Stochastic Models for blockchain analysis

Blockchain risk analysis

Pierre-O. Goffard

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

13 avril 2022

Blockchain risk analysis

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

Cramer-Lunberg model

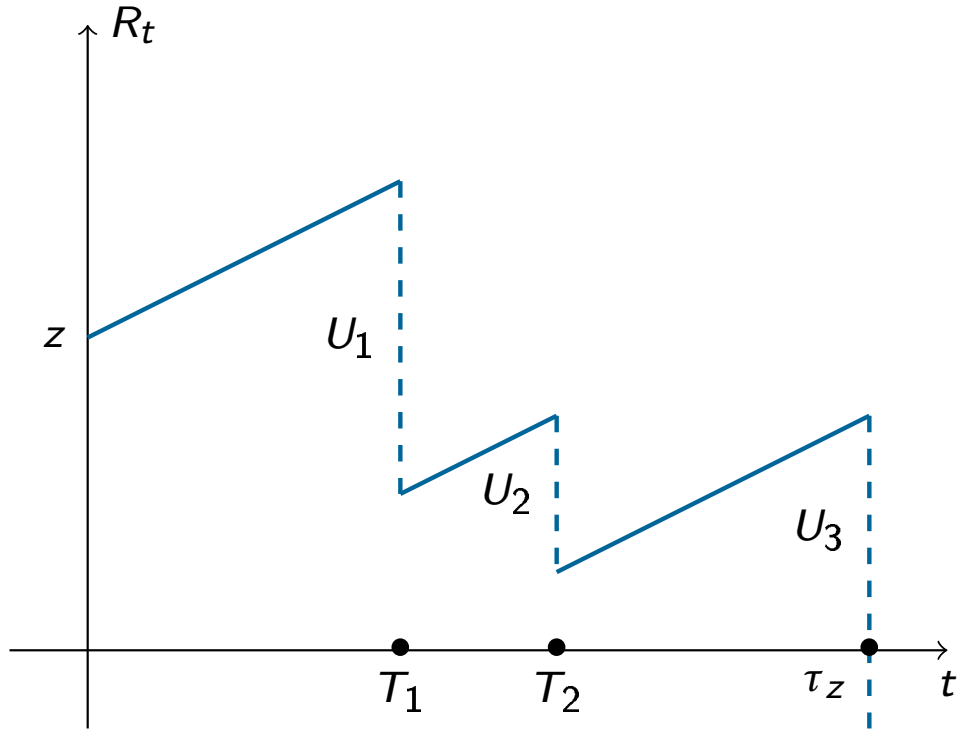
Insurance risk theory

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 λ
- The U_i's are the randomly sized compensations
  - ↪ non-negative, **i.i.d.**



Ruin probabilities

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.

Ruin probability computation

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 γ 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 τ_z.

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

Link to double spending

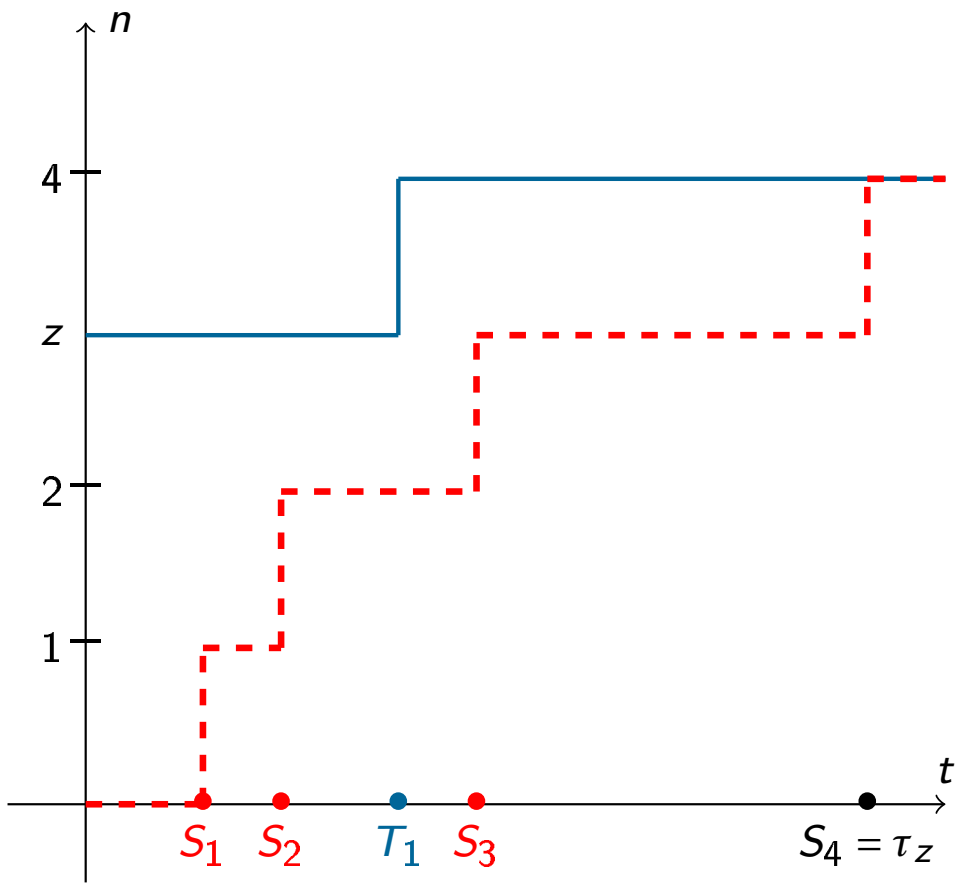
- Suppose that

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

  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

Link to double spending

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

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

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

- 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

Link to double spending

Mining cryptocurrency in PoW equipped blockchain is energy consuming

↪ Operational cost for miners

Per time unit a miner pays

$$c = \pi_W \cdot W \cdot q,$$

where

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

Fact

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

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

$$f_{\tau_z}(t) = \mathbb{E}\left[\frac{z}{z+N_t} f_{S_{N_t+z}}(t)\right],\ \text{for}\ t \geq 0.$$

Sketch of the proof

Link to double spending

Let's condition upon the values of N_t,

- if $N_t = 0$ then

$$\tau_z = S_z \text{ and } f_{\tau_z | N_t = 0}(t) = f_{S_z}(t)$$

- If $N_t = n$ for $n \geq 1$ then

$$\{\tau_z = t\} = \bigcup_{k=1}^{n} \{T_k \leq S_{z+k-1}\} \cup \{S_{n+z} = t\}$$

We have

$$\begin{aligned} f_{\tau_z | N_t = n}(t) &= \mathbb{P}(U_{1:n} \leq S_z/t, \ldots, U_{n:n} \leq S_{z+n-1}/t \,\big|\, S_{n+z} = t) f_{S_{n+z}}(t) \\ &= \frac{z}{z+n} f_{S_{n+z}}(t). \end{aligned}$$

Thanks to the properties of the Abel-Gontcharov polynomials.

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.

C. Grunspan and R. Pérez-Marco, "ON PROFITABILITY OF NAKAMOTO DOUBLE SPEND," *Probability in the Engineering and Informational Sciences*, pp. 1–15, feb 2021.

M. Brown, E. Peköz, and S. Ross, "BLOCKCHAIN DOUBLE-SPEND ATTACK DURATION," *Probability in the Engineering and Informational Sciences*, pp. 1–9, may 2020.

J. Jang and H.-N. Lee, "Profitable double-spending attacks," *Applied Sciences*, vol. 10, p. 8477, nov 2020.

Dual risk model

Link to blockchain mining

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

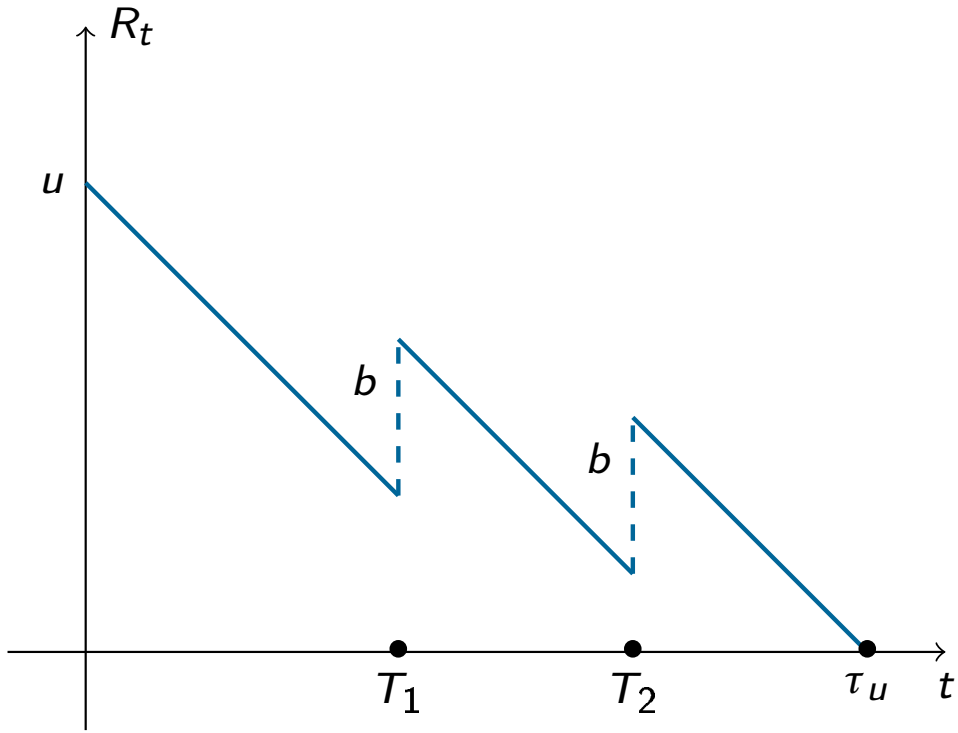
- owns $u \geq 0$ at the beginning
- spend $c = \pi_W \cdot W \cdot p$ per time unit
- finds block at a rate $p\lambda$, where λ is the arrival rate of blocks

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

Link to blockchain mining

Fact

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

Define the ruin time

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

- Risk measure

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

- Profitability measure

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

Miner's dilemna

Link to blockchain mining

Use ψ and V to compare solo mining to

- Joining a mining 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.

- Deviating from the protocol (selfish mining)

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`.

Tractable formulas follow from

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

where $T \sim \text{Exp}(t)$.

When mining solo

Link to blockchain mining

Theorem (profit and ruin when mining solo)

For any $u \geq 0$, we have

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

and

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

where ρ^* is the negative solution of the equation

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

Lambert function

The solution ρ^* of (1) is given by

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

where $W(.)$ denotes the Lambert function.

Sketch of the proof I

Link to blockchain mining

Recall that the time horizon is random $T \sim \text{Exp}(t)$, we condition upon what happen during the time interval $(0,h)$, with $h < u/c$ so that ruin does not occur before h. Three possibilities

(i) $T > h$ and there is no block discovery during $(0,h)$

(ii) $T < h$ and there is no block discovery during $(0,T)$

(iii) There is a block discovery before time T and in the interval $(0,h)$

For the expected profit $\widehat{V}(u,t)$, we get

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

Sketch of the proof

Link to blockchain mining

Now we take the derivative with respect to h and set $h=0$ to obtain

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

Equation (2) is an advanced functional differential equation with boundary condition

$$\widehat{V}(0,t)=0 \text{ and such that } 0\leq\widehat{V}(u,t)\leq u-ct+p\lambda bt \text{ for } u>0.$$

Consider solutions of the form

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

where A,B,C and ρ are constants to be determined. Substituting (3) in (2) together with the boundary condition yields the system of equations

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

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

Sketch of the proof

Link to blockchain mining

We then have $A = -t(p\lambda b - c)$, $B = 1$, $C = t(p\lambda b - c)$ and ρ is solution of

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

which admits one negative and one positive solution. As $A < 0$, we have to choose the negative solution $\rho^* < 0$ in order to ensure $\widehat{V}(u,t) > 0$. Substituting A, B, C and ρ^* in (3) yields the result. Similarly, the ruin probability is solution to

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

with initial condition $\widehat{\psi}(0,t) = 1$ and boundary condition $\lim_{u\to\infty}\widehat{\psi}(u,t) = 0$.

How does a mining pool works ?

Link to blockchain mining

A set of miners $I \subset \{1,\dots,n\}$ join forces and gather a share

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

of the total mining power.

- a pool manager coordinates
- miners prove their contribution by submiting *shares*

Definition (share)

A *share* is a partial solution to the cryptopuzzle

The pool manager sets

- the redistribution system
- the relative difficulty $q \in (0,1)$ of finding a *share* compared to finding a block
- the pool participation fee f

Redistribution systems

Link to blockchain mining

Miners should be retributed in proportion to their contribution to the mining effort.

Proportional reward system

A *round* is the time elapsed between two block discoveries

- s_i the number of shares submitted by miner $i \in I$ during the *round*
- Each miner receives at the end of the *round*

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

where f represents the pool manager's cut.

- The system is fair as $\frac{s_i}{\sum_{i\in I} s_i}$ should converges toward $\frac{p_i}{\sum_{i\in I} p_i}$

What's wrong with going proportional ?

Link to blockchain mining

Fact

The proportional reward system is fair but it is not incentive compatible

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.

Why ?

- The durations of a round is random
  - ↪ A *share* is worth less in longer round ⇒ *pool hoping*
    - M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011.
  - ↪ Apply a discounting factor on the value of a *share*
    - slush pool, "Reward system specifications," 2021.
- A miner may postpone the communication of a solution
  - ↪ She may awaits for her number of *share* to match her actual hashpower
- Absolutely no risk tranfer from miners to manager
  - ↪ f should be low

Pay-per-Share (PPS) reward system

Link to blockchain mining

The pool manager gives out

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

for each submitted share and keep the block reward.

Miner's viewpoint

$$R_t^i = u_i - ct + M_t^i w,\ t \geq 0.$$

where

- $(M_t^i)_{t\geq 0}$ is a Poisson process with intensity $p_i\mu = p_i\lambda/q$
- μ corresponds to the rate at which the network find *shares*

Manager's viewpoint

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

where

- $(M_t^I)_{t\geq 0}$ is a Poisson process with intensity $p_I\mu = p_I\lambda/q$
- $(N_t^I)_{t\geq 0}$ is a Poisson process with intensity $p_I\lambda$

Pool manager at risk ?

Link to blockchain mining

For mathematical convenience we replace the deterministic reward by stochastic ones, the wealth of the pool manager becomes

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

where

- $(M_t)_{t\geq 0}$ and $(N_t)_{t\geq 0}$ are Poisson processes with intensity $\mu^* = \mu - \lambda$ and λ
- $(W_i)_{i\geq 0}$ and $(B_j)_{j\geq 0}$ are two independent sequence of **iid** exponentially distributed random variables with mean w and $b^* = b - w$

Poisson process superposition

A block discovery triggers automatically a payment to the miner, specifying

- the intensity of M_t as $\mu^* = \mu - \lambda$
- the size of the upward jumps as $b^* = b - w$

allows us to isolate the downward jumps and make the Poisson processes independent.

Pool manager at risk ?

Link to blockchain mining

Theorem (Profit and ruin of the pool manager)

The ruin probability is given by

$$\widehat{\psi}(u,t) = (1 - Rw)e^{-Ru},\ u \geq 0,$$

and the expected profit is given by

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

where R is the (unique) solution with positive real part of

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

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

Sketch of the Proof I

Link to blockchain mining

We condition upon what happen during the time interval $(0,h)$. Four possibilities

(i) $T > h$ and no jump during $(0,h)$
(ii) $T < h$ and no jump over $(0,T)$
(iii) An upward jump in the interval $(0,h)$
(iv) A downward jump in the interval $(0,h)$

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

Differentiating with respect to h and letting $h \to 0$ yields the following integral equation

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

with boundary conditions $\widehat{V}(u,t) = 0$ for all $u < 0$ and $0 \leq \widehat{V}(u,t) \leq u + (\lambda b^* - \mu^* w)t$. Let us plug in the ansatz

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

Sketch of the Proof II

Link to blockchain mining

- Comparing the terms in e^{-ru} gives and equation for r

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

  of which only the positive solution $R>0$ is valid due to the boundary conditions.
- Comparing the terms in u yields $d_1=1$
- Comparing the terms in 1 yields

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

- Comparing the terms in $e^{-u/w}$

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

Problem caused by mining

Link to blockchain mining

- *R&D* arm race, consuming a lot of energy and generating large amounts of e-waste

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.

- A threat on centralization ?

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.

Blockwithholding strategies

Link to blockchain mining

Why ?

- Relative revenue greater than their fair share
- Honest miners waste resources
  - ↪ Honest miner might quit making malicious miners more powerful
- Slow down the pace of block arrivals
  - ↪ Downward adjustment of the cryptopuzzle difficulty

Difficulty adjustments

The cryptopuzzle difficulty is adjusted every 2,016 blocks to ensure 1 block every ten minutes on average.

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.

Blockwithholding strategies

Link to blockchain mining

Why ?

- Relative revenue greater than their fair share
- Honest miners waste resources
  - ↪ Honest miner might quit making malicious miners more powerful
- Slow down the pace of block arrivals
  - ↪ Downward adjustment of the cryptopuzzle difficulty

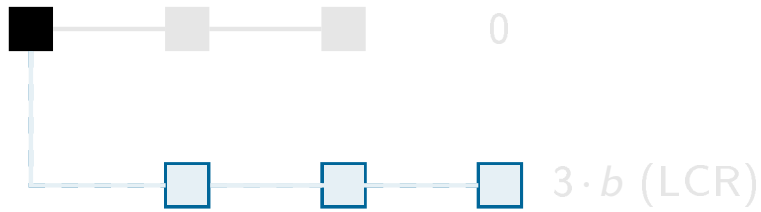
Difficulty adjustments

The cryptopuzzle difficulty is adjusted every 2,016 blocks to ensure 1 block every ten minutes on average.

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.

Blockwithholding strategies

Link to blockchain mining



Why ?

- Relative revenue greater than their fair share
- Honest miners waste resources
  - ↪ Honest miner might quit making malicious miners more powerful
- Slow down the pace of block arrivals
  - ↪ Downward adjustment of the cryptopuzzle difficulty

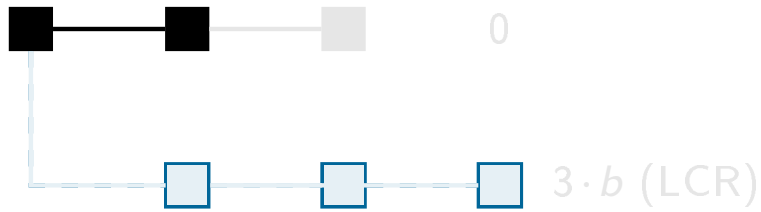
Difficulty adjustments

The cryptopuzzle difficulty is adjusted every 2,016 blocks to ensure 1 block every ten minutes on average.

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.

Blockwithholding strategies

Link to blockchain mining



Why ?

- Relative revenue greater than their fair share
- Honest miners waste resources
  - ↪ Honest miner might quit making malicious miners more powerful
- Slow down the pace of block arrivals
  - ↪ Downward adjustment of the cryptopuzzle difficulty

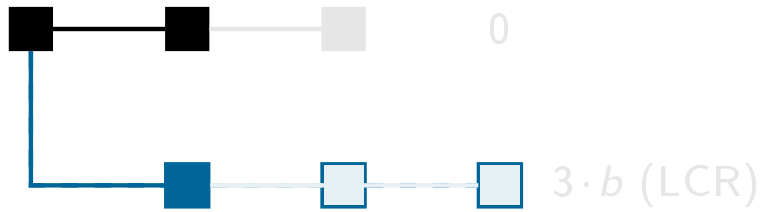
Difficulty adjustments

The cryptopuzzle difficulty is adjusted every 2,016 blocks to ensure 1 block every ten minutes on average.

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.

Blockwithholding strategies

Link to blockchain mining



Why ?

- Relative revenue greater than their fair share
- Honest miners waste resources
  - ↪ Honest miner might quit making malicious miners more powerful
- Slow down the pace of block arrivals
  - ↪ Downward adjustment of the cryptopuzzle difficulty

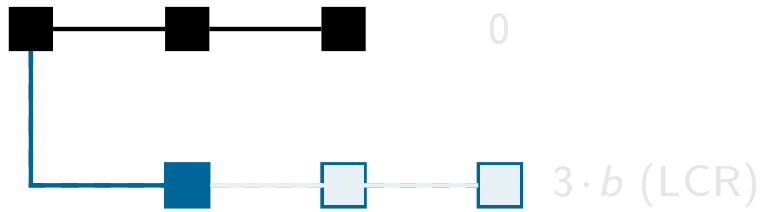
Difficulty adjustments

The cryptopuzzle difficulty is adjusted every 2,016 blocks to ensure 1 block every ten minutes on average.

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.

Blockwithholding strategies

Link to blockchain mining



Why ?

- Relative revenue greater than their fair share
- Honest miners waste resources
  - ↪ Honest miner might quit making malicious miners more powerful
- Slow down the pace of block arrivals
  - ↪ Downward adjustment of the cryptopuzzle difficulty

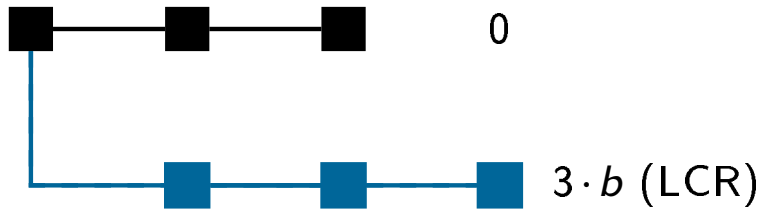
Difficulty adjustments

The cryptopuzzle difficulty is adjusted every 2,016 blocks to ensure 1 block every ten minutes on average.

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.

Blockwithholding strategies

Link to blockchain mining



Why ?

- Relative revenue greater than their fair share
- Honest miners waste resources
  - ↪ Honest miner might quit making malicious miners more powerful
- Slow down the pace of block arrivals
  - ↪ Downward adjustment of the cryptopuzzle difficulty

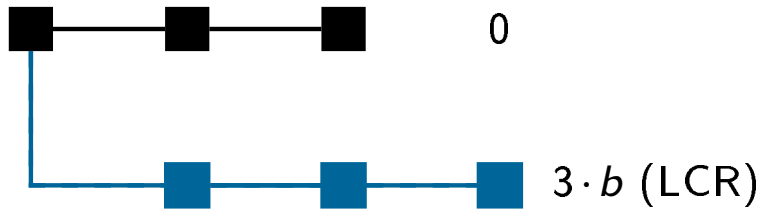
Difficulty adjustments

The cryptopuzzle difficulty is adjusted every 2,016 blocks to ensure 1 block every ten minutes on average.

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.

Blockwithholding strategies

Link to blockchain mining



Why ?

- Relative revenue greater than their fair share
- Honest miners waste resources
  - ↪ Honest miner might quit making malicious miners more powerful
- Slow down the pace of block arrivals
  - ↪ Downward adjustment of the cryptopuzzle difficulty

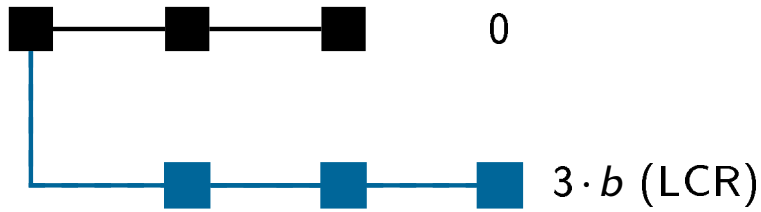
Difficulty adjustments

The cryptopuzzle difficulty is adjusted every 2,016 blocks to ensure 1 block every ten minutes on average.

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.

Blockwithholding strategies

Link to blockchain mining



Why ?

- Relative revenue greater than their fair share
- Honest miners waste resources
  - ↪ Honest miner might quit making malicious miners more powerful
- Slow down the pace of block arrivals
  - ↪ Downward adjustment of the cryptopuzzle difficulty

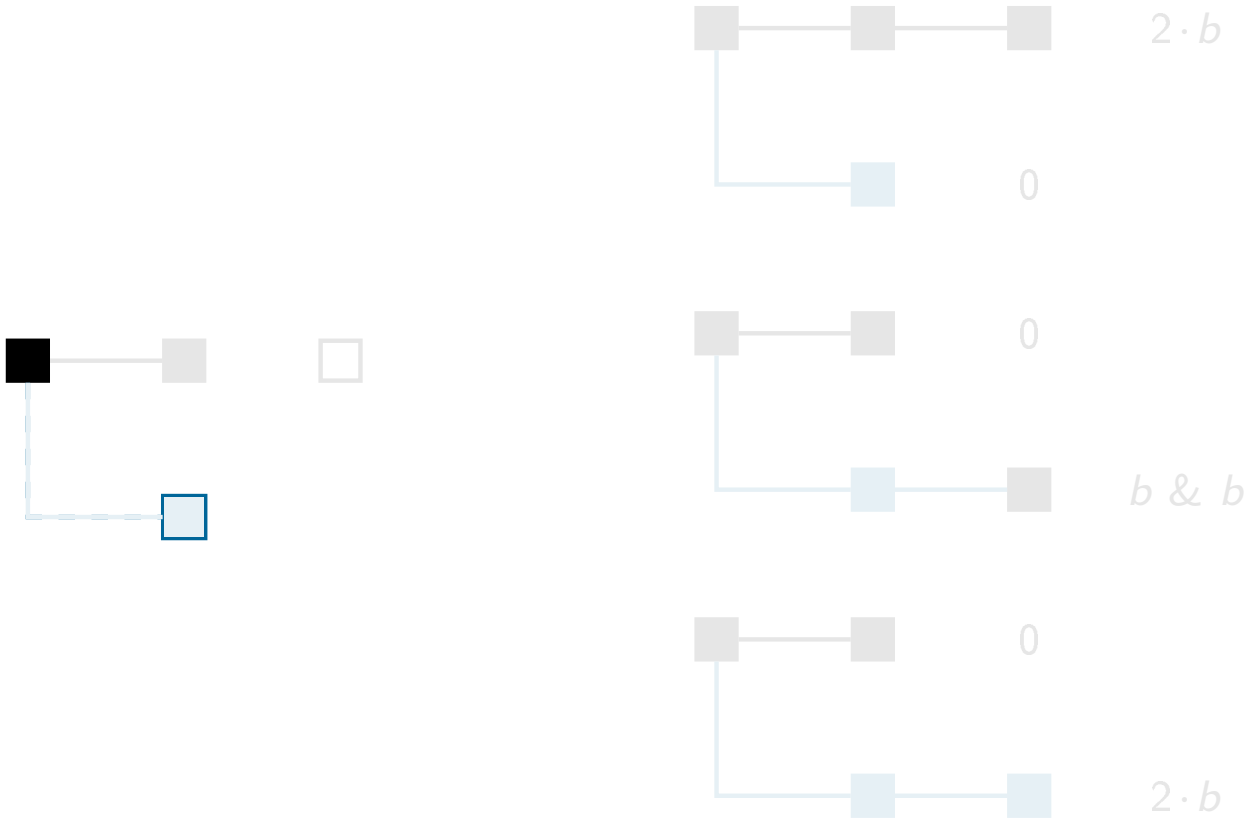
Difficulty adjustments

The cryptopuzzle difficulty is adjusted every 2,016 blocks to ensure 1 block every ten minutes on average.

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.

Tied selfish mining

Link to blockchain mining

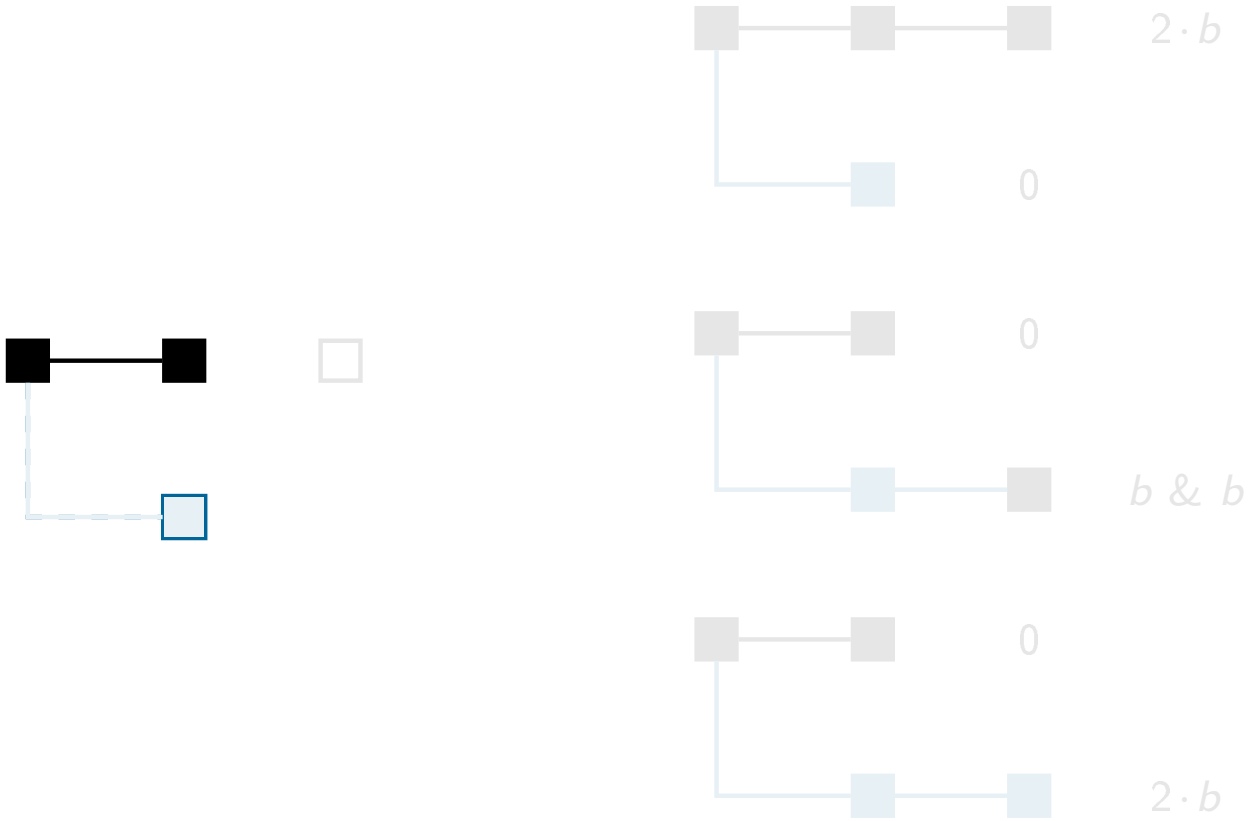


Fact

The outcome of the fork when the honest miners find the subsequent block depends on the connectivity parameter $q \in (0,1)$ of the malicious nodes.

Tied selfish mining

Link to blockchain mining

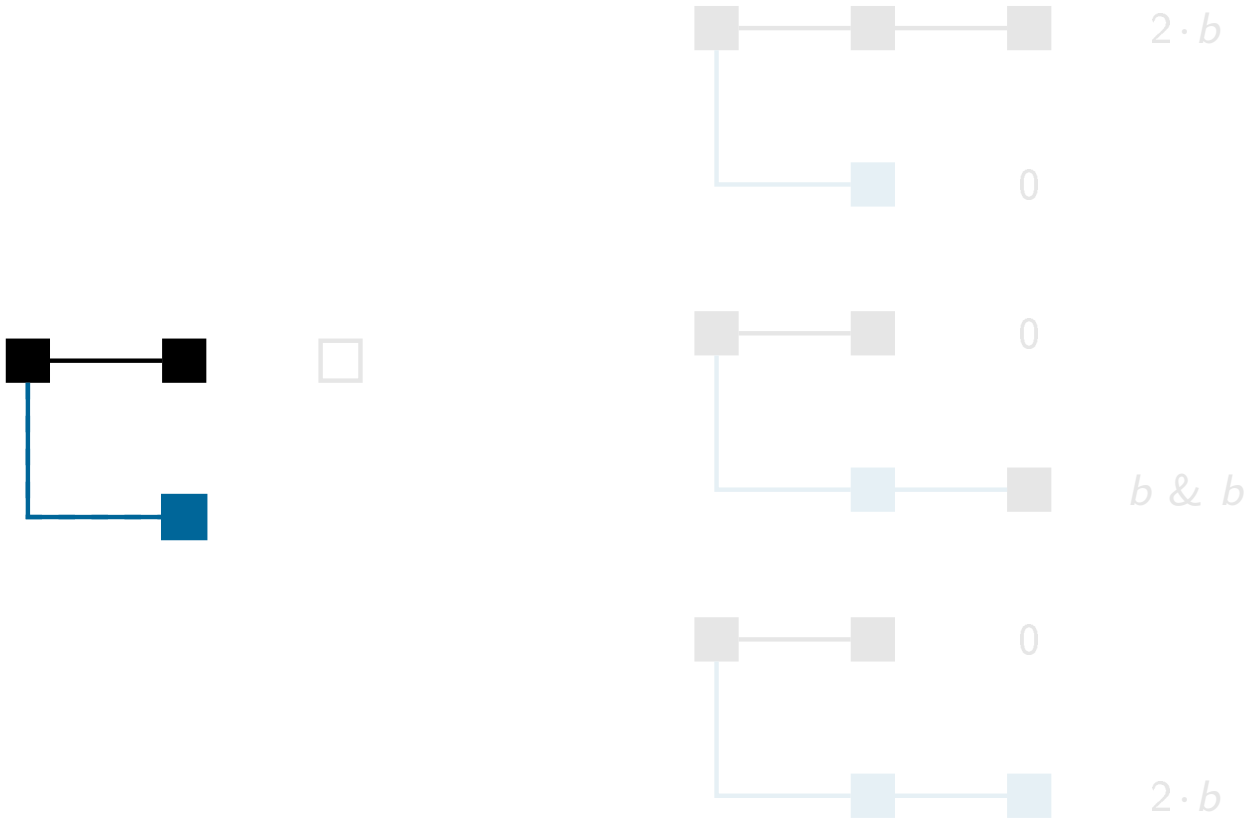


Fact

The outcome of the fork when the honest miners find the subsequent block depends on the connectivity parameter $q \in (0,1)$ of the malicious nodes.

Tied selfish mining

Link to blockchain mining

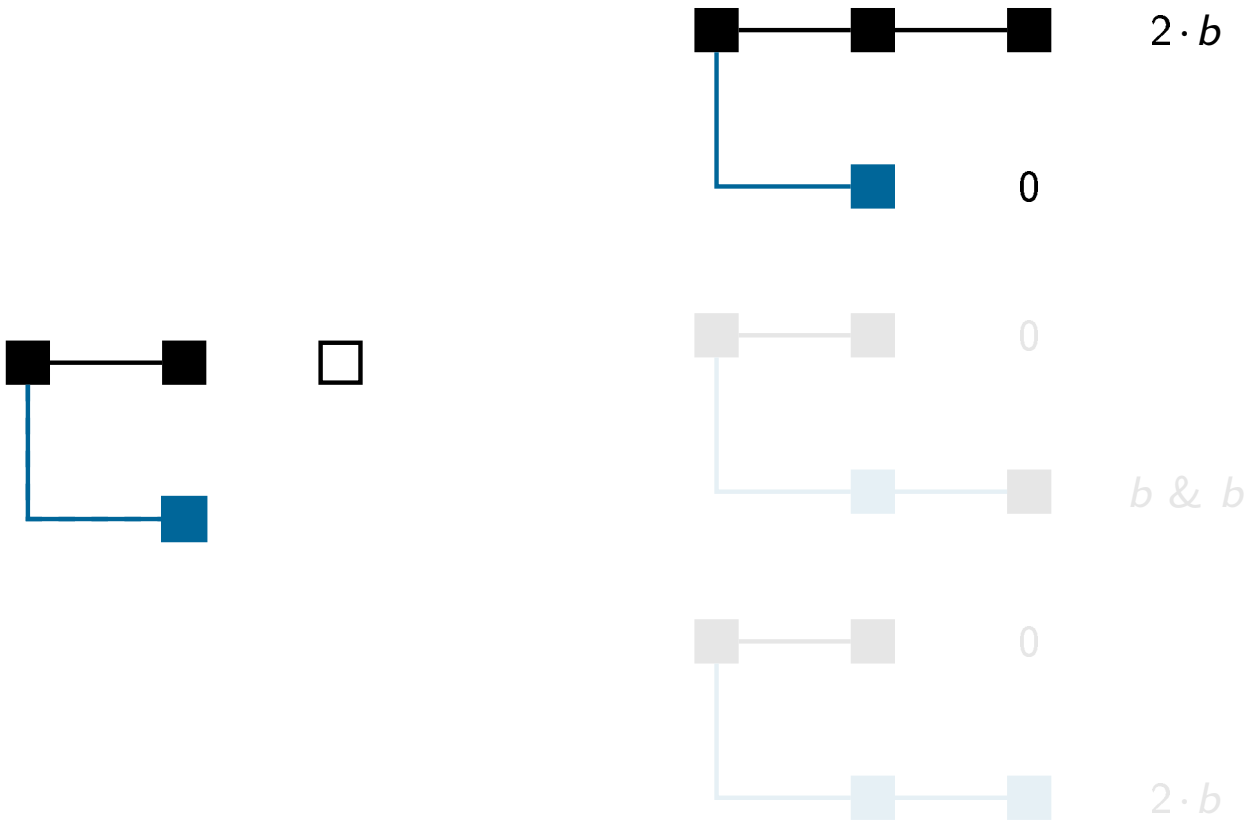


Fact

The outcome of the fork when the honest miners find the subsequent block depends on the connectivity parameter $q \in (0,1)$ of the malicious nodes.

Tied selfish mining

Link to blockchain mining

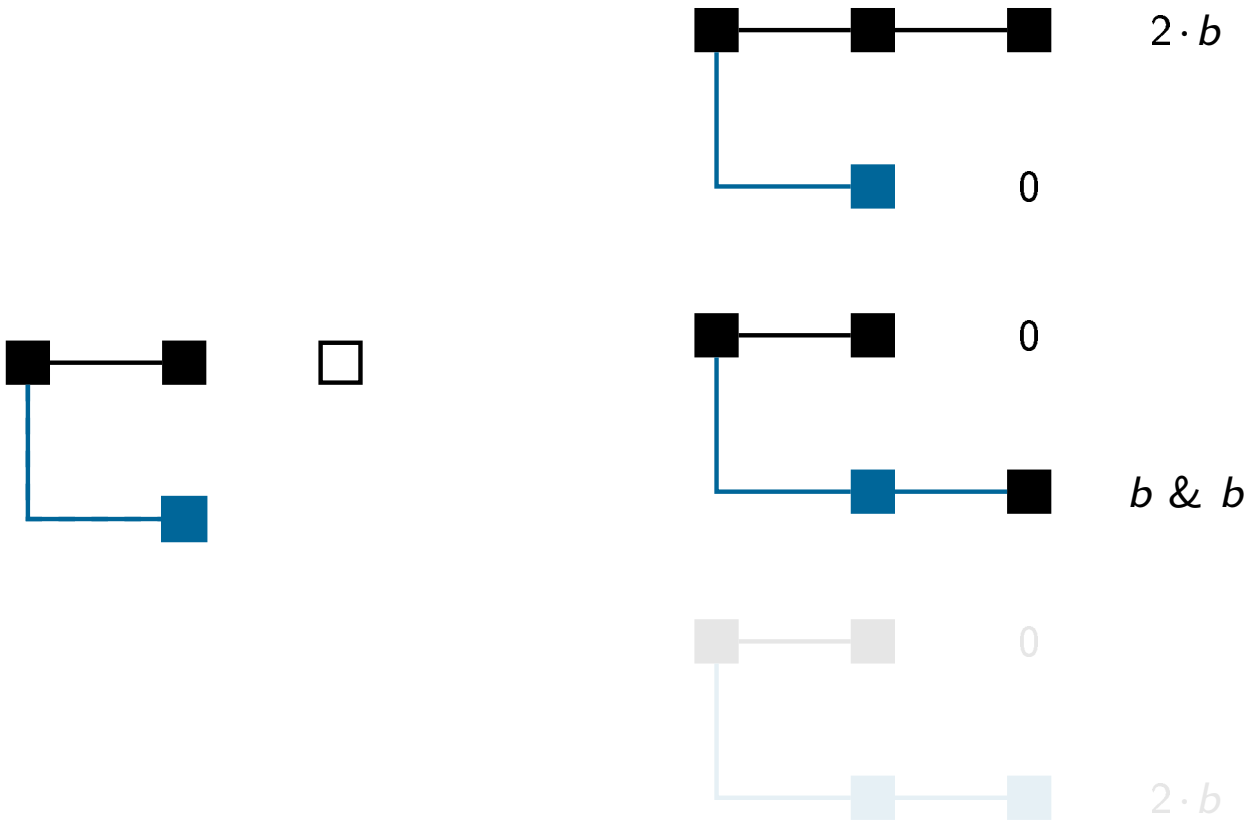


Fact

The outcome of the fork when the honest miners find the subsequent block depends on the connectivity parameter $q \in (0,1)$ of the malicious nodes.

Tied selfish mining

Link to blockchain mining

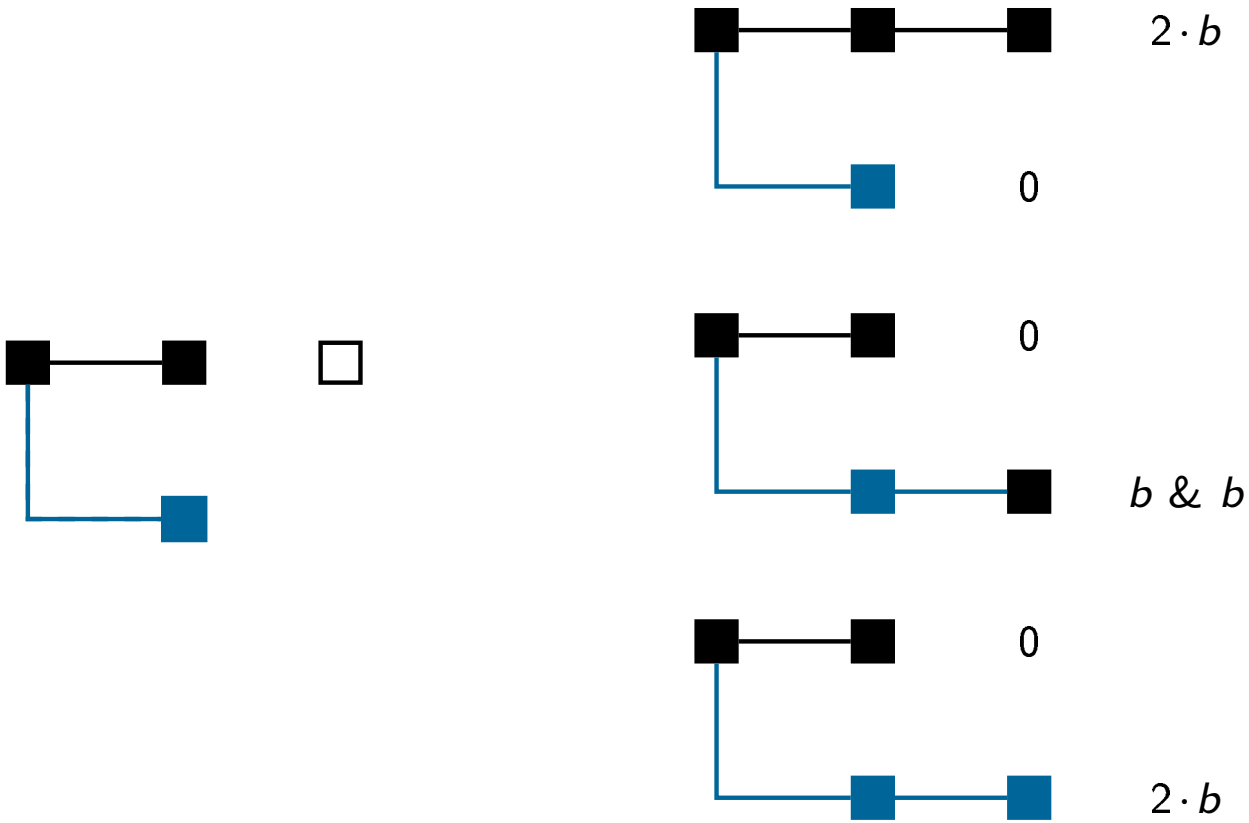


Fact

The outcome of the fork when the honest miners find the subsequent block depends on the connectivity parameter $q \in (0,1)$ of the malicious nodes.

Tied selfish mining

Link to blockchain mining

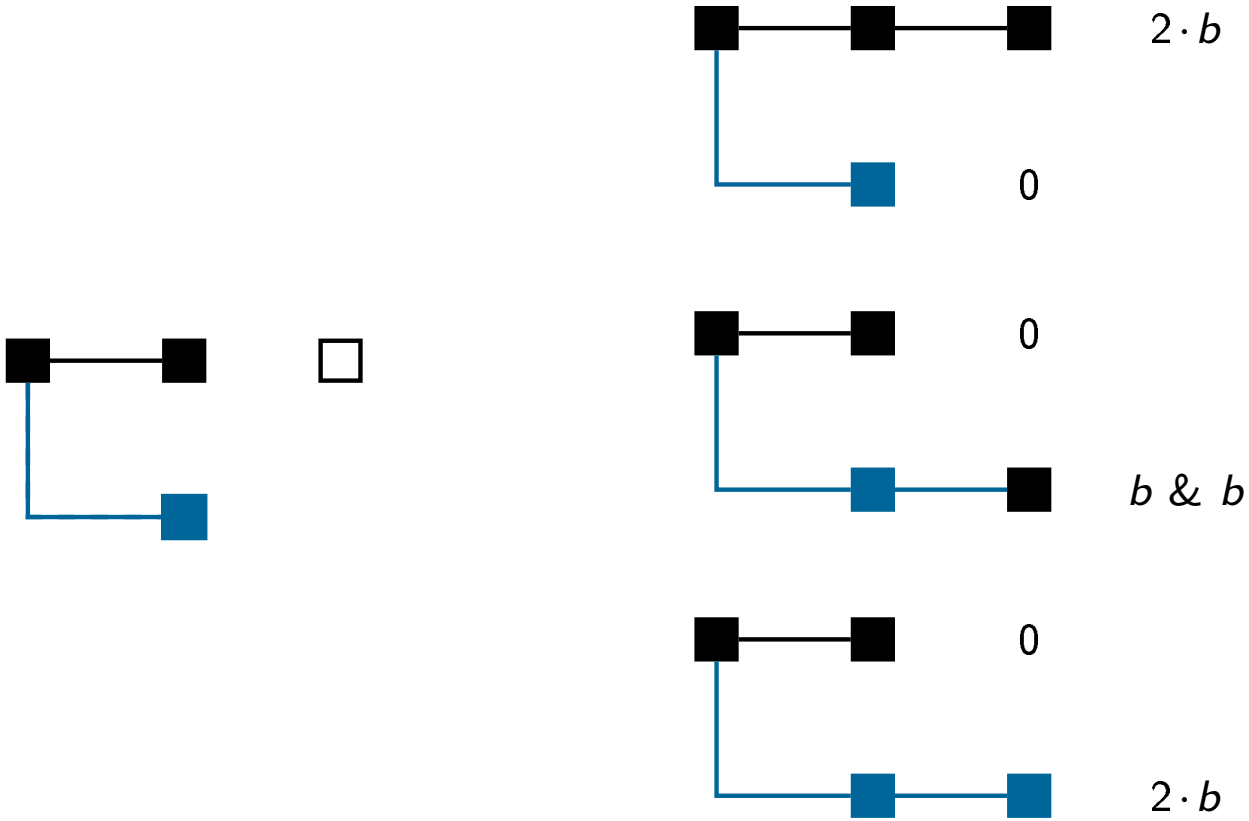


Fact

The outcome of the fork when the honest miners find the subsequent block depends on the connectivity parameter $q \in (0,1)$ of the malicious nodes.

Tied selfish mining

Link to blockchain mining



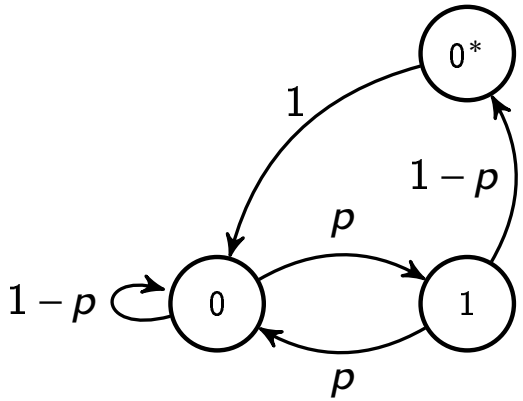
Fact

The outcome of the fork when the honest miners find the subsequent block depends on the connectivity parameter $q \in (0,1)$ of the malicious nodes.

Markov model

Link to blockchain mining

- Let $(Z_n)_{n\geq 0}$ be the number of blocks in the selfish miner's buffer with state space $\{0, 0^*, 1\}$.
- The transition graph is given by



- The reward collecting process is also Markovian as

$$f[Z_{n-1}, \xi_n, \zeta_n] = \begin{cases} 0, & \text{if } Z_{n-1} = 0, \\ 0, & \text{if } Z_{n-1} = 1 \ \& \ \xi_n = 0, \\ 2, & \text{if } Z_{n-1} = 1 \ \& \ \xi_n = 1, \\ 0, & \text{if } Z_{n-1} = 0^* \ \& \ \xi_n = 0 \ \& \ \zeta_n = 0, \\ 1, & \text{if } Z_{n-1} = 0^* \ \& \ \xi_n = 0 \ \& \ \zeta_n = 1, \\ 2, & \text{if } Z_{n-1} = 0^* \ \& \ \xi_n = 1. \end{cases}$$

where $\xi_n \sim \text{Ber}(p)$ and $\zeta_n \sim \text{Ber}(q)$

Wealth of a selfish miner

Link to blockchain mining

The wealth process of a selfish miner is given by

$$R_t = u - c \cdot t + b \cdot \sum_{n=1}^{N_t} f(Z_k, \xi_n, \zeta_n).$$

where N_t is a Poisson process with intensity λ that corresponds to the arrival of blocks in the blockchain.

- The net profit condition reads as

$$\frac{b}{t}\mathbb{E}\left[\sum_{n=1}^{N_t} f(Z_k, \xi_n, \zeta_n)\right] > c$$

- Once stationarity is reached we have

$$\mathbb{P}(Z_\infty = 0) = \frac{1}{1+2p-p^2},\ \mathbb{P}(Z_\infty = 1) = \frac{p}{1+2p-p^2},\ \text{and}\ \mathbb{P}(Z_\infty = 0^*) = \frac{p(1-p)}{1+2p-p^2},$$

and the net profit condition correspondingly reads

$$b\lambda \frac{qp(1-p)^2 + 4p^2 - 2p^3}{1+2p-p^2} - c > 0.$$

Expected profit of a selfish miner

Link to blockchain mining

Define

$$\widehat{\psi}_z(u,t) \equiv \mathbb{E}(\psi_z(u,T)) = \mathbb{E}\Big(\psi(u,T)\Big|Z_0 = z\Big) \text{ and } \widehat{V}_z(u,t) \equiv \mathbb{E}(V_z(u,T)) = \mathbb{E}\Big(R_T \mathbb{I}_{\tau_u > T}\Big|Z_0 = z\Big)$$

Theorem

For any $u \geq 0$, the ruin probability and expected profit of a selfish miner are given by

$$\widehat{\psi}_0(u,t) = C_1\, \mathrm{e}^{\rho_1\, u} + \mathrm{e}^{\rho_2\, u}\,[C_2\, \cos(\rho_3\, u) + C_3\, \sin(\rho_3\, u)],$$

and

$$\widehat{V}_0(u,t) = A_1\, \mathrm{e}^{\rho_1\, u} + \mathrm{e}^{\rho_2\, u}\,[A_2\, \cos(\rho_3\, u) + A_3\, \sin(\rho_3\, u)] + u + C,$$

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.

C. Grunspan and R. Pérez-Marco, "On profitability of selfish mining," 2019.

Conclusion and perspectives

Link to blockchain mining

- Selfish mining entails a waste of resources for everybody
- Including a difficulty adjustment can make it strategic
- Possible extensions
  1. Consider stochastic jumps
  2. Consider the actual selfish mining strategy
  3. Consider generalization of the selfish mining strategy

     A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Financial Cryptography and Data Security*, pp. 515–532, Springer Berlin Heidelberg, 2017.

     ↪ Stochastic control problem !
  4. Better understanding of the connectivity parameter q

     J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Bitcoin blockchain dynamics : The selfish-mine strategy in the presence of propagation delay," *Performance Evaluation*, vol. 104, pp. 23–41, 2016.

     ↪ Graph theory !