On the Security and Performance of Proof of Work Blockchains

区块链工作量证明的安全性与性能

选题背景

Part One 选题背景

1 Consensus Layer

- PoW共识机制是区块链中最广泛的应用的共识机制（Proof of Work(PoW)\PoS\PoC）
- Block interval：定义了内容写入区块的时延
- PoW安全

2 Network Layer

- Block size
- Information propagation mechanism
- Advertisement-based information dissemination;Send headers;Unsolicited block push;Relay networks;Hybrid Push/Advertisement Systems

3 Stale blocks

旧区块指不在最长链中的区块

	Bitcoin	Litecoin	Dogecoin	Ethereum
Block interval	10 min	2.5 min	1 min	10-20 seconds
Public nodes	6000	800	600	4000 [12]
Mining pools	16	12	12	13
t_{MBP}	8.7 s [9]	1.02 s	0.85 s	0.5 - 0.75 s [13]
r_s	0.41%	0.273%	0.619%	6.8%
s_B	534.8KB	6.11KB	8KB	1.5KB

Table 1: Comparison of different Bitcoin forks, Ethereum and the impact of parameter choices on the network propagation times. Stale block rate (r_s) and average block size (s_B) were measured over the last 10000 blocks. t_{MBP} stands for median block propagation time.

论文结构

Part Two 论文结构

介绍 → 研究背景 → PoW安全模型 → PoW区块链的安全和性能 → 相关工作 → 总结

结构概览

最近的研究指出，基于PoW的区块链的性能在不损害安全性的前提下不能再提升了。但是工作量证明区块链的安全和性能之间的关系并没有深入的细节的研究。

本文解决了这个问题，提出了一个新的量化框架分析PoW区块链各项共识和网络参数的安全和性能影响。

本文框架由2个元素组成：1 区块链实例；2 区块链安全模型

研究方法

Part Three 研究方法

● Security Model

- Stale block rate r_s
  Mining power **α**
  Mining costs $c_m \in [0, \alpha]$
  The number of block confirmations **k**
  Propagation ability
  The impact of eclipse attacks
- Adversary action: Adopt Override Match Wait Exit
- Single-player decision problem **M:=<S,A,P,R> M(Markov Decision Process)**
  S: state space ; **A** :action space ; **P**:stochastic transition matrix; **R**:reward matrix
- S $(l_a, l_h, b_e, fork)$
  fork: **relevant; irrelevant; active**
- Eclipse attacks
  no eclipse attack

Part Three 研究方法

● Optimal Strategies Selfish Mining

自私挖矿最佳防御策略

我们是自私挖矿模型中第一个:1）得到块传输次数，块大小，块产生间隔等参数的；2）得到已知的网络漏洞如eclipse attack

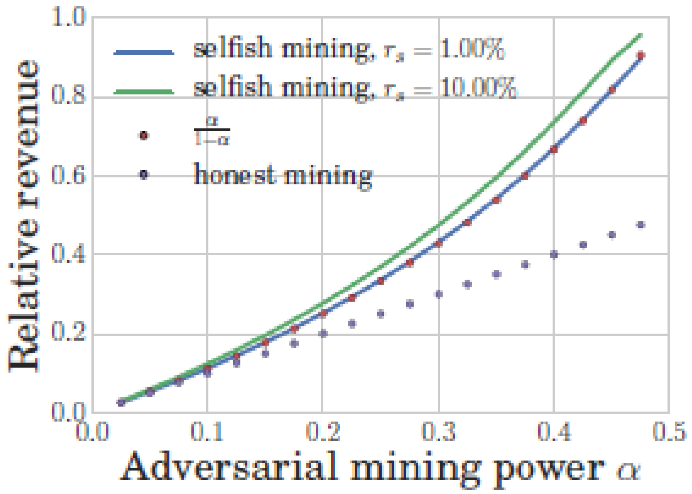


Figure 2: Selfish mining for r_s of 1%, 10%.

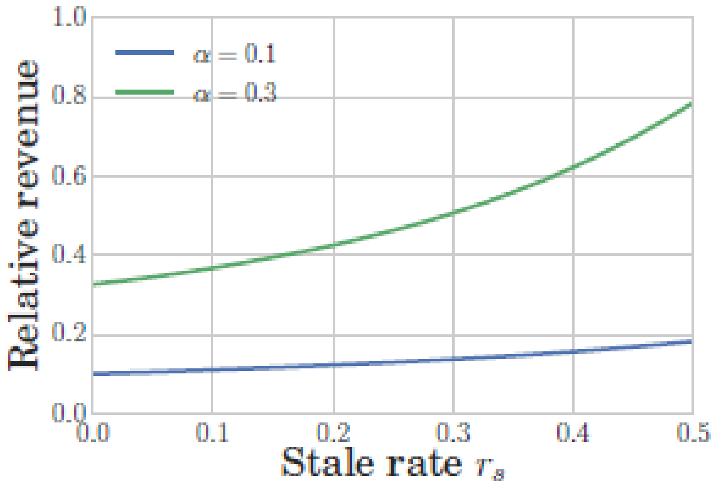


Figure 3: Selfish mining for $\alpha = 0.1$ and 0.3.

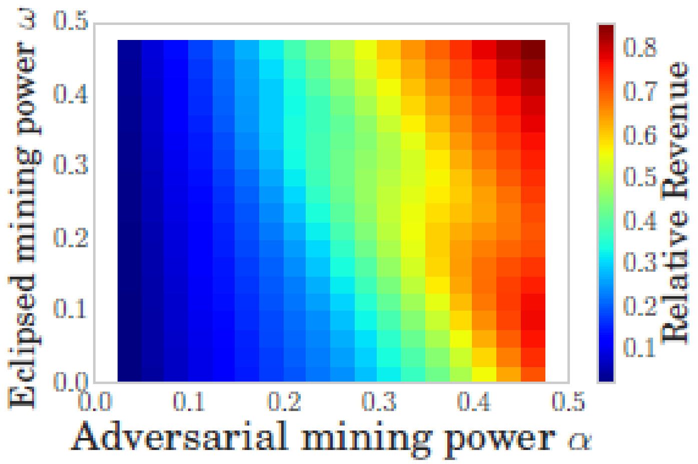


Figure 4: Selfish mining with eclipse attacks.

Part Three 研究方法

● Double-Spending MDP

State × Action	Resulting State	Probability	Reward (in Block reward)
$(l_a, l_h, b_e, \cdot)$, adopt	$(1, 0, 0, i)$	α	$(-c_m, l_h)$
	$(1, 0, 1, i)$	ω	$(-c_m, l_h)$
	$(0, 1, 0, r)$	$(1-\alpha-\omega)\cdot(1-r_s)$	$(-c_m, l_h)$
	$(0, 0, 0, i)$	$(1-\alpha-\omega)\cdot r_s$	$(-c_m, l_h)$
$(l_a, l_h, b_e, \cdot)$, override	$\left(l_a - l_h, 0, b_e - \lceil (l_h+1)\frac{b_e}{l_a} \rceil, i\right)$	α	$\left(\lfloor (l_h+1)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$
	$\left(l_a - l_h, 0, b_e - \lceil (l_h+1)\frac{b_e}{l_a} \rceil + 1, i\right)$	ω	$\left(\lfloor (l_h+1)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$
	$\left(l_a - l_h - 1, 1, b_e - \lceil (l_h+1)\frac{b_e}{l_a} \rceil, r\right)$	$(1-\alpha-\omega)\cdot(1-r_s)$	$\left(\lfloor (l_h+1)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$
	$\left(l_a - l_h - 1, 0, b_e - \lceil (l_h+1)\frac{b_e}{l_a} \rceil, i\right)$	$(1-\alpha-\omega)\cdot r_s$	$\left(\lfloor (l_h+1)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$
(l_a, l_h, b_e, i), wait (l_a, l_h, b_e, r), wait	(l_a+1, l_h, b_e, i)	α	$(-c_m, 0)$
	(l_a+1, l_h, b_e+1, i)	ω	$(-c_m, 0)$
	(l_a, l_h+1, b_e, r)	$(1-\alpha-\omega)\cdot(1-r_s)$	$(-c_m, 0)$
	(l_a, l_h, b_e, i)	$(1-\alpha-\omega)\cdot r_s$	$(-c_m, 0)$
(l_a, l_h, b_e, a), wait (l_a, l_h, b_e, r), match	(l_a+1, l_h, b_e, a)	α	$(-c_m, 0)$
	(l_a+1, l_h, b_e+1, a)	ω	$(-c_m, 0)$
	$(l_a - l_h, 1, b_e - \lceil (l_h)\frac{b_e}{l_a} \rceil, r)$	$\gamma\cdot(1-\alpha-\omega)\cdot(1-r_s)$	$\left(\lfloor (l_h)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$
	(l_a, l_h+1, b_e, r)	$(1-\gamma)\cdot(1-\alpha-\omega)\cdot(1-r_s)$	$(-c_m, 0)$
	(l_a, l_h, b_e, a)	$(1-\alpha-\omega)\cdot r_s$	$(-c_m, 0)$
$(l_a, l_h, b_e, \cdot)$, exit	exit	1	$(l_a - b_e + v_d, 0)$

Table 2: State transition and reward matrices for optimal selfish mining and double-spending strategies in PoW blockchains. α is the mining power of the attacker, ω is the mining power of the eclipsed node, b_e is the number of blocks in the attacker chain that were mined by the eclipsed node, γ is the fraction of nodes that an attacker can reach faster than the honest network, r_s is the stale block rate and v_d is the value of the double-spend. The actions override and match are feasible only when $l_a > l_h$ or $l_a \geq l_h$, respectively. We discount the mining costs $c_m \in [0, \alpha]$ in the state transition reward only for double-spending. The fork label (last element of the state) is denoted by i, r and a for *irrelevant*, *relevant* and *active* respectively. For a reward tuple (a, b), a corresponds to the adversary's costs, while b represents the reward for the honest network for selfish mining.

Part Three 研究方法

Optimal Strategies for Double-Spending

- pymdptoolbox library
- PolicyIteration algorithm

l_a \ l_h	0	1	2	3	4	5	6	7	8
0	w**	*a*	***	***	***	***	***	***	***
1	w**	ww*	ww*	*a*	***	***	***	***	***
2	w**	ww*	ww*	ww*	ww*	*a*	***	***	***
3	w**	ww*	ww*	ww*	ww*	ww*	*a*	***	***
4	w**	ww*	ww*	ww*	ww*	ww*	ww*	*a*	***
5	w**	ww*	ww*	ww*	ww*	ww*	ww*	ww*	*a*
6	w**	ww*	ww*	ww*	ww*	ww*	ww*	ww*	ww*
7	e**	e**	e**	e**	e**	e**	e**	w**	ww*
8	***	***	***	***	***	***	***	e**	w**

Table 3: Optimal double-spending strategy for $\alpha = 0.3, \gamma = 0, r_s = 0.41\%, c_m = \alpha, \omega = 0$ and $v_d = 19.5$. The rows correspond to the length l_a of the adversary's chain and the columns correspond to the length l_h of the honest network's chain. The three values in each table entry correspond to the fork labels *irrelevant*, *relevant* and *active*, where * marks an unreachable state and *w*, *a* and *e* denote the *wait*, *adopt* and *exit* actions, respectively.

Part Three 研究方法

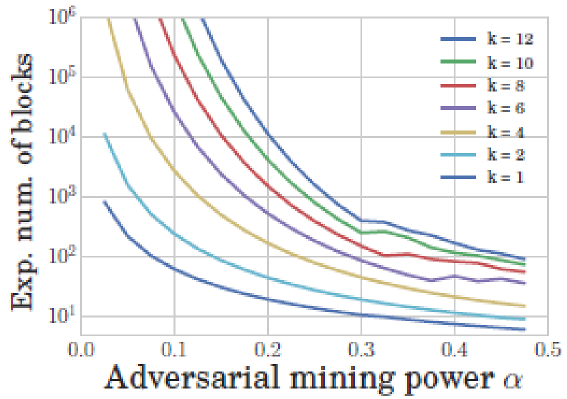


Figure 5: Expected number of blocks for successful double-spending given $r_s = 0.41\%, \gamma = 0, c_m = \alpha$ and $\omega = 0$.

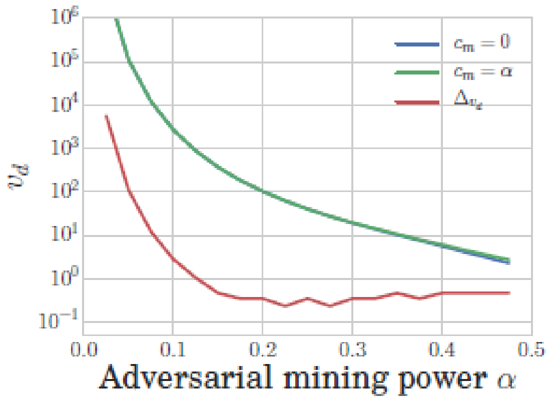


Figure 6: Impact of the mining cost c_m on the security of double spending ($r_s = 0.41\%$, $\gamma = 0, \omega = 0$). Δ_{v_d} is the difference in costs.

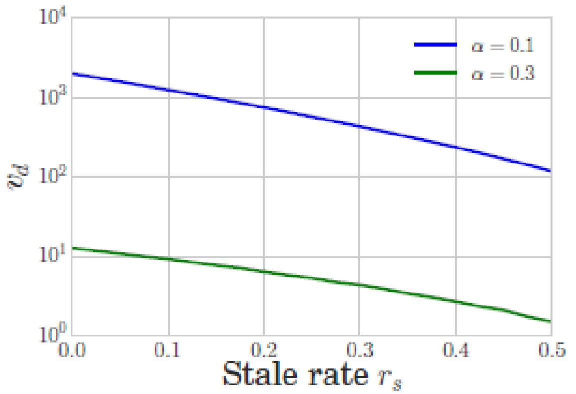
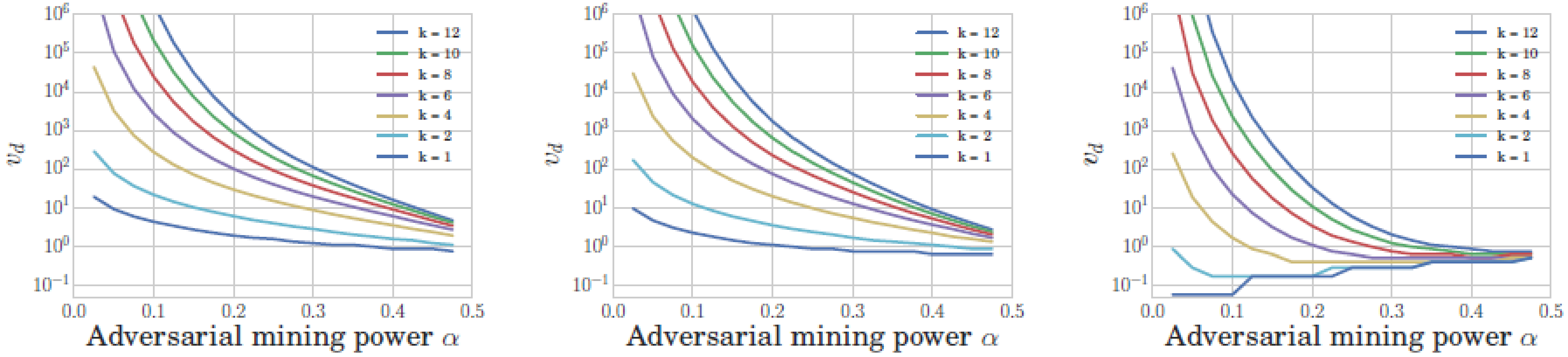


Figure 7: Impact of stale block rate r_s on the security of double-spending given $\gamma = 0.5$, $\omega = 0$ for $\alpha = 0.1, \alpha = 0.3$ and $k = 6$.



(a) $\gamma = 0$ (b) $\gamma = 0.5$ (c) $\gamma = 1$

Figure 8: Impact of the propagation parameter γ. We observe that the higher is γ, the lower is v_d for double-spending to be more profitable than honest mining. $r_s = 0.41\%$ (Bitcoin's stale block rate), $c_m = \alpha$ (maximum mining costs), $\omega = 0$ (no eclipse attack).

Part Three 研究方法

Bitcoin vs. Ethereum

- Uncle reward
  uncle block
- Uniform tie breaking

State × Action	Resulting State	Probability	Reward	Condition
$(l_a, l_h, \cdot, nr)$, adopt	$(1, 0, \text{relevant}, nr)$	α	$-c_m$	-
	$(0, 1, \text{relevant}, nr)$	$(1-\alpha)\cdot(1-r_s)$	$-c_m$	-
	$(0, 0, \text{relevant}, nr)$	$(1-\alpha)\cdot r_s$	$-c_m$	-
$(l_a, l_h, \cdot, inc)$, adopt	$(1, 0, \text{relevant}, nr)$	α	$r_u - c_m$	-
	$(0, 1, \text{relevant}, nr)$	$(1-\alpha)\cdot(1-r_s)$	$r_u - c_m$	-
	$(0, 0, \text{relevant}, nr)$	$(1-\alpha)\cdot r_s$	$r_u - c_m$	-
$(l_a, l_h, \cdot, rel)$, adopt	$(1, 0, \text{relevant}, rel)$	α	$-c_m$	-
	$(0, 1, \text{relevant}, inc)$	$(1-\alpha)\cdot(1-r_s)$	$-c_m$	-
	$(0, 0, \text{relevant}, rel)$	$(1-\alpha)\cdot r_s$	$-c_m$	-
$(l_a, l_h, \cdot, \cdot)$, override	$(l_a - l_h, 0, \text{relevant}, nr)$	α	$l_h + 1 - c_m$	$l_a > l_h$
	$(l_a - l_h - 1, 1, \text{relevant}, nr)$	$(1-\alpha)\cdot(1-r_s)$	$l_h + 1 - c_m$	$l_a > l_h$
	$(l_a - l_h - 1, 0, \text{relevant}, nr)$	$(1-\alpha)\cdot r_s$	$l_h + 1 - c_m$	$l_a > l_h$
$(l_a, l_h, \text{relevant}, nr)$, wait	$(l_a + 1, l_h, \text{relevant}, nr)$	α	$-c_m$	-
	$(l_a, l_h + 1, \text{relevant}, nr)$	$(1-\alpha)\cdot(1-r_s)$	$-c_m$	-
	$(l_a, l_h, \text{relevant}, nr)$	$(1-\alpha)\cdot r_s$	$-c_m$	-
$(l_a, l_h, \text{relevant}, inc)$, wait	$(l_a + 1, l_h, \text{relevant}, inc)$	α	$-c_m$	-
	$(l_a, l_h + 1, \text{relevant}, inc)$	$(1-\alpha)\cdot(1-r_s)$	$-c_m$	-
	$(l_a, l_h, \text{relevant}, inc)$	$(1-\alpha)\cdot r_s$	$-c_m$	-
$(l_a, l_h, \text{relevant}, rel)$, wait	$(l_a + 1, l_h, \text{relevant}, rel)$	α	$-c_m$	-
	$(l_a, l_h + 1, \text{relevant}, inc)$	$(1-\alpha)\cdot(1-r_s)$	$-c_m$	-
	$(l_a, l_h, \text{relevant}, rel)$	$(1-\alpha)\cdot r_s$	$-c_m$	-
$(l_a, l_h, \text{active}, nr)$, wait $(l_a, l_h, \text{relevant}, nr)$, match	$(l_a + 1, l_h, \text{active}, nr)$	α	$-c_m$	$l_h > 6$
	$(l_a + 1, l_h, \text{active}, rel)$	α	$-c_m$	$l_h \leq 6$
	$(l_a - l_h, 1, \text{relevant}, nr)$	$\gamma\cdot(1-\alpha)\cdot(1-r_s)$	$l_h - c_m$	-
	$(l_a, l_h + 1, \text{relevant}, nr)$	$(1-\gamma)\cdot(1-\alpha)\cdot(1-r_s)$	$-c_m$	$l_h > 6$
	$(l_a, l_h + 1, \text{relevant}, inc)$	$(1-\gamma)\cdot(1-\alpha)\cdot(1-r_s)$	$-c_m$	$l_h \leq 6$
	$(l_a, l_h, \text{active}, nr)$	$(1-\alpha)\cdot r_s$	$-c_m$	$l_h > 6$
	$(l_a, l_h, \text{active}, rel)$	$(1-\alpha)\cdot r_s$	$-c_m$	$l_h \leq 6$
$(l_a, l_h, \text{active}, inc)$, wait $(l_a, l_h, \text{relevant}, inc)$, match	$(l_a + 1, l_h, \text{active}, inc)$	α	$-c_m$	-
	$(l_a - l_h, 1, \text{relevant}, nr)$	$\gamma\cdot(1-\alpha)\cdot(1-r_s)$	$l_h - c_m$	-
	$(l_a, l_h + 1, \text{relevant}, inc)$	$(1-\gamma)\cdot(1-\alpha)\cdot(1-r_s)$	$-c_m$	-
	$(l_a, l_h, \text{active}, inc)$	$(1-\alpha)\cdot r_s$	$-c_m$	-
$(l_a, l_h, \text{active}, rel)$, wait $(l_a, l_h, \text{relevant}, rel)$, match	$(l_a + 1, l_h, \text{active}, rel)$	α	$-c_m$	-
	$(l_a - l_h, 1, \text{relevant}, nr)$	$\gamma\cdot(1-\alpha)\cdot(1-r_s)$	$l_h - c_m$	-
	$(l_a, l_h + 1, \text{relevant}, inc)$	$(1-\gamma)\cdot(1-\alpha)\cdot(1-r_s)$	$-c_m$	-
	$(l_a, l_h, \text{active}, rel)$	$(1-\alpha)\cdot r_s$	$-c_m$	-
$(l_a, l_h, \cdot, nr)$, release	$(l_a, l_h, \cdot, rel)$	1	0	$l_h \leq 6 \wedge l_h > 1 \wedge l_a \geq 1$
$(l_a, l_h, \cdot, \cdot)$, exit	exit	1	$l_a + v_d$	$l_a > l_h \wedge l_a > k$

Table 4: State transition and reward matrices for an MDP for optimal double-spending strategies in Ethereum where r_u is the uncle reward (i.e. $\frac{7}{8}$). Every state includes a flag (where nr = not released, rel = released, inc = included) indicating whether an attacker block has been or will be included as an uncle in the honest chain. The release action corresponds to the release of the first block of the attackers fork with the intention to be included as uncle in the honest chain. Therefore, it is only feasible if $1 < l_h \leq 6$ and $l_a \geq 1$, since it is otherwise equivalent to a match or override or the honest chain is too long to include it as uncle. With the release action, no block is mined and a state transitions from not released to released, which transitions to included with the next block mined on the honest chain. In Ethereum, γ is fixed at 0.5 and a match is possible even without a prepared block.

Part Three 研究方法

● Optimal Strategies for Double-Spending

双花攻击最佳防御策略

Uncle reward & Uniform tie breaking

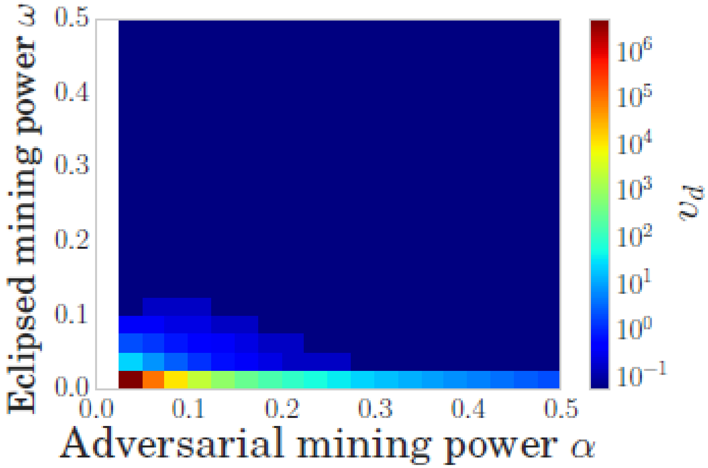


Figure 9: Full eclipse attack for $r_s = 0.41\%$, $\gamma = 0$ and $c_m = 0$.

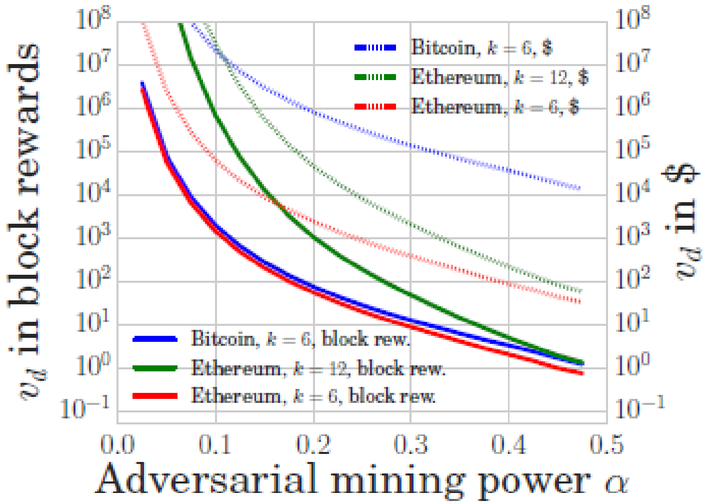


Figure 10: Double-spending resistance of Ethereum ($k \in \{6, 12\}$) vs. Bitcoin ($k = 6$). USD exchange rate of 2016-04-20.

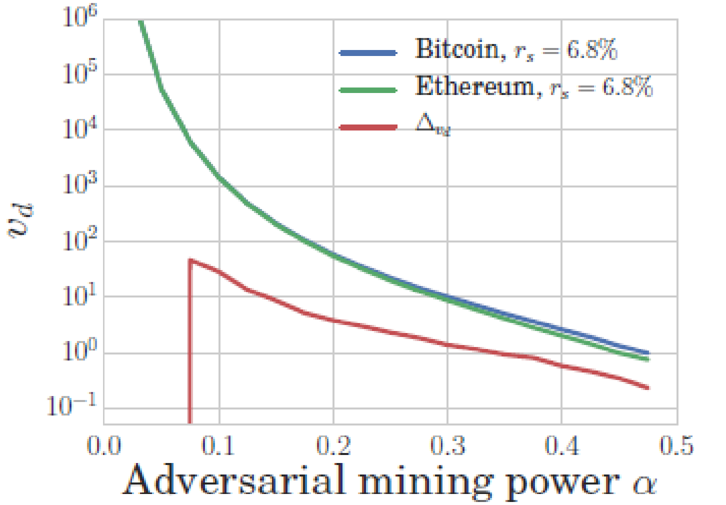


Figure 11: Direct comparison between Ethereum and Bitcoin with $k = 6$, $r_s = 6.8\%$ and their respective difference Δ_{v_d}.

分析讨论

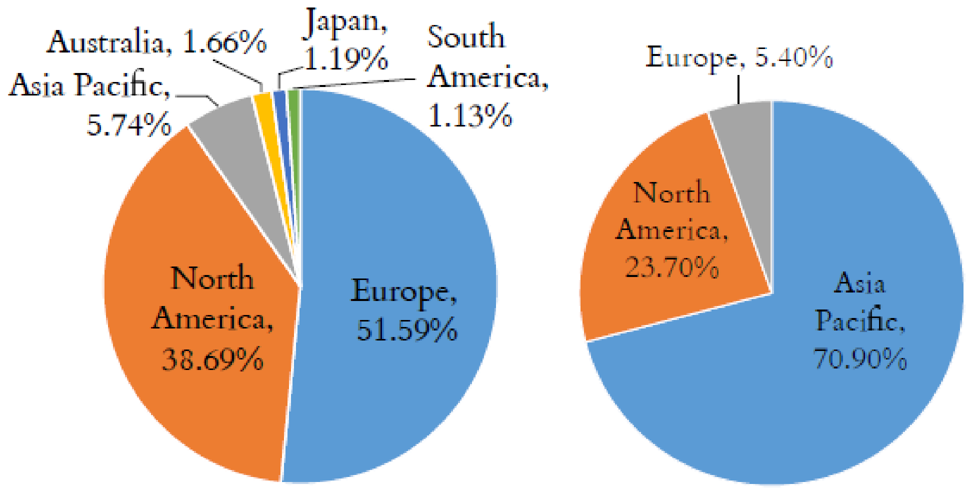
区块链模拟器

Consensus parameter	Description
Block interval distribution	Time to find a block
Mining power distribution of the miners	PoW power distribution
Network-layer parameter	Description
Block size distribution	Variable transaction load
# of reachable network nodes	Open TCP port nodes
Geo. distribution of nodes	Worldwide distribution
Geo. mining pool distribution	Worldwide distribution
# of connections per node	Within network
# of connections of the miners	Within network
Block request management system	Possible Protocols
Standard mechanism (inv/getdata)	Default
Unsolicited block push	Miner only push block
Relay network	Miner network
Sendheaders	Bitcoin v0.12

Table 5: Parameters of the blockchain simulation.

Part Four 分析讨论

区块链模拟器



(a) Node distribution. (b) Miner distribution.

Figure 12: Geographical distribution of Bitcoin nodes and miners used in our simulator.

Part Four 分析讨论

01 Simulator Validation
模拟器验证

02 Impact of the Block Interval
区块间隔的影响

03 Impact of the Block size
区块大小的影响

04 Throuhhput
吞吐量

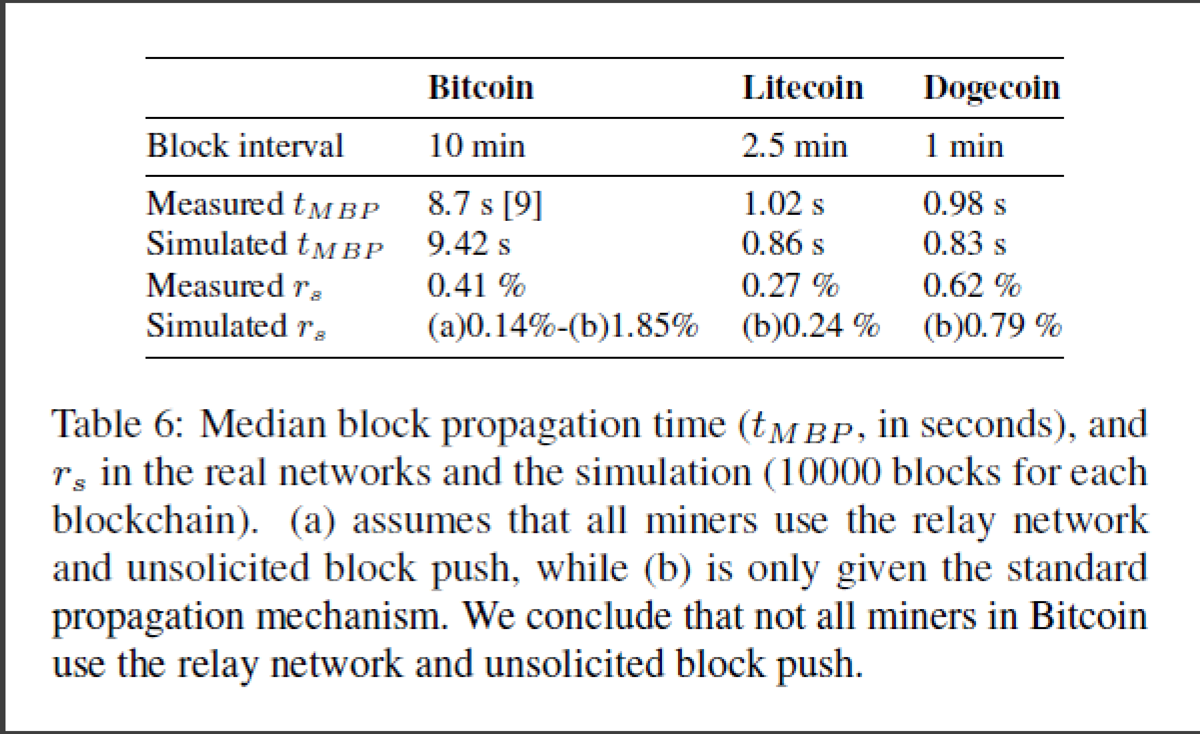
评价结果

我们从以上四个方面来讨论我们的实验结果

Part Four 分析讨论

Simulator Validation

模拟器验证



	Bitcoin	Litecoin	Dogecoin
Block interval	10 min	2.5 min	1 min
Measured t_{MBP}	8.7 s [9]	1.02 s	0.98 s
Simulated t_{MBP}	9.42 s	0.86 s	0.83 s
Measured r_s	0.41 %	0.27 %	0.62 %
Simulated r_s	(a)0.14%-(b)1.85%	(b)0.24 %	(b)0.79 %

Table 6: Median block propagation time (t_{MBP}, in seconds), and r_s in the real networks and the simulation (10000 blocks for each blockchain). (a) assumes that all miners use the relay network and unsolicited block push, while (b) is only given the standard propagation mechanism. We conclude that not all miners in Bitcoin use the relay network and unsolicited block push.

2015.5-2015.11区块大小和区块生成率

6个月的数据：24000Bitcoin blocks，100000Litecoin and 240000 Dogecoin blocks

Part Four 分析讨论

Impact of the Block Interval

区块间隔的影响

	Case 1				Case 2				Case 3				Case 4			
Block interval	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}
25 minutes	35.73	1.72 %	12.47	0.34	25.66	0.16 %	12.86	0.33	22.50	0.03 %	12.89	0.33	22.44	0.02 %	12.89	0.33
10 minutes	14.7	1.51 %	12.52	0.34	10.65	0.13 %	12.88	0.33	9.41	0.14 %	12.86	0.33	9.18	0.13 %	12.87	0.33
2.5 minutes	4.18	1.82 %	12.45	0.34	2.91	0.16 %	12.86	0.33	2.60	0.16 %	12.86	0.33	2.59	0.15 %	12.86	0.33
1 minute	2.08	2.15 %	12.35	0.34	1.34	0.35 %	12.81	0.33	1.30	0.25 %	12.83	0.33	1.27	0.29 %	12.77	0.33
30 seconds	1.43	2.54 %	12.06	0.34	0.84	0.45 %	12.78	0.33	0.84	0.51 %	12.77	0.33	0.84	0.52 %	12.69	0.33
20 seconds	1.21	3.20 %	11.73	0.34	0.67	0.86 %	12.68	0.33	0.69	0.85 %	12.68	0.33	0.68	0.82 %	12.68	0.33
10 seconds	1.00	4.77 %	10.73	0.35	0.35	1.73 %	12.46	0.34	0.33	1.41 %	12.54	0.34	0.53	1.59 %	12.50	0.34
5 seconds	0.89	8.64 %	10.08	0.37	0.37	2.94 %	11.85	0.34	0.45	2.99 %	11.80	0.34	0.44	3.05 %	11.78	0.34
2 seconds	0.84	16.65 %	7.35	0.41	0.40	6.98 %	10.47	0.36	0.39	7.28 %	10.37	0.36	0.38	7.10 %	10.42	0.36
1 seconds	0.82	26.74 %	4.37	0.53	0.53	12.44 %	8.34	0.39	0.38	12.59 %	8.24	0.39	0.37	12.52 %	8.30	0.39
0.5 seconds	0.82	38.15 %	2.78	0.60	0.61	20.62 %	6.22	0.42	0.49	20.87 %	6.16	0.42	0.36	21.10 %	6.02	0.42

Table 7: Impact of the block interval on the median block propagation time (t_{MBP}) in seconds, and the stale block rate r_s, v_d and r_{rel} given the current Bitcoin block size distribution, an adversary with $\alpha = 0.3$ and $k = 6$. Case 1 refers to the standard block propagation mechanism, Case 2 refers to standard mechanism plus unsolicited block push, Case 3 to the combination of Case 2 plus the relay network and Case 4 to the send headers with unsolicited block push and relay network.

Part Four 分析讨论

Impact of the Block size

区块大小的影响

	Case 1				Case 2				Case 3				Case 4			
Block Size	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}
0.1 MB	3.18	0.32 %	12.80	0.33	2.12	0.03 %	12.89	0.33	2.02	0.03 %	12.89	0.33	2.02	0.2 %	12.90	0.33
0.25 MB	7.03	0.88 %	12.67	0.33	4.93	0.11 %	12.87	0.33	4.49	0.05 %	12.88	0.33	4.46	0.17 %	12.87	0.33
0.5 MB	13.62	1.63 %	12.48	0.34	9.84	0.13 %	12.87	0.33	8.65	0.05 %	12.88	0.33	8.64	0.06 %	12.87	0.33
1 MB	27.67	3.17 %	11.79	0.34	20.01	0.38 %	12.79	0.33	17.24	0.07 %	12.88	0.33	17.14	0.07 %	12.88	0.33
2 MB	57.79	6.24 %	10.57	0.36	44.6	1.12 %	12.61	0.34	35.49	0.08%	12.87	0.33	35.38	0.1 %	12.86	0.33
4 MB	133.30	11.85 %	8.20	0.38	126.57	5.46 %	10.51	0.35	78.01	0.12 %	12.85	0.33	78.40	0.13 %	12.66	0.33
8 MB	571.50	29.97 %	4.11	0.53	875.97	15.64 %	7.64	0.41	555.49	0.43 %	12.65	0.33	550.25	0.4 %	12.68	0.33

Table 8: Impact of the block size on the median block propagation time (t_{MBP}) in seconds, the stale block rate r_s, v_d and r_{rel}, given the current Bitcoin block generation interval and an adversary with $\alpha = 0.3$ and $k = 6$.

区块大小对中央区块传播时间的影响

Part Four 分析讨论

Throughput

吞吐量

tps	v_d	r_{rel}	Block size	Block interval
33.4	12.75	0.33	0.25MB	30 seconds
40	12.38	0.34	0.10MB	10 seconds
50	12.45	0.34	0.25MB	20 seconds
66.7	12.06	0.34	0.25MB	15 seconds
66.7	12.65	0.33	0.50MB	30 seconds
66.7	12.71	0.33	1.00MB	1 minute

Table 9: Throughput in transactions per second (tps) vs. security measured in v_d and r_{rel} for an adversary with 30% mining power, $k = 6$ and given 16 mining pools.

主要结论

Part Five 主要结论

新的定量框架

- PoW blockchains
- Blockchain parameters

Bitcoin & Ethereum

Bitcoin的区块链比Ethereum的区块链更安全，Ethereum会用uncle reward 来奖励矿工，并形成uniform tie breaking来解决区块链分叉。

交易量

现存的PoW区块链可以得到一分钟60个交易的吞吐量，并且不严重影响区块链的安全。

量化评价旧块率

首次提出量化评价PoW区块链中对抗自私挖矿和双花攻击的最优策略中旧块率影响。

参考文献

Part Six 参考文献

[1] Bitcoin block size limit controversy, 2016. Available from:https://en.bitcoin.it/wiki/Block_size_limit_controversy.

[2] Frederik Armknecht, Jens-Matthias Bohli, Ghassan O Karame, Zongren Liu, and Christian A Reuter. Outsourced proofs of retrievability. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pages 831–843. ACM, 2014.

[3] Bitnodes. Bitnodes ip crawler. Available from: https://github.com/ayeowch/bitnodes.

[4] V. Buterin. A next-generation smart contract and decentralized application platform, 2014.

[5] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In OSDI, volume 99, pages 173–186, 1999.

[6] Coinmarketcap. Coinmarketcap. Available from: https://coinmarketcap.com/.

[7] Matt Corallo. Bitcoin relay network. Available from: http://bitcoinrelaynetwork.org/.

[8] Nicolas T. Courtois and Lear Bahack. On subversive miner strategies and block withholding attack in bitcoin digital currency. CoRR, abs/1402.1718, 2014.

[9] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer,Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena,Elaine Shi, and Emin Gün. On scaling decentralized blockchains. In Proc. 3rd Workshop on Bitcoin and Blockchain Research, 2016.

[10] C. Decker and R. Wattenhofer. Information Propagation in the Bitcoin Network. In 13-th IEEE International Conference on Peer-to-Peer Computing, 2013.

[11] Ethereum. Ethereum tie breaking. Available from: https://github.com/ethereum/go-ethereum/commit/bcf565730b1816304947021080981245d084a930.

[12] Ethereum. ethernodes. Available from: https://www.ethernodes.org/network/1.

[13] Ethereum. ethstats. Available from: https://ethstats.net/.

[14] Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, and Robbert van Renesse. Bitcoin-ng: A scalable blockchain protocol. arXiv preprint arXiv:1510.02037, 2015.

[15] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography and Data Security, pages 436–454. Springer, 2014.

[16] The Finney Attack, 2013. Available from: https://en.bitcoin.it/wiki/Weaknesses#The_.22Finney.22_attack.

[17] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 281–310.Springer, 2015.

THANK YOU FOR WATCHING