La sécurité de Bitcoin

Pascal Lafourcade

Maître de conférences

LIMOS

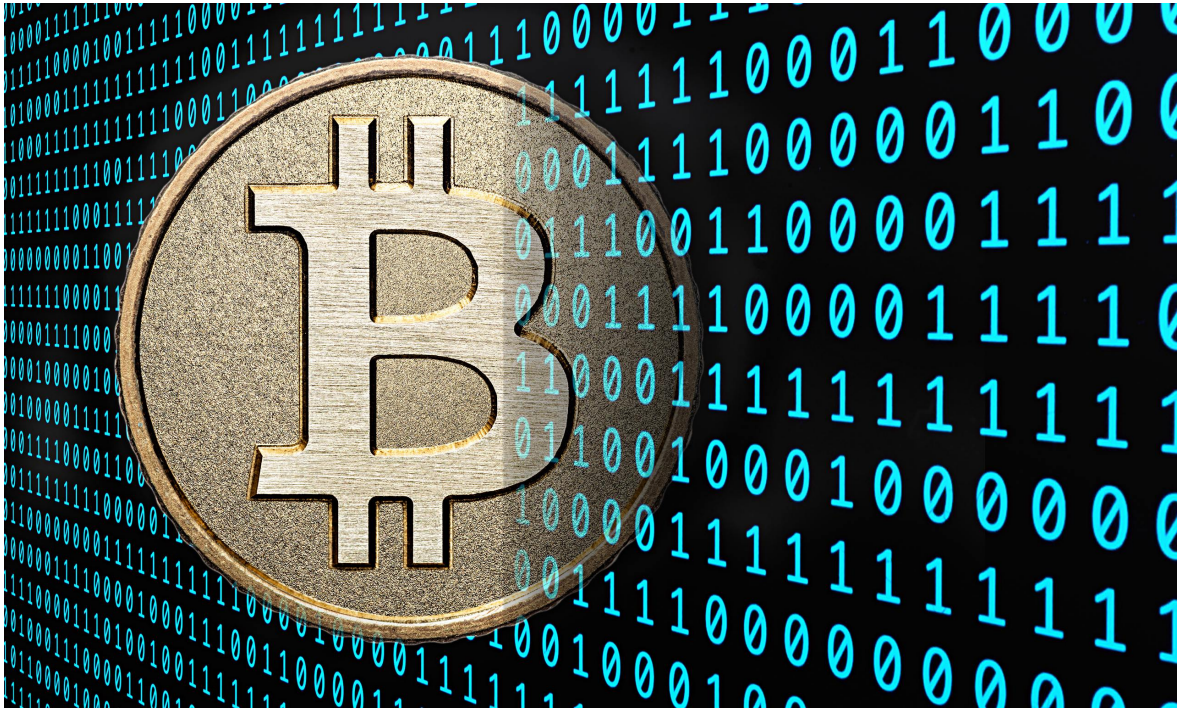
UNIVERSITÉ Clermont Auvergne

Mars 2018

TEDx Clermont

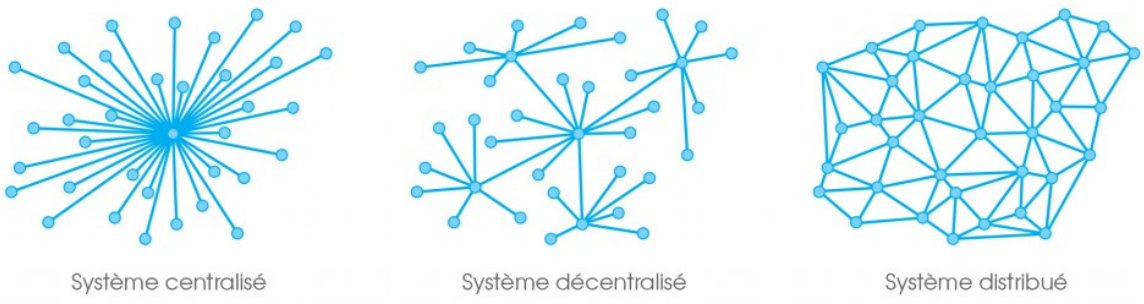
x = independently organized TED event

La révolution Bitcoin 2009



Bitcoin

- Cryto-monnaie décentralisée et distribuée



Source : blockchainfrance.net.

La revue européenne des médias et du numérique n° 37 - hiver 2015-2016 - http://la-rem.eu

Donc inarrêtable

21 millions BTC

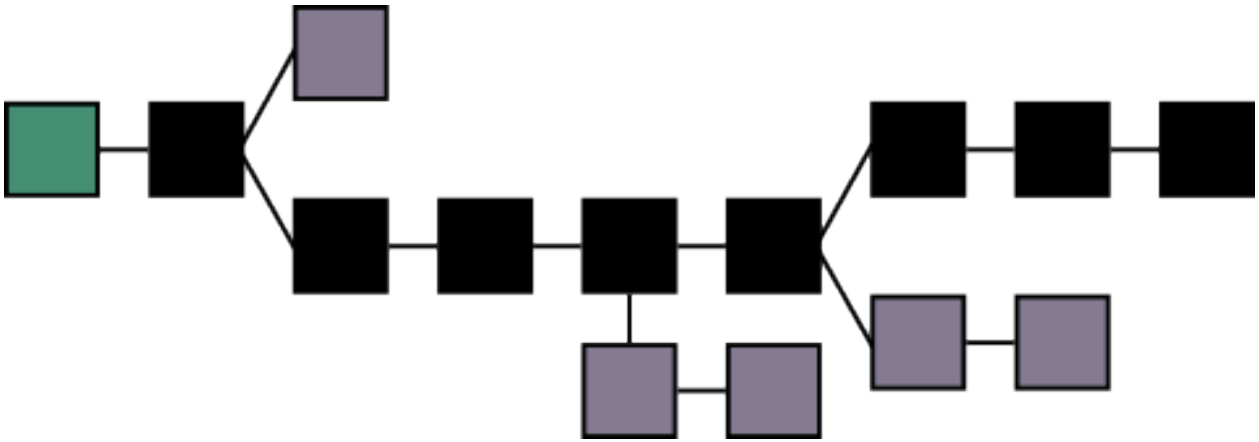
Propriétés d'une monnaie électronique

- Non-Falsifiable (Unforgeable)

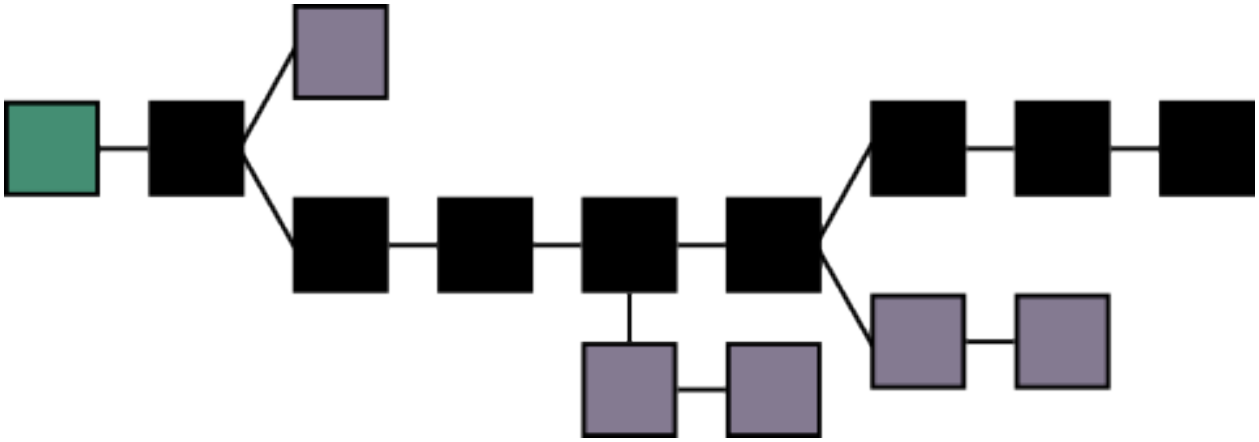
- Eviter la double dépense & identifiation fraudeur
  & "présemption d'innocence"

- Respect de la vie privée :
  - Anonymat faible : non identification d'un acheteur
  - Anonymat fort : non traçabilité d'un acheteur

Infalsifiable

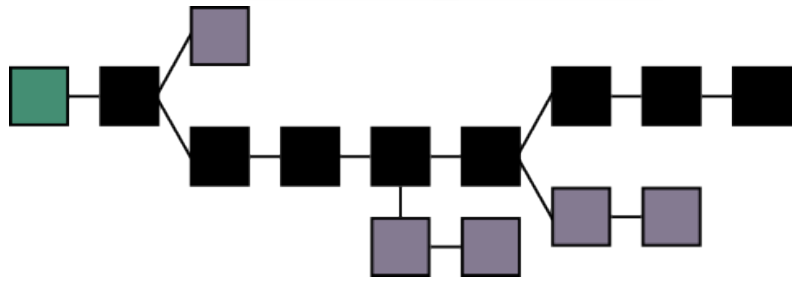


Infalsifiable



- Attaque de 51 %
- Hard fork

Auditable



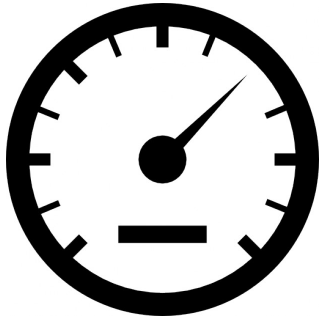
Traçable

Traçable

MONERO

ZCASH

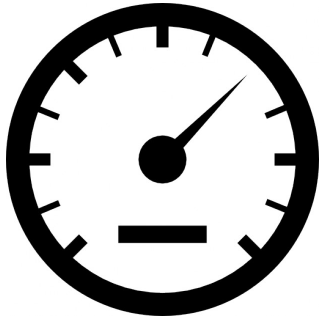
Limitations



10 minutes = 1 block

Taille des transactions 1 Mo

Limitations



10 minutes = 1 block

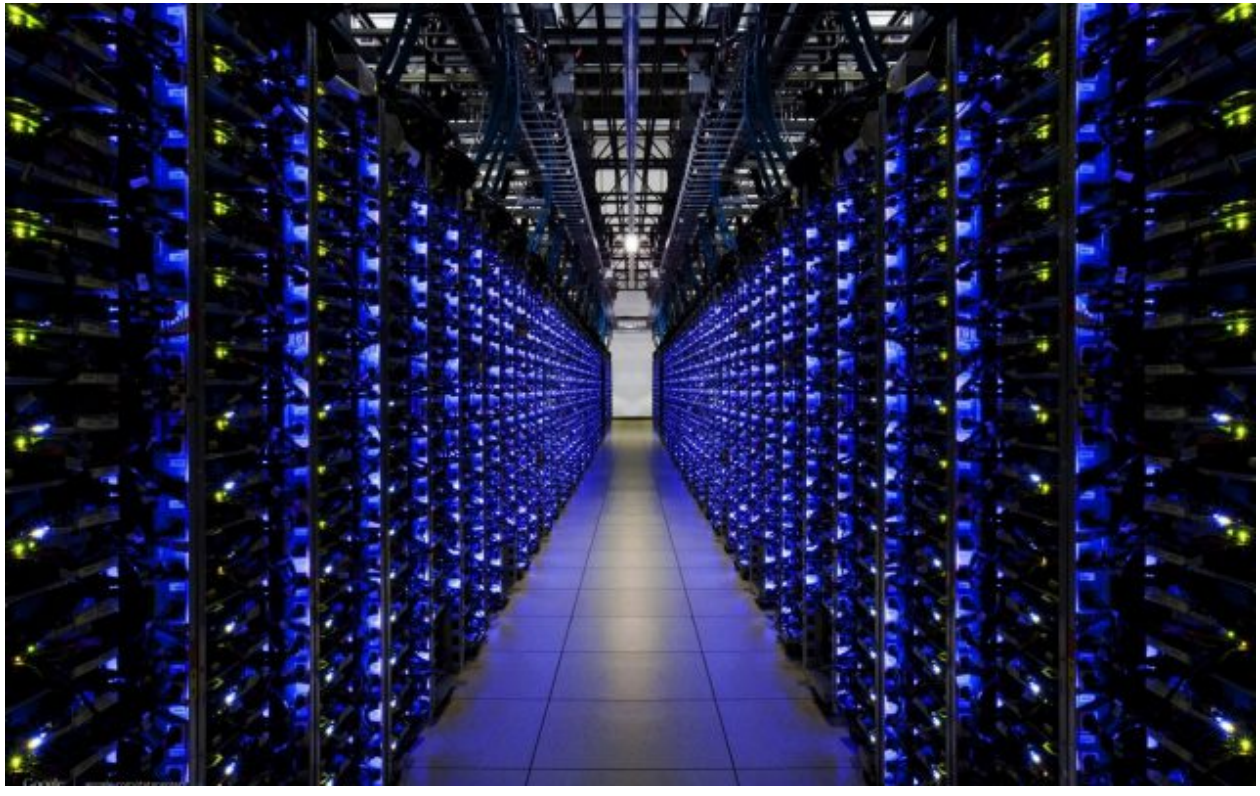
Taille des transactions 1 Mo

Lightning Network

ETHEREUM

12 secondes

Energievore



Energievore

Proof of Stake
Lightning Network

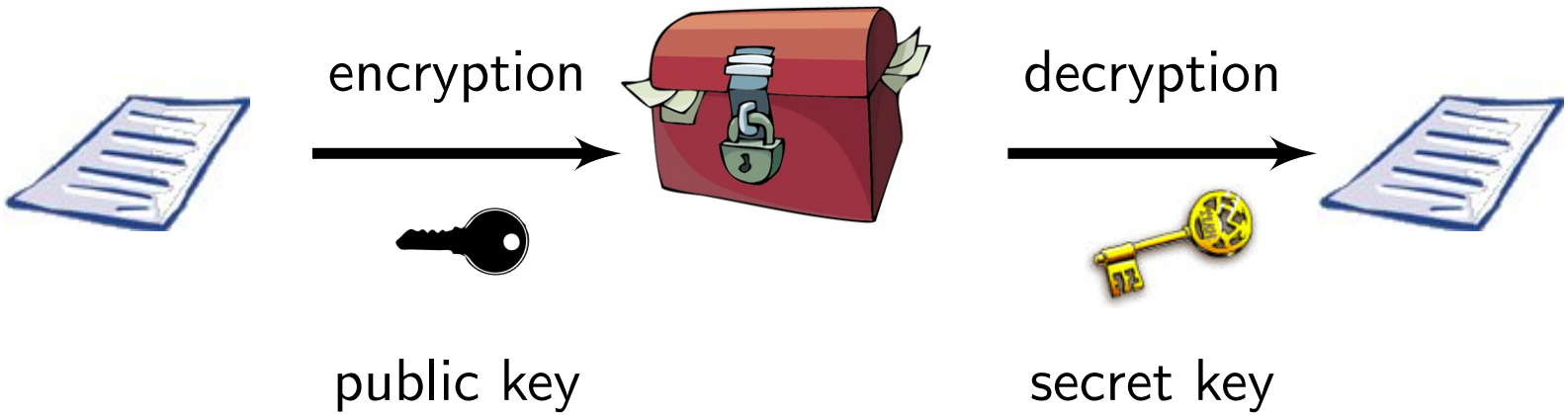
Merci pour votre attention

Les blockchains en 50 Questions ?

Comprendre le fonctionnement et les enjeux de cette technologie innovante

Juin 2018

Chiffrement à clef publique et signature



Chiffrement à clef publique et signature