

# Blockchains et Cryptomonnaies

Malik Koné

24 février 2021

# Sommaire

1. Introduction
2. Le Bitcoin et sa blockchain
3. Détails techniques
4. Les blockchains de 2ème et 3ème génération
5. La Crypto-économie
6. Conclusion

# Internet

HTTP - 1990



1995

TCP/IP - 1974



1984

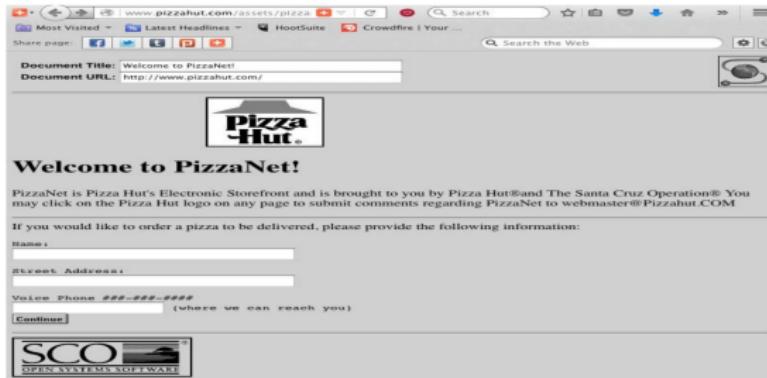
Ethernet - 1974



1979

# Comment commerçer sur Internet ?

Première vente : une pizza en 1994



## Le problème

Comment commerçer directement les uns avec les autres sans un intermédiaire de confiance ?

# Cryptographie

Comment communiquer en présence d'adversaires ?

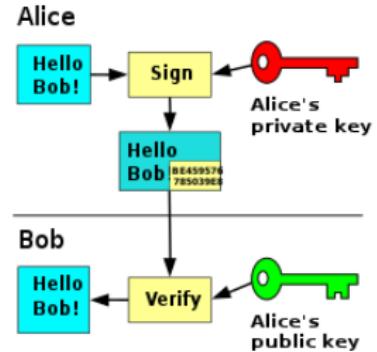


Scytale déchiffreur du temps de l'antiquité



L'enigma Machine.  
1920 - 2ème guerre

mondiale



Cryptographie asymétrique (de 1976 à aujourd'hui)

# De nombreuses tentatives de monnaies cryptographiques

- ▶ DigiCash (David Chaum) – 1989
- ▶ Mondex (National Westminster Bank) – 1993
- ▶ CyberCash (Lynch, Melton, Crocker & Wilson) – 1994
- ▶ E-gold (Gold & Silver Reserve) - 1996
- ▶ Hashcash (Adam Back) - 1997
- ▶ Bit Gold (Nick Szabo) - 1998
- ▶ B-Money (Wei Dai) - 1998
- ▶ Lucre (Ben Laurie) - 1999

... mais elles ont échouées

# Développement des moyen de paiements électroniques

SSL/TLS - 1996



1998

HTTP - 1990



1995

TCP/IP - 1974



1984

Ethernet - 1974



1979

# Bitcoin : un monnaie électronique décentralisée

From Satoshi Nakamoto <satoshi<at>vistomail.com>

Subject : Bitcoin P2P e-cashe 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."

*J'ai travaillé sur un nouveau système de paiement électronique direct sans tiers de confiance.*

# Un nouvelle couche Internet ?

les transactions programmables



2009

???

SSL/TLS - 1996



1998

HTTP - 1990



1995

TCP/IP - 1974



1984

Ethernet - 1974



1979  
24 février

# Enfin !

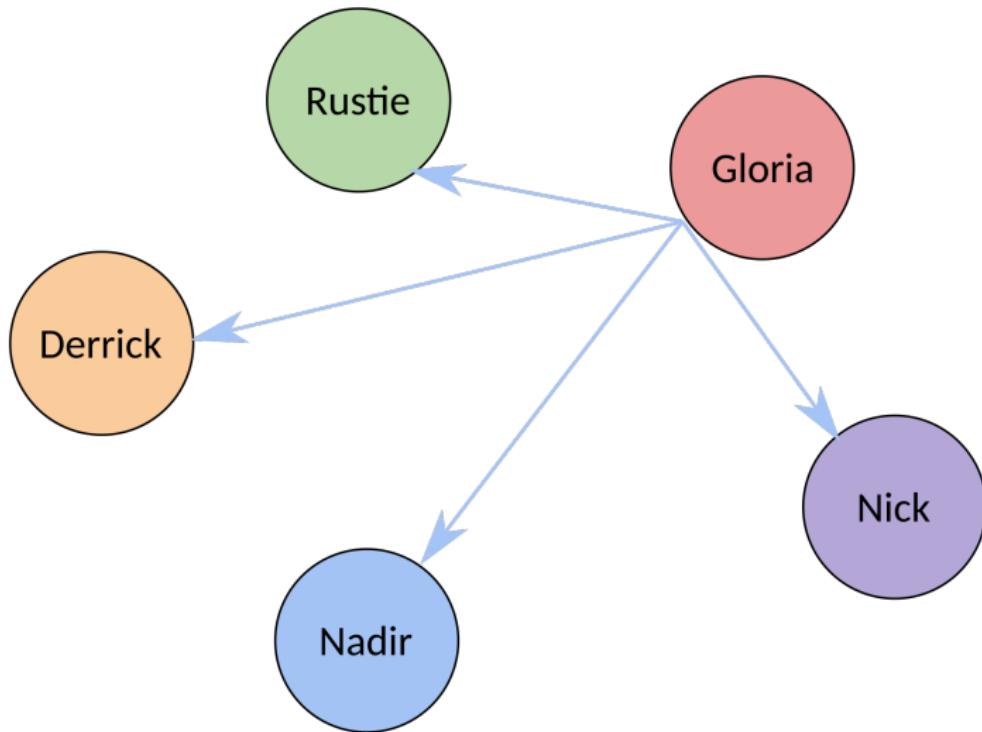
La première pizza achetée en ligne sans intermédiaires

Le 18 mai 2010, Une pizza pour des Bitcoin

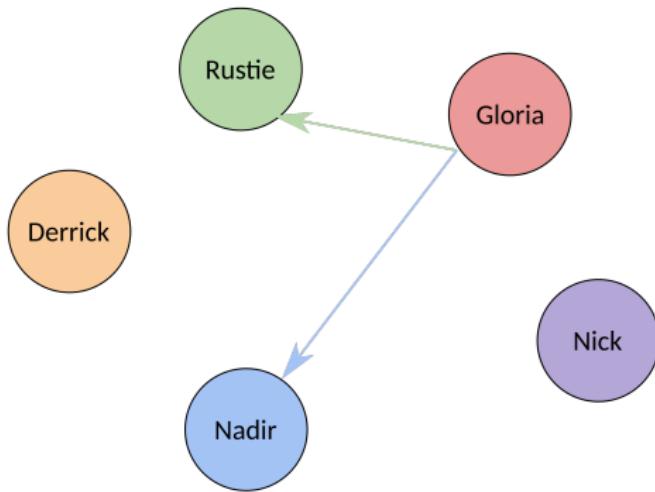


La blockchain est un journal comptable ouvert

# Diffuser ses transactions (utxo)

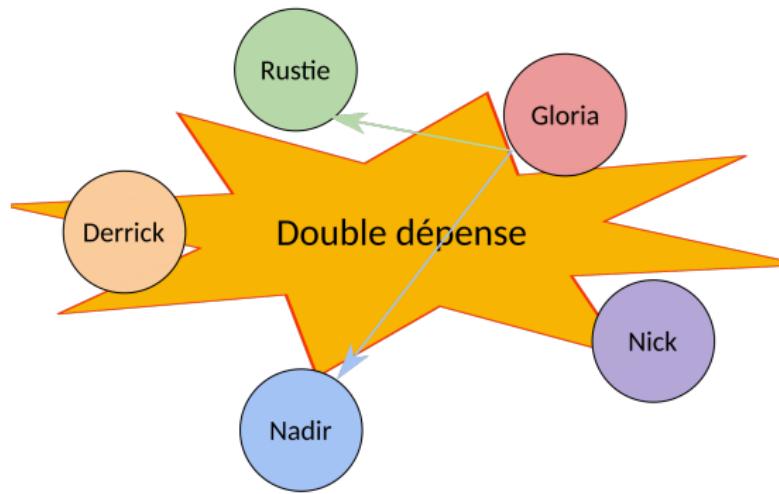


# L'attaque de la double dépense



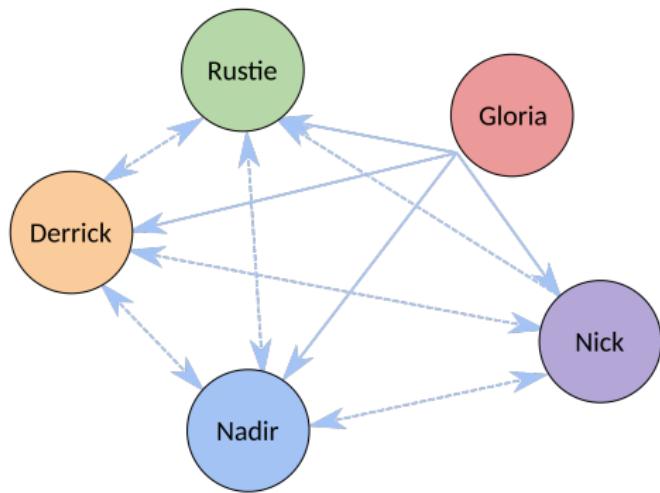
si c'est gloria qui informe tout le monde, qui l'empêche de dépenser deux fois le même montant ?

# L'attaque de la double dépense



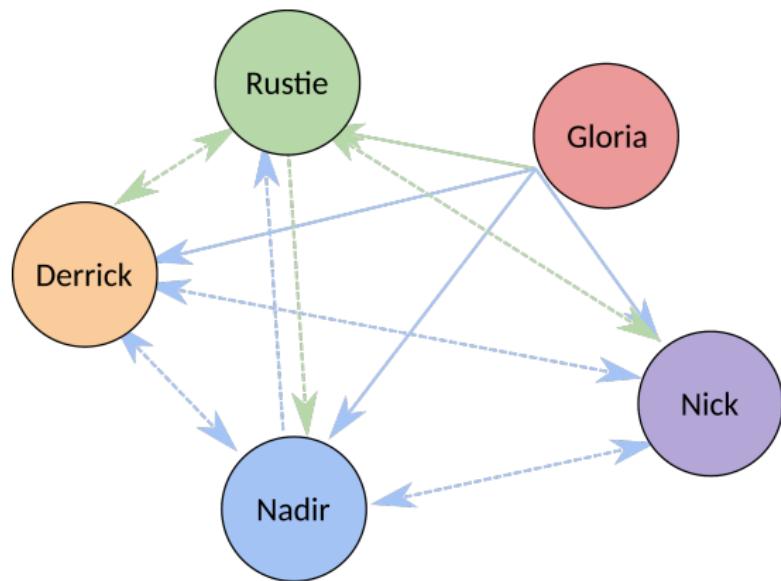
si c'est gloria qui informe tout le monde, qui l'empêche de dépenser deux fois le même montant ?

# La validation par les pairs



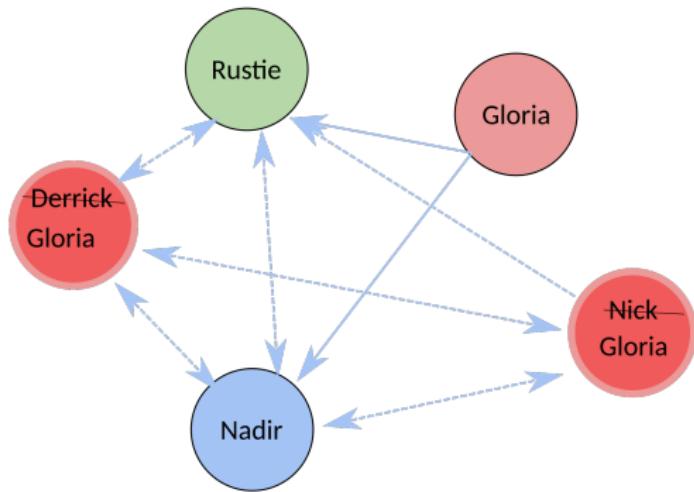
Un système de vote ?

## La validation par les pairs



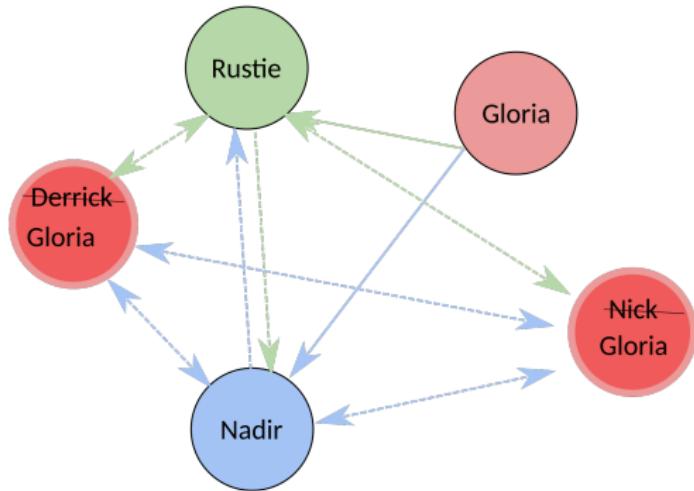
nécessite une majorité de personnes honêtes, mais...

# Etrange : L'attaque sybile



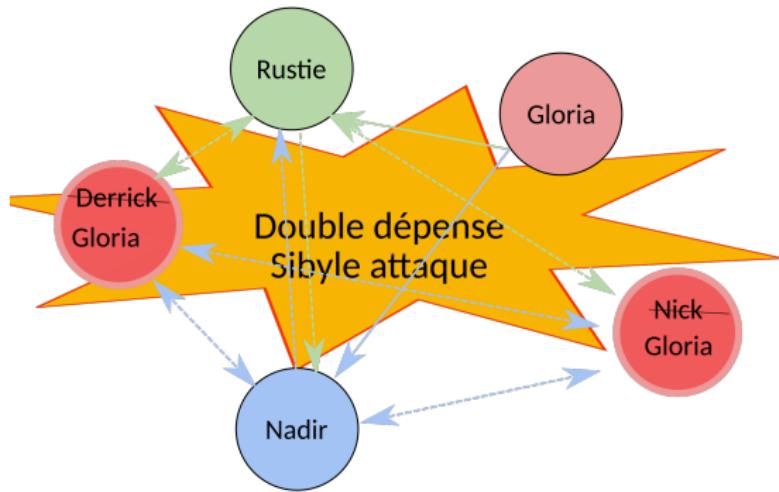
- ▶ Simple de générer des identités multiples pour approuver ses propres transactions
- ▶ une identité un vote, ne peut pas marcher.
- ▶ Le vote doit être couteux.

# Etrange : L'attaque sybile



- ▶ Simple de générer des identités multiples pour approuver ses propres transactions
- ▶ une identité un vote, ne peut pas marcher.
- ▶ Le vote doit être couteux.

# Etrange : L'attaque sybile

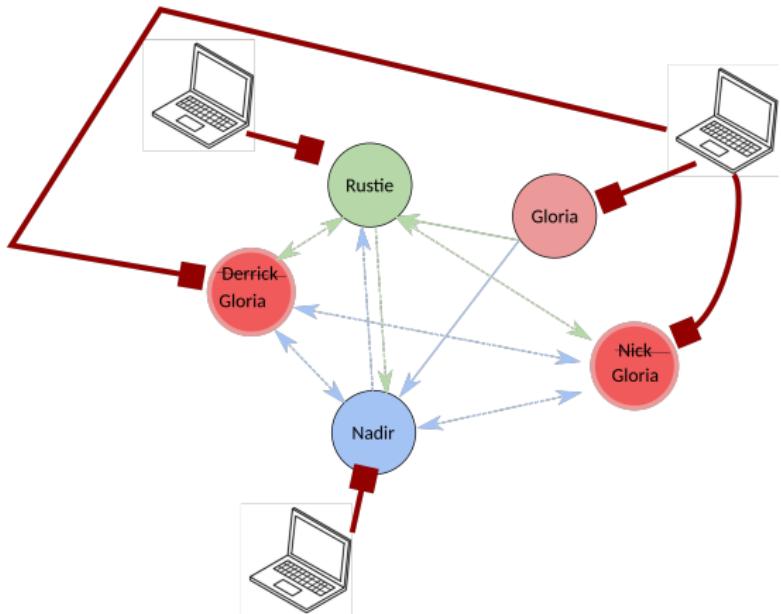


- ▶ Simple de générer des identités multiples pour approuver ses propres transactions
- ▶ une identité un vote, ne peut pas marcher.
- ▶ Le vote doit être couteux.

# Preuve par travail

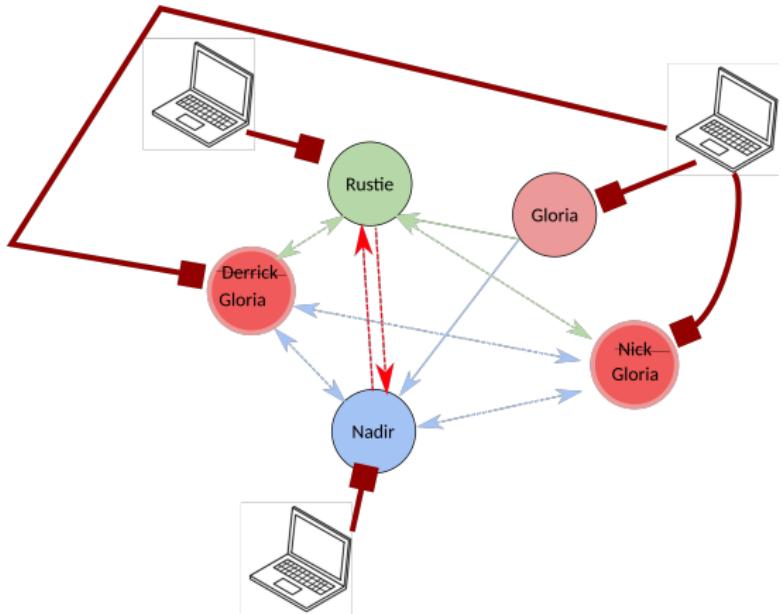
- ▶ Pour voter il faut faire quelque chose de difficile, où on ne peut pas tricher
- ▶ tester les solutions d'un problème au hasard, par exemple

# La preuve par la travail (suite)



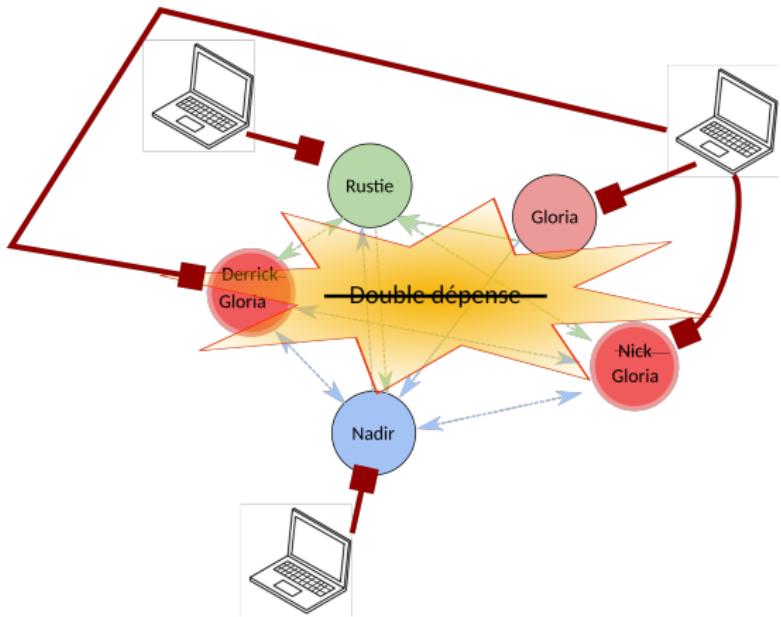
- ▶ eg. Un processeur un vote
- ▶ c'est couteux de falsifier
- ▶ ça marche

# La preuve par la travail (suite)



- ▶ eg. Un processeur un vote
- ▶ c'est couteux de falsifier
- ▶ ça marche

# La preuve par la travail (suite)



- ▶ eg. Un processeur un vote
- ▶ c'est couteux de falsifier
- ▶ ça marche

# Les limites de la blockchain bitcoin

- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ Coût énergétique
- ▶ Concentration du hashing power
- ▶ jeux d'instructions limités

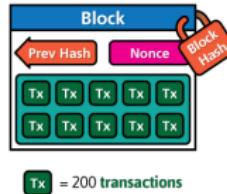
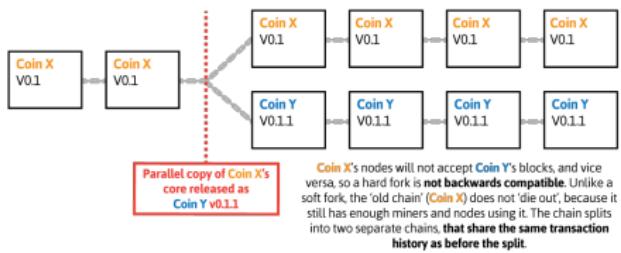


Illustration by CryptoGraphics.info

# Les limites de la blockchain bitcoin

- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ Coût énergétique
- ▶ Concentration du hashing power
- ▶ jeux d'instructions limités

Illustration by Cryptocomics.info

# Les limites de la blockchain bitcoin

- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ Coût énergétique
- ▶ Concentration du hashing power
- ▶ jeux d'instructions limités

# Les limites de la blockchain bitcoin

- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ Coût énergétique
- ▶ Concentration du hashing power
- ▶ jeux d'instructions limités

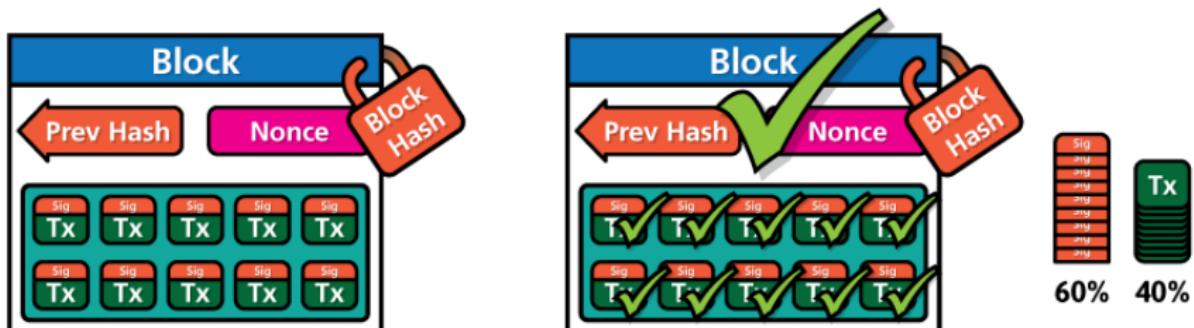
# Les limites de la blockchain bitcoin

- ▶ Vitesse de traitement des transactions
- ▶ Politique : forks
- ▶ Coût énergétique
- ▶ Concentration du hashing power
- ▶ jeux d'instructions limités

# Améliorer la vitesse des transactions

- ▶ segwit
- ▶ lightning network

# SegWit



**Tx** = 200 transactions

Illustration by CryptoGraphics.info

# SegWit

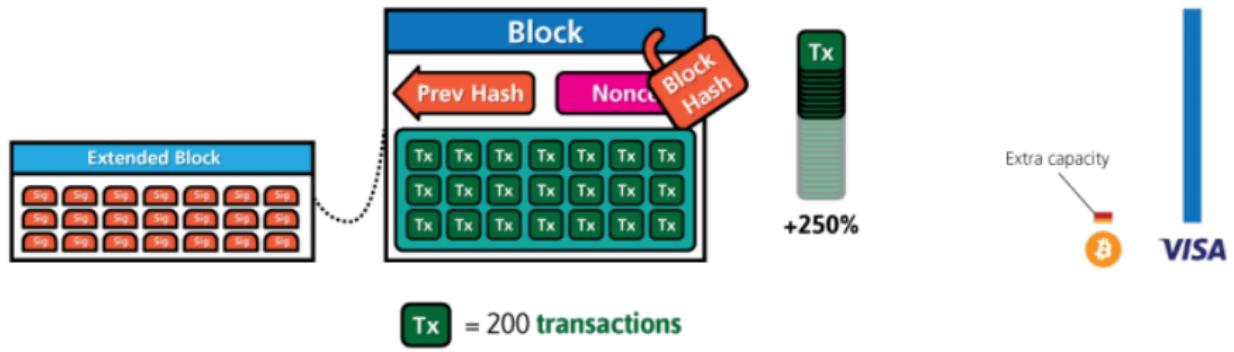
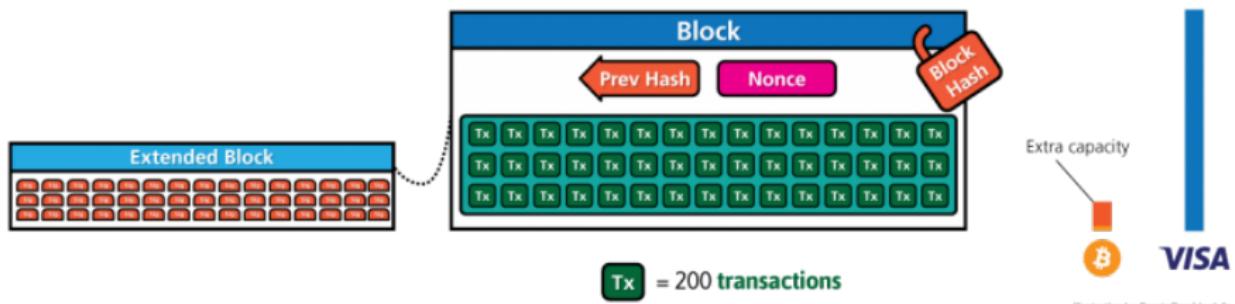
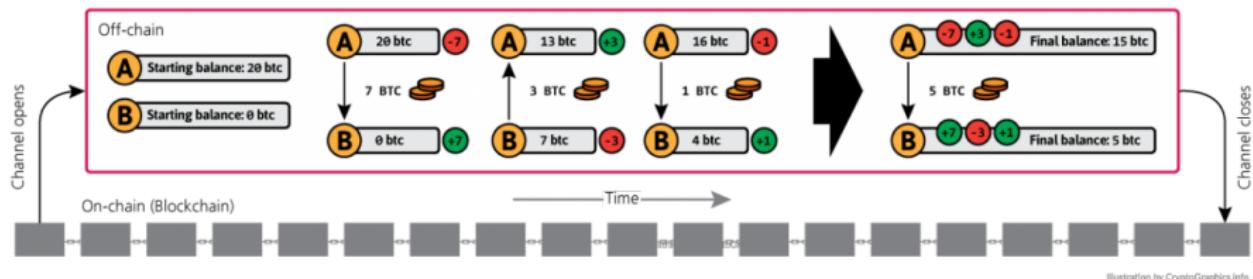


Illustration by CryptoGraphics.info

# SegWit 2x



# Lightning Network



# Lightning Network



# Etherum

Blockchain de 2ème génération : Turing Complet

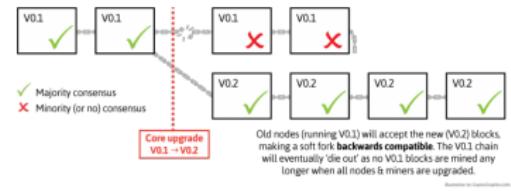
- ▶ Système comptable classique (pas d'utxo)
- ▶ Turing complet
- ▶ dApps et « smart-contrats »
- ▶ ETH et gaz



# Cardano

## Blockchain de 3ème génération : Politique et Trésor

- ▶ Des évolutions sans fork grâce à un Trésor
- ▶ Consensus : Proof of Stack (POS) et Ouroboros
- ▶ Smart Contract sécurisés
- ▶ Utxo



# Cardano



## Blockchain de 3ème génération : Politique et Trésor

- ▶ Des évolutions sans fork grâce à un Trésor
- ▶ Consensus : Proof of Stack (POS) et Ouroboros
- ▶ Smart Contract sécurisés
- ▶ Utxo

# Définition de la monnaie

Poids à peser Akan

## Classiquement

Une monnaie c'est :

1. Une réserve de valeur
2. un moyen (intermédiaire) pour les échanges
3. une unité de compte



# Historique des Monnaies

## Le Troc

- ▶ Matière vivante
  - ▶ pécule, pécuniaire, relatif au bétail
- ▶ Prêts avec intérêts à Babylone
  - ▶ mais annulation des dettes chaque 50 ans (jublié)



pecū (latin pour bétail)

# Historique des Monnaies



- ▶ d'où les salaire, le solde



- ▶ d'où les espèces
- ▶ pratique, inaltérable

# Historique des monnaies

## Banques & billets

- ▶ pièce de monnaie *de moindre valeur*,
  - ▶ garantie par l'État
- ▶ Bâtons de comptage
- ▶ Billets de banque :
  - ▶ vers 618 (Chine),
  - ▶ Conversion en or possible jusqu'en 1970 (USA)

# Historique des monnaies

## Banques & billets

- ▶ pièce de monnaie *de moindre valeur*,
  - ▶ garantie par l'État
- ▶ Bâtons de comptage
- ▶ Billets de banque :
  - ▶ vers 618 (Chine),
  - ▶ Conversion en or possible jusqu'en 1970 (USA)



Stock et Föld

# Historique des monnaies

## Banques & billets

- ▶ pièce de monnaie *de moindre valeur*,
  - ▶ garantie par l'État
- ▶ Bâtons de comptage
- ▶ Billets de banque :
  - ▶ vers 618 (Chine),
  - ▶ Conversion en or possible jusqu'en 1970 (USA)



Note de promesse,  
Jioazi (Chine) ;  
Continental Note (US)

# La Monnaie aujourd'hui

- ▶ Système de réserve fractionnaire
  - ▶ Billet de banque à valeur légale uniquement
    - ▶ *instrument de paiement en vigueur*
  - ▶ Preuve d'une dette
  - ▶ Argent électronique
    - ▶ compte en banque
    - ▶ des unités de compte



stock-exchange de WallStreet

# L'économie de la blockchain

Captation de la valeur

## L'Internet

### Couche Applicative



### Couche protocolaire (TCP /IP)

Captation de la valeur

## La Blockchain

### Front end



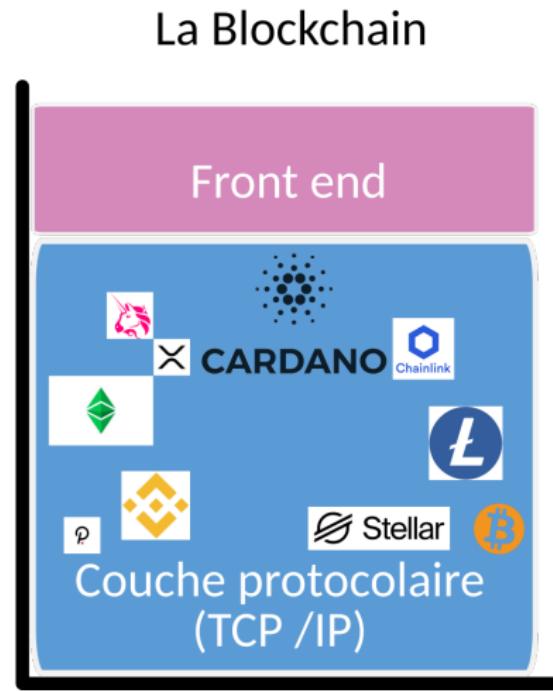
### Couche protocolaire (TCP /IP)

Différences entre Internet et la blockchain

# Les différents types de jetons électronique

- ▶ jeton utilitaires
- ▶ jeton d'applications
- ▶ jeton de sécurité
- ▶ jeton de protocol

Captation de la valeur



# Idées de dApps pour nos problèmes

- ▶ Transports
- ▶ Automatisation des Marchés
- ▶ Identité digitales
- ▶ Financements
- ▶ Application de téléphonie
- ▶ Paiements

# Challenges

- ▶ Questions techniques
- ▶ Concurrence avec les entreprises en place
- ▶ Questions légales

Merci

## Ressources et inspirations

- ▶ la blockchain au MIT ([OCW.mit.edu](https://ocw.mit.edu))
- ▶ la blockchain à Berkley (Edx)
- ▶ la cryptographie à Standford (Coursera)
- ▶ les dApps avec la fondation Linux (Coursera)