Contrer la double dépense dans la blockchain Bitcoin

R. Ludinard,
ENSAI / CREST UMR 9194

Joint work with
E. Anceaume, CNRS UMR 6074,
T. Lajoie-Mazenc, KTH / CNRS,
B. Sericola, Inria Rennes - Bretagne Atlantique

École nationale
de la statistique
et de l'analyse
de l'information

Outline

Outline

Bitcoin

- Système pair-à-pair
- Trois types d'acteurs : utilisateur, pair, mineur
- Transactions : transfert de valeur entre deux utilisateurs
- Historique des transactions émises dans le système
- Registre répliqué sur chaque pair

Bitcoin

- Système pair-à-pair
- Trois types d'acteurs : utilisateur, pair, mineur
- Transactions : transfert de valeur entre deux utilisateurs
- Historique des transactions émises dans le système
- Registre répliqué sur chaque pair

Problème

En l'absence de tiers de confiance, comment

- vérifier la validité d'une transaction ?
- vérifier l'unicité d'une transaction ?
- enregistrer les transactions émises ?

ENSAI

Blocs

- Compétition des mineurs pour enregistrer les transactions
- Transactions incluses dans des blocs
- Mineurs essaient de trouver une PoW valide
- Blocs ajoutés à la blockchain
- Mineur ayant créé le bloc est rémunéré par la coinbase

Transactions

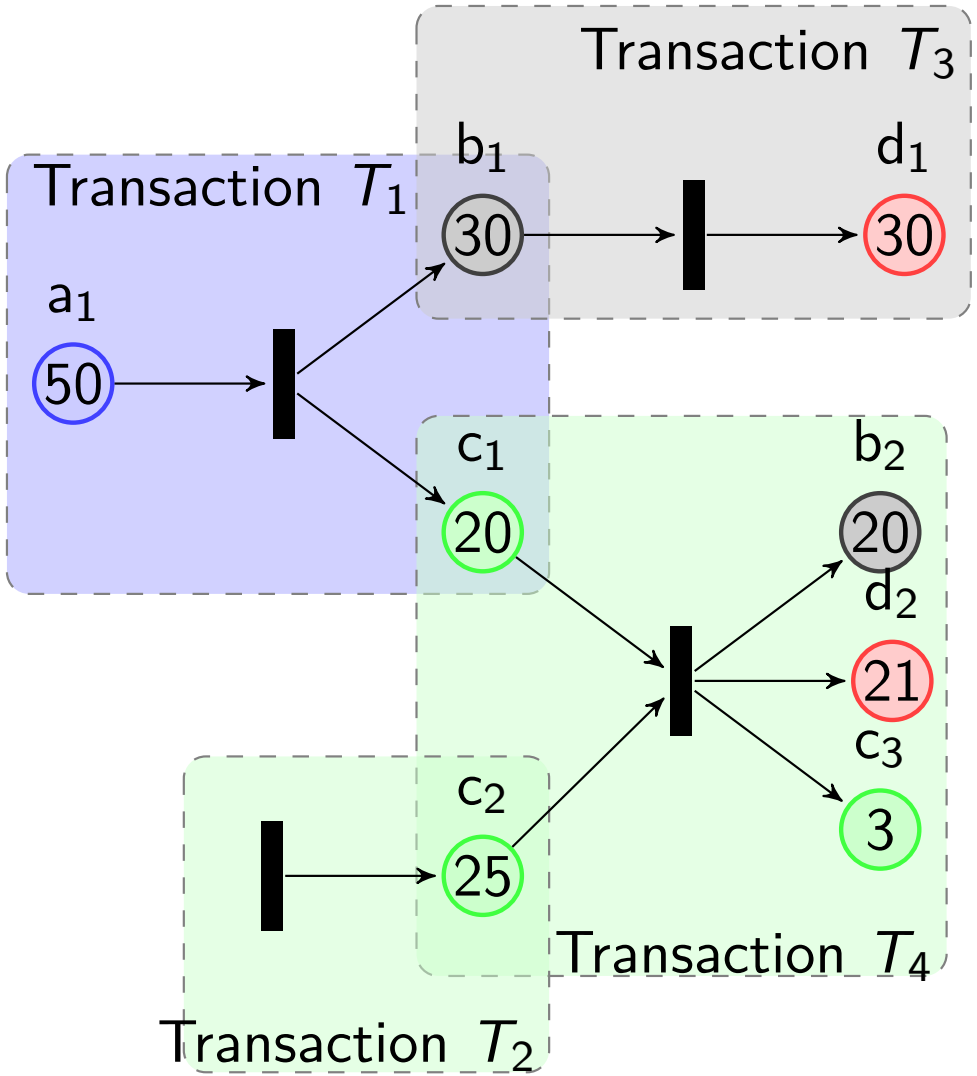
Transactions bien formées

Une transaction T est dite *bien formée* si

i) toutes les entrées appartiennent à l'utilisateur émettant T

ii) le montant total en entrée est supérieur au montant de sortie.

Transactions



Validité d'une transaction

- Vue locale de chaque pair p : $\mathscr{V}_k^{(p)} = \mathscr{P}_k^{(p)} \cup \mathscr{B}^{(p)}$.

Definition

Étant donné un pair p du réseau Bitcoin, p considère la k-ème transaction $T = (I, O)$ reçue comme *localement* valide si et seulement si les trois proproétés suivantes sont vérifiées :

$$\forall a \in I, \exists T' = (I', O') \in \mathscr{V}_{k-1}^{(p)}, \quad a \in O' \tag{1}$$

$$\forall T' = (I', O') \in \mathscr{V}_{k-1}^{(p)}, \quad I \cap I' = \emptyset \tag{2}$$

$$\forall a \in O, \forall T' = (I', O') \in \mathscr{V}_{k-1}^{(p)}, \quad a \notin O'. \tag{3}$$

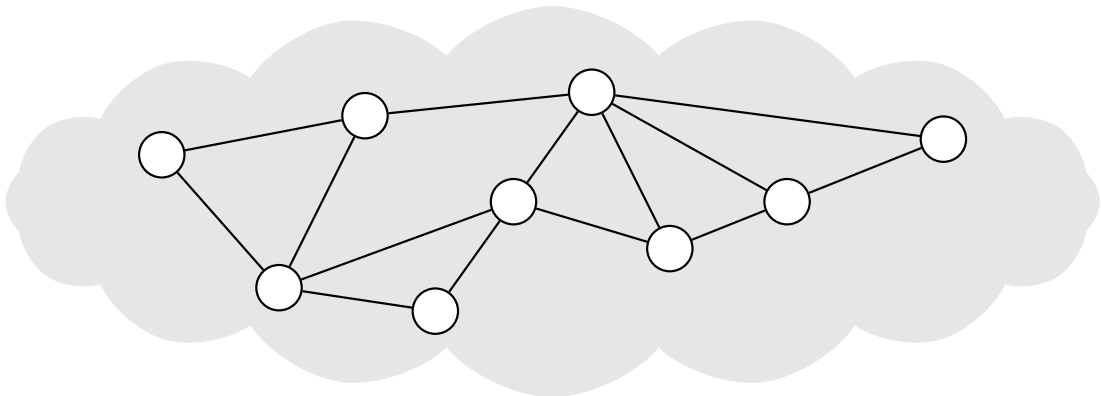
- Toute transaction valide est ajoutée à $\mathscr{P}_k^{(p)}$ et diffusée dans le réseau

ENSAI

Utilisation des transactions

Seller

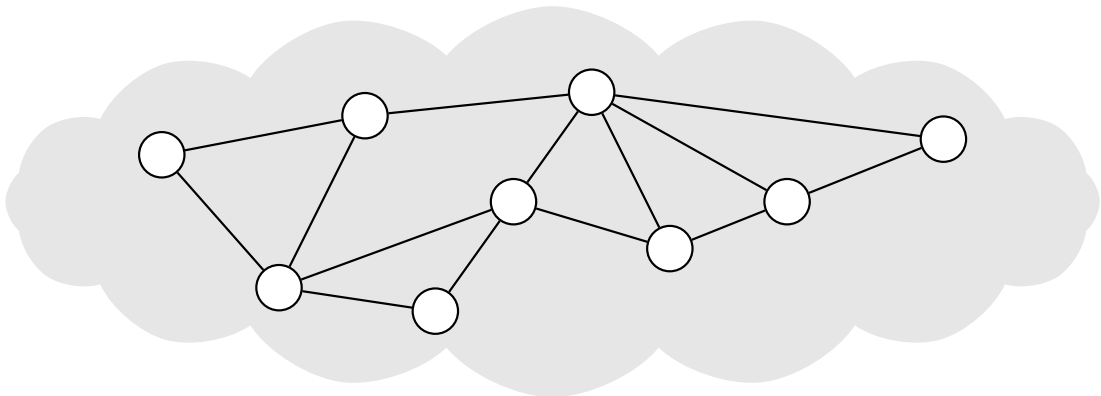
Client



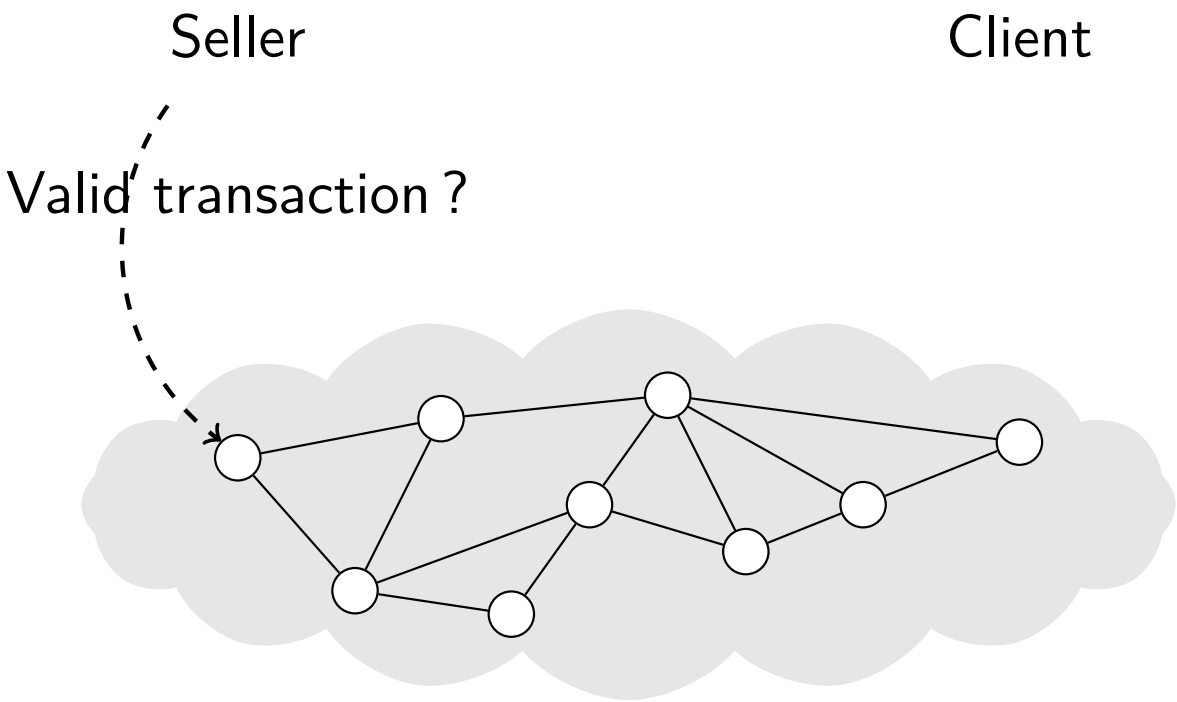
Utilisation des transactions

Signed transaction

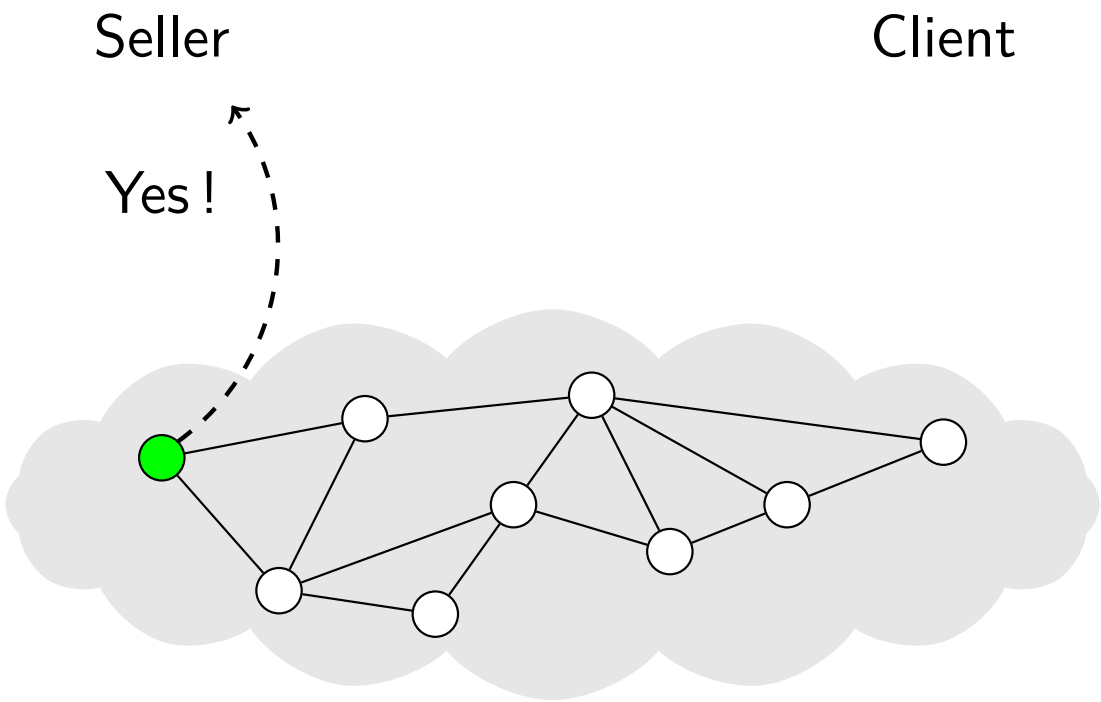
Seller ⇠- - - - - - - - - - - - - - - - - - Client



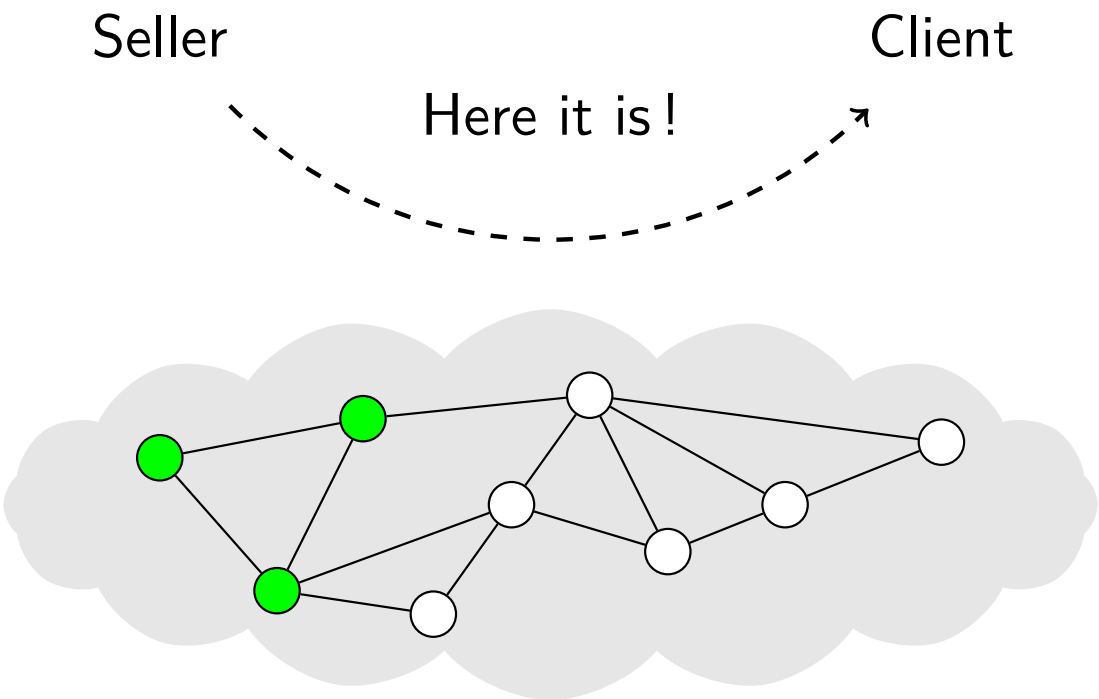
Utilisation des transactions



Utilisation des transactions

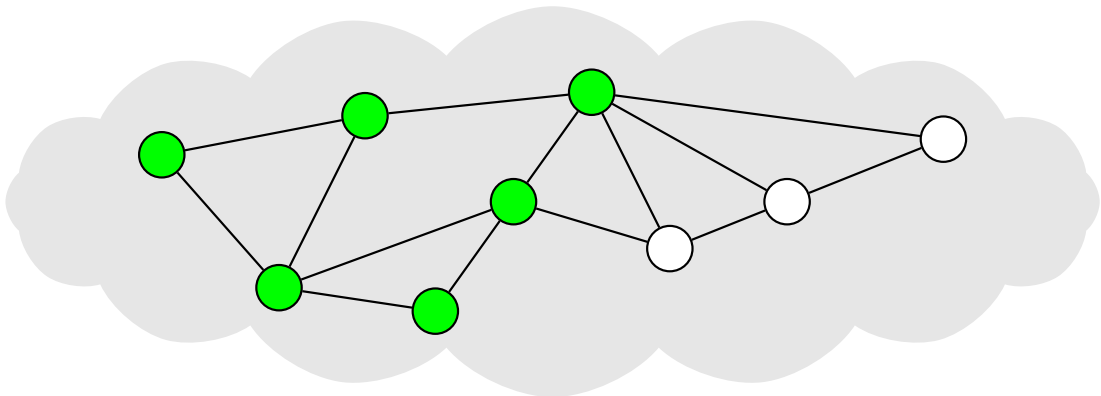


Utilisation des transactions



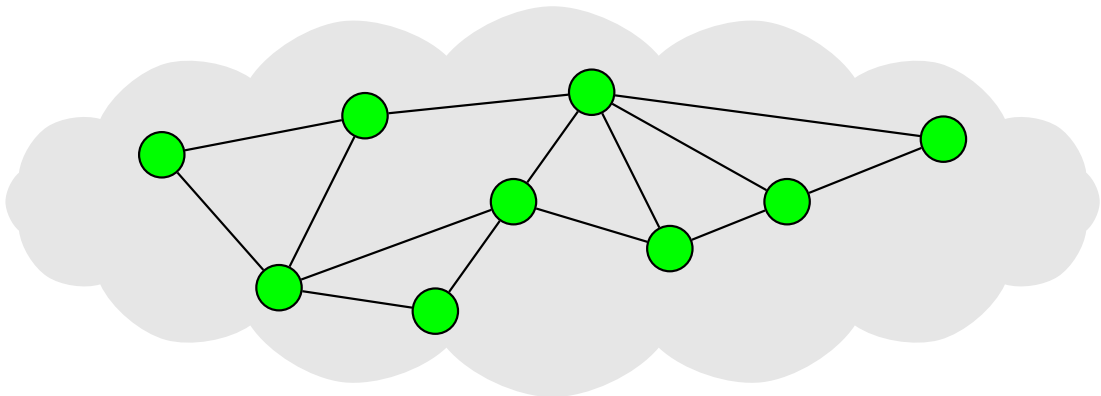
Utilisation des transactions

Seller Client



Utilisation des transactions

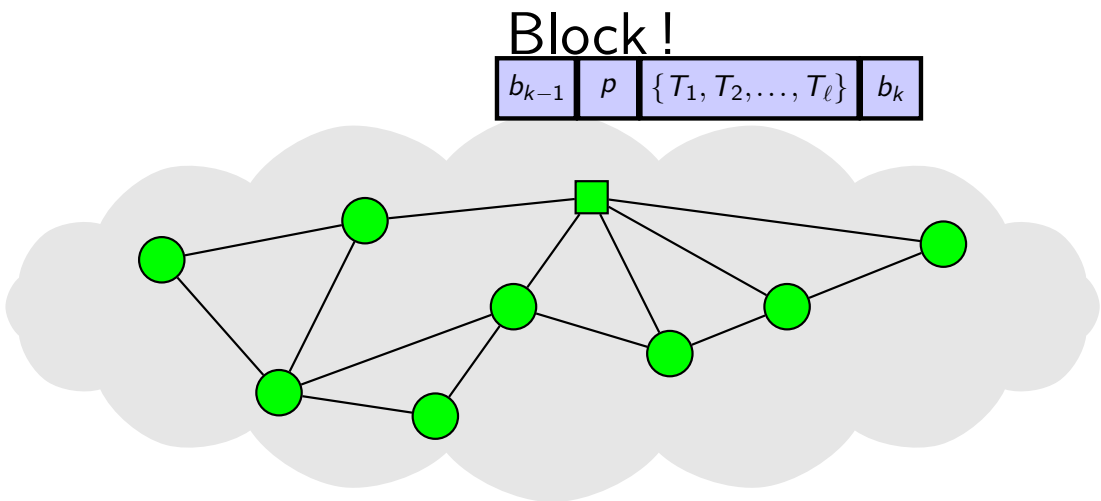
Seller Client



Transactions et blocs

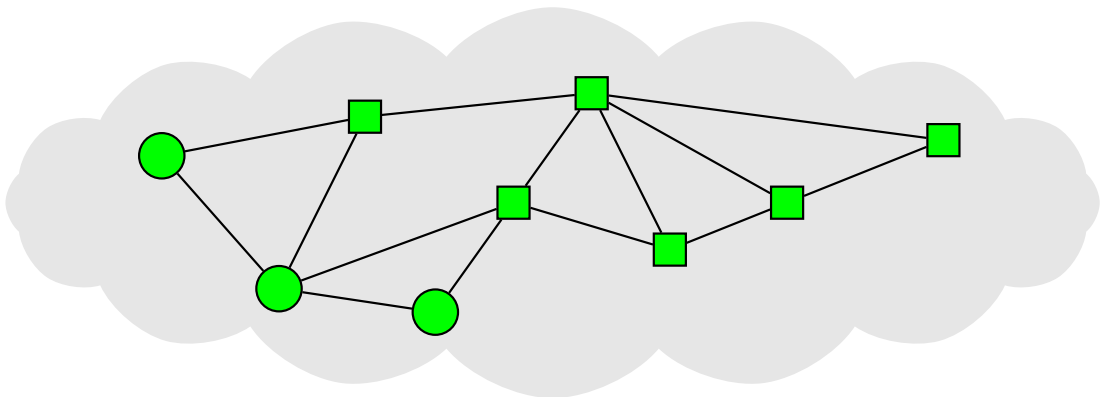
Seller

Client



Transactions et blocs

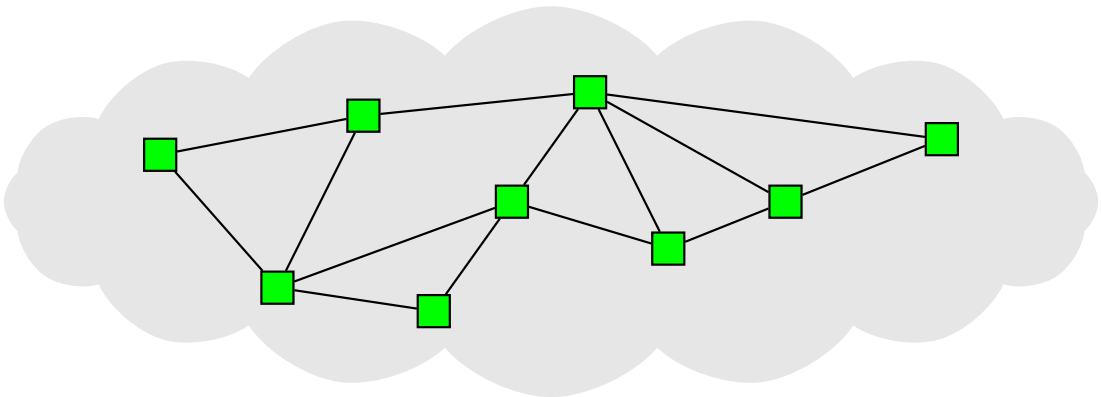
Seller Client



Transactions et blocs

Seller Client

Transaction confirmed



Confirmation des transactions

Confirmation locale de transaction

Étant donné un pair q du réseau Bitcoin, et une transaction localement valide T,

$$T \text{ est localement confirmée} \iff \exists! B \in \mathscr{B}^{(q)}, T \in B.$$

Le *niveau local de confirmation* de la transaction T par le pair q est égal à la profondeur du bloc B , *i.e.* la distance en nombre de blocs entre B et la queue de la blockchain (B inclus).

Situation de double dépense

Situation de double dépense

Étant donné un compte Bitcoin a_i, a_i est en situation de double dépense s'il existe deux transactions $T_1 = (I_1, O_1)$ et $T_2 = (I_2, O_2)$ telles que :

$$T_1, T_2 \in \bigcup_p \mathscr{V}^{(p)} \wedge a_i \in I_1 \cap I_2.$$

Transaction non conflictuelle

Une transaction $T = (I, O)$ est dite *non conflictuelle* si $\forall a \in I$, a n'est pas en situation de double dépense et la transaction $T' = (I', O') \in \mathscr{V}^{(p)}$ telle que $a \in O'$ est non conflictuelle.

Propriétés Bitcoin

Vivacité

Une transaction non conflictuelle finira par atteindre un niveau de confirmation “suffisant” pour un pair correct.

Sûreté

Une transaction non conflictuelle ayant un niveau de confirmation “suffisant” pour un pair correct finira par l’être pour tous les pairs corrects du système et le sera au même niveau de confirmation.

ENSAI

Propriétés Bitcoin

Vivacité

Une transaction non conflictuelle finira par atteindre un niveau de confirmation “suffisant” pour un pair correct.

Sûreté

Une transaction non conflictuelle ayant un niveau de confirmation “suffisant” pour un pair correct finira par l’être pour tous les pairs corrects du système et le sera au même niveau de confirmation.

Ces propriétés

- garantissent un préfixe de vue commun à tous les pairs corrects
- portent sur les transactions non conflictuelles

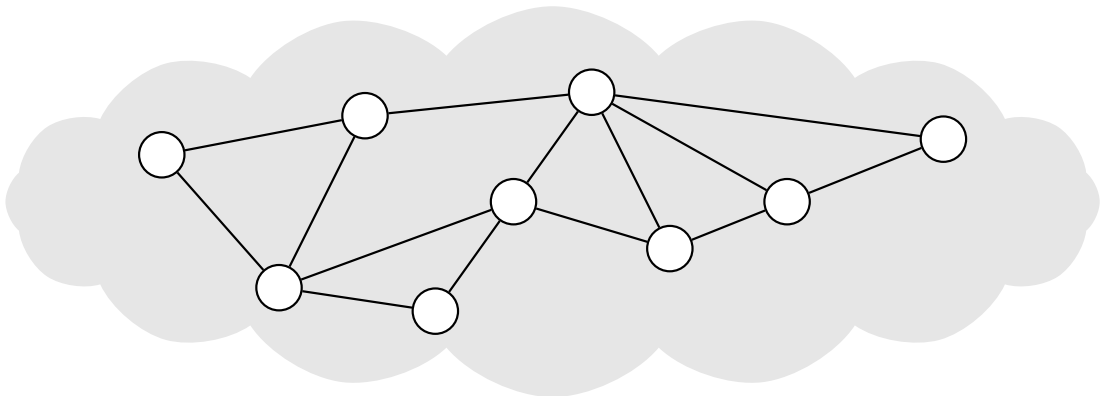
$\Rightarrow$ Aucune garantie à la reception. . .

ENSAI

Attaque par double dépense

Seller

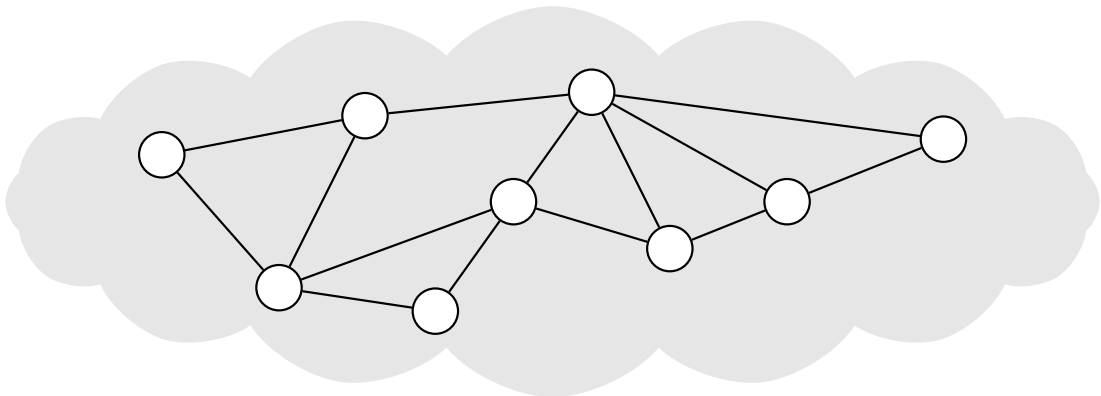
Client



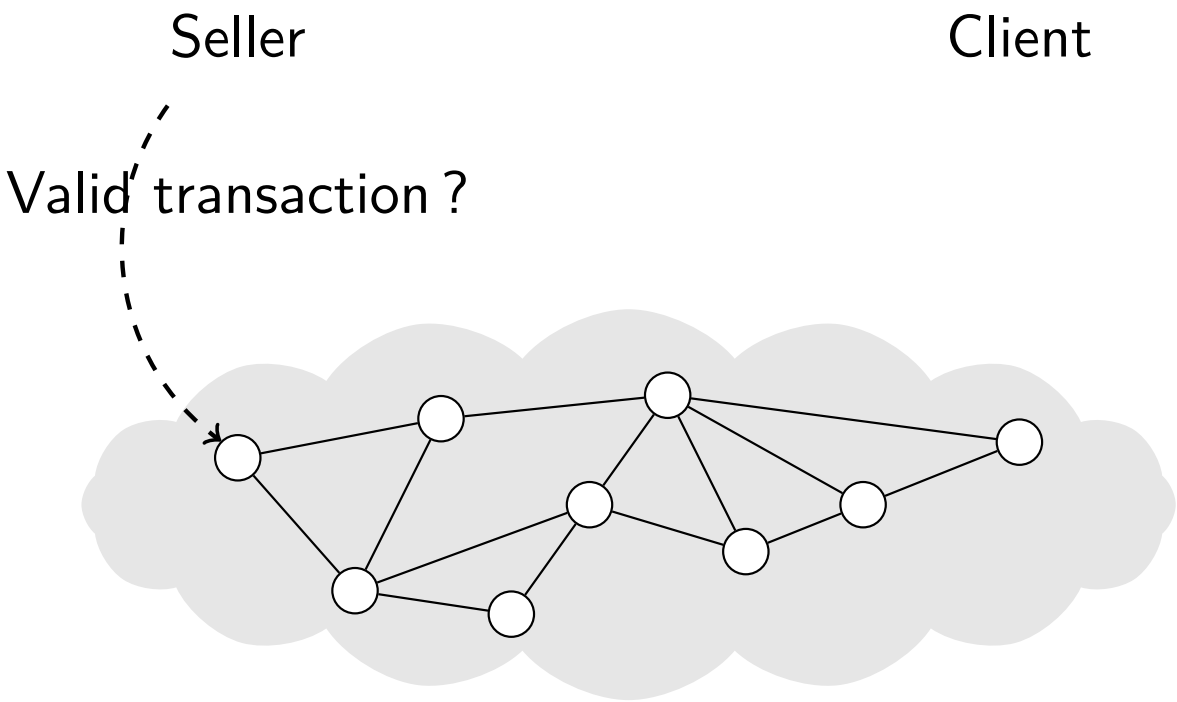
Attaque par double dépense

Signed transaction

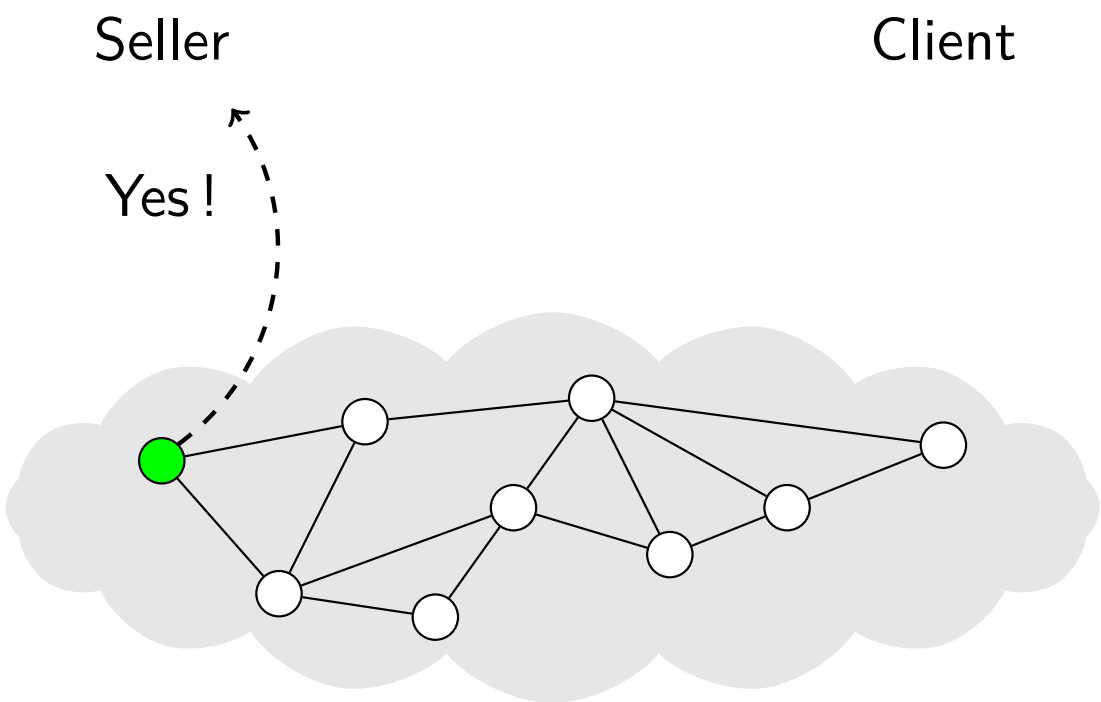
Seller ⇠- - - - - - - - - - - - - - - - - - Client



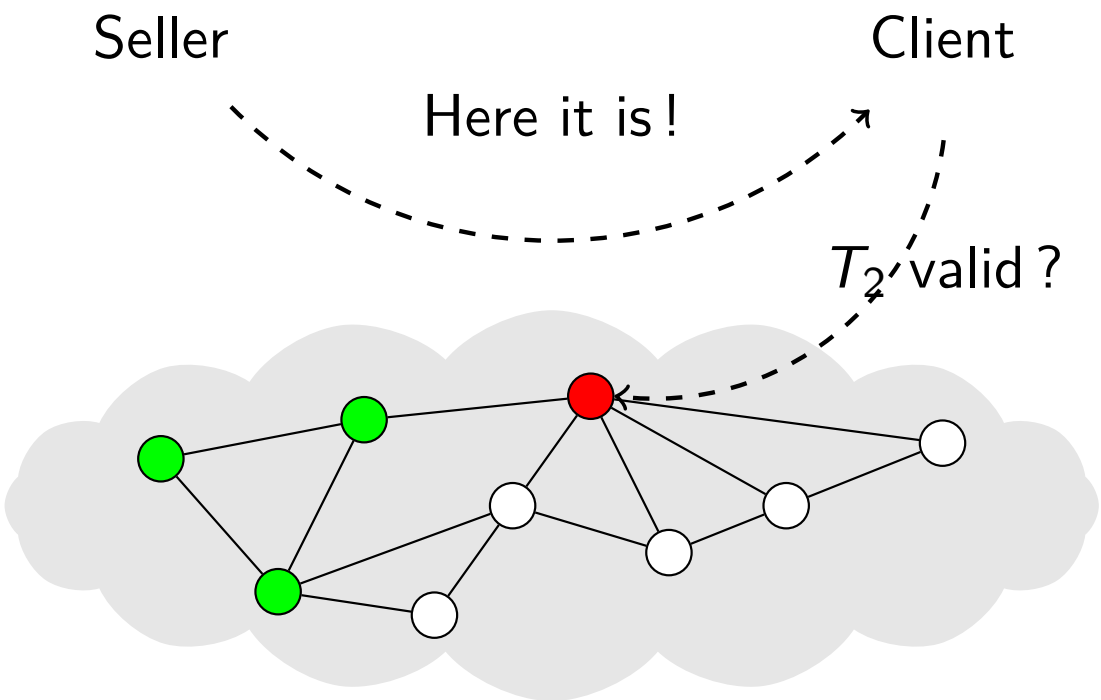
Attaque par double dépense



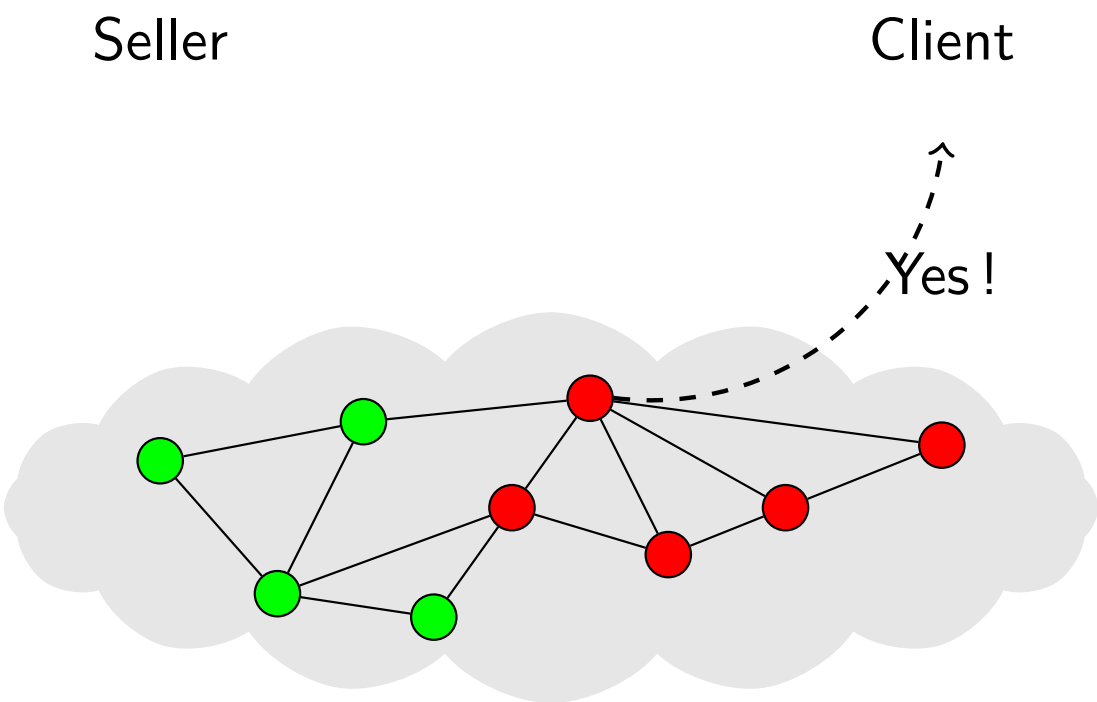
Attaque par double dépense



Attaque par double dépense



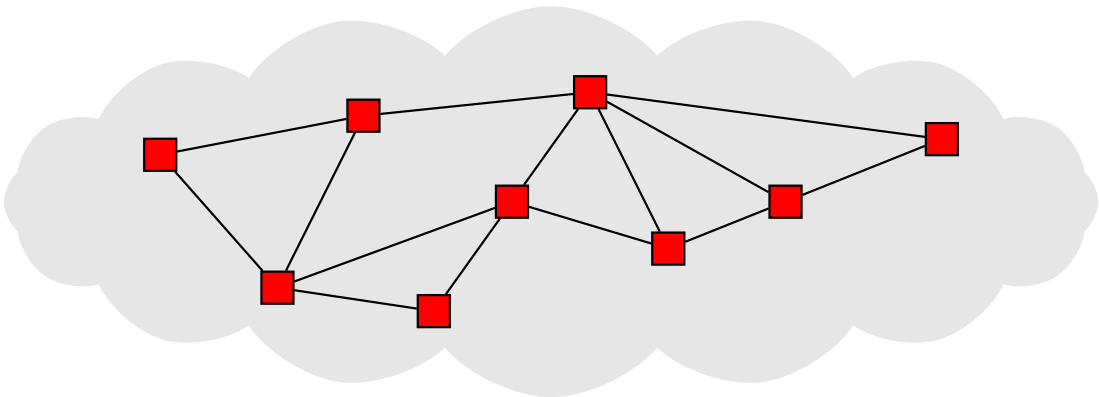
Attaque par double dépense



Attaque par double dépense

Seller Client

Green transaction rejected



Outline

Trois propositions d'améliorations

- **BitcoinNG :** I. Eyal, A. E. Gencer, E. G. Sirer et R. V. Renesse, "Bitcoin-NG : A scalable blockchain protocol", *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2016.
- **PeerCensus :** C. Decker, J. Seidel et R. Wattenhofer, "Bitcoin Meets Strong Consistency", *International Conference on Distributed Computing and Networking (ICDCN)*, 2016.
- **ByzCoin :** E. Kokoris-Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser et B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing.", *USENIX Security Symposium (USENIX Security)*, 2016.

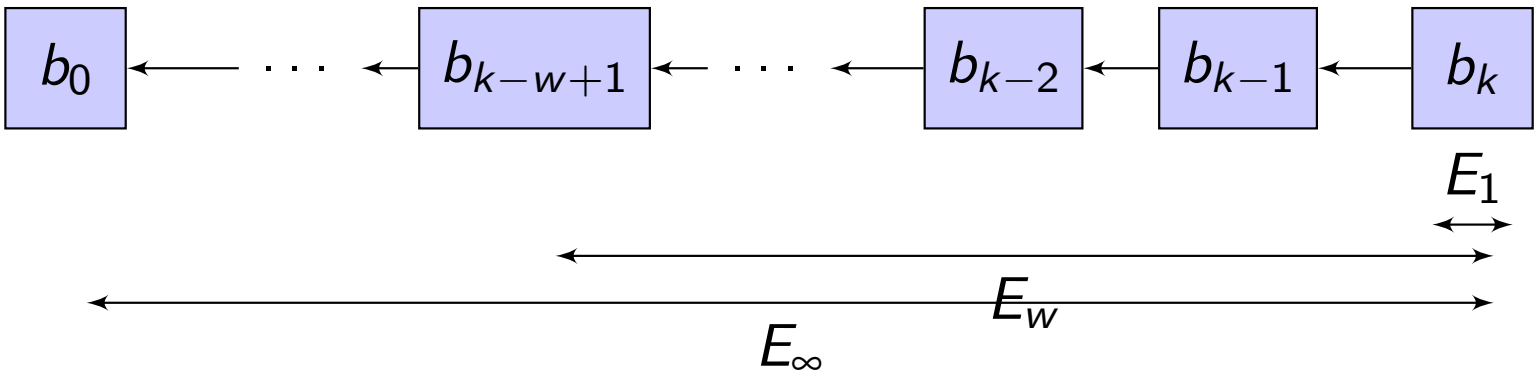
ENSAI

Trois propositions d'améliorations

- BitcoinNG [NSDI 2016]
- PeerCensus [ICDCN 2016]
- ByzCoin [Usenix Security 2016]

$\Rightarrow$ s'appuient exclusivement sur les mineurs

$\Rightarrow$ et sur un ensemble E_ℓ avec $\ell \in \{1, w, \infty\}$



BitcoinNG [NSDI 2016]

$\Rightarrow$ Introduire une cohérence forte dans Bitcoin

$\Rightarrow$ Découpler génération de bloc et validation des transactions

BitcoinNG [NSDI 2016]

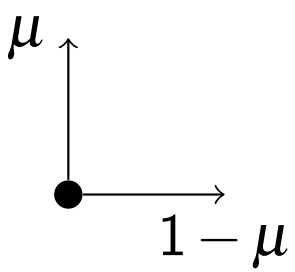
$\Rightarrow$ Introduire une cohérence forte dans Bitcoin

$\Rightarrow$ Découpler génération de bloc et validation des transactions

- Créer un bloc $\Leftrightarrow$ Élire un leader
- Leader valide toutes les transactions
- Transactions validées sont éligibles à l'inclusion dans un bloc

Évaluation de la sûreté

- Adversaire contrôlant $\mu \in (0,1)$ mineurs
- $B_k = (h, m) \in \mathbb{N}^* \times \mathbb{N}$,
  - k=taille de la blockchain,
  - h=nombre de blocs générés par des mineurs honnêtes,
  - m=nombre de blocs générés par des mineurs malveillants.
- $B_0 = (1, 0)$



BitcoinNG [NSDI 2016]

$\Rightarrow$ Introduire une cohérence forte dans Bitcoin

$\Rightarrow$ Découpler génération de bloc et validation des transactions

- Créer un bloc $\Leftrightarrow$ Élire un leader
- Leader valide toutes les transactions
- Transactions validées sont éligibles à l'inclusion dans un bloc

Deux limitations :

- Le leader valide toutes les transactions...
- Problèmes de sûreté :
  - $\Rightarrow$ Un leader malveillant sera élu (proportion μ)
  - $\Rightarrow$ Le leader a tout pouvoir pour réordonner les transactions

ENSAI

PeerCensus [ICDCN 2016]

$\Rightarrow$ Introduire une cohérence forte dans Bitcoin

$\Rightarrow$ Découpler génération de bloc et validation des transactions

Les membres de E_∞ s'accordent sur :

- la validité des transactions
- et la composition de E_∞

PeerCensus [ICDCN 2016]

$\Rightarrow$ Introduire une cohérence forte dans Bitcoin

$\Rightarrow$ Découpler génération de bloc et validation des transactions

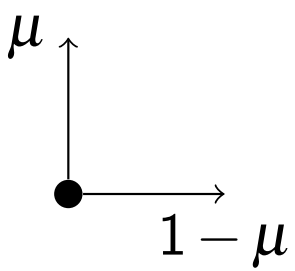
Les membres de E_∞ s'accordent sur :

- la validité des transactions
- et la composition de E_∞

- $E_\infty = \{$ mineurs ayant créé un bloc présent dans la blockchain$\}$
- $|E_\infty| \approx 435000$
- Complexité des algorithmes de consensus résilients aux byzantins $\mathcal{O}(n^3)$

Évaluation de la sûreté

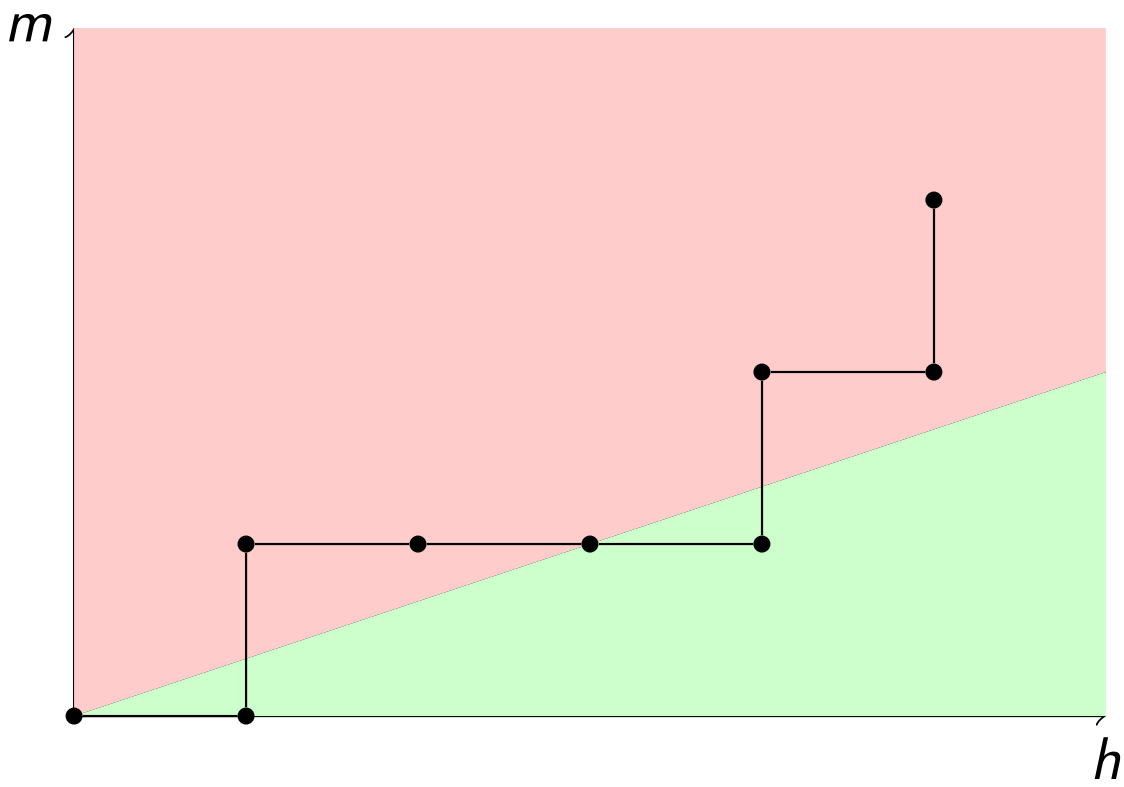
- Adversaire contrôlant $\mu \in (0,1)$ mineurs
- $B_k = (h, m) \in \mathbb{N}^* \times \mathbb{N}$,
  - k=taille de la blockchain,
  - h=nombre de blocs générés par des mineurs honnêtes,
  - m=nombre de blocs générés par des mineurs malveillants.
- $B_0 = (1, 0)$



ENSAI

Évaluation de la sûreté

- $\mathscr{S} = \{(h,m) \in \mathbb{N}^* \times \mathbb{N} \mid h \geq 2m+1\}$,
- $\mathscr{P} = \{(h,m) \in \mathbb{N}^* \times \mathbb{N} \mid h \leq 2m\}$.



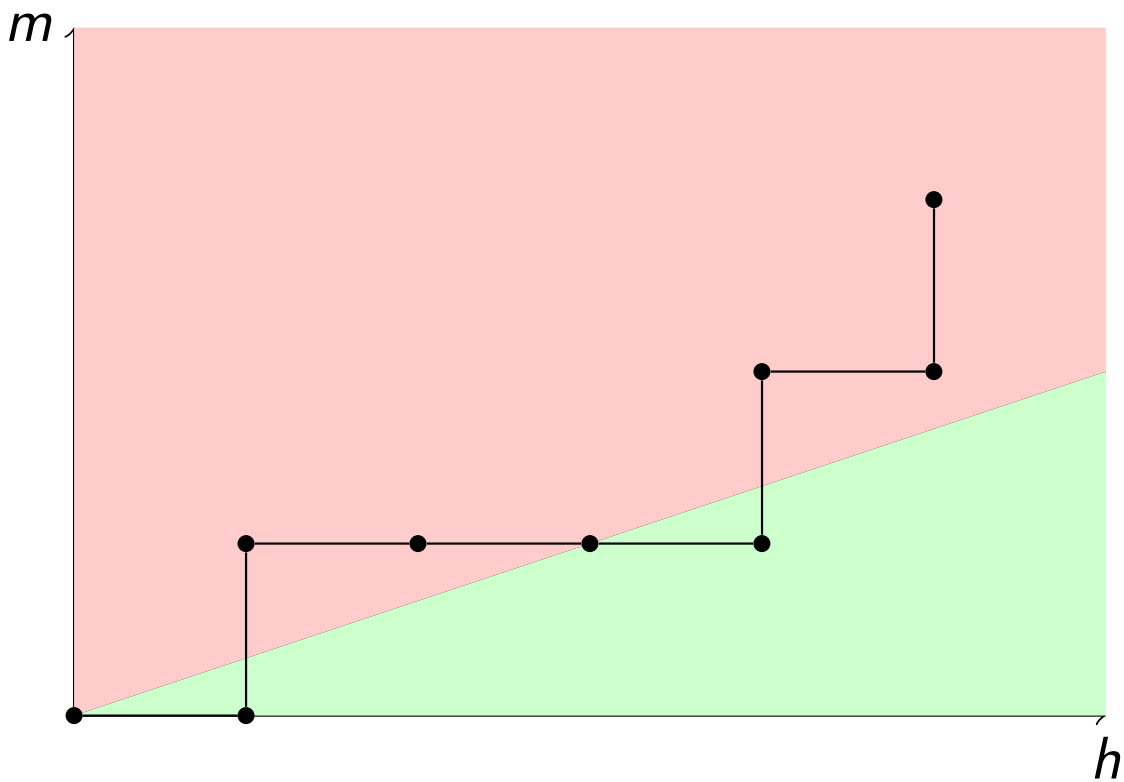
Évaluation de la sûreté

$$\mathbb{P}\{B_k = (h,m)\} = \binom{m+h-1}{h-1}(1-\mu)^{h-1}\mu^m 1_{\{k=m+h-1\}}.$$

$$\mathbb{P}\{B_k \in \mathscr{S}\} = \sum_{h=\lceil 2k/3\rceil}^{k} \binom{k}{h}(1-\mu)^h \mu^{k-h}.$$

$$\lim_{k\longrightarrow\infty} \mathbb{P}\{B_k \in \mathscr{S}\} = \begin{cases} 0 & \text{if} \quad \mu > 1/3 \\ 1/2 & \text{if} \quad \mu = 1/3 \\ 1 & \text{if} \quad \mu < 1/3. \end{cases}$$

Évaluation de la sûreté

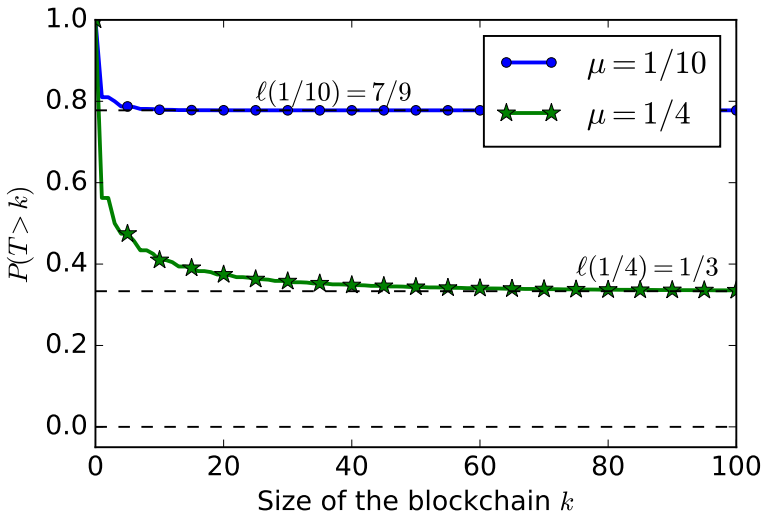


Évaluation de la sûreté

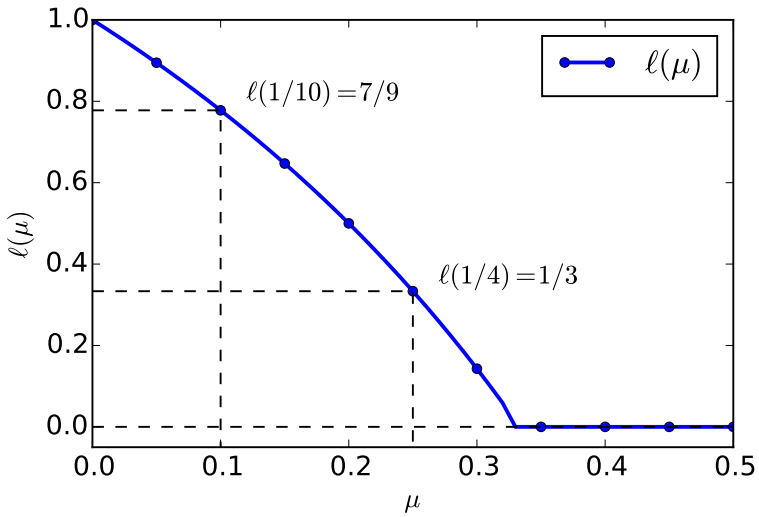
$$\mathbb{P}\{T > k\} = \frac{1}{1-\mu} \sum_{h=\lceil 2k/3 \rceil + 1}^{k+1} \binom{k+1}{h} (1-\mu)^h \mu^{k+1-h}$$
$$- \frac{3\mu}{1-\mu} \sum_{h=\lceil 2k/3 \rceil + 1}^{k} \binom{k}{h} (1-\mu)^h \mu^{k-h}.$$

$$\ell(\mu) = \lim_{k \longrightarrow \infty} \mathbb{P}\{T > k\} = \begin{cases} 0 & \text{if} \quad \mu > 1/3 \\ 1 - \dfrac{2\mu}{1-\mu} & \text{if} \quad \mu \leq 1/3. \end{cases}$$

Évaluation de la sûreté



(a) $\mathbb{P}\{T > k\}$ en fonction de μ et de la taille de la blockchain k



(b) Comportement asymptotique de $\mathbb{P}\{T > k\}$ en fonction de μ

ByzCoin [USENIX Security 2016]

$\Rightarrow$ Introduire une cohérence forte dans Bitcoin

$\Rightarrow$ Découpler génération de bloc et validation des transactions

Les membres de E_w s'accordent sur :

- la validité des transactions
- les nouveaux entrants dans E_w

Évaluation de la sûreté

- Adversaire contrôlant $\mu \in (0,1)$ mineurs
- $B_k = (h, m) \in \mathbb{N}^* \times \mathbb{N}$,
- $B_0 = (1, 0)$
- $\mathscr{S}_w = \{(m_0, \ldots, m_{w-1}) \in \{0,1\}^w \mid \sum_{i=0}^{w-1} m_i \leq (w-1)/3\}$,
- $\mathscr{P}_w = \{(m_0, \ldots, m_{w-1}) \in \{0,1\}^w \mid \sum_{i=0}^{w-1} m_i > (w-1)/3\}$

$$\mathbb{P}\{W_k \in \mathscr{S}_w\} = \sum_{\ell=0}^{(w-1)/3} \binom{w}{\ell} \mu^\ell (1-\mu)^{w-\ell}.$$

Évaluation de la sûreté

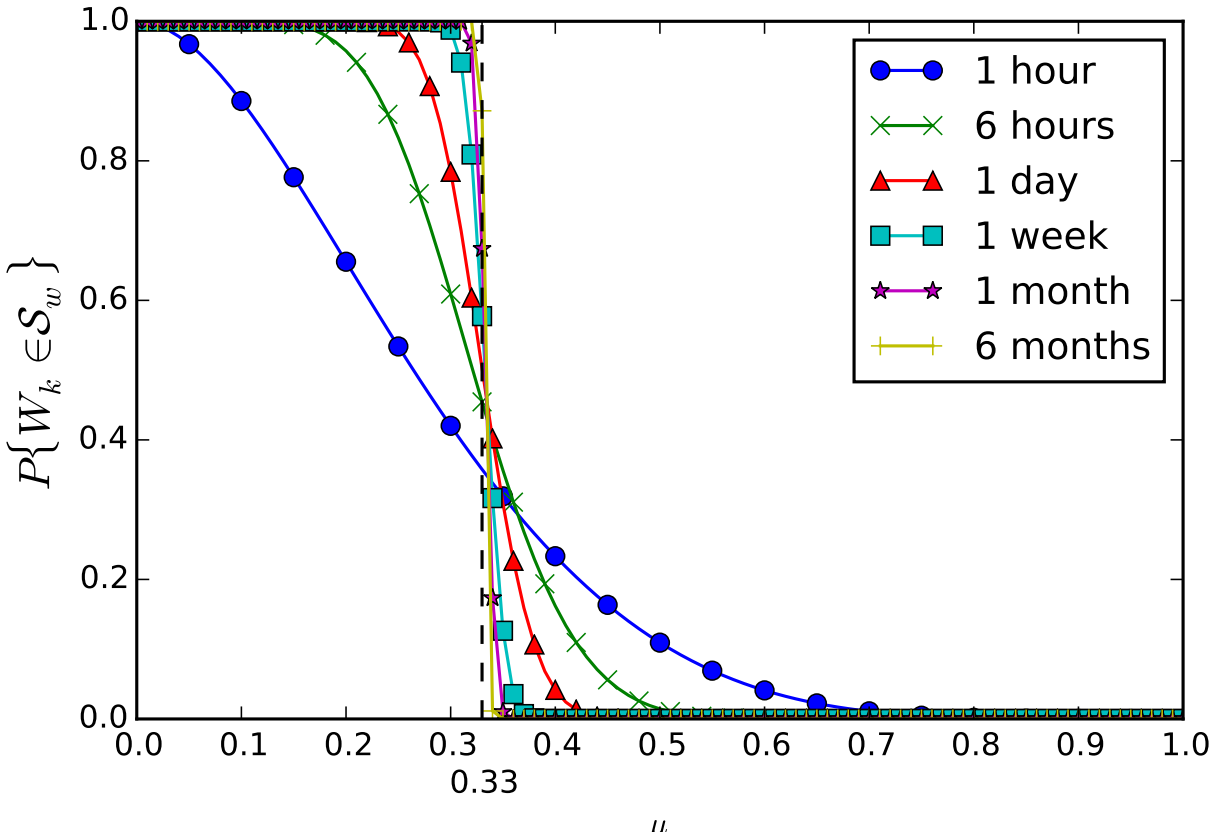
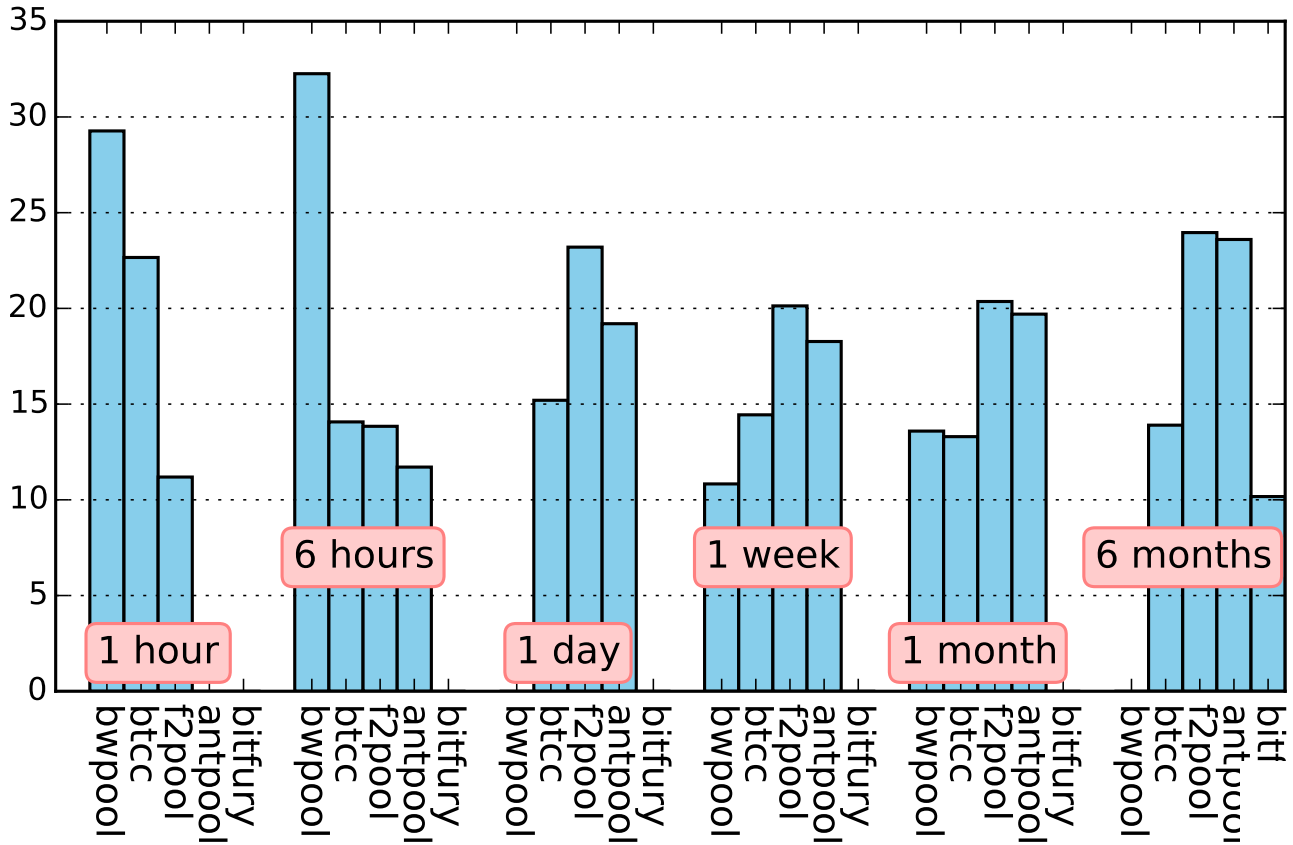


FIGURE – $\mathbb{P}\{W_k \in \mathscr{S}_w\}$ en fonction de μ and w

Évaluation de la sûreté

FIGURE – Proportion des blocs minés par les 5 mining pools les plus représentés en fonction de la durée w



Outline

Conclusion

- Bitcoin :
  - mécanismes,
  - garanties,
  - limitations.
- S'appuyer exclusivement sur les mineurs est dangereux
- Réel besoin de théorie pour comprendre et améliorer Bitcoin

E. Anceaume, T. Lajoie-Mazenc, R. Ludinard, B. Sericola, "Safety Analysis of Bitcoin Improvement Proposals", *Network Computing and Applications (IEEE NCA)*, 2016.

ENSAI