Blockchain miner's risk management

Pierre-O. Goffard

Université de Strasbourg
goffard@unistra.fr

June 6, 2023

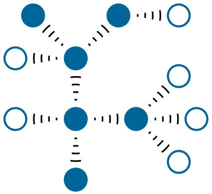
1 PoW Blockchain

2 Blockchain miner's risk model

Blockchain

A decentralized data ledger made of blocks maintained by achieving consensus in a P2P network.

- Decentralized
- Public/private
- Permissionned/permissionless
- Immutable
- Incentive compatible



Focus of the talk

Public and permissionless blockchain equipped with the Proof-of-Work protocol.

Applications of blockchain: Cryptocurrency

PoW Blockchain

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

- Transaction anonymity
- No need for a thrusted third party

What's inside a block?

A block consists of

- a header
- a list of "transactions" that represents the information recorded through the blockchain.

The header usually includes

- the date and time of creation of the block,
- the block height which is the index inside the blockchain,
- the hash of the block
- the hash of the previous block.

Question

What is the hash of a block?

Cryptographic Hash function

A function that maps data of arbitratry size (message) to a bit array of fixed size (hash value)

$$h : \{0,1\}^* \mapsto \{0,1\}^d.$$

A good hash function is

- deterministic
- quick to compute
- One way
  - $\hookrightarrow$ For a given hash value $\overline{h}$ it is hard to find a message m such that
  $$h(m) = \overline{h}$$
- Colision resistant
  - $\hookrightarrow$ Impossible to find m_1 and m_2 such that
  $$h(m_1) = h(m_2)$$
- Chaotic
  $$m_1 \approx m_2 \Rightarrow h(m_1) \neq h(m_2)$$

SHA-256

The SHA-256 function which converts any message into a hash value of 256 bits.

Example

The hexadecimal digest of the message

`Is Defi the future?`

is

`50f3257a3d22a56247a8978fd2505e8cdd64e1cb06e52c941d09e234722dc275`

Mining a block

PoW Blockchain

```
Block Hash: 1fc23a429aa5aaf04d17e9057e03371f59ac8823b1441798940837fa2e318aaa
Block Height: 0
Time:2022-02-25 12:42:04.560217
Nonce:0
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 0}, {'sen
der': 'Satoshi', 'recipient': 'Pierre-O', 'amount': 5, 'fee': 2}]
Previous block hash: 0
Mined: False
--------------
```

Figure: A block that has not been mined yet.

Mining a block

The maximum value for a 256 bits number is

$$T_{\max} = 2^{256} - 1 \approx 1.16e^{77}.$$

Mining consists in drawing at random a nonce

$$\text{Nonce} \sim \text{Unif}(\{0, \dots, 2^{32} - 1\}),$$

until

$$h(\text{Nonce}|\text{Block info}) < T,$$

where T is referred to as the target.

Difficulty of the cryptopuzzle

$$D = \frac{T_{\max}}{T}.$$

Mining a block

If we set the difficulty to $D = 2^4$ then the hexadecimal digest must start with at least 1 leading 0

```
Block Hash: 0869032ad6b3e5b86a53f9dded5f7b09ab93b24cd5a79c1d8c81b0b3e748d226
Block Height: 0
Time:2022-02-25 13:41:48.039980
Nonce:2931734429
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 0}, {'sen
der': 'Satoshi', 'recipient': 'Pierre-O', 'amount': 5, 'fee': 2}]
Previous block hash: 0
Mined: True
--------------
```

Figure: A mined block with a hash value having on leading zero.

The number of trial is geometrically distributed

- Exponential inter-block times
- Lenght of the blockchain = Poisson process

Bitcoin protocol

PoW Blockchain

- One block every 10 minutes on average
- Depends on the hashrate of the network
- Difficulty adjustment every 2,016 blocks ($\approx$ two weeks)

Risky business

Steady operational cost VS infrequent capital gains

Dual risk model

Blockchain miner's risk model

Consider a miner

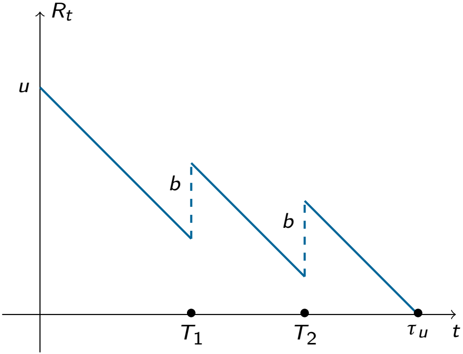
- of hashrate $p \in (0,1)$
- that owns $u \geq 0$ at $t = 0$
- spends $c = \pi_W \cdot W \cdot p$ per time unit
- who finds $p\lambda$ blocks on average per time unit, where λ is the average number of blocks found by the network

The wealth of such a miner is given by

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

où

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



Expected profit if no failure

The ruin time is defined as

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

- Risk measure

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

- Profitability measure

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

A miner's dilemma

Blockchain miner's risk model

Use ψ and V to compare mining solo to

- pool mining
  - M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011.
  - Hansjörg Albrecher, Dina Finger, and Pierre-O. Goffard.
    Blockchain mining in pools: Analyzing the trade-off between profitability and ruin.
    Insurance: Mathematics and Economics, 105:313–335, jul 2022.
    10.1016/j.insmatheco.2022.04.004.
- deviating from the prescribed 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.
  - Hansjoerg Albrecher and Pierre-Olivier Goffard.
    On the profitability of selfish blockchain mining under consideration of ruin.
    Operations Research, 70(1):179–200, jan 2022.
    10.1287/opre.2021.2169.

Analytical expressions for

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

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

Solo mining

Theorem (profit and ruin when mining solo)

For $u \geq 0$, with

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

and

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

where ρ^* is the only nonnegative solution of

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

Lambert function

The solution ρ^* of (2) 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.

Mining pool?

Let $I \subset \{1, \ldots, n\}$ be a set of miners with cumulated hashpower

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

- A pool manager coordinates the joint effort
- Miners show their work by submitting partial solutions (*share*)

The pool manager chooses

- the participant remuneration system
- the relative difficulty $q \in (0,1)$ of finding a *share* VS finding a proper solution
- the amount of management fees f

Remuneration system

Miners must be compensated pro-rata to their contribution to the mining effort.

Proportional scheme

A round is the time elapsed between two block discovery

- s_i is the number of *shares* submitted by $i \in I$ during the *round*
- Each miner receives
$$(1-f)\cdot b\cdot \frac{s_i}{\sum_{i\in I} s_i},$$
at the end the round, where f is the pool manager's cut.
- The system is deemed fair if $\frac{s_i}{\sum_{i\in I} s_i} \approx \frac{p_i}{\sum_{i\in I} p_i}$

What's wrong about going proportional

Blockchain miner's risk model

Remarque

This scheme 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.

- The duration of *rounds* is random
  - ↪ A *share* loses value when the *round* last for too long ⇒ *pool hoping*

    M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011.
  - ↪ Apply a discount factor to *shares*

    slush pool, "Reward system specifications," 2021.
- A miner may postpone the communication of a solution
  - ↪ to wait for her proportion of submitted *shares* to improve
- No risk transfer from miner to pool manager
  - ↪ f must be small

The Pay-per-Share (PPS) system

The manager pays

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

for every *share* and keeps the block finding reward.

Miner's wealth

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

where

- $(M_t^i)_{t\geq 0}$ is a Poisson process with intensity $p_i\mu = p_i\lambda/q$
- μ is the average number of *shares* submitted by the network

Manager's wealth

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

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 $p_I\lambda$

---

https://en.bitcoin.it/wiki/Comparison_of_mining_pools

Pool manager's risk

Blockchain miner's risk model

Theorem (Profits and loss of a pool manager)

The ruin probability is given by

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

and the expected wealth is

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

where R is the only solution to

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

with positive real part.

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

Problem related to mining pools

- Arm race, ramping electricity consumption and e-waste generation
  - 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 decentralization?
  - 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.

https://btc.com/stats/pool?pool_mode=year

Solo mining

Theorem (profit and ruin when mining solo)

For $u \geq 0$, with

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

and

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

where ρ^* is the only nonnegative solution of

$$-c\rho + p\lambda(e^{b\rho} - 1) = 1/t. \tag{2}$$

Lambert function

The solution ρ^* of (2) 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

The time-horizon is random with $T \sim \text{Exp}(t)$, we condition upon the events occuring in $(0, h)$, with $h < u/c$ so that ruin cannot occur before h. Three possibilities

(i) $T > h$ and no blocks $(0, h)$

(ii) $T < h$ and no blocks $(0, T)$

(iii) One block found before T and h

The expected profit $\widehat{V}(u, t)$ satisfies

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

Sketch of the proof

Differentiating with respect to h and setting $h=0$, we get

$$c\widehat{V}'(u,t)+\left(\frac{1}{t}+p\lambda\right)\widehat{V}(u,t)-p\lambda\widehat{V}(u+b,t)-\frac{u}{t}=0, \tag{3}$$

Equation (3) is an advanced differential equation with boundary conditions

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

Consider solutions of the form

$$\widehat{V}(u,t)=Ae^{\rho u}+Bu+C,\ u\geq 0, \tag{4}$$

where A,B,C and ρ are constants to be determined. Substituting (4) in (3) together with boundary conditions

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

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

Sketch of the proof

We get $A = -t(p\lambda b - c)$, $B = 1$, $C = t(p\lambda b - c)$ and ρ verifies

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

The latter has two solutions on the real line, one negative and the other is positive. As $A < 0$, we must take $\rho^* < 0$ to ensure that $\widehat{V}(u,t) > 0$. Substituting A, B, C and ρ^* in (4) yields the result. Similarly, the ruin probability satisfies

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

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

Pool manager's risk

Theorem (Profits and loss of a pool manager)

The ruin probability is given by

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

and the expected wealth is

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

where R is the only solution to

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

with positive real part.

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

Conditionning upon the events that occur during $(0,h)$. Four possibilities

(i) $T>h$ and no jumps $(0,h)$

(ii) $T<h$ and no jumps $(0,T)$

(iii) an upward jump $(0,h)$

(iv) a downward jump $(0,h)$

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

Differentiating with respect to h and letting $h\to 0$, yields

$$
\lambda\int_0^\infty \widehat{V}(u+x,t)\,dF_B(x)-(\lambda+\mu^*+1/t)\widehat{V}(u,t)+\mu^*\int_0^u \widehat{V}(u-y,t)\,dF_W(y)+u/t=0,\quad u\geq 0,\quad (5)
$$

with boundary conditions $\widehat{V}(u,t)=0$ pour tout $u<0$ et $0\leq\widehat{V}(u,t)\leq u+(\lambda b^*-\mu^* w)t$. Consider solutions of the form

$$
Ce^{-ru}+d_1u+d_0
$$

Sketch of the proof II

- Gathering the terms in factor of e^{-ru} yields an equation for r with

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

  with nonnegative solution $R>0$, negative is impossible because $0\leq \widehat{V}(u,t)\leq u+(\lambda b^*-\mu^* w)t$
- Gathering the terms in factor of u, yields $d_1=1$
- Gathering the terms in factor of 1, yields

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

- Gathering the terms in factor of $e^{-u/w}$, yields

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