

Stochastic Models for blockchain analysis

Simple models for blockchain performance analysis

Pierre-O. Goffard

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

8 août 2021



The three dimensions of blockchain analysis

- 1 Security of PoW blockchain
- 2 Decentralization in PoS blockchain
- 3 Blockchain efficiency

Double spending attack

Security of PoW blockchain

- 1 Mary transfers 10 BTCs to John
- 2 The honest transaction is recorded in the honest chain and John ships the good.
- 3 Mary transfers to herself the exact same BTCs
- 4 The malicious transaction is recorded into a hidden, dark, secret chain
 - Mary has friends among the miners to help her out
 - The two chains are copycat up to the one transaction

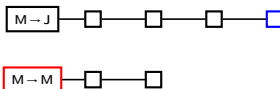
Fact (Bitcoin has only one rule)

The longest chain is to be trusted

Double spending in practice

Security of PoW blockchain

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 α*

Double spending is unlikely to succeed.



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

Mathematical set up

Security of PoW blockchain

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

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

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

Double spending rate of success

Security of PoW blockchain

Double spending occurs at time

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

Theorem (Double spending theorem)

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

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

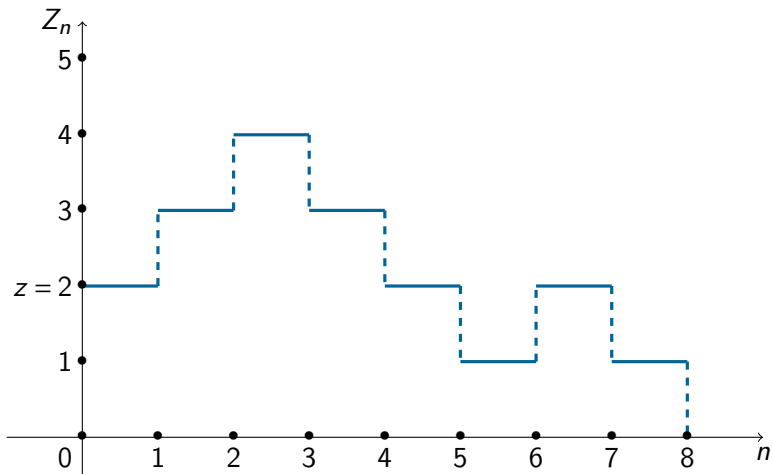


Figure – A trajectory of the process $(Z_n)_{n \geq 0}$. Gambler's ruin problem

Proof of the double spending theorem I

Security of PoW blockchain

Analogy with the gambler's ruin problem. Using a first step analysis, we have

$$\phi(z) = p\phi(z+1) + (1-p)p\phi(z-1), \quad z \geq 1. \quad (1)$$

We also have the boundary conditions

$$\phi(0) = 1 \text{ and } \lim_{z \rightarrow +\infty} \phi(z) = 0 \quad (2)$$

Equation (1) is a linear difference equation of order 2 associated to the following characteristic equation

$$px^2 - x + 1 - p = 0$$

which has two roots on the real line with

$$r_1 = 1, \text{ and } r_2 = \frac{1-p}{p}.$$

The solution of (1) is given by

$$\phi(z) = A + B \left(\frac{1-p}{p} \right)^z,$$

Proof of the double spending theorem II

Security of PoW blockchain

where A and B are constant. Using the boundary conditions (2), we deduce that

$$\phi(z) = \left(\frac{1-p}{p} \right)^z$$

as announced.

Refinements of the double spending problem

Security of PoW blockchain

The number of blocks M found by the attacker until the honest miners find α blocks is a negative binomial random variable with **pmf**

$$\mathbb{P}(M = m) = \binom{\alpha + m - 1}{m} p^\alpha q^m, \quad m \geq 0.$$

The number of block that the honest chain is ahead of the dishonest one is given by

$$Z = (\alpha - M)_+.$$

Applying the law of total probability yields the probability of successful double spending with

$$\mathbb{P}(\text{Double Spending}) = \mathbb{P}(M \geq \alpha) + \sum_{m=0}^{\alpha-1} \binom{\alpha + m - 1}{m} q^\alpha p^m.$$



M. Rosenfeld, "Analysis of hashrate-based double spending," *arXiv preprint arXiv :1402.2009*, 2014.

Refinements of the double spending problem

Security of PoW blockchain

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

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



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.

Proof of Stake protocol

Decentralization in PoS blockchain

PoS is the most popular alternative to PoW.

- A block validator is selected according to the number of native coins she owns
- Update the blockchain and receive a reward or do nothing

Two problems

- ⚠ Nothing at stake \Rightarrow Consensus postponed
- ⚠ Rich gets richer \Rightarrow Risk of centralization

Nothing-at-Stake

Decentralization in PoS blockchain

If given the opportunity a node will always append a new block

- Everlasting fork if any

Perpetuating disagreement prevent users to exchange which lower the coin value.

Theorem (Saleh 2020)

To get consensus faster and almost surely

- *Set a minimum stake to outweigh the benefit of the reward*
- *Set up a modest reward schedule $\sum_{t=1}^{\infty} \text{Reward}_t < \infty$*



F. Saleh, "Blockchain without waste : Proof-of-stake," *The Review of Financial Studies*, vol. 34, pp. 1156–1190, jul 2020.

Risk of centralization ?

Decentralization in PoS blockchain

Efficiency

Blockchain efficiency

Efficiency is characterized by

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

We focus on a PoW equipped blockchain and study the above quantities using a queueing model.

Queueing model settings

Blockchain efficiency

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

This is a $M/M^b/1$ queue [2] [3]



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 queueing process eventually reaches stationarity if

$$\mu \cdot b > \lambda. \quad (3)$$

We denote by N the length of the queue upon stationarity.

Theorem (The blockchain efficiency theorem)

Assume that (3) holds then N is geometrically distributed

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

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 $|z^| > 1$.*

Proof of the efficiency theorem I

Blockchain efficiency

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

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

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

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

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

$$\mathbb{P}(N^q = n) := \alpha_n = \int_0^\infty P_n(x) dx. \quad (4)$$

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

Blockchain efficiency

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 $h \rightarrow 0$ leads to

$$P'_n(x) = -(\lambda + \mu)P_n(x) + \lambda P_{n-1}(x), \quad n \geq 1. \quad (5)$$

Similarly for $n = 0$, we have

$$P'_0(x) = -(\lambda + \mu)P_0(x). \quad (6)$$

We denote by $\xi(x) = \mu$ the hazard function of the block arrival time (constant as it is exponentially distributed). The system of differential equations (5), (6) admits boundary conditions at $x = 0$ with

$$\begin{cases} P_n(0) = \int_0^{+\infty} P_{n+b}(x) \xi(x) dx = \mu \sum_{m=0}^b \alpha_{n+b}, & n \geq 1, \\ P_0(0) = \mu \sum_{n=0}^b \alpha_n, & n = 0, \dots, b \end{cases} \quad (7)$$

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

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

Proof of the efficiency theorem III

Blockchain efficiency

By differentiating with respect to x , we get (using (5) and (6))

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

and therefore

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

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

$$G(z) = \frac{G(z; 0)}{\lambda(1-z) + \mu} \tag{8}$$

Proof of the efficiency theorem IV

Blockchain efficiency

Using the boundary conditions (7), we write

$$\begin{aligned} G(z; 0) &= \mu \sum_{n=0}^{\infty} P_n(0) z^n \\ &= P_0(0) + \sum_{n=1}^{+\infty} P_n(0) z^n \\ &= \mu \sum_{n=0}^b \alpha_n + \mu \sum_{n=1}^{+\infty} \alpha_{n+b} z^n \\ &= \mu \sum_{n=0}^b \alpha_n + \mu z^{-b} \left[G(z) - \sum_{n=0}^b \alpha_n z^n \right] \end{aligned} \tag{9}$$

Replacing the left hand side of (9) by (8), multiplying on both side by z^b and rearranging yields

$$\frac{G(z)}{M(z)} [z^b - M(z)] = \sum_{n=0}^{b-1} \alpha_n (z^b - z^n), \tag{10}$$

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

Proof of the efficiency theorem V

Blockchain efficiency

denote by z_k , $k=1,\dots,b-1$ the remaining $b-1$ zeros. Given the polynomial form of the right hand side of (10), the fundamental theorem of algebra indicates that the number of zeros is b . The left hand side can be rewritten as

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

we deduce that there is one zeros outside \mathcal{C} , we can further show that it is a real number z^* . Multiplying both side of (10) 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 is then a geometric random variable with parameter $p = \frac{1}{z^*}$.

Latency and throughputs




Blockchain efficiency

- Latency is the confirmation time of a transaction
 - From Little's law it follows that the mean confirmation time is given by

$$\text{Latency} = \frac{p}{(1-p)\lambda} + \frac{1}{\mu}$$

- Throughput is the number of transaction confirmed per time unit

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

-  F. Saleh, “Blockchain without waste : Proof-of-stake,” *The Review of Financial Studies*, vol. 34, pp. 1156–1190, jul 2020.
-  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.