MAD M1 Actuariat/ES

Chapitre III: Martingale, processus de branchement et marche aléatoire

Pierre-Olivier Goffard

Université de Lyon 1
ISFA
pierre-olivier.goffard@univ-lyon1.fr

ISFA
January 30, 2023

I. Martingale à temps discret

Definition 1 (Processus adapté)

Un processus $(X_n)_{n\in\mathbb{N}}$ est adapté à la filtration $\mathscr{F}_n$ ($\mathscr{F}_n$-adapté), si X_n est mesurable par rapport à la tribu $\mathscr{F}_n$.

Remarque 1

La filtration $\sigma(X_0,\ldots,X_n)$ est la plus petite filtration rendant le processus $(X_n)_{n\in\mathbb{N}}$ adapté.

Definition 2 (martingale, sur-martingale, sous-martingale)

Soit $(X_n)_{n\in\mathbb{N}}$ un processus $\mathscr{F}_n$-adapté tel que $\mathbb{E}(|X_n|)<\infty$ pour tout $n\in\mathbb{N}$. On dit que

- Une martingale si
$$\mathbb{E}(X_{n+1}|\mathscr{F}_n)=X_n, \text{ pour tout } n\in\mathbb{N}.$$
- Une sur-martingale si
$$\mathbb{E}(X_{n+1}|\mathscr{F}_n)\leq X_n, \text{ pour tout } n\in\mathbb{N}.$$
- Une sous-martingale si
$$\mathbb{E}(X_{n+1}|\mathscr{F}_n)\geq X_n, \text{ pour tout } n\in\mathbb{N}.$$

Remarque 2

Une sur-martingale décroit en moyenne tandis qu'une sous-martingale croit en moyenne. On note également que si $(X_n)_{n\in\mathbb{N}}$ est une martingale alors

$$\mathbb{E}(X_m|\mathscr{F}_n) = X_n, \text{ pour tout } 0 \leq n \leq m.$$

On note également que cela entraine

$$\mathbb{E}(X_m) = \mathbb{E}(X_n) = \mathbb{E}(X_0).$$

Exemple 1

1. Soit $X_1,\ldots,X_n$ une suite de v.a. i.i.d. tels que $\mathbb{E}(X_i)=0$ pour tout $i\geq 1$ alors leur somme
$$S_n = X_1+\ldots+X_n, \text{ pour tout } n\geq 1,$$
définit une martingale par rapport à la filtration $\mathscr{F}_n=\sigma(X_1,\ldots,X_n)$. En effet,
$$\mathbb{E}(S_{n+1}|\mathscr{F}_n)=\mathbb{E}(S_n+X_{n+1}|\mathscr{F}_n)=S_n+\mathbb{E}(X_{n+1})=S_n.$$

2. Soit Soit $X_1,\ldots,X_n$ une suite de v.a. positives i.i.d. tels que $\mathbb{E}(X_i)=1$ pour tout $i\geq 1$ alors leur produit
$$M_n=\prod_{i=1}^{n} X_i,\ n\geq 1,$$
définit une martingale par rapport à la filtration $\sigma(X_1,\ldots,X_n)$. En effet,
$$\mathbb{E}(M_{n+1}|\mathscr{F}_n)=\mathbb{E}(X_{n+1}M_n|\mathscr{F}_n)=M_n\mathbb{E}(X_{n+1})=M_n.$$

3. Soit ξ une v.a. tel que $\mathbb{E}(|\xi|)<\infty$, le processus $M_n=\mathbb{E}(\xi|\mathscr{F}_n)$, $n\geq 1$ qui correspond à la valeur moyenne de la variable aléatoire ξ étant donnée l'information collectée $\mathscr{F}_n$ jusqu'a l'instant $n\geq 1$, définit une martingale avec
$$\mathbb{E}(M_{n+1}|\mathscr{F}_n)=\mathbb{E}(\mathbb{E}(\xi|\mathscr{F}_{n+1})|\mathscr{F}_n)=\mathbb{E}(\xi|\mathscr{F}_n)=M_n.$$

Definition 3 (Processus prévisible)

Un processus $(H_n)_{n\in\mathbb{N}}$ est $\mathscr{F}_n$-prévisible si

$$H_n \text{ est borné et } \mathscr{F}_{n-1}\text{-mesurable.}$$

Proposition 1

Soit $(X_n)_{n\in\mathbb{N}}$ un processus adapté et $(H_n)_{n\in\mathbb{N}}$ un processus prévisible alors le processus définie par

$$(H.X)_0 = 0,\ (H.X)_n = H_1(X_1 - X_0) + \ldots + H_n(X_n - X_{n-1}),\ n \geq 1$$

est une martingale (resp. une surmartingale) si $(X_n)_{n\in\mathbb{N}}$ est une martingale (resp. sur-martingale).

preuve:
Il faut montrer que

$$\mathbb{E}[(H.X)_{n+1} - (H.X)_n | \mathscr{F}_n] = 0.$$

On note que

$$\mathbb{E}[(H.X)_{n+1} - (H.X)_n | \mathscr{F}_n] = \mathbb{E}[H_{n+1}(X_{n+1} - X_n) | \mathscr{F}_n] = 0.$$

□

Theoreme 1 (du temps d'arrêt optionnel)

Soient $(X_n)_{n\in\mathbb{N}}$ une martingale (rsp. sur-martingale) et τ un $\mathscr{F}_n$ temps d'arrêt. Le processus $(X_{n\wedge\tau})_{n\in\mathbb{N}}$ est une martingale (resp. une sur-martingale). De plus, si τ est bornée alors

$$\mathbb{E}(X_\tau) = \mathbb{E}(X_0).$$

preuve:
On remarque que le processus définie par

$$H_n = \mathbb{I}_{\tau\geq n} = 1 - \mathbb{I}_{\tau\leq n-1}$$

est prévisible et que

$$(X_{n\wedge\tau})_{n\in\mathbb{N}} = X_0 + (H.X)_n$$

est donc une martingale (si $(X_n)_{n\in\mathbb{N}}$ est une martingale). Comme τ est bornée alors il existe $N\in\mathbb{N}$ tel que $\tau\leq N$ presque surement. On en déduit que

$$\mathbb{E}(X_\tau) = \mathbb{E}(X_{\tau\wedge N}) = \mathbb{E}(X_0).$$

Theoreme 2 (De convergence des martingales)

Soit $(X_n)_{n\geq 0}$ une martingale positive alors

$$X_\infty := \lim_{n\to\infty} X_n \text{ existe presque surement.}$$

II. Le processus de branchement

Le processus de branchement permet de suivre l'évolution d'une population. Soit X une variable aléatoire de comptage telle que

$$\mathbb{P}(X=0)>0 \text{ et } \mathbb{E}(X)<\infty.$$

X correspond au nombre d'enfants d'un individu. On définit une suite (à deux indices) de variables aléatoires

$$\left(X_r^{(n)}\right)_{n,r\in\mathbb{N}}$$

indépendantes et distribuées comme X de sorte que $X_r^{(n+1)}$ désigne le nombre de descendants (membre de la génération $n+1$) de l'individu r (qui appartient à la génération n). Le processus $(Z_n)_{n\in\mathbb{N}}$ définie par

$$Z_0=1,\ Z_{n+1}=X_1^{(n+1)}+\ldots+X_{Z_n}^{(n+1)}$$

correspond à la taille de la génération $n+1$. On observe $(Z_n)_{n\in\mathbb{N}}$ définie une chaine de Markov puisque conditionnelement à $Z_n=z_n\in\mathbb{N}$, $Z_{n+1}=X_1^{(n+1)}+\ldots+X_{z_n}^{(n+1)}$ est indépendant de $Z_0,\ldots,Z_{n-1}$.

Proposition 2 (Fonction génératrice des probabilités)

La fonction génératrice des probabilités de $(Z_n)_{n\in\mathbb{N}}$ vérifie

$$G_{Z_n}(s) = \mathbb{E}\left(s^{Z_n}\right) = G_{Z_{n-1}}\left[G_X(s)\right],\ n \geq 1.$$

preuve:
On a

$$\begin{aligned}
G_{Z_n}(s) &= \mathbb{E}\left(s^{Z_n}\right) \\
&= \mathbb{E}\left(s^{X_1^{(n)}+\ldots+X_{Z_{n-1}}^{(n)}}\right) \\
&= \mathbb{E}\left\{\mathbb{E}\left(s^{X_1^{(n)}+\ldots+X_{Z_{n-1}}^{(n)}}\right)\middle| Z_{n-1}\right] \\
&= \mathbb{E}\left\{\prod_{k=1}^{Z_{n-1}}\mathbb{E}\left(s^{X_k^{(n)}}\right)\middle| Z_{n-1}\right\} \\
&= \mathbb{E}\left\{\prod_{k=1}^{Z_{n-1}} G_X(s)\right] \\
&= \mathbb{E}\left\{G_X(s)^{Z_{n-1}}\right\} = G_{Z_{n-1}}\left[G_X(s)\right]
\end{aligned}$$

On note

$$\pi_n := \mathbb{P}(Z_n = 0),\ n \geq 1,$$

la probabilité d'extinction à la génération n. On a

$$\pi_n = G_X(\pi_{n-1}),\ n \geq 1, \tag{1}$$

et la probabilité d'une éventuelle extinction

$$\pi = \mathbb{P}(Z_n = 0,\ \text{pour un}\ n \geq 1)$$

Comme $\{Z_{n-1} = 0\} \subset \{Z_n = 0\}$ alors $A_n = \{Z_n = 0\}$ est une suite croissante d'évènements alors π est la plus petite solution (car la suite π_n est croissante) de l'équation

$$\pi = G_X(\pi),\ \pi \in [0,1]. \tag{2}$$

Theoreme 3 (Probabilité d'extinction)

- *Si* $\mathbb{E}(X) > 1$ *alors* π *est l'unique solution de l'équation* (2) *entre* 0 *et 1 strictement.*
- *Si* $\mathbb{E}(X) \leq 1$ *alors* $\pi = 1$

preuve:
La fonction $\pi \mapsto G_X(\pi)$ est une fonction strictement croissante telle que

$$G_X(0) = \mathbb{P}(X = 0) > 0 \text{ et } G_X(1) = 1.$$

On note que $G'_X(1) = \mathbb{E}(X)$ ce qui donne la pente de la tangente en $\pi = 1$. On en déduit que si $\mathbb{E}(X) \leq 1$ alors la pente est plus faible que celle de la fonction $\pi \mapsto \pi$ donc la seule solution de (2) est $\pi = 1$ sinon on peut trouver $\pi \in]0,1[$ solution de (2).
□
Notons $\mu = \mathbb{E}(X)$

Proposition 3

Le processus défini par

$$M_n = Z_n/\mu^n, n \geq 0,$$

est une martingale.

preuve:
Nous avons

$$\mathbb{E}(M_{n+1}|M_n) = \mathbb{E}(Z_{n+1}/\mu^{n+1}|Z_n) = \mathbb{E}(Z_{n+1}|Z_n)/\mu^{n+1} = Z_n\mu/\mu^{n+1} = M_n.$$

□
D'après le théorème de convergence des martingales positives $\lim M_n = M_\infty$ existe.

- Si $\mu \leq 1$ alors $M_\infty = 0$ presque sûrement. Il s'agit d'une illustration du lemme de Fatou puisque

$$0 = \mathbb{E}(M_\infty) < \lim \mathbb{E}(M_n) = 1.$$

- Si $\mu > 1$, on tente d'identifier la loi de M_∞ en calculant

$$\lim E(e^{-\lambda M_n}) = E(e^{-\lambda M_\infty}), \lambda > 0.$$

En effet $M_n \to M_\infty$ implique que $\mathbb{E}(e^{-\lambda M_n}) \to \mathbb{E}(e^{-\lambda M_n})$ puis en notant que $e^{-\lambda M_n} < 1$ on applique le théorème de convergence dominée.

III. La marche aléatoire sur $\mathbb{Z}$

La marche aléatoire sur $\mathbb{Z}$ est une chaine de Markov $(X_n)_{n\in\mathbb{N}}$ dont l'espace d'état est $\mathbb{Z}$ définie par

$$X_n = X_{n-1} + \xi_n,\ n \geq 1.$$

où $\xi_1, \xi_2, \ldots,$ sont des variables aléatoires i.i.d. distribuées comme ξ avec

$$\mathbb{P}(\xi = 1) = p \text{ et } \mathbb{P}(\xi = -1) = 1 - p.$$

Theoreme 4

La marche aléatoire sur $\mathbb{Z}$ est irréductible et

- *Récurrente si $p = 1/2$.*
- *Transiente sinon.*

preuve:

Pour montrer ce résultat, on étudie la distribution du temps S_0 de retour à 0. On a

$$\mathbb{P}_0(S_0 < \infty) = \sum_{n=1}^{+\infty} \mathbb{P}_0(S_0 = n).$$

On remarque que les trajectoires allant de 0 à 0 sont nécessairement de longueur paire et

$$\mathbb{P}_0(S_0 = 2n+1) = 0,\ \text{pour } n = 0, 1, \ldots.$$

et

$$\mathbb{P}_0(S_0 < \infty) = \sum_{n=1}^{+\infty} \mathbb{P}_0(S_0 = 2n).$$

On a exactement $\binom{2n}{n}$ trajectoires possibles, celle qui nous intéresse (pour lesquels $S_0 = 2n$) sont celles qui ne repassent pas par 0 entre l'instant 0 et $2n$ (On parle d'excursions). Leur nombre est donné par

$$2 \times C_{n-1} = 2 \times \frac{1}{n} \binom{2n-2}{n-1} \tag{3}$$

Definition 4 (Nombre de Catalan)

Les nombres de Catalan sont définis par

$$C_n = \frac{1}{n+1} \binom{2n}{n}, \text{ pour } n \geq 0,$$

et vérifie

$$C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k} \text{ pour } n \geq 1 \tag{4}$$

Exemple 2 (Mots de Dyck)

C_n correspond aux nombre de mots de $2n$ lettres comprenant respectivement n A et n B, tels que lu de gauche à droite le nombre de A demeure supérieur ou égal au nombre de B. La relation de récurrence (4) s'explique par le fait qu'un mot de Dyck contenant plus de deux lettres est obtenu par la concaténation de deux mots de Dyck.

Dans le problème considéré, on s'intéresse aux nombres de mots tels que le nombre de A (interprétés comme des $+1$) soit strictement supérieur au nombre de B (interprétés comme des -1). Alors notre mot commence nécessairement par un A et fini sur un B. La portion entre ce A et ce B est un mot de Dyck contenant $2n-2$ lettres. On a C_{n-1} possibilités. Le facteur 2 dans (3) s'explique par la symétrie du problème puisque l'on peut considérer les trajectoires dans lesquels les -1 dominent les $+1$. La probabilité d'une trajectoire quelconque de longueur $2n$ contenant n "+1" et n "−1" est donnée par $p^n(1-p)^n$, on en déduit que

$$\begin{aligned}\mathbb{P}_0(S_0<\infty) &= \sum_{k=1}^{+\infty}\mathbb{P}_0(S_0=k)=\sum_{k=1}^{+\infty}2C_{n-1}[p(1-p)]^n \\ &= 2p(1-p)\sum_{k=0}^{+\infty}C_n[p(1-p)]^n=2p(1-p)C[p(1-p)], \qquad (5)\end{aligned}$$

où $C(x) = \sum_{n=0}^{+\infty} C_n x^n$. Or, on a

$$\begin{aligned} C(x) &= 1 + \sum_{n=1}^{+\infty} C_n x^n = 1 + x \sum_{n=0}^{+\infty} C_{n+1} x^n \\ &= 1 + x \sum_{n=0}^{+\infty} \sum_{k=0}^{n} C_k C_{n-k} x^n = 1 + x \sum_{k=0}^{+\infty} \sum_{n=k}^{n} C_k C_{n-k} x^n \\ &= 1 + x \sum_{k=0}^{+\infty} C_k \sum_{n=0}^{n} C_n x^{n+k} = 1 + x C(x)^2 \end{aligned}$$

Par suite, $C(x) = \frac{1-\sqrt{1-4x}}{2x}$. En substituant dans (5), on obtient

$$\mathbb{P}_0(S_0 < \infty) = 1 - |1-2p|$$

On en déduit que si $p \neq 1/2$ alors $\mathbb{P}_0(S_0 < \infty) < 1$ et la chaine est transitoire sinon $\mathbb{P}_0(S_0 < \infty) = 1$ et la chaine est récurrente.

Remarque 3 (Divergence lorsque $p \neq 1/2$)

Dans le cas d'une chaine de Markov $(X_n)_{n\in\mathbb{N}}$ sur un espace ordonné et dénombrable (comme $\mathbb{N}$ ou $\mathbb{Z}$), si la chaine est transitoire alors elle diverge vers ∞. Par exemple dans le cas de la chaine aléatoire sur $\mathbb{Z}$, on a par la loi des grands nombre

$$\frac{X_n}{n} = \frac{X_0}{n} + \frac{1}{n}\sum_{k=1}^{n} \xi_k \underset{n\to+\infty}{\longrightarrow} 2p-1.$$

On en déduit que

$$X_n \to \begin{cases} -\infty, & \text{si } p < 1/2, \\ ?(0\times\infty), & \text{si } p = 1/2, \\ +\infty, & \text{si } p > 1/2. \end{cases}$$

Dans le cas $p = 1/2$ le processus oscille. Par le théorème centrale limite, on observe que pour n très grand $Z_n \sim \mathrm{N}(z, \sqrt{n})$.

Proposition 4

Le processus défini par

$$M_n = X_n - n(2p-1),\ n \geq 0,$$

est une martingale.

preuve:
Soit $\mathscr{F}_n = \sigma(\xi_i,\ i \leq n)$ la filtration naturelle du processus $(X_n)_{n\geq 0}$. On a

$$\mathbb{E}(M_{n+1}|\mathscr{F}_n) = \mathbb{E}(X_{n+1}|\mathscr{F}_n) - (2p-1) = M_n + \mathbb{E}(\xi_{n+1} - (2p-1)|\mathscr{F}_n) - (2p-1) = M_n.$$

Exemple 3 (Le problème de la ruine du parieur)

Un joueur entre dans un casino avec x\$ en poche, il paye 1\$ pour participer,

- Il gagne et remporte 2\$ avec une probabilité p
- Il perd avec une probabilité $q = 1 - p$

sa richesse après chaque partie est modélisée par un processus $(X_n)_{n\in\mathbb{N}}$. On suppose qu'il rentre chez lui si sa richesse devient nulle ou atteint un niveau $a \geq x$. On note $\phi(x,a)$ la probabilité qu'il rentre à la maison ruiné.

Proposition 5

La probabilité de ruine est donnée par

$$\phi(x,a) = \begin{cases} \frac{(q/p)^x - (q/p)^a}{1-(q/p)^a}, & si\ p > q, \\ \frac{a-x}{a}, & si\ p = q. \end{cases}$$

preuve 1: Analyse à un pas

On note que

$$\phi(a,a) = 0 \text{ et } \phi(0,a) = 1$$

Soit $0 < x < a$, lors de la première partie,

- Il perd avec probabilité q et repart avec un niveau de richesse $x-1$,

- Il gagne avec probabilité p et repart avec un niveau de richesse $x+1$.

On en déduit que

$$\phi(x,a) = p\phi(x+1,a) + q\phi(x-1,a) \tag{6}$$

De plus, comme $p+q=1$ alors

$$\phi(x,a) = p\phi(x,a) + q\phi(x,a). \tag{7}$$

L'opération (6)-(7) donne

$$\phi(x+1,a) - \phi(x,a) = \frac{q}{p}\left[\phi(x,a) - \phi(x-1,a)\right]. \tag{8}$$

Soit

$$u_k = \phi(k+1,a) - \phi(k,a),\ \ k = 0,\ldots,a-1$$

Supposons que $p \neq q$, alors en remplaçant dans (8) cela donne

$$u_k = \left(\frac{q}{p}\right) u_{k-1} = \ldots = \left(\frac{q}{p}\right)^k u_0. \tag{9}$$

En sommant (9) pour k allant de 1 à $a-1$, on obtient

$$-\phi(1,a) = [\phi(1,a)-1]\frac{q/p-(q/p)^a}{1-q/p} \Leftrightarrow \phi(1,a) = \frac{q/p-(q/p)^a}{1-(q/p)^a} \tag{10}$$

En sommant (9) pour k allant de 1 à $x-1$, on obtient

$$\phi(x,a)-\phi(1,a)=[\phi(1,a)-1]\frac{q/p-(q/p)^x}{1-q/p} \tag{11}$$

L'insertion de (10) dans (11) donne

$$\phi(x,a)=\frac{(q/p)^x-(q/p)^a}{1-(q/p)^a}$$

Dans le cas où $p=q$, on a $u_k=u_0=[\phi(1,a)-1],\ k=1$, on applique le même raisonnement que précédemment pour trouver que

$$\phi(x,a)=\frac{a-x}{a}.$$

□

preuve 2: martingale

La richesse du parieur est donnée par une marche aléatoire $(X_n)_{n\geq 0}$, avec $X_0 = x$. Supposons que $p = q = 1/2$ alors $(X_n)_{n\geq 1}$ est une martingale. Les temps aléatoires

$$\tau_0 = \inf\{n \geq 0 \ ; \ X_n = 0\} \text{ et } \tau_a = \inf\{n \geq 0 \ ; \ X_n = a\}$$

sont des temps d'arrêt et donc $\tau = \min(\tau_0, \tau_a)$ est aussi un temps d'arrêt. On remarque que $\phi(x,a) = \mathbb{P}(\tau = \tau_0) = \mathbb{P}(X_\tau = 0)$. On applique le théorème 1, pour trouver que

$$x = \mathbb{E}(X_0) = \mathbb{E}(X_\tau) = a\mathbb{P}(X_\tau = a) \Leftrightarrow \mathbb{P}(X_\tau = 0) = \frac{a-x}{a}.$$

Supposons que $p \neq q$, on introduit une autre Martingale!

Lemme 1 (martingale de Wald)

Le processus

$$M_n = \exp\left[s(X_n - x) - n\kappa_\xi(s)\right], \ n \geq 0,$$

est une martingale pour tout $s > 0$, où $\kappa_\xi(s) = \log\left[\mathbb{E}\left(e^{s\xi}\right)\right]$ désigne la fonction génératrice des cumulants de ξ.

preuve du lemme:

Soit $\mathscr{F}_n = \sigma(\xi_i,\ i \le n)$ la filtration naturelle du processus $(X_n)_{n\in\mathbb{N}}$. On a

$$\begin{aligned}\mathbb{E}(M_{n+1}|\mathscr{F}_n) &= \mathbb{E}\{\exp[s(X_n+\xi_{n+1}-x)-n\kappa_\xi(s)]\}\\ &= \mathbb{E}[\exp(s\xi_{n+1})]\exp[s(X_n-x)-(n+1)\kappa_\xi(s)]\\ &= \exp[s(X_n-x)-n\kappa_\xi(s)]\end{aligned}$$

□

On note que l'équation $\kappa_\xi(s)=0$ est équivalente à

$$pe^s + qe^{-s} = 1$$

et a pour solution $\gamma = \log(q/p)$. Le processus $R_n = \exp[\gamma(X_n - x)],\ n \ge 0$ est une martingale d'après le lemme 1. On applique le théorème du temps d'arrêt optionel 1 au processus $(R_n)_{n\ge0}$ avec le temps d'arrêt τ, ce qui donne

$$1 = \mathbb{E}(R_0) = \mathbb{E}(R_\tau) = e^{-\gamma x}\mathbb{P}(R_\tau = 0) + e^{\gamma(a-x)}\mathbb{P}(R_\tau = 0)$$

Ce qui équivaut à

$$\phi(x,a) = \frac{e^{\gamma x} - e^{\gamma a}}{1 - e^{\gamma a}} = \frac{(q/p)^x - (q/p)^a}{1-(q/p)^a}.$$

□

Exemple 4 (Le problème de la double dépense dans les transactions validées par *blockchain*)

Marie achète un bien à Julien en l'échange de 10 BTCs.

- Julien attends que la transactions intègre un bloc, voir que plusieurs blocs soient créés avant d'expédier le bien.
- Une fois le bien reçu, Marie émet un transaction transférant les mêmes BTCs vers un porte-monnaie lui appartenant.
- Des mineurs malhonnêtes travaillent sur une chaine concurrente à la chaine de bloc principale
  - ↪ les deux chaines sont identiques à la transaction frauduleuse prêt.
- Si la chaine malhonnête rattrape la chaine principale (en termes de nombre de bloc) alors la transaction de Marie à Julien est remplacée par la transaction de Marie à elle-même.

On modélise par $(X_n)_{n\in\mathbb{N}}$ la différence entre les nombres de blocs dans la chaine honnête et malhonnêtes à l'instant n, on suppose qu'à chaque instant un bloc est créé, il rejoint

- La chaine honnête avec probabilité p,
- La chaine malhonnête avec probabilité $q = 1 - p$.

On suppose que la chaine honnêtes a x blocs d'avance. La probabilité de succès de la double dépense est donnée par

$$\phi(x) = \mathbb{P}\left(X_n = 0, \text{ pour un certain } n \in \mathbb{N} | X_0 = x\right) = \lim_{a \to +\infty} \phi(x, a) = \left(\frac{q}{p}\right)^x.$$

Pour plus de détails, on pourra lire le *white paper* de Satoshi Nakamoto [4]

Mes notes se basent sur les documents [5, 2, 1, 3, 6].


Maryann Hohn.
PSTAT160A: Applied Stochastic Processes - Lecture notes.
2017.


Nabil Kazi-Tani.
Modèles aléatoires discrets - Cours scannés ISFA.
2017.


Jean-François Le Gall.
Intégration, probabilités et processus aléatoires.
Ecole Normale Supérieure de Paris, 2006.


Satoshi Nakamoto.
Bitcoin: A peer-to-peer electronic cash system.
2008.
https://bitcoin.org/bitcoin.pdf.


Lionel Truquet.
Statistique des processus 3A - Note de cours.
http://www.ensai.fr/files/_media/documents/Enseignants%20chercheurs%20-%20doctorants/ltruquet%20-%20documents/polystatdesprocessus2.pdf.


David Williams.
Probability with martingales.
Cambridge university press, 1991.