# Stochastic Models for Blockchain analysis

Pierre-O. Goffard

Université de Strasbourg
goffard@unistra.fr

13 avril 2024

# Agenda

1. Security of PoW blockchains
   - Double spending attack
   - Insurance risk theory
   - Double spending in Satoshi's framework
   - Double spending with Poisson processes
2. Decentralization in PoS blockchain
3. Blockchain efficiency

# Agenda

**Security of PoW blockchains**

1. Security of PoW blockchains
   - Double spending attack
   - Insurance risk theory
   - Double spending in Satoshi's framework
   - Double spending with Poisson processes
2. Decentralization in PoS blockchain
3. Blockchain efficiency

# Double spending attack



I. Security of PoW blockchains
I.1 Double spending attack

1. Mary transfers 10 BTCs to John
2. The transaction is recorded in the public branch of the blockchain and John ships the good.
3. Mary transfers to herself the exact same BTCs
4. The malicious transaction is recorded into a private branch of the blockchain
   - Mary has friends among the miners to help her out
   - The two chains are copycat up to the one transaction

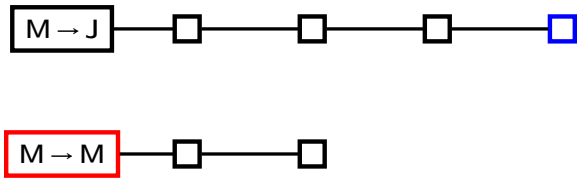
**Fact (Bitcoin has only one rule)**

The longest chain is to be trusted

# Double Spending attack



Vendor are advised to wait for $\alpha \in \mathbb{N}$ of confirmations so that the honest chain is ahead of the dishonest one.




In the example, vendor awaits $\alpha = 4$ confirmations, the honest chain is ahead of the dishonest one by $z = 2$ blocks.

**Fact (PoW is resistant to double spending)**

- Attacker does not own the majority of computing power
- Suitable $\alpha$

Double spending is unlikely to succeed.

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

# Double Spending Attack



Assume that

- $R_0 = z \geq 1$ (the honest chain is z blocks ahead)
- at each time unit a block is created
  - ↪ in the honest chain with probability $p$
  - ↪ in the dishonest chain with probability $q = 1 - p$

The process $(R_n)_{n \geq 0}$ is a random walk on $\mathbb{Z}$ with

$$R_n = z + Y_1 + \ldots + Y_n,$$

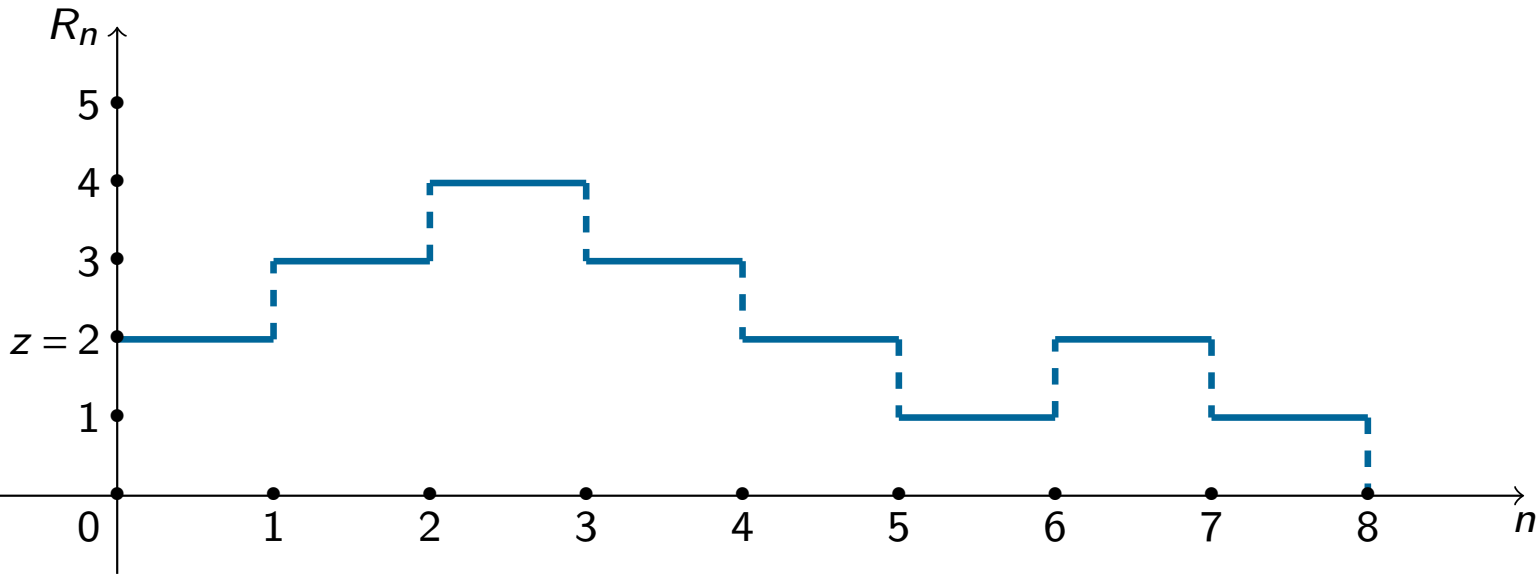
where $Y_1, \ldots, Y_n$ are the **i.i.d.** steps of the random walk.

# Double Spending Attack



Double spending occurs at time

$$\tau_z = \inf\{n \in \mathbb{N}\,;\ R_n = 0\}.$$




Goal : Find

$$\psi(z) = \mathbb{P}(\tau_z < \infty)$$

# Insurance risk theory



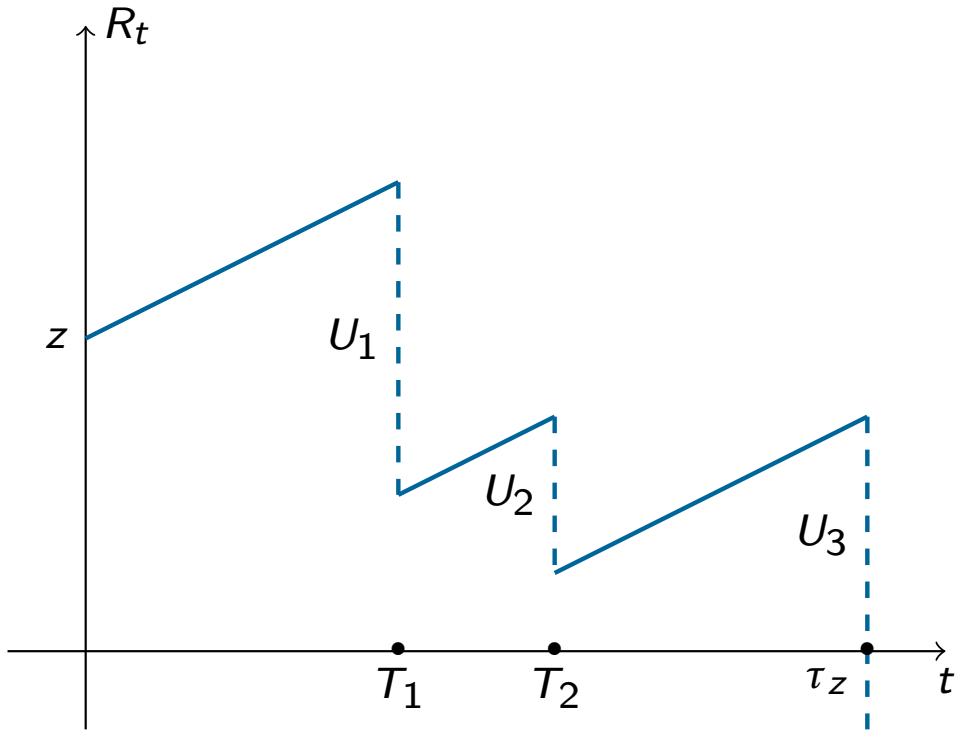
## I.2 Insurance risk theory

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

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

where

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



# Insurance risk theory



Define the ruin time as

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

and the ruin probabilities as

$$\psi(z,t) = \mathbb{P}(\tau_z < t) \text{ and } \psi(z) = \mathbb{P}(\tau_z < \infty)$$

We look for $z$ such that

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

given that

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

with

$$\eta > 0 \text{ (net profit condition)}$$

otherwise

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

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

# Insurance risk theory



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

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

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

**Theorem (Representation of the ruin probability)**

If $S_t \overset{\text{a.s.}}{\to} -\infty$, and 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 $\xi(z) = S_{\tau_z} - z$ denotes the deficit at ruin.

# Sketch of Proof



- Because of the net profit condition $S_t = \sum_{i=1}^{N_t} U_i - ct \to -\infty$ as $t \to \infty$
- $(S_t)_{t \geq 0}$ is a Lévy process, let $\gamma$ be the (unique, positive) solution to

$$\kappa(\theta) = 0 \text{ (Cramer-Lundberg equation).}$$

- $(e^{\gamma S_t})_{t \geq 0}$ is a Martingale then apply the Optional stopping theorem at $\tau_z$.

# Double spending in Satoshi's framework



## I.3 Double spending in Satoshi's framework

**Double spending theorem**

If $p > q$ then the double-spending probability is given by

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

- 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



## I.4. Double spending with Poisson processes

Let the length of honest and dishonest chain be driven by counting processes

- Honest chain $\Rightarrow z + N_t$ , $t \geq 0$, where $z \geq 1$.
- Malicious chain $\Rightarrow M_t$ , $t \geq 0$
- Study the distribution of the first-*rendez-vous* time

$$\tau_z = \inf\{t \geq 0 \ , \ M_t = z + N_t\}.$$


P.-O. Goffard, "Fraud risk assessment within blockchain transactions," *Advances in Applied Probability*, vol. 51, pp. 443–467, jun 2019.
`https://hal.archives-ouvertes.fr/hal-01716687v2`.

R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Modeling and analysis of block arrival times in the bitcoin blockchain," *Stochastic Models*, vol. 36, pp. 602–637, jul 2020.

# Double spending with Poisson processes



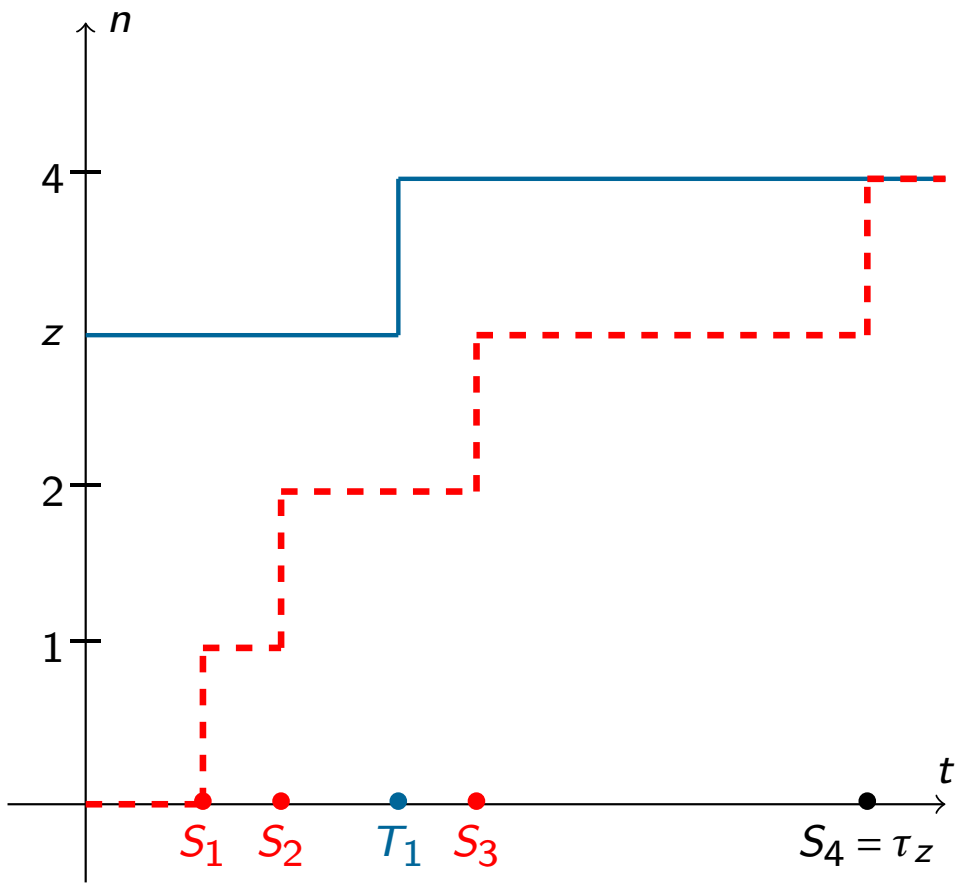
- Suppose that

$$N_t \sim \text{Pois}(\lambda t) \text{ and } M_t \sim \text{Pois}(\mu t)$$

  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



**Double spending theorem**

If $\lambda > \mu$ then the double-spending probability is given by

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

- $\kappa(\theta) = 0$ 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

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

P.-O. Goffard, "Fraud risk assessment within blockchain transactions," *Advances in Applied Probability*, vol. 51, pp. 443–467, jun 2019.
`https://hal.archives-ouvertes.fr/hal-01716687v2`.

# Agenda

**Decentralization in PoS blockchain**

1. Security of PoW blockchains
   - Double spending attack
   - Insurance risk theory
   - Double spending in Satoshi's framework
   - Double spending with Poisson processes
2. Decentralization in PoS blockchain
3. Blockchain efficiency

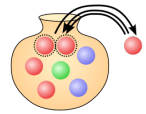
# Risk of centralization ?



II. Decentralization in PoS blockchains
II.1 Average stake owned by each peers

PoS algorithm

- Draw a coin at random
- The owner of the coin append a block and collect the reward
- The block appender is more likely to get selected during the next round

Similar to Polya's urn 

- Consider an urn of $N$ balls of color in $E = \{1, \ldots, p\}$
- Draw a ball of color $x \in E$
- Replace the ball together with $r$ balls of color $x$

$p$ is the number of peers and $r$ is the size of the block reward.

**Theorem**

The proportion of coins owned by each peer is stable on average over the long run

I. Roșu and F. Saleh, "Evolution of shares in a proof-of-stake cryptocurrency," *Management Science*, vol. 67, pp. 661–672, feb 2021.

# Mathematical framework

**Decentralization in PoS blockchain**

Let's consider a network $E = \{1, \dots, p\}$ of size $p$ and $r$ be the block reward. At time $n = 0$

- Peer $x$ has $Z_0^{(x)}$ coins
- The total number of coins is given by

$$Z_0 = \sum_{x \in E} Z_0^{(x)}$$

The number of coins owned by each peer evolves over time as

$$Z_n^{(x)} = Z_0^{(x)} + r \sum_{k=1}^{n} \mathbb{I}_{A_k^{(x)}},$$

where

$$A_n^{(x)} = \text{ A coin of peer } x \in E \text{ is drawn during round } n \geq 1.$$

The total number of coins is given by

$$Z_n = Z_0 + nr.$$

Let $(W_n^{(x)})_{n \geq 0}$ be the proportion of coins owned by $x \in E$, we have

$$W_n^{(x)} = \frac{Z_n^{(x)}}{Z_n}$$

and $\mathscr{F}_n = \sigma(\{Z_k^{(x)}, x \in E, k \leq n\})$. Note that $\mathbb{P}(A_n^{(x)} | \mathscr{F}_{n-1}) = W_{n-1}^{(x)}$.

# Proof



**Theorem**

$$\mathbb{E}\left(W_n^{(x)}\right) = \frac{Z_0^{(x)}}{Z_0},\ x \in E\ , n \geq 0.$$

We show that $(W_n^{(x)})_{n\geq 0}$ is a martingale. We have that

$$\begin{aligned}
\mathbb{E}\left[W_n^{(x)} | \mathscr{F}_{n-1}\right] &= \mathbb{E}\left[\frac{Z_{n-1}^{(x)} + r\mathbb{I}_{A_n^{(x)}}}{Z_0 + rn}\middle| \mathscr{F}_{n-1}\right] \\
&= \frac{Z_{n-1}^{(x)}}{Z_0 + rn} + \frac{rW_{n-1}^{(x)}}{Z_0 + rn} \\
&= \frac{W_{n-1}^{(x)}[Z_0 + r(n-1)]}{Z_0 + rn} + \frac{rW_{n-1}^{(x)}}{Z_0 + rn} \\
&= W_{n-1}^{(x)}.
\end{aligned}$$

It then follows that $\mathbb{E}\left(W_n^{(x)}\right) = W_0^{(x)} = \frac{Z_0^{(x)}}{Z_0},\ x \in E\ , n \geq 0$. The long term average of the stake of each peer is stable

# What is the limiting distributions of the shares ?



II.2 Asymptotic distribution of stakes owned by each peers

**Theorem (Convergence toward a Dirichlet distribution)**

Suppose that $r = 1$, we have that

$$\left(W_\infty^{(1)}, \ldots, W_\infty^{(p)}\right) \sim \mathrm{Dir}\left(Z_0^{(1)}, \ldots, Z_0^{(p)}\right).$$

**Fact**

The most desirable situation corresponds to all the peers being equally likely to be selected.

Decentrality maybe measure by Shannon's entropy

$$H(\mu^*) = -\mathbb{E}\left\{\sum_x \mu^*(x) \ln[\mu^*(x)]\right\} = -\sum_x \frac{N}{N_x}\left[\psi(N_x+1) - \psi(N+1)\right],$$

where $\psi(x) = \frac{\mathrm{d}}{\mathrm{d}x}\ln[\Gamma(x)]$ is the digamma function, to be compared to $\ln(p)$.

# Extensions and perspectives

**Decentralization in PoS blockchain**

- How to include more peers along the way ?
- What if the peers are not simply buy and hold investors ?
- Find ways to monitor decentralization and take action if necessary

I. Roșu and F. Saleh, "Evolution of shares in a proof-of-stake cryptocurrency," *Management Science*, vol. 67, pp. 661–672, feb 2021.

# Agenda

**Blockchain efficiency**

1. Security of PoW blockchains
   - Double spending attack
   - Insurance risk theory
   - Double spending in Satoshi's framework
   - Double spending with Poisson processes
2. Decentralization in PoS blockchain
3. Blockchain efficiency

# Efficiency

**Blockchain efficiency**

III. Efficiency of PoW blockchains

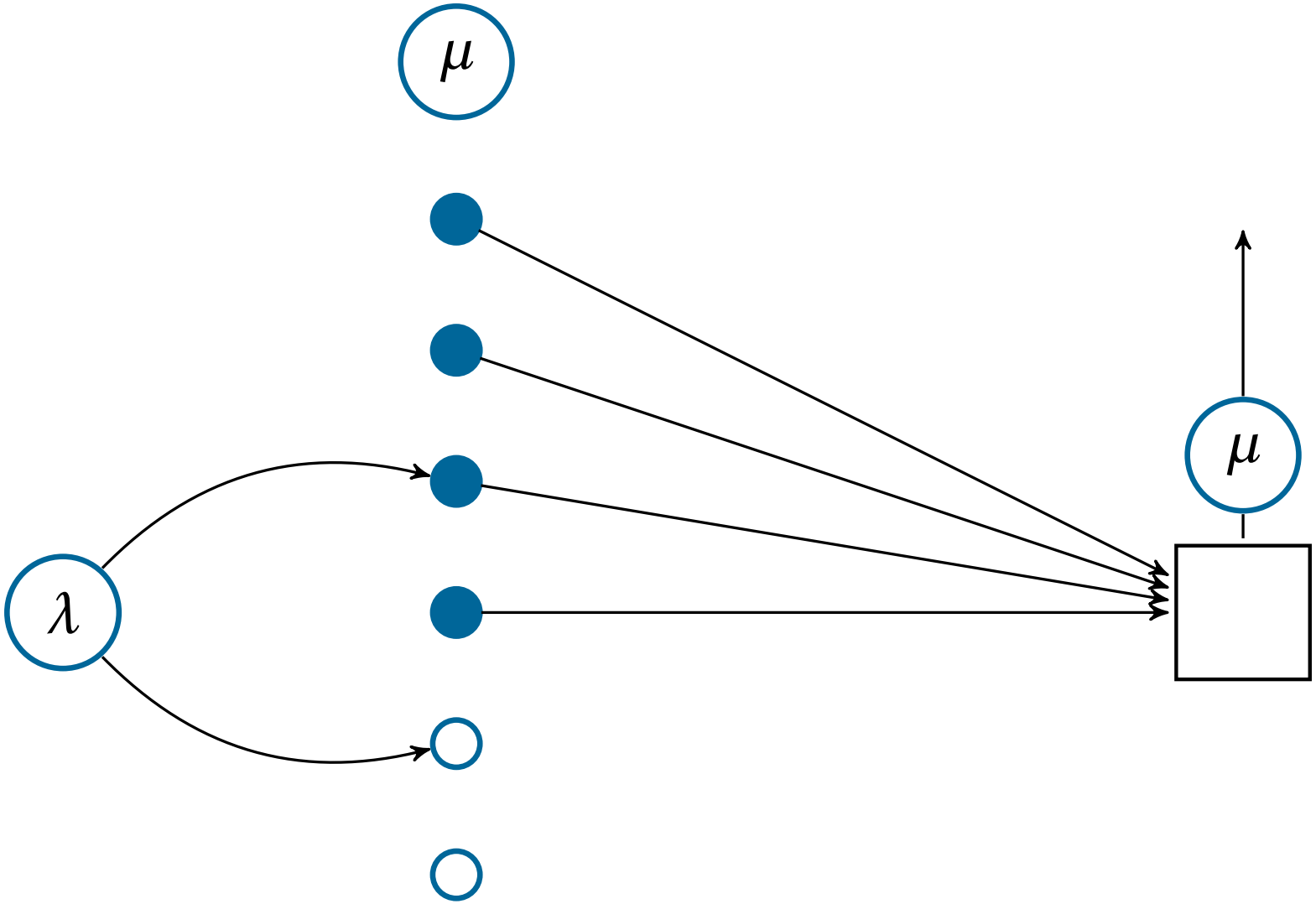
Efficiency is characterized by

- Throughputs : Number of transaction being processed per time unit
- Latency : Average transaction confirmation time

# Efficiency

**Blockchain efficiency**

## III.1 A queueing model with bulk service



# Queueing setting

**Blockchain efficiency**

- Poisson arrival with rate $\lambda > 0$ for the transactions
- Poisson arrival with rate $\mu > 0$ for the blocks
- Block size $b \in \mathbb{N}^* \Rightarrow$Batch service

⚠ The server is always busy

This is somekind of $M/M^b/1$ queue.


Y. Kawase and S. Kasahara, "Transaction-confirmation time for bitcoin : A queueing analytical approach to blockchain mechanism," in *Queueing Theory and Network Applications*, pp. 75–88, Springer International Publishing, 2017.

N. T. J. Bailey, "On queueing processes with bulk service," *Journal of the Royal Statistical Society : Series B (Methodological)*, vol. 16, pp. 80–87, jan 1954.

D. R. Cox, "The analysis of non-markovian stochastic processes by the inclusion of supplementary variables," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 51, pp. 433–441, jul 1955.

# Queue length distribution

**Blockchain efficiency**

The queueuing process eventually reaches stationarity if

$$\mu \cdot b > \lambda. \tag{1}$$

We denote by $N^q$ the length of the queue upon stationarity.

**The blockchain efficiency theorem**

Assume that (1) holds then $N^q$ is geometrically distributed

$$\mathbb{P}(N^q = n) = (1-p) \cdot p^n,$$

where $p = 1/z^*$ and $z^*$ is the only root of

$$-\frac{\lambda}{\mu} z^{b+1} + z^b \left( \frac{\lambda}{\mu} + 1 \right) - 1,$$

such that $|z^*| > 1$.

# Latency and throughputs



## III.2 Throughputs and latency computation

### Little's law

Consider a stationary queueing system and denote by

- $1/\lambda$ the mean of the unit inter-arrival times
- $L$ be the mean number of units in the system
- $W$ be the mean time spent by units in the system

We have

$$L = \lambda \cdot W$$

J. D. C. Little, "A proof for the queuing formula :L= $\lambda$W," *Operations Research*, vol. 9, pp. 383–387, jun 1961.

- Latency is the confirmation time of a transaction

$$\text{Latency} = W + \frac{1}{\mu} = \frac{\mathbb{E}(N^q)}{\lambda} + \frac{1}{\mu} = \frac{p}{(1-p)\lambda} + \frac{1}{\mu}.$$

- Throughput is the number of transaction confirmed per time unit

$$\text{Throughput} = \mu\mathbb{E}(N^q \mathbb{I}_{N^q \leq b} + b\mathbb{I}_{N^q > b}) = \mu \sum_{n=0}^{b} n(1-p)p^n + bp^{b+1}.$$

# Perspective

**Blockchain efficiency**

1. Include some priority consideration to account for the transaction fees


Y. Kawase, , and S. Kasahara, "Priority queueing analysis of transaction-confirmation time for bitcoin," *Journal of Industrial & Management Optimization*, vol. 16, no. 3, pp. 1077–1098, 2020.


2. Go beyond the Poisson process framework


Q.-L. Li, J.-Y. Ma, and Y.-X. Chang, "Blockchain queue theory," in *Computational Data and Social Networks*, pp. 25–40, Springer International Publishing, 2018.

Q.-L. Li, J.-Y. Ma, Y.-X. Chang, F.-Q. Ma, and H.-B. Yu, "Markov processes in blockchain systems," *Computational Social Networks*, vol. 6, jul 2019.

# Refinements of the double spending problem

Let the length of honest and dishonest chain be driven by counting processes

- Honest chain $\Rightarrow z + N_t$ , $t \geq 0$, where $z \geq 1$.
- Malicious chain $\Rightarrow M_t$ , $t \geq 0$
- Study the distribution of the first-*rendez-vous* time

$$\tau_z = \inf\{t \geq 0 \ , \ M_t = z + N_t\}.$$

If $N_t \sim \text{Pois}(\lambda t)$ and $M_t \sim \text{Pois}(\mu t)$ such that $\lambda > \mu$ then

$$\psi(z) = \left(\frac{\mu}{\lambda}\right)^z, \ z \geq 0.$$


P.-O. Goffard, "Fraud risk assessment within blockchain transactions," *Advances in Applied Probability*, vol. 51, pp. 443–467, jun 2019.
https://hal.archives-ouvertes.fr/hal-01716687v2.

R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Modeling and analysis of block arrival times in the bitcoin blockchain," *Stochastic Models*, vol. 36, pp. 602–637, jul 2020.

# Dirichlet distribution

## Dirichlet distribution

A random vector $(Z_1,\ldots,Z_p)$ has a Dirichlet distribution $\mathrm{Dir}(\alpha_1,\ldots,\alpha_p)$ with **pdf**

$$f(z_1,\ldots,z_p;\alpha_1,\ldots,\alpha_p) = \frac{1}{B(\alpha)}\prod_{i=1}^{p} z_i^{\alpha_i-1},$$

for $\alpha_1,\ldots,\alpha_p > 0$, $0 < z_1,\ldots,z_p < 1$ and $\sum_{i=1}^{p} z_i = 1$, where

$$B(\alpha) = \frac{\prod_{i=1}^{p}\Gamma(\alpha_i)}{\Gamma(\sum_{i=1}^{p}\alpha_i)}.$$

# Proof I

We have that

$$\mathbb{P}(X_1 = x) = \frac{N_x}{N} \tag{2}$$

and

$$\mathbb{P}(X_{n+1} = x) = \frac{N_x + \sum_{i=1}^{n} \delta_{X_i}(x)}{N+n} = \frac{N_x + \lambda_n(x)}{N+n} = m_n(x) \tag{3}$$

where $\delta_{X_i}$ denotes the Dirac measure at $X_i$.
A sequence that satisfies (2) and (3) is said to be a Polya sequence with parameter $N_x$, $x \in E$.

## Lemma

*There is an equivalence between the two following statements*

(i) $X_1, X_2, \ldots$, *is a Polya sequence*

(ii) $\mu^* \sim Dir(N_x, x \in E)$ *and* $X_1, X_2, \ldots$ *given* $\mu^*$ *are* ***iid*** *as* $\mu^*$

Consider the event $A_n = \{X_1 = x_1, \ldots, X_n = x_n\}$. Induction on $n$ allows us to show that (i) is equivalent to

$$\mathbb{P}(A_n) = \frac{\prod_{x \in E} N_x^{[\lambda_n(x)]}}{N^{[n]}}, \tag{4}$$

# Proof II

where $\lambda_n(x)$ is the number of $i$'s in $1,\ldots,n$ for which $x_i = x$ and $a^{[k]} = a(a+1)\ldots(a+k-1)$. Now assume that $(ii)$ holds true, then

$$\mathbb{P}(A_n|\mu^*) = \prod_{x\in E} \mu^*(x)^{\lambda_n(x)},$$

recall that $\mu^*$ is a random vector, indexed on $E$, We denote by $\mu^*(x)$ the component associated with $x \in E$. The law of total probability then yields

$$\mathbb{P}(A_n) = \mathbb{E}\left[\prod_{x\in E} \mu^*(x)^{\lambda_n(x)}\right], \tag{5}$$

which is the same as (4). Applying the lemma together with the law of large number yields

$$n^{-1}\sum_{i=1}^{n} \delta_{X_i}(x) \to \mu^*(x) \text{ as } n \to \infty.$$

and then $m_n(x) \to \mu^*(x)$.

D. Blackwell and J. B. MacQueen, "Ferguson distributions via polya urn schemes," *The Annals of Statistics*, vol. 1, mar 1973.

# Proof of the efficiency theorem I

Let $N_t^q$ be the number of transactions in the queue at time $t \geq 0$ and $X_t$ the time elapsed since the last block was found. Further define

$$P_n(x,t)\mathrm{d}x = \mathbb{P}[N_t^q = n, X_t \in (x, x+\mathrm{d}x)]$$

If $\lambda < \mu \cdot b$ holds then the process admits a limiting distribution given by

$$\lim_{t\to\infty} P_n(x,t) = P_n(x).$$

We aim at finding the distribution of the queue length upon stationarity

$$\mathbb{P}(N^q = n) := \alpha_n = \int_0^\infty P_n(x)\mathrm{d}x. \tag{6}$$

Consider the possible transitions over a small time lapse h during which no block is being generated. Over this time interval, either

- no transactions arrives
- one transaction arrives

# Proof of the efficiency theorem II

We have for $n \geq 1$

$$P_n(x+h) = e^{-\mu h}\left[e^{-\lambda h}P_n(x) + \lambda h e^{-\lambda h}P_{n-1}(x)\right]$$

Differentiating with respect to $h$ and letting $h \to 0$ leads to

$$P_n'(x) = -(\lambda+\mu)P_n(x) + \lambda P_{n-1}(x), \ n \geq 1. \tag{7}$$

Similarly for $n = 0$, we have

$$P_0'(x) = -(\lambda+\mu)P_0(x). \tag{8}$$

We denote by

$$\xi(x)\mathrm{d}x = \mathbb{P}(x \leq X < x+\mathrm{d}x | X \geq x) = \mu \mathrm{d}x$$

the hazard function of the block arrival time (constant as it is exponentially distributed). The system of differential equations (7), (8) admits boundary conditions at $x = 0$ with

$$\begin{cases} P_n(0) = \int_0^{+\infty} P_{n+b}(x)\xi(x)\mathrm{d}x = \mu\alpha_{n+b}, & n \geq 1, \\ P_0(0) = \mu\sum_{n=0}^{b}\alpha_n, & n = 0,\ldots,b \end{cases} \tag{9}$$

# Proof of the efficiency theorem III

Define the probability generating function of $N^q$ at some elapsed service time $x \geq 0$ as

$$G(z;x) = \sum_{n=0}^{\infty} P_n(x) z^n.$$

By differentiating with respect to $x$, we get (using (7) and (8))

$$\frac{\partial}{\partial x} G(z;x) = -[\lambda(1-z)+\mu]\, G(z;x)$$

and therefore

$$G(z;x) = G(z;0) \exp\{-[\lambda(1-z)+\mu]\, x\}$$

We get the probability generating function of $N^q$ by integrating over $x$ as

$$G(z) = \frac{G(z;0)}{\lambda(1-z)+\mu} \tag{10}$$

# Proof of the efficiency theorem IV

Using the boundary conditions (9), we write

$$\begin{aligned} G(z;0) &= \sum_{n=0}^{\infty} P_n(0) z^n \\ &= P_0(0) + \sum_{n=1}^{+\infty} P_n(0) z^n \\ &= \mu \sum_{n=0}^{b} \alpha_n + \mu \sum_{n=1}^{+\infty} \alpha_{n+b} z^n \\ &= \mu \sum_{n=0}^{b} \alpha_n + \mu z^{-b} \left[ G(z) - \sum_{n=0}^{b} \alpha_n z^n \right] \end{aligned} \tag{11}$$

Replacing the left hand side of (11) by (10), multiplying on both side by $z^b$ and rearranging yields

$$\frac{G(z)}{M(z)} [z^b - M(z)] = \sum_{n=0}^{b-1} \alpha_n (z^b - z^n), \tag{12}$$

where $M(z) = \mu/(\lambda(1-z)+\mu)$. Using Rouche's theorem, we find that both side of the equation shares $b$ zeros inside the circle $\mathscr{C} = \{z \in \mathbb{C}\,;\, |z| < 1+\epsilon\}$ for some epsilon.

# Proof of the efficiency theorem V

**Rouche's theorem**

Let $\mathscr{C} \in \mathbb{C}$ and $f$ and $g$ two holomorphic functions on $\mathscr{C}$. Let $\partial\mathscr{C}$ be the contour of $\partial\mathscr{C}$. If

$$|f(z) - g(z)| < |g(z)|, \ \forall z \in \partial\mathscr{C}$$

then $Z_f - P_f = Z_g - P_g$, where $Z_f$, $P_f$, $Z_g$, and $P_g$ are the number of zeros and poles of $f$ and $g$ respectively.

We have $\partial\mathscr{C} = \{z \in \mathbb{C} \, ; \, |z| = 1 + \epsilon\}$. The left hand side can be rewritten as

$$G(z)\left[-\frac{\lambda}{\mu}z^{b+1} + \left(1 + \frac{\lambda}{\mu}\right)z^b - 1\right].$$

Define $f(z) = -\frac{\lambda}{\mu}z^{b+1} + \left(1 + \frac{\lambda}{\mu}\right)z^b - 1$ and $g(z) = \left(1 + \frac{\lambda}{\mu}\right)z^b$. We have

$$|f(z) - g(z)| = |-\frac{\lambda}{\mu}z^{b+1} - 1| < \frac{\lambda}{\mu}(1+\epsilon)^{b+1} + 1 \to \frac{\lambda}{\mu} + 1, \text{ as } \epsilon \to 0.$$

# Proof of the efficiency theorem VI

and

$$|g(z)| = \left(1+\frac{\lambda}{\mu}\right)(1+\epsilon)^b \to \frac{\lambda}{\mu}+1, \text{ as } \epsilon \to 0.$$

Regarding the right hand side, define $f(z) = \sum_{n=0}^{b-1} \alpha_n (z^b - z^n)$ and $g(z) = \sum_{n=0}^{b-1} \alpha_n z^b$. We have

$$|f(z)-g(z)| < |\sum_{n=0}^{b-1} \alpha_n z^n| < \sum_{n=0}^{b-1} \alpha_n (1+\epsilon)^n \to \sum_{n=0}^{b-1} \alpha_n, \text{ as } \epsilon \to 0.$$

and

$$|g(z)| = (1+\epsilon)^b \sum_{n=0}^{b-1} \alpha_n \to \sum_{n=0}^{b-1} \alpha_n, \text{ as } \epsilon \to 0.$$

One of them is 1, and we denote by $z_k$, $k = 1, \ldots, b-1$ the remaining $b-1$ zeros. Given the polynomial form of the right hand side of (12), the fundamental theorem of algebra indicates that the number of zero is $b$. Given the left hand side

$$G(z)\left[-\frac{\lambda}{\mu}z^{b+1} + \left(1+\frac{\lambda}{\mu}\right)z^b - 1\right].$$

# Proof of the efficiency theorem VII

we deduce that there is one zeros outside $\mathscr{C}$, we can further show that it is a real number $z^*$. Multiplying both side of (12) by $(z-1)\prod_{k=1}^{b-1}(z-z_k)$, and using $G(1)=1$ yields

$$G(z)=\frac{1-z^*}{z-z^*}.$$

$N^q$ is then a geometric random variable with parameter $p=\frac{1}{z^*}$.