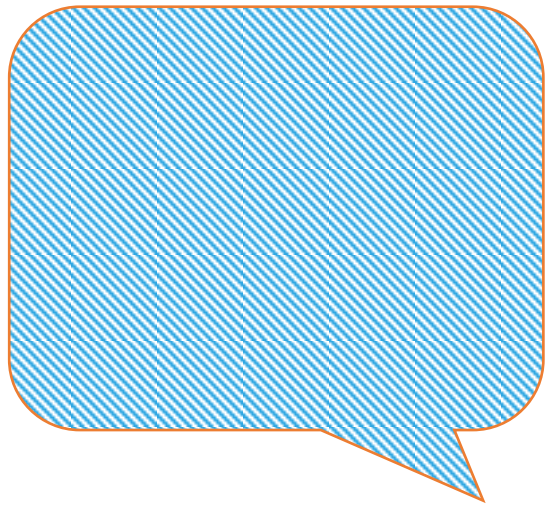
BLOCKCHAINS: Usos y Abusos

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL

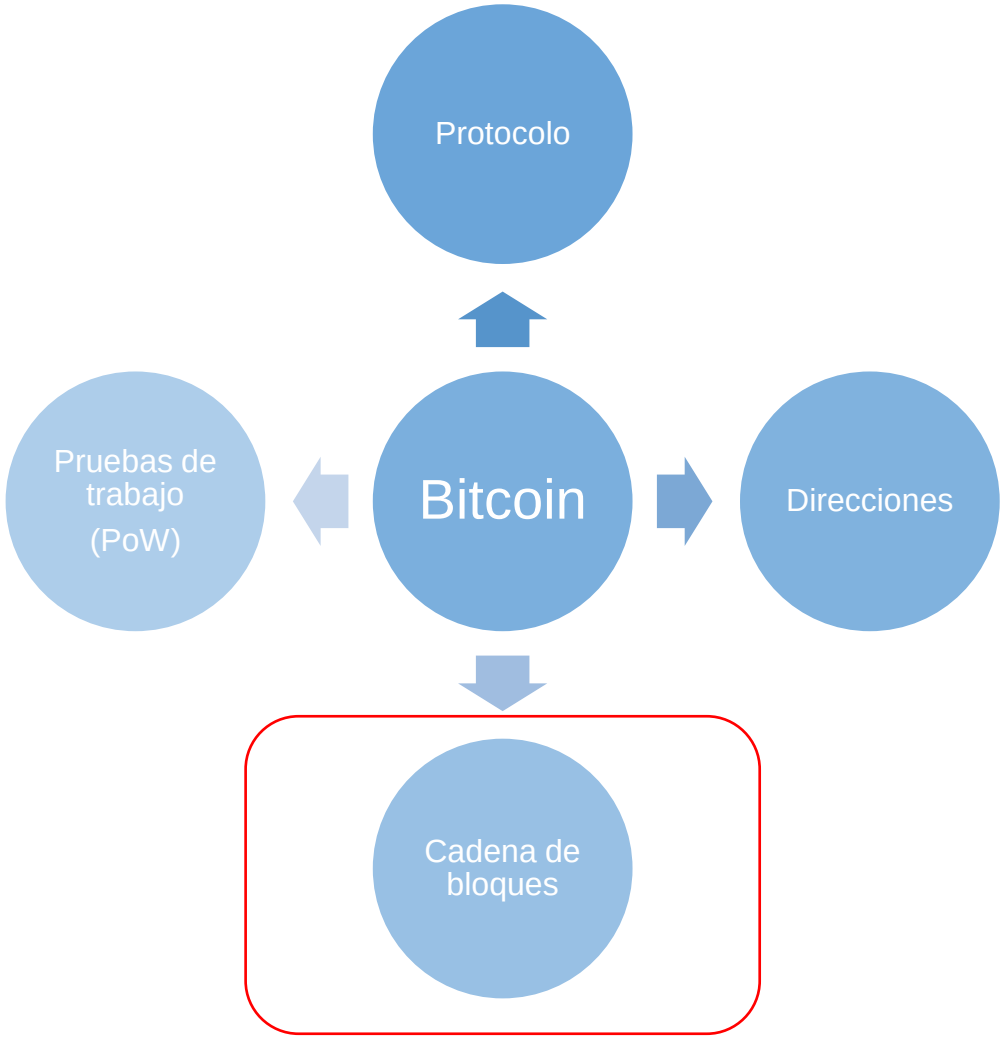


- Oscar Delgado (UAM)
- David Arroyo (UAM)
- Jesús Díaz Vico (BEEVA)
- Luis Hernández (CSIC)

✉ oscar.delgado@uam.es

Índice

"Registro **distribuido** e **inmutable** de datos"



¿Qué hace esta idea **diferente**?

No **autoridad central** = No fallo, no corrupción, no prohibición

No es el primer algoritmo de **consenso distribuido**, pero sí el más exitoso

¿Sistema descentralizado? ¿De verdad?

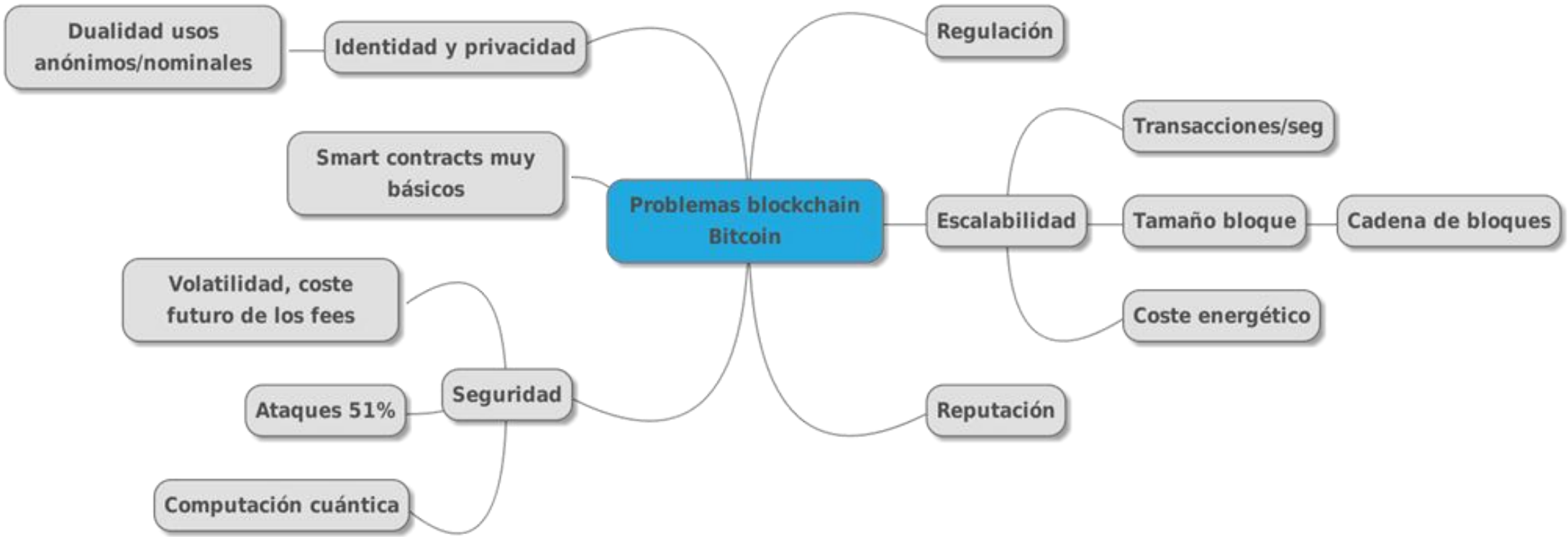
Wladimir J. van der Laan

Gavin Andresen

Peter Wuille

Cory Fields

Matt Corallo


Problemas blockchain Bitcoin
Regulación
Escalabilidad
Transacciones/seg
Tamaño bloque
Cadena de bloques
Coste energético
Reputación
Identidad y privacidad
Dualidad usos anónimos/nominales
Smart contracts muy básicos
Seguridad
Volatilidad, coste futuro de los fees
Ataques 51%
Computación cuántica

Vulnerabilidades

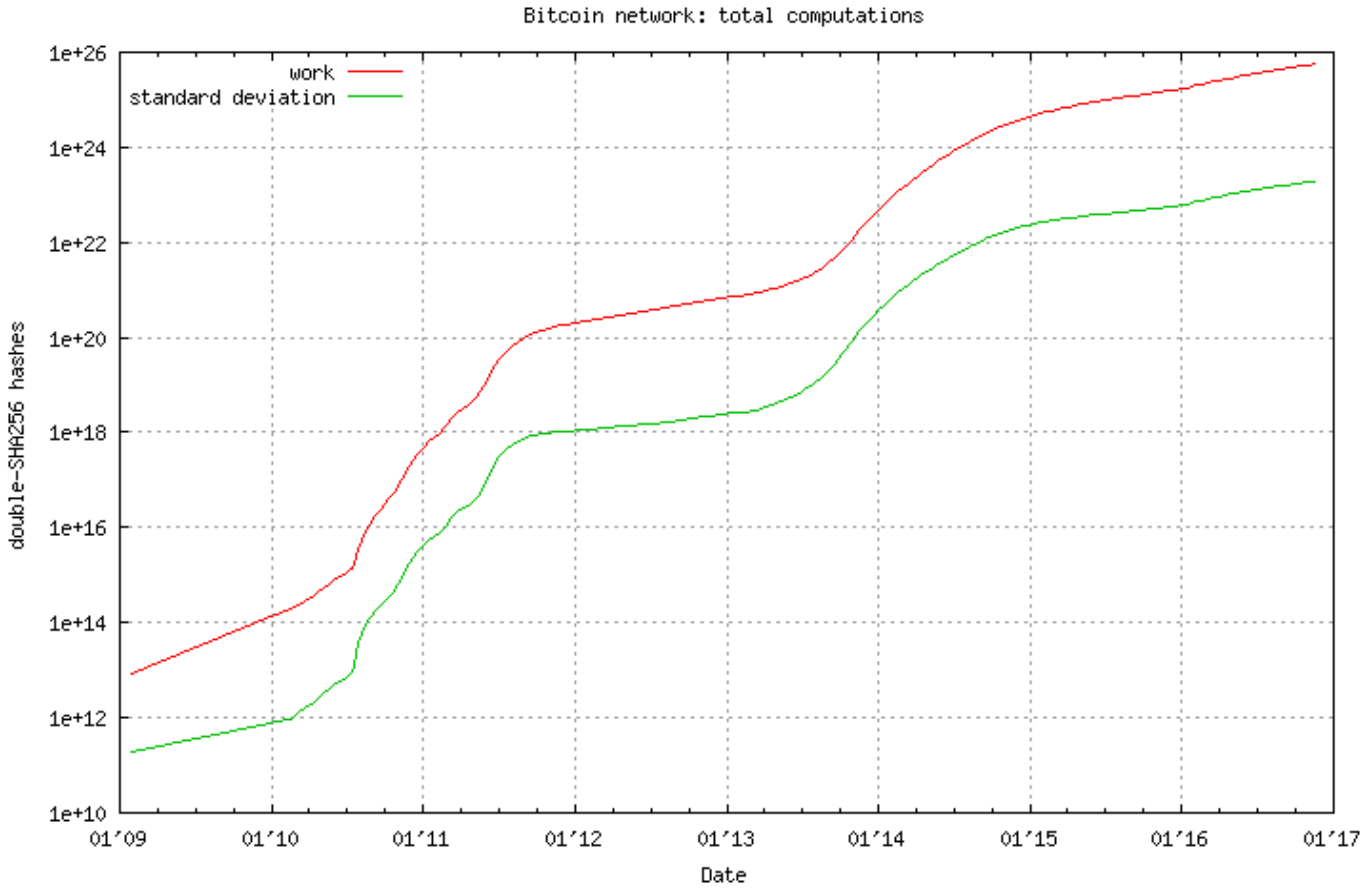
- Bugs software
- Escalabilidad
- Ataque del 51%
- Minado egoísta
- Identidad

Seguridad termodinámica

- El problema del doble gasto puede ser visto como un problema termodinámico: reescribir la cadena de bloques implica gastar una considerable cantidad de energía.
- ¿Cuánta, exactamente?

Fuente: *Bitcoin's Security Model Revisited*. Sompolinsky and Zohar

Hagamos algunos cálculos



Fuente: *bitcoin.sipa.be*

Hagamos algunos cálculos

- Necesitaríamos unos 10^{26} hashes para regenerar la cadena completa
- El *Antminer S9* se considera el dispositivo más eficiente del mercado

Fuente: *bitcoin.sipa.be*

Antminer S9

1. Hash Rate: 14 TH/s ±5%
2. Consumo energético: 1375W + 7%
3. Eficiencia energética: 0.098 J/GH + 7%

Coste por GH/s
$ 0.1500

Fuente: *bitcoin.sipa.be*

Hagamos algunos cálculos

$1\ J \approx 2{,}777777778 \cdot 10^{-7}\ kWh$

10^{26} hashes · 0,1 J / 10^{9} hashes = 10^{16} J

10^{16} J = 2.777.777.778 kWh · 0,172€/kWh = 477,7 M €

Fuente: *bitcoin.sipa.be*

Checkpoints en código

```
checkpointData = (CCheckpointData) {
    boost::assign::map_list_of
    ( 11111, uint256S("0x0000000069e244f73d78e8fd29ba2fd2ed618bd6fa2ee92559f542fdb26e7c1d"))
    ( 33333, uint256S("0x000000002dd5588a74784eaa7ab0507a18ad16a236e7b1ce69f00d7ddfb5d0a6"))
    ( 74000, uint256S("0x0000000000573993a3c9e41ce34471c079dcf5f52a0e824a81e7f953b8661a20"))
    (105000, uint256S("0x00000000000291ce28027faea320c8d2b054b2e0fe44a773f3eefb151d6bdc97"))
    (134444, uint256S("0x00000000000005b12ffd4cd315cd34ffd4a594f430ac814c91184a0d42d2b0fe"))
    (168000, uint256S("0x000000000000099e61ea72015e79632f216fe6cb33d7899acb35b75c8303b763"))
    (193000, uint256S("0x000000000000059f452a5f7340de6682a977387c17010ff6e6c3bd83ca8b1317"))
    (210000, uint256S("0x0000000000000048b95347e83192f69cf0366076336c639f9b7228e9ba171342e"))
    (216116, uint256S("0x00000000000001b4f4b433e81ee46494af945cf96014816a4e2370f11b23df4e"))
    (225430, uint256S("0x00000000000001c108384350f74090433e7fcf79a606b8e797f065b130575932"))
    (250000, uint256S("0x0000000000000003887df1f29024b06fc2200b55f8af8f35453d7be294df2d214"))
    (279000, uint256S("0x0000000000000001ae8c72a0b0c301f67e3afca10e819efa9041e458e9bd7e40"))
    (295000, uint256S("0x00000000000000004d9b4ef50f0f9d686fd69db2e03af35a100370c64632a983")),
    1397080064, // * UNIX timestamp of last checkpoint block
    36544669,   // * total number of transactions between genesis and last checkpoint
                //   (the tx=... number in the SetBestChain debug.log lines)
    60000.0     // * estimated number of transactions per day after checkpoint
};
}
```

09 Abril 2014

Fuente: *bitcoin.sipa.be*

OK, rehagamos los cálculos

$1\ J \approx 2{,}777777778 \cdot 10^{-7}\ kWh$

$(10^{26} - 10^{23})\ hashes \cdot 0{,}1\ J / 10^{9}\ hashes = 9{,}99 \cdot 10^{15}\ J$

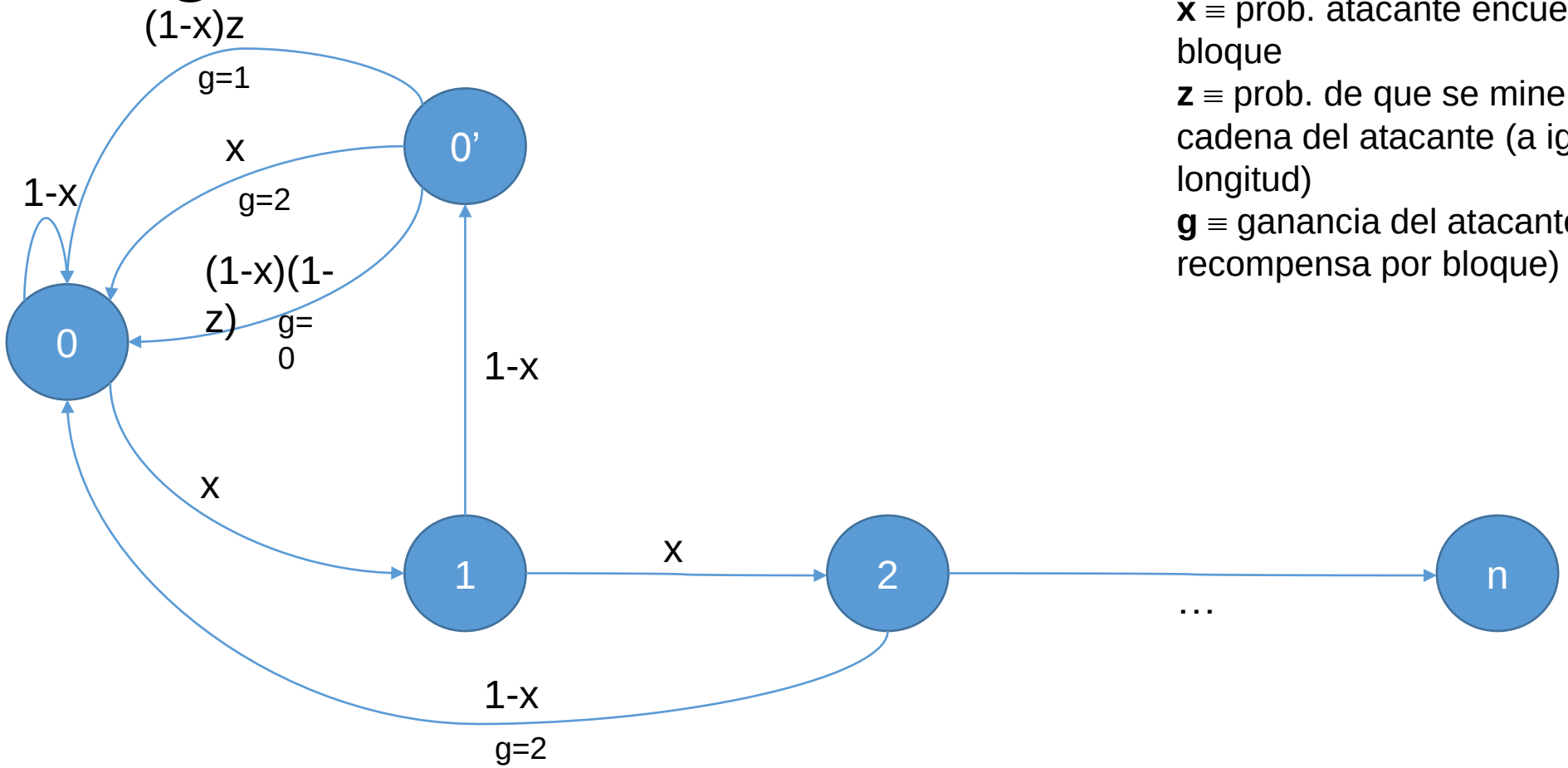
$9{,}99 \cdot 10^{15}\ J = 2.777.777.778\ kWh \cdot 0{,}172€/kWh =$ 477,3 M €

Fuente: *bitcoin.sipa.be*

Ataque del minado **egoísta**

- Presentado en 2013 por Eyal & Sirer de la Universidad de Cornell
- **Idea**: cuando mines un bloque, no lo publiques
- Con sólo un 25% del *hashrate*, la estrategia permite ganar más de lo que correspondería

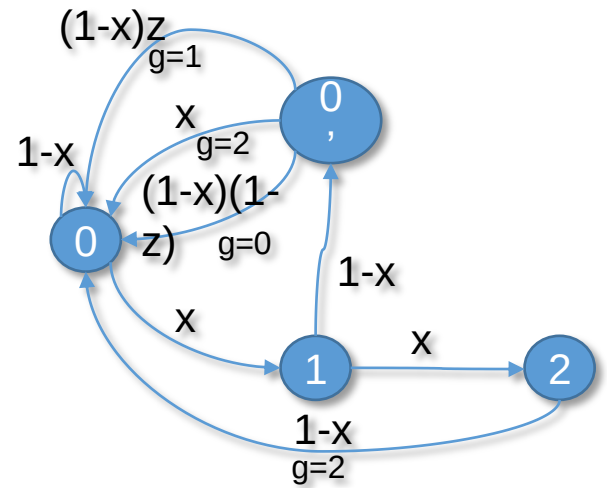
Ataque del minado **egoísta**

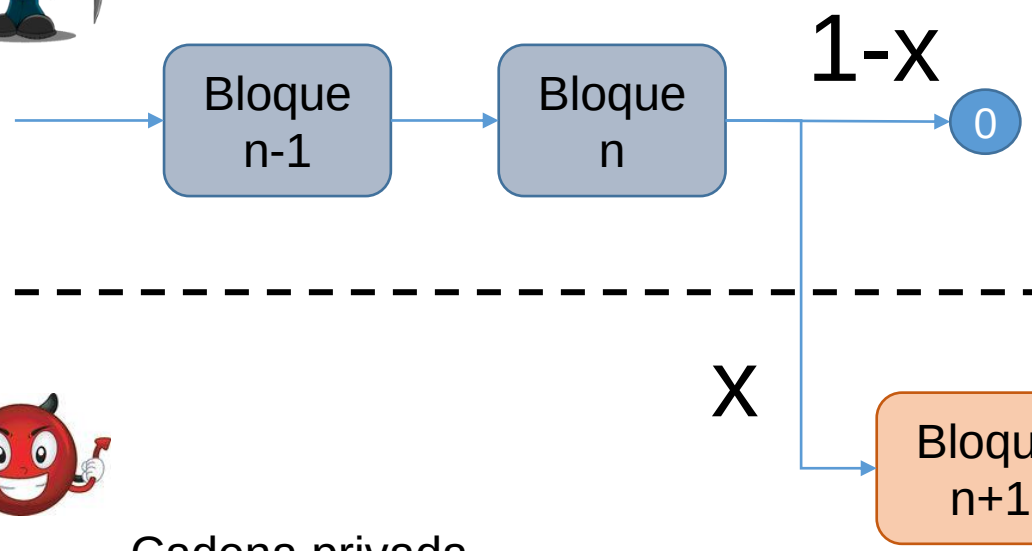


x ≡ prob. atacante encuentre un bloque
z ≡ prob. de que se mine en la cadena del atacante (a igual de longitud)
g ≡ ganancia del atacante (en recompensa por bloque)

Transición 0 → 1: Atacantes minan un bloque

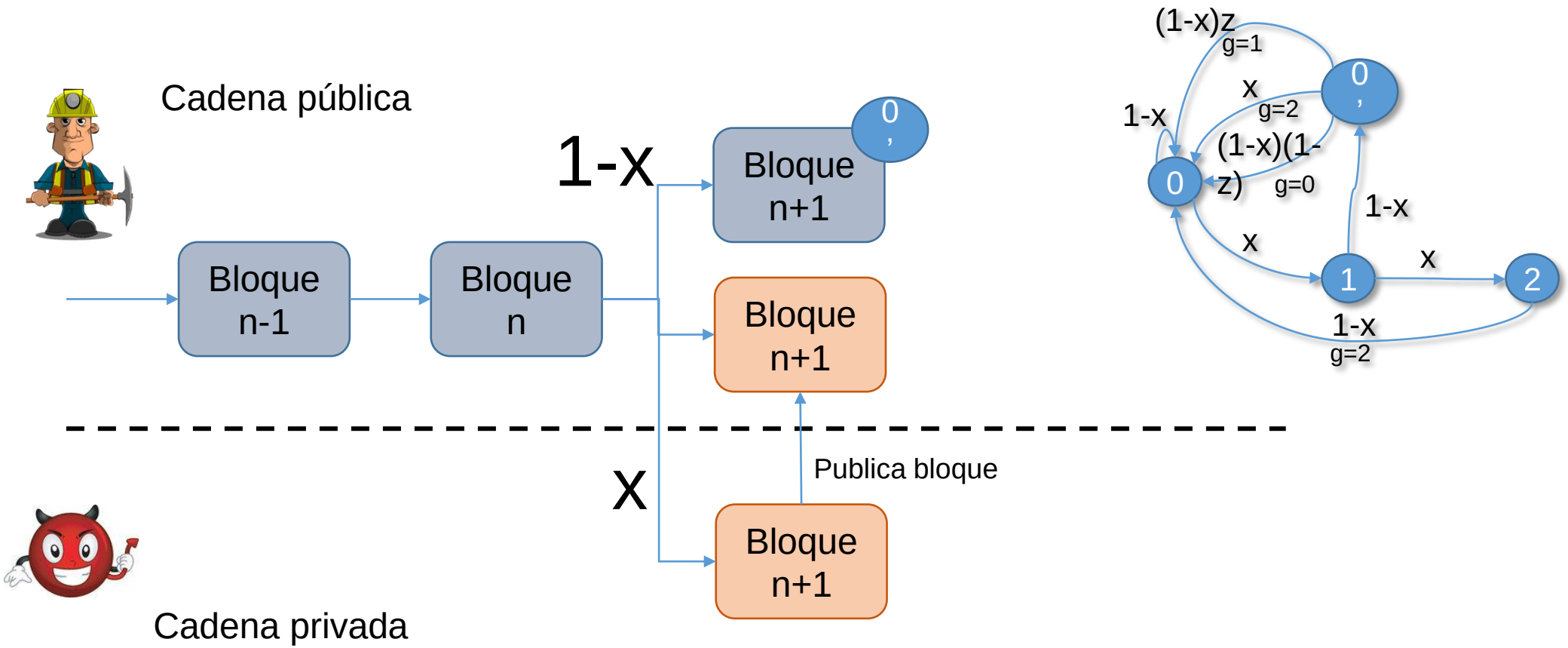
Cadena pública





Cadena privada

Transición 1 → 0' : Red encuentra un bloque



Transición 0' → 0 : La cadena pública se recupera

Cadena pública

Atacantes no ganan nada

Bloque n-1

Bloque n

Bloque n+1

Bloque n+2

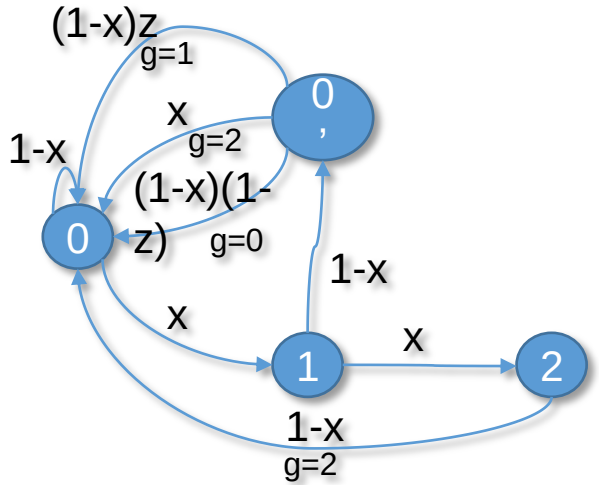
0

Bloque n+1

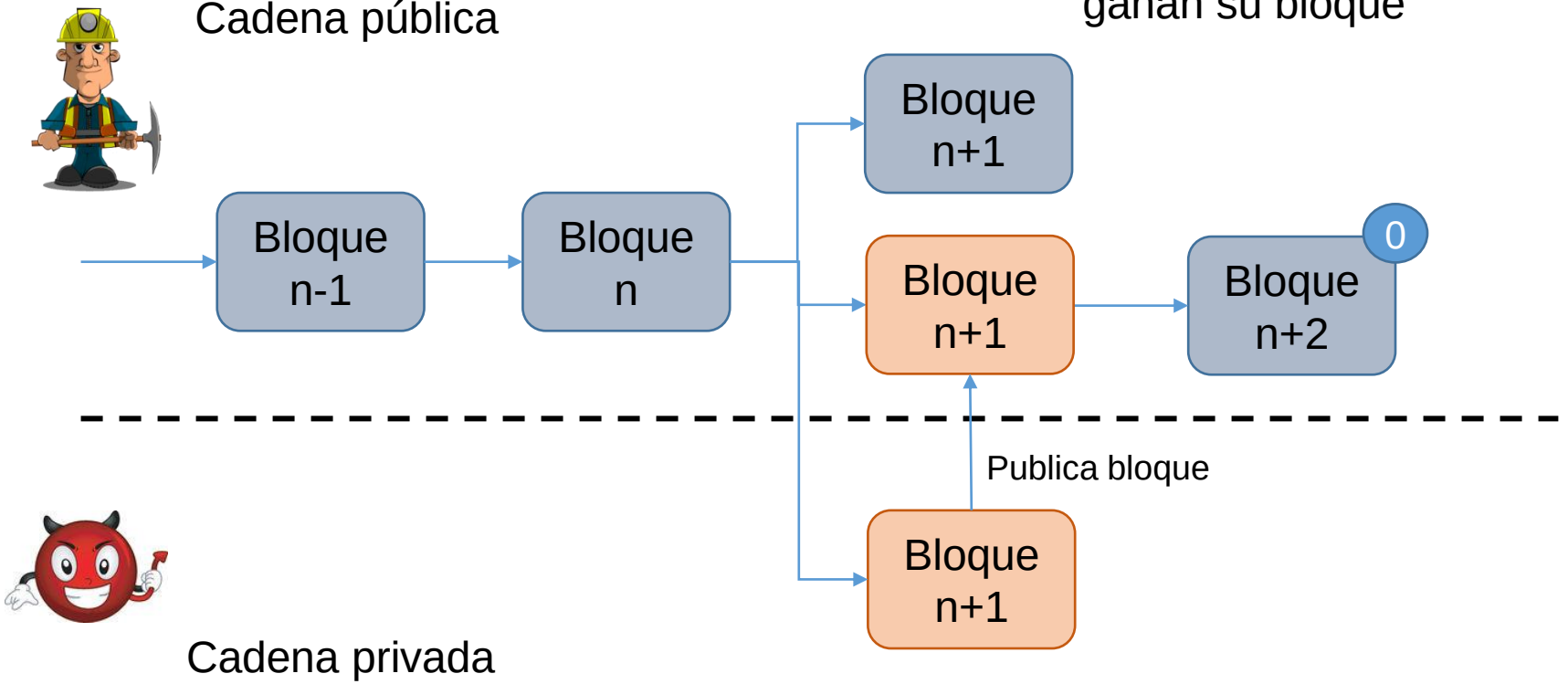
Publica bloque

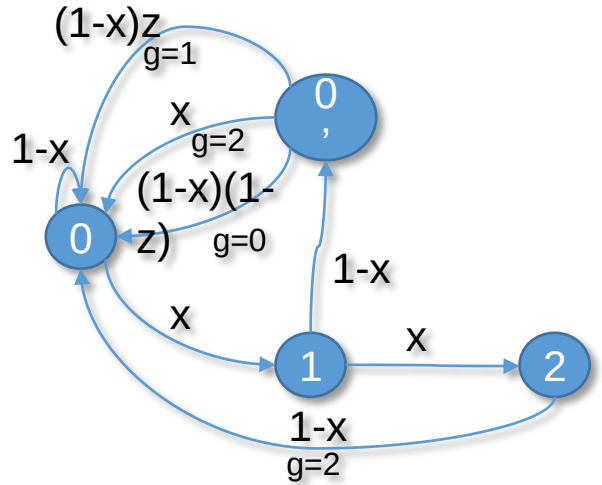
Bloque n+1

Cadena privada



Transición 0' → 0 : Ambas partes ganan





Transición 0’ → 0 : Los atacantes ganan

Cadena pública

Los atacantes ganan dos bloques

Bloque n-1

Bloque n

Bloque n+1

Bloque n+1

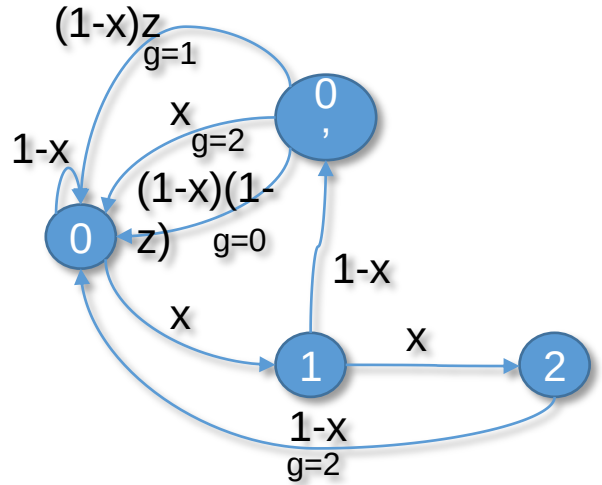
0

Bloque n+2

Publica bloque

Bloque n+1

Cadena privada



Revisitando el ataque del

51%

Número de confirmaciones

% del *hashrate* global

$\alpha \backslash conf$	1	2	3	4	5	6	7	8	9	10
2%	0.24%	0.02%	≈0%	≈0%	≈0%	≈0%	≈0%	≈0%	≈0%	≈0%
6%	2.16%	0.42%	0.09%	0.02%	≈0%	≈0%	≈0%	≈0%	≈0%	≈0%
10%	5.98%	1.85%	0.60%	0.20%	0.07%	0.03%	≈0%	≈0%	≈0%	≈0%
14%	11.66%	4.88%	2.11%	0.93%	0.42%	0.19%	0.09%	0.04%	0.02%	≈0%
18%	19.13%	9.94%	5.32%	2.90%	1.60%	0.89%	0.50%	0.28%	0.16%	0.09%
22%	28.27%	17.33%	10.89%	6.95%	4.48%	2.91%	1.91%	1.25%	0.83%	0.55%
26%	38.90%	27.17%	19.36%	13.97%	10.17%	7.45%	5.49%	4.06%	3.01%	2.23%
30%	50.70%	39.33%	30.98%	24.64%	19.73%	15.88%	12.84%	10.41%	8.46%	6.89%
34%	63.23%	53.37%	45.55%	39.14%	33.81%	29.31%	25.49%	22.21%	19.39%	16.95%
38%	75.80%	68.45%	62.25%	56.85%	52.09%	47.85%	44.03%	40.58%	37.45%	34.56%
42%	87.35%	83.09%	79.31%	75.86%	72.68%	69.72%	66.95%	64.33%	61.83%	59.44%
46%	96.26%	94.88%	93.61%	92.41%	91.27%	90.17%	89.10%	88.05%	86.99%	85.82%
48%	98.98%	98.59%	98.23%	97.88%	97.54%	97.21%	96.88%	96.54%	96.15%	95.60%
50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Fuente: *Bitcoin's Security Model Revisited*. Sompolinsky and Zohar

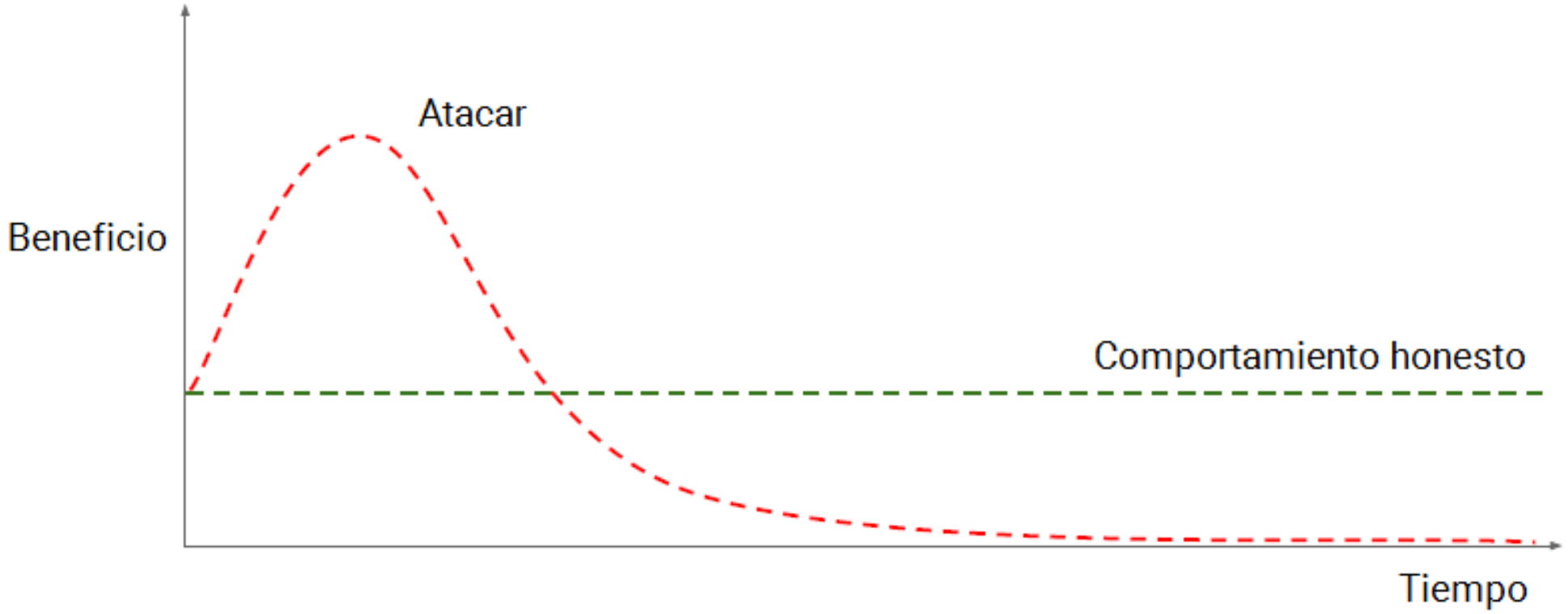
Ataque del minado **egoísta**

- Inicialmente el ataque haría la red más lenta y vulnerable al doble gasto
- Si ganara adeptos, la ventaja del pool egoísta podría ser definitiva

¿Por qué no vemos estos ataques?

- ¿Desconocimiento por parte de los mineros?
- ¿Demasiado riesgo y/o capital necesario?
- ¿Dificultad de beneficiarse del doble gasto?
- ¿Honor entre mineros?

¿Ataco o no ataco?



Ataques entre *pools* de minado

- Resultado presentado en 2015 por Eyal [2]
- Esencialmente, un ataque basado en el minado egoísta aplicado a *pools*.
- **Spoiler**: el actual sistema de *pools* no forma un equilibrio de Nash:
  "Si solo uno de los pools ataca, éste puede incrementar su beneficio"

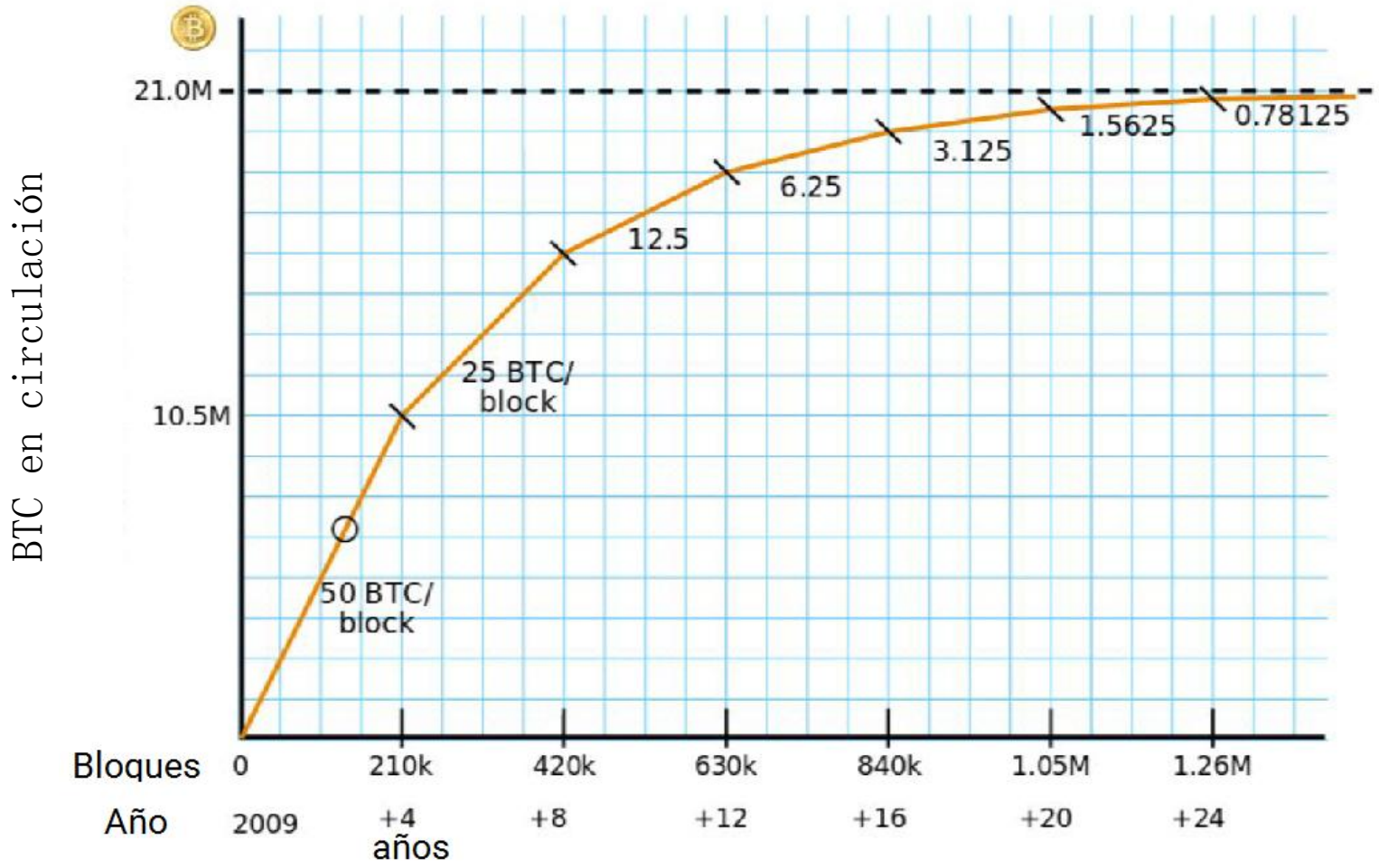
Dilema del minero: dilema del prisionero

Pool 2 \ Pool 1	No atacar	Atacar
No atacar	$(r_1 = 1, r_2 = 1)$	$(r_1 > 1, r_2 = \tilde{r}_2 < 1)$
Atacar	$(r_1 = \tilde{r}_1 < 1, r_2 > 1)$	$(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$

La situación es inestable porque
el ataque puede ser anónimo

Fuente: *Eyal [2]*

Evolución futura de los costes por transacción



Actualmente, la recompensa por bloque produce más del 99% beneficio de un minero

Posibles contramedidas a la centralización

- Debida al coste energético:
  - **Memory-hard proof of work**: pruebas de trabajo que requieren mucha memoria RAM, luego los ASICs no dan ventaja adicional.
  - Algunas propuestas o sistemas que las usen:
    - *Ethereum* (Ethash).
    - *Equihash* (propuesta académica) [4]
- Debida al control de los desarrolladores *core*:
  - **Futarquía**: modelo descentralizado de gobernanza [5]
  - Propuestas en sistemas relacionados:
    - Gobernanza de DAOs.
    - Blockchains autorregulables (Tezos) [6]

NO existe un buen modelo formal de la seguridad

- La cadena de bloques funciona en la práctica, pero no en teoría
- Es muy difícil analizar el impacto de las cuestiones abiertas:
  - Minado egoísta, ataques entre *pools*
  - Evolución futura de las fees
  - Modelo de gobernanza
  - Otras pruebas de trabajo

Referencias

[1] Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamoto. 2008

[2] The Miner's Dilemma. Ittay Eyal. 2015

[3] A Longitudinal Study of Bitcoin Transaction Fees. Möser and Böhme. 2015

[4] Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. Biryukov, Khovratovich. 2015

[5] An Introduction to Futarchy. Buterin. 2014

[6] Tezos: A Self-Amending Crypto-Ledger Position Paper. Goodman. 2014