

Gestion des risques des mineurs de la blockchain

Pierre-O. Goffard

Institut de Science Financières et d'Assurances
pierre-olivier.goffard@univ-lyon1.fr

14 octobre 2021

1 Introduction

2 Théorie du risque en assurance

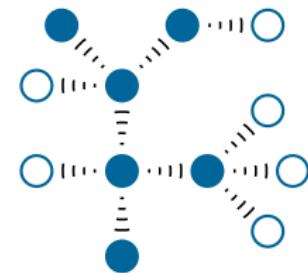
3 Lien avec la blockchain

Chaine de blocs

Introduction

Un registre sous la forme d'une suite de blocs maintenu par un réseau dont les noeuds appliquent un protocole de consensus

- Décentralisé
- Publique/privée
- Autorisé/Sans autorisation
- Inaltérable
- Système de récompense



On se concentre sur une chaine de blocs publiques équipée du protocole par preuve de travail.

Blocs

Introduction

Un bloc contient

- un indice
- un horodatage
- la valeur de hachage du bloc
- la valeur de hachage du bloc précédent
- Des transactions (les données enregistrées dans la chaîne de blocs)

```
Block Height: 0
Block Hash: a52bea61a9f4131588cc101e8e1c731fa9f69f16934c5ab3a05a2134a42c13e0
Time: 2021-07-12 10:03:04.812744
Block data: [{"sender": "Coinbase", "recipient": "Satoshi", "amount": 100, "fee": 1}]
Mined: False
Previous block hash: 0
-----
```

Protocole de consensus

Introduction

Mécanisme pour permettre aux noeuds du réseau de s'accorder sur les informations à inclure dans les blocs.

Trois dimensions à analyser

- 1** Efficacité
- 2** Décentralisation
- 3** Sécurité



X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms : mechanism, design and applications," *Science China Information Sciences*, vol. 64, nov 2020.

Preuve de travail

Introduction

Les noeuds sont en concurrence pour trouver la solution d'un problème via un procédé de type essai/erreur.

PoW

- 1 Choisir une nombre aléatoire (nonce)

$$X \sim \{1, \dots, 2^{32}\}.$$

- 2 Tant que $X > L$, où L correspond à la difficulté on recommence

Les noeuds sont choisis en fonction de leur puissance de calcul.



- S. Nakamoto, "Bitcoin : A peer-to-peer electronic cash system." Available at <https://bitcoin.org/bitcoin.pdf>, 2008.

Usage de la blockchain : Les cryptomonnaies

Introduction



S. Nakamoto, "Bitcoin : A peer-to-peer electronic cash system." Available at <https://bitcoin.org/bitcoin.pdf>, 2008.



- Transactions anonymes
- Fournir une monnaie stable dans certaine région du monde
- Transferts de valeur internationaux
- Pas d'autorité centrale

Le modèle de ruine de Cramer-Lunberg

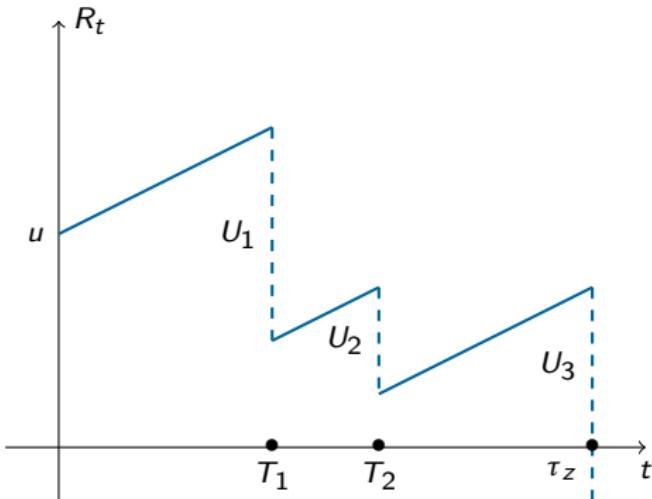
Théorie du risque en assurance

La réserve financière d'une compagnie d'assurance est donnée par

$$R_t = u + ct - \sum_{i=1}^{N_t} U_i, \quad t \geq 0,$$

où

- $u > 0$ est la réserve initial
- c est le taux de prime
- $(N_t)_{t \geq 0}$ est un processus de comptage égale au nombre de sinistres reportés à l'instant $t \geq 0$
 - ↪ Processus de Poisson d'intensité λ
- Les U_i sont les indemnisations
 - ↪ Suite de variables aléatoires positives, i.i.d., et indépendantes de N_t



Probabilités de ruine

Théorie du risque en assurance

Le temps de ruine est donné par

$$\tau_u = \inf\{t \geq 0 ; R_t < 0\}$$

et la probabilité de ruine par

$$\psi(u, t) = \mathbb{P}(\tau_u < t) \text{ et } \psi(u) = \mathbb{P}(\tau_u < \infty)$$

Trouver u tel que

$$\mathbb{P}(\text{Ruin}) = \alpha \text{ (0.005)},$$

avec

$$c = (1 + \eta)\lambda \mathbb{E}(U),$$

où

$$\eta > 0 \text{ (Condition de profitabilité)}$$

sinon

$$\psi(u) = 1.$$



S. Asmussen and H. Albrecher, *Ruin Probabilities*.
WORLD SCIENTIFIC, sep 2010.

Modèle de risque dual

Lien avec la blockchain

Soit un mineur

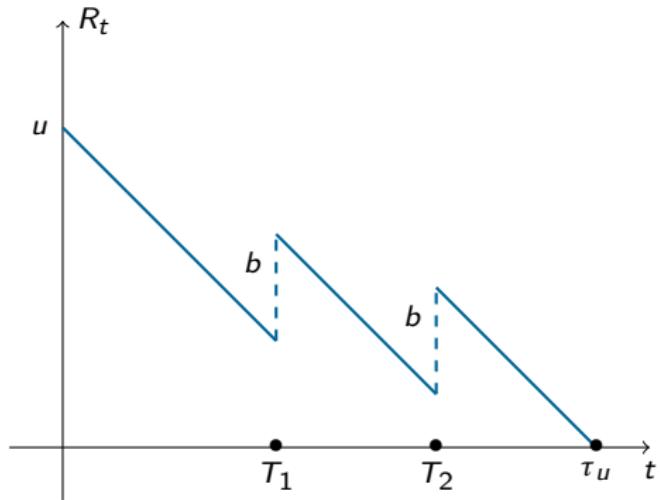
- dont la part de puissance de calcul est $p \in (0,1)$
- qui détient $u \geq 0$ initialement
- dépense $c = \pi_W \cdot W \cdot p$ par unité de temps
- trouve en moyenne $p\lambda$ blocs par unité de temps, où λ est le nombre de bloc trouvés par l'ensemble du réseau

La richesse du mineur est donnée par

$$R_t = u - c \cdot t + N_t \cdot b, \text{ (modèle de risque dual)}$$

où

- $(N_t)_{t \geq 0}$ est un processus de Poisson d'intensité $p \cdot \lambda$
- b est la récompense associée à l'ajout d'un bloc (6.25 BTC) bitcoinhalf.com



Profit espéré si solvabilité

Lien avec la blockchain

Remarque

Le coût opérationnel constant compensé par des récompenses peu fréquentes rend l'activité de minage risquée.

Le temps de ruine est défini par

$$\tau_u = \inf\{t \geq 0 ; R_t \leq 0\}$$

■ Mesure de risque

$$\psi(u, t) = \mathbb{P}(\tau_u \leq t)$$

■ Mesure de performance

$$V(u, t) = \mathbb{E}(R_t \mathbb{I}_{\tau_u > t})$$

Le dilemne du mineur

Lien avec la blockchain

ψ and V permettent de comparer le minage individuel

- au minage au sein d'un pool



M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011.



H. Albrecher, D. Finger, and P.-O. Goffard, "Blockchain mining in pools : Analyzing the trade-off between profitability and ruin," 2021.

- à la déviation par rapport au protocole (minage égoïste)



I. Eyal and E. G. Sirer, "Majority is not enough : Bitcoin mining is vulnerable," in *Financial Cryptography and Data Security*, pp. 436–454, Springer Berlin Heidelberg, 2014.



H. Albrecher and P.-O. Goffard, "On the profitability of selfish blockchain mining under consideration of ruin," *To appear in Operations Research*, May 2021.
<https://arxiv.org/abs/2010.12577>.

Des formules analytiques sont données pour

$$\hat{\psi}(u, t) = \mathbb{E}[\psi(u, T)] \text{ and } \hat{V}(u, t) = \mathbb{E}[V(u, T)],$$

où $T \sim \text{Exp}(t)$.

Minage solo

Lien avec la blockchain

Theorem (profit and ruin when mining solo)

Pour $u \geq 0$, on a

$$\hat{\psi}(u, t) = e^{\rho^* u},$$

et

$$\hat{V}(u, t) = u + (p\lambda b - c)t(1 - e^{\rho^* u}),$$

où ρ^* est la solution négative de l'équation

$$-c\rho + p\lambda(e^{b\rho} - 1) = 1/t. \quad (1)$$

Lambert function

La solution ρ^* de (1) est donnée par

$$\rho^* = -\frac{p\lambda t + 1}{ct} - \frac{1}{b} W\left[-\frac{p\lambda b}{c} e^{-b\left(\frac{p\lambda t + 1}{ct}\right)}\right],$$

où $W(\cdot)$ désigne la fonction de Lambert.

Elements de preuve

Lien avec la blockchain

L'horizon de temps est aléatoire avec $T \sim \text{Exp}(t)$, on réalise un bilan de probabilité sur l'intervalle $(0, h)$, avec $h < u/c$ ce qui rend la ruine impossible avant h . Trois possibilités

- (i) $T > h$ et pas de nouveau bloc sur $(0, h)$
- (ii) $T < h$ et pas de nouveau bloc sur $(0, T)$
- (iii) Un bloc est découvert avant T et h

Pour la richesse espérée $\hat{V}(u, t)$, on a

$$\begin{aligned}\hat{V}(u, t) &= e^{-h(1/t+p\lambda)} \hat{V}(u - ch, t) + \int_0^h \frac{1}{t} e^{-s(1/t+p\lambda)} (u - cs) ds \\ &+ \int_0^h p\lambda e^{-s(1/t+p\lambda)} \hat{V}(u - cs + b, t) ds.\end{aligned}$$

Elements de preuve

Lien avec la blockchain

On dérive par rapport à h et on prend $h=0$ pour obtenir

$$c\hat{V}'(u,t) + \left(\frac{1}{t} + p\lambda\right)\hat{V}(u,t) - p\lambda\hat{V}(u+b,t) - \frac{u}{t} = 0, \quad (2)$$

L'équation (2) est une équation différentielle avec avance. Les conditions limites sont

$$\hat{V}(0,t) = 0 \text{ et tel que } 0 \leq \hat{V}(u,t) \leq u - ct + p\lambda bt \text{ pour } u > 0.$$

Considérons les solutions de la forme

$$\hat{V}(u,t) = Ae^{\rho u} + Bu + C, \quad u \geq 0, \quad (3)$$

où A, B, C et ρ sont des constantes à déterminer. La substitution de (3) dans (2) en tenant compte des conditions initiales mène au système d'équations

$$\begin{cases} 0 = ctp + (1 + p\lambda t) - p\lambda te^{\rho b}, \\ 0 = B(1 + tp\lambda) - p\lambda tB - 1, \\ 0 = Bct + C(1 + tp\lambda) - p\lambda tBb - p\lambda tC, \\ 0 = A + C. \end{cases}$$

. H. L. Smith, *An introduction to delay differential equations with applications to the life sciences*. Springer, New York, 2011.

Elements de preuve

Lien avec la blockchain

On obtient $A = -t(p\lambda b - c)$, $B = 1$, $C = t(p\lambda b - c)$ et ρ solution de

$$c\rho + (1 + p\lambda t) - p\lambda t e^{\rho b} = 0,$$

qui admet une solution négative et une solution positive. Comme $A < 0$, nous devons prendre la solution négative $\rho^* < 0$ pour satisfaire la condition $\hat{V}(u, t) > 0$. La substitution de A, B, C et ρ^* dans (3) renvoie le résultat.

De manière analogue, la probabilité de ruine vérifie

$$c\hat{\psi}'(u, t) + (p\lambda + 1/t)\hat{\psi}(u, t) - p\lambda\hat{\psi}(u + b, t) = 0$$

avec les conditions initiales $\hat{\psi}(0, t) = 1$ et la condition limite $\lim_{u \rightarrow \infty} \hat{\psi}(u, t) = 0$.

Comment fonctionne un pool de minage ?

Lien avec la blockchain

Un ensemble de mineurs $I \subset \{1, \dots, n\}$ totalise une proportion

$$p_I = \sum_{i \in I} p_i,$$

de la puissance de calcul du réseau.

- Un gestionnaire coordonne cette association
- Les mineurs prouvent leur contributions en soumettant des solutions partielles (*parts*)

Le gestionnaire décide

- du système de rémunération
- de la difficulté relative $q \in (0, 1)$ de trouver une *part* plutôt qu'une vraie solution
- des frais de participation f

Système de redistribution

Lien avec la blockchain

Les mineurs doivent être rémunéré à hauteur de leur contribution à l'effort de minage.

Rémunération proportionnel

Un tour est le temps séparant la découverte de deux blocs

- s_i est le nombre de *parts* soumis par le mineur $i \in I$ durant le *tour*
- Chaque mineur reçoit à la fin du *tour*

$$(1-f) \cdot b \cdot \frac{s_i}{\sum_{i \in I} s_i},$$

où f représente le taux de frais perçu par le gestionnaire.

- Le système est dit juste si $\frac{s_i}{\sum_{i \in I} s_i}$ converge vers $\frac{p_i}{\sum_{i \in I} p_i}$

Le problème du système proportionnel

Lien avec la blockchain

Remarque

Le système de rémunération proportionnel est juste mais pas incitatif.



O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions," in *Financial Cryptography and Data Security*, pp. 477–498, Springer Berlin Heidelberg, 2017.

- La durée des *tours* est aléatoire
 - Une *part* perd de la valeur lorsque le *tour* s'éternise \Rightarrow *pool hoping*
 - M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011.
 - Appliquer un facteur d'actualisation à la valeur des *parts*
 - slush pool, "Reward system specifications," 2021.
- Un mineur peut retarder la communication d'une solution
 - Pour attendre que son taux de *part* soit en accord avec sa puissance de calcul
- Aucun transfert de risque des mineurs vers le gestionnaire
 - f doit être minimale

Le système Pay-per-Share (PPS)

Lien avec la blockchain

Le gestionnaire paie

$$w = (1 - f) \cdot q \cdot b$$

pour chaque *part* et conserve l'intégralité de la récompense des blocs.

Richesse du mineur

$$R_t^I = u_I - ct + M_t^I w, \quad t \geq 0.$$

où

- $(M_t^I)_{t \geq 0}$ est un processus de Poisson d'intensité $p_I \mu = p_I \lambda / q$
- μ correspond au nombre moyen de *parts* soumises par le réseau

Richesse du gestionnaire

$$R_t^I = u_I - M_t^I w + N_t^I b, \quad t \geq 0.$$

où

- $(M_t^I)_{t \geq 0}$ est un processus de Poisson d'intensité $p_I \mu = p_I \lambda / q$
- $(N_t^I)_{t \geq 0}$ est un processus de Poisson d'intensité $p_I \lambda$

Risque du gestionnaire

Lien avec la blockchain

On remplace les récompenses déterministes par des récompenses aléatoires, la richesse du gestionnaire devient

$$R_t = u - \sum_{i=1}^{M_t} W_i + \sum_{j=1}^{N_t} B_j, \quad t \geq 0.$$

où

- $(M_t)_{t \geq 0}$ et $(N_t)_{t \geq 0}$ sont des processus de Poisson d'intensité respective $\mu^* = \mu - \lambda$ et λ
- $(W_i)_{i \geq 0}$ et $(B_j)_{j \geq 0}$ sont deux suites indépendantes de variables aléatoires **iid** de loi exponentielle de moyenne w et $b^* = b - w$.

Superposition de processus de Poisson

La découverte d'un bloc est associé au paiement d'une part aux mineurs

- L'intensité de M_t est donnée par $\mu^* = \mu - \lambda$
- La moyenne des récompense pour la découverte d'un bloc est donnée par $b^* = b - w$

Cela permet de distinguer les sauts vers le haut et vers le bas tout en rendant les processus de Poisson indépendants.

Risque du gestionnaire

Lien avec la blockchain

Théorème (Pertes et profits du gestionnaire)

La probabilité de ruine est donnée par

$$\hat{\psi}(u, t) = (1 - R w) e^{-R u}, \quad u \geq 0,$$

et la richesse espérée par

$$\hat{V}(u, t) = (1 - R w)[w - t(\lambda b^* - \mu^* w)] e^{-R u} + u + t(\lambda b^* - \mu^* w),$$

où R est la seule solution

$$-(t^{-1} + \lambda + \mu^*) + \lambda(1 + b^* r)^{-1} + \mu^*(1 - wr)^{-1} = 0.$$

de partie réelle positive.



H. Albrecher, D. Finger, and P.-O. Goffard, "Blockchain mining in pools : Analyzing the trade-off between profitability and ruin," 2021.

Elements de preuve I

Lien avec la blockchain

Bilan de probabilité sur l'intervalle $(0, h)$. Quatre possibilités

- (i) $T > h$ et pas de saut sur $(0, h)$
- (ii) $T < h$ et pas de saut sur $(0, T)$
- (iii) Un saut vers le haut sur $(0, h)$
- (iv) Un saut vers le bas sur $(0, h)$

$$\begin{aligned}\hat{V}(u, t) &= e^{-(\frac{1}{t} + \lambda + \mu^*)h} \hat{V}(u, t) + \frac{1}{t} \int_0^h e^{-s/t} e^{-(\lambda + \mu^*)s} u ds \\ &+ \lambda \int_0^h e^{-\lambda s} e^{-(1/t + \mu^*)s} \int_0^\infty \hat{V}(u+x, t) dF_B(x) ds \\ &+ \mu^* \int_0^h e^{-\mu^* s} e^{-(1/t + \lambda)s} \int_0^u \hat{V}(u-y, t) dF_W(y) ds.\end{aligned}$$

On dérive par rapport à h et on fait tendre $h \rightarrow 0$, ce qui mène à l'équation intégrale

$$\lambda \int_0^\infty \hat{V}(u+x, t) dF_B(x) - (\lambda + \mu^* + 1/t) \hat{V}(u, t) + \mu^* \int_0^u \hat{V}(u-y, t) dF_W(y) + u/t = 0, \quad u \geq 0, \quad (4)$$

munie des conditions initiales $\hat{V}(u, t) = 0$ pour tout $u < 0$ et $0 \leq \hat{V}(u, t) \leq u + (\lambda b^* - \mu^* w)t$. On considère des solutions de la forme

$$Ce^{-ru} + d_1 u + d_0$$

Elements de preuve II

Lien avec la blockchain

- Par comparaison des termes en e^{-ru} on obtient une équation pour r avec

$$-(t^{-1} + \lambda + \mu^*) + \lambda(1 + b^* r)^{-1} + \mu^*(1 - wr)^{-1} = 0$$

dont l'unique solution positive $R > 0$ est valide au vu de la borne

$$0 \leq \hat{V}(u, t) \leq u + (\lambda b^* - \mu^* w)t$$

- Par comparaison des termes en u , il vient $d_1 = 1$
- Par comparaison des termes en 1 il vient

$$d_0 = t(\lambda b^* - \mu^* w)$$

- Par comparaison des termes en $e^{-u/w}$, on a

$$C = (1 - R w)[w - t(\lambda b^* - \mu^* w)]$$

Problèmes liés au minage

Lien avec la blockchain

- Course à l'armement, Consommation électrique importante et génération de e-déchet
 -  C. Bertucci, L. Bertucci, J.-M. Lasry, and P.-L. Lions, "Mean field game approach to bitcoin mining," 2020.
 -  H. Alsabah and A. Capponi, "Bitcoin mining arms race : R&d with spillovers," *SSRN Electronic Journal*, 2018.
- Une menace sur la décentralisation ?
 -  L. W. Cong, Z. He, and J. Li, "Decentralized mining in centralized pools," *The Review of Financial Studies*, vol. 34, pp. 1191–1235, apr 2020.
 -  Z. Li, A. M. Reppen, and R. Sircar, "A mean field games model for cryptocurrency mining," 2019.