BCCon 全球区块链生态技术大会
Global Blockchain Eco-Technology Conference

几种挖矿攻击及其相关缓解措施

彭峙酿

360核心安全安全研究员

主办方 Geekbang 极客邦科技 InfoQ

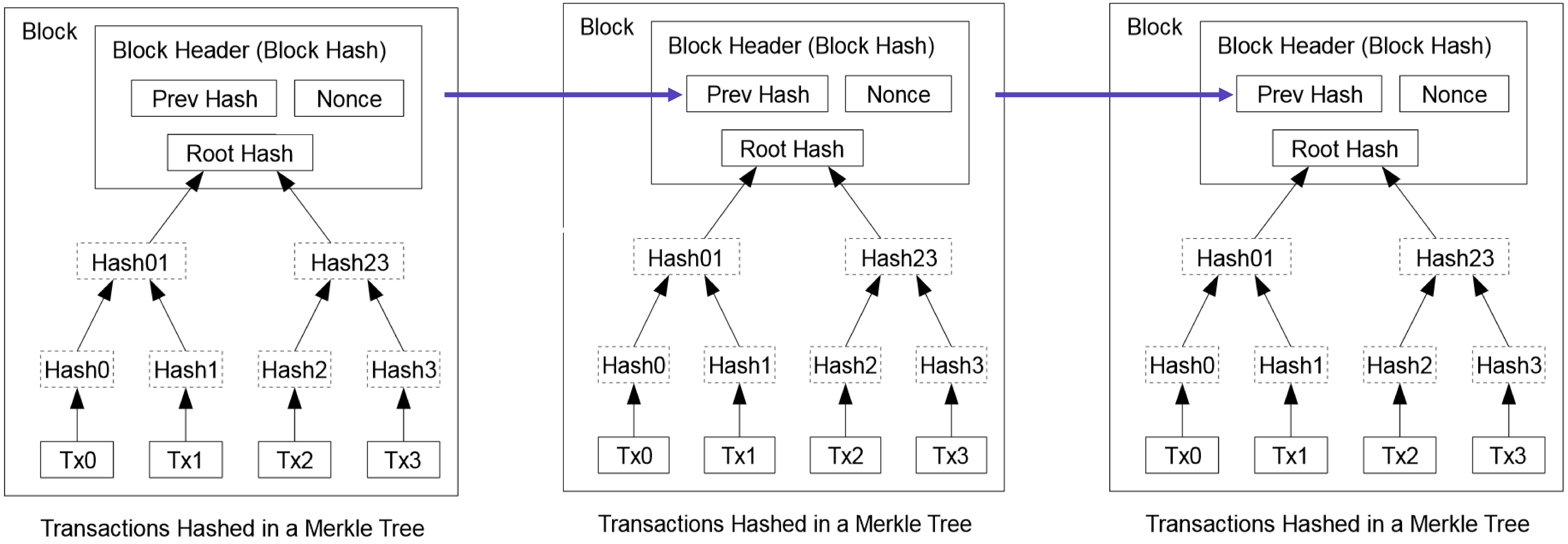
TABLE OF

CONTENS 大纲

- 基础概念
- 双花攻击
- 跳币攻击
- 自私挖矿
- 攻击矿池

基础概念

区块链



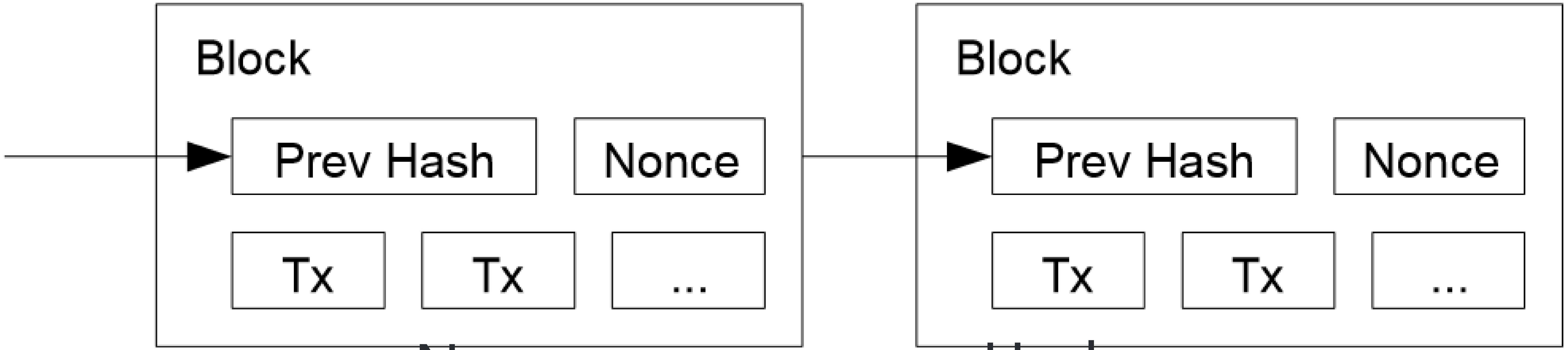
区块链接成链

每个区块头包含了上一个区块头的哈希值

工作量证明(Proof-of-Work)

比特币工作量证明算法：SHA256

持续增加Nonce值，直到找到



内容

Nonce

Hash

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

满足条件

挖矿

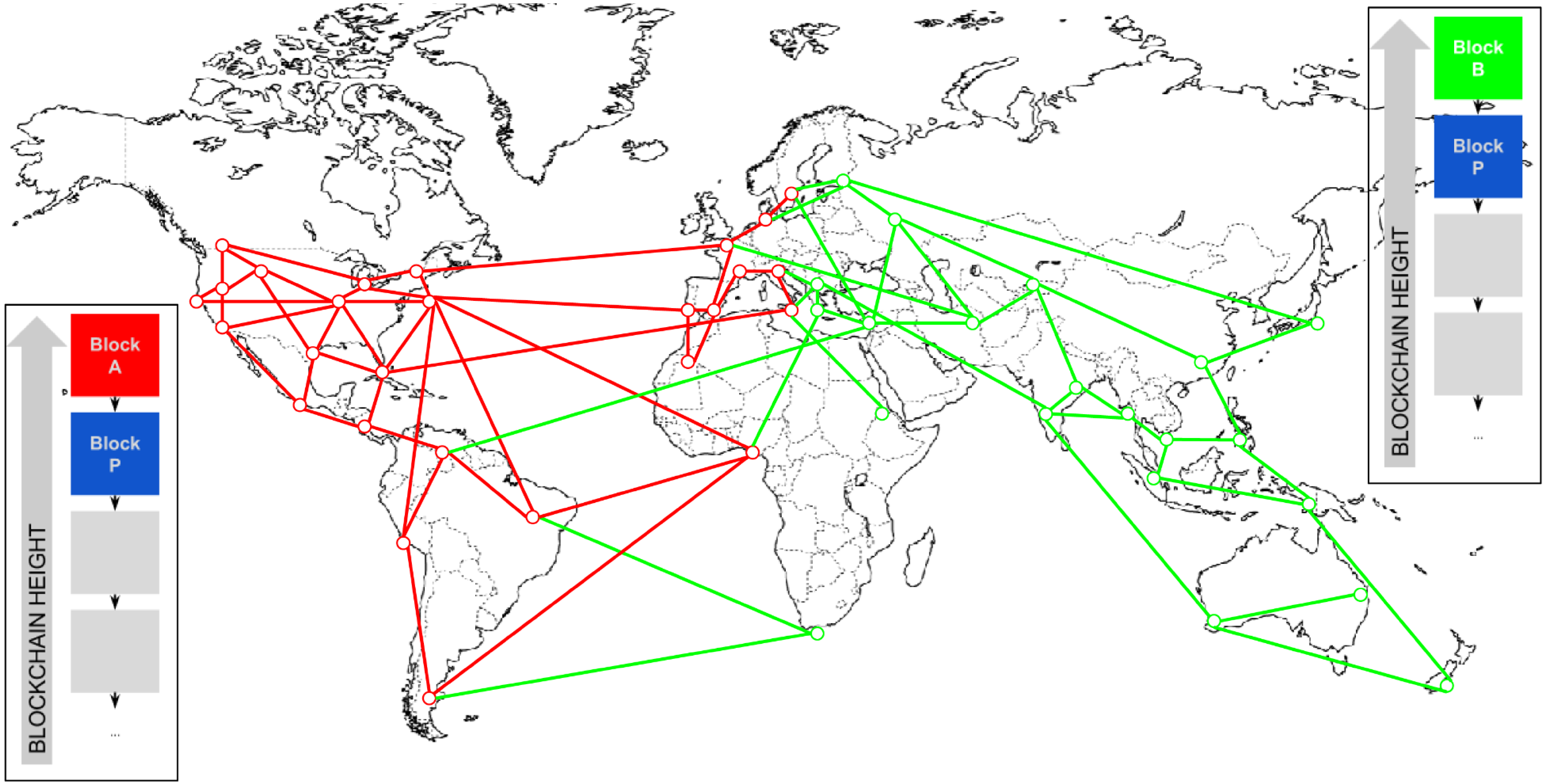
PoW计算被称为 挖矿

挖矿的人被称为 矿工

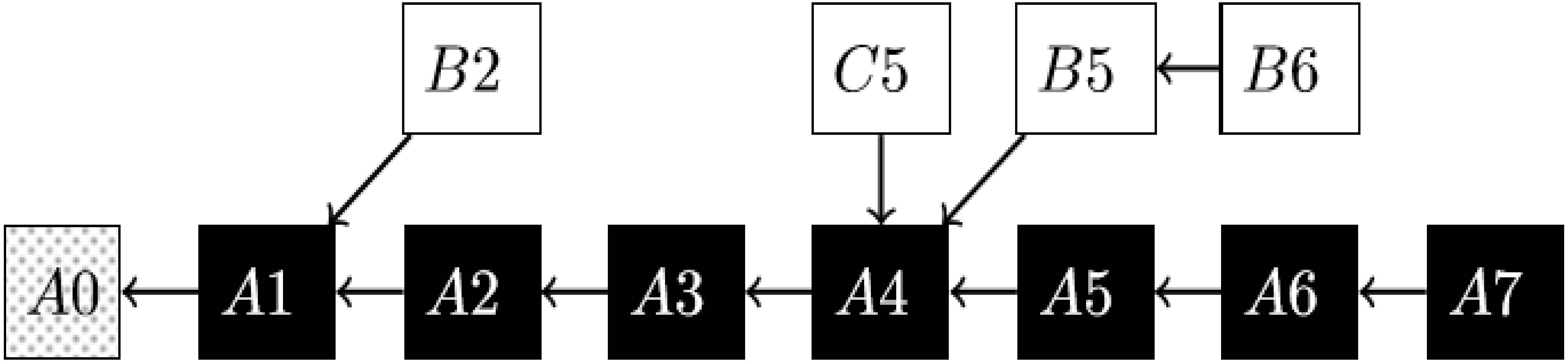
奖励：矿工费 交易手续费（≈12.5BTC）

本质：随机选择下一个出块者

分叉


Block
A
Block
P
...
BLOCKCHAIN HEIGHT
Block
B
Block
P
...
BLOCKCHAIN HEIGHT

分叉



选取工作量最大的链作为当前链

几种挖矿攻击

双花攻击

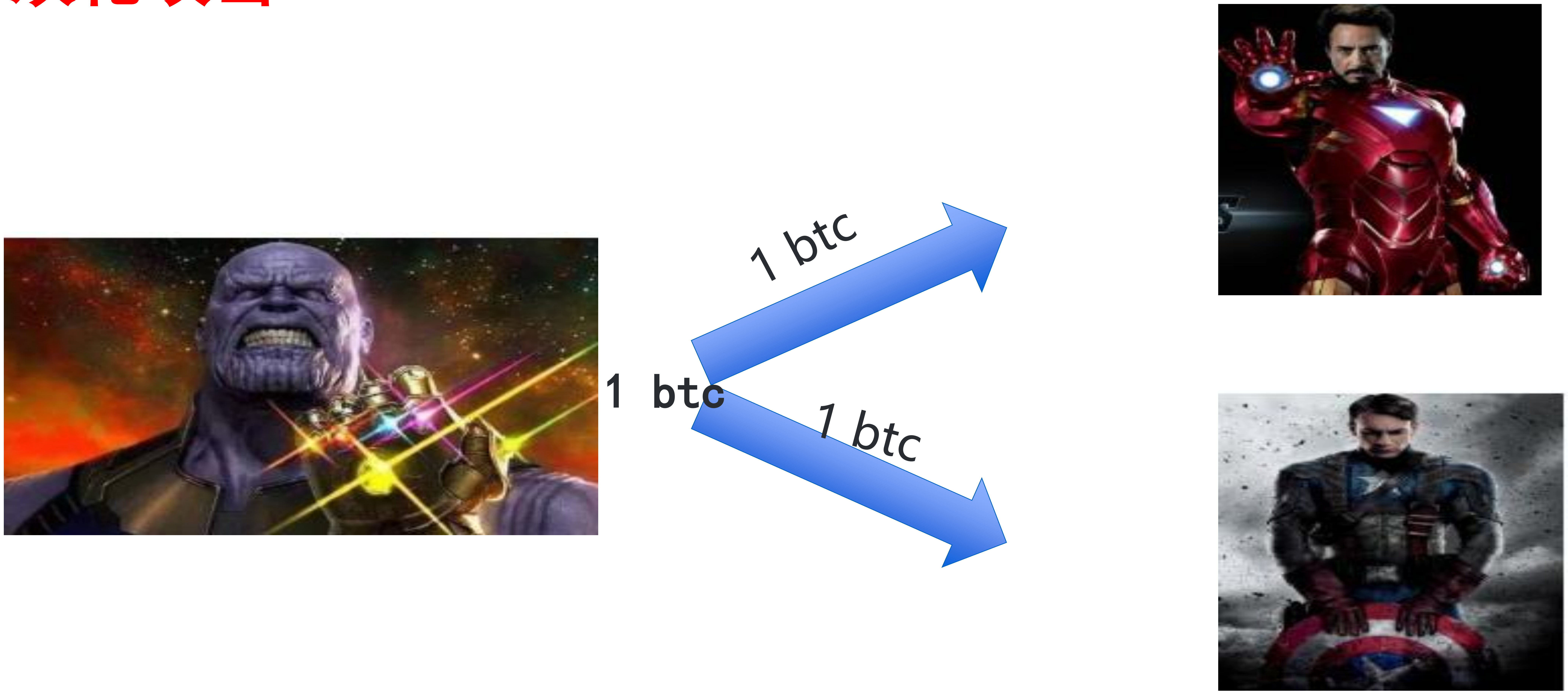
跳币攻击

自私挖矿

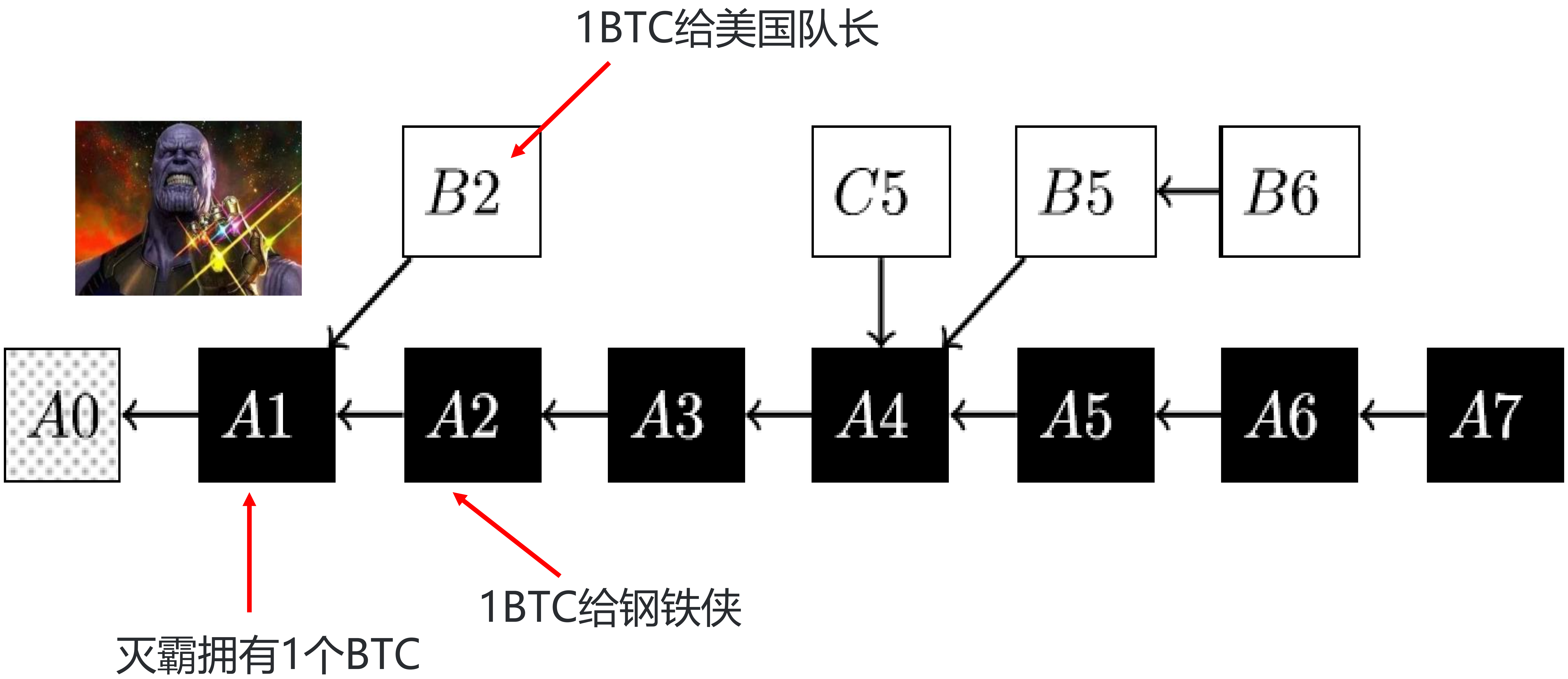
攻击矿池

双花攻击

双花攻击



分叉


1BTC给美国队长
B2
C5
B5
B6
A0
A1
A2
A3
A4
A5
A6
A7
1BTC给钢铁侠
灭霸拥有1个BTC

双花攻击

Finney攻击

竞争攻击

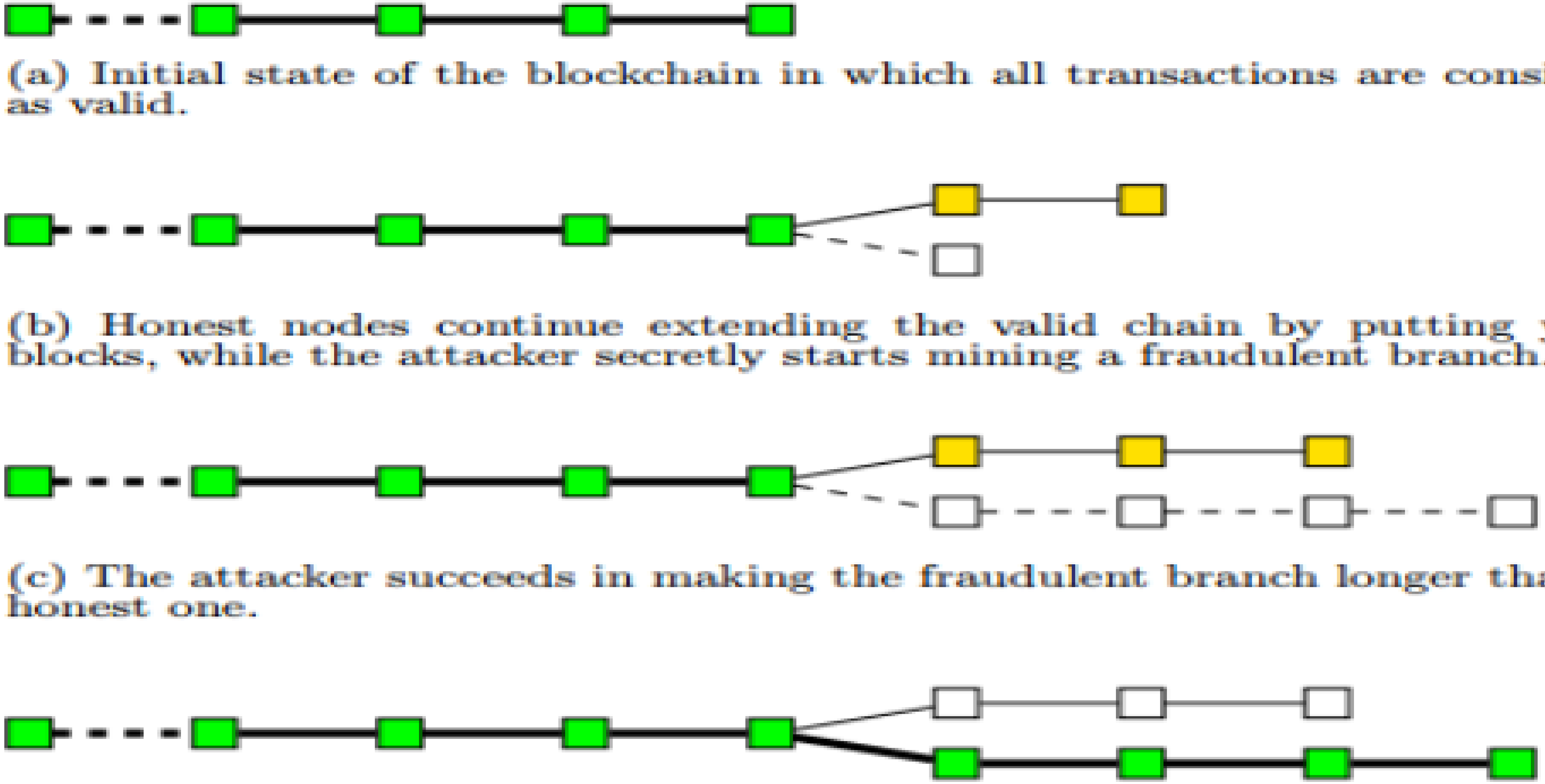
暴力搜索

Vector 76攻击

51%攻击

…

51%攻击



(a) Initial state of the blockchain in which all transactions are considered as valid.

(b) Honest nodes continue extending the valid chain by putting yellow blocks, while the attacker secretly starts mining a fraudulent branch.

(c) The attacker succeeds in making the fraudulent branch longer than the honest one.

(d) The attacker's branch is published and is now considered the valid one.

小于50%算力

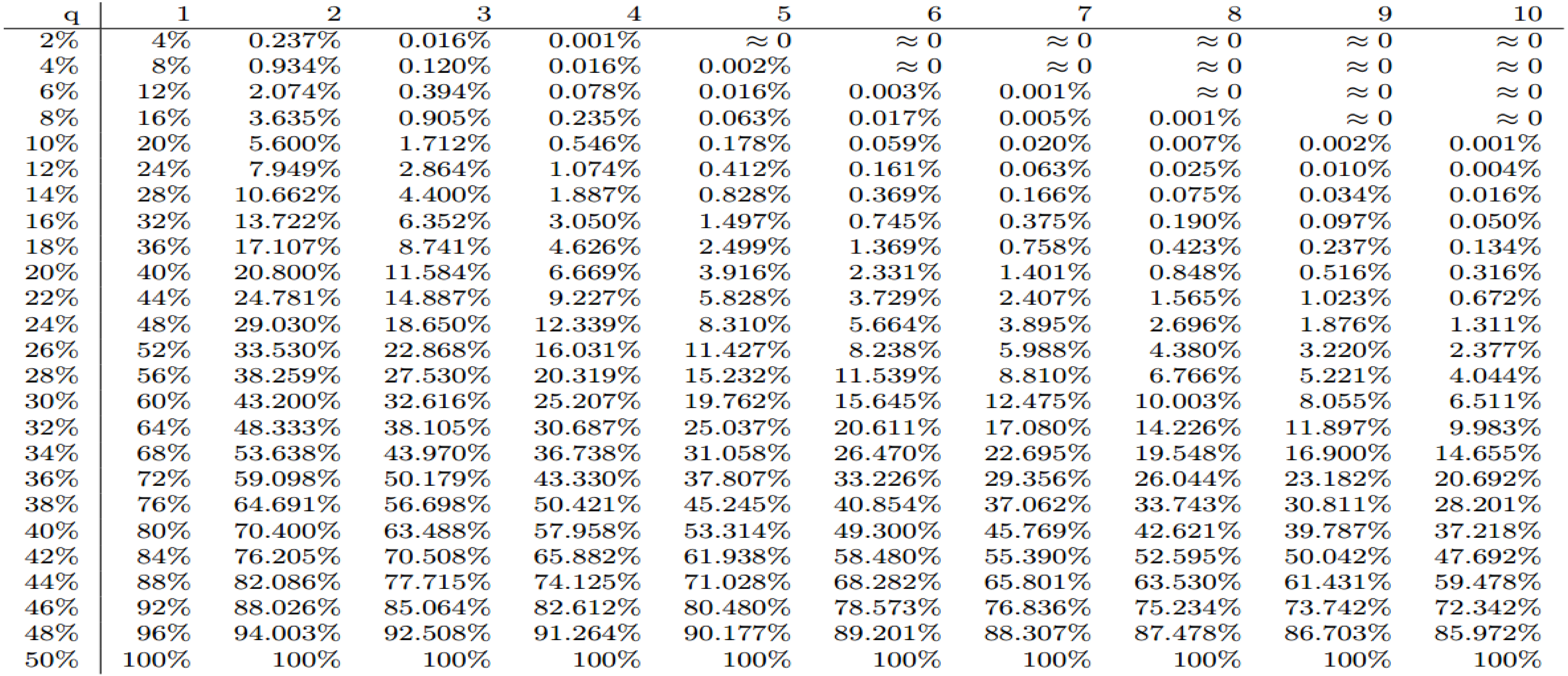
攻击者的算力：$q < 50\%$

防御策略：等待 n 个块确认

小于50%算力下攻击成功率：

$$r = 1 - \sum_{m=0}^{n} \binom{m+n-1}{m} \cdot ((1-\mathrm{q})^{\mathrm{n}}\mathrm{q}^{\mathrm{m}} - (1-\mathrm{q})^{\mathrm{m}}\mathrm{q}^{\mathrm{n}})$$

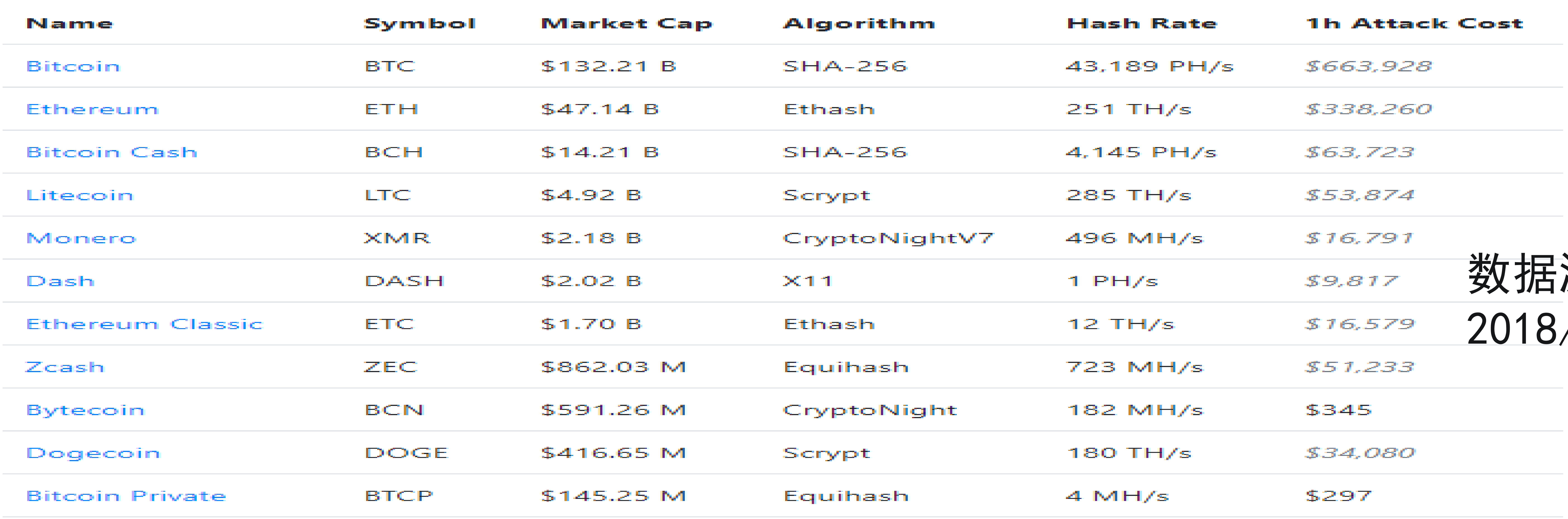
攻击成功率



q	1	2	3	4	5	6	7	8	9	10
2%	4%	0.237%	0.016%	0.001%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
4%	8%	0.934%	0.120%	0.016%	0.002%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
6%	12%	2.074%	0.394%	0.078%	0.016%	0.003%	0.001%	≈ 0	≈ 0	≈ 0
8%	16%	3.635%	0.905%	0.235%	0.063%	0.017%	0.005%	0.001%	≈ 0	≈ 0
10%	20%	5.600%	1.712%	0.546%	0.178%	0.059%	0.020%	0.007%	0.002%	0.001%
12%	24%	7.949%	2.864%	1.074%	0.412%	0.161%	0.063%	0.025%	0.010%	0.004%
14%	28%	10.662%	4.400%	1.887%	0.828%	0.369%	0.166%	0.075%	0.034%	0.016%
16%	32%	13.722%	6.352%	3.050%	1.497%	0.745%	0.375%	0.190%	0.097%	0.050%
18%	36%	17.107%	8.741%	4.626%	2.499%	1.369%	0.758%	0.423%	0.237%	0.134%
20%	40%	20.800%	11.584%	6.669%	3.916%	2.331%	1.401%	0.848%	0.516%	0.316%
22%	44%	24.781%	14.887%	9.227%	5.828%	3.729%	2.407%	1.565%	1.023%	0.672%
24%	48%	29.030%	18.650%	12.339%	8.310%	5.664%	3.895%	2.696%	1.876%	1.311%
26%	52%	33.530%	22.868%	16.031%	11.427%	8.238%	5.988%	4.380%	3.220%	2.377%
28%	56%	38.259%	27.530%	20.319%	15.232%	11.539%	8.810%	6.766%	5.221%	4.044%
30%	60%	43.200%	32.616%	25.207%	19.762%	15.645%	12.475%	10.003%	8.055%	6.511%
32%	64%	48.333%	38.105%	30.687%	25.037%	20.611%	17.080%	14.226%	11.897%	9.983%
34%	68%	53.638%	43.970%	36.738%	31.058%	26.470%	22.695%	19.548%	16.900%	14.655%
36%	72%	59.098%	50.179%	43.330%	37.807%	33.226%	29.356%	26.044%	23.182%	20.692%
38%	76%	64.691%	56.698%	50.421%	45.245%	40.854%	37.062%	33.743%	30.811%	28.201%
40%	80%	70.400%	63.488%	57.958%	53.314%	49.300%	45.769%	42.621%	39.787%	37.218%
42%	84%	76.205%	70.508%	65.882%	61.938%	58.480%	55.390%	52.595%	50.042%	47.692%
44%	88%	82.086%	77.715%	74.125%	71.028%	68.282%	65.801%	63.530%	61.431%	59.478%
46%	92%	88.026%	85.064%	82.612%	80.480%	78.573%	76.836%	75.234%	73.742%	72.342%
48%	96%	94.003%	92.508%	91.264%	90.177%	89.201%	88.307%	87.478%	86.703%	85.972%
50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

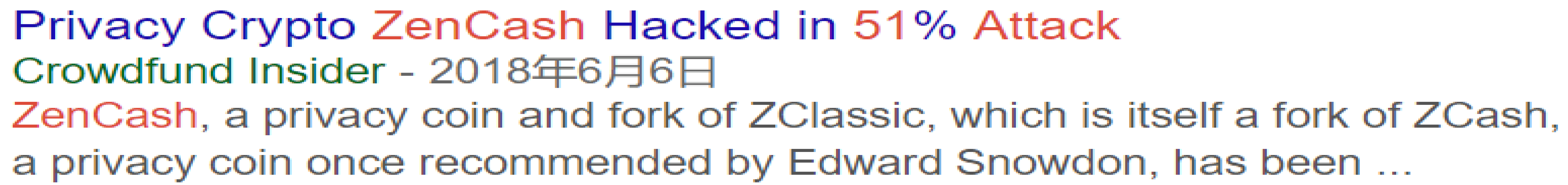
Table 1: The probability of a successful double spend, as a function of the attacker's hashrate q and the number of confirmations n.

51%攻击的实际成本



Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost
Bitcoin	BTC	$132.21 B	SHA-256	43,189 PH/s	$663,928
Ethereum	ETH	$47.14 B	Ethash	251 TH/s	$338,260
Bitcoin Cash	BCH	$14.21 B	SHA-256	4,145 PH/s	$63,723
Litecoin	LTC	$4.92 B	Scrypt	285 TH/s	$53,874
Monero	XMR	$2.18 B	CryptoNightV7	496 MH/s	$16,791
Dash	DASH	$2.02 B	X11	1 PH/s	$9,817
Ethereum Classic	ETC	$1.70 B	Ethash	12 TH/s	$16,579
Zcash	ZEC	$862.03 M	Equihash	723 MH/s	$51,233
Bytecoin	BCN	$591.26 M	CryptoNight	182 MH/s	$345
Dogecoin	DOGE	$416.65 M	Scrypt	180 TH/s	$34,080
Bitcoin Private	BTCP	$145.25 M	Equihash	4 MH/s	$297

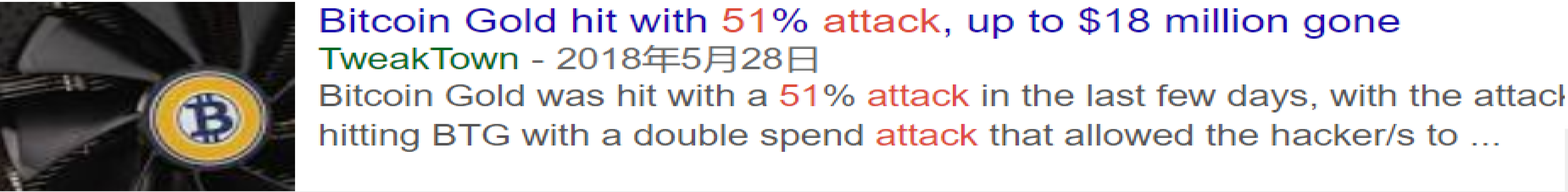
数据源:crypto51.app
2018/7/23



Privacy Crypto ZenCash Hacked in 51% Attack

Crowdfund Insider - 2018年6月6日

ZenCash, a privacy coin and fork of ZClassic, which is itself a fork of ZCash, a privacy coin once recommended by Edward Snowdon, has been ...



Bitcoin Gold hit with 51% attack, up to $18 million gone

TweakTown - 2018年5月28日

Bitcoin Gold was hit with a 51% attack in the last few days, with the attacl hitting BTG with a double spend attack that allowed the hacker/s to ...

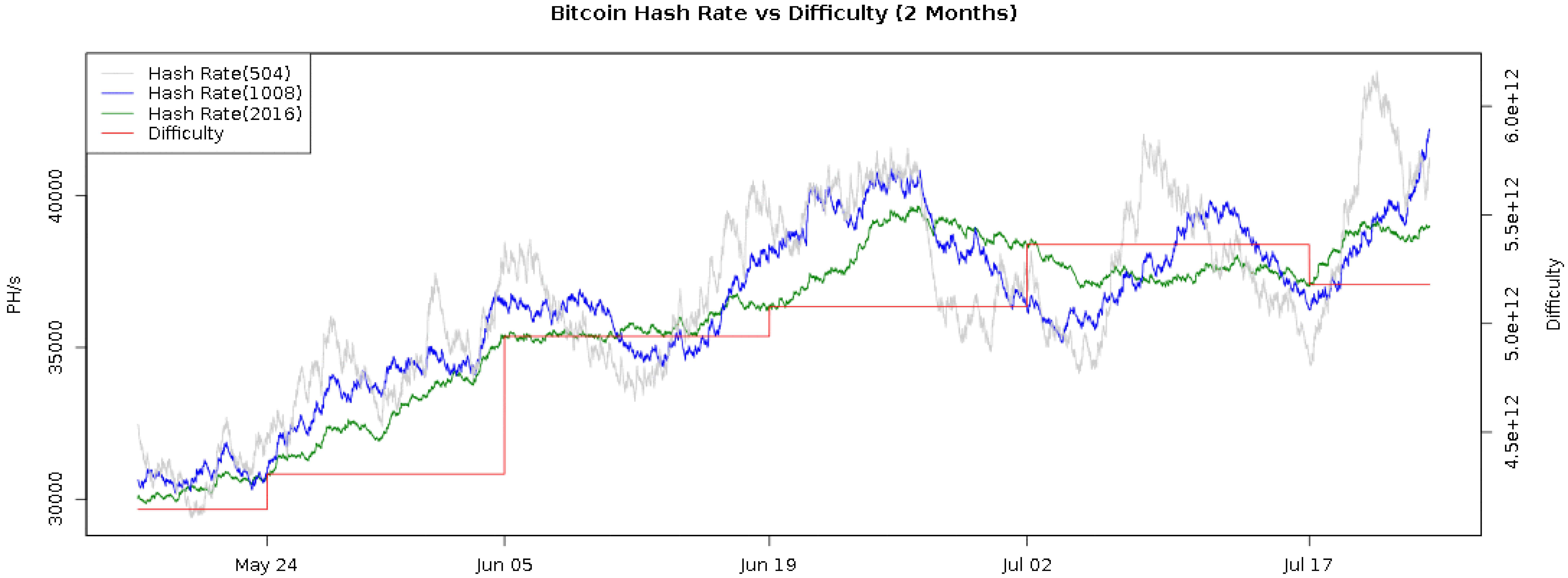
缓解措施

增大确认数N
监控网络
设置检查点

跳币攻击

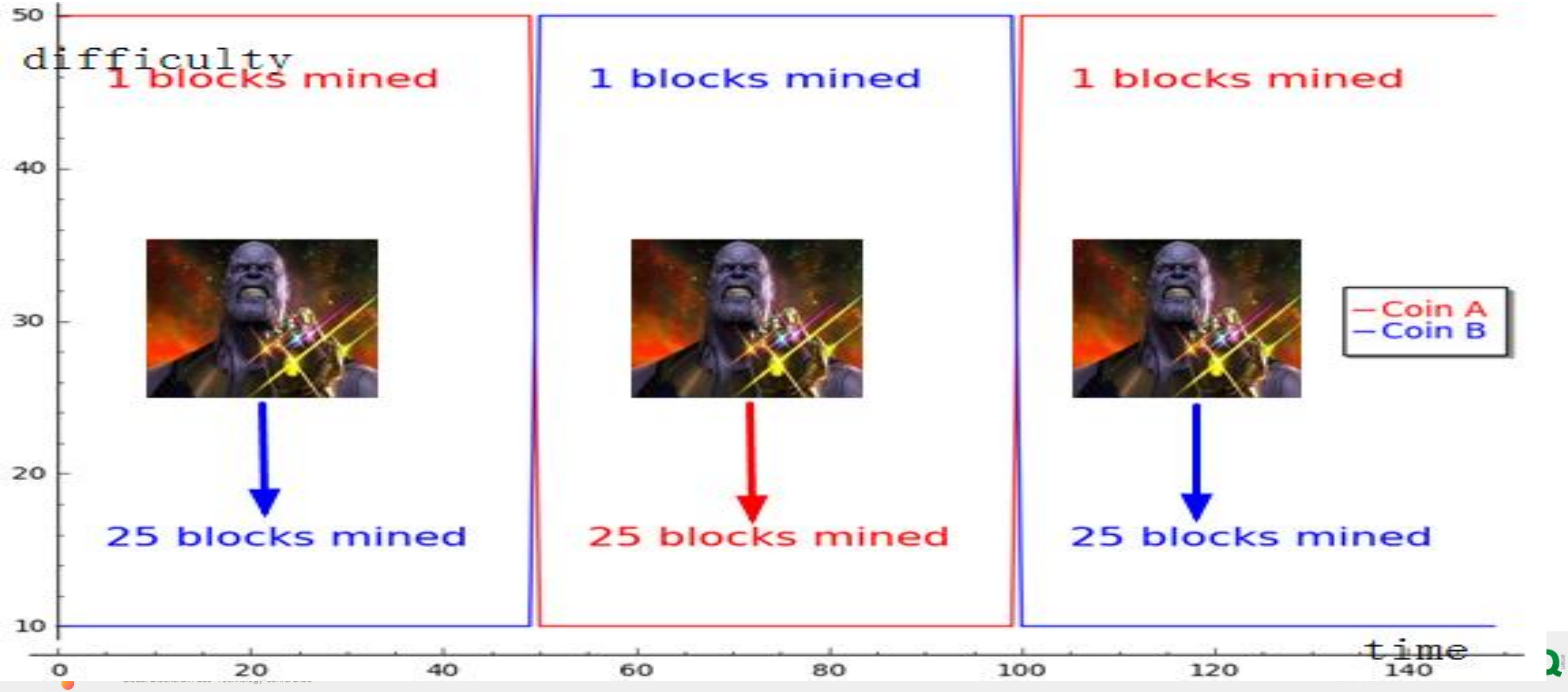
比特币难度调整算法

下一块难度=当前难度*(目标出块时间)/当前出块时间

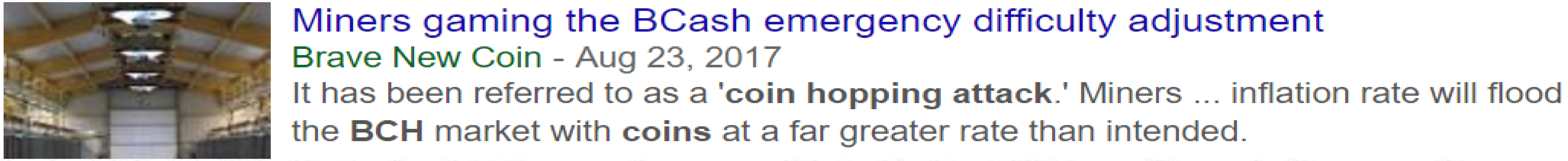


跳池攻击

攻击者算力：4X
A币诚实矿工算力：1X
B币诚实矿工算力：1X



BCH紧急难度调整算法

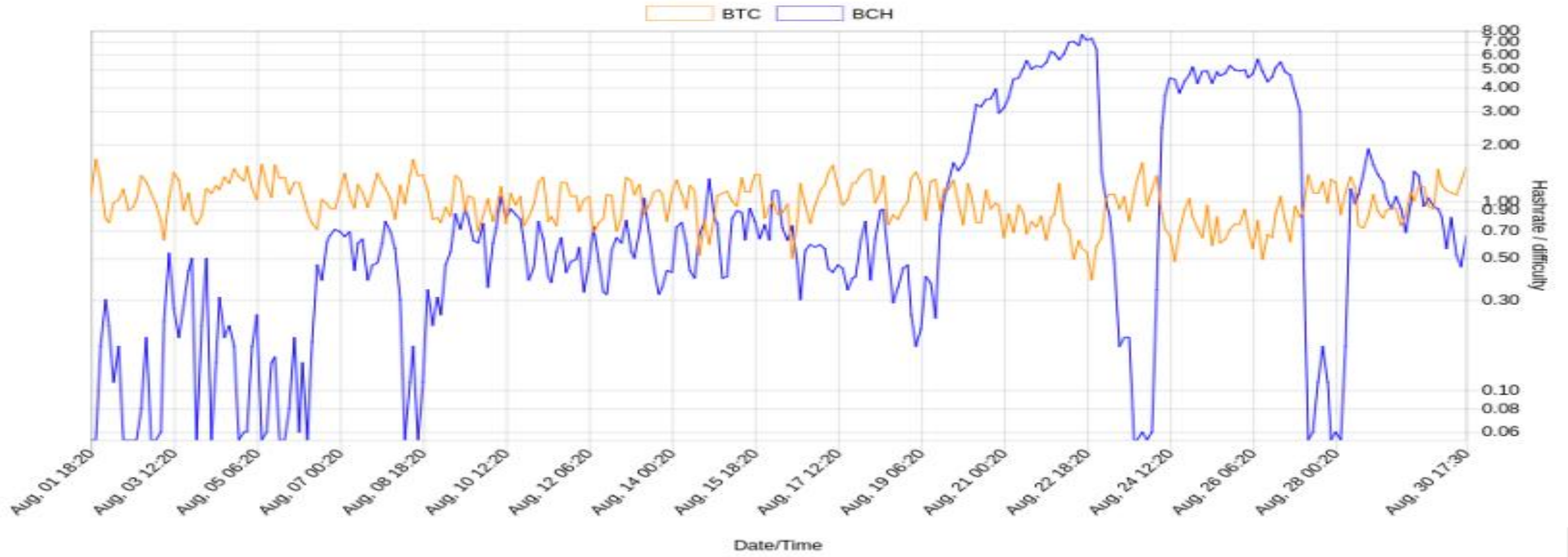


Miners gaming the BCash emergency difficulty adjustment

Brave New Coin - Aug 23, 2017

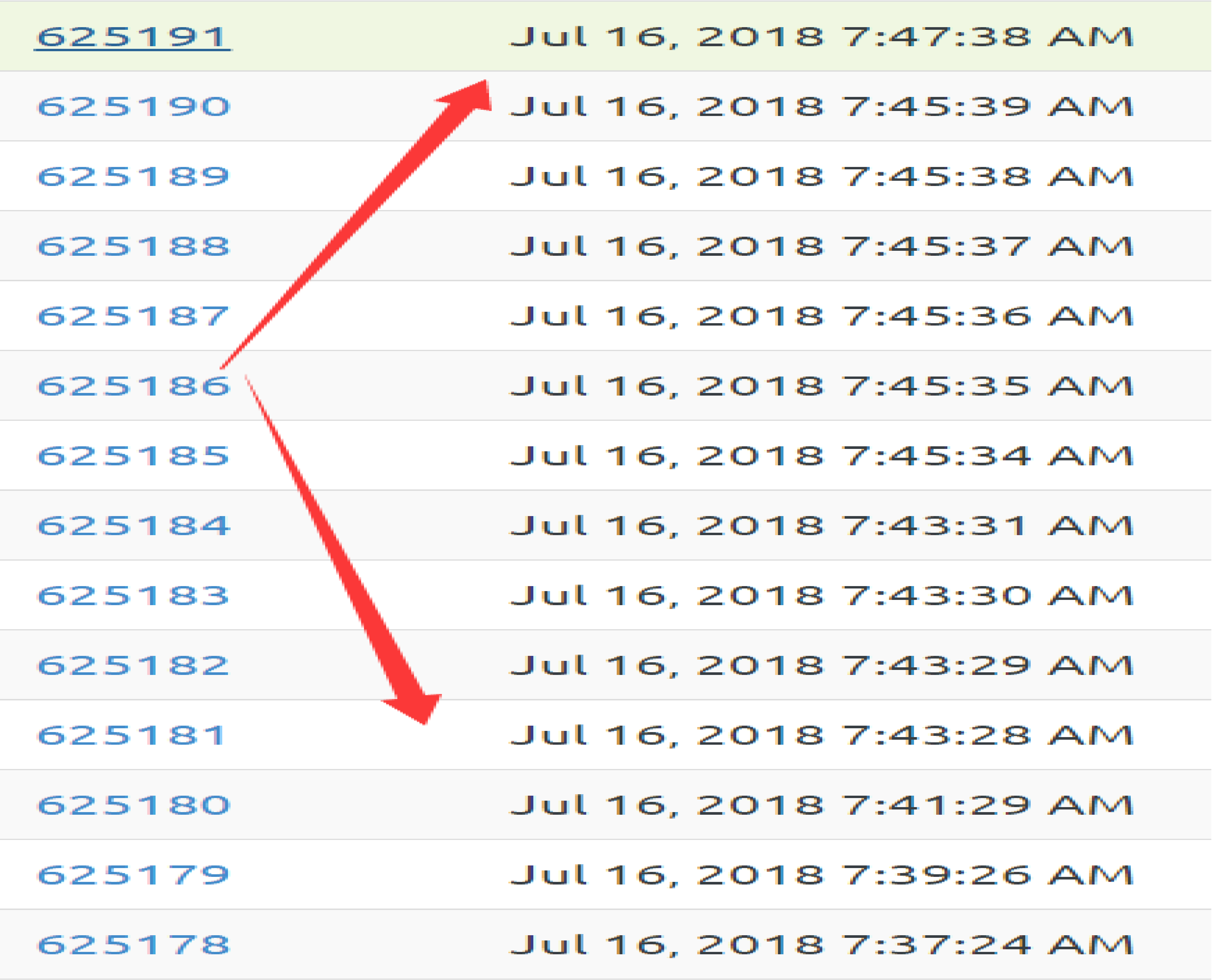
It has been referred to as a '**coin hopping attack**.' Miners ... inflation rate will flood the **BCH** market with **coins** at a far greater rate than intended.

Hashrate divided by difficulty. A ratio of > 1.0 means (on average) faster blocks, < 1.0 slower. (log scale, 3h averages)



跳池攻击（针对小币）

十倍算力攻击者（比特币糖果）：



625191	Jul 16, 2018 7:47:38 AM
625190	Jul 16, 2018 7:45:39 AM
625189	Jul 16, 2018 7:45:38 AM
625188	Jul 16, 2018 7:45:37 AM
625187	Jul 16, 2018 7:45:36 AM
625186	Jul 16, 2018 7:45:35 AM
625185	Jul 16, 2018 7:45:34 AM
625184	Jul 16, 2018 7:43:31 AM
625183	Jul 16, 2018 7:43:30 AM
625182	Jul 16, 2018 7:43:29 AM
625181	Jul 16, 2018 7:43:28 AM
625180	Jul 16, 2018 7:41:29 AM
625179	Jul 16, 2018 7:39:26 AM
625178	Jul 16, 2018 7:37:24 AM

其他攻击技巧：

- 时间戳修改
- 时间劫持
- 扣块
- 丢块
- 自私挖矿
- ……

缓解措施

变种DAA算法:

- Zawy算法
- Digshield算法
- Dark Gravity Wave算法
- MIDAS算法
- ……

困难点:

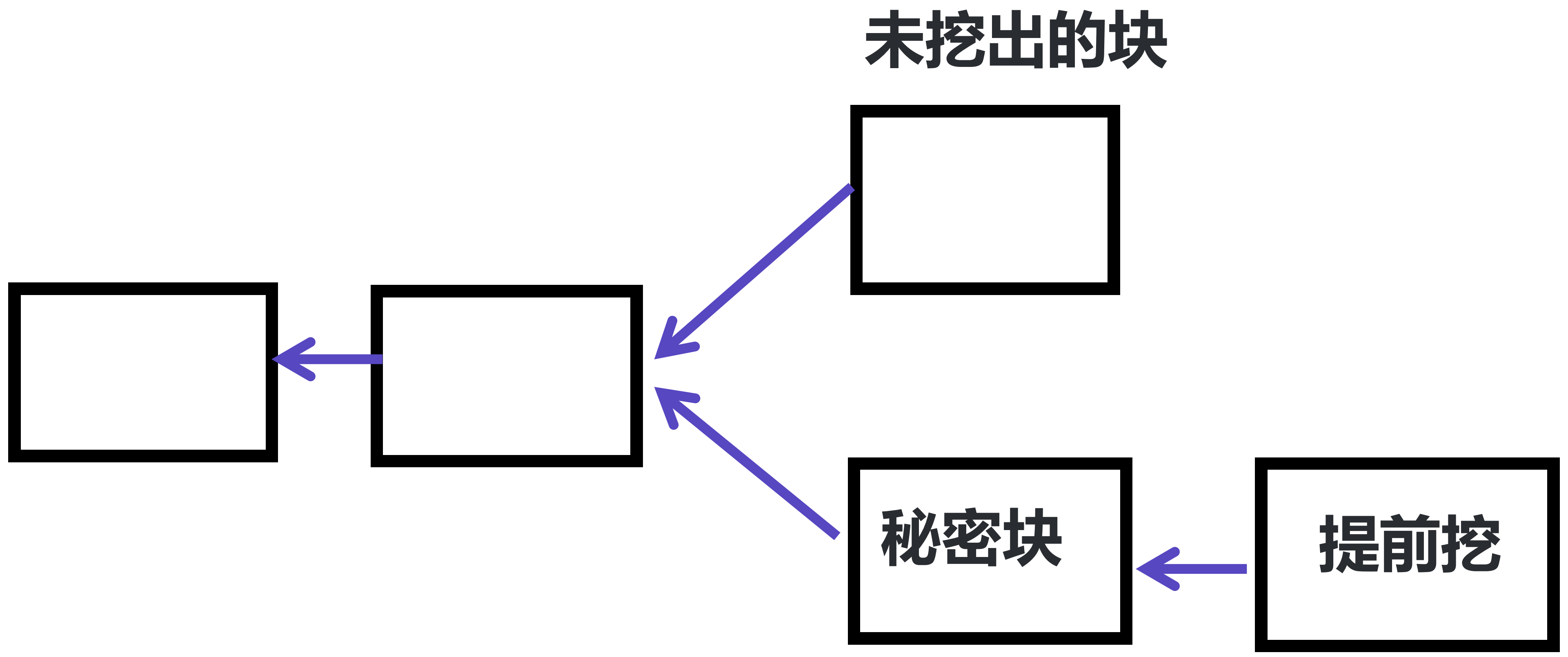
1. 抵抗多种攻击技巧
2. 数学上消除攻击者优势
3. 常数出块时间

DAA攻击仿真:

https://github.com/edwardz246003/DAA_simulator

自私挖矿

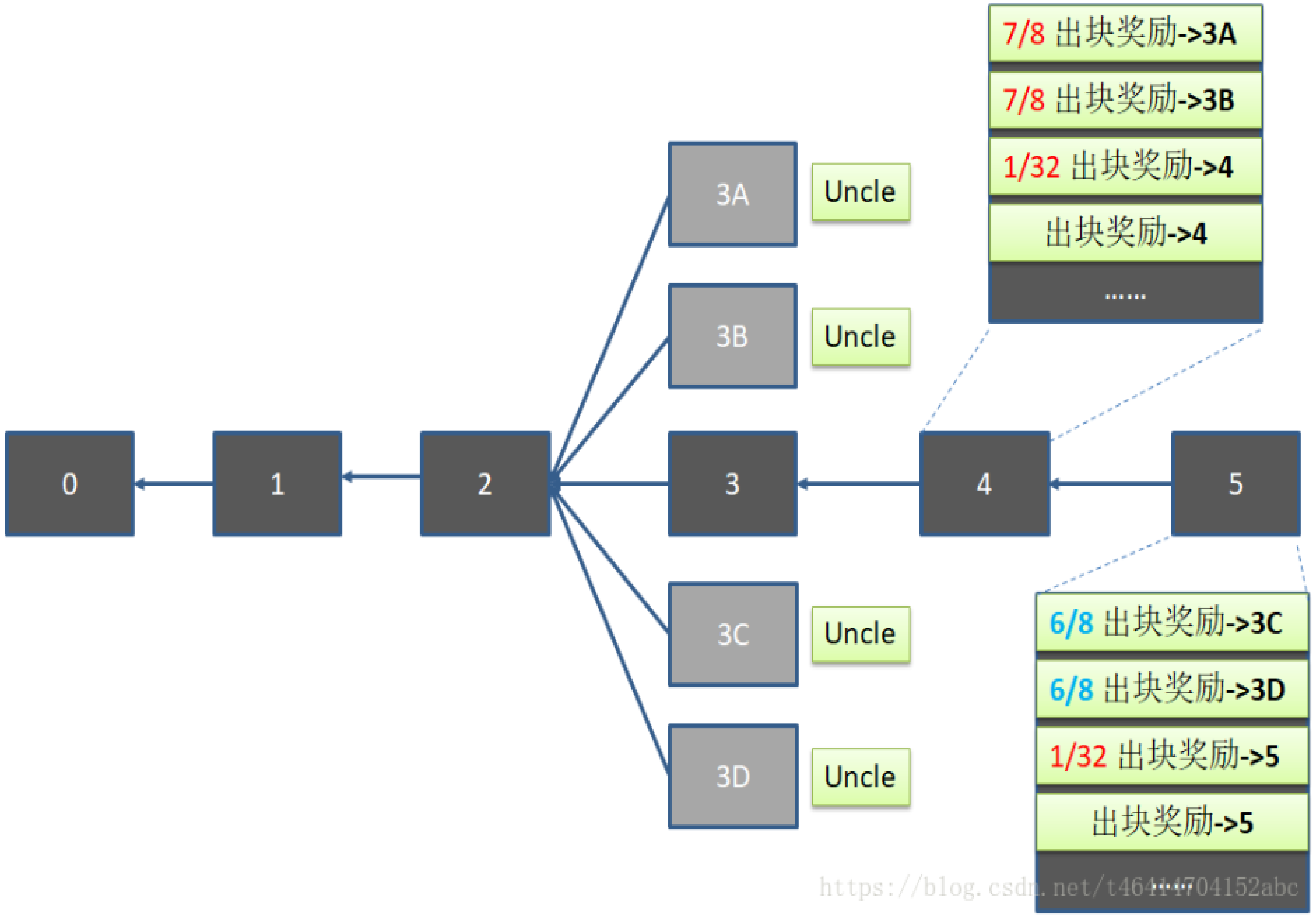
比特币自私挖矿



主动产生分叉
让诚实矿工在无效块上浪费时间
需要更强的网络能力
理论可行

Uncle mining

以太坊出块时间15s
网络延迟可能带来更大的分叉
GHOST协议

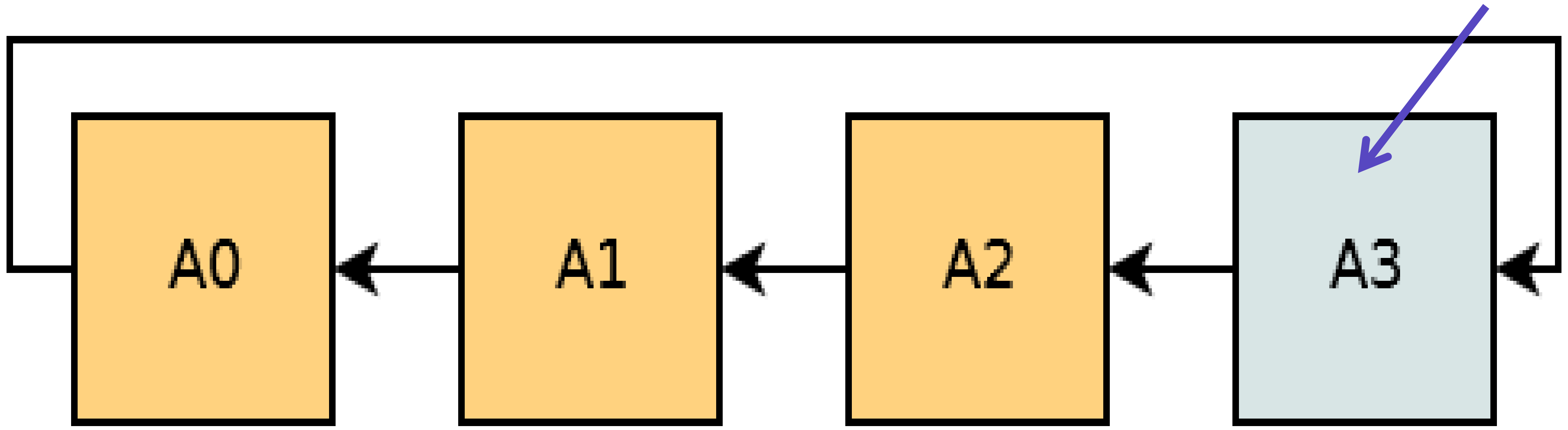


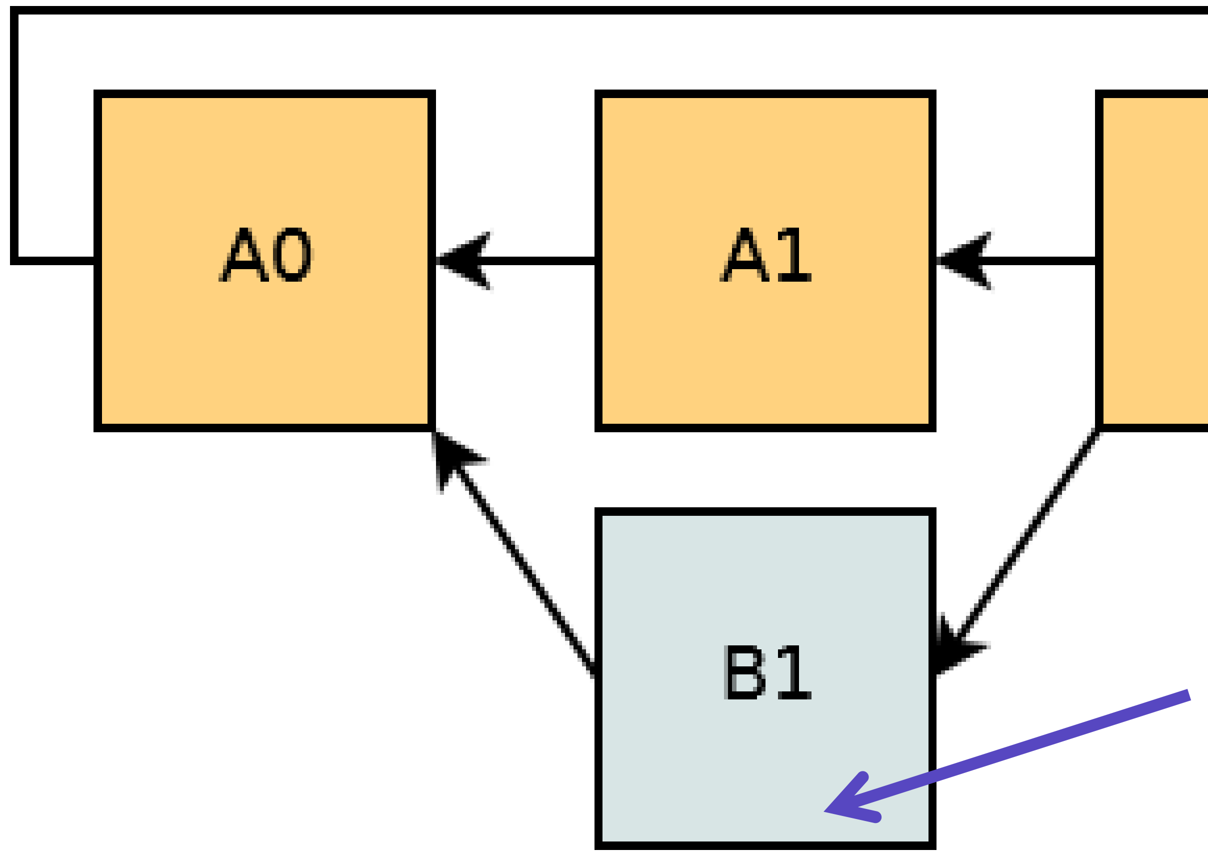
Uncle mining

以太坊出块时间15s
网络延迟可能带来更大的分叉
GHOST协议

Uncle mining

正常矿工(假设有25%算力)
收益为R*1/4 (R为每个块产出)





Uncle mining
出块难度为3/4
收益为:R*1/3*7/8≈R*0.29

诚实矿工收益：R*0.33!
以太坊挖矿：非竞争/非零和

攻击矿池

针对矿池的攻击

跳池攻击

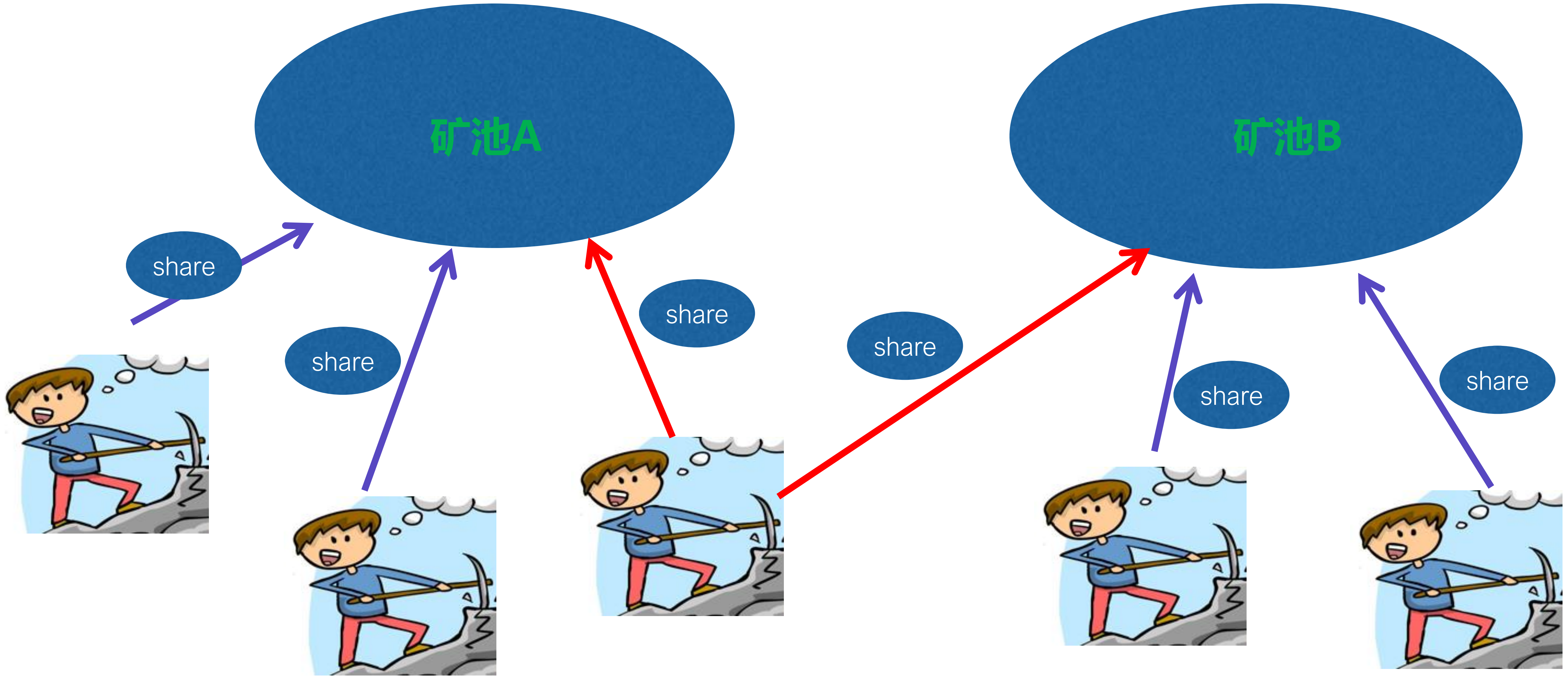
扣块攻击

智能合约增强

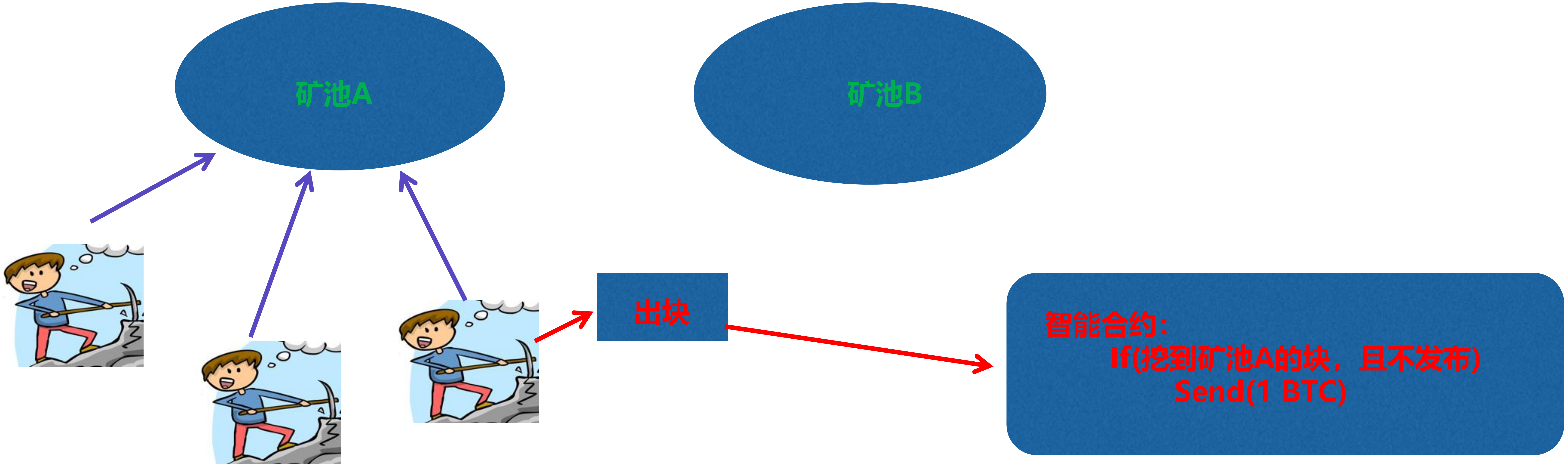
虚假算力攻击

…

跳池攻击

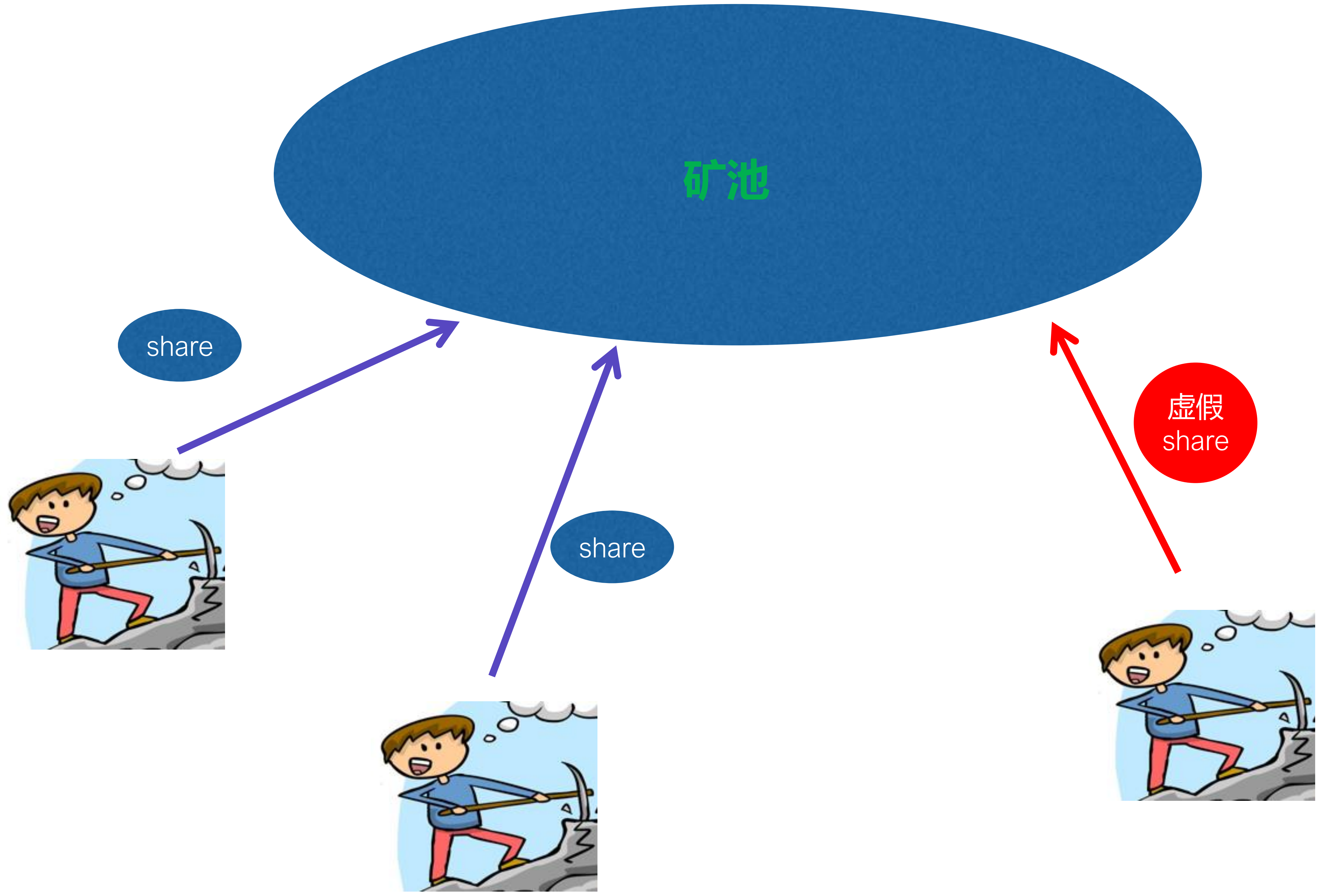


扣块攻击



智能合约：
If(挖到矿池A的块，且不发布)
Send(1 BTC)

虚假算力攻击



Equihash verifier漏洞

Equihashverify:

https://github.com/joshuayabut/equihashverify

z-nomp使用

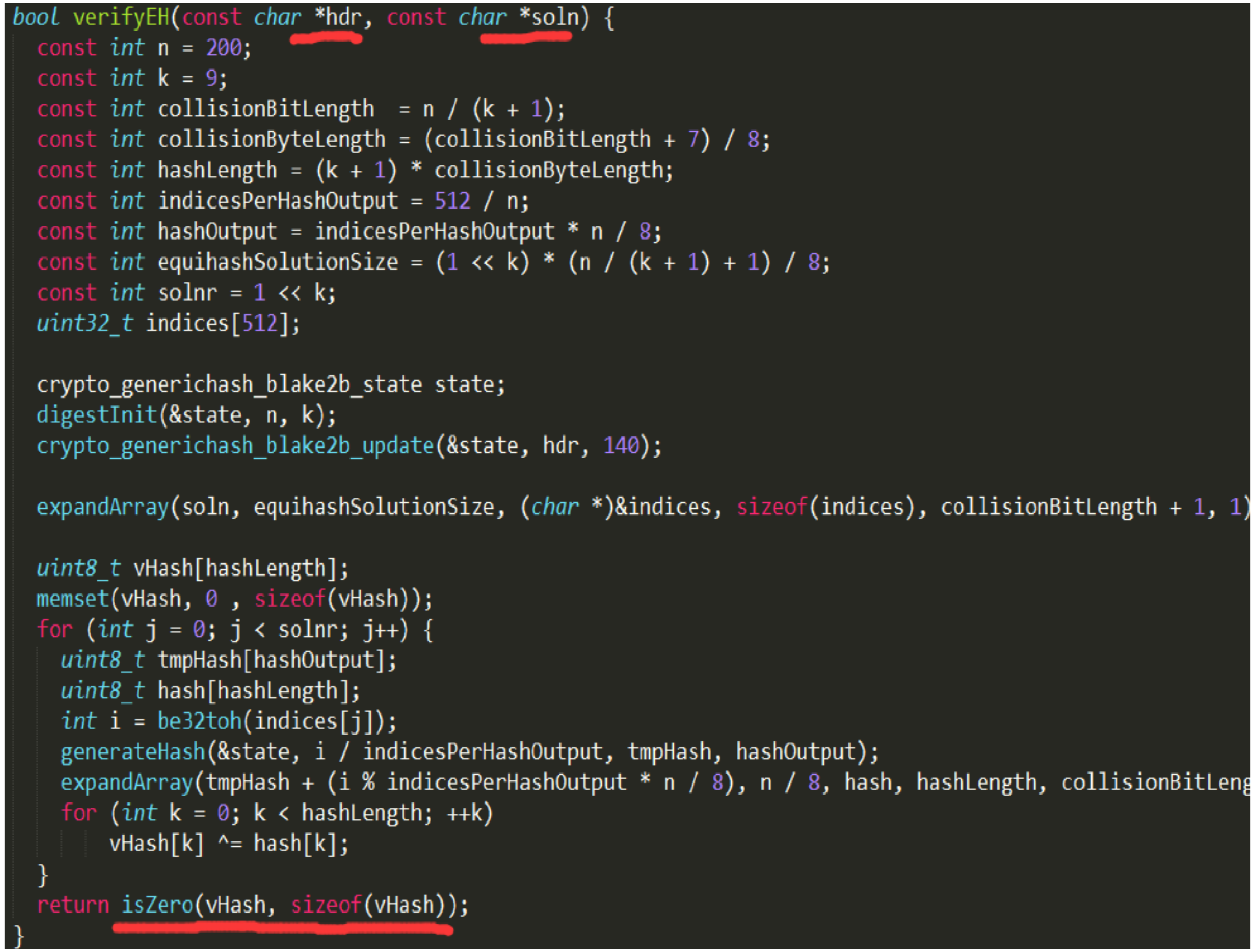
Equihash算法的错误实现

攻击者产生假算力

受到影响的数字货币:

Zcash, Bitcoin Gold, Zencash, Bitcoin Private, Zclassic, Komodo, Hush, BitcoinZ, Bitcoin Candy, NewBTG, Bitcoin Faith, Bitcoin nano, Bitcoin pizza, Bitocin world ……

Equihash verifier漏洞



```
bool verifyEH(const char *hdr, const char *soln) {
  const int n = 200;
  const int k = 9;
  const int collisionBitLength  = n / (k + 1);
  const int collisionByteLength = (collisionBitLength + 7) / 8;
  const int hashLength = (k + 1) * collisionByteLength;
  const int indicesPerHashOutput = 512 / n;
  const int hashOutput = indicesPerHashOutput * n / 8;
  const int equihashSolutionSize = (1 << k) * (n / (k + 1) + 1) / 8;
  const int solnr = 1 << k;
  uint32_t indices[512];

  crypto_generichash_blake2b_state state;
  digestInit(&state, n, k);
  crypto_generichash_blake2b_update(&state, hdr, 140);

  expandArray(soln, equihashSolutionSize, (char *)&indices, sizeof(indices), collisionBitLength + 1, 1)

  uint8_t vHash[hashLength];
  memset(vHash, 0 , sizeof(vHash));
  for (int j = 0; j < solnr; j++) {
    uint8_t tmpHash[hashOutput];
    uint8_t hash[hashLength];
    int i = be32toh(indices[j]);
    generateHash(&state, i / indicesPerHashOutput, tmpHash, hashOutput);
    expandArray(tmpHash + (i % indicesPerHashOutput * n / 8), n / 8, hash, hashLength, collisionBitLeng
    for (int k = 0; k < hashLength; ++k)
        vHash[k] ^= hash[k];
  }
  return isZero(vHash, sizeof(vHash));
}
```

hash(hdr, x1)^ hash(hdr, x2) ^…^ ^…^. hash(hdr, x512)

没有检查重复值

$$\{x_1=1, x_2=1, x_3=1, \cdots, x_{512}=1\}$$

Exploitation: https://github.com/edwardz246003/equihash_attacker

后记

区块链安全很复杂

任何攻击都有可能

新共识协议的安全性需要更多关注

新技术会带来新的攻击

主办方 Geekbang> 极客邦科技 InfoQ

THANKS

BCCon
Global
Blockchain
Eco-Technology
Conference