

# Introduction: le protocol du Bitcoin et le consensus

Malik Koné

July 27, 2020

# Sommaire

Qu'est ce que le Bitcoin?

L'identité

Clefs publiques et clefs privées

La transaction

Le modèle UTXO

La blockchain

Le consensus

La diffusion

La Validation

Preuve par le travail

En Résumé

# Concepts de base: Bitcoin et Blockchain

1 Crypto-monnaie et la plus connue. Elle est complétement digitale, décentralisée. Elle se base sur des principes de cryptographie et d'économie.

Le Bitcoin, fait référence:

- ▶ à une communauté, au réseau et au logiciel
- ▶ c'est une unité monétaire
- ▶ scripts pour des transferets conditionnés (smart contracts)



La blockchain

- ▶ une structure de données qui concerne l'historique des événements (pas seulement des transactions)

# génèse du bitcoin : le mouvement cypherpunk

cypherpunk (ou  
crypto-anarchistes)

- ▶ des libertaires
- ▶ Liberté individuelle
- ▶ Propriété privée
- ▶ Technophiles

Exemple

- ▶ Julian Assange
- ▶ Anonymous
- ▶ Edward Snowden



# L'innovation de "Satoshi Nakamoto"

Problèmes des systèmes décentralisés:

- ▶ Problème de la double dépense
- ▶ Journaux comptables différents
- ▶ Victimes de personnes malicieuses

La blockchain et le protocole de consensus sont une solution



# Bitcoin et Banques

## Méfiance vis à vis des banques

- ▶ Elles savent qui sont leur clients
- ▶ Elles seules garantissent l'intégrité des transactions
- ▶ Elles collectent puis redistribuent les fonds
- ▶ Elles sont sujettes aux lois des gouvernements

## Confiance dans la blockchain

- ▶ Les utilisateurs gèrent eux même leur vraie identité
- ▶ Tout le monde peut vérifier les transactions
- ▶ les fonds sont envoyés directement d'un utilisateur à l'autre
- ▶ Il y a de la confiance car tout le monde est sujet au même algorithme de consensus

# Identité

Qu'est ce qu'une preuve d'identité ?

A quoi ça peut servir ?

(dans le contexte des transaction financières)

- ▶ *Pause 15 minutes, donnez vos réponses sur*  
<http://edu.numerique.ci/moodle>

# Identité (suite)

## Dans le contexte financier

- ▶ Sert s'authentifier
  - ▶ recevoir de l'argent
  - ▶ dépenser son l'argent
  - ▶ réclamer et prouver la propriété de biens
- ▶ Sert à la tracabilité

## Dans la vie de tous les jours

- ▶ Numéros de téléphones et codes pin
- ▶ Adresses postales et clefs de boites au lettre
- ▶ Clefs publiques et Clefs privées

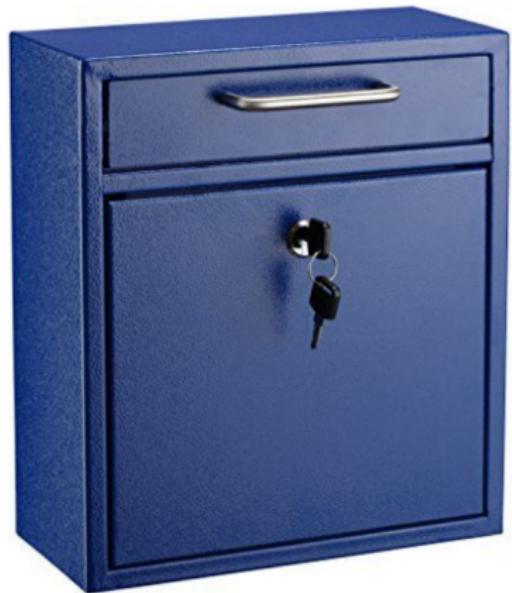
# Clefs publiques et clefs privées

## Analogy

- ▶ Clef privée : clef physique
- ▶ Clef publique: l'adresse, la porte

## Utilité

- ▶ clef publique pour recevoir (à peu près)
- ▶ clef privée pour récupérer et prouver que c'est à vous.



# Création des clefs

- ▶ La clef privée: un nombre au hasard parmis  $2^{160}$  possibilités

# Création des clefs

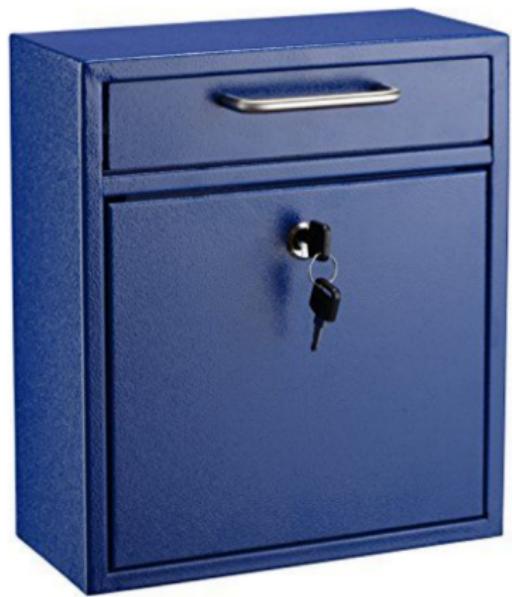
- ▶ La clef privée: un nombre au hasard parmis  $2^{160}$  possibilité
- ▶ La clef publique, générée à partir de la clef privée

# Création des clefs

- ▶ La clef privée: un nombre au hasard parmis  $2^{160}$  possibilité
- ▶ La clef publique, générée à partir de la clef privée
- ▶ Les addresses publiques sont générées à partir de la clef publique

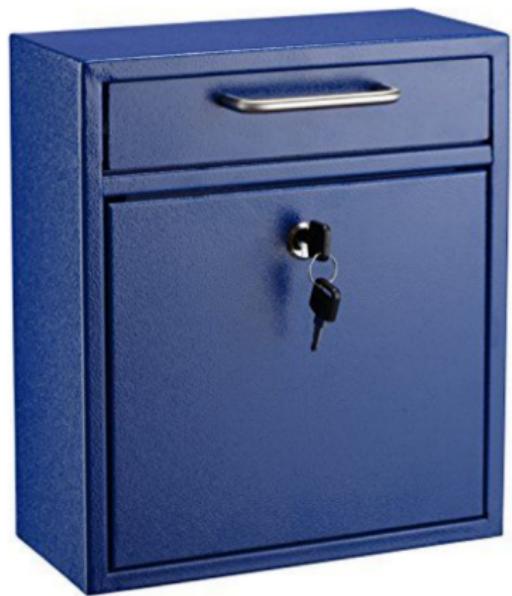
# Sécurité des clefs

- ▶  $2^{160}$  clefs possibles,



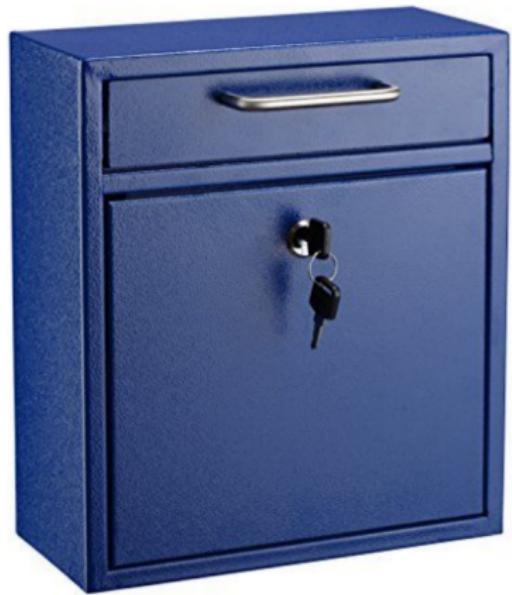
# Sécurité des clefs

- ▶  $2^{160}$  clefs possibles,
- ▶ environs  $2^{63}$  grains de sable sur terre



# Sécurité des clefs

- ▶  $2^{160}$  clefs possibles,
- ▶ environs  $2^{63}$  grains de sable sur terre
- ▶ Chance d'avoir le même grain de sable  
 $<0.0001\%$



# Sécurité des clefs

- ▶  $2^{160}$  clefs possibles,
- ▶ environs  $2^{63}$  grains de sable sur terre
- ▶ Chance d'avoir le même grain de sable  
 $<0.0001\%$
- ▶ Il y a des milliard de milliards d'adresses pour tous les humains



# Validité d'une transaction

*pause (10 minutes)*

- ▶ Qu'est qui rend une transaction valide ?
- ▶ répondre dans <http://edu.numerique.ci/moodle>

# Validité d'une transaction (suite)

- ▶ une signature
- ▶ disponibilité des fonds
- ▶ ne pas faire cette transaction avec quelqu'un d'autre au même moment

## Exemples ?

- ▶ par chèque
- ▶ avec des Espèces
- ▶ avec orange monney

# Le Modèle UTXO

UTXO : Unspent transaction Output (transaction non utilisée). C'est la façon dont les paiement se font avec les bitcoins

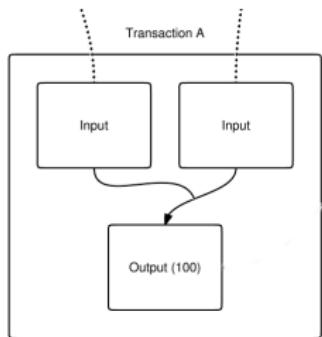
- ▶ Banques et comptes bancaires
- ▶ tirelires
  - ▶ Plus simple, mais nécessite de garder une trace de ses tirelires

## Pratique

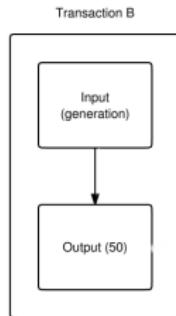
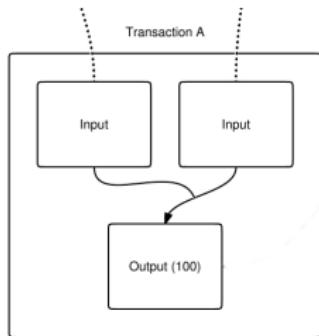
- ▶ Allons voir des transactions sur un explorateur de bloc
- ▶ le premier bloc
- ▶ une [un bloc plus récent](#)

Liens sur [edu.numerique.ci/moodle](http://edu.numerique.ci/moodle)

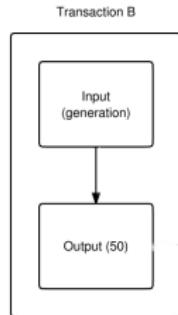
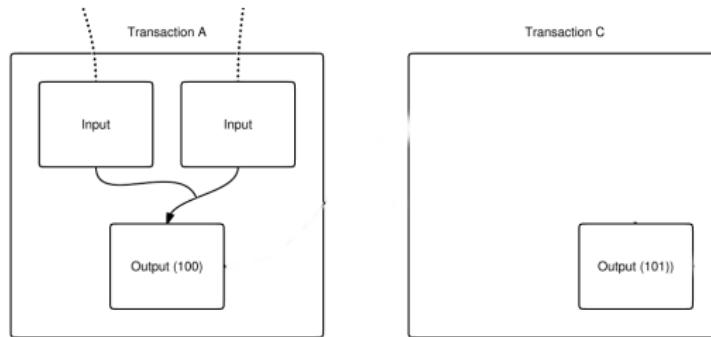
# UTXO en détail



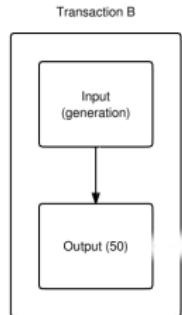
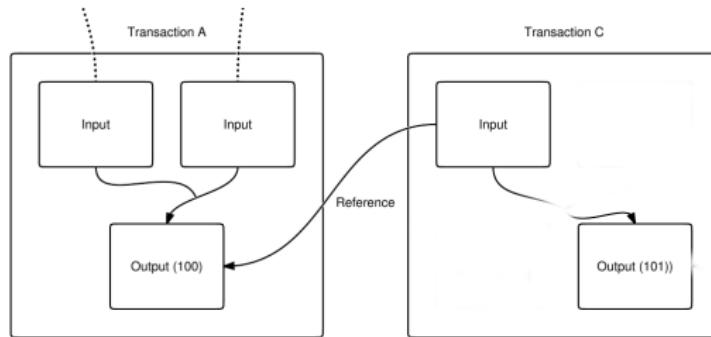
# UTXO en détail



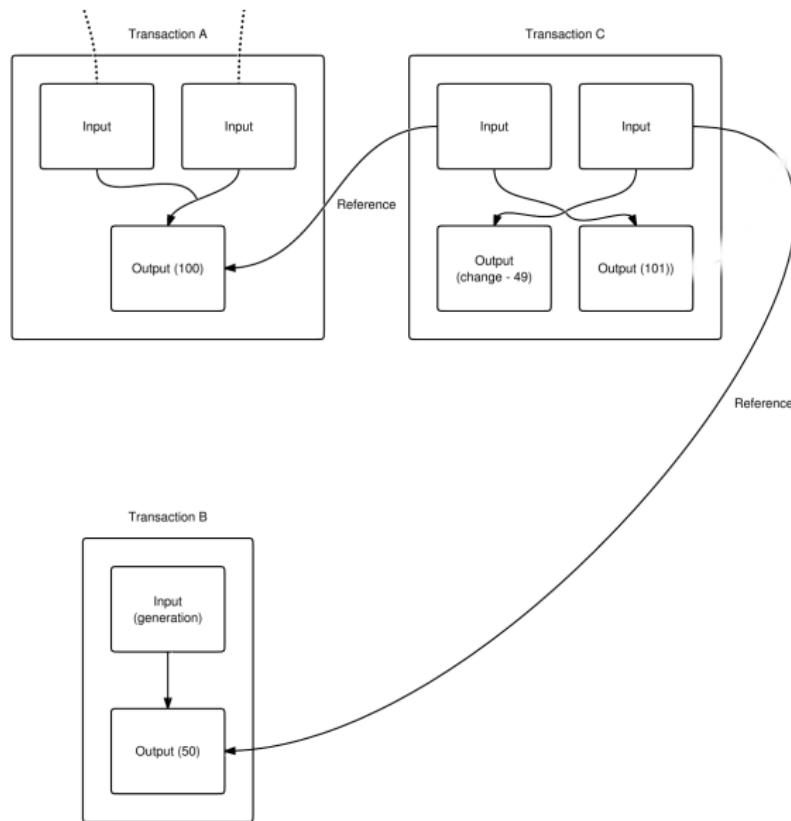
# UTXO en détail



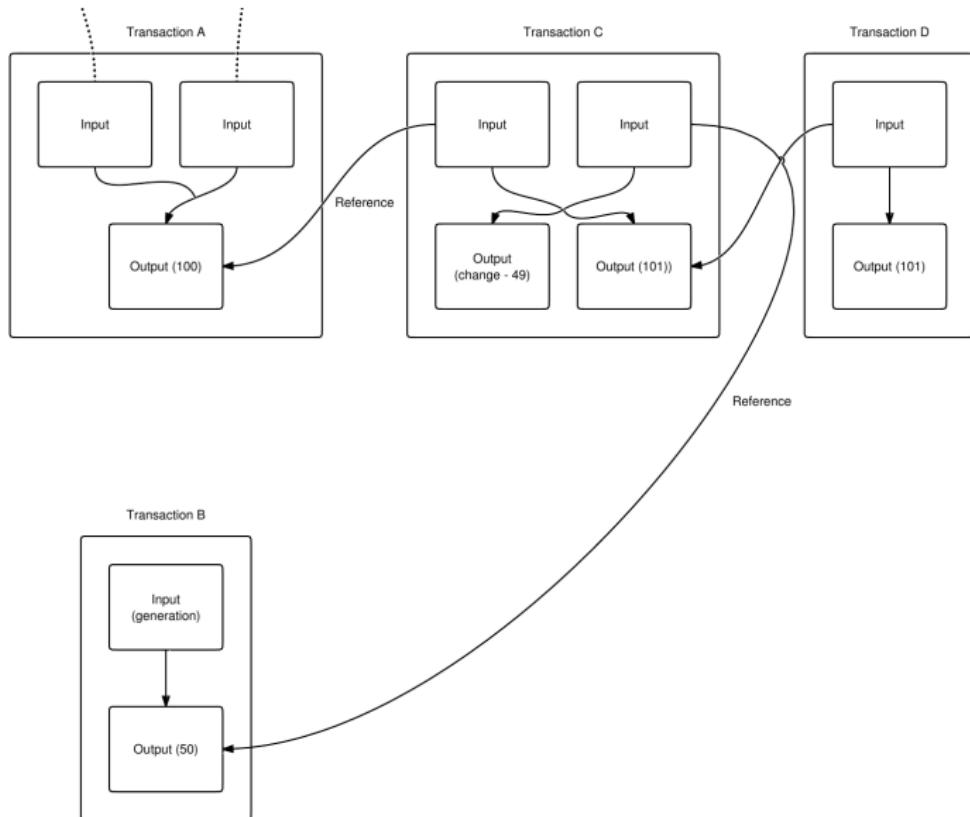
# UTXO en détail



# UTXO en détail



# UTXO en détail



# Base de données distribuée

- ▶ DLT: Distributed Ledger Technologie (ou journal comptable distribué)

## Histoire comptable

# Base de données distribuée

- ▶ DLT: Distributed Ledger Technologie (ou journal comptable distribué)

## Histoire comptable

- ▶ Journal simple ≈ 3000 av JC (Inde)

# Base de données distribuée

- ▶ DLT: Distributed Ledger Technologie (ou journal comptable distribué)

## Histoire comptable

- ▶ Journal simple ≈ 3000 av JC (Inde)
- ▶ Journal à deux entrées ≈ 1340 ap JC (Italy)

# Base de données distribuée

- ▶ DLT: Distributed Ledger Technologie (ou journal comptable distribué)

## Histoire comptable

- ▶ Journal simple ≈ 3000 av JC (Inde)
- ▶ Journal à deux entrées ≈ 1340 ap JC (Italy)
- ▶ Journal à entrées multiples ≈ 2008 ap JC (Internet)

# Base de données distribuée

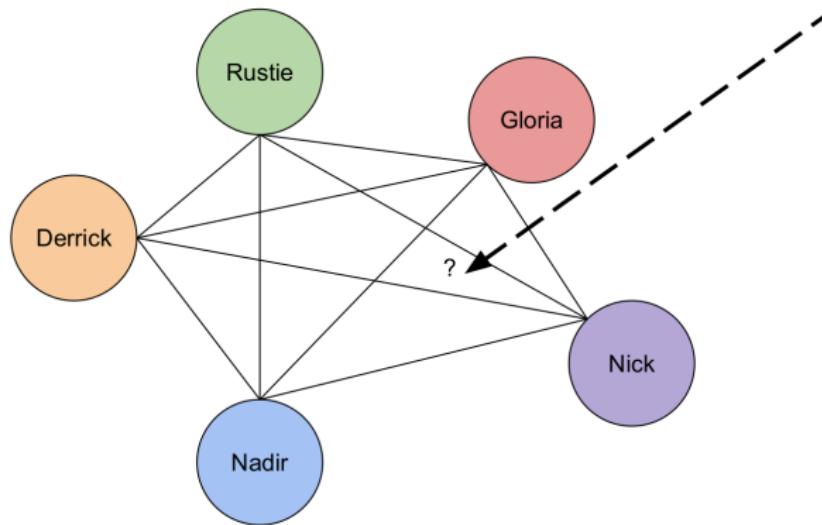
- ▶ DLT: Distributed Ledger Technologie (ou journal comptable distribué)

## Histoire comptable

- ▶ Journal simple ≈ 3000 av JC (Inde)
- ▶ Journal à deux entrées ≈ 1340 ap JC (Italy)
- ▶ Journal à entrées multiples ≈ 2008 ap JC (Internet)

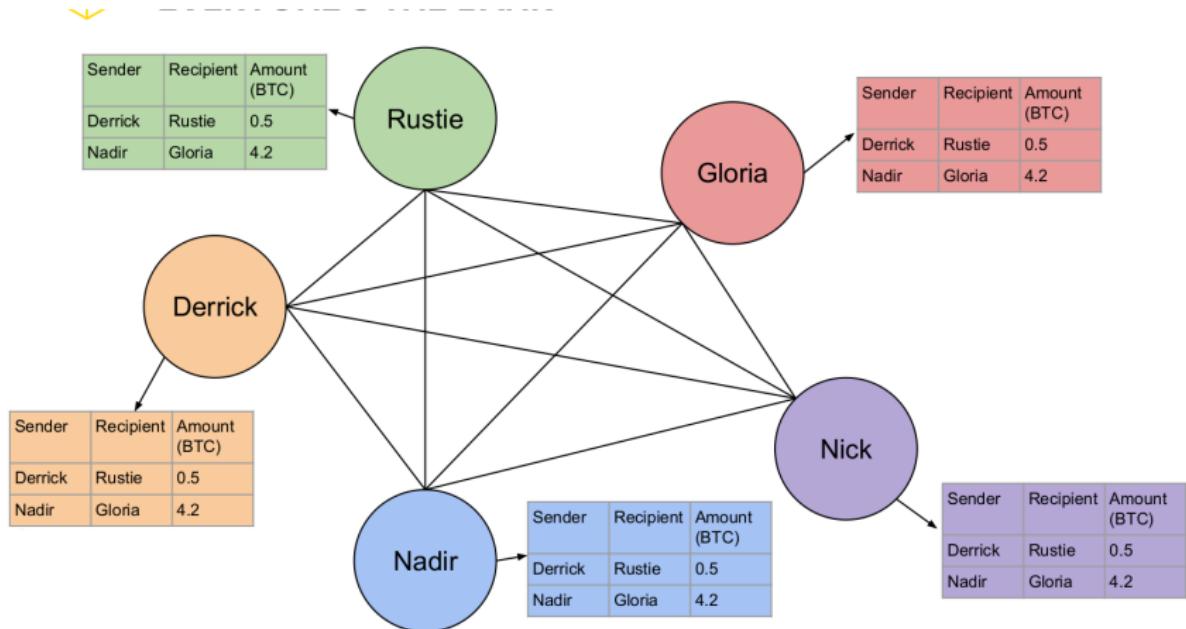
(la monnaie de l'île Yap)

# Une banque gérée par tout le monde



Sender	Recipient	Amount (BTC)
Derrick	Nadir	0.5
Rustie	Gloria	4.2

# Une banque gérée par tout le monde



# la blockchain

Sender	Recipient	Amount (BTC)
Derrick	Rustie	0.5
Nadir	Gloria	4.2
Nick	Gloria	23
Rustie	Derrick	3.2
Nadir	Rustie	0.3
Gloria	Nick	17

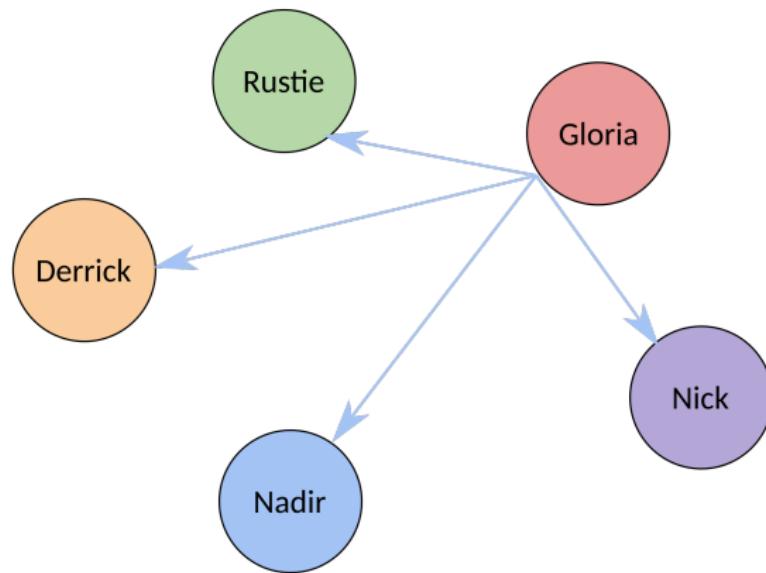


Sender	Recipient	Amount (BTC)
Derrick	Rustie	0.5
Nadir	Gloria	4.2

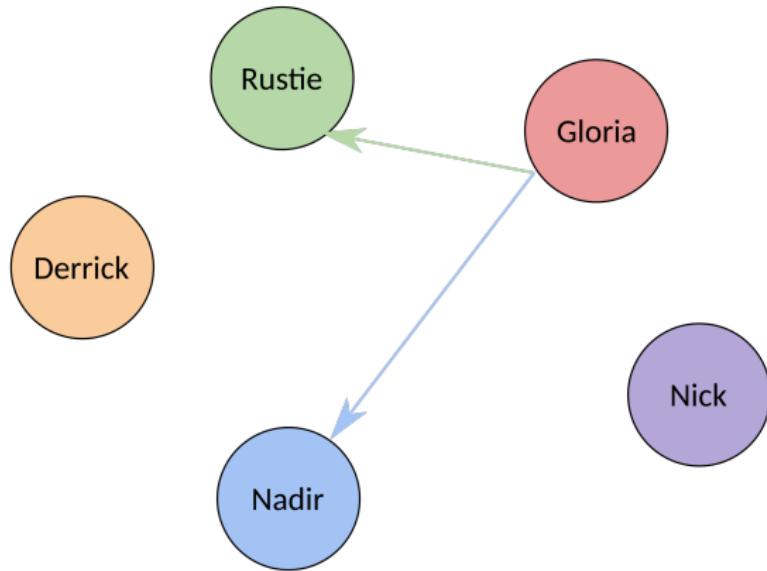
Sender	Recipient	Amount (BTC)
Nick	Gloria	23
Rustie	Derrick	3.2

Sender	Recipient	Amount (BTC)
Nadir	Rustie	0.3
Gloria	Nick	17

# Diffuser les événements

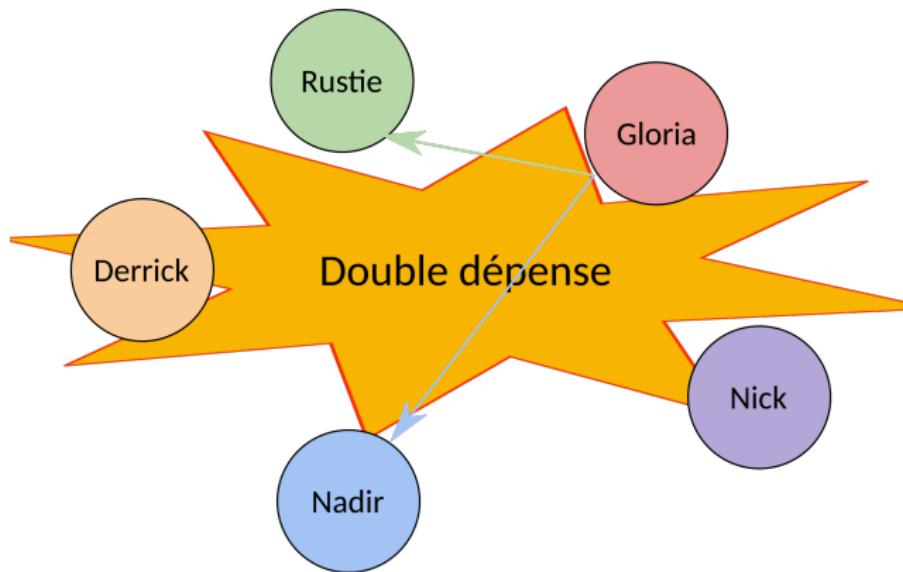


# L'attaque de la double dépense



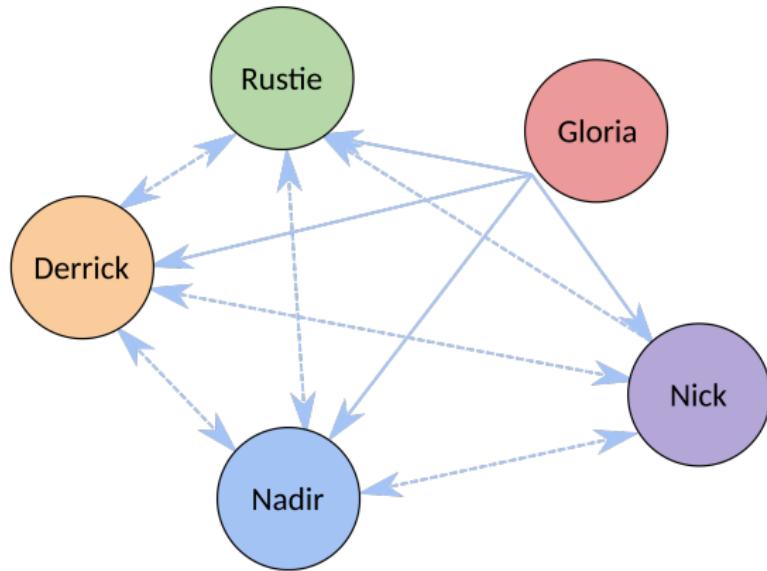
si gloria envois à tout le monde elle peut dépenser deux fois le même montant (pas de banque pour vérifier)

# L'attaque de la double dépense



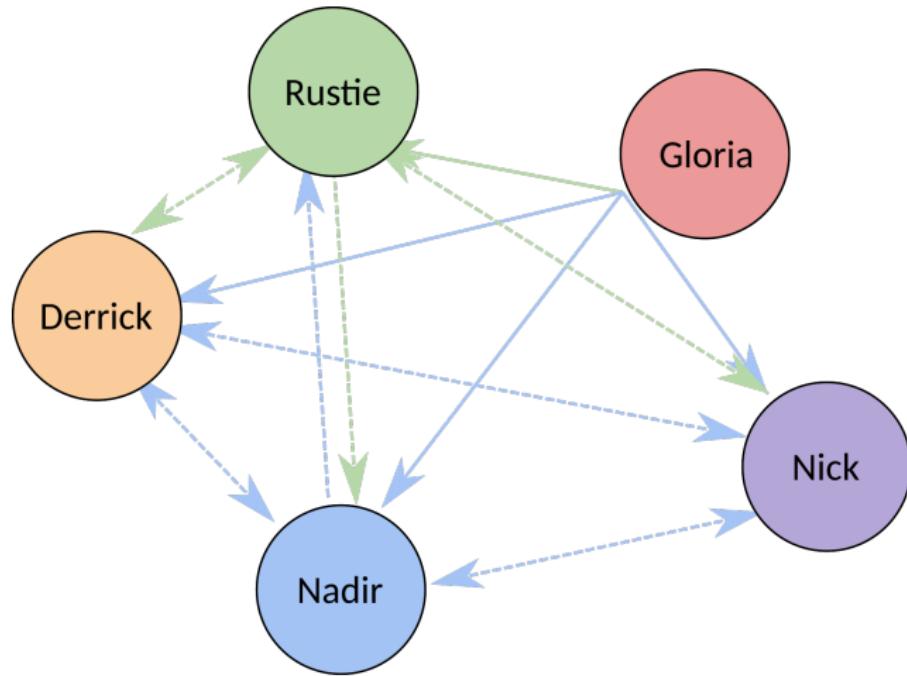
si gloria envois à tout le monde elle peut dépenser deux fois le même montant (pas de banque pour vérifier)

# La validation par les pairs



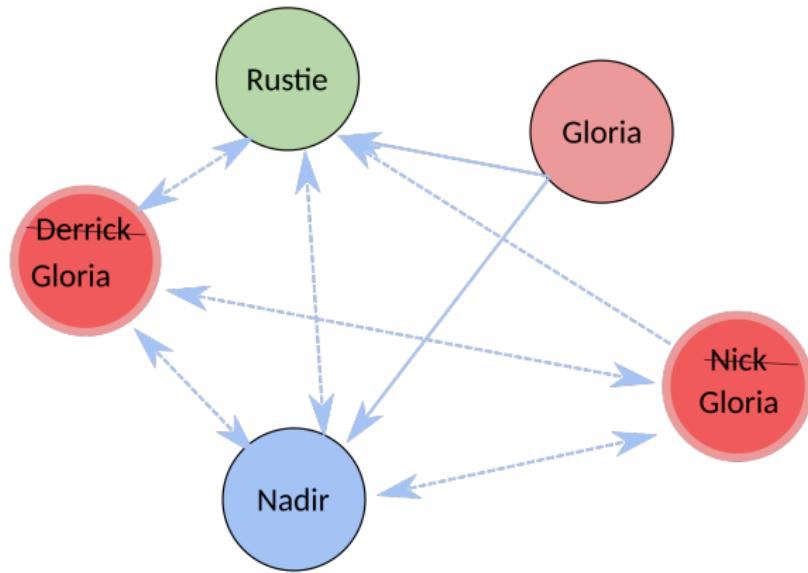
On diffuse à tout le monde, et on vote

# La validation par les pairs



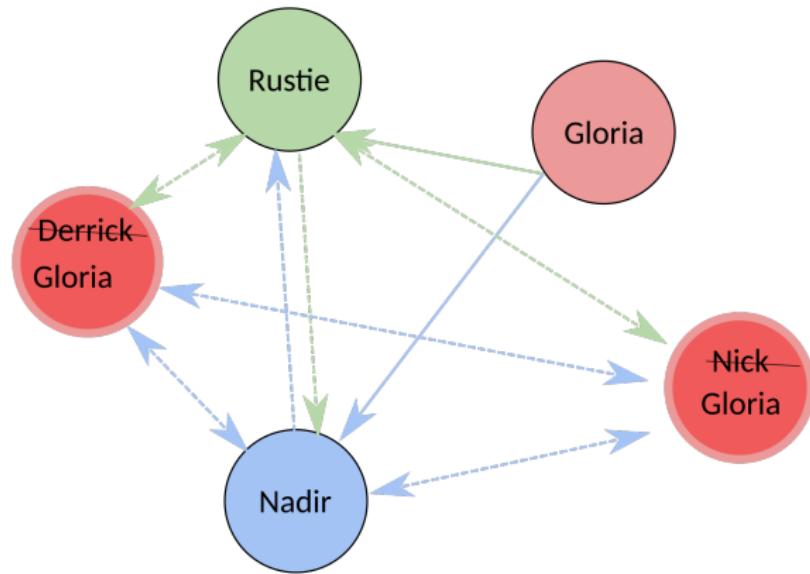
Nécessite une majorité de personnes honnêtes, mais...

# Etrange: L'attaque sybil



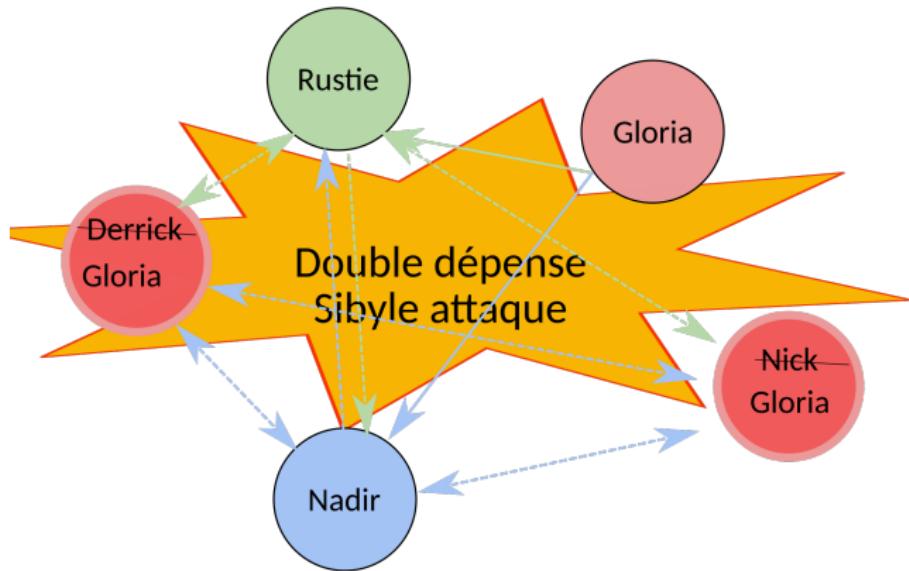
- ▶ Simple de générer des identités multiples pour approuver ses propres transactions

## Etrange: L'attaque sybil



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

# Etrange: L'attaque sybil

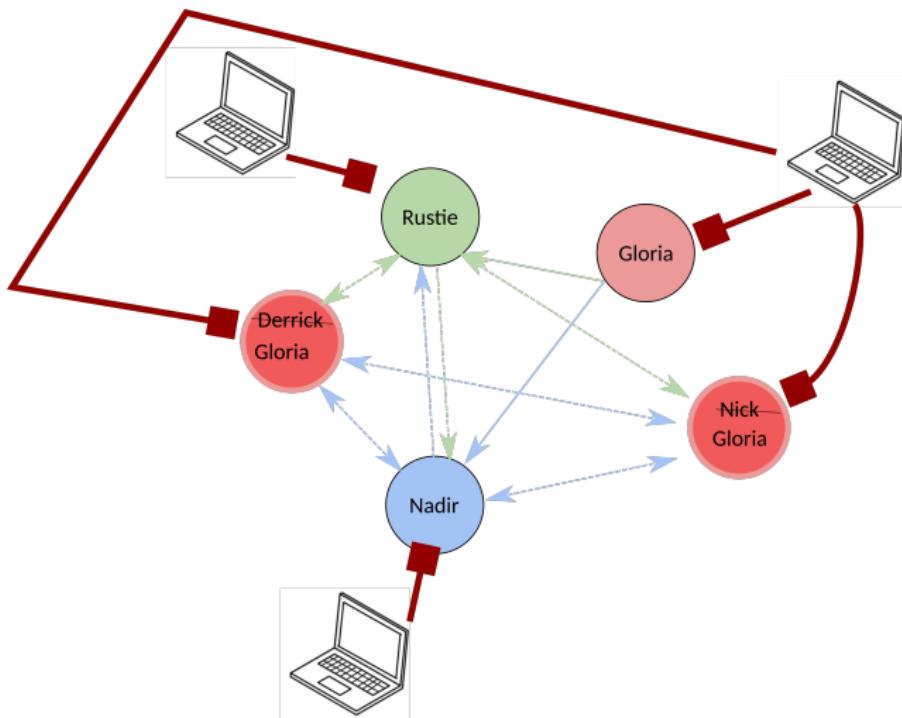


- ▶ Simple de générer des identités multiples pour approuver ses propres transactions
- ▶ une identité un vote, ne peut pas marcher.
- ▶ Le vote doit être couteux.

# Preuve par travail

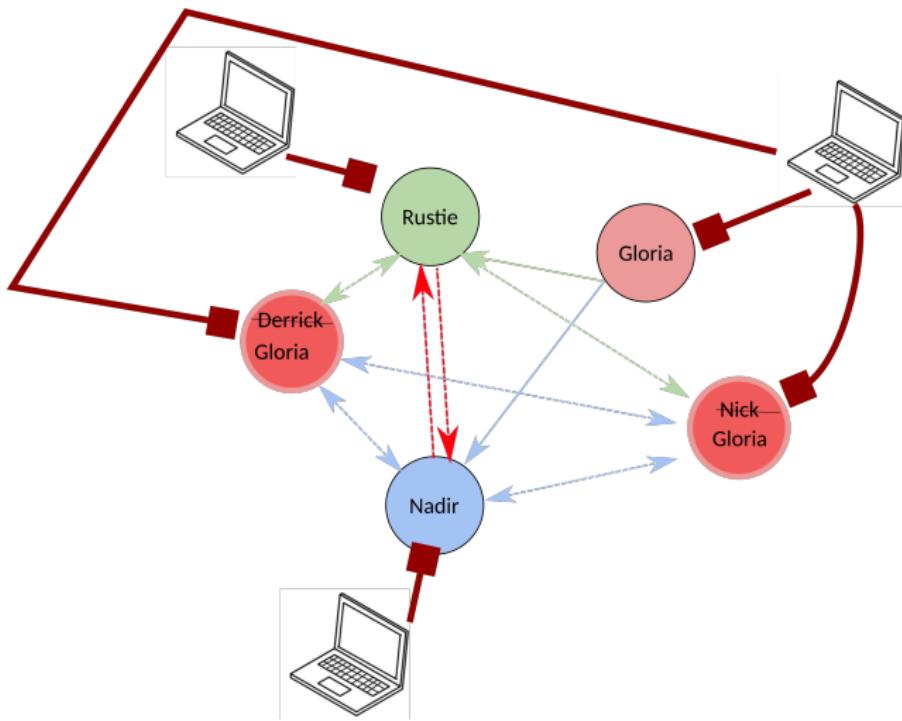
- ▶ Pour voter faire quelque chose de difficile, où on ne peut pas tricher
- ▶ tester les solutions d'un problème au hasard, par exemple

# La preuve par la travail (suite)



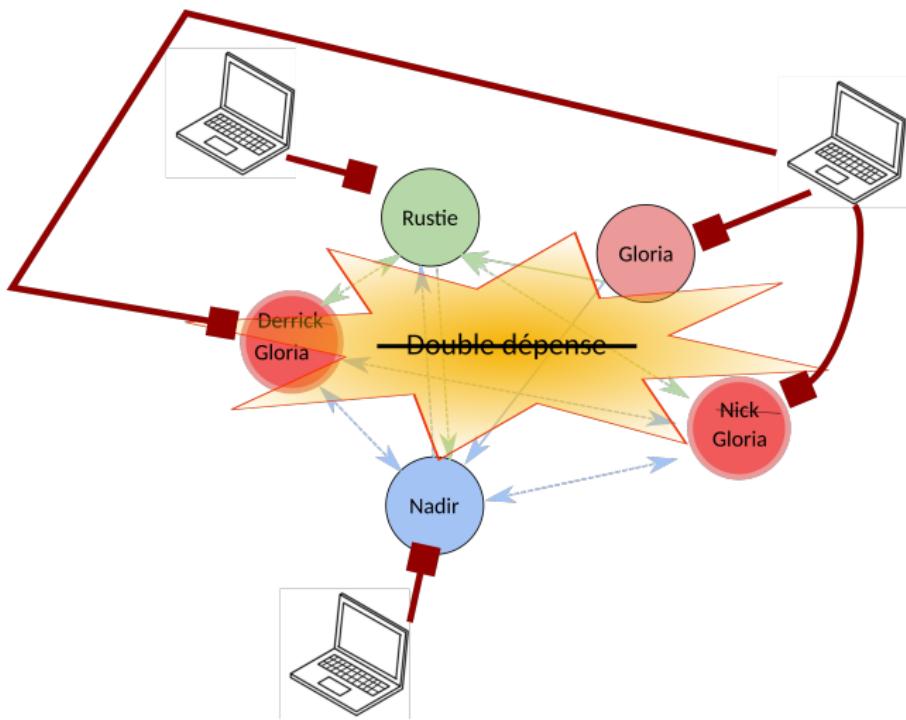
- ▶ eg. Un processeur un vote

# La preuve par la travail (suite)



- ▶ eg. Un processeur un vote
- ▶ c'est coûteux de falsifier

# La preuve par la travail (suite)



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

# Bitcoin et blockchain

Un réseau décentralisé

un journal comptable distribué et infalsifiable

Un mécanisme pour atteindre le consensus sur l'histoire du bitcoin

Un ensemble de règles pour générer les tokens et faire les mises à jour du software

## Rappels:

- ▶ identité : clefs publique, clefs privées
- ▶ transaction: à la façon de tirelires
- ▶ journal comptable publique et distribué
- ▶ consensus

## Particularité

- ▶ pseudo anonymité
- ▶ Décentralisé
- ▶ Infalsifiable
- ▶ Ne requiert pas d'avoir confiance en autrui.