Stochastic Models for blockchain analysis

Blockchain risk analysis

Pierre-O. Goffard

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

5 septembre 2021

Blockchain risk analysis

1. Insurance risk theory
2. Link to double spending
3. Link to blockhain mining

Cramer-Lunberg model

Insurance risk theory

The financial reserves of an insurance company over time have the following dynamic

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

where

- $u > 0$ denotes the initial reserves
- c is the premium rate
- $(N_t)_{t\geq 0}$ is a counting process that models the claim arrival
  - $\hookrightarrow$ Poisson process with intensity λ
- The U_i's are the randomly sized compensations
  - $\hookrightarrow$ non-negative, **i.i.d.**

Ruin probabilities

Define the ruin time as

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

and the ruin probabilities as

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

We look for u such that

$$\mathbb{P}(\text{Ruin}) = \alpha \;(0.05),$$

given that

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

with $\eta > 0$.

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

Wald's Martingale

Let

$$S_t = z - R_t,\ t \geq 0$$

Theorem (Wald exponential Martingale)

If $\{S_t\ ,\ t \geq 0\}$ *is a Lévy process or a random walk then*

$$\{\exp\left[\theta S_t - t\kappa(\theta)\right]\ ,\ t \geq 0\},\ \textit{is a martingale,}$$

where $\kappa(\theta) = \log \mathbb{E}\left(e^{\theta S_1}\right)$.

Proof I

Insurance risk theory

Ruin probability computation

Theorem (Representation of the ruin probability)

If

- $S_t \overset{\textbf{a.s.}}{\rightarrow} -\infty$,
- *There exists* $\gamma > 0$ *such that* $\{e^{\gamma S_t}\ ,\ t \geq 0\}$ *is a martingale*

then

$$\mathbb{P}(\tau_z < \infty) = \frac{e^{-\gamma z}}{\mathbb{E}\left[e^{\gamma\xi(z)}|\tau_z < \infty\right]},$$

where

$$\xi(z) = S_{\tau_z} - z \text{ denotes the deficit at ruin.}$$

Proof I

Insurance risk theory

Double spending in Satoshi's framework

Link to double spending

- The risk reserve process is $R_t = z + Y_1 + \ldots + Y_t$.
- The claim surplus process is $S_t = -(Y_1 + \ldots + Y_t)$.
- $\kappa(\theta) = 0$ is equivalent to

$$pe^{-\theta} + qe^{\theta} = 1.$$

$\hookrightarrow$ $\gamma = \log(p/q)$.

- If $p > q$ then $S(t) \to -\infty$.
- $\xi(z) = S_{\tau_z} - z = 0$ **a.s.**

Thus,

$$\mathbb{P}(\tau_z < \infty) = \left(\frac{q}{p}\right)^z.$$

Double spending with Poisson processes

- Suppose that
$$N_t \sim \text{Pois}(\lambda t) \text{ and } M_t \sim \text{Pois}(\mu t)$$
such that $\lambda > \mu$.
- The risk reserve process is $R_t = z + N_t - M_t$.
- The claim surplus process is $S_t = M_t - N_t$.

Fact

The difference of two Poisson processes is not a Poisson process, However it is Lévy !

Double spending with Poisson processes

- $\kappa(\theta)=0$ is equivalent to

$$\mu e^{\theta}+\lambda e^{-\theta}-(\lambda+\mu)=0.$$

$\hookrightarrow$ $\gamma=\log(\lambda/\mu)$.

- If $\lambda>\mu$ then $S(t)\to-\infty$.
- $\xi(z)=S_{\tau_z}-z=0$ a.s.

Thus

$$\mathbb{P}(\tau_z<\infty)=\left(\frac{\mu}{\lambda}\right)^z.$$

Double spending cost

Mining cryptocurrency in PoW equipped blockchain is energy consuming

$\hookrightarrow$ Operational cost for miners

Per time unit a miner pays

$$c = \pi_W \cdot W \cdot p$$

where

- π_W is the electricty price per kWh
- W is the consumption of the network `https://cbeci.org/`
- p is the miner's hashpower

The cost of double spending is $c \cdot \tau_z$

Finite horizon double spending

Link to double spending

Theorem (p.d.f. of the double spending time)

If $\{N_t\ ,\ t \geq 0\}$ is a Poisson process then the **p.d.f.** *of τ_z is given by*

$$f_{\tau_z}(t) = \mathbb{E}\left[\frac{z}{z+N(t)} f_{\Delta^S}^{*[N(t)+z]}(t)\right],\ \textit{for } t \geq 0.$$

Proof I

Link to double spending

Dual risk model

Link to blockchain mining

A blockchain miner with hashpower share $p \in (0,1)$ that

- owns $u \geq 0$ at the beginning
- spend $c = \pi_W \cdot W \cdot p$ per time unit
- finds block at a rate $p\lambda$, where λ is the arrival rate of blocks

The miner's surplus is given by

$$R_t = u - c \cdot t + N_t \cdot b, \text{ (Dual risk model)}$$

where

- $(N_t)_{t\geq 0}$ is a Poisson process with intensity $p \cdot \lambda$
- b is the block finding reward (6.25 BTC) `bitcoinhalf.com`

Expected profit given not ruin

Fact

The steady operational cost compensated by infrequent capital gains makes mining a risky business.

Define the ruin time

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

- Risk measure

$$\psi(u,t) = \mathbb{P}(\tau \geq)$$

- Profitability measure

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

Miner's dilemna

Link to blockhain mining

- Joining a mining pool
- Deviating from the protocol (selfish mining)

Link to blockhain mining

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