



Lundi 24 juillet



blockchain

Partie 1 : Bitcoin

Sommaire

1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

2. Smart-contract

Cardano : blockchain de 3^e génération

A quoi peuvent servir les smart contract ?

Notions de départ

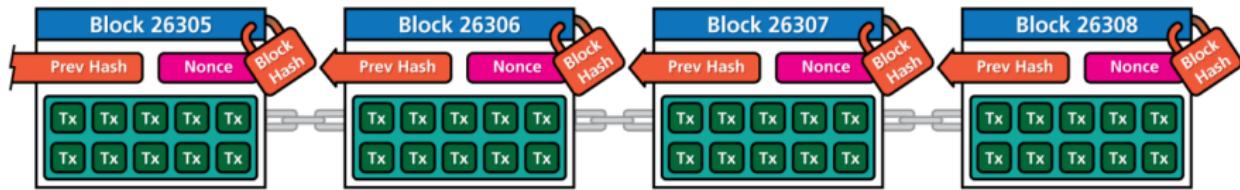


Illustration by CryptoGraphics.info

Blockchain

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

Cryptoéconomie

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

Sommaire

1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

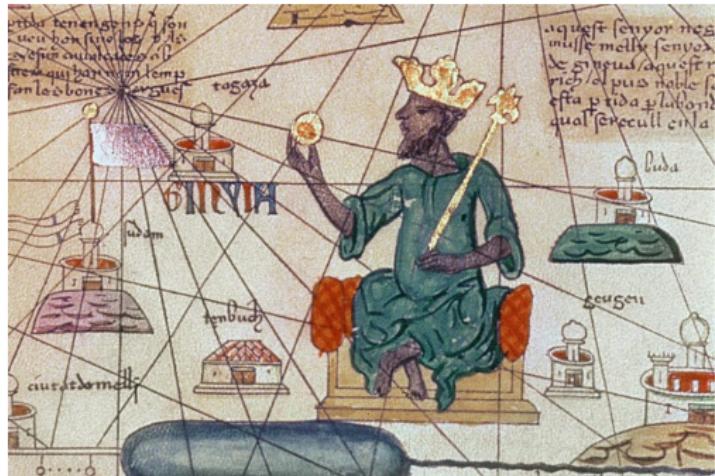
2. Smart-contract

Cardano : blockchain de 3^e génération

A quoi peuvent servir les smart contract ?

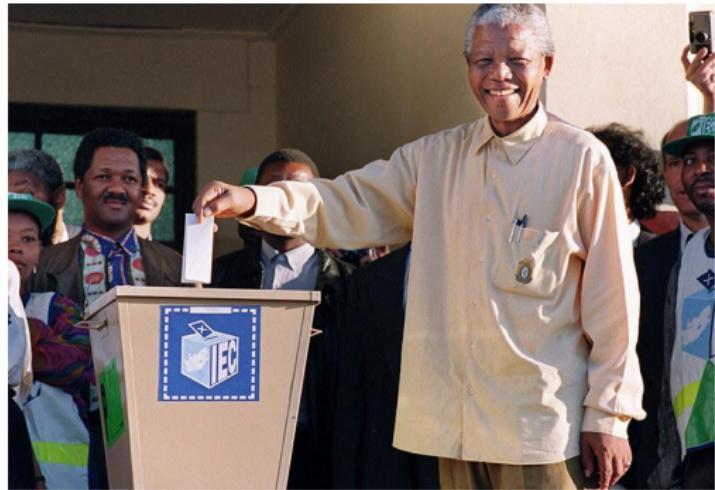
Les rôles sur la blockchain

- ▶ Les empereurs
 - ▶ Ils créent
- ▶ les élus
 - ▶ Ils écrivent
- ▶ les mineurs
 - ▶ Ils fouillent
- ▶ les utilisateurs
 - ▶ Ils utilisent



Les rôles sur la blockchain

- ▶ Les empereurs
 - ▶ Ils créent
- ▶ les élus
 - ▶ Ils écrivent
- ▶ les mineurs
 - ▶ Ils fouillent
- ▶ les utilisateurs
 - ▶ Ils utilisent



Les rôles sur la blockchain

- ▶ Les empereurs
 - ▶ Ils créent
- ▶ les élus
 - ▶ Ils écrivent
- ▶ les mineurs
 - ▶ Ils fouillent
- ▶ les utilisateurs
 - ▶ Ils utilisent



Les rôles sur la blockchain

- ▶ Les empereurs
 - ▶ Ils créent
- ▶ les élus
 - ▶ Ils écrivent
- ▶ les mineurs
 - ▶ Ils fouillent
- ▶ les utilisateurs
 - ▶ Ils utilisent



Sommaire

1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

2. Smart-contract

Cardano : blockchain de 3^e génération

A quoi peuvent servir les smart contract ?

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

La Naissance du Bitcoin

Cyber-Anarchisme

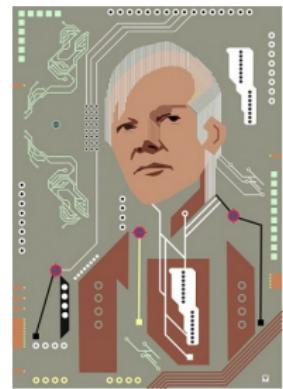
From : Satoshi Nakamoto satoshi@vistomail.com

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. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

2. Smart-contract

Cardano : blockchain de 3^e génération

A quoi peuvent servir les smart contract ?

Que vaut la blockchain ?



2009

???

SSL/TLS - 1996



HTTP - 1990



TCP/IP - 1974



Ethernet - 1974



Cela dépendra de son utilité

Sommaire

1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

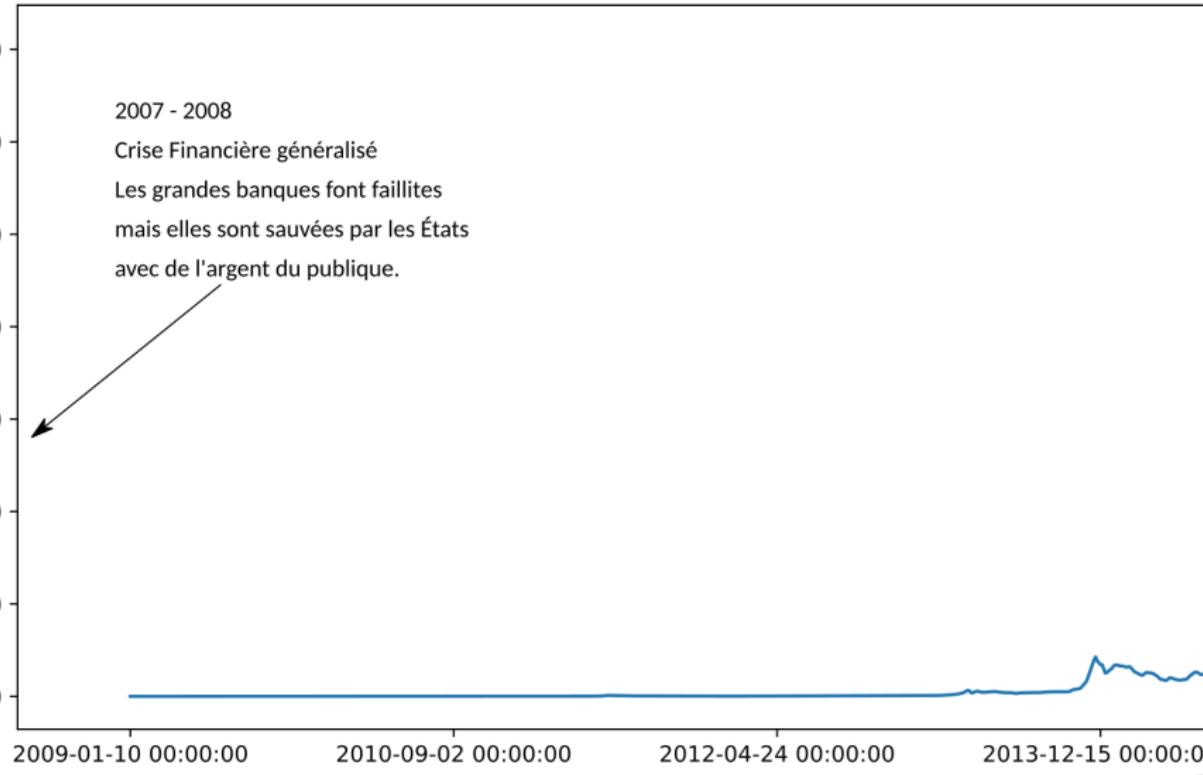
2. Smart-contract

Cardano : blockchain de 3^e génération

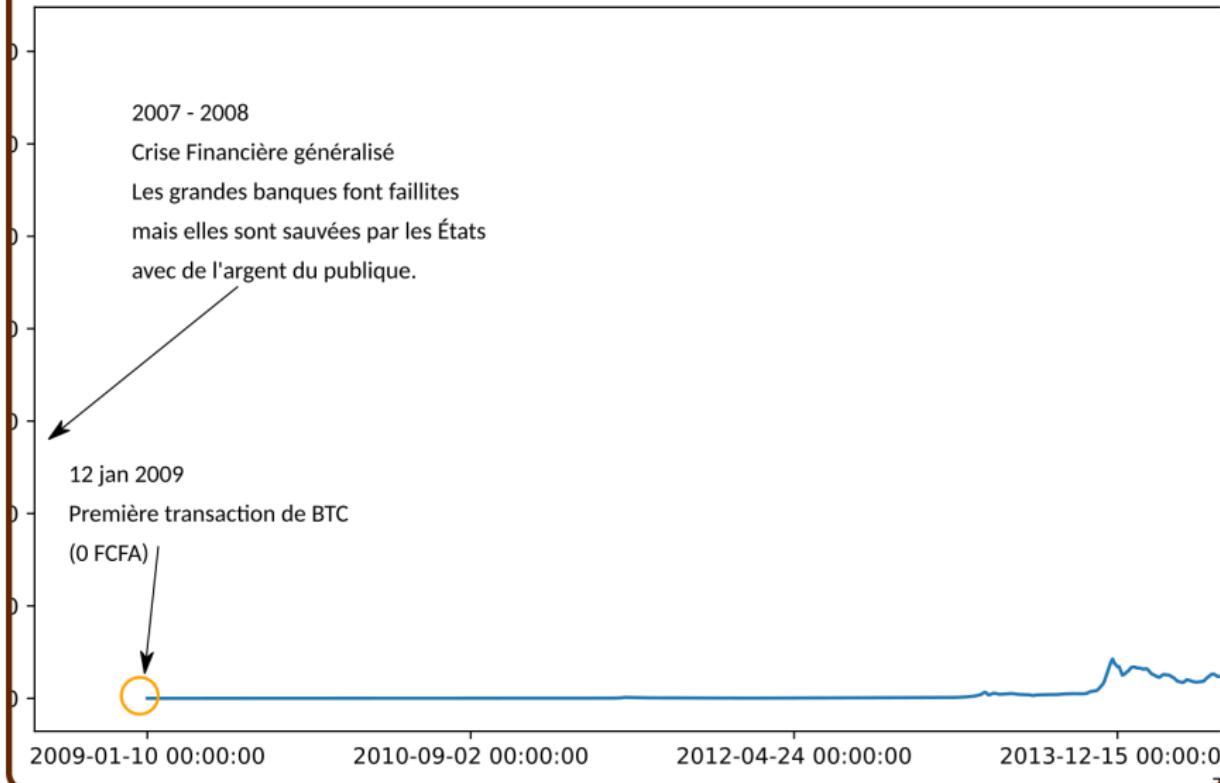
A quoi peuvent servir les smart contract ?

Les débuts

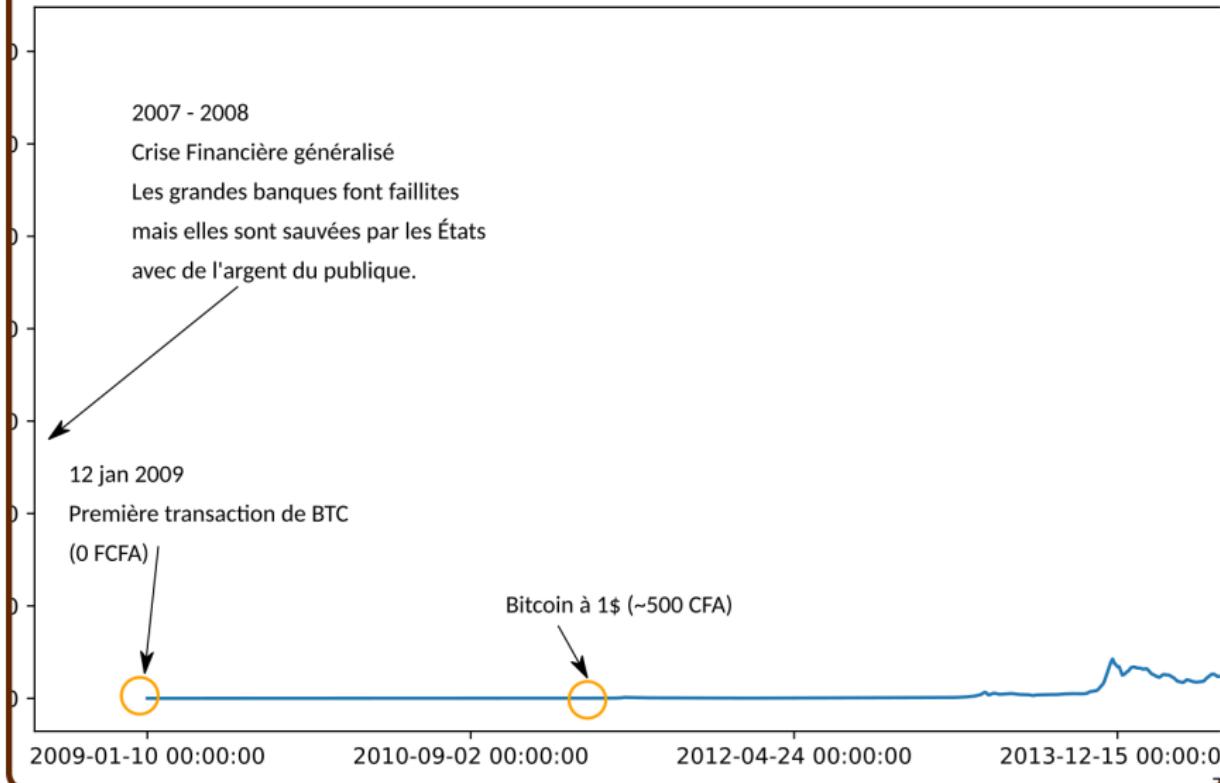
2007 - 2008
Crise Financière généralisé
Les grandes banques font faillites
mais elles sont sauvées par les États
avec de l'argent du public.



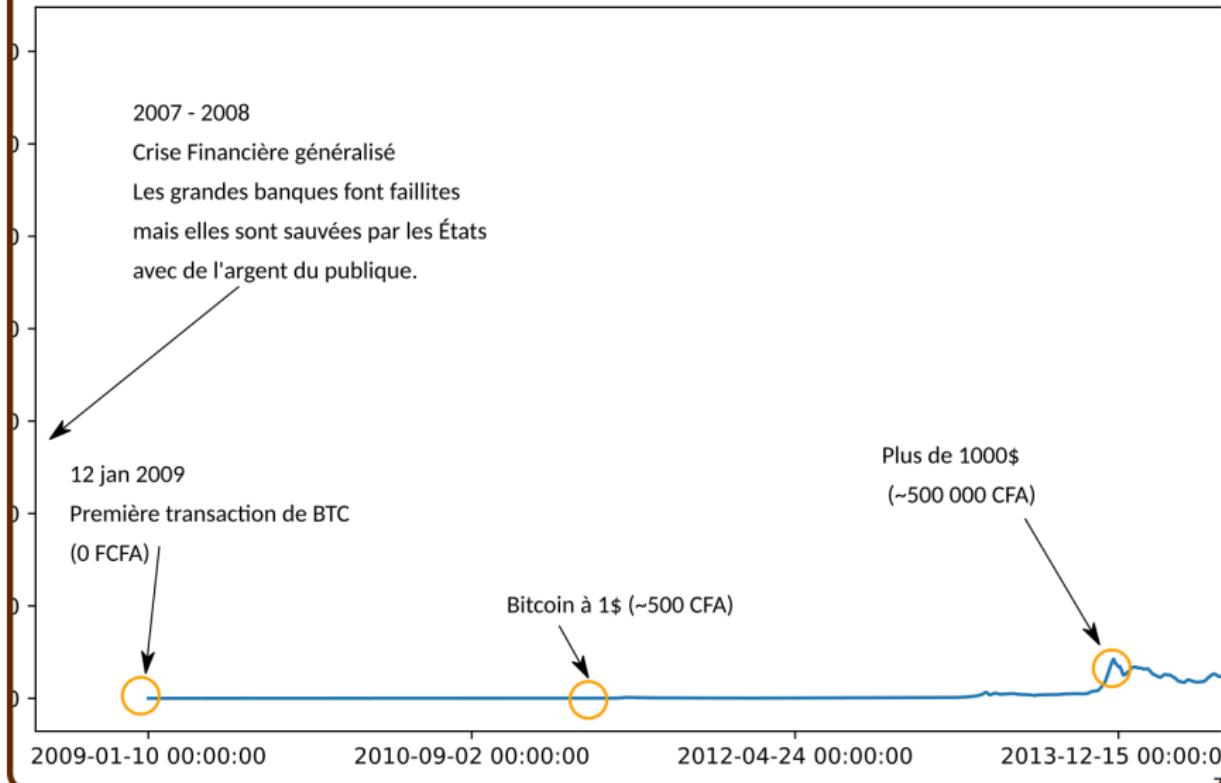
Les débuts



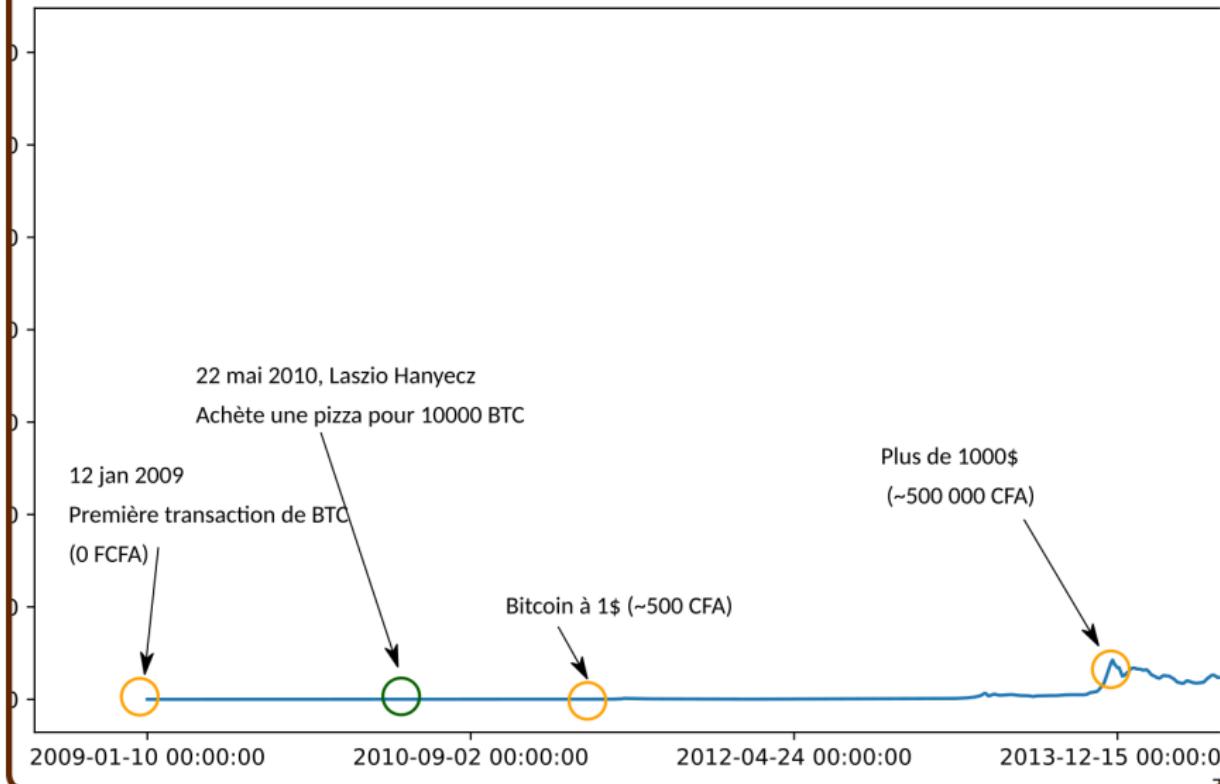
Les débuts



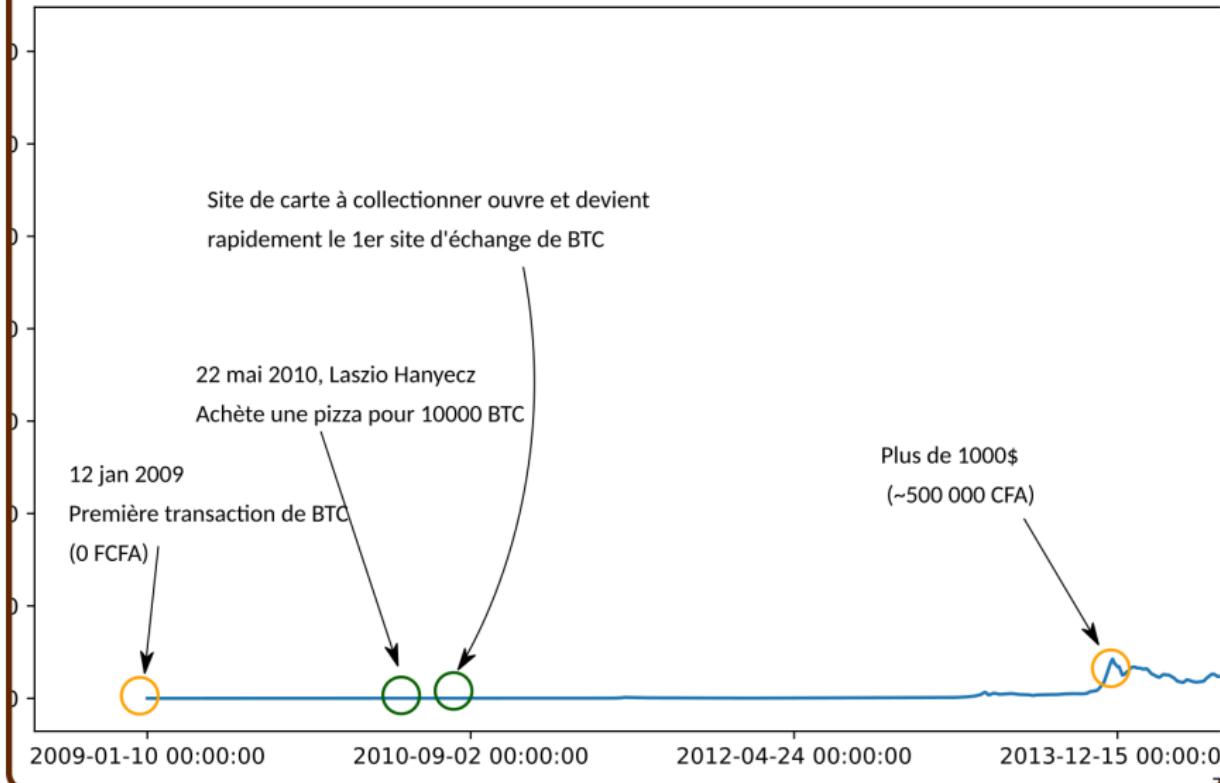
Les débuts



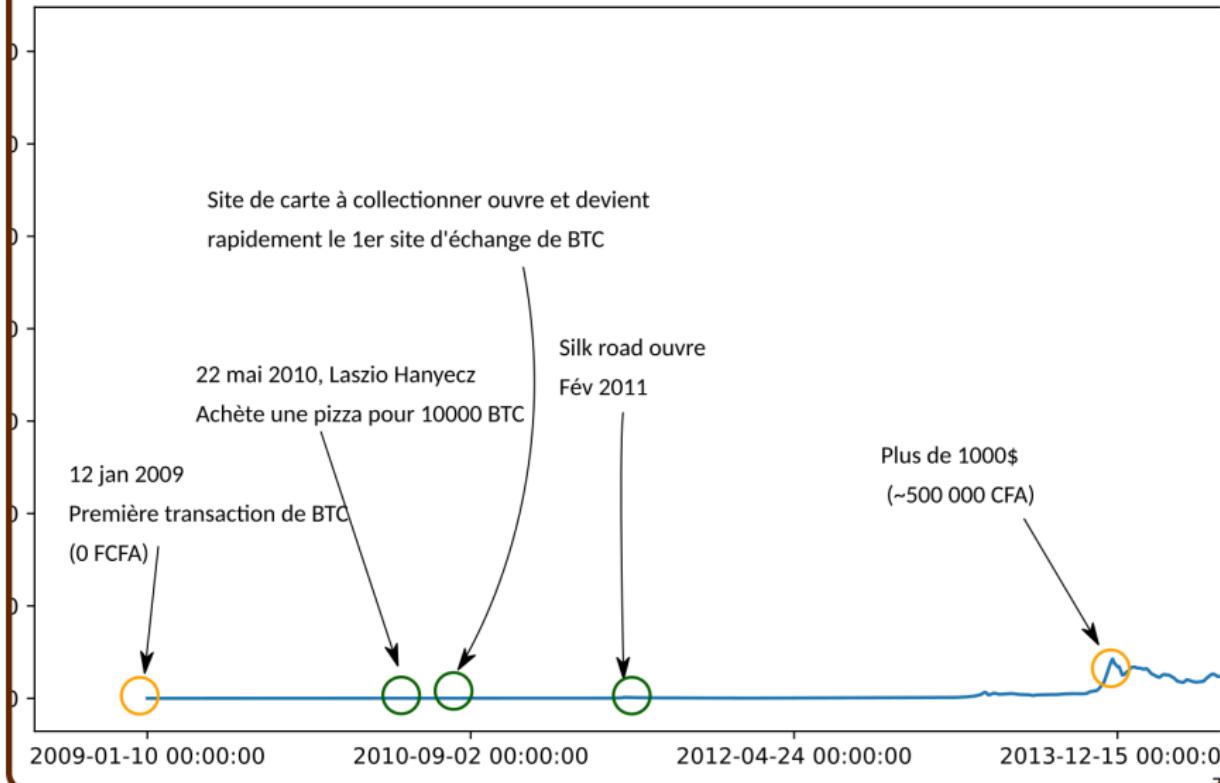
Les débuts



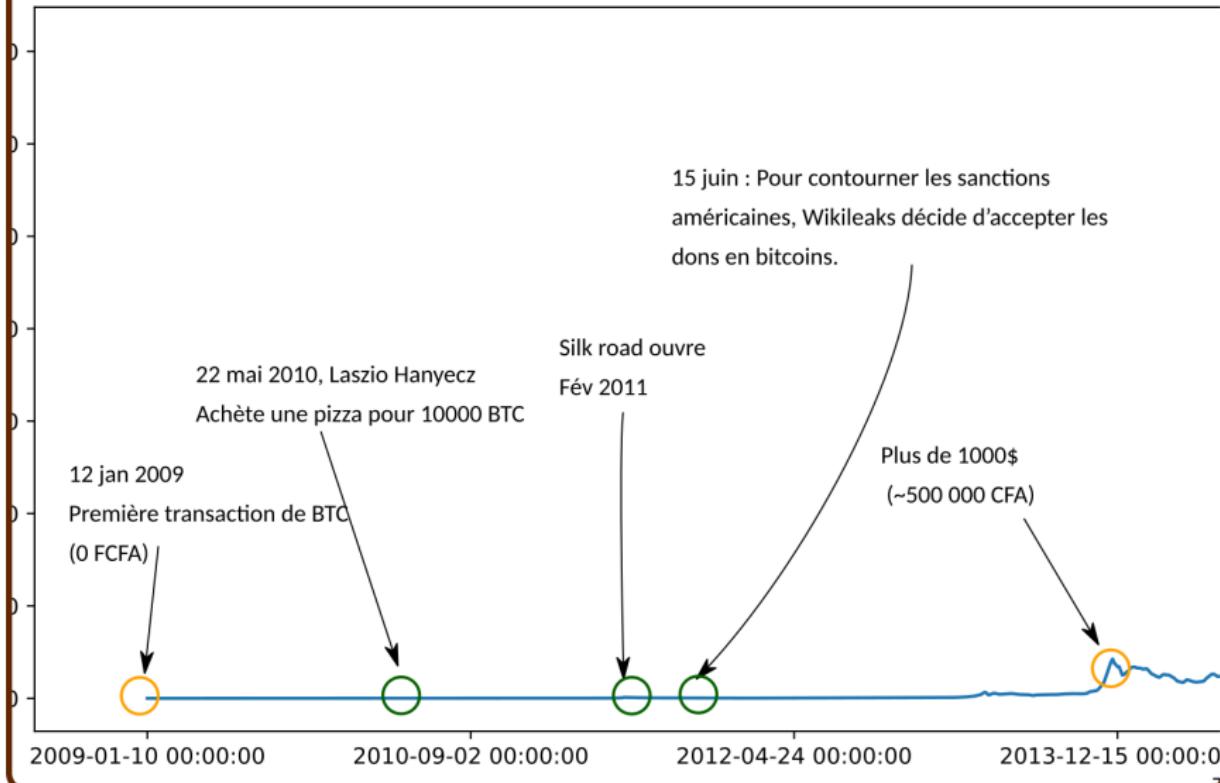
Les débuts



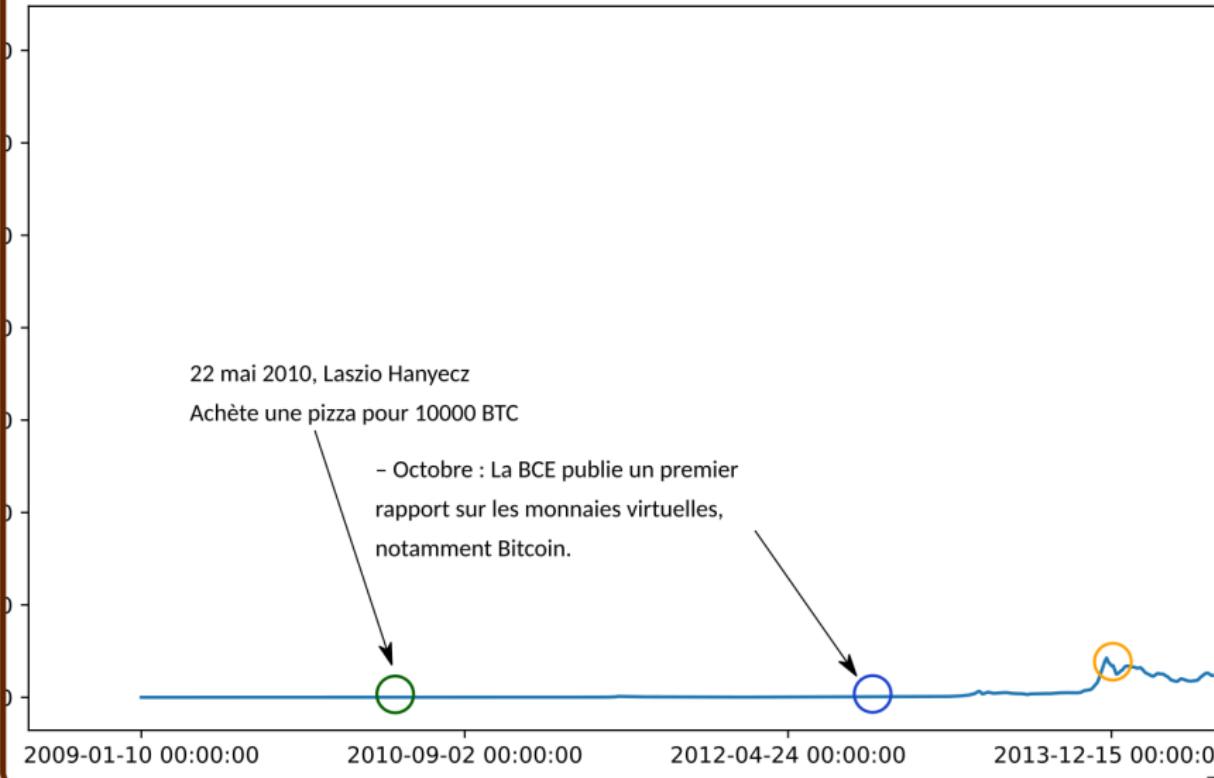
Les débuts



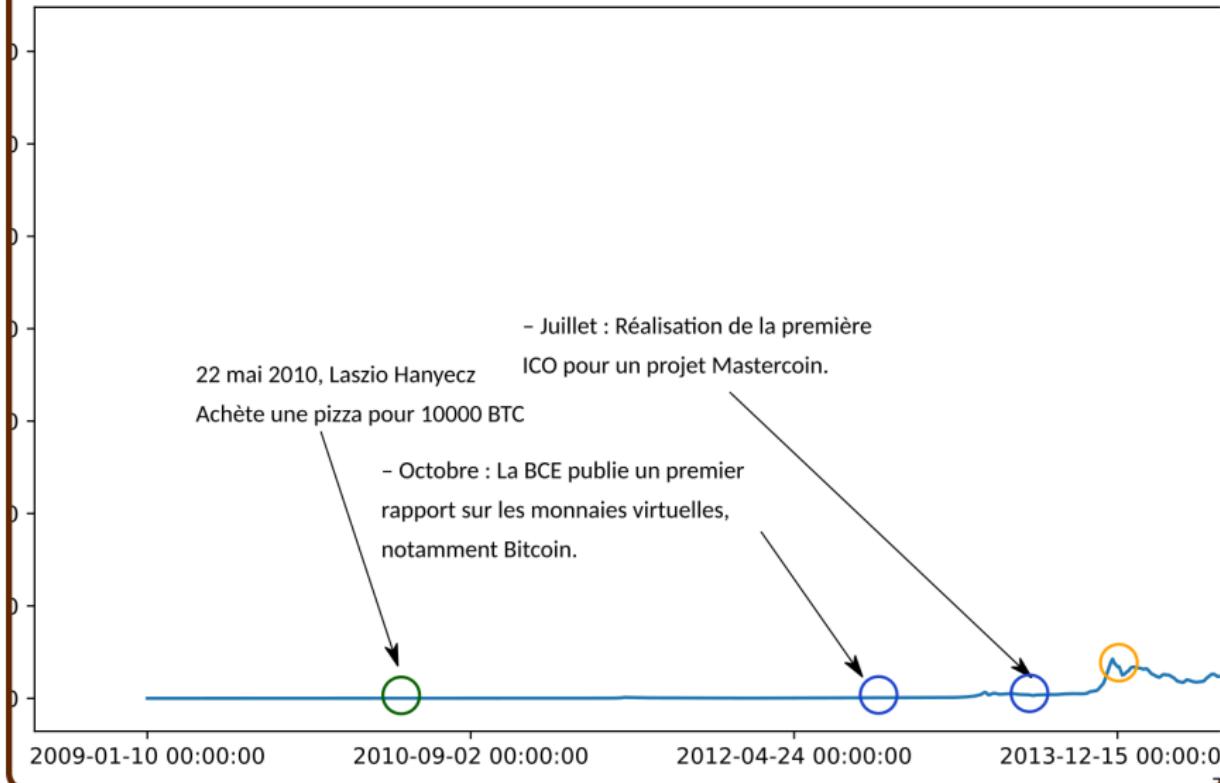
Les débuts



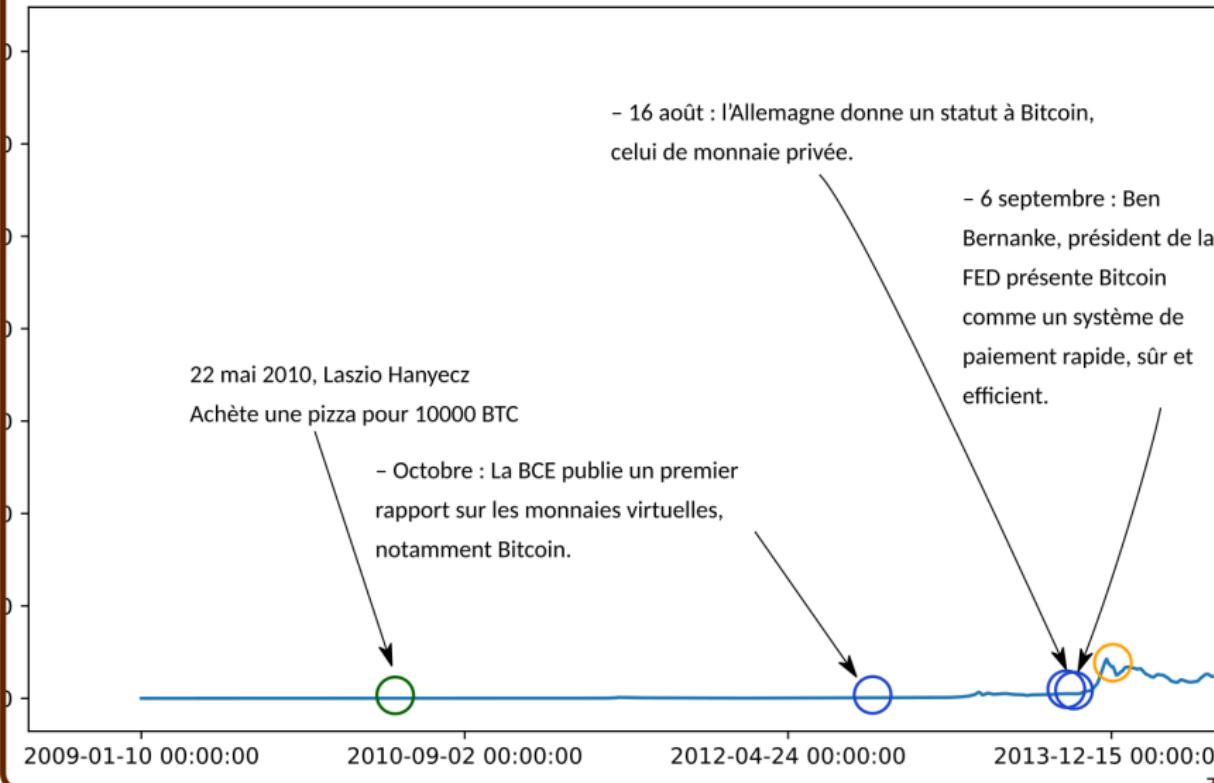
Les débuts



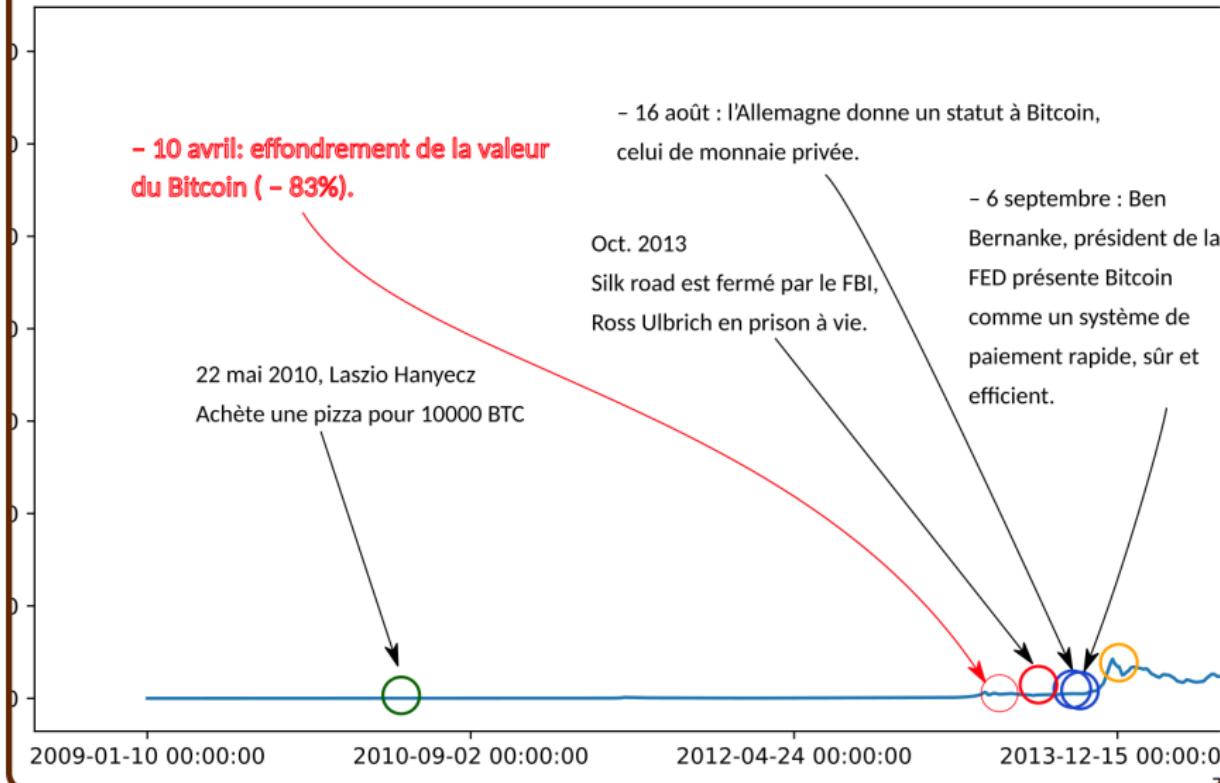
Les débuts



Les débuts



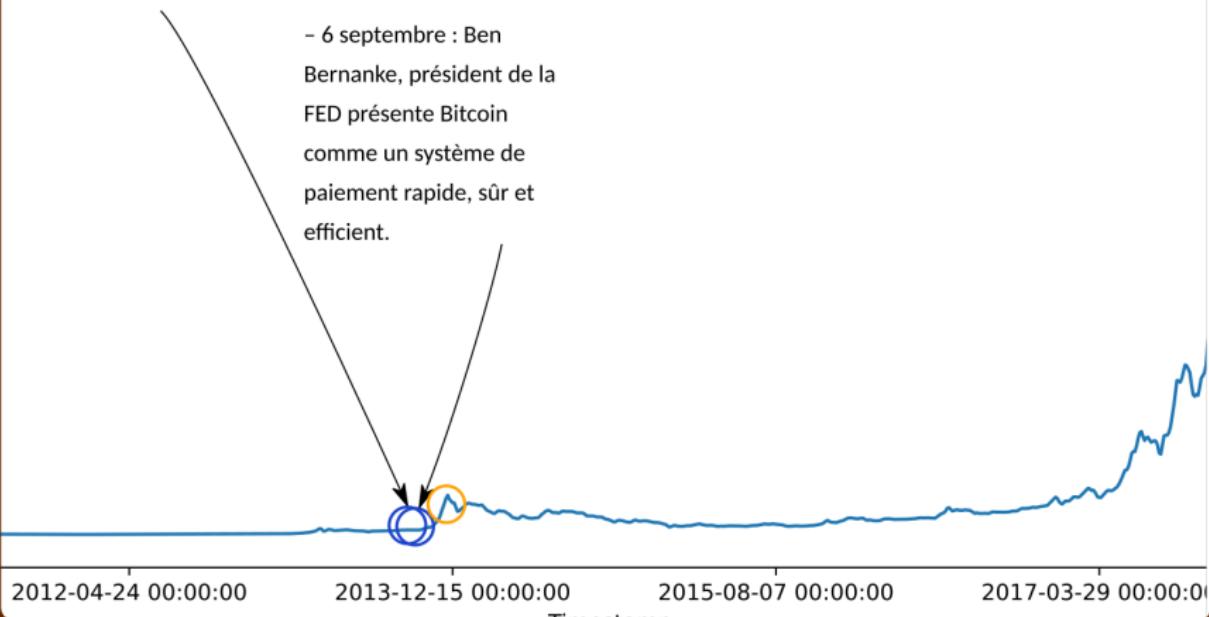
Les débuts



Adoption

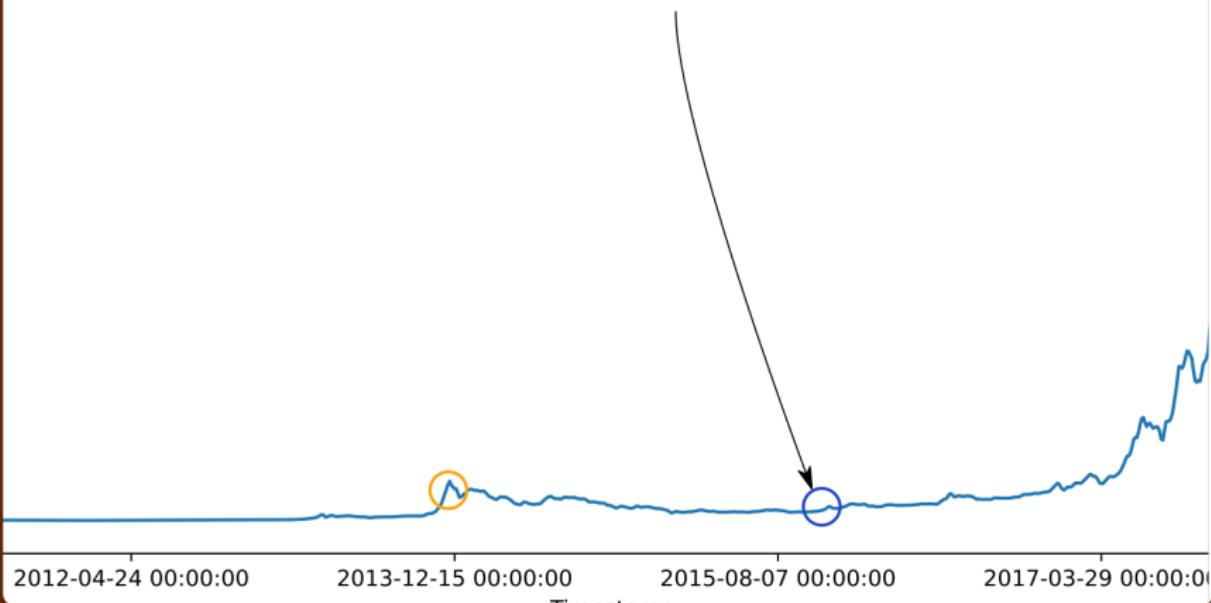
- 16 août : l'Allemagne donne un statut à Bitcoin, celui de monnaie privée.

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



Adoption

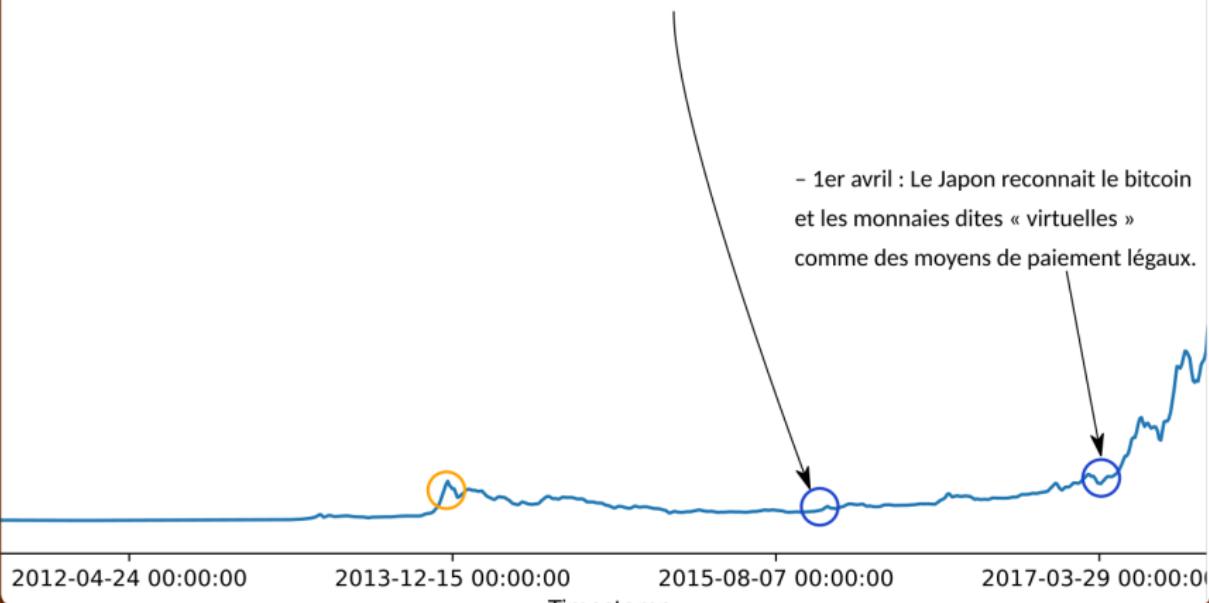
- 15 septembre : neuf banques d'investissement s'associent pour définir des standards d'implémentation d'une future blockchain privée.



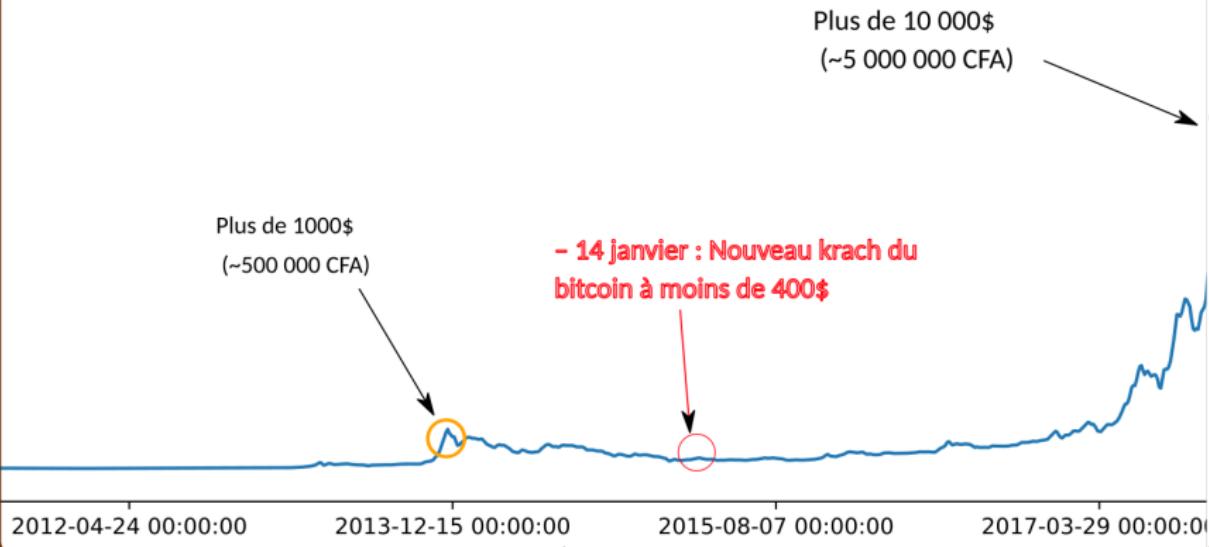
Adoption

- 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.

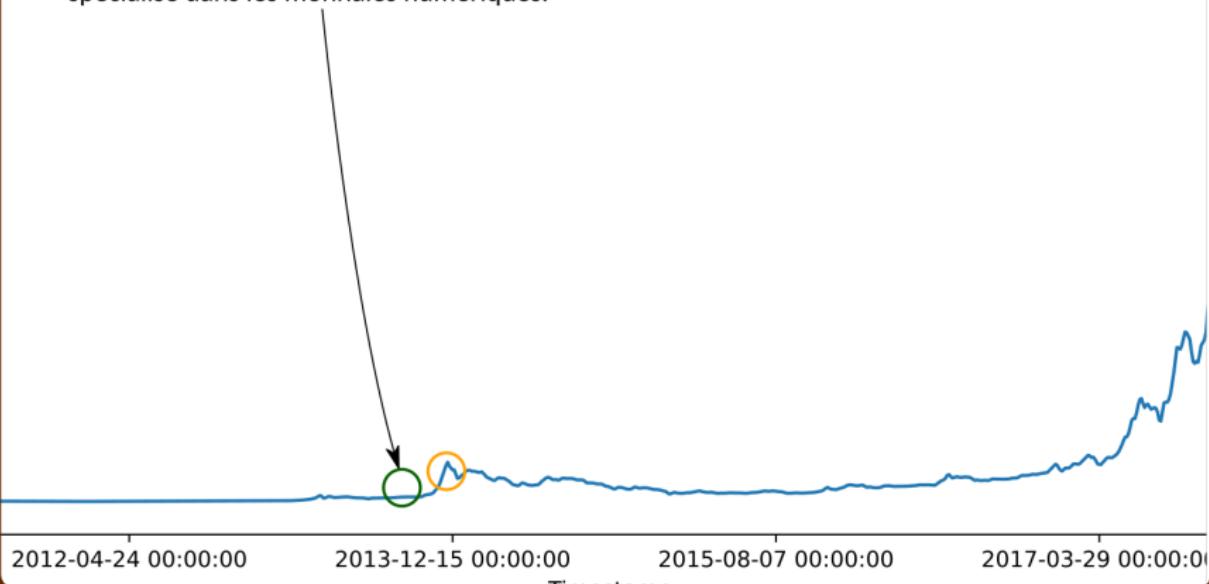


Adoption



Adoption

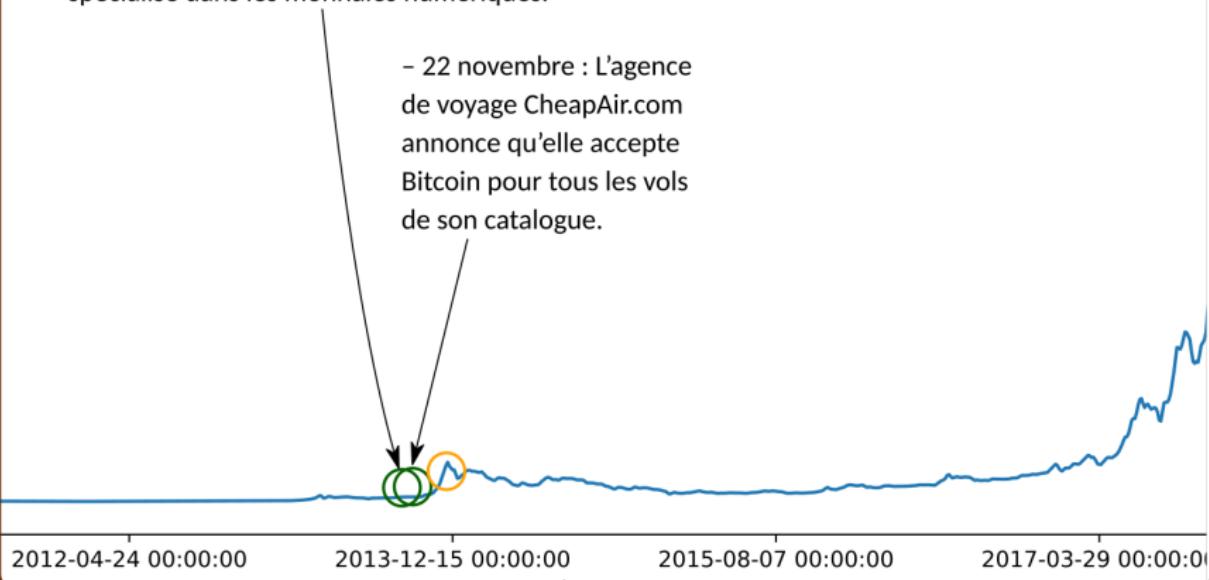
- 21 novembre : L'Université de Nicosie accepte que les frais de scolarité soient payés en bitcoins et annonce l'ouverture d'un Master de sciences économiques spécialisé dans les monnaies numériques.



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.

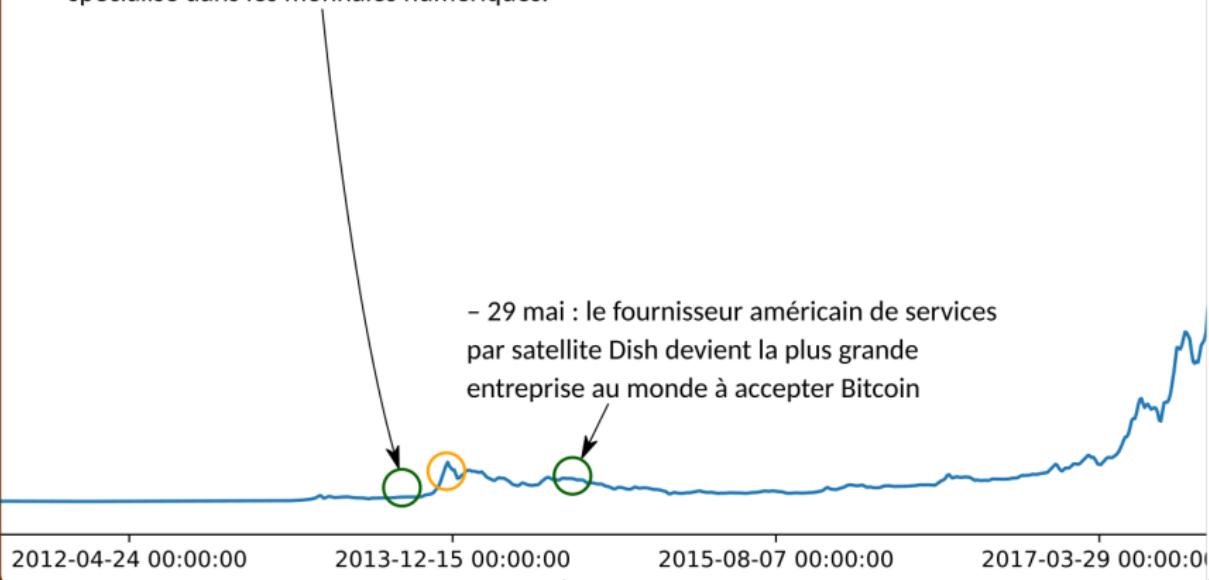
- 22 novembre : L'agence de voyage CheapAir.com annonce qu'elle accepte Bitcoin pour tous les vols de son catalogue.



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.

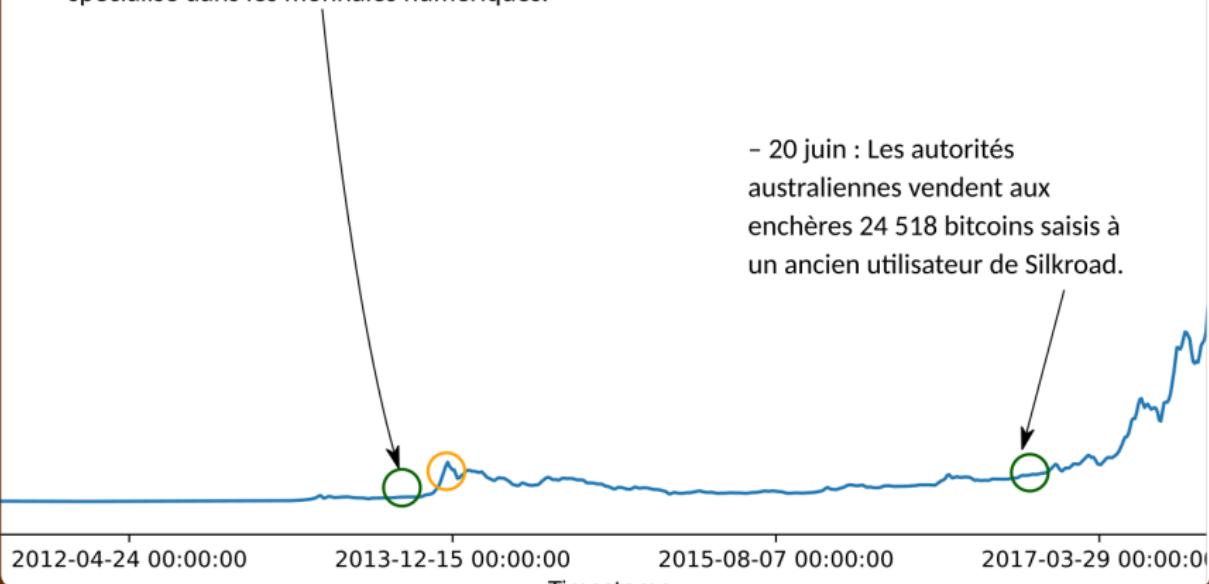
- 29 mai : le fournisseur américain de services par satellite Dish devient la plus grande entreprise au monde à accepter Bitcoin



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.

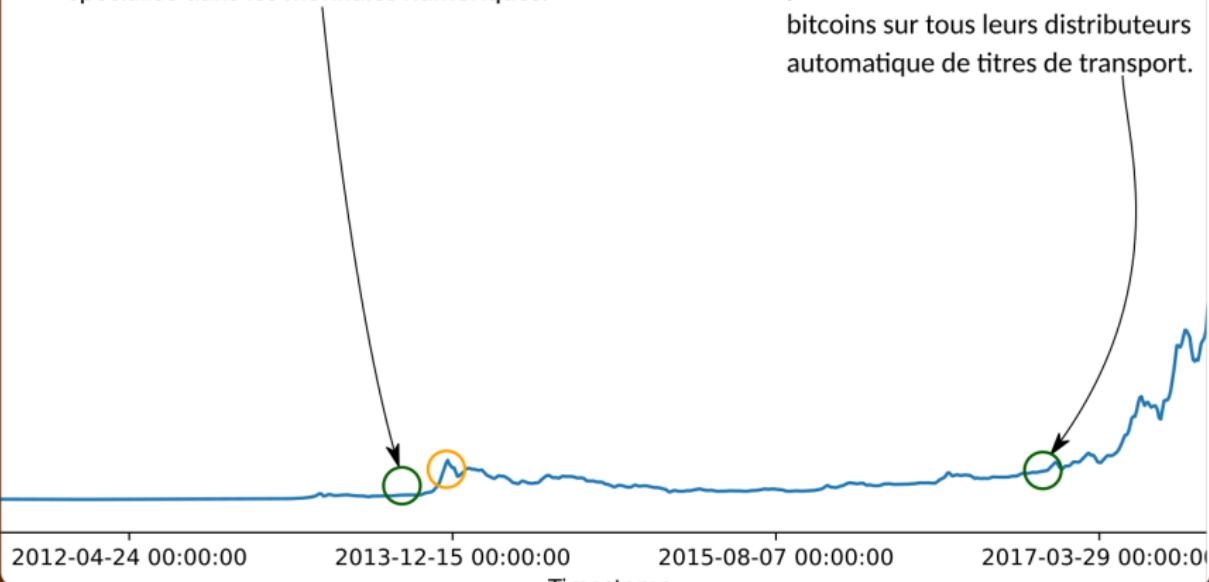
- 20 juin : Les autorités australiennes vendent aux enchères 24 518 bitcoins saisis à un ancien utilisateur de Silkroad.

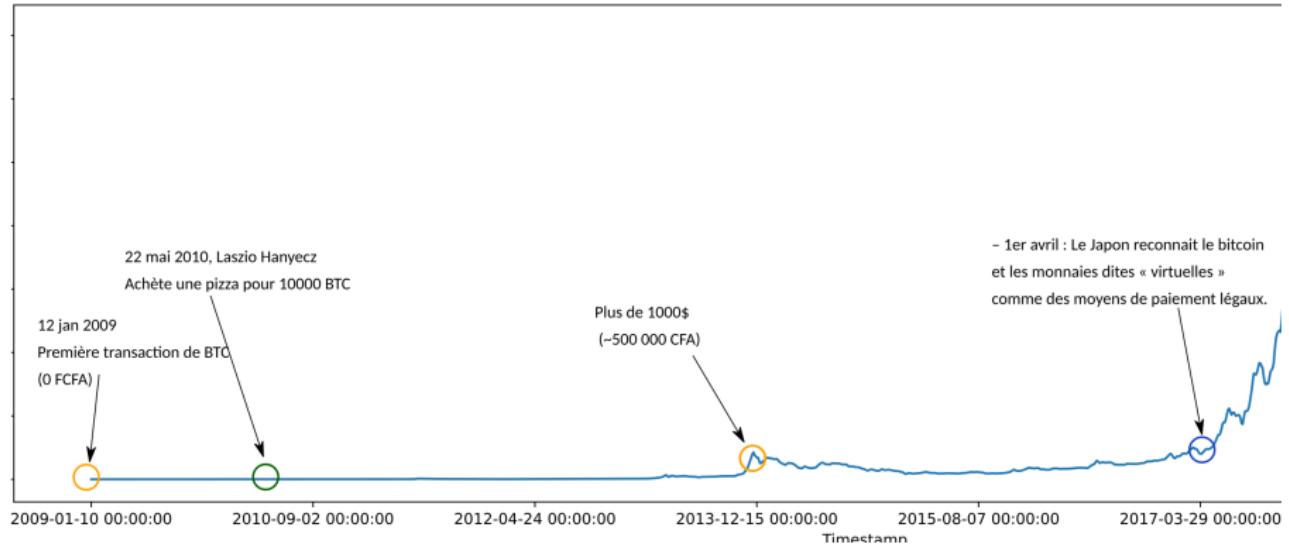


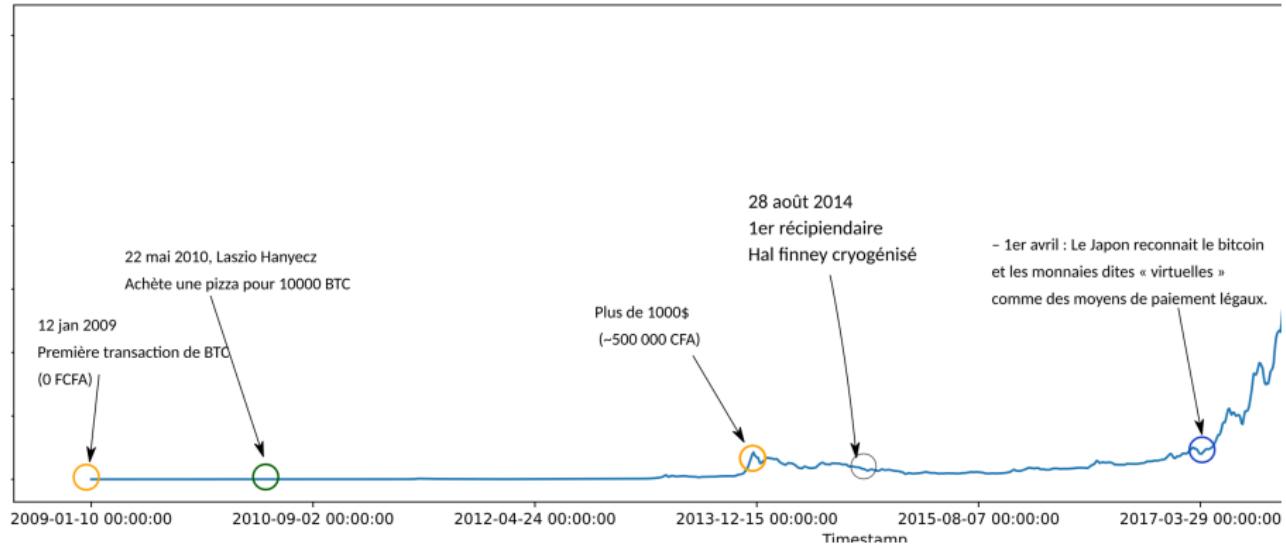
Adoption

- 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.

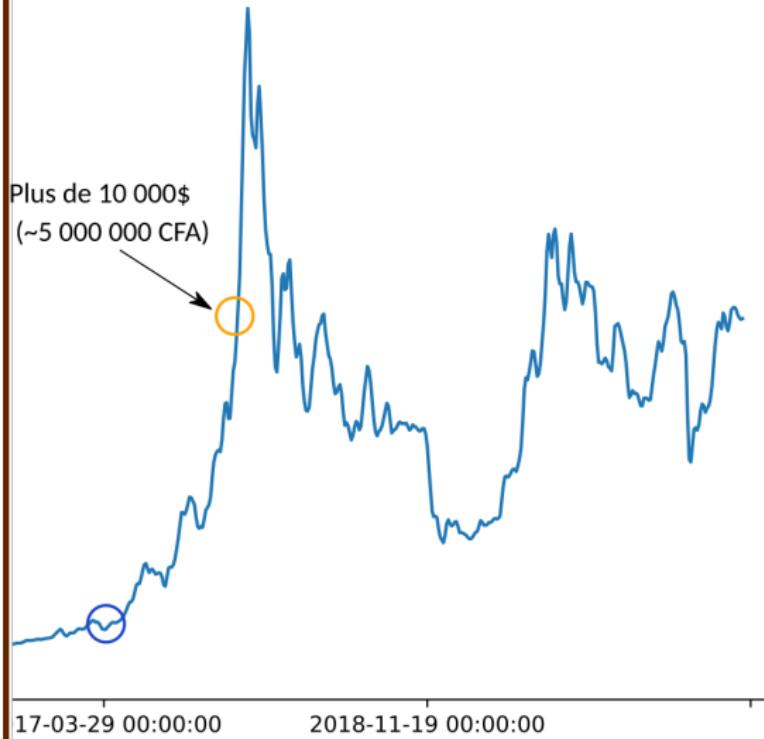
- 11 novembre : Les Chemins de fer fédéraux suisses testent, pour une période de deux ans, la vente de bitcoins sur tous leurs distributeurs automatique de titres de transport.



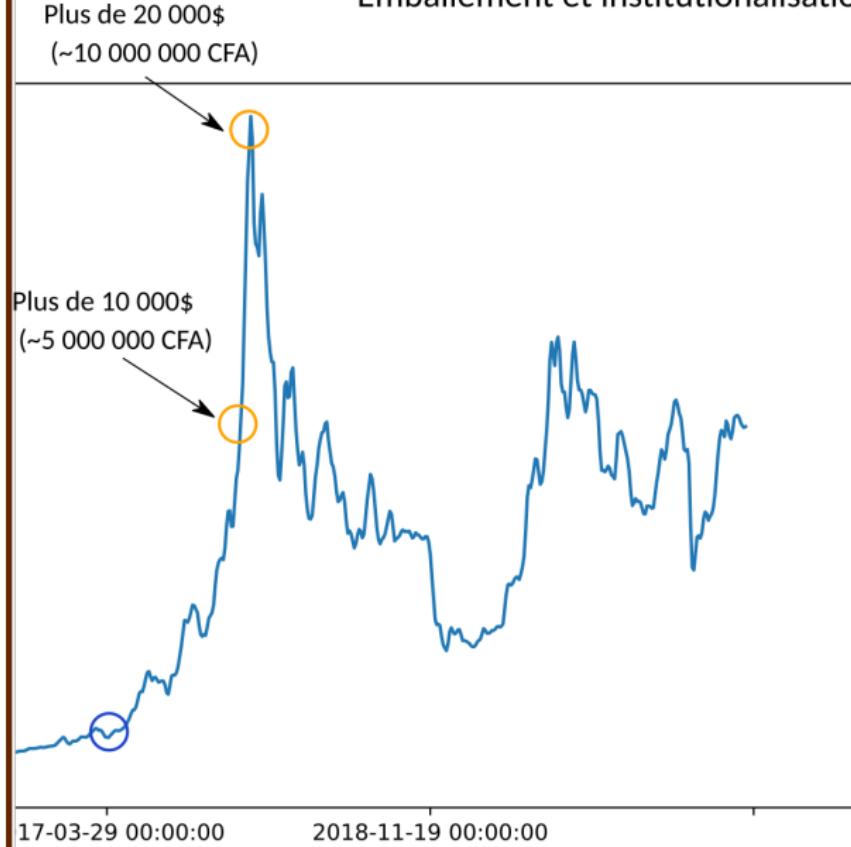




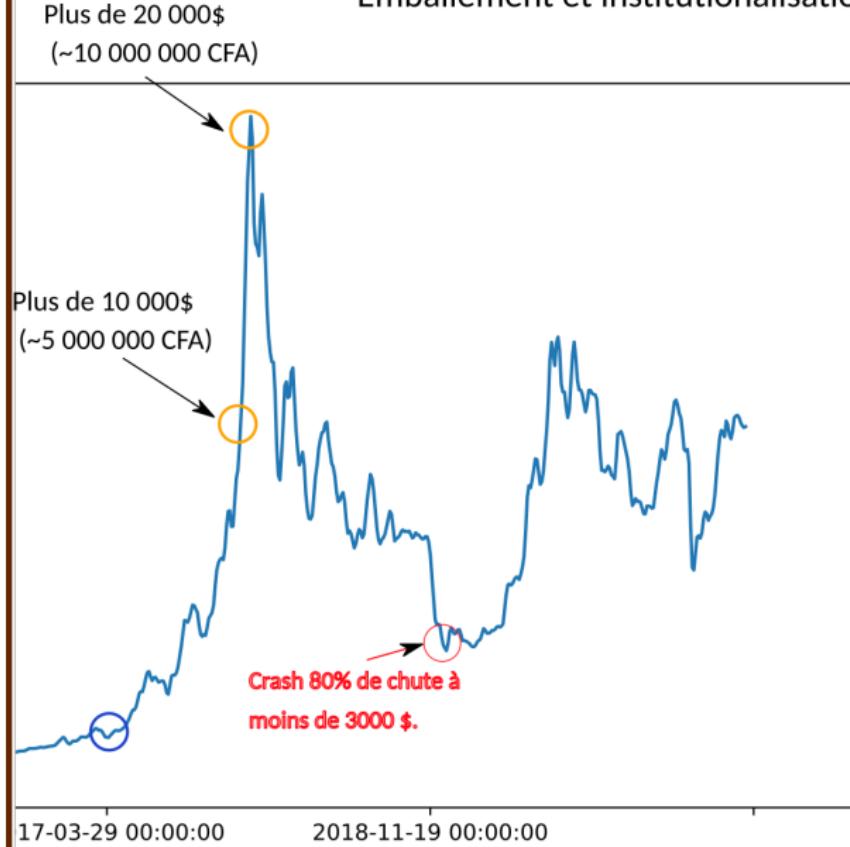
Emballage et institutionalisation



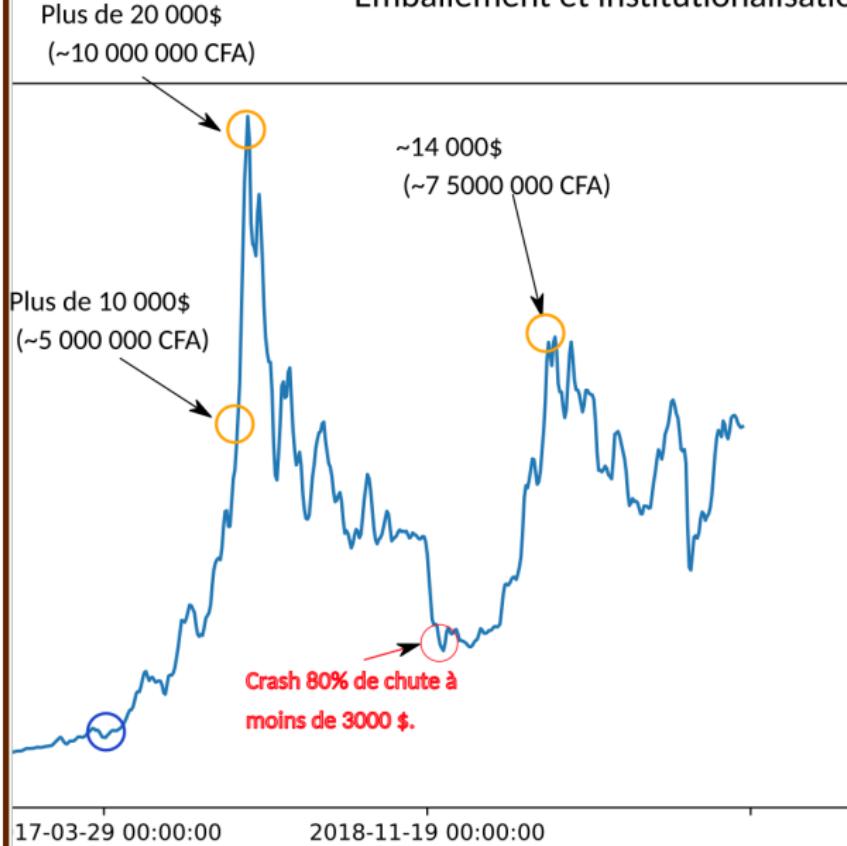
Emballage et institutionalisation



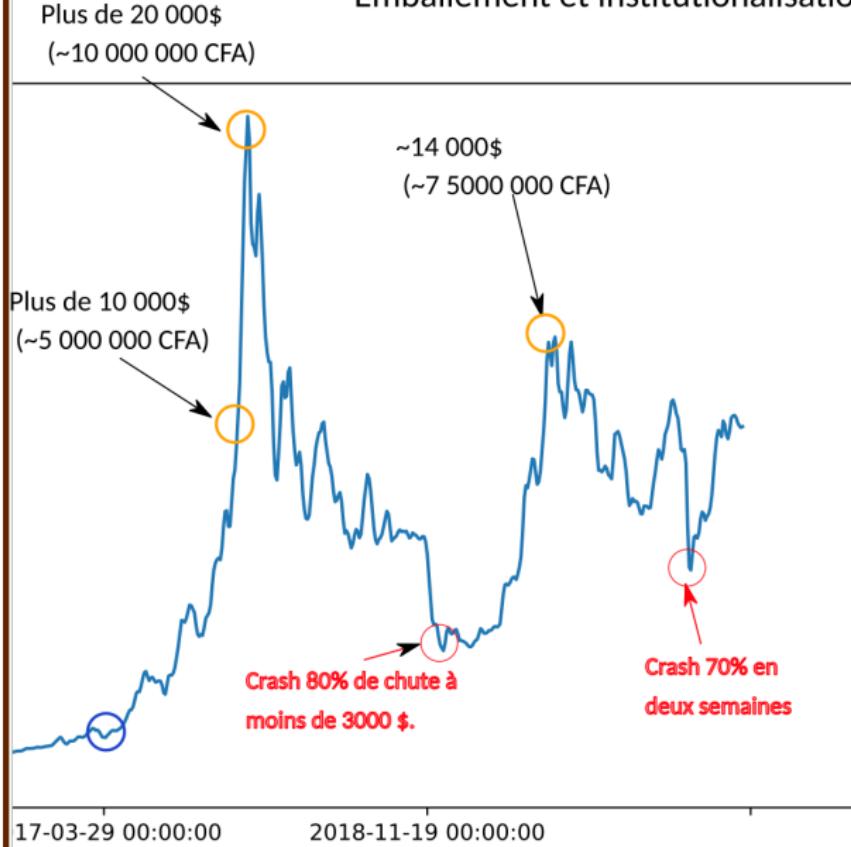
Emballage et institutionalisation



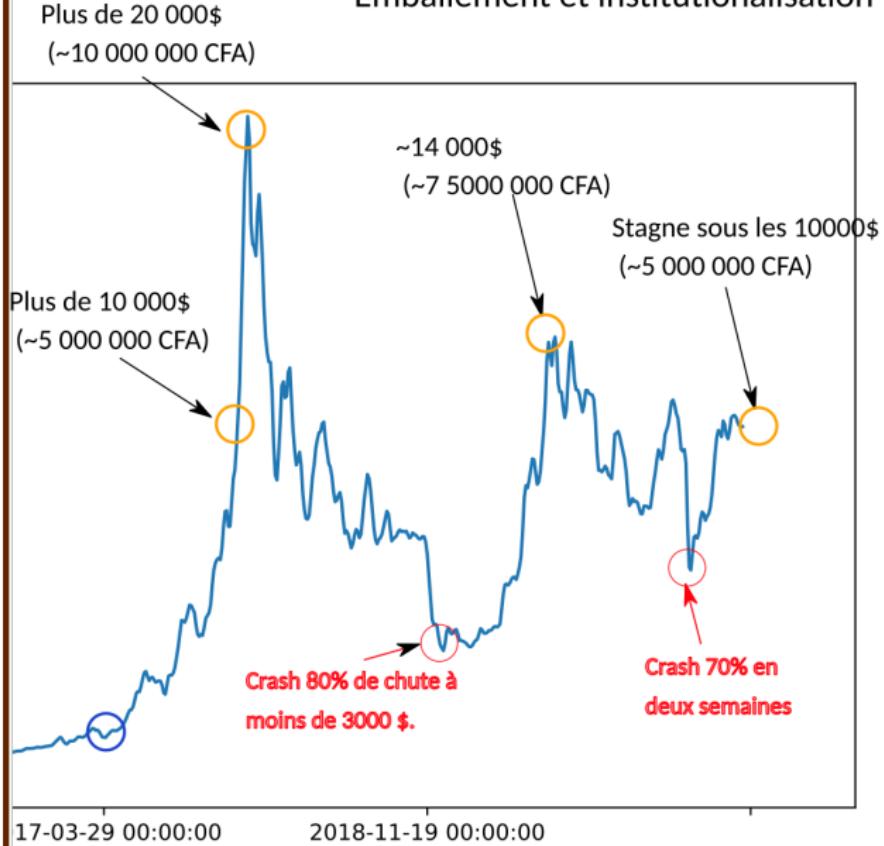
Emballage et institutionalisation



Emballage et institutionalisation



Emballage et institutionalisation



Emballage et institutionalisation

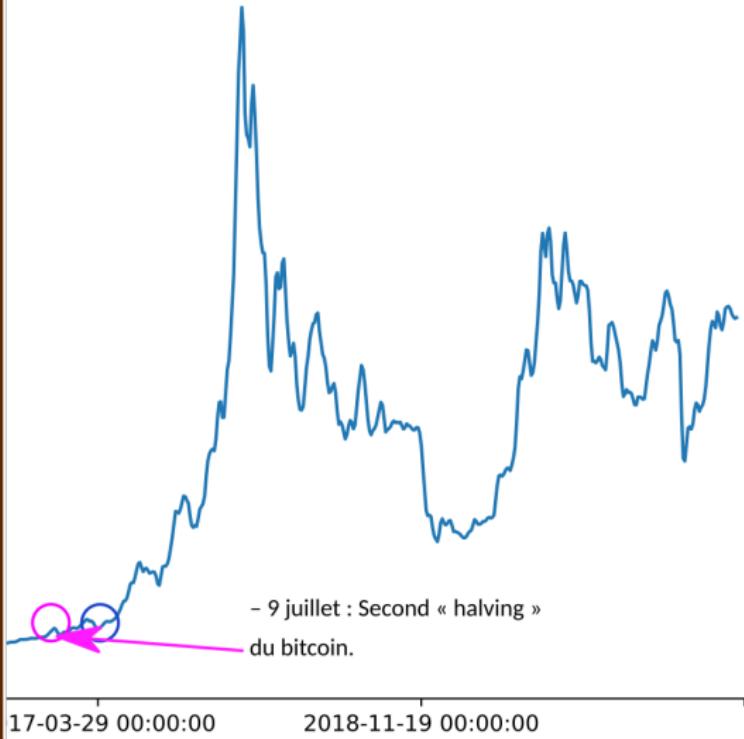
- 22 février : Le ministère des finances de la République fédérale d'Allemagne entérine un cadre fiscal favorable au bitcoin.



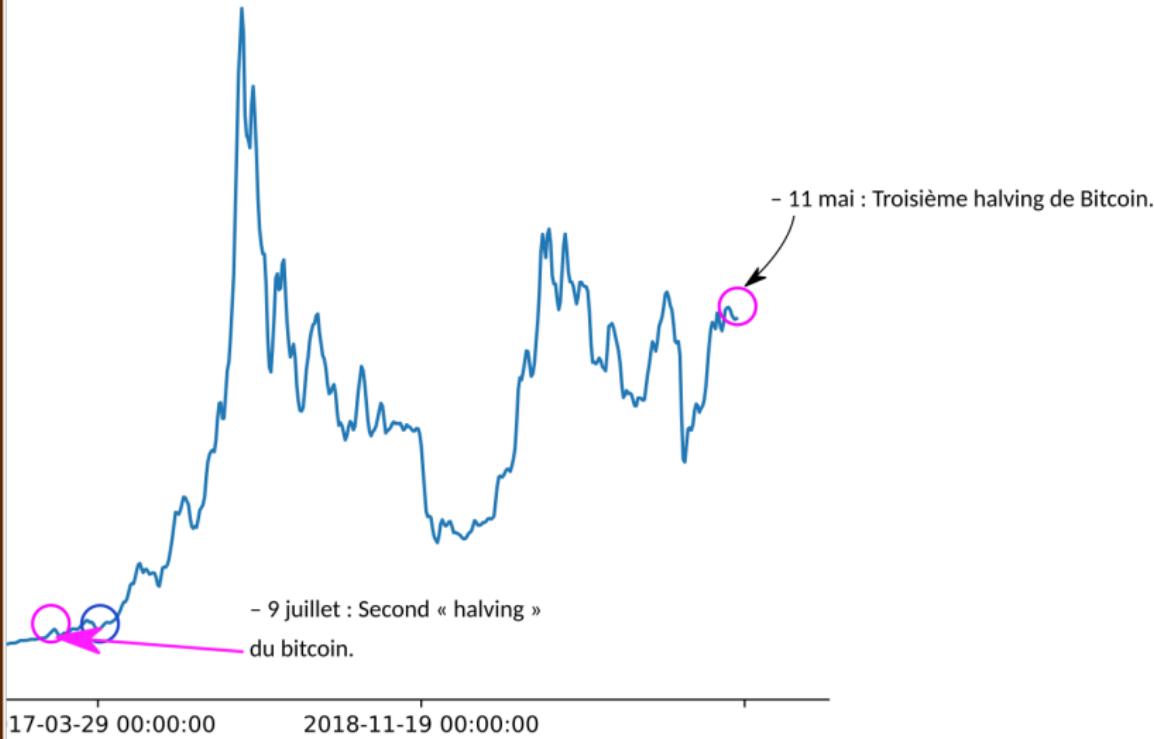
Emballage et institutionalisation

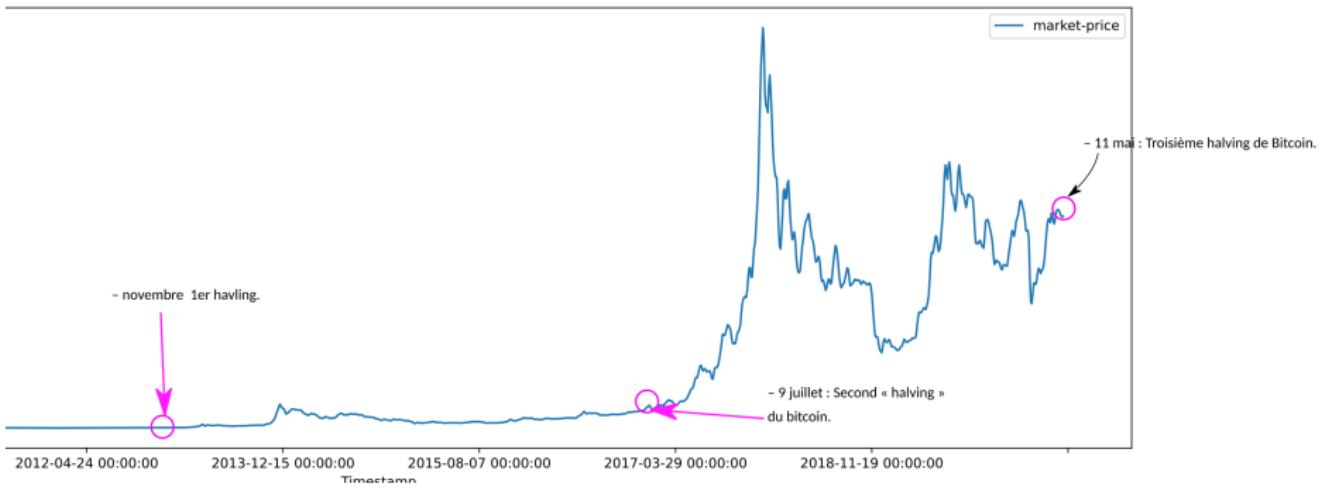


Emballage et institutionalisation

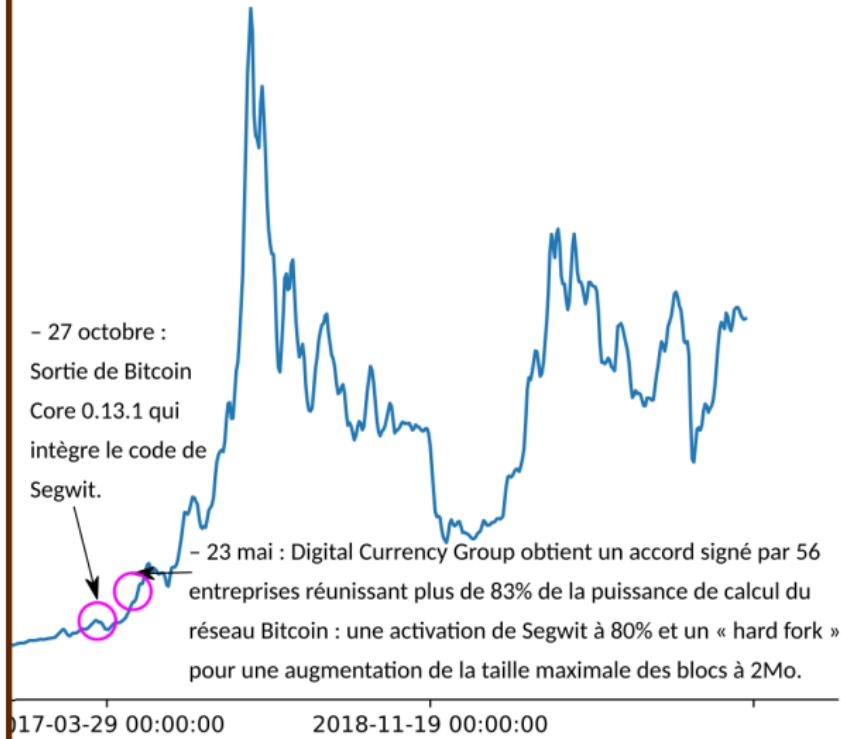


Emballage et institutionalisation



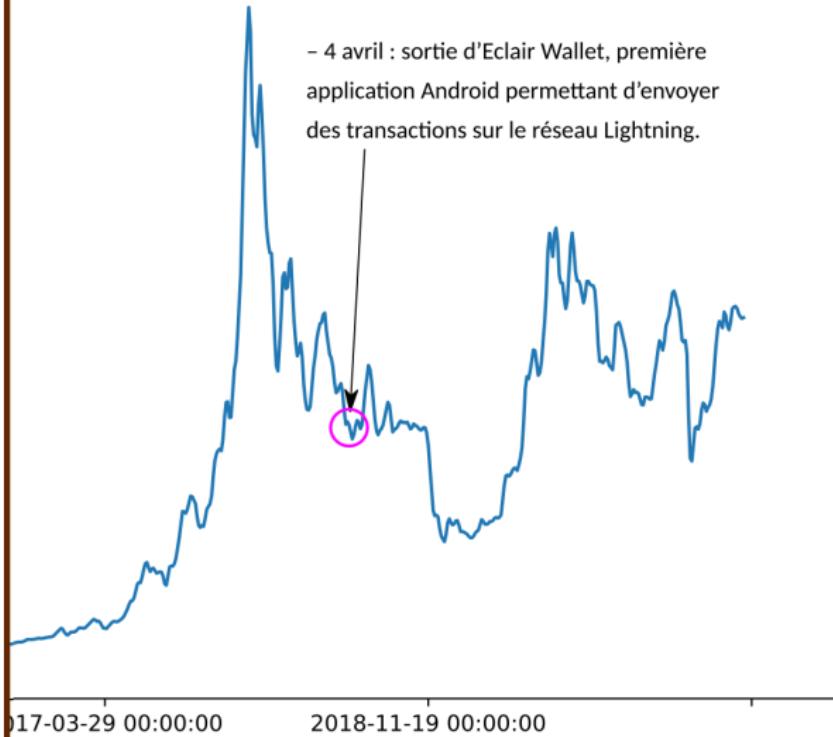


Emballage et institutionalisation

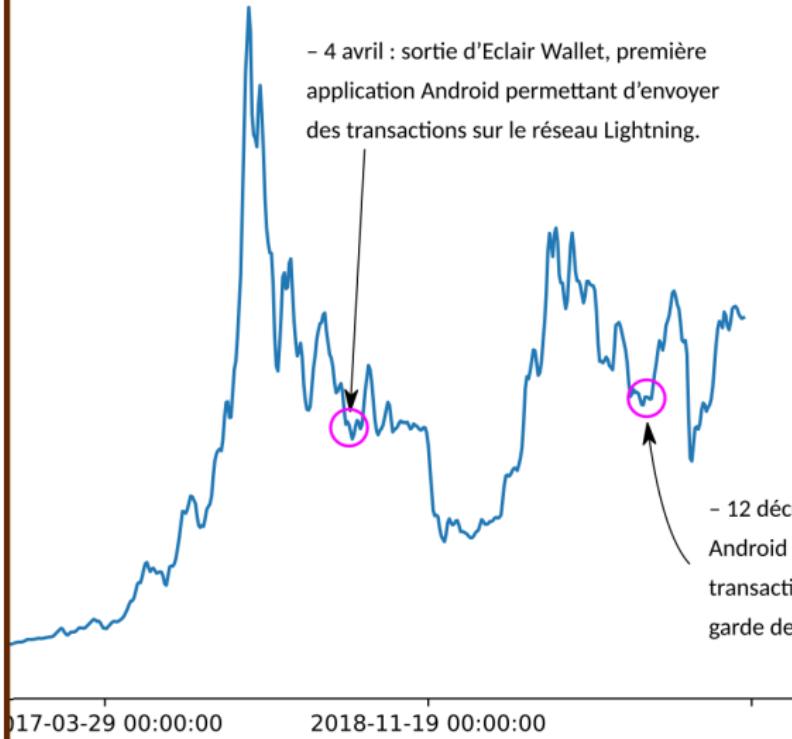


Emballage et institutionalisation

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



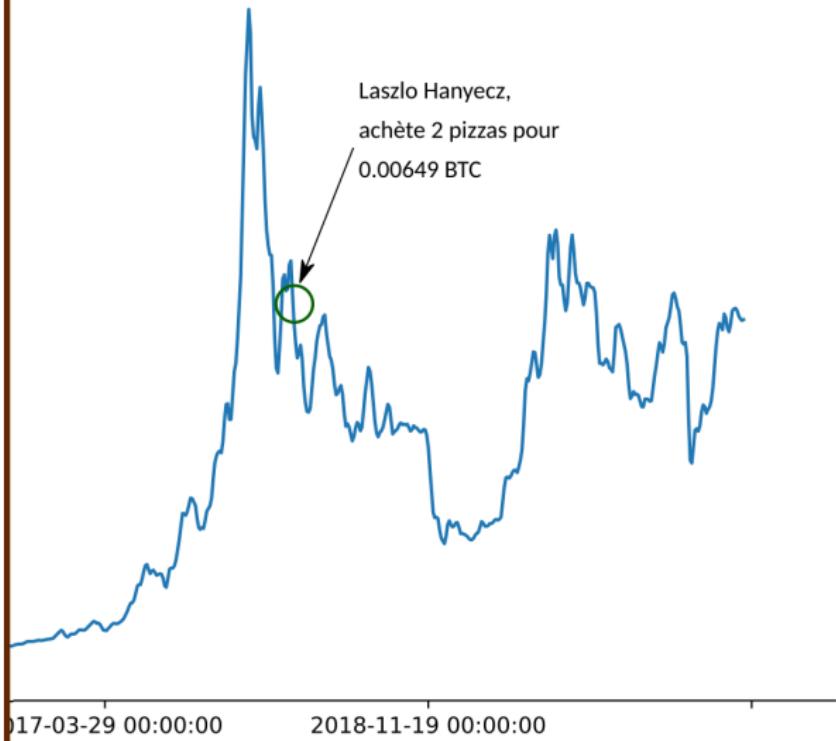
Emballage et institutionnalisation



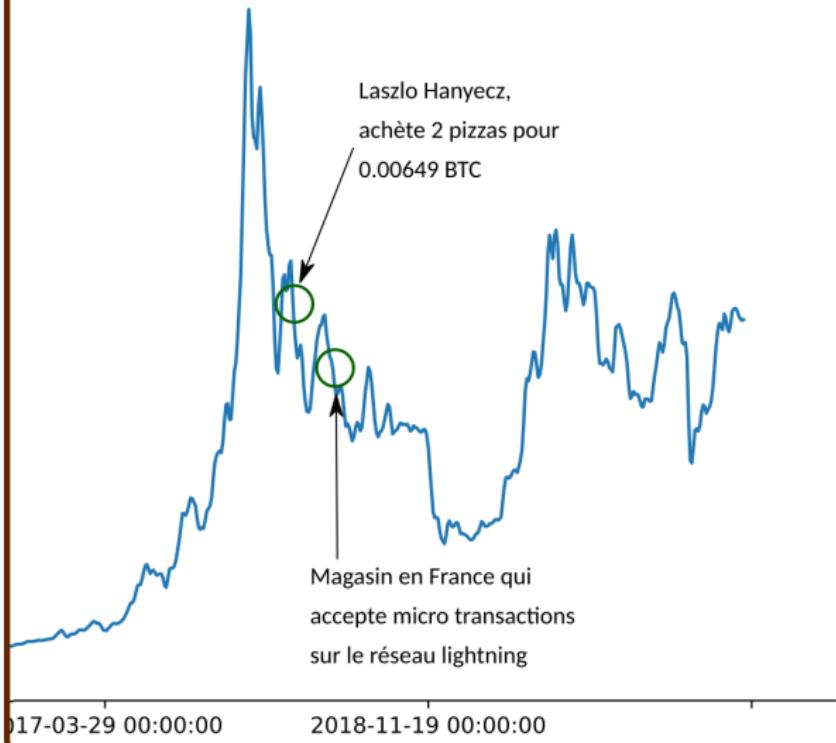
- 4 avril : sortie d'Eclair Wallet, première application Android permettant d'envoyer des transactions sur le réseau Lightning.

- 12 décembre : Sortie de Phoenix, une application Android permettant de réaliser très facilement des transactions sur le Lightning Network sans confier la garde de ses satoshis à un tiers de confiance.

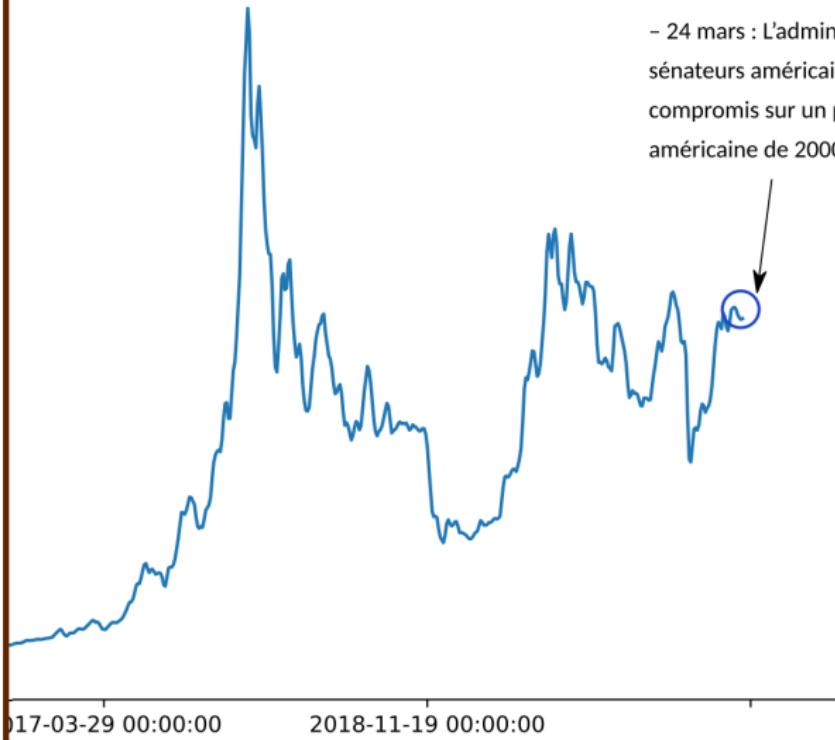
Emballage et institutionalisation



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 ?



Sommaire

1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

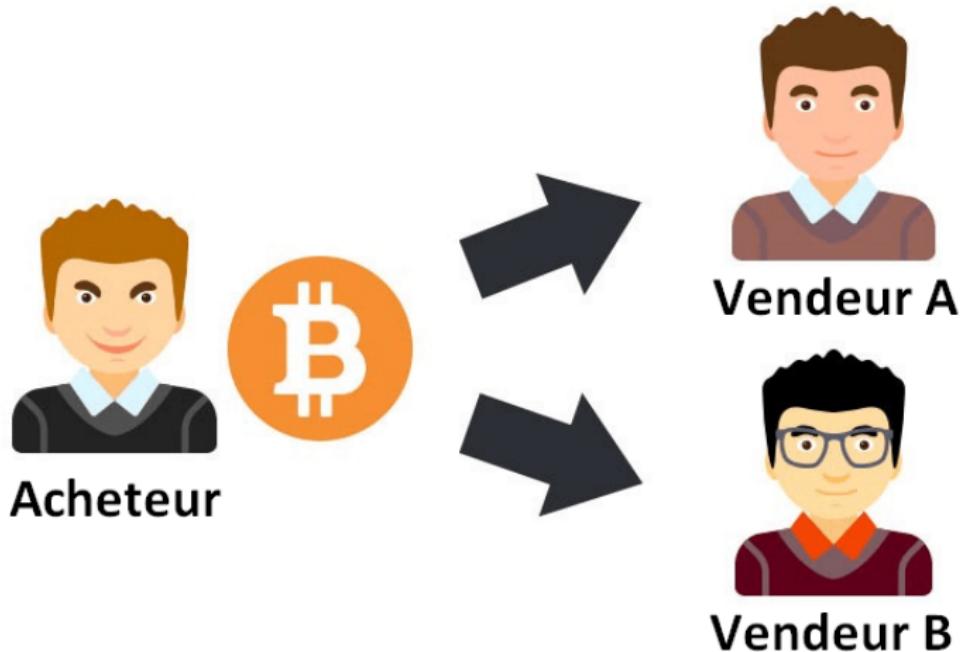
Pour conclure sur la blockchain

2. Smart-contract

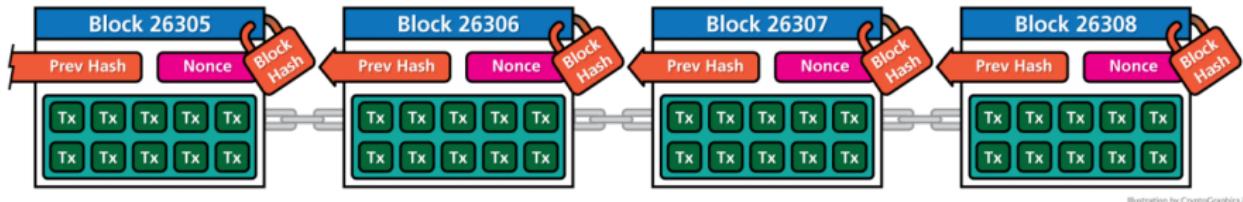
Cardano : blockchain de 3^e génération

A quoi peuvent servir les smart contract ?

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

Il faut former la plus longue chaîne possible !

Comment le problème est-il résolu ?

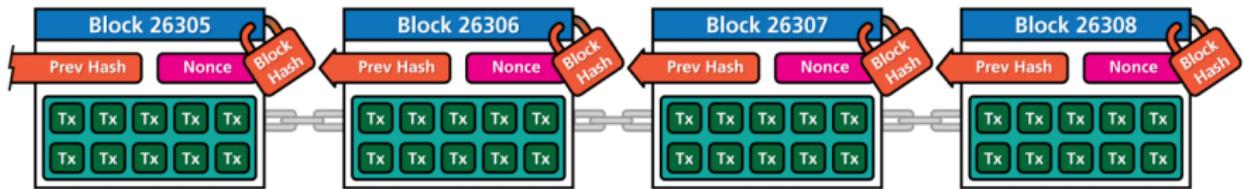


Illustration by CryptoGraphics.info

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

Il faut former la plus longue chaîne possible !

Comment le problème est-il résolu ?

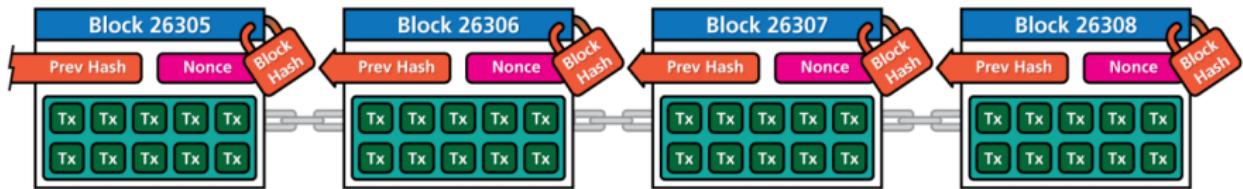


Illustration by CryptoGraphics.info

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

Il faut former la plus longue chaîne possible !

Comment le problème est-il résolu ?

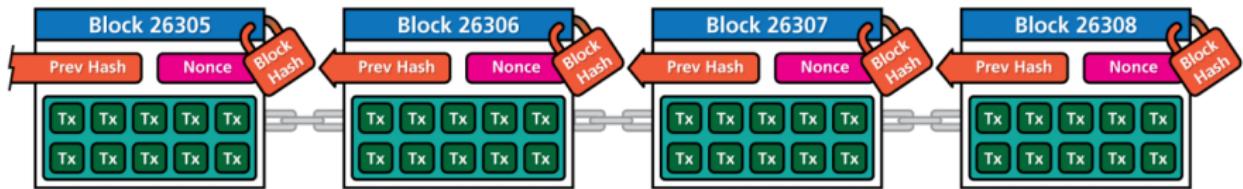


Illustration by CryptoGraphics.info

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

Il faut former la plus longue chaîne possible !

Comment le problème est-il résolu ?

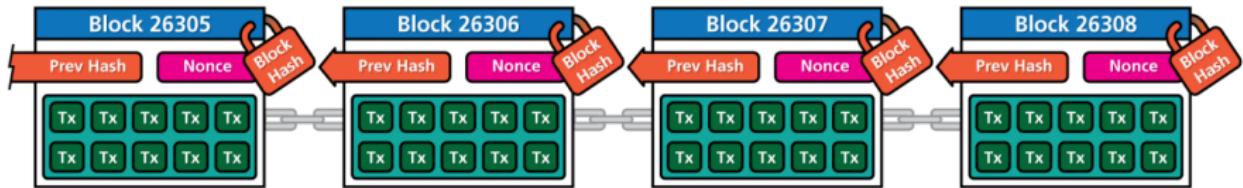


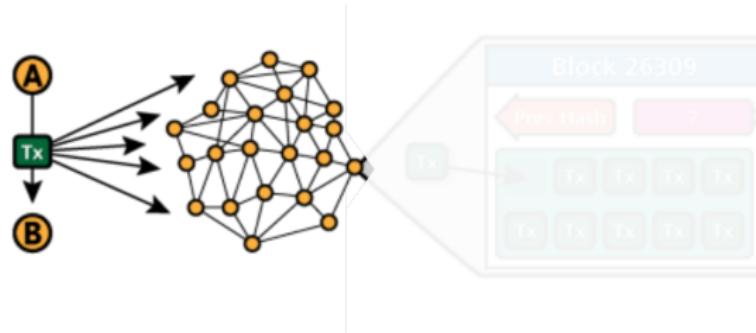
Illustration by CryptoGraphics.info

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

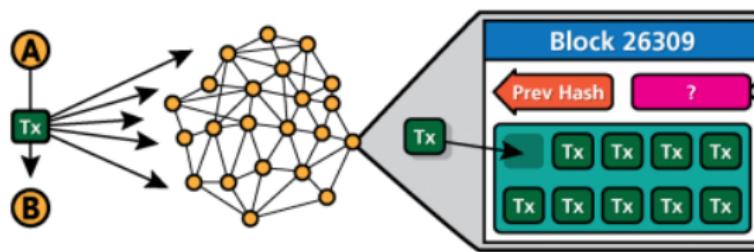
Il faut former la plus longue chaîne possible !

Plus techniquement comment cela fonctionne ?



Tx : ".1 BTC pour Bob, signé Alice"

Plus techniquement comment cela fonctionne ?



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

Plus techniquement comment cela fonctionne ?

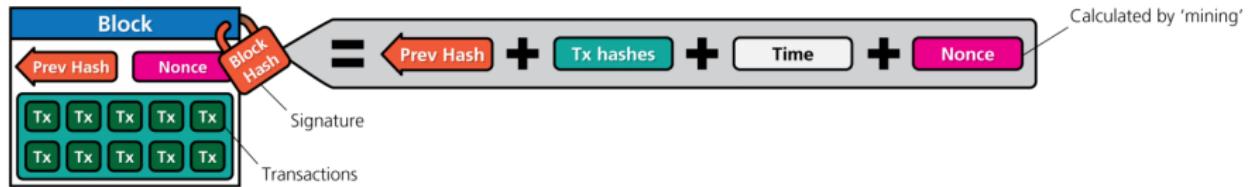


Illustration by CryptoGraphics.info

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

- ▶ il contient une récompense (coinbase)

Plus techniquement comment cela fonctionne ?

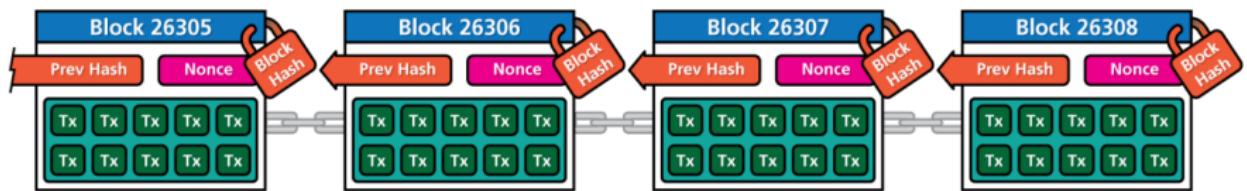


Illustration by CryptoGraphics.info

Les autres mineurs :

- ▶ Vérifient le nonce
- ▶ Ajoutent le nouveau block à la chaîne
- ▶ Recommencent la course pour
 1. allonger la chaîne
 2. obtenir des bitcoins

Alors c'est quoi le Bitcoin dans tout ça ?



À quoi ça sert ?

- ▶ C'est une unité de compte
 - ▶ C'est la récompense pour les mineurs
- ▶ Ça devient un moyen d'échange
- ▶ Ça devient une réserve de valeur

Alors c'est quoi le Bitcoin dans tout ça ?



À quoi ça sert ?

- ▶ C'est une unité de compte
 - ▶ C'est la récompense pour les mineurs
- ▶ Ça devient un moyen d'échange
- ▶ Ça devient une réserve de valeur

Alors c'est quoi le Bitcoin dans tout ça ?



À quoi ça sert ?

- ▶ C'est une unité de compte
 - ▶ C'est la récompense pour les mineurs
- ▶ Ça devient un moyen d'échange
- ▶ Ça devient une réserve de valeur

On ne le mange pas mais il fait manger depuis 2009 !



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

Sommaire

1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

2. Smart-contract

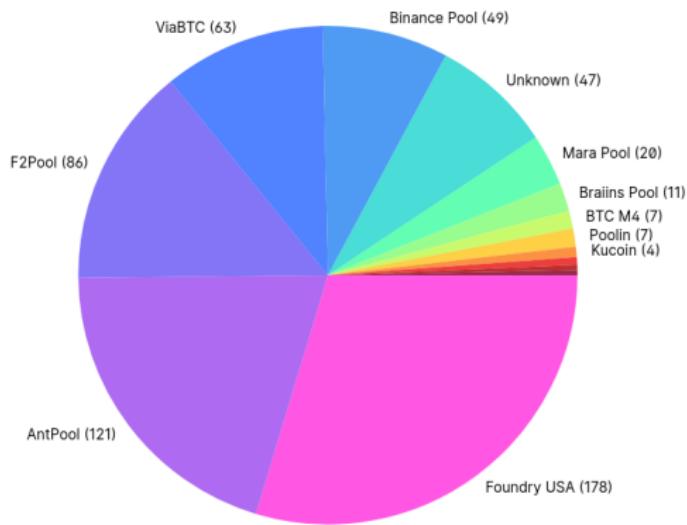
Cardano : blockchain de 3^e génération

A quoi peuvent servir les smart contract ?

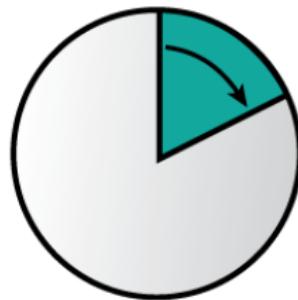
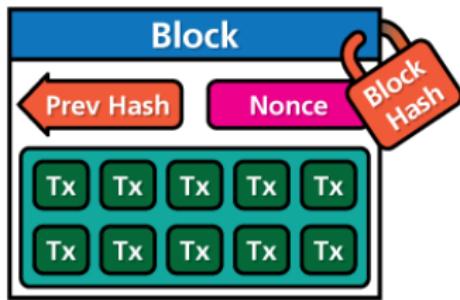
Coût énergétique



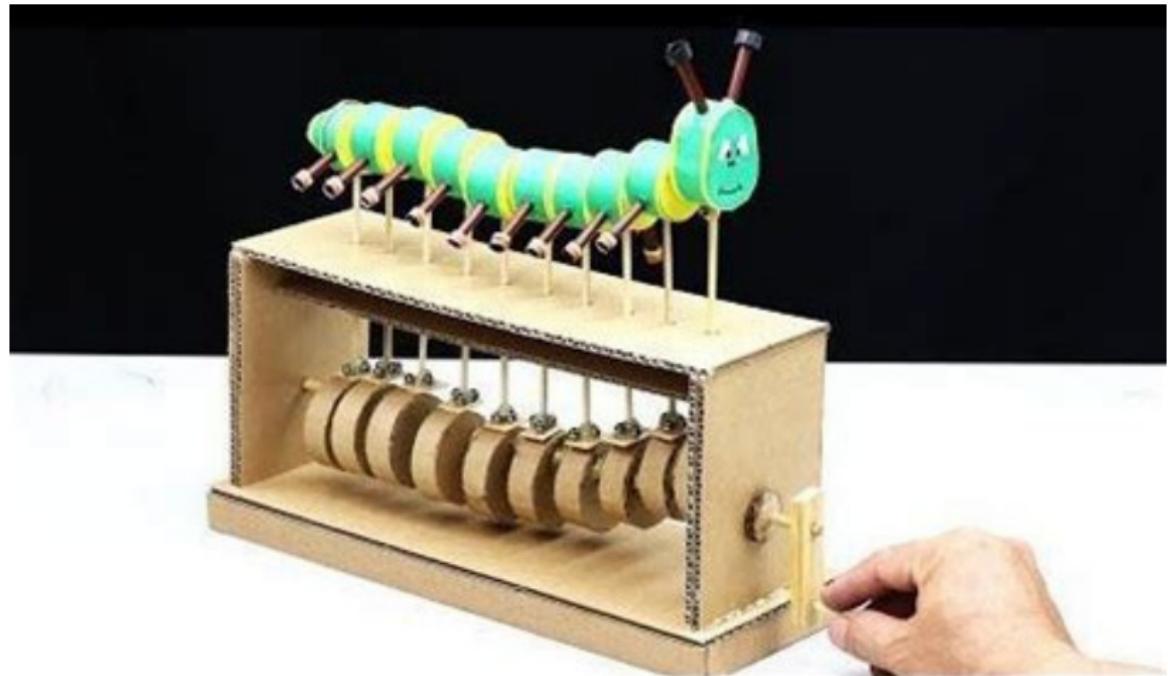
Concentration du hashrate (Juillet 2023)



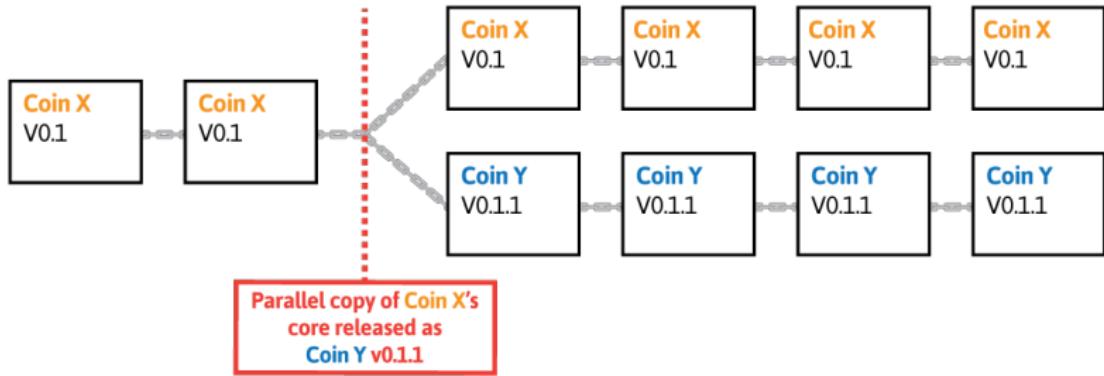
Vitesse de traitement des transactions



Jeux d'instructions limités



Difficile à adapter : Hard-forks



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 des transactions

Manque d'adaptabilité

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 des transactions

Manque d'adaptabilité

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 des transactions

Manque d'adaptabilité

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 des transactions

Manque d'adaptabilité

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 des transactions

Manque d'adaptabilité

Sommaire

1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

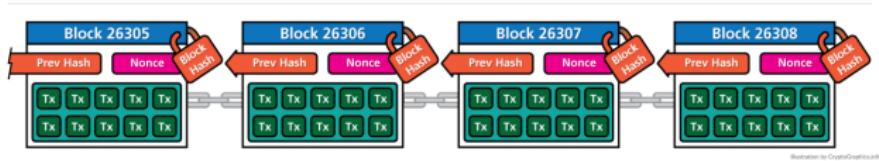
Pour conclure sur la blockchain

2. Smart-contract

Cardano : blockchain de 3^e génération

A quoi peuvent servir les smart contract ?

La blockchain



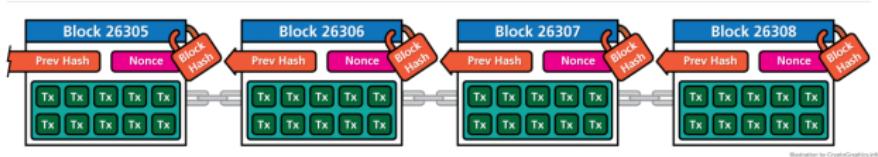
c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

La blockchain



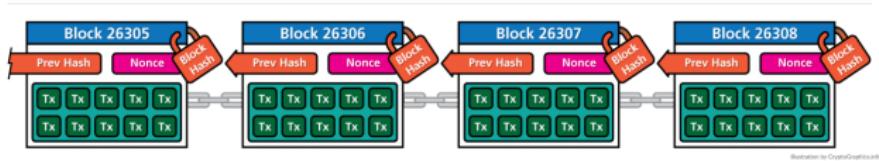
c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

La blockchain



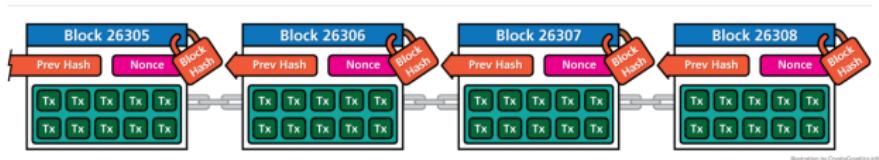
c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

La blockchain



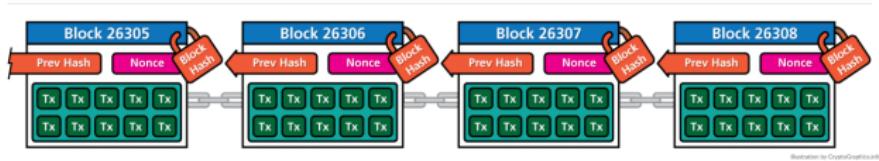
c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

La blockchain



c'est

- ▶ Une technologie d'archivage sécurisée
- ▶ Distribuée
- ▶ Utilisant la cryptographie
- ▶ Fonctionnant sans autorité centrale ou tier de confiance
- ▶ Plus robuste

mais...

- ▶ Gourmande en espace et en ressources
- ▶ Lente
- ▶ Pas nécessairement anonyme
- ▶ Difficile à améliorer et à faire évoluer
- ▶ Plus compliquée

Sommaire

1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

2. Smart-contract

Cardano : blockchain de 3^e génération

A quoi peuvent servir les smart contract ?

Cardano : blockchain de 3^e génération

1, 2, et ⋯ 3 !

Originalité du projet

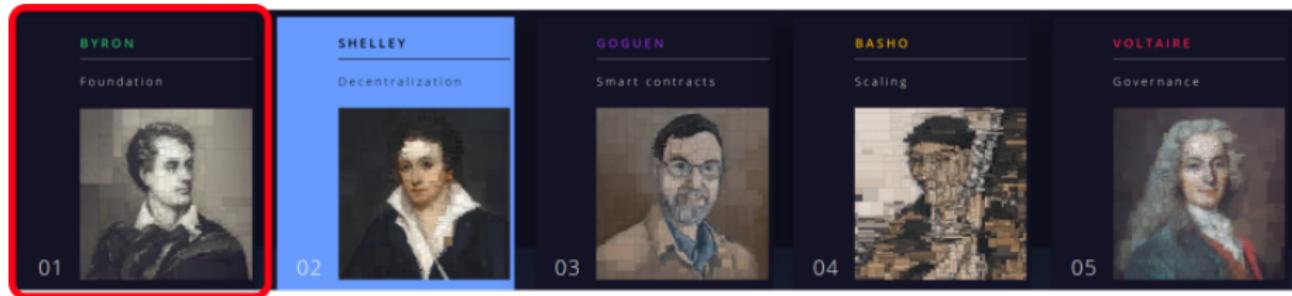
1^{er} blockchain scientifique



CARDANO

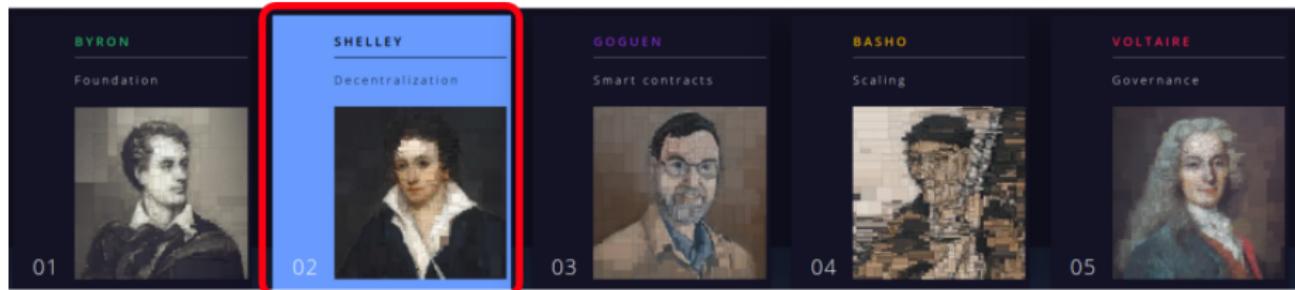
BYRON Foundation  01	SHELLEY Decentralization  02	GOGUEN Smart contracts  03	BASHO Scaling  04	VOLTAIRE Governance  05
---	---	---	---	--

Les fondations



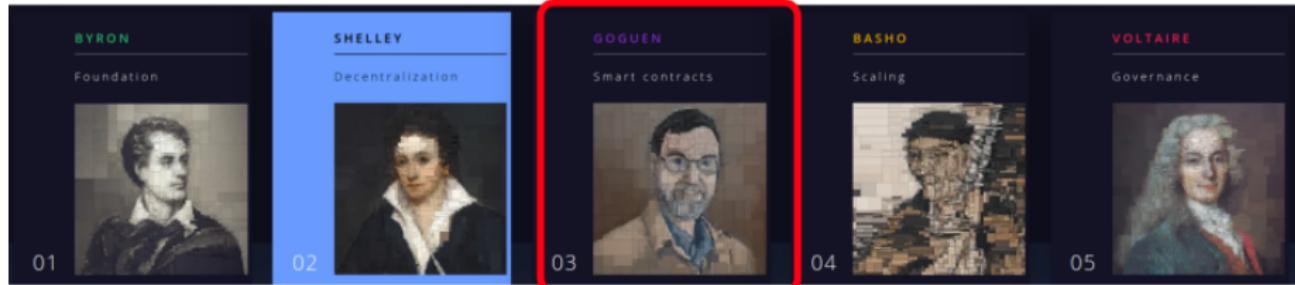
Ouroboros Proof of Stake

La décentralisation



Stacking et pools

Les smart-contract



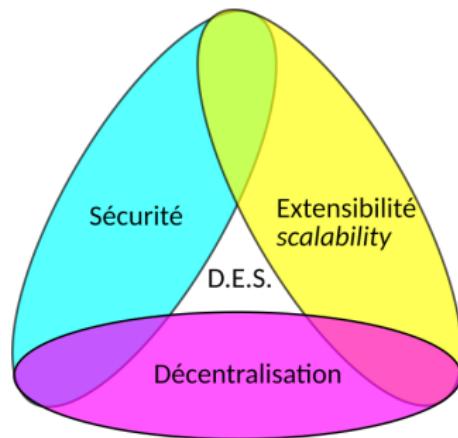
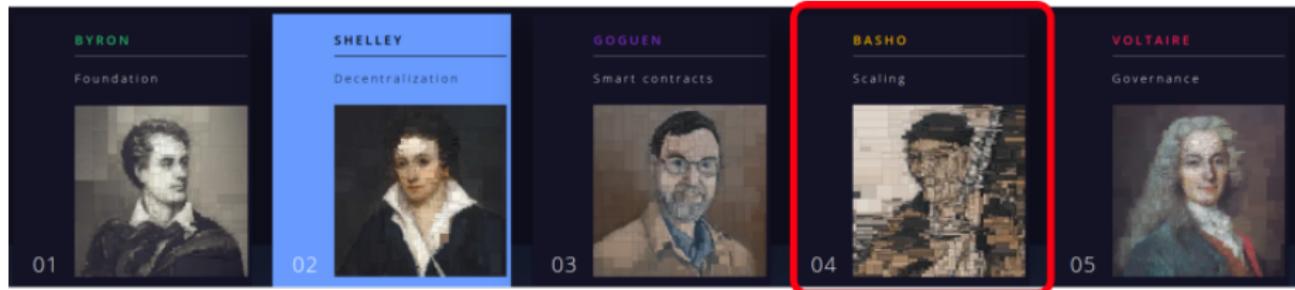
```
-- | Checks if a date is before the given end date.
beforeEnd :: Date -> EndDate -> Bool
beforeEnd (Date d) (Fixed e) = d <= e
beforeEnd (Date _) Never     = True

-- | Check that the date in the redeemer is before the limit in the datum.
validateDate :: Data -> Data -> Data -> ()
-- The 'check' function takes a 'Bool' and fails if it is false.
-- This is handy since it's more natural to talk about booleans.
validateDate datum redeemer _ = check $ case (fromData datum, fromData redeemer) of
    -- We can decode both the arguments at the same time: 'Just' means that
    -- decoding succeeded.
    (Just endDate, Just date) -> beforeEnd date endDate
    -- One or the other failed to decode.
    _                           -> False
```



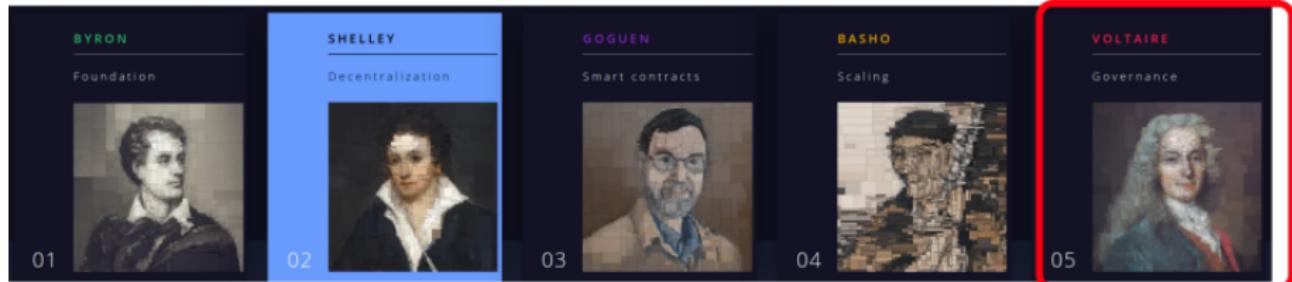
Smart-contract

Mise à l'échelle : plus Grand, plus Vite plus Robuste



Trilemme des blockchains
Bitcoin et blockchains

La gouvernance : reponsabilité et répartition du pouvoir



Voter pour le Trésor

Sommaire

1. Blockchain et Bitcoin

Notions de départ

Les types d'utilisateurs

La Naissance du Bitcoin

Que vaut la blockchain ?

Historique du cours du Bitcoin

Quel est le problème résolu

Les limites

Pour conclure sur la blockchain

2. Smart-contract

Cardano : blockchain de 3^e génération

A quoi peuvent servir les smart contract ?

Application purement financières

Collection de projets DEFI sur Cardano

- ▶ Sous-monnaies
 - ▶ stable coins (USDT)
- ▶ Produits dérivés
- ▶ Contrat hedging
 - ▶ assurances, SchellingCoin
- ▶ Compte d'épargne (Compound)
- ▶ Application notariale (Proof of Existence)
- ▶ contrat de travail (Ethlance)
- ▶ loterie (PoolTogether)
- ▶ Marché distribués (SundaeSwap)



Applications semi-financières

Monnaies et données

Être payés pour, ou fournir, des données (Ocean protocol)

Gestions des identités (Atala Prism)

- ▶ Gestion de nom de domaine (nameCoin)
- ▶ Gestion d'ID (uPort)
- ▶ Gestion de fichiers (filecoin)
- ▶ Gestion de contenu (streemit)
- ▶ Réseaux sociaux décentralisés (mastodon)



Applications semi-financières

Monnaies et données

Être payés pour, ou fournir, des données (Ocean protocol)

Gestions des identités (Atala Prism)

- ▶ Gestion de nom de domaine (nameCoin)
- ▶ Gestion d'ID (uPort)
- ▶ Gestion de fichiers (filecoin)
- ▶ Gestion de contenu (streemit)
- ▶ Réseaux sociaux décentralisés (mastodon)

Autres Applications :

- ▶ Calcul distribué (seti@home, folding@home)

Applications non-financières

- ▶ Vote en ligne
- ▶ Gouvernance décentralisé



Applications Autonomes et Décentralisé

DA : Decentralised Autonomous

- ▶ DAC communauté (vote égalitaire)
- ▶ DAC corporation (plutocratie)

DAO : Decentralised Autonomous Organisation

Peut fonctionner avec des individus ne parlant pas la même langue

- ▶ Automatise de la gouvernance
- ▶ Des techniques pour changer les règles de gouvernance

Divers

- ▶ ICO : Initial coin offering
- ▶ ASIC : Application specific integrated circuits



Merci et à bientôt

Wadaci -> Whatsapp et Telegram.

Contact -> Traoré Michel 01 60 302 718

Formulaire -> <https://tinyurl.com/adhesion-wadaci>



Issa Traoré (PhD)
Malik Koné (PhD)