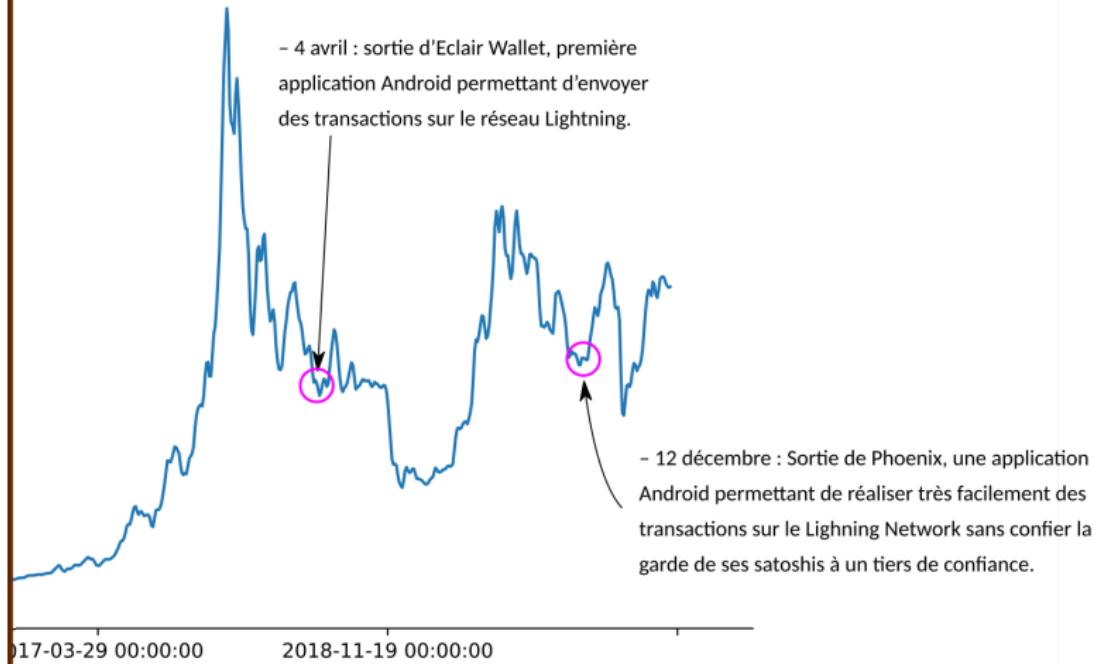
- 4 avril : sortie d'Eclair Wallet, première application Android permettant d'envoyer des transactions sur le réseau Lightning.



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Un problème de taille

## Emballage et institutionalisation



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Un problème de taille

## Emballage et institutionalisation



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Un problème de taille

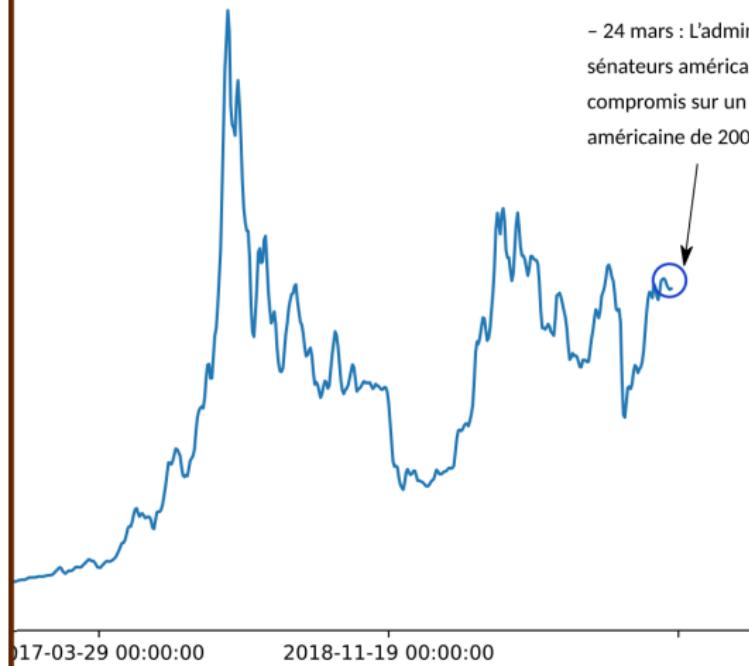
## Emballage et institutionalisation



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

## └ Un problème de taille

## Emballage et institutionalisation



└ Bitcoin : Blockchain de 1<sup>re</sup> génération

└ Un problème de taille

et aujourd'hui ?

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

# Sommaire

## 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

## 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

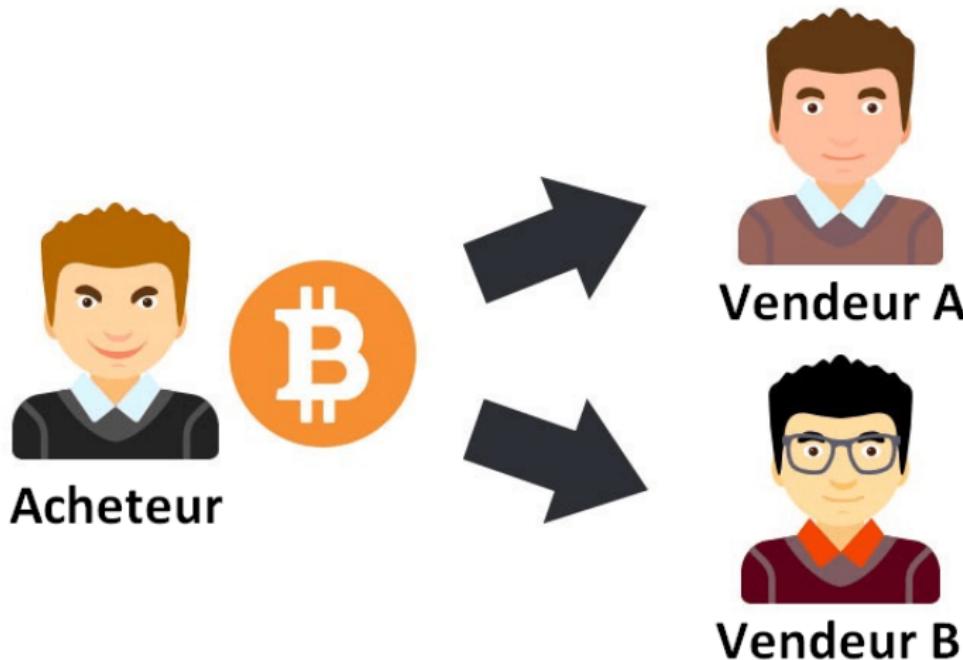
- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- **Solutions techniques**
- Les limites

## 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

## L'obstacle principal

### La double dépense



## Comment le problème est-il résolu ?

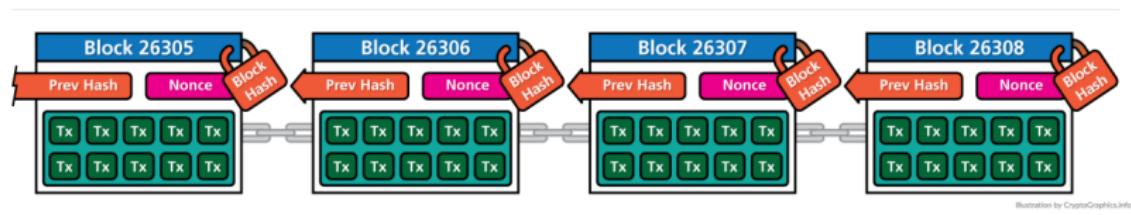
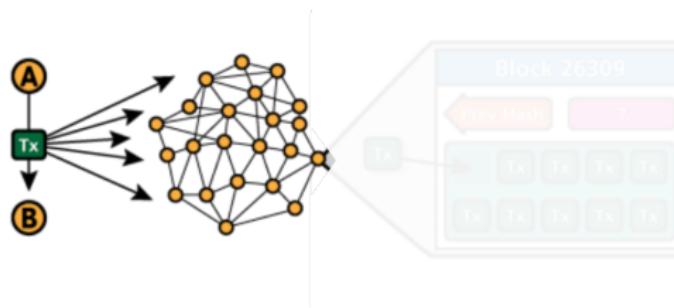


Illustration by CryptoGraphics.info

avec un journal comptable d'enregistrements,

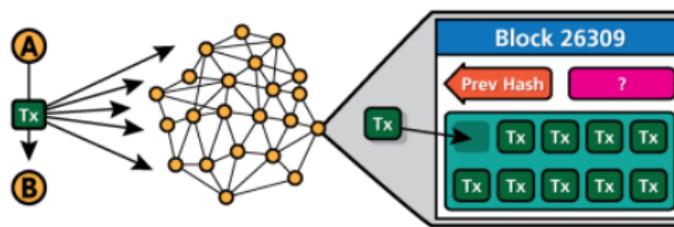
- ▶ organisés en blocks **infalsifiables**
- ▶ qui s'**enchainent** les uns aux autres,
- ▶ de façon unique,
- ▶ dans un réseau **public et décentralisé**.

## Plus techniquement comment cela fonctionne ?



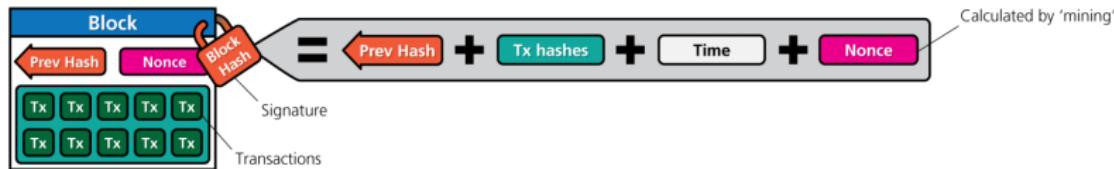
Tx : ".00012300 BTC pour Binta, signé Amadou"

## Plus techniquement comment cela fonctionne ?



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

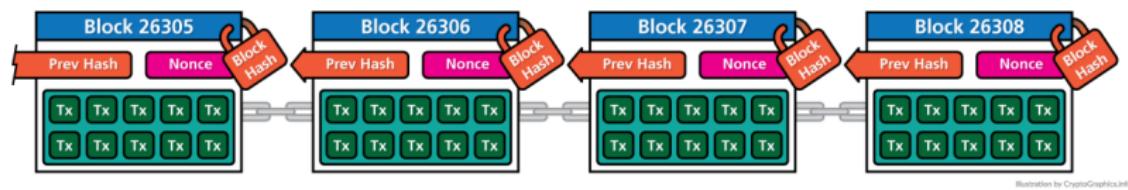
## Plus techniquement comment cela fonctionne ?



Le 1<sup>er</sup> mineur à trouver un **bon nonce**, publie le bloc

- ▶ il contient une récompense (*coinbase*)

## Plus techniquement comment cela fonctionne ?



Les autres mineurs :

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

ça marche !



- ▶ 18/05/2010, les Pizza à  $10^{~000}$  BTC de Laslo  
(bitcointalk.org)

└ Bitcoin : Blockchain de 1<sup>re</sup> génération

  └ Les limites

## Sommaire

### 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

### 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- Solutions techniques
- **Les limites**

### 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

- └ Bitcoin : Blockchain de 1<sup>re</sup> génération
- └ Les limites

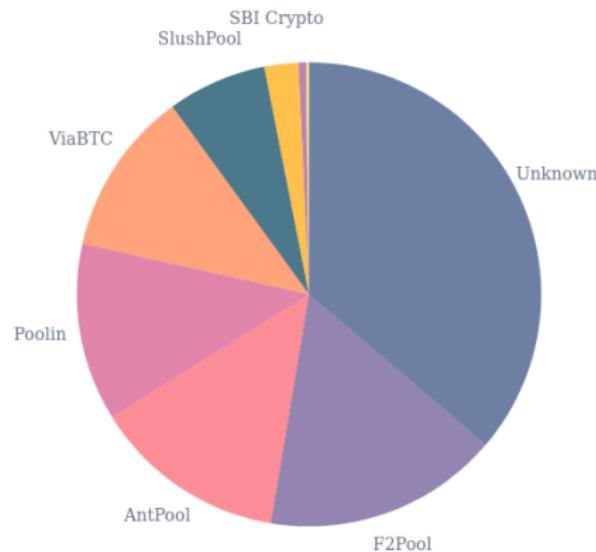
## Limites de la blockchain bitcoin 1/4

### Coût énergétique



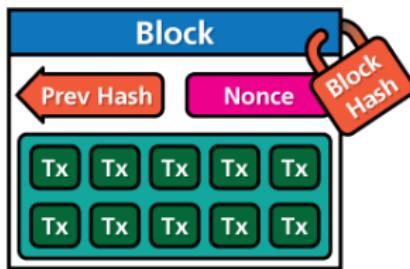
## Limites de la blockchain bitcoin 2/4

### Concentration du hashrate (juin 2021)



## Limites de la Blockchain bitcoin 3/4

### Vitesse de traitement des transactions



**Tx** = 200 transactions

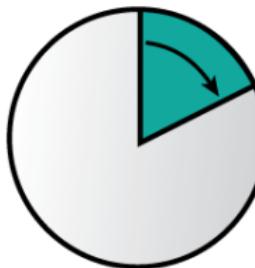
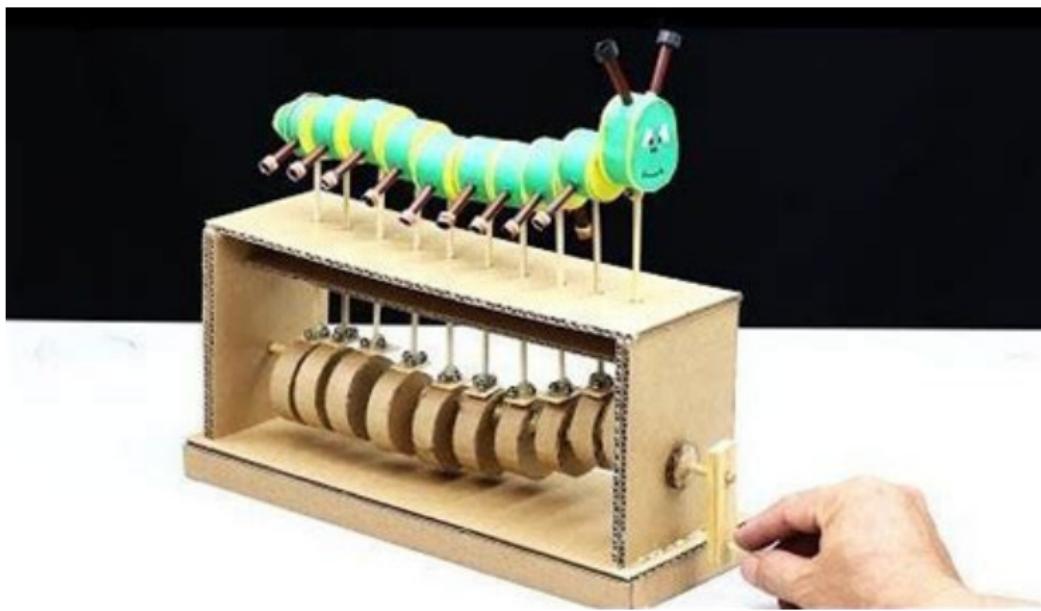


Illustration by CryptoGraphics.info

## Limites de la Blockchain bitcoin 4/4

Jeux d'instructions limités



└ Les améliorations

└ Ethereum : Blockchain de 2<sup>e</sup> génération

## Sommaire

### 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

### 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- Solutions techniques
- Les limites

### 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

└ Les améliorations

└ Ethereum : Blockchain de 2<sup>e</sup> génération

## Blockchain de 2<sup>e</sup> génération : Etherum

*Un système d'exploitation décentralisé*



└ Les améliorations

└ Ethereum : Blockchain de 2<sup>e</sup> génération

# Applications décentralisées (smart contracts)

## Services financiers décentralisés (DeFi)

- ▶ Financements participatifs
- ▶ Marchés de pairs à pairs
- ▶ Paiements internationaux
- ▶ Objets connectés
- ▶ Monnaies dirigées



└ Les améliorations

└ Ethereum : Blockchain de 2<sup>e</sup> génération

## Les limites d'Etherum

- ▶ Pas assez sécurisé
- ▶ Coûteux
- ▶ Difficile à améliorer



└ Les améliorations

└ Cardano : Blockchain de 3<sup>e</sup> génération

## Sommaire

### 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

### 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- Solutions techniques
- Les limites

### 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

└ Les améliorations

└ Cardano : Blockchain de 3<sup>e</sup> génération

## Blockchain de 3<sup>e</sup> génération

**CARDANO**

*1<sup>er</sup> blockchain scientifique*

The timeline consists of five colored boxes, each containing a portrait and text:

- BYRON**: Foundation. Portait of Lord Byron.
- SHELLEY**: Decentralization. Portait of Percy Bysshe Shelley.
- GOGUEN**: Smart contracts. Portait of Charles Hoskinson.
- BASHO**: Scaling. Portait of a person in a pixelated style.
- VOLTAIRE**: Governance. Portait of Voltaire.

Below each box is a number from 01 to 05, and at the bottom are navigation icons.

└ Les améliorations

└ Cardano : Blockchain de 3<sup>e</sup> génération

## Avantages de Cardano



- ▶ gouvernance
- ▶ sécurité
- ▶ efficience énergétique

└ Les améliorations

└ Conclusion

# Sommaire

## 1. Introduction

- Notions de départ
- Qui utilise la Blockchain

## 2. Bitcoin : Blockchain de 1<sup>re</sup> génération

- La Naissance du Bitcoin
- Que vaut la blockchain ?
- Historique du cours du Bitcoin
- Un problème de taille
- Solutions techniques
- Les limites

## 3. Les améliorations

- Ethereum : Blockchain de 2<sup>e</sup> génération
- Cardano : Blockchain de 3<sup>e</sup> génération
- Conclusion

└ Les améliorations

└ Conclusion

## Proposition d'un Air drop

- ▶ Si vous voulez et quand vous voudrez essayer une cryptomonnaie

Installez Yoroi-wallet

- ▶ depuis app-store (ou autres)
- ▶ remplissez [tinyurl.com/anz5fk](http://tinyurl.com/anz5fk)
- ▶ ou contactez  
malikykone@kone@gmail.com
- ▶ et je vous enverrais des ADA



Merci à tous

