

Samedi 21 Janvier 2023



LOCKCHAINS

Consensus et Cryptographie

Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

3. Systèmes distribués

- Système distribués
- Les Généraux Byzantins
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

4. Perspectives

- Perspectives

De quoi allons-nous parler ?



Cryptographie & Consensus

- ▶ Outils de la cryptographie
- ▶ Systèmes distribués
- ▶ Les différents Consensus

Universalité et Smart-contracts

- ▶ Applications distribuées (dApp)
- ▶ Ethereum et Cardano
- ▶ Quelles applications ?

Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

3. Systèmes distribués

- Système distribués
- Les Généraux Byzantins
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

4. Perspectives

- Perspectives

Une chaîne de blocs

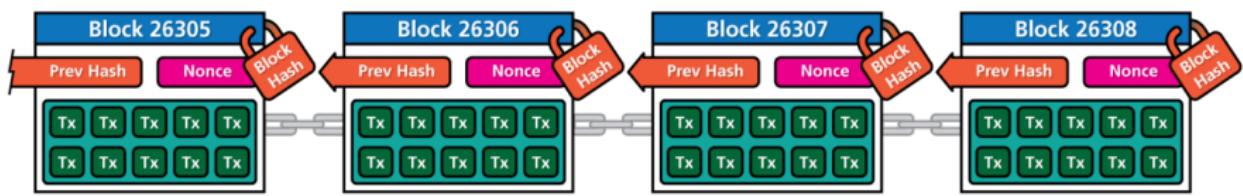


Illustration by CryptoGraphics.info

Maintenu par ses utilisateurs

Une chaîne de blocs

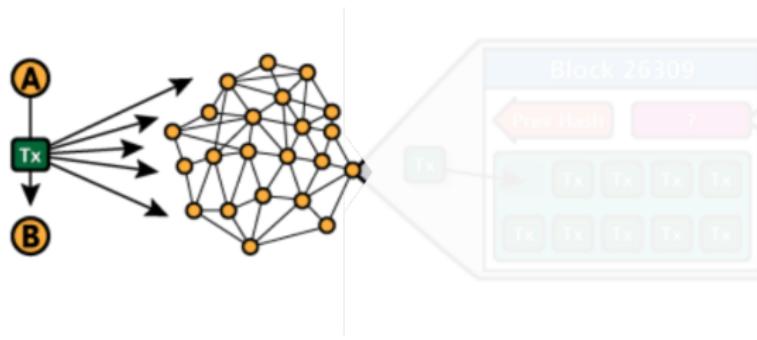


Maintenu par ses utilisateurs

Empereurs, Élus, Mineurs, vous et moi.

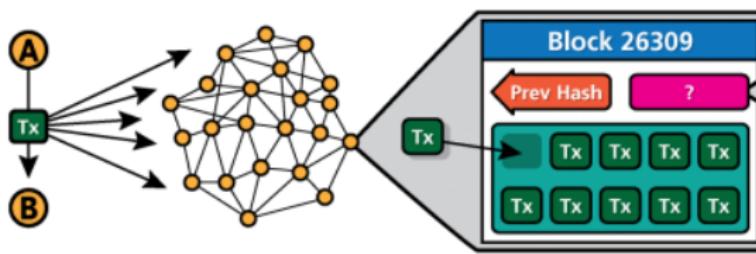


C'est un DLT : *Distributed Ledger Technology*



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

C'est un DLT : *Distributed Ledger Technology*



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

C'est un DLT : *Distributed Ledger Technology*

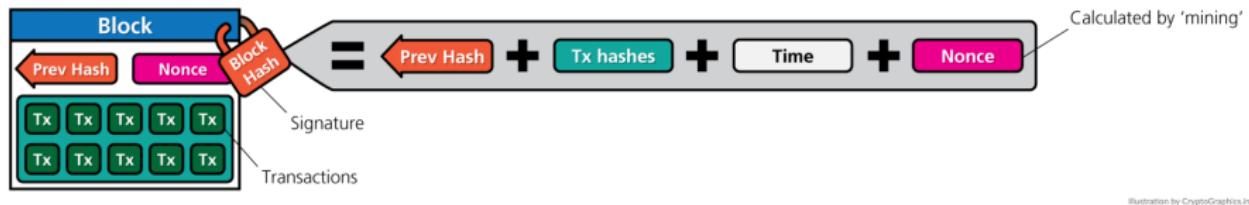
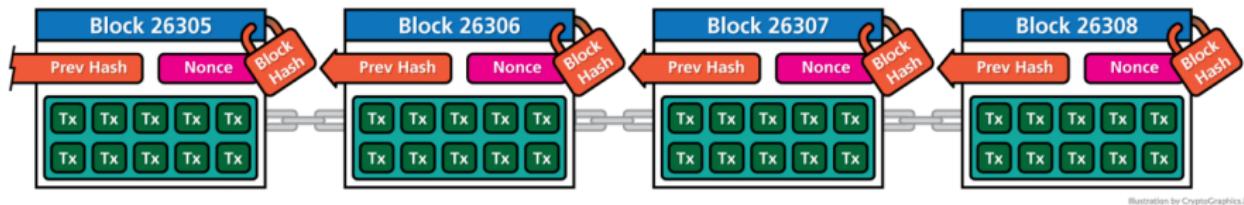


Illustration by CryptoGraphics.info

Le 1^{er} mineur à gagner un **bon nonce**, annonce son bloc

- ▶ avec une récompense (coinbase)
- ▶ c'est un **élu** (ou leader)

C'est un DLT : *Distributed Ledger Technology*



Les autres mineurs :

- ▶ Vérifient le bloc
- ▶ Ajoutent le nouveau block **a la plus longue chaîne**
- ▶ Puis une nouvelle **loterie** commence.

Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- **Transactions (tx)**
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

3. Systèmes distribués

- Système distribués
- Les Généraux Byzantins
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

4. Perspectives

- Perspectives

Validité d'une transaction

Qu'est qui rend une transaction valide ?

Validité d'une transaction

Qu'est qui rend une transaction valide ?

Il faut ...

- ▶ Des fonds disponibles
- ▶ Une identité (signature)
- ▶ Pas de duplication
- ▶ un compte bancaire ?

Confiance !

Validité d'une transaction

Qu'est qui rend une transaction valide ?

Confiance !

Il faut ...

- ▶ Des fonds disponibles
- ▶ Une identité (signature)
- ▶ Pas de duplication
- ▶ un compte bancaire ?



en Mme. La-Garde ?

Le Modèle des UTXO : Unspent Transaction Output

Les UTXO sont comme des tirelires



Connaître le contenu de sa tirelire

Le Modèle des UTXO : Unspent Transaction Output

Les UTXO sont comme des tirelires



Tout dépenser quand on l'utilise

Ça ressemble à quoi une transaction dans un bloc ?

Explorons avec l'explorer.btc.com

Summary		
Height	4 772,825	Relayed By
Confirmations	33	Difficulty
Block Size	1,490,918 Bytes	Block Reward
Stripped Size	834,141 Bytes	Fee Reward
Weight	3,993,541	Tx Count
Time	2023-01-06 16:13:57	Tx Volume
Merkle Root	87627170327be1ef52a37d7370448ac879f021a0210f06000b4325fb6288999	
Version	0x00060000	
Nonce	0x6f066641	
Bits	0x17707042	
Other Explorers		BLOCKCHAIR
Transactions (1258)		
Input (i)	Output (j)	Fee
0254eaf090e0890d17580a74fc0235855w7cb00f0ee8322eaec7bd37e1b4f04 corbase	0 Satoshi/vB/s 0.45389325 BTC 3t8CkLbb3vew1x3K4o0dm2k-1d7YK6K18T2 SegWit commitment output 0 Unable to decode output address	Fee: 0.45389325 BTC
74ad13a29e7185a22330f1b27ac143d0e02ff0bae5af1778ed57387 309yZd8iCLB754gwoc2B1H5w71R030GhDyQ	518 Satoshi/vB/s 0.00085422 BTC 3t54XeHbfcrymzze3weC8zavCv0t13dpz2nW bc1q7lak2y13t7gx7915...059f6daew1qpk95cfwta	Fee: 0.00085422 BTC
98ce0640330a8f50a2d7f2355ebf506a7965fe3a7a7f3a7ad56cc375e798 35vTQF627eweswlebrFaPrDex25601t 3t5qj8kqgRvxJ8yjy2K6KHf20KHe1u6LQQ	201 Satoshi/vB/s 0.00047600 BTC 3t4Kyyrl0gDak2hL2cap0ct0xx253jeFvF8 bc1q54d4verryf7nx4...qhsf6muydegz449fj4k	Fee: 0.00047600 BTC

Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

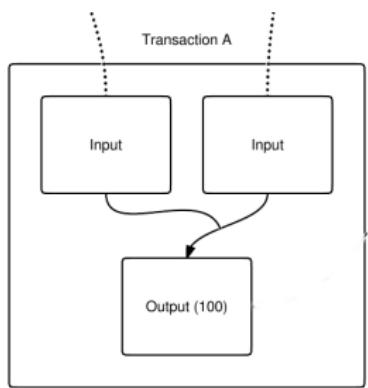
- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

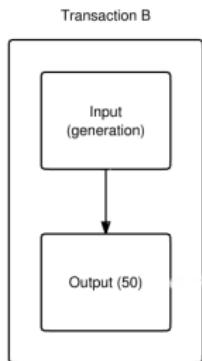
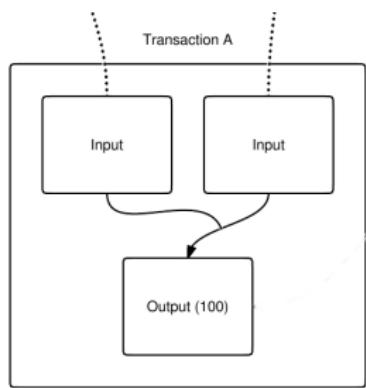
3. Systèmes distribués

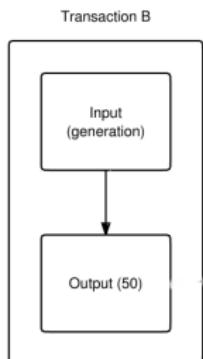
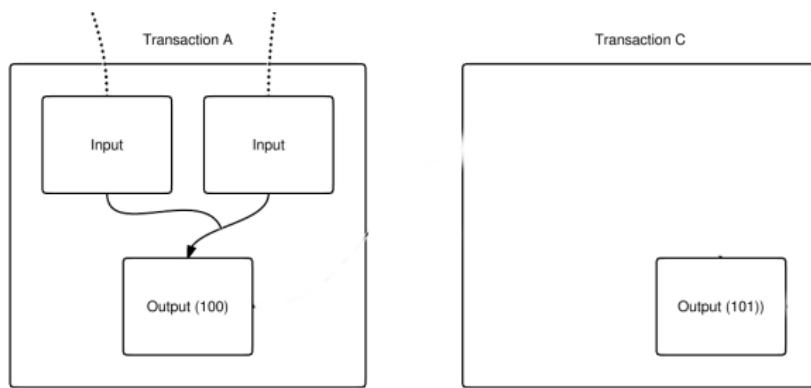
- Système distribués
- Les Généraux Byzantins
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

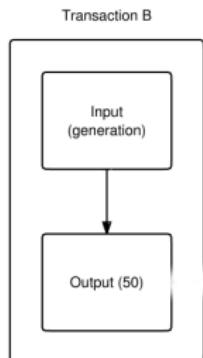
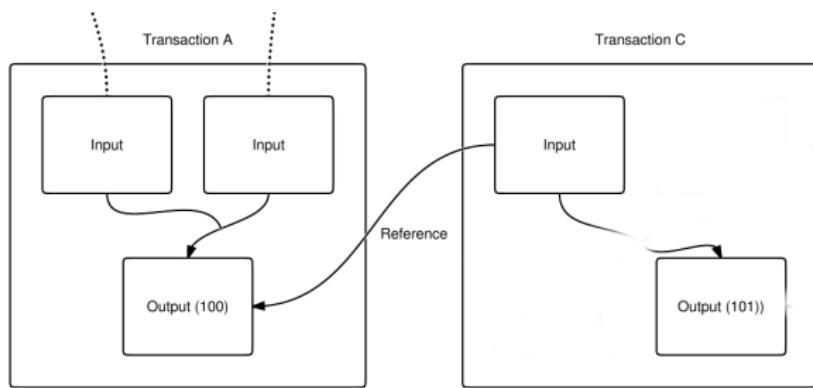
4. Perspectives

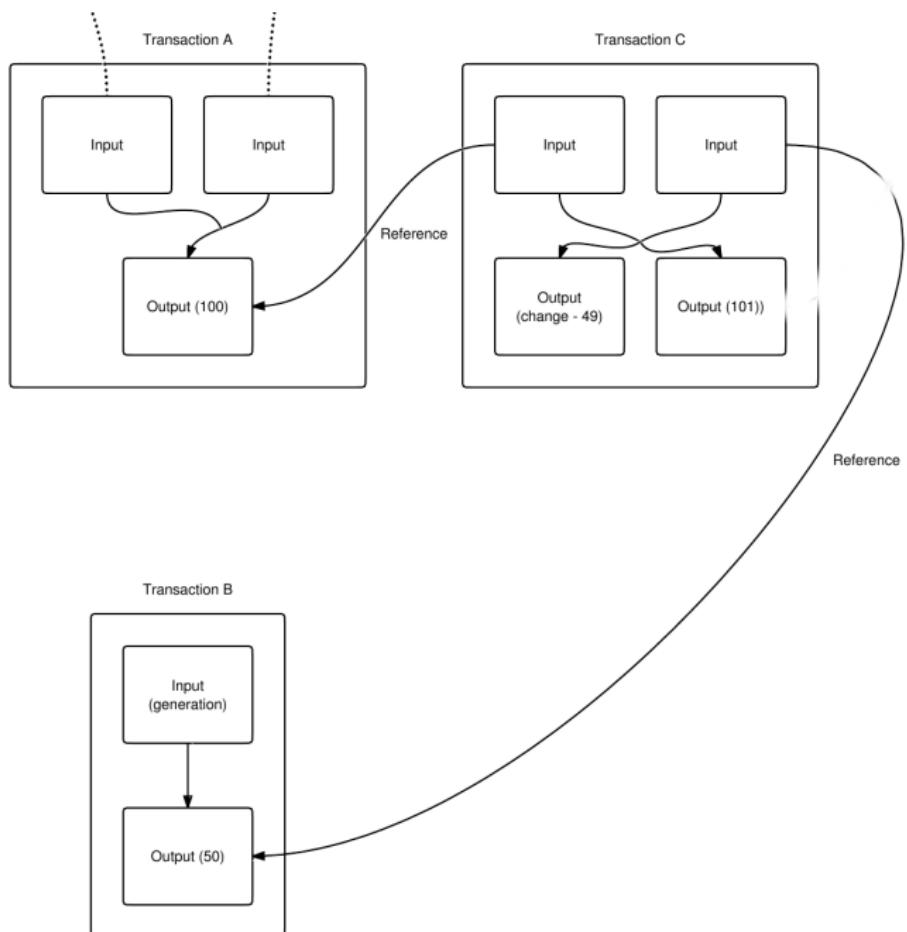
- Perspectives

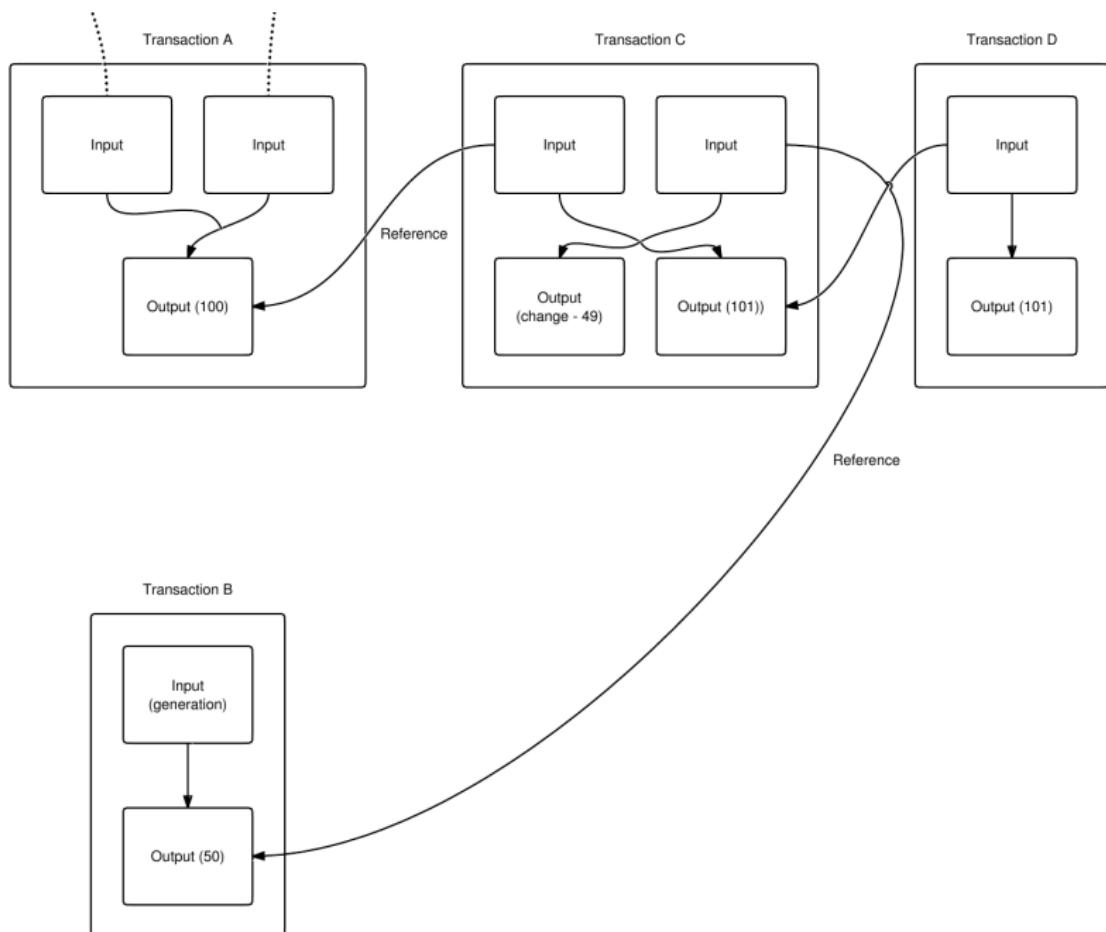












En résumé

- ▶ Chaque pièce est unique (non fungible)
- ▶ on réfère des pièces particulières lorsqu'on les dépense
- ▶ les pièces sont consommées et de nouvelles créées
- ▶ on ne peut dépenser une pièce qu'une fois.

Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- **Hash et signatures**
- Comment vérifier les transactions
- Sécurité des clés

3. Systèmes distribués

- Système distribués
- Les Généraux Byzantins
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

4. Perspectives

- Perspectives

Propriété des Hash

- ▶ Résistance à la préimage
- ▶ Résistance à collision
- ▶ impossible de produire la signature d'un autre
- ▶ impossible de remonter en message en regardant la signature
- ▶ même output pour input identique

SHA256 et RIPEMD160

quantum resistant

Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- **Comment vérifier les transactions**
- Sécurité des clés

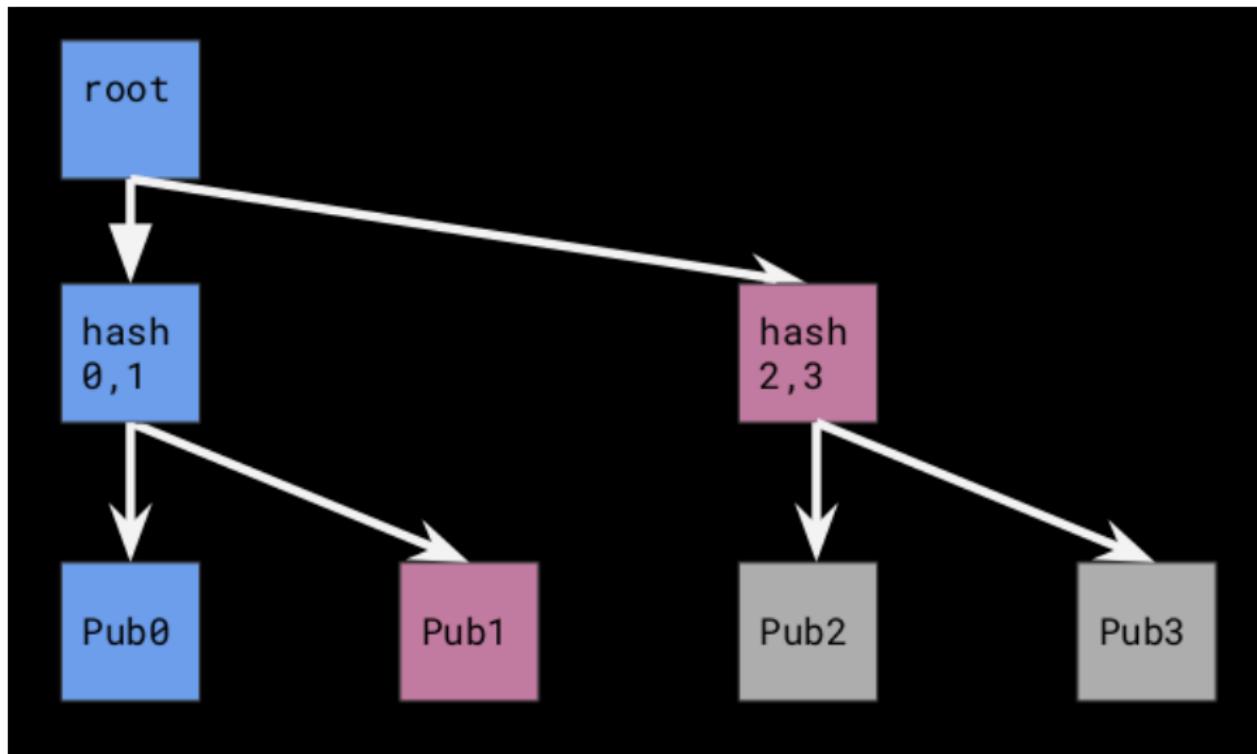
3. Systèmes distribués

- Système distribués
- Les Généraux Byzantins
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

4. Perspectives

- Perspectives

Arbre de Merkle



Arbre de Merkle

Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

3. Systèmes distribués

- Système distribués
- Les Généraux Byzantins
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

4. Perspectives

- Perspectives

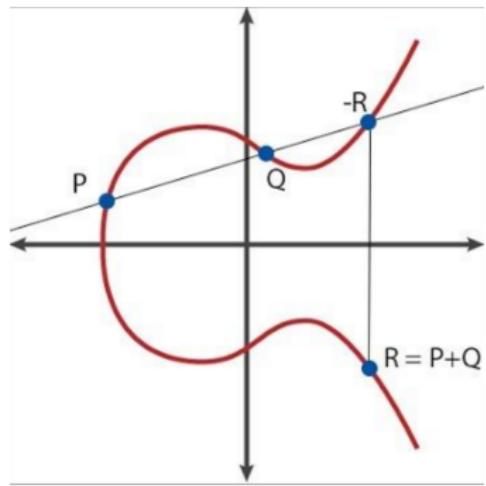
Création des clefs

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

ECDSA elliptic Curve Digital Signature Algorithm

Génération des clés

- ▶ Si on connaît P et $Q \rightarrow R$
- ▶ Mais R ne permet pas de trouver P et Q



$$\text{Courbe elliptique } y^2 = x^3 + 7$$

Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

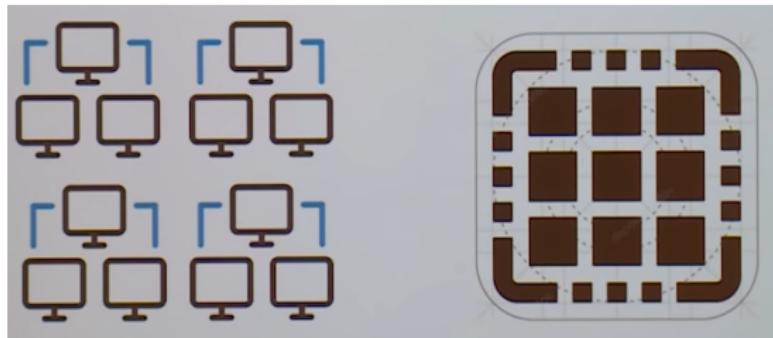
3. Systèmes distribués

- Système distribué
- Les Généraux Byzantins
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

4. Perspectives

- Perspectives

De l'infiniment petit à l'infiniment grand



Petit

Grand



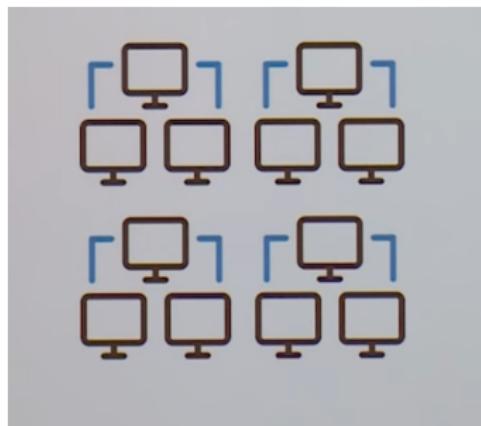
Avec mémoire partagée



Avec envois de messages

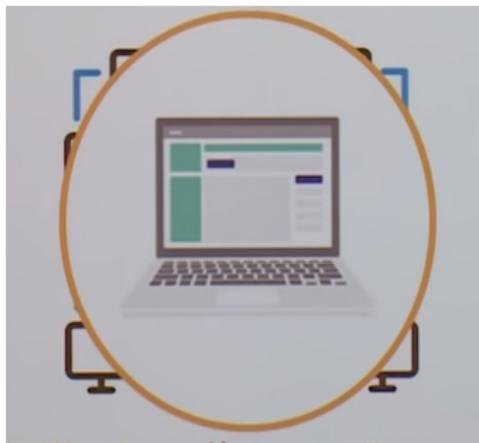
Propriétés des Systèmes distribués

- ▶ **Robustesse** : la machine fonctionne toujours
- ▶ **Atomocité** : elle est perçue comme une seule machine



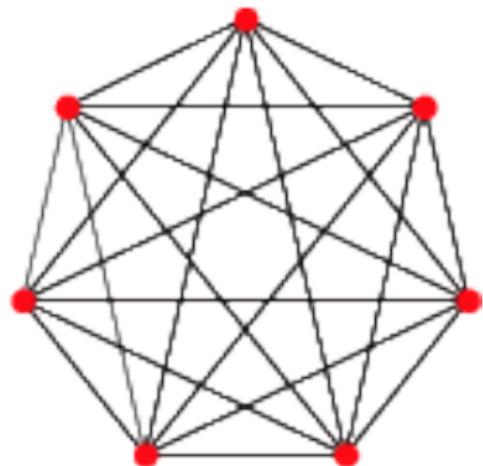
Propriétés des Systèmes distribués

- ▶ **Robustesse** : la machine fonctionne toujours
- ▶ **Atomocité** : elle est perçue comme une seule machine



Problèmes des Systèmes distribués

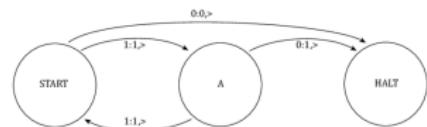
- ▶ Complexité
- ▶ Perte de l'universalité



Problèmes des Systèmes distribués

- ▶ Complexité
- ▶ Perte de l'universalité

Tout ce qui était calculable l'était avec la
Machine de Turing



Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

3. Systèmes distribués

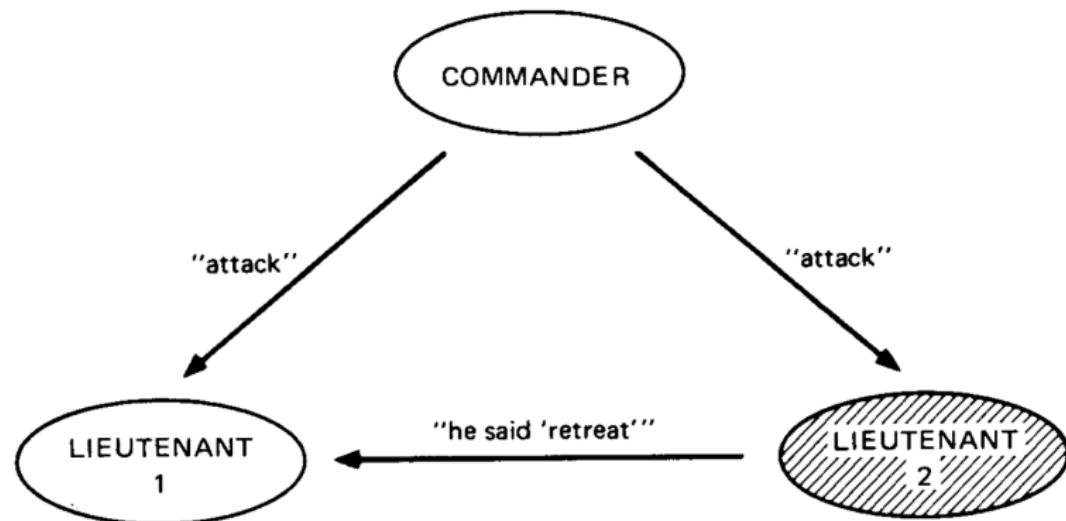
- Système distribués
- **Les Généraux Byzantins**
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

4. Perspectives

- Perspectives

Attaque ou retraite ?

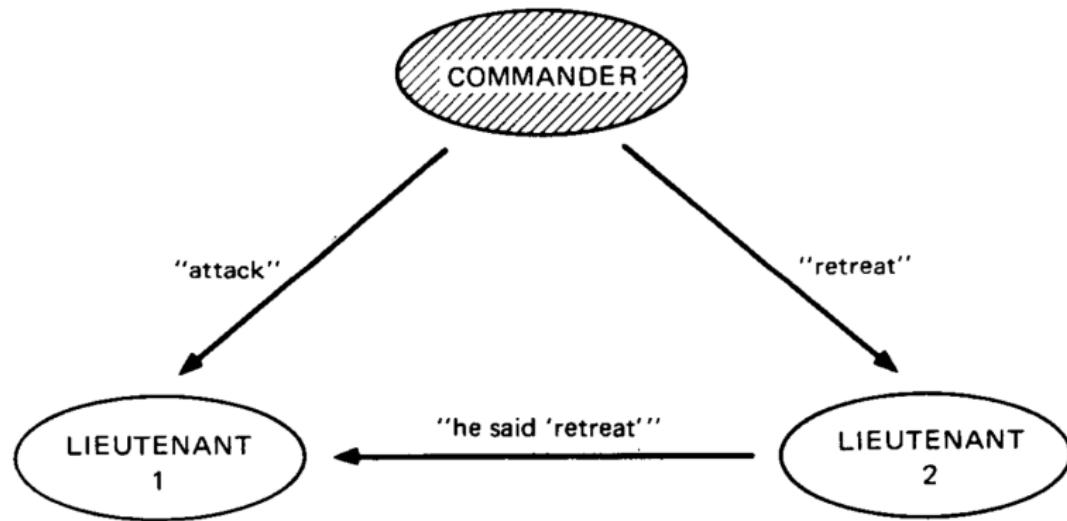
Le problème des généraux Byzantins



Le lieutenant est un traître

Attaque ou retraite ?

Le problème des généraux Byzantins



Le commandant est un traître

BFT Systems

Systèmes tolérants aux fautes Byzantines

- ▶ Nombre et participants connus
- ▶ Election d'un leader
- ▶ Traites Punis

Sans signature

- ▶ honnête majorité obligatoire

Avec signature

- ▶ Pas de majorité obligatoire

Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

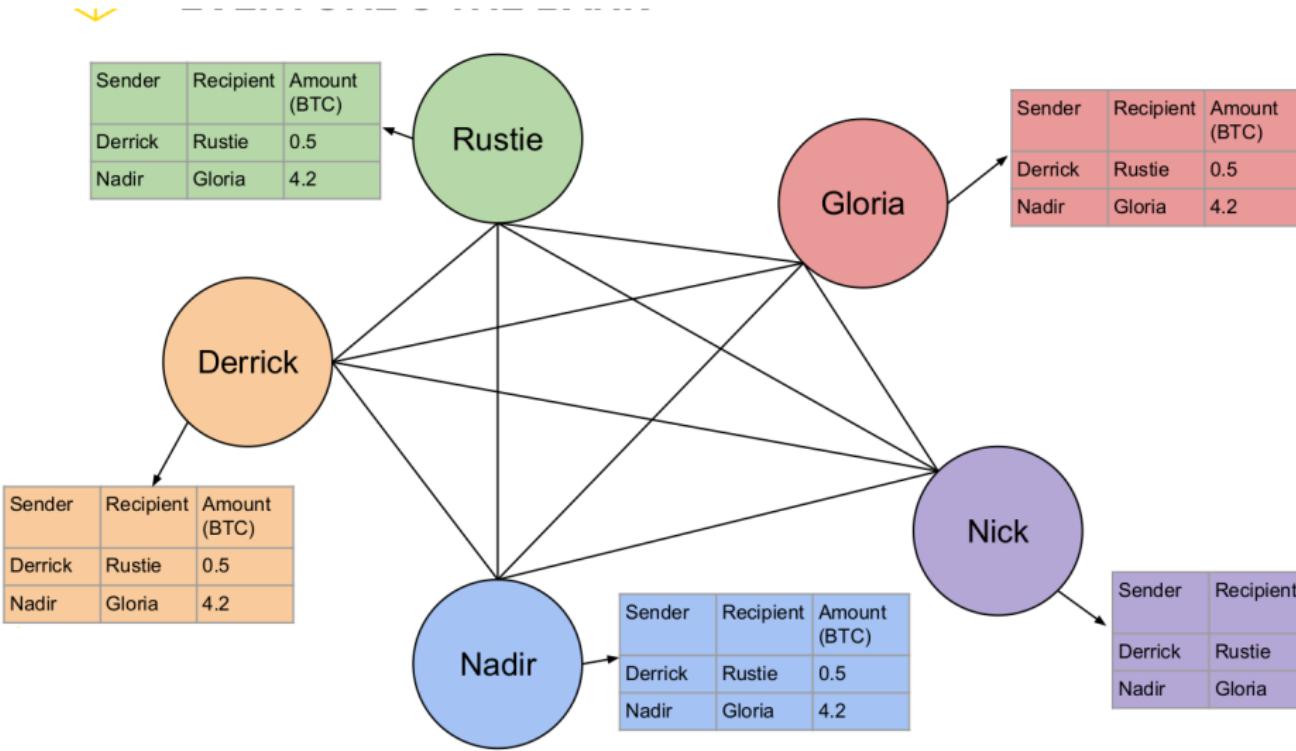
3. Systèmes distribués

- Système distribués
- Les Généraux Byzantins
- **Blockchains et consensus**
- Comment maintenir le Consensus autrement ?

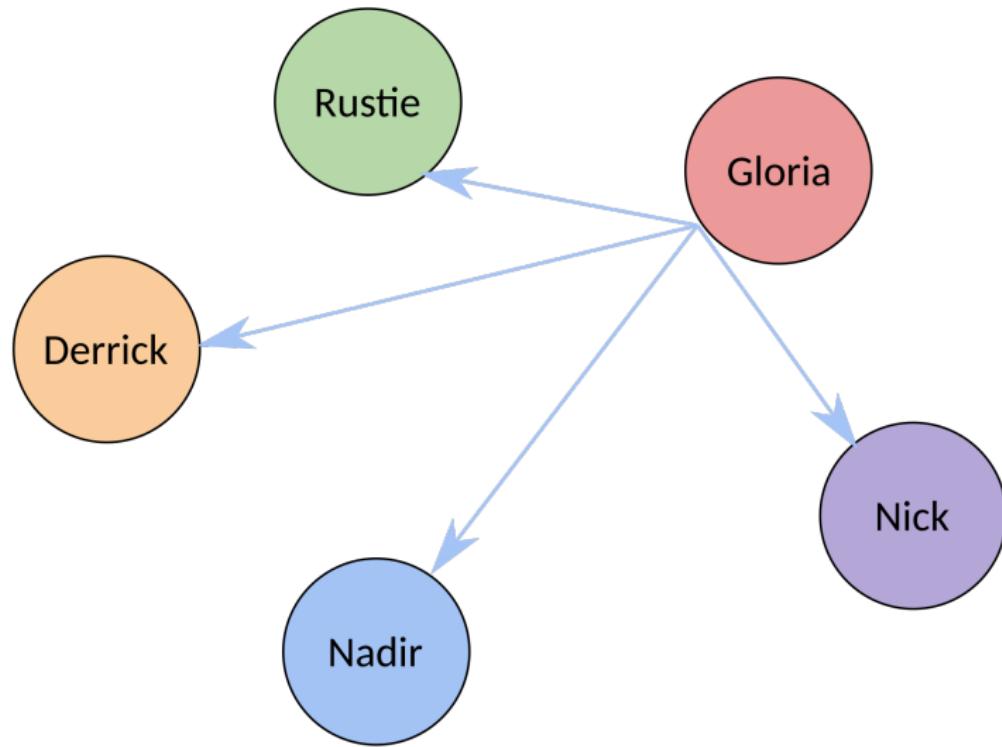
4. Perspectives

- Perspectives

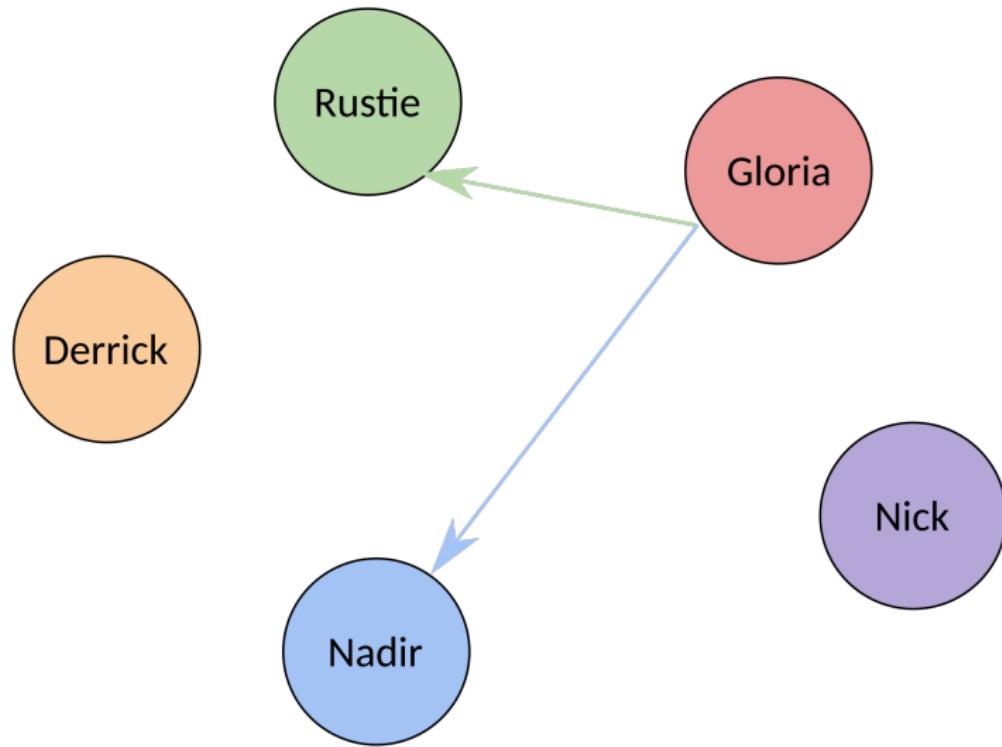
Preuve de travail (PoW) : Consensus de Nakamoto



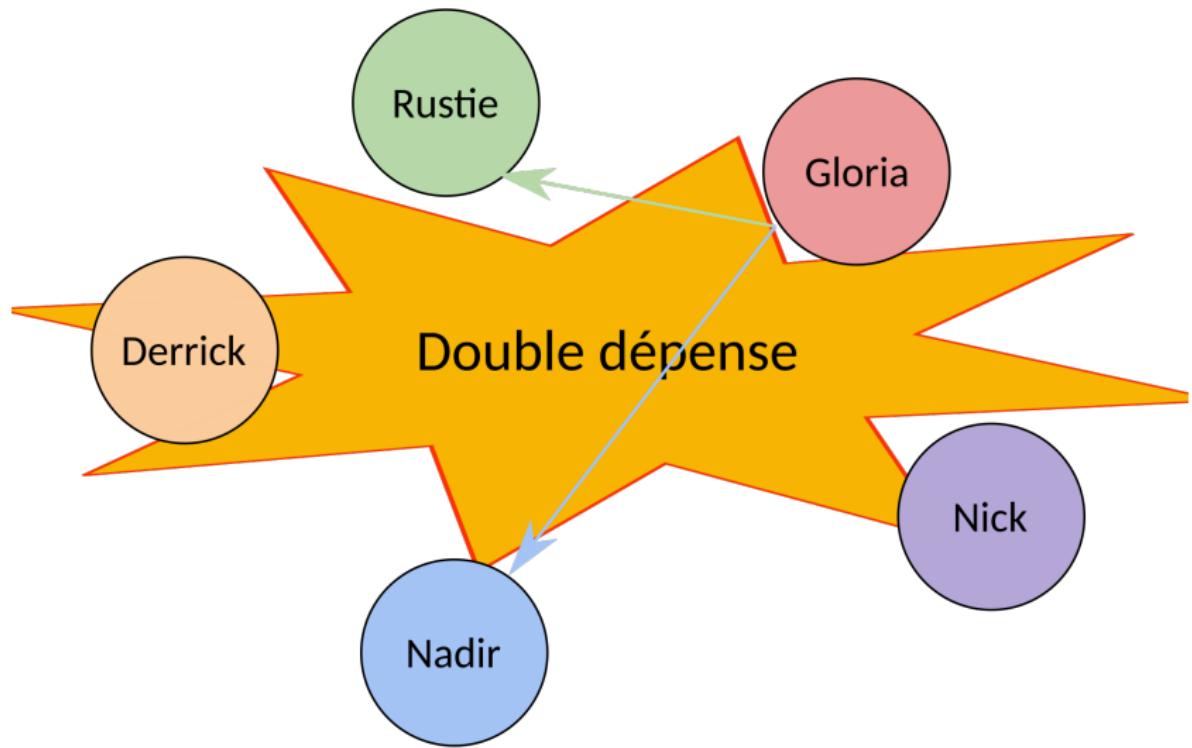
Preuve de travail (PoW) : Consensus de Nakamoto



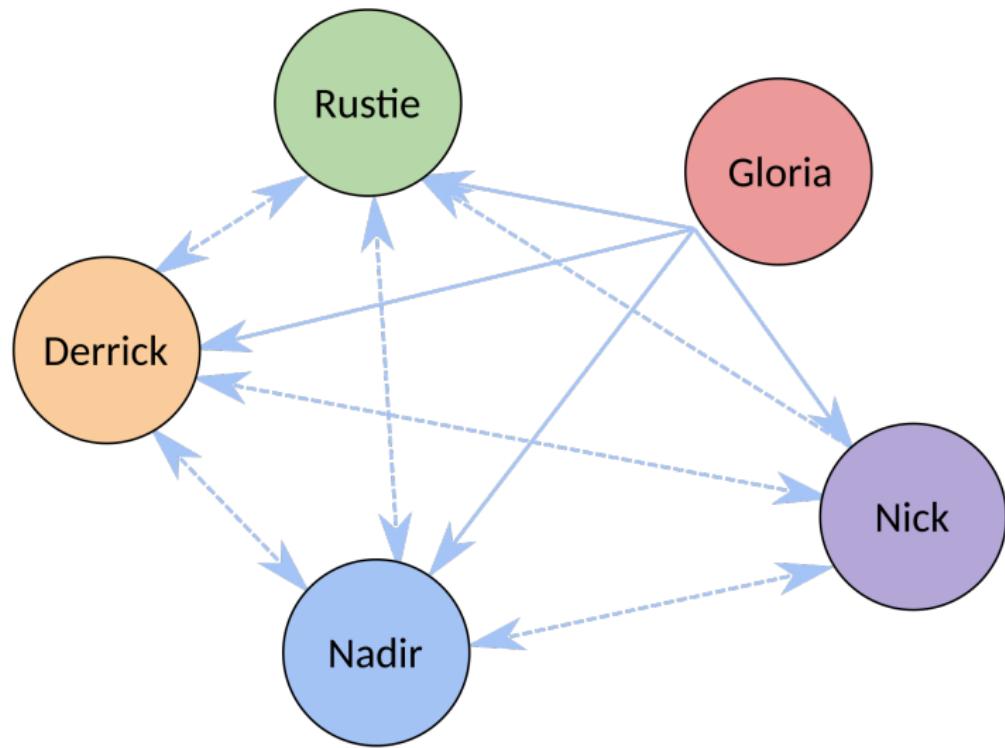
Preuve de travail (PoW) : Consensus de Nakamoto



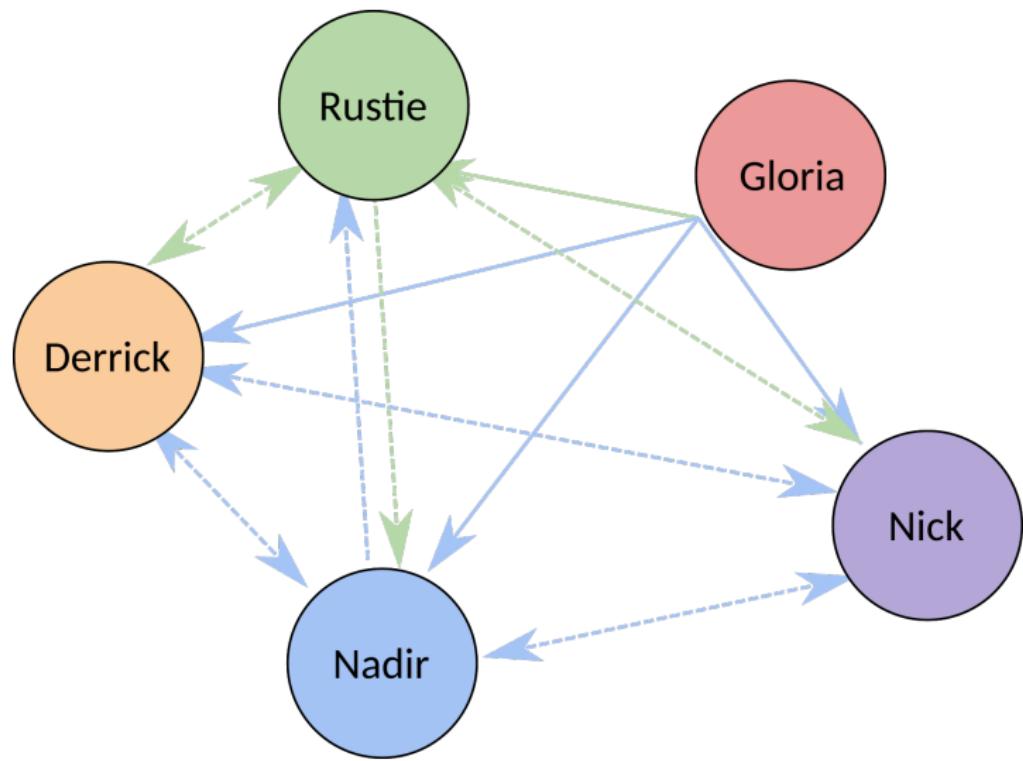
Preuve de travail (PoW) : Consensus de Nakamoto



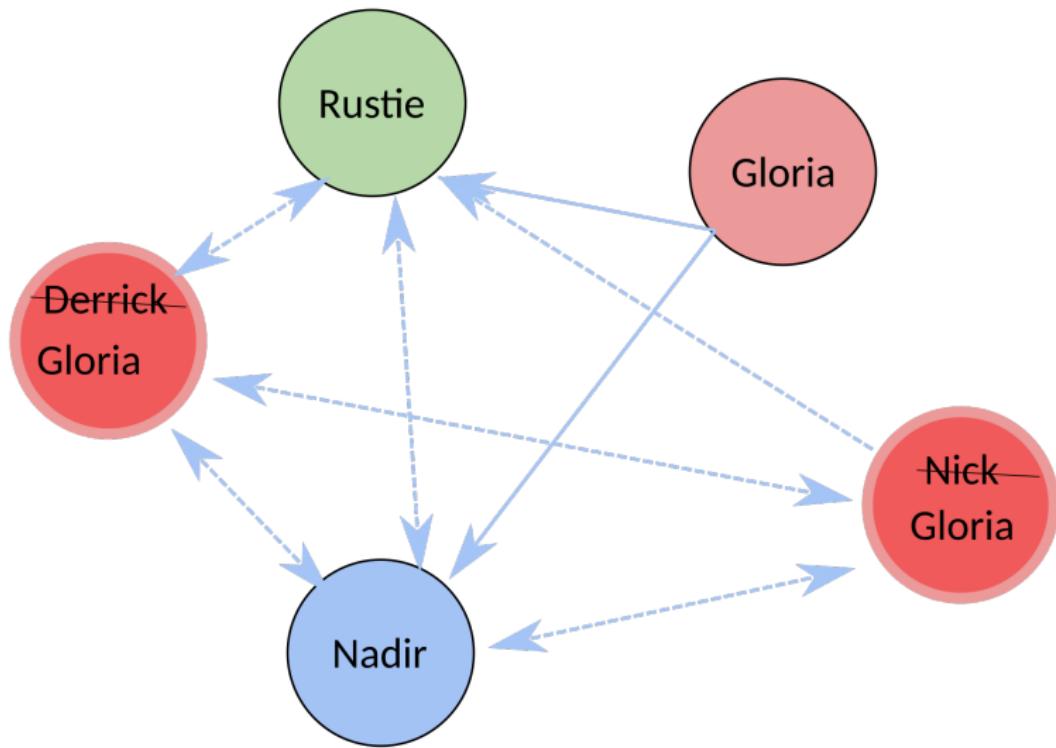
Preuve de travail (PoW) : Consensus de Nakamoto



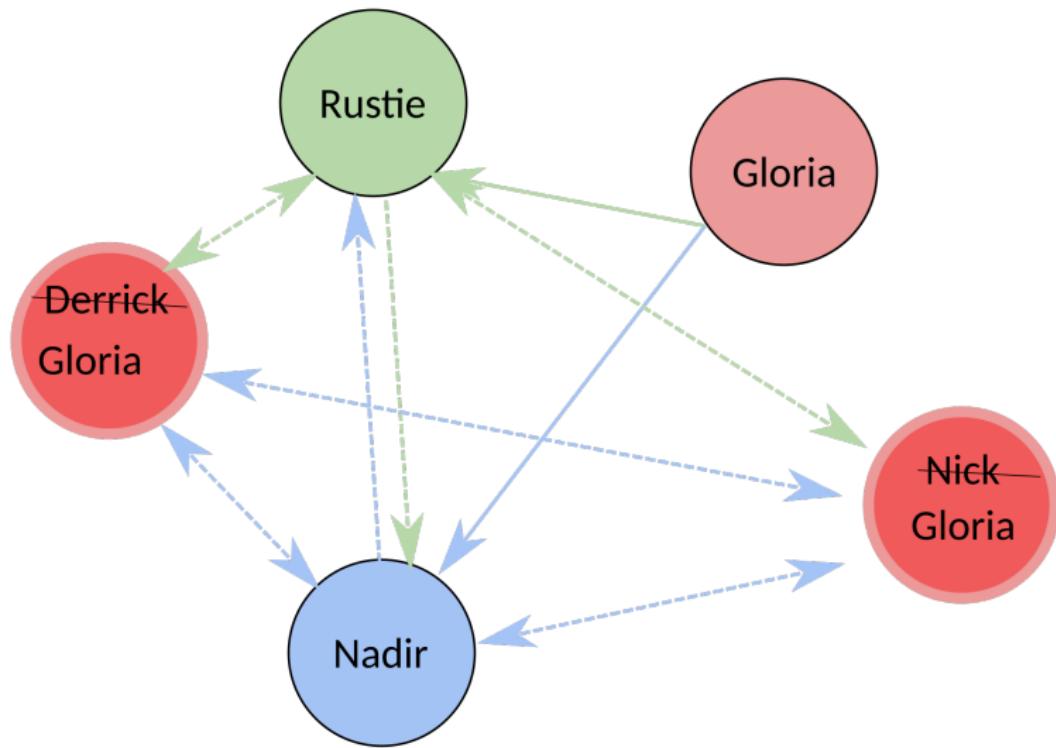
Preuve de travail (PoW) : Consensus de Nakamoto



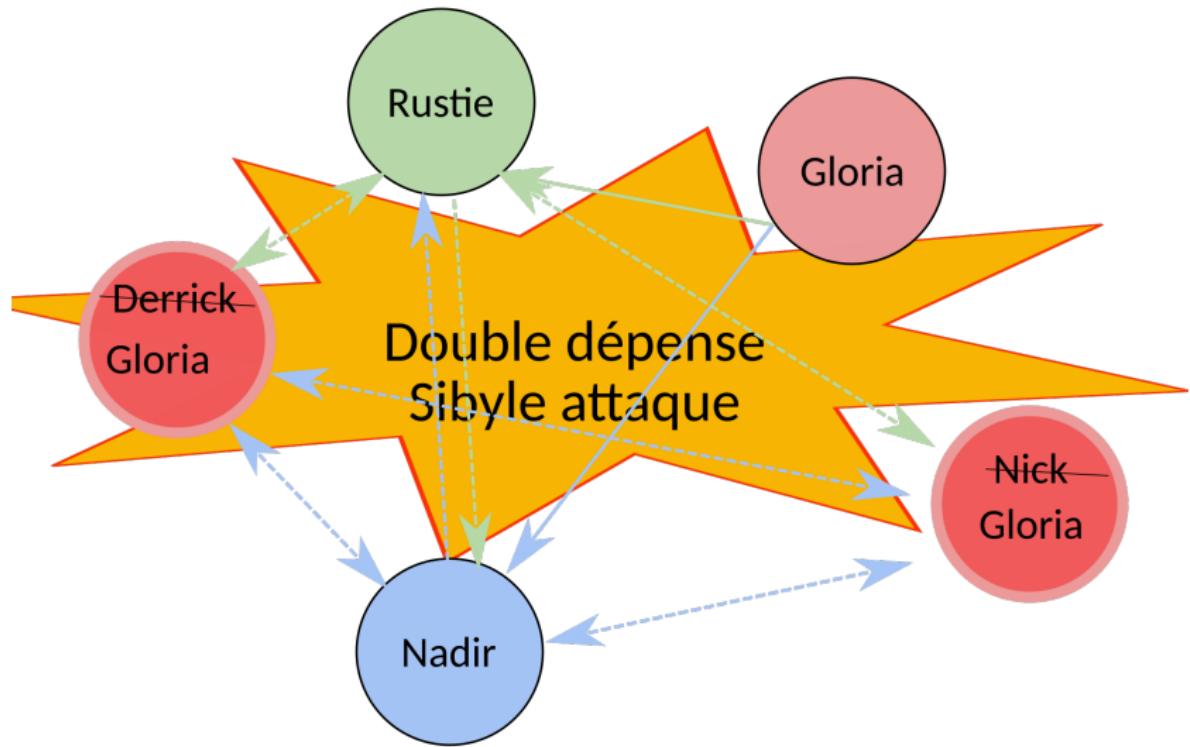
Preuve de travail (PoW) : Consensus de Nakamoto



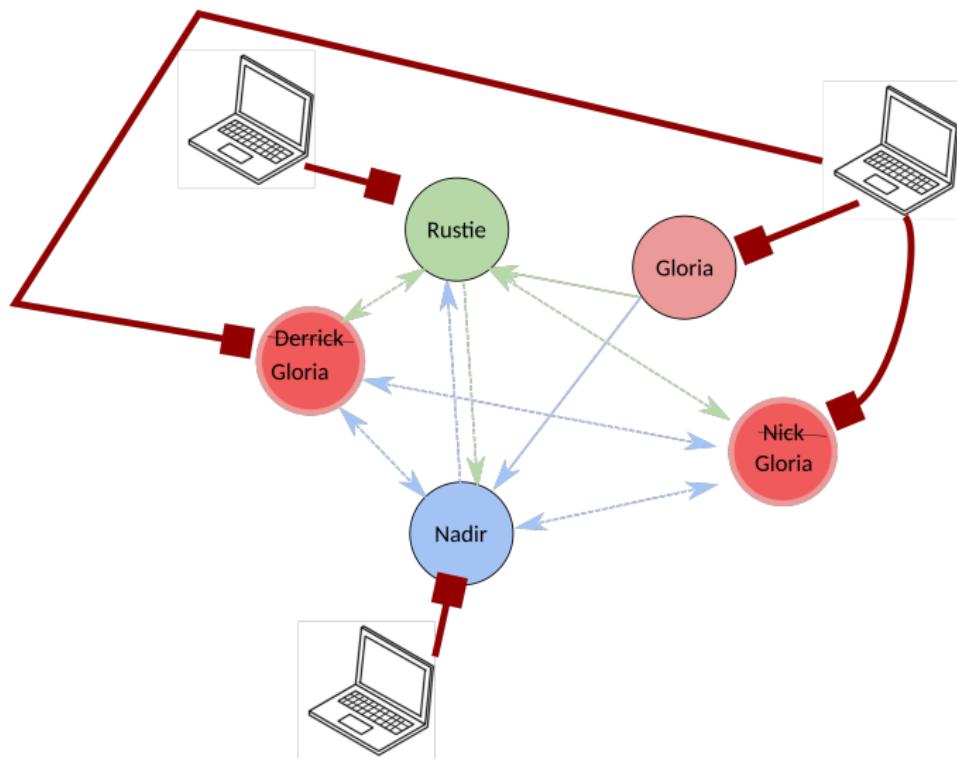
Preuve de travail (PoW) : Consensus de Nakamoto



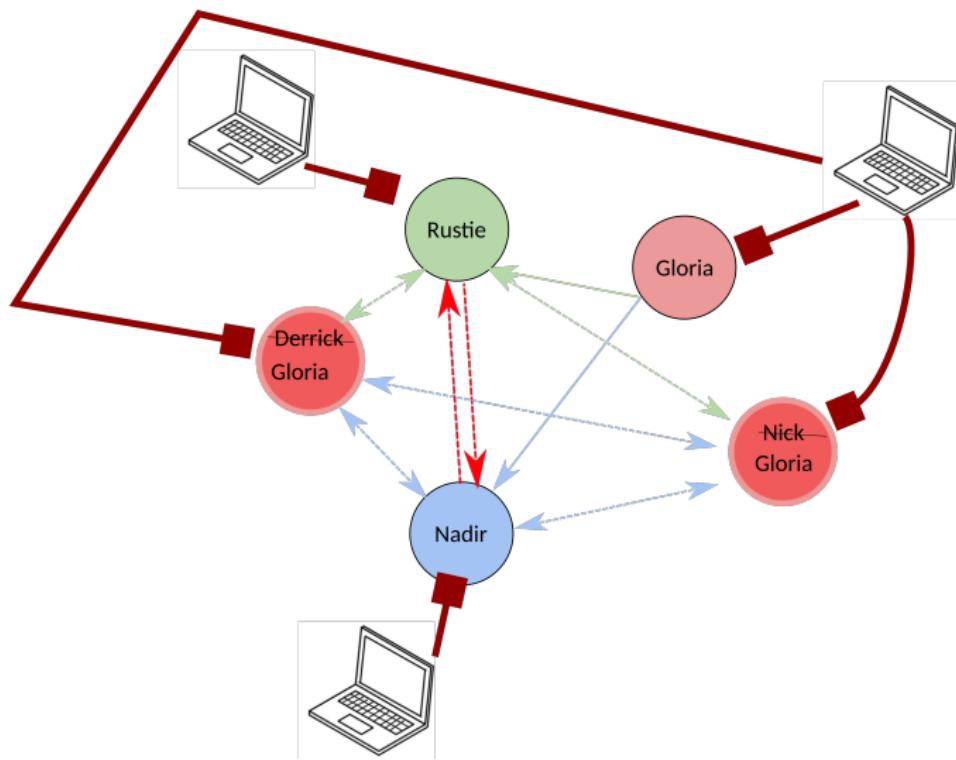
Preuve de travail (PoW) : Consensus de Nakamoto



Preuve de travail (PoW) : Consensus de Nakamoto



Preuve de travail (PoW) : Consensus de Nakamoto



Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

3. Systèmes distribués

- Système distribués
- Les Généraux Byzantins
- Blockchains et consensus
- **Comment maintenir le Consensus autrement ?**

4. Perspectives

- Perspectives

Consensus basé un enjeu

PoS, DPoS

BFT-based POS



Ouroboros Praos (Cardano)

- ▶ Tendermint (Cosmos)
- ▶ Algorand (ALG)
- ▶ Casper FFG (ETH)

Consensus basé un enjeu

PoS, DPoS



Ouroboros Praos (Cardano)

BFT-based POS



Tendermint (Cosmos Hub)

- ▶ Tendermint (Cosmos)
- ▶ Algorand (ALG)
- ▶ Casper FFG (ETH)

Consensus basé un enjeu

PoS, DPoS



BFT-based POS

Algorand

Algorand

Ouroboros Praos (Cardano)

- ▶ Tendermint (Cosmos)
- ▶ Algorand (ALG)
- ▶ Casper FFG (ETH)

Consensus basé un enjeu

PoS, DPoS



Ouroboros Praos (Cardano)

BFT-based POS



casper

Casper FFG (ETH)

- ▶ Tendermint (Cosmos)
- ▶ Algorand (ALG)
- ▶ Casper FFG (ETH)

D'autres consensus

- ▶ PoH (Histoire) Solana
- ▶ Preuve d'espace (Chia)
- ▶ POA (autorité)
- ▶ PoET (elapsed Time)

Consensus Exotique

- ▶ PoH (Preuve de non dépense)
- ▶ PoU (Preuve d'usage)
- ▶ PoST (temps d'enjeu)
- ▶ PoL (preuve de vie)

D'autres consensus

- ▶ PoH (Histoire) Solana
- ▶ Preuve d'espace (Chia)
- ▶ POA (autorité)
- ▶ PoET (elapsed Time)

Consensus Exotique

- ▶ PoH (Preuve de non dépense)
- ▶ PoU (Preuve d'usage)
- ▶ PoST (temps d'enjeu)
- ▶ PoL (preuve de vie)

D'autres consensus

- ▶ PoH (Histoire) Solana
- ▶ Preuve d'espace (Chia)
- ▶ POA (autorité)
- ▶ PoET (elapsed Time)



Consensus Exotique

- ▶ PoH (Preuve de non dépense)
- ▶ PoU (Preuve d'usage)
- ▶ PoST (temps d'enjeu)
- ▶ PoL (preuve de vie)

D'autres consensus

- ▶ PoH (Histoire) Solana
- ▶ Preuve d'espace (Chia)
- ▶ POA (autorité)
- ▶ PoET (elapsed Time)



Consensus Exotique

- ▶ PoH (Preuve de non dépense)
- ▶ PoU (Preuve d'usage)
- ▶ PoST (temps d'enjeu)
- ▶ PoL (preuve de vie)

D'autres consensus

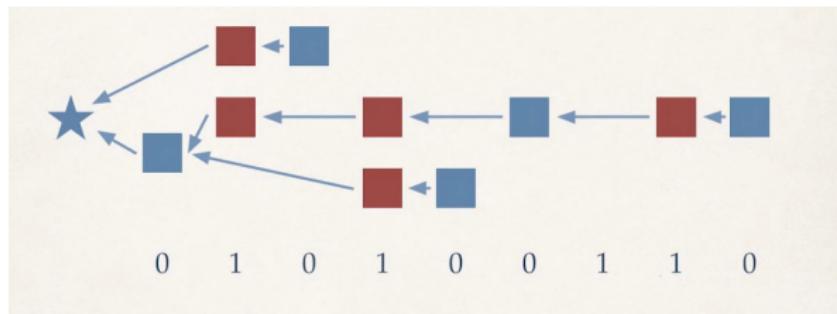
- ▶ PoH (Histoire) Solana
- ▶ Preuve d'espace (Chia)
- ▶ POA (autorité)
- ▶ PoET (elapsed Time)



Consensus Exotique

- ▶ PoH (Preuve de non dépense)
- ▶ PoU (Preuve d'usage)
- ▶ PoST (temps d'enjeu)
- ▶ PoL (preuve de vie)

Vulnérabilité des POS

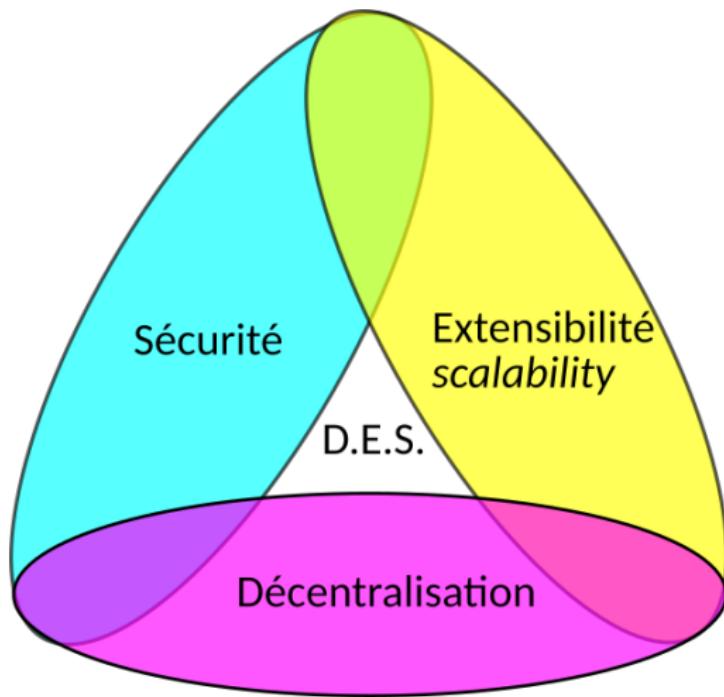


Simulation gratuite

- ▶ Il n'y rien en jeu
- ▶ Corruption postérieur
- ▶ Attaque longue distance (long range attack)
- ▶ Trafic sur l'enjeu (stake grinding attack)

Optimisations

Le trilemme



Optimisations

Vitesses : Segwit

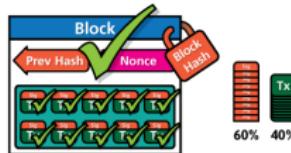
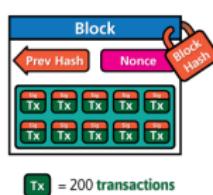
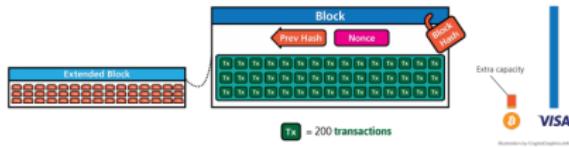
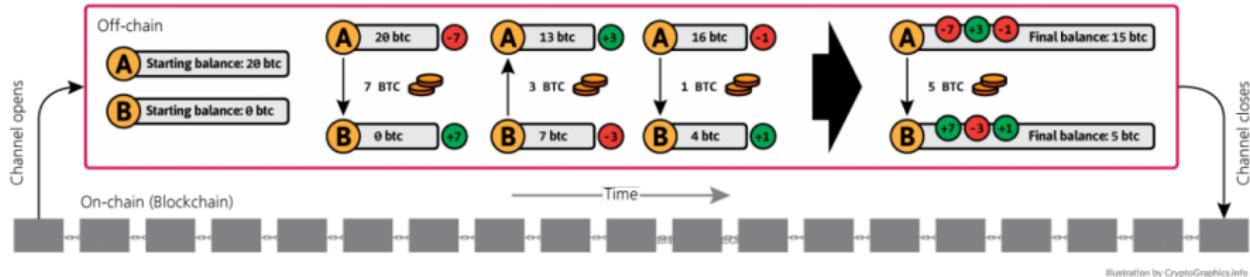


Illustration by CryptoGraphics.info

Vitesses : Segwit 2x



Vitesses : Améliorations lightning



Sommaire

1. Introduction

- De quoi allons-nous parler ?
- C'est quoi déjà la blockchain Bitcoin

2. La cryptographie au service de la blockchain

- Transactions (tx)
- Le modèle UTXO plus en détail
- Hash et signatures
- Comment vérifier les transactions
- Sécurité des clés

3. Systèmes distribués

- Système distribués
- Les Généraux Byzantins
- Blockchains et consensus
- Comment maintenir le Consensus autrement ?

4. Perspectives

- Perspectives

- ▶ Comment maintenir les consensus ?
- ▶ Cryptographie à l'épreuve des ordinateurs quantiques ?
- ▶ Quelle avenir pour les blockchains publiques ?

Merci

[plain]