针对中本聪共识协议的自私挖矿性能分析

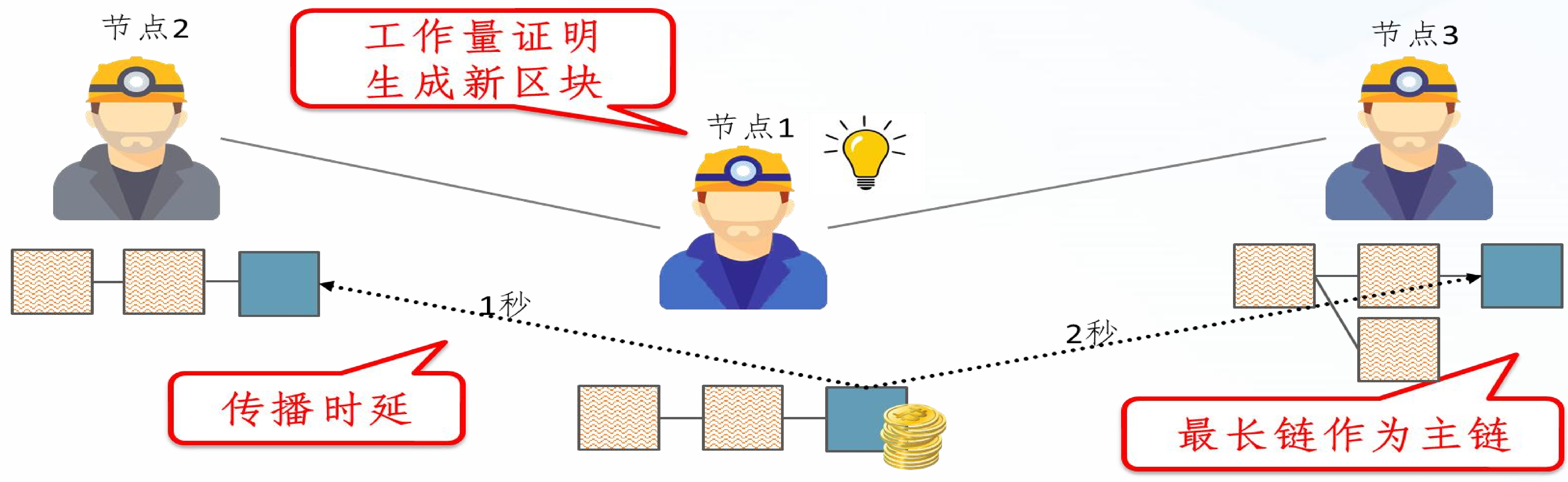
Xia Q, Dou W, et al. The Impact Analysis of Multiple Miners and Propagation Delay on Selfish Mining. Proceedings of IEEE Computers, Software, and Applications Conference (COMPSAC). 2021: 694-703.

夏清 窦文生 张凤军 梁赓

中国科学院软件研究所

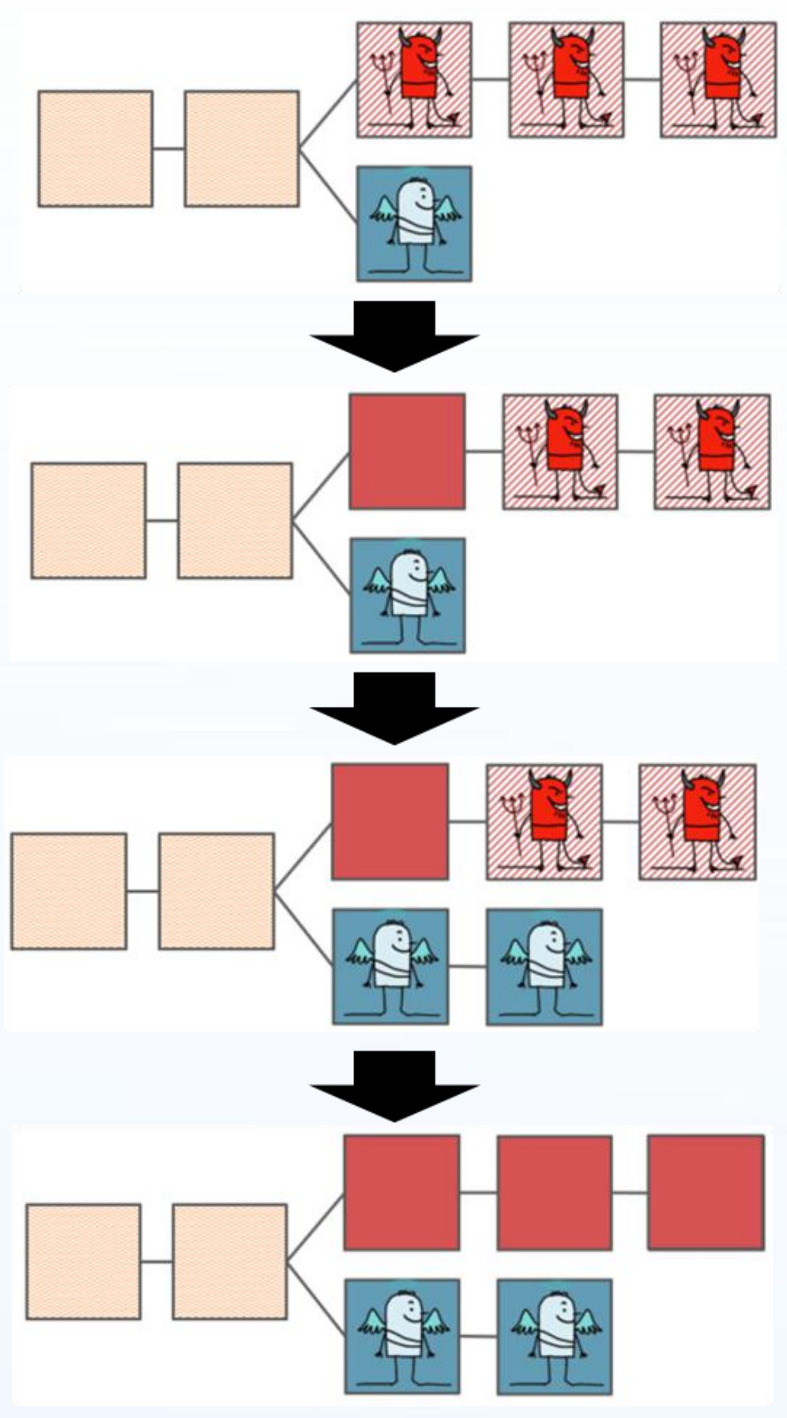
联系人：张凤军 13439308245 fengjun@iscas.ac.cn

研究背景

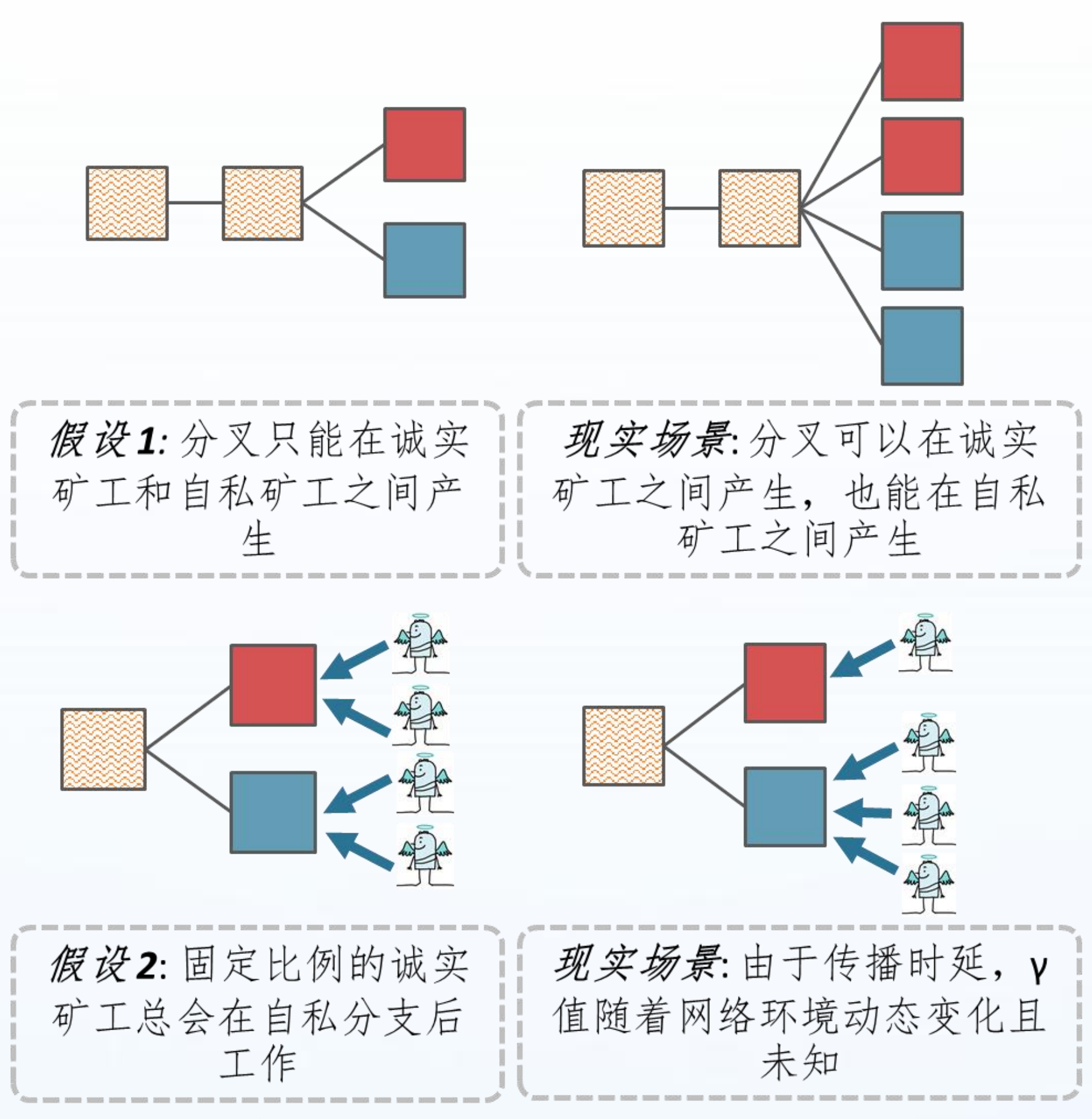


比特币作为一种流行的去中心化加密货币，已经引起了公众的广泛关注。比特币利用中本聪共识协议对区块链账本达成共识。然而，中本聪共识协议可能会遭受自私挖矿攻击。现有关于自私挖矿的研究通常假设总挖矿算力分为两部分（即诚实算力和自私算力），并忽略了区块的网络传播时延。这些假设无法反映现实世界场景，在现实场景中，多个矿工同时竞争生成区块并以一定的传播时延传播区块。因此，区块链系统中的现实因素，即多矿工和传播延迟，如何影响自私挖矿仍是未知的。本文探讨了多矿工和传播延迟对自私挖矿的影响。首先，我们提出了一种可以处理这些现实因素的新自私挖矿策略。其次，我们设计了一种模拟方法来分析新策略的性能。从实证研究中，我们观察到许多可用于防御自私挖矿攻击的新发现。例如，孤块率较高的区块链系统更容易受到自私挖矿攻击。

研究方法



自私挖矿攻击



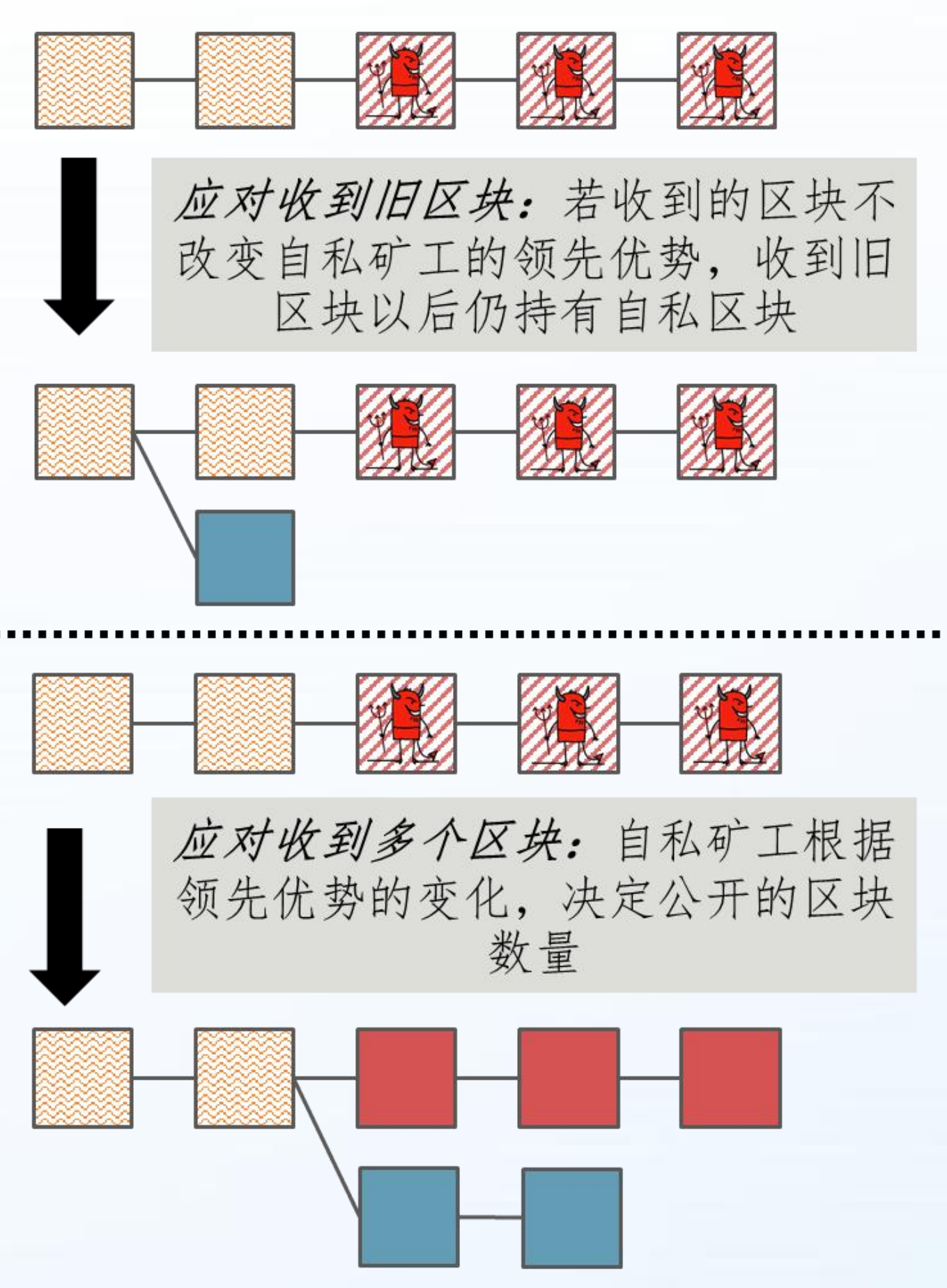
假设1: 分叉只能在诚实矿工和自私矿工之间产生

现实场景: 分叉可以在诚实矿工之间产生，也能在自私矿工之间产生

假设2: 固定比例的诚实矿工总会在自私分支后工作

现实场景: 由于传播时延，γ值随着网络环境动态变化且未知

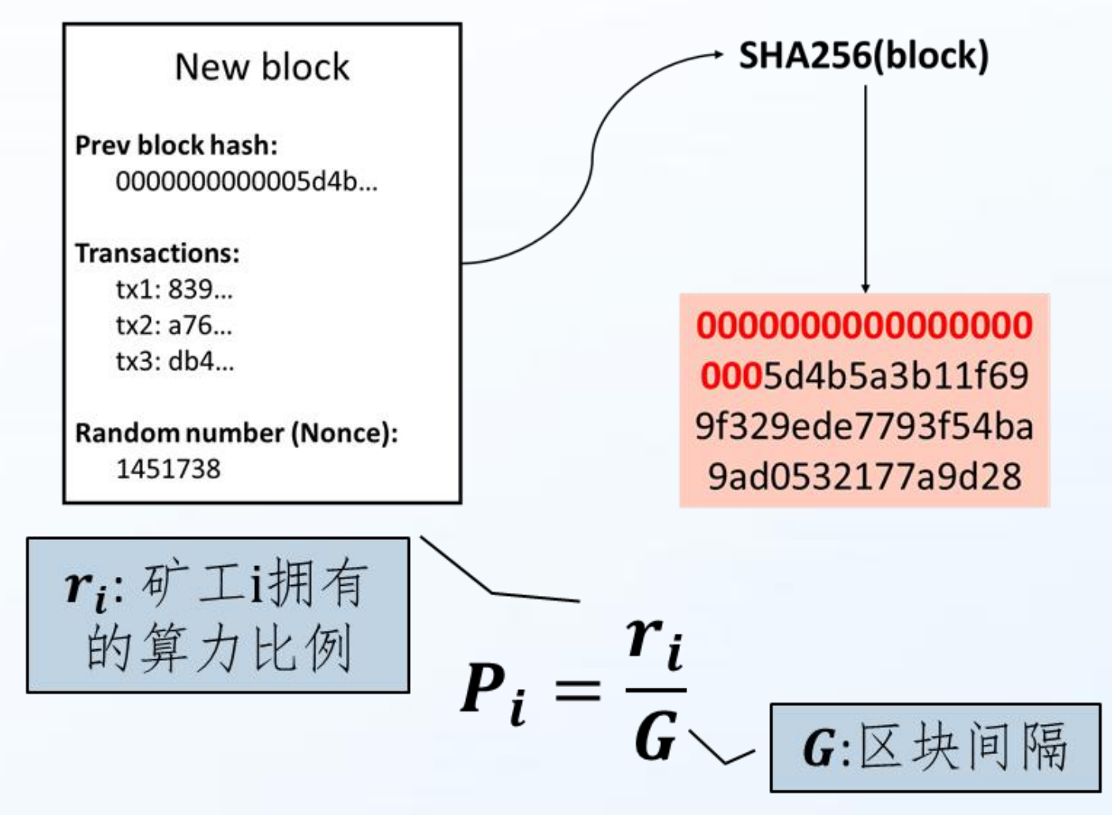
现有工作假设不符合现实场景



应对收到旧区块：若收到的区块不改变自私矿工的领先优势，收到旧区块以后仍持有自私区块

应对收到多个区块：自私矿工根据领先优势的变化，决定公开的区块数量

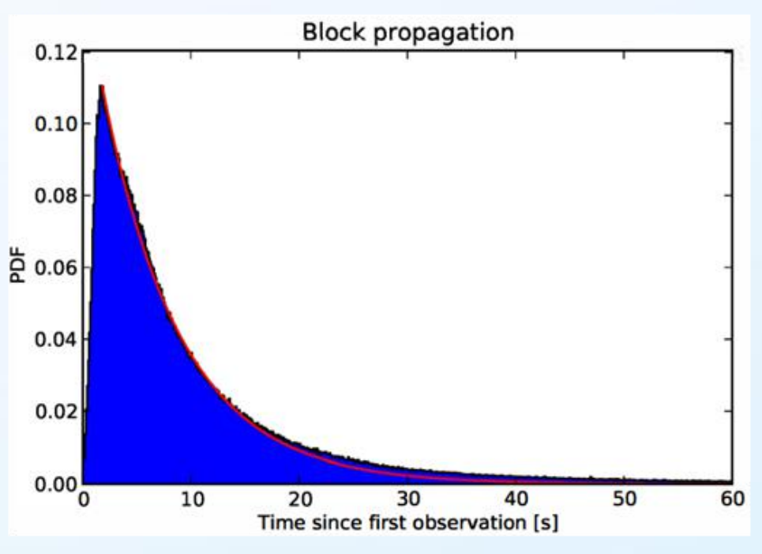
实际的自私挖矿策略



r_i: 矿工i拥有的算力比例

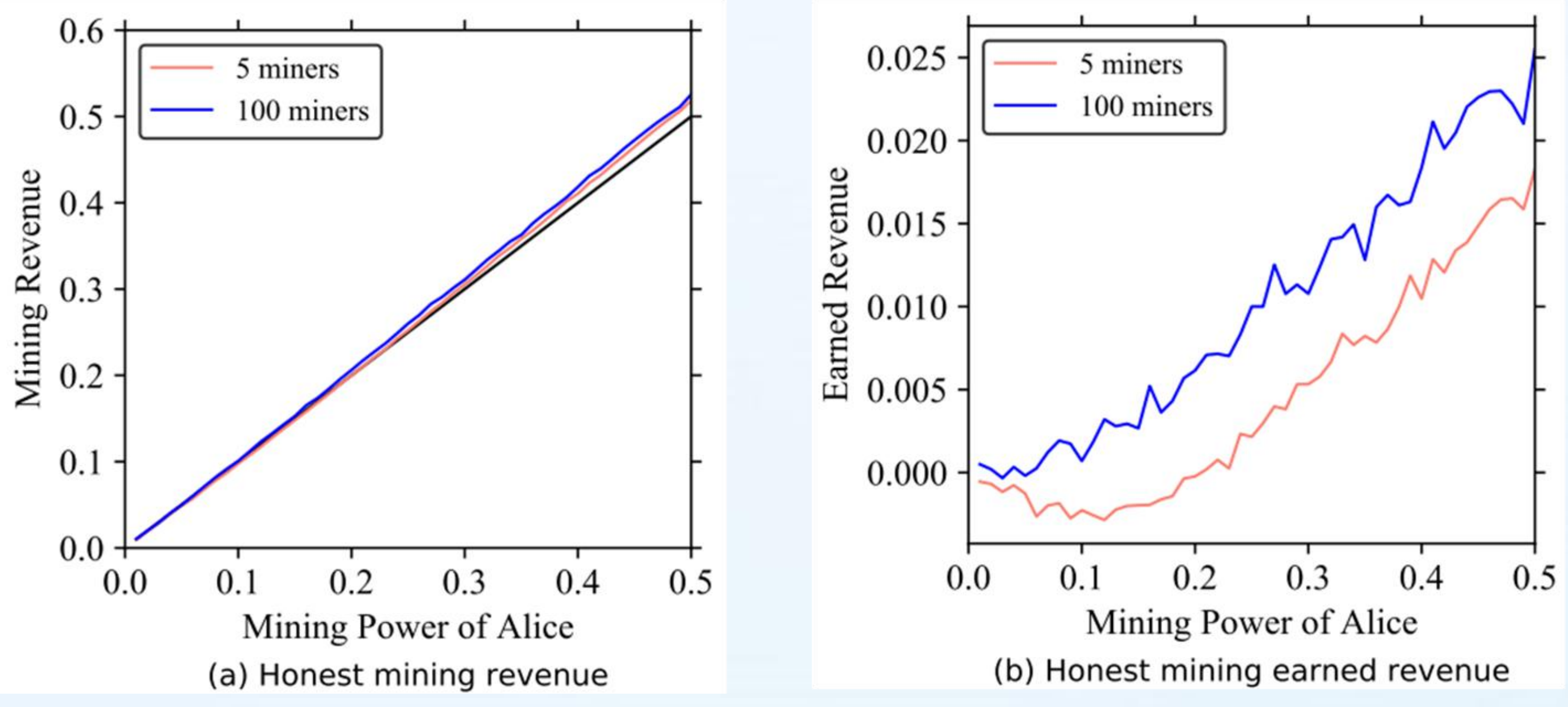
$$P_i = \frac{r_i}{G}$$

G:区块间隔



基于工作量证明的区块产生时间、分布式系统传播时延均符合几何分布

主要成果

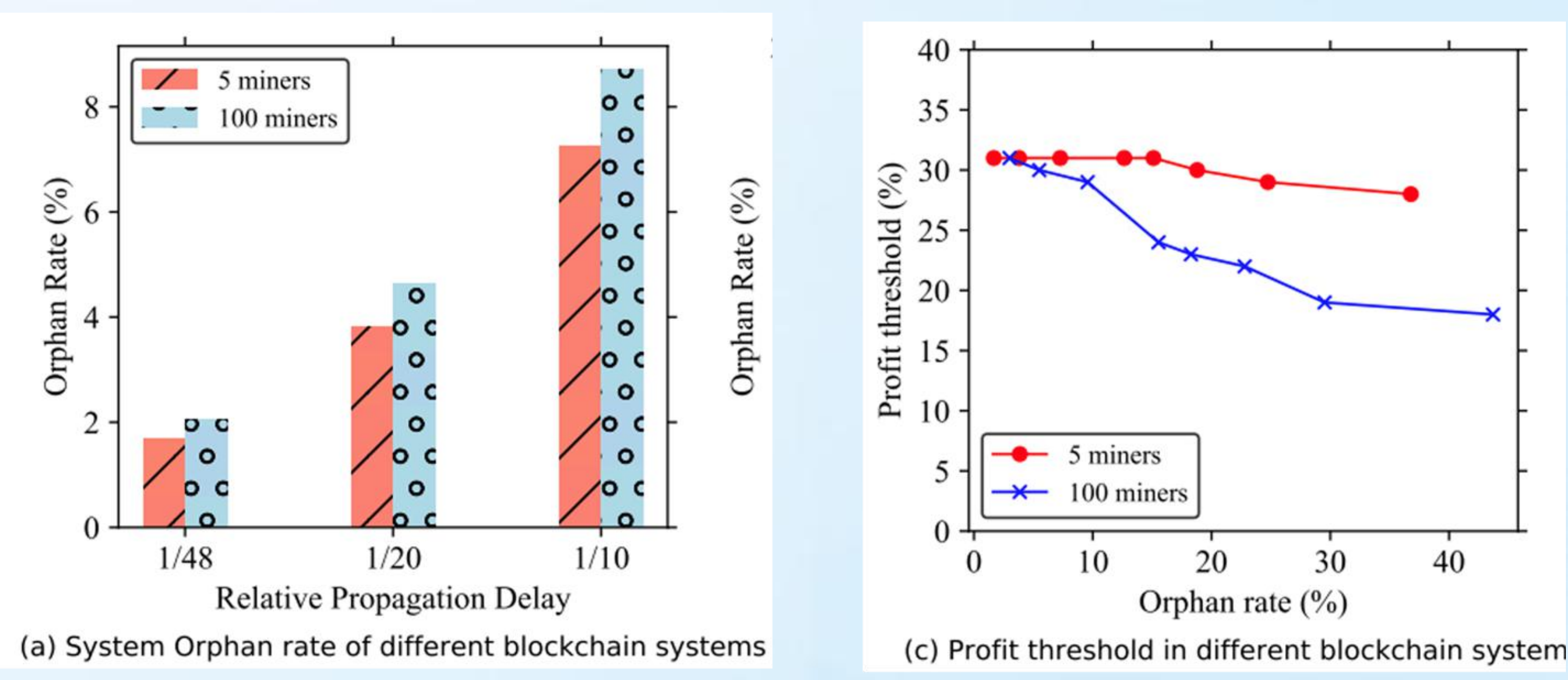


(a) Honest mining revenue

(b) Honest mining earned revenue

单个矿工在多诚实矿工系统中的诚实收益

- 拥有足够多算力的矿工在诚实挖矿中具有内在优势，该优势在矿工数量多的系统中更明显

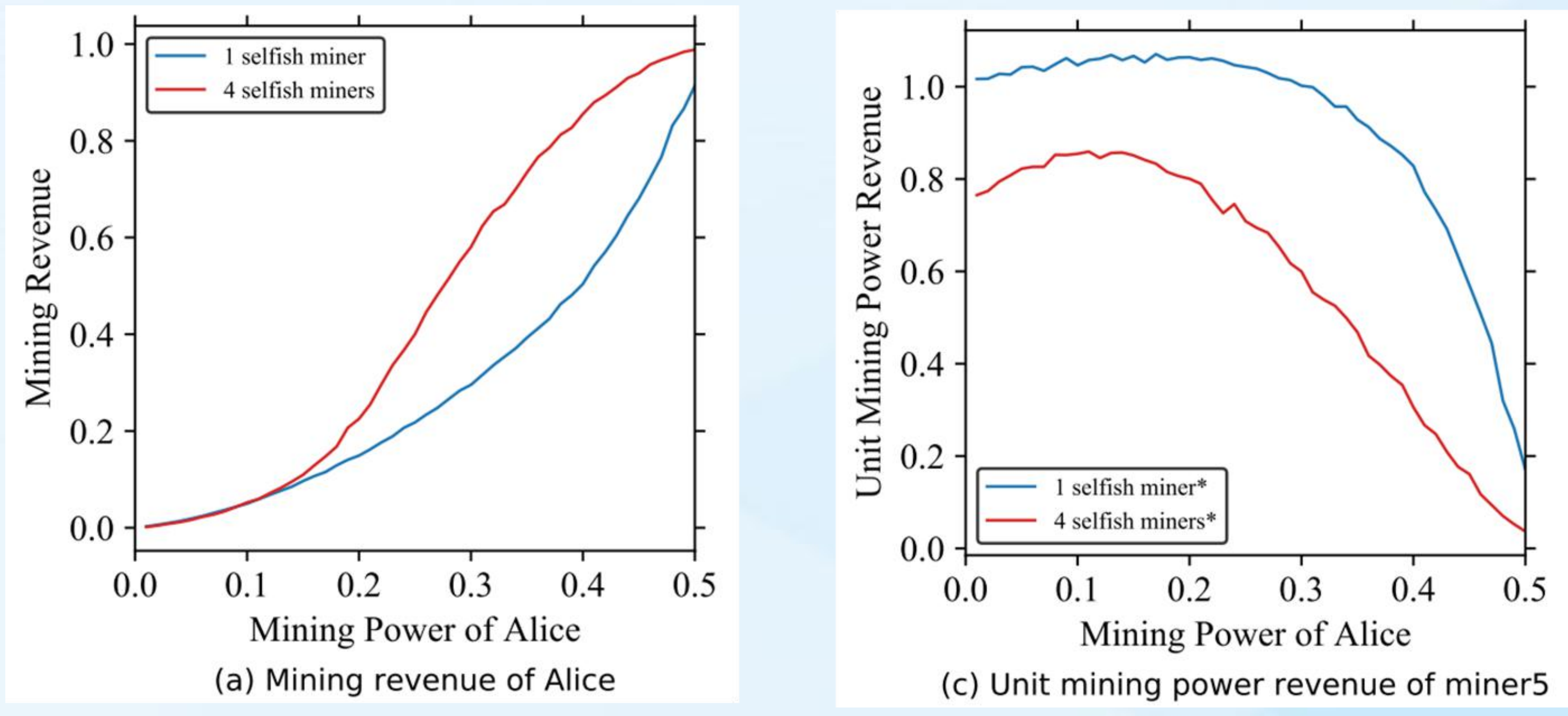


(a) System Orphan rate of different blockchain systems

(c) Profit threshold in different blockchain system

不同孤块率系统应对自私挖矿的收益阈值

- 更多的矿工数量以及更长的传播时延导致更高的系统孤块率，随着统孤块率提高，自私挖矿的收益阈值逐渐降低（即系统安全性降低

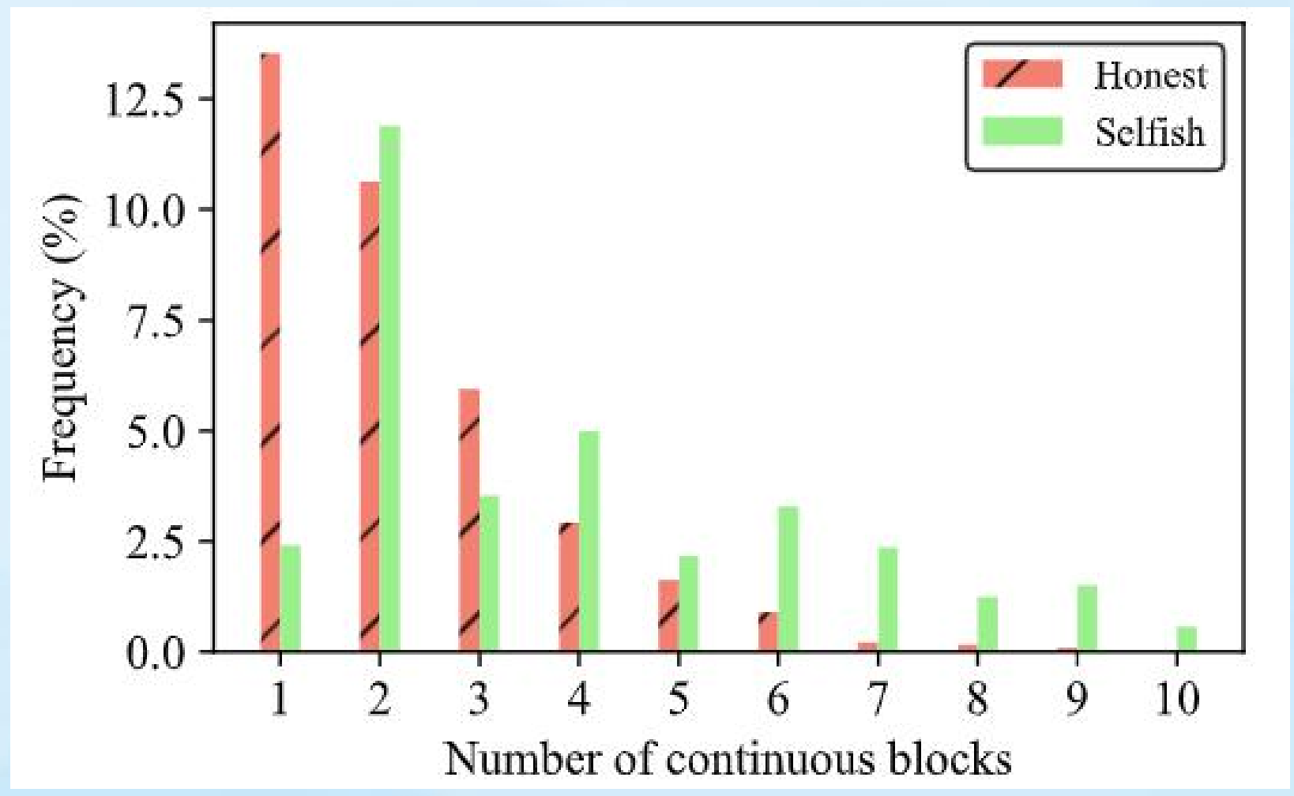


(a) Mining revenue of Alice

(c) Unit mining power revenue of miner5

单个矿工在多自私系统中的自私收益

- 多自私矿工互相竞争时，拥有算力最多的自私矿工可以获益，然而其他算力少的自私矿工不能获益



连续产生多个主链区块的频率

- 自私挖矿导致连续多个主链区块由自私矿工产生

$$\begin{cases} blockReward\ (Conti = 1, \ldots, 4) \\ \dfrac{blockReward}{Conti\ - 2}\ (Conti\ \geq 5) \end{cases}$$

- 通过修改共识协议中的主链收益机制，可使自私矿工的收益大幅降低