

# Blockchain miner's risk management

Pierre-O. Goffard

Institut de Science Financières et d'Assurances  
[pierre-olivier.goffard@univ-lyon1.fr](mailto:pierre-olivier.goffard@univ-lyon1.fr)

May 18, 2022

**1** Introduction

**2** Insurance risk theory

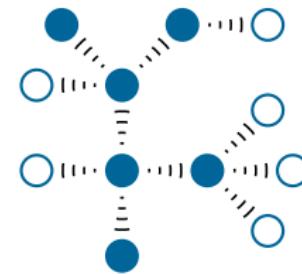
**3** Application to blockchain miner risk management

# Blockchain

## Introduction

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.

# Consensus protocols

## Introduction

The mechanism to make all the nodes agree on a common data history.

The three dimensions of blockchain systems analysis

### 1 Efficiency

- Throughputs
- Transaction confirmation time

### 2 Decentralization

- Fair distribution of the accounting right

### 3 Security

- Resistance to attacks



X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: mechanism, design and applications," *Science China Information Sciences*, vol. 64, nov 2020.

# Applications of blockchain: Cryptocurrency

## Introduction



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



- Transaction anonymity
- Banking and reliable currency in certain regions of the world
- Money Transfer worldwide (at low fare)
- No need for a trusted third party

# Decentralized finance

## Introduction

DEFI creates new financial architecture

- + Non custodial
- + Anonymous
- + Permissionless
- + openly auditable
- Unregulated
- Tax evasion
- Fraud
- Money laundering

Extends the Bitcoin promises to more complex financial operations

- Collateralized lending
- Decentralized Exchange Platform
- Tokenized assets
- Fundraising vehicle (ICO, STO, ...)



S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "Sok: Decentralized finance (defi)," 2021.

# What's inside a block?

## Introduction

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

## Introduction

A function that maps data of arbitrary 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

→ For a given hash value  $\bar{h}$  it is hard to find a message  $m$  such that

$$h(m) = \bar{h}$$

- Collision resistant
  - 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

## Introduction

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

### Example

The hexadecimal digest of the message

Moritz Voss is the man

is

50f3257a3d22a56247a8978fd2505e8cdd64e1cb06e52c941d09e234722dc275

# Mining a block

## Introduction

```
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}, {"sender": "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

## Introduction

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

## Introduction

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}, {"sender": "Satoshi", "recipient": "Pierre-O", "amount": 5, "fee": 2}]
Previous block hash: 0
Mined: True
-----
```

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

The number of trial is geometrically distributed

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

# Bitcoin protocol

## Introduction

- One block every 10 minutes on average
- Depends on the hashrate of the network
- Difficulty adjustment every 2,016 blocks ( $\approx$  two weeks)
- Reward halving every 210,000 blocks

Check out <https://www.bitcoinblockhalf.com/>

Risky business

Steady operational cost VS infrequent capital gains

# Cramer-Lunberg risk model

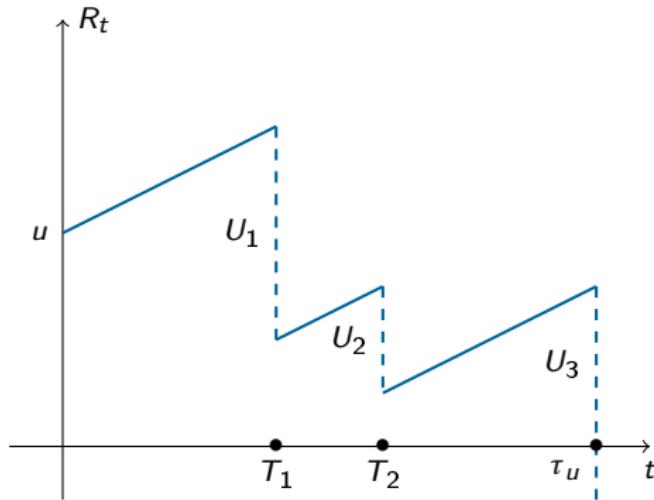
## Insurance risk theory

The financial reserves of a nonlife insurance company is given by

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

où

- $u > 0$  the initial reserves
- $c$  is the premium rate
- $(N_t)_{t \geq 0}$  is the claim frequency up to time  $t \geq 0$ .
  - ↪ Poisson process with intensity  $\lambda$
- The  $U_i$ 's are the claim amounts
  - ↪ Nonnegative random variables, i.i.d., and independent from  $N_t$



# Ruin probability

Insurance risk theory

Define the ruin time as

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

and the ruin probability as

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

Find  $u$  such that

$$\mathbb{P}(\text{Ruin}) = \alpha \ (0.005),$$

with

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

where

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

otherwise

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



S. Asmussen and H. Albrecher, *Ruin Probabilities*.

WORLD SCIENTIFIC, sep 2010.

# Dual risk model

Application to blockchain miner risk management

Consider a miner

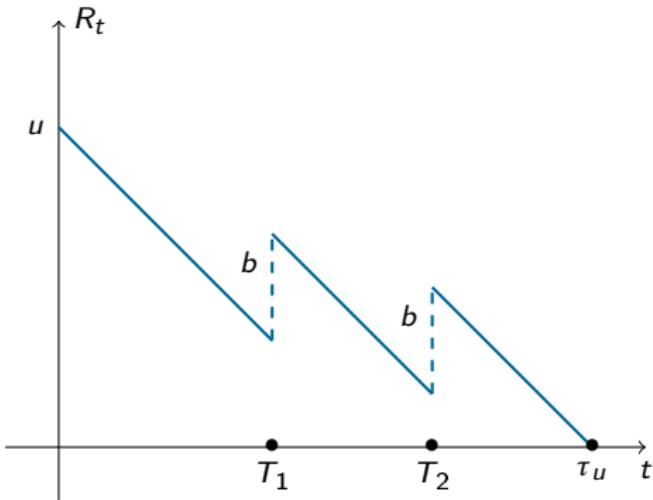
- of hashrate  $p \in (0,1)$
- that owns  $u \geq 0$  at  $t=0$
- spends  $c = \pi_W \cdot W \cdot p$  per time unit
- who finds  $p\lambda$  blocks on average per time unit, where  $\lambda$  is the average number of blocks found by the network

The wealth of such a miner is given by

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

ou

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



# Expected profit if no failure

Application to blockchain miner risk management

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

## Application to blockchain miner risk management

Use  $\psi$  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-Olivier Goffard.

Blockchain mining in pools: Analyzing the trade-off between profitability and ruin.  
to appear in Insurance: Mathematics and Economics, April 2022.  
URL <https://hal.archives-ouvertes.fr/hal-03336851>.

- 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.



Hansjörg 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

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

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

# Solo mining

Application to blockchain miner risk management

Theorem (profit and ruin when mining solo)

For  $u \geq 0$ , with

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

and

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

where  $\rho^*$  is the only nonnegative solution of

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

Lambert function

The solution  $\rho^*$  of (1) is given by

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

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

# Sketch of the proof

Application to blockchain miner risk management

The time-horizon is random with  $T \sim \text{Exp}(t)$ , we condition upon the events occurring 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  $\hat{V}(u, t)$  satisfies

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

# Sketch of the proof

## Application to blockchain miner risk management

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

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

Equation (2) is an advanced differential equation with boundary conditions

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

Consider solutions of the form

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

where  $A, B, C$  and  $\rho$  are constants to be determined. Substituting (3) in (2) together with boundary conditions

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

---

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

# Sketch of the proof

Application to blockchain miner risk management

We get  $A = -t(p\lambda b - c)$ ,  $B = 1$ ,  $C = t(p\lambda b - c)$  and  $\rho$  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  $\hat{V}(u, t) > 0$ . Substituting  $A, B, C$  and  $\rho^*$  in (3) yields the result. Similarly, the ruin probability satisfies

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

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

# Mining pool?

Application to blockchain miner risk management

Let  $I \subset \{1, \dots, n\}$  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

Application to blockchain miner risk management

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

Application to blockchain miner risk management

## 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 hopping*
    - 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

Application to blockchain miner risk management

The manager pays

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

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

Miner's wealth

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

where

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

Manager's wealth

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

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's risk

Application to blockchain miner risk management

Let us consider randomized rewards

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

where

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

## Poisson process superposition

A block discovery triggers the payment of a *share* to the miners

- The intensity of  $M_t$  is given by  $\mu^* = \mu - \lambda$
- The block finding reward is then  $b^* = b - w$

A distinction is made here between jumps up and down.

# Pool manager's risk

Application to blockchain miner risk management

Theorem (Profits and loss of a pool manager)

The ruin probability is given by

$$\hat{\psi}(u, t) = (1 - R w) e^{-R u}, \quad u \geq 0,$$

and the expected wealth is

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

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 |

## Application to blockchain miner risk management

Conditioning 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  $(0, h)$

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

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

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

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

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

# Sketch of the proof II

## Application to blockchain miner risk management

- 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  
 $0 \leq \hat{V}(u, t) \leq u + (\lambda b^* - \mu^* w)t$

- 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

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

# Problem related to mining pools

Application to blockchain miner risk management

- 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.