A Unified Analytical Model for Proof-of-X Schemes

Article *in* Computers & Security · June 2020

DOI: 10.1016/j.cose.2020.101934

CITATIONS
4

READS
103

7 authors, including:

Guangsheng Yu
University of Technology Sydney
14 PUBLICATIONS **63** CITATIONS
SEE PROFILE

Xuan Zha
University of Technology Sydney
15 PUBLICATIONS **188** CITATIONS
SEE PROFILE

Xu Wang
University of Technology Sydney
21 PUBLICATIONS **257** CITATIONS
SEE PROFILE

Wei Ni
The Commonwealth Scientific and Industrial Research Organisation
303 PUBLICATIONS **2,845** CITATIONS
SEE PROFILE

A Unified Analytical Model for Proof-of-X Schemes

Guangsheng Yu[a,b,*], Xuan Zha[a,c], Xu Wang[a,b], Wei Ni[d], Kan Yu[e], J. Andrew Zhang[a], Ren Ping Liu[a,b]

[a] *Global Big Data Technologies Centre, University of Technology Sydney, Australia*
[b] *Food Agility CRC Ltd, 81 Broadway, Ultimo, NSW, Australia, 2007*
[c] *China Academy of Information and Communications Technology (CAICT), China*
[d] *Data61, CSIRO, Australia*
[e] *The Department of Computer Science and Information Technology, La Trobe University, Bendigo, Victoria, Australia*

Abstract

Nakamoto protocol, practically solving the Byzantine Generals Problem, can support a variety of proof-based consensus engines, referred to as Proof-of-X (PoX) in permissionless Blockchains. However, there has been to date in lack of a general approach for each miner to evaluate its steady-state profit against the competitors. This paper presents a Markov model which captures explicitly the weighted resource distribution of PoX schemes in large-scale networks and unifies the analysis of different PoX schemes. The new model leads to the development of three new unified metrics for the evaluation, namely, *Resource Sensitivity*, *System Convergence*, and *Resource Fairness*, accounting for security, stability, and fairness, respectively. The generality and applicability of our model are validated by simulation results, revealing that among typically non-Fairness-oriented PoX schemes (such as Proof-of-Work (PoW) and Proof-of-Stake (PoS)), the strongly restricted coinage-based PoS with a Pareto-distributed resource can offer the best performance on *Resource Sensitivity*, while Proof-of-Publication (PoP) with normal-distributed resource performs the best on *System Convergence*. Our simulations also reveal the important role of

*Corresponding author
Email addresses: Guangsheng.Yu@uts.edu.au (Guangsheng Yu), zhaxuan@caict.ac.cn (Xuan Zha), Xu.Wang-1@uts.edu.au (Xu Wang), Wei.Ni@data61.csiro.au (Wei Ni), k.yu@latrobe.edu.au (Kan Yu), Andrew.Zhang@uts.edu.au (J. Andrew Zhang), Renping.Liu@uts.edu.au (Ren Ping Liu)

carefully designed *Resource Fairness* parameter in balancing *Resource Sensitivity* and *System Convergence* and improving the performance compared with other non-Fairness-oriented PoX schemes.
Keywords: Blockchain, Consensus, Nakamoto protocol, Proof-of-X schemes, Markov chain

1. Introduction

Nakamoto protocol in Bitcoin [1] was proposed to address the Byzantine Generals Problem [2] other than the traditional Byzantine Fault Tolerance (BFT) protocol. The consensus engine of the Nakamoto protocol was first proposed as Proof-of-Work (PoW), and has been extended to other virtual-mining-based variations (e.g., Proof-of-Stake (PoS)) and subsequently generalized to Proof-of-X (PoX)-based consensus algorithms [3, 4]. PoX schemes take advantage of probabilistic consensus algorithms, and introduce a publicly Verifiable Random Function (p-VRF) with only communication overhead of $O(N)$ (N is the number of miners). Along with the PoX schemes have been widely adopted in a variety of applications (such as Proof-of-Collaboration (PoC) [5] and Proof-of-Distribution (PoD) [6] in Internet-of-Things systems), as well as the comparison between BFT schemes and PoX schemes becoming attractive [7, 8, 9], the studies on PoX schemes become increasingly interesting for large-scale networks.

In PoX schemes, the computation resource used in PoW can be replaced using any other publicly-verifiable system resources with customized parameters (e.g., account balance/coinage in PoS and task progress in PoC), as long as the p-VRF can hold. Several recent papers analyzed the PoW, PoS and their variations [10, 11, 12, 13], but none of them was able to evaluate the long-term steady state of the system and the impact of the distribution of system resource on the state. There also lacks a general analytical model for PoX schemes. Such a model would be important to enable each miner to estimate its profit against competitors based on its source. This is important for the traditional mining industry [14] and any public services based on permissionless Blockchains.

In this paper, we propose a new unified analytical model which is able to quantify the profit of individual miners in any of the popular permissionless PoX-based Blockchains. By applying the model, miners can estimate their profit against their resources under different PoX schemes. The new model captures proposed changes in the system resource distribution of PoX schemes by designing an infinite-dimensional Markov chain. A set of expressions is established to efficiently evaluate the mining probability of a miner, given the amount of system resource owned by the miner. The type and distribution of system resources can be customized in line with system requirements.

We develop a new general presentation to unify a variety of system resource distributions in PoX schemes, such as PoW, PoS, and Proof-of-Publication (PoP). Specifically, we characterize probabilistically the system resource owned by a miner. The instantaneous probability with which the miner can mine a block at any instant is generalized to be captured by two new configurable functions respectively accounting for the specific fairness measures of a PoX scheme and the dependence of mining success on the resource distributions in the scheme.

We also design three new performance metrics, namely, *Resource Sensitivity*, *System Convergence*, and *Resource Fairness*, to evaluate the different PoX-based consensus algorithms systematically and consistently. The metrics are quantifiable based on the average mining probabilities that the proposed infinite-dimensional Markov model is able to derive under the new unified measure of system resource distributions.

As revealed by our analysis, in PoX-based consensus algorithms where the monopoly of block generation is prevented and diversity is maintained, miners can maximize the profits with strong double-spending-resistance and controllable cost-risk assessment, thereby contributing to a healthy and sustainable mining ecosystem. Specifically, the system resource has the weakest impact on the average mining probability for each participating miner when a configurable function delivering positive correlation takes effects, which leads to the best *Resource Sensitivity*. Better *System Convergence* can be achieved in PoX schemes

with normal-distributed system resource than that with a Pareto-distributed system resource, unless the schemes are designed to restrict the monopoly of block generation. Good fairness or balanced resources play important roles in fast convergence. The proposed fairness function can be implemented in a distributed manner, to improve the fairness between miners and speed up the convergence.

The rest of this paper is organized as follows. Section 2 discusses the preliminary knowledge. In Section 3, a Markov analytical model is presented. The considered network setting is also discussed in Section 4, followed by the simulation and analysis on different existing PoX-based consensus algorithms in terms of three proposed metrics in Section 5. Section 6 reviews related works. In Section 7, conclusions are drawn.

2. Preliminary

In this section, the security model considered in Bitcoin is discussed to illustrate the relationship between Bitcoin's security model and our proposed metric, *Resource Sensitivity*, as will be shown in Section 3.4.1. A hybrid PoW-based consensus is introduced, as it inspires the design of the proposed *Degree function*, and can be regarded as a origin of the PoX scheme.

2.1. Bitcoin's Security Model

In Bitcoin's model [1], security is measured by the probability δ with which an attacker can catch up with the loyal miners to dominate the block generation. δ is considered to be subject to the Poisson Distribution, as given by

$$\delta = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}(1 - (\frac{q}{p})^{z-k}),$$

where p denotes the probability of a loyal node being the current block generator and q denotes the probability of a malicious node being the current block generator. $p > q$, $\lambda = z\frac{q}{p}$, and $k \leq z$, where z denotes how much the malicious node falls behind the loyal miners in terms of block height.

Table 1: Expressions of (non-)Fairness-oriented PoX schemes

<table>
<tr><td colspan="4">Non-Fairness-oriented, let $\Upsilon(\omega_i) = \omega_i$</td></tr>
<tr><td colspan="2">The PoX schemes</td><td>Types of the System Resource</td><td>ω_i†</td><td>$f_{i,h}$</td></tr>
<tr><td colspan="2">Proof-of-Work [1]</td><td>Computation power</td><td rowspan="2">PD⋆</td><td rowspan="2">$\alpha\omega_i$</td></tr>
<tr><td colspan="2">Proof-of-Activity (PoA) [15]</td><td>Online duration</td></tr>
<tr><td rowspan="3">Proof-of-Publication (PoP) [3]</td><td>Proof-of-Memory [16]</td><td>Memory</td><td rowspan="3">ND‡</td><td rowspan="3">$\alpha\omega_i$</td></tr>
<tr><td>Proof-of-Storage [17]</td><td>Disk Storage</td></tr>
<tr><td>Proof-of-Distribution [6]</td><td>Packets Forwarding</td></tr>
<tr><td colspan="2">Proof-of-Stake (Coinage, Strong restriction) [18, 5]</td><td rowspan="2">Account Coinage</td><td rowspan="2">PD</td><td>$\alpha\omega_i \min\{h-1, H\}$</td></tr>
<tr><td colspan="2">Proof-of-Stake (Coinage, Weak restriction)</td><td>$\alpha\omega_i \min\{h, H\}$</td></tr>
<tr><td colspan="5">Fairness-oriented, let $\Upsilon(\omega_i) = \zeta(\omega_i)$, where $\zeta(\omega_i)$ can be defined to be partitioned</td></tr>
<tr><td colspan="2">The PoX schemes</td><td>Types of the System Resource</td><td>ω_i†</td><td>$f_{i,h}$</td></tr>
<tr><td colspan="2">Proof-of-Stake-Velocity [19]</td><td>Account Coinage</td><td>PD</td><td>$\alpha\zeta_i(\omega_i)\mu(\min\{h, H\})$</td></tr>
</table>

† The type of distribution a set of system resource expected to follow is dependent to the considered PoX scheme shown in the first column (see the detail in Section 5.1).

⋆ Pareto distribution. It describes an 80/20-rule-based wealth inequality (see the detail in Section 5.1).

‡ Normal distribution.

2.2. PoX-based Consensus Algorithms

PoW is generalized to the PoX scheme. The PoX scheme describes a system where a unique miner is elected to generate a new block based on a publicly verifiable system resource ratio. The PoX scheme proposed in [3, 4] can be described as follows,

$$\mathcal{P}_{i,\gamma}^{win} = \mathbb{F}\left(\frac{\omega_i}{\sum \omega_i}, \gamma_i\right), \quad \gamma_i \to \omega_i, \tag{1}$$

where $\mathcal{P}_i^{win}$ is the probability of Node-i being elected as the generator of the block, and ω_i is the amount of system resource owned by Node-i. $\sum \omega_i$ is the total amount of system resources across the network, e.g., computation power, token balance, etc.

Function $\mathbb{F}(\cdot)$ denotes a p-VRF applied during the consensus process to randomly select the block generator, subject to the distribution of $\mathcal{P}_i^{win}$, as given in (1). Therein, $\mathbb{F}(\cdot)$ and γ_i can be customized to meet different requirements, and γ_i is used to adjust how much impact is ω_i having on $\mathcal{P}_i^{win}$ (denoted as $\gamma_i \to \omega_i$). For example, a hybrid of PoW and PoP [6] defines γ to be the number of packets that a particular miner has distributed and forwarded, which can accordingly decrease the difficulty to win the puzzle-solving race.

In order to select the block generator in a large-scale network with an unknown network size in practice, a PoX-based algorithm can be any consensus algorithm subject to the Longest Chain Rule [4] that leverages a p-VRF based on any verifiable system resource. We consider two different types of system resources. They are 1) system resources which are independent to its transmission bandwidth (typically, this type implies that the the considered system resource ratio in (1) does not take the transmission bandwidth into account, and this type of resource can be considered independently without network connection); and 2) network resource (typically, the transmission bandwidth corresponds to the network performance). Such algorithm includes, but is not limited to, the consensus algorithms listed in Table 1. For example, [6] considers ω_i as the total

amount of system resource that a specific miner i owns, part of which is γ_i in the form of the number of distributed packets. $\mathbb{F}(\cdot)$ can be a height-oriented factor in Proof-of-Stake-Velocity (PoS-Velocity) [19], e.g., a function with variables ω_i and $\gamma_i \rightarrow h$ (indicating $\mathcal{P}_i^{win}$ is height-oriented with positive correlation). In other words, the longer it has been since the last time a miner was elected as the block generator, the more likely the miner is elected as the block generator in the current round.

The following model is proposed to generalize (1) based on an infinite-dimensional Markov chain. It can be used to describe the PoX-based consensus algorithms in a long-term stable system, in order to evaluate the distribution of the mining winners, and predict the cost-benefit ratio.

3. New Infinite-Dimensional Markov Chain Model for PoX Schemes

In this section, we first provide an overview of the proposed model along with its network settings followed by the detail of the model. The proposed metrics, *Resource Sensitivity*, *System Convergence*, and *Resource Fairness* will be elaborated.

3.1. Overview

For illustration convenience, we consider large-scale synchronous Blockchain networks with reference to the settings of [20] (that at most one miner can successfully mine a block within a time slot). We further consider a sparse Blockchain system in which the value of $\frac{t}{T}$ is sufficiently small and negligible with t denoting the block propagation delay and T denoting the block period. Also, we consider attack strategies which are resource-oriented, where attackers mainly leverage the double spending attacks and selfish mining to maliciously rollback the history based on their current dominated system resource ratio.

The analytical model is designed for analyzing the long-term steady-state (i.e., the probability of each state can be predicted as the system becomes stable) of PoX-based consensus algorithms. This is achieved by considering the resource

distribution that is weighed by a Degree function and a Fairness function (which will be defined in Section 3.3.2). The analytical model features an infinite-dimensional Markov chain to investigate the long-term steady state. We also propose three metrics, namely, *Resource Sensitivity*, *System Convergence*, and *Resource Fairness* (which will be defined in Section 3.4), for evaluation and simulation. To be specific, a generalized form of $\mathcal{P}_{i,\gamma}^{win}$ (the probability of Node-i elected to be the block generator in a particular round) can be obtained, $\mathcal{P}_i$. By using $\mathcal{P}_i$, we can evaluate the PoX-based consensus algorithms in terms of the proposed metrics - *Resource Sensitivity*, *System Convergence*, and *Resource Fairness*.

3.2. System Model - Small-slotted mechanism

In this section, we describe the system model. The notations used are listed in Table 2.

Our proposed analytical model starts with a small-slotted system, where the period of any miner mining a block is denoted as a "round", while a "miner" denotes any node participating in the race to win for the block generator of each round. Each round refers to a block height number and is divided into many small time slots. The number of time slots contained in a round depends on the expected block period, i.e., T. Each of the slots lasts a constant short time. The gap between two consecutive slots can be reduced to satisfy the assumption referred to [20]. This assumption is reasonable as we can make the slots arbitrarily small; see Fig. 1.

Each miner can potentially generate a new block on block height n, based on the amount of its system resources, as can be done by evaluating (1). In some PoX schemes, such as coinage-based PoS and PoS-Velocity, (1) can be affected by the awaiting gap h of each miner, with an upper bound H. The awaiting gap is the gap between the considered miner being the elected generator from the last round to present. There exist the following three possible scenarios for a miner within a slot.

1. *Scenario 1:* None of the miners mines a valid block in the network.

Table 2: Parameters of the analytical model

Symbols	**Description**
h	Awaiting gap that is miner-specific, the gap since the last round a designated miner being the winner until it wins again.*
$\Phi(\cdot)$	A Degree function measuring the impact of h on $f_{i,h}$
$\Upsilon(\cdot)$	A Fairness function defining whether the monopoly of system resource can be avoided
ω_i	The amount of system resource owned by Node-i
N	The number of miners among the entire network
H	The upper bound of h
α	A constant network parameter, normalizing the mining probability $f_{i,h}$ in terms of the size of a time slot
$\Pr(x\|y)$	The transition probability from awaiting gap y to awaiting gap x
R	The mining probability of the entire network per slot
$f_{i,h}$	The mining probability of Node-i per slot at awaiting gap-h
$\pi(h)$	The steady probability of a miner at awaiting gap-h in an arbitrary slot
$\overline{\mathcal{T}_i}$	The average number of awaiting gap for Node-i being the winner since its last winning
$\mathcal{P}_i$	A generalized form of $\mathcal{P}_{i,\gamma}^{win}$ in (1) based on the proposed model
t	The block propagation time
T	The expected value of block period (round)

* This can be any level of grain. For example, it can be block-height-oriented (in terms of the block height), as shown in Section 5 or time-oriented [5]. Alternatively, it can be a customized level of grain can replace the block height or time to meet specific requirements.

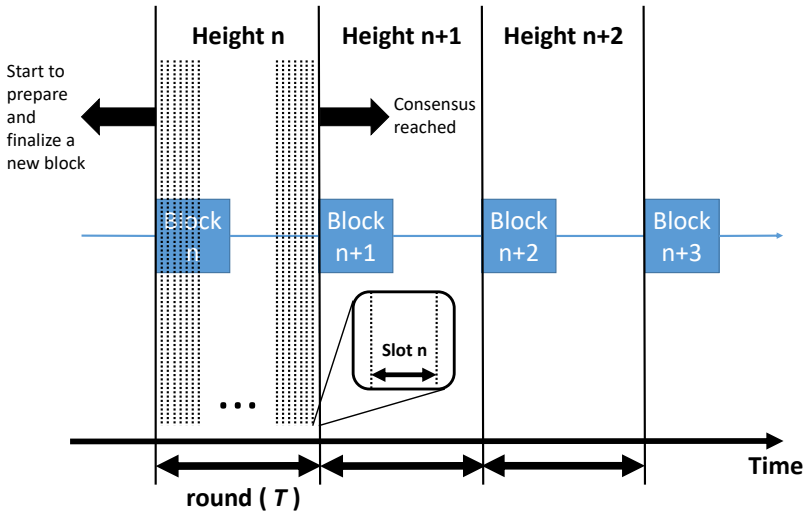


Figure 1: The small-slotted mechanism divides a round into multiple slots. The number of slots contained in a round is subject to the expected value of the block period T.

2. *Scenario 2:* This miner does not mine its own block but accepts a block mined by another miner;
3. *Scenario 3:* This miner mines a block, and the block is immediately accepted by other miners at the beginning of next slot, prior to the mining for the next round;

3.3. The Proposed Analytical Model

To clarify *Scenarios 1-3* in Section 3.2, we present an infinite-dimensional Markov chain. For simplicity, $\Pr(\cdot)$ denotes the simple form of $\Pr(i,\cdot)$ for Node-i; $\pi(\cdot)$ denotes the simple form of $\pi_i(\cdot)$ for Node-i.

3.3.1. The infinite-dimensional Markov chain

Let $\Pr(x|y)$ denote the transition probability of an individual node/miner from awaiting gap y to the awaiting gap x at two consecutive slots. The transition

probability at Node-i can be given by

$$\Pr(h|h) = 1 - R; \tag{2a}$$

$$\Pr(h+1|h) = R - \Pr(1|h); \tag{2b}$$

$$\Pr(1|h) = \begin{cases} f_{i,h}, & \text{if} \quad 1 < h \leq H; \\ f_{i,H}, & \text{if} \quad h > H; \\ 1 - R + f_{i,h}, & \text{if} \quad h = 1; \\ 0, & \text{otherwise.} \end{cases} \tag{2c}$$

In (2), R denotes the mining probability of the whole network at a slot. We consider R is consistent over time, as it must take some k slots for miners to generate a new block for a specific round, while k depending on a constant T can also be considered to be constant in the long term. Recall that h is miner-specific (and is the simple form of h_i). h is not the actual height of the chain, but the awaiting gap which can be block-height-oriented (see Table 2), between the previous round where a miner being the block generator and the current round where the same miner being selected again.

In (2), a miner running at an awaiting gap h within the considered slot behaves either in the following way.

- Eq. (2a) refers to *Scenario 1*. It provides the transition probability that no new block is mined in the network during this time slot. Thus, the miner is still at the awaiting gap h in the next slot.

- Eq. (2b) refers to *Scenario 2*. It provides the transition probability that this miner does not generate a new block, and a new block generated by another miner is finalized. Thus its awaiting gap h increases by 1, with a probability of $R - \Pr(1|h)$.

- Eq. (2c) refers to *Scenario 3*. It provides the transition probability that the miner is elected as the block generator to finalize a new block. Thus,

its awaiting gap h returns to 1, with a probability of $f_{i,h}$ if $1 < h \leq H$. Otherwise, $f_{i,H}$ remains unchanged if $h > H$ with an upper bound H set.

With an increasingly comparable network latency t, the probability of finalizing a valid block per unit time (the slot time) decreases. This leads to a larger average number of slots contained in a round due to the increasing likelihood of forks per slot time, which results in a slower block period; see (2). The deviation (decreased probability of the generation of a valid block per slot time) implicitly captures the impact of network delay in practical asynchronous networks on the overall mining process and block miming at block-n. Intuitively, the deviation depends on the value of $\frac{t}{T}$. The probability of finalizing a valid block per slot time incur deviation away from the estimated one derived from our model as $\frac{t}{T}$ increases. In such way, the deviation can correspond to the value of $\frac{t}{T}$.

To simplify and satisfy the small-slotted mechanism, we consider a small $\frac{t}{T}$ where t denotes the propagation delay and T denotes the expected block period (more details in Section 4.1). Thus the miners avoid needing to consider forking, and have sufficient time to mine a potential unique block at the same block height-n among all received block at height-(n-1). With the help of a game-theoretic incentive scheme [1], the miners are willing to be consistent with each other about the finalized block for the current round (the block is broadcast and accepted by all miners), e.g., based on the difficulty defined in Bitcoin [1] or Ethereum [21]. In other words, this situation can be interpreted to a small-slotted mechanism with sufficiently small and negligible $\frac{t}{T}$, i.e., the first generated block can be finalized and accepted by all miners immediately to reach the consensus, and consistency can be satisfied by the end of this round. Thus, the infinite-dimensional Markov Chain satisfies our proposed small-slotted mechanism, hence *Scenarios 1-3* as defined above can hold. As a consequence for the results of our calculation and simulation, a small $\frac{t}{T}$ minimizes the impact of propagation latency.

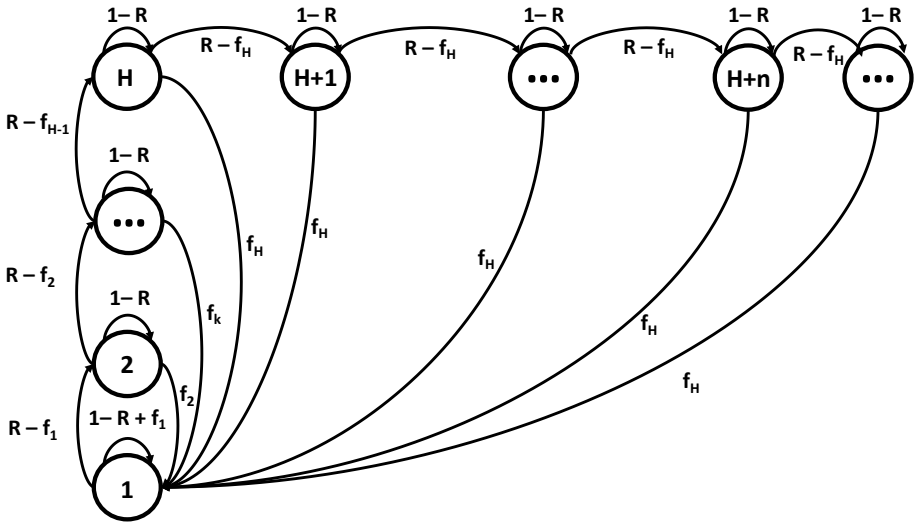


Figure 2: The state transition of the proposed infinite-dimensional Markov chain at Node-i. $f_{i,h}$ is denoted as f_h for simplicity.

3.3.2. The per-miner-per-slot mining probability $f_{i,h}$

According to (2c), $f_{i,h}$ provides the per-slot mining probability of Node-i at awaiting gap-h. $f_{i,h}$ depends on other nodes. It reflects the system resource distribution of a specific node, Node-i, at the state with the awaiting gap h. We propose the following expression for $f_{i,h}$ to unify it for a range of popular PoX schemes:

$$f_{i,h} = \alpha \Upsilon(\omega_i)\Phi(h, H) \leq R. \tag{3}$$

Here, $\Upsilon(\cdot)$ and $\Phi(\cdot)$ are defined as the Fairness function and Degree function, respectively.

- *Fairness function* indicates whether the weighted resource distribution is Fairness-oriented, and how *Resource Fairness* affects the weighted resource distribution if any.
- *Degree function* can be customized in terms of the awaiting gap h, along

with an upper bound H. It measures how much the awaiting gap impacts on the resource distributed to each miner, in turn, the probability that a miner is elected to be the block generator.

For example, $\Upsilon(\omega_i) = \omega_i$ indicates an inactive Fairness function, while $\Upsilon(\cdot)$ can be a partition function if $f_{i,h}$ is Fairness-oriented (so that the impact from a high ω_i to $f_{i,h}$ can be restrictive). α is a network-level parameter normalizing the probability and accounting for the size of a time slot. $\Phi(\cdot)$ can be either equal to 1 (an inactive Degree function), or customized depending on the awaiting gap h and an upper bound H. For example, $\Phi(\cdot) = \min\{h, H\}$ (a positive Degree function that delivers a positive correlation of $f_{i,h}$ and h), outputting the minimum value between the current h and H, is used in the existing PoS consensus algorithm [18]. The expressions for $f_{i,h}$ under currently popular PoX schemes are shown in Table 1.

3.3.3. Steady-state probability

In this section, the steady-state probability of a miner at awaiting gap-h at an arbitrary slot is evaluated. The steady-state probability, denoted by $\pi(h)$, can be calculated in three cases, i.e., $h = 1$, $1 < h \leq H$ and $h > H$. We consider that any $f_{i,h}$ with awaiting gap $\forall h > H$, equals to $f_{i,h}$. $\pi(h)$ can be derived based on (2) as follows.

In the case of $1 < h \leq H$:

The steady-state probability $\pi(h)$ can be given by

$$\begin{aligned} \pi(h) &= \Pr(h|h-1)\pi(h-1) + \Pr(h|h)\pi(h) \\ &= (R - f_{i,h-1})\pi(h-1) + (1-R)\pi(h), \quad 1 < h \leq H, \end{aligned} \tag{4}$$

which is derived from (2). In particular, $\pi(h)$ is equal to the sum of the probabilities, 1) that *Scenario 2* happens given that the considered node is on the

awaiting gap $h-1$, i.e., $\Pr(h|h-1)\pi(h-1)$; and that 2) *Scenario 1* happens given that the considered node is on the awaiting gap h, i.e., $\Pr(h|h)\pi(h)$.

By rearranging (4), $\pi(h)$ can be rewritten as

$$\pi(h) = \frac{R - f_{i,h-1}}{R}\pi(h-1) \tag{5a}$$

$$= \pi(1)\prod_{h'=1}^{h-1}\frac{R - f_{i,h'}}{R}, \quad 1 < h \leq H, \tag{5b}$$

where (5b) is obtained by recursively substituting $\pi(h-1)$ with $\pi(h-1)$, $\pi(h-2)$, $\cdots$, $\pi(2)$ into the right-hand side of (5a).

In the case of $h > H$:

The steady-state probability $\pi(h)$ can be given by

$$\begin{aligned}\pi(h) &= \Pr(H+1|H)\pi(h-1) + \Pr(h|h)\pi(h) \\ &= (R - f_{i,h})\pi(h-1) + (1-R)\pi(h), \quad h > H,\end{aligned} \tag{6}$$

which is also derived from (2). In particular, $\pi(h)$ is equal to the sum of the probabilities that, 1) *Scenario 1* happens given that the considered node is on the awaiting gap h, i.e., $\Pr(h|h)\pi(h)$; and that 2) *Scenario 2* happens given that the considered node is on the awaiting gap $h-1$, i.e., $\Pr(H+1|H)\pi(h-1)$.

Note that in our proposed model, there exist the states with $h > H$ in which the probability of *Scenario 2* is unchanged (i.e., $\Pr(H+1|H)$). The probability that the miner of interest has an awaiting gap H can be interpreted as an accumulation of all $\pi(h)$ with $h > H$, i.e., $\lim_{h\to\infty}\sum_{x=H+1}^{h}\pi(x)$.

By rearranging (6), $\pi(h)$ can be rewritten as

$$\pi(h) = \frac{R - f_{i,h}}{R}\pi(h-1) = \pi(H)\left(\frac{R - f_{i,H}}{R}\right)^{h-H} \tag{7a}$$

$$= \pi(1)\left(\frac{R - f_{i,H}}{R}\right)^{h-H}\prod_{h'=1}^{H-1}\frac{R - f_{i,h'}}{R}, \quad h > H, \tag{7b}$$

where (7a) can be converted $\pi(h)$ to multiple of $\pi(H)$, and (7b) is obtained by substituting $\pi(H)$ into (5b).

In the case of $h = 1$:

As $\lim_{h\to\infty} \sum_{x=1}^{h} \pi(x) = 1$, we can add up $\pi(h)$ in all the three cases, i.e., $h = 1$, $1 < h \leq H$, and $h > H$, as given by

$$\begin{aligned} 1 &= \pi(1) + \sum_{x=2}^{H} \pi(x) + \lim_{h\to\infty} \sum_{x=H+1}^{h} \pi(x) \\ &= \pi(1) \left[1 + \sum_{h=2}^{H} \left(\prod_{h'=1}^{h-1} \frac{R - f_{i,h'}}{R} \right) + \frac{R - f_{i,H}}{f_{i,H}} \prod_{h'=1}^{H-1} \frac{R - f_{i,h'}}{R} \right], \end{aligned} \tag{8}$$

wherein,

$$\begin{aligned} \lim_{h\to\infty} \sum_{x=H+1}^{h} \pi(x) &= \lim_{h\to\infty} \sum_{x=H+1}^{h} \pi(H) \left(\frac{R - f_{i,H}}{R} \right)^{x-H} \\ &= \pi(H) \left(\frac{R - f_{i,H}}{R} \right) \frac{1}{1 - \frac{R - f_{i,H}}{R}} \\ &= \pi(H) \frac{R - f_{i,H}}{f_{i,H}}, \end{aligned}$$

which is derived from (7a). Also from (8), the steady probability $\pi(1)$ can be obtained as

$$\pi(1) = \frac{1}{1 + \sum_{h=2}^{H} \left(\prod_{h'=1}^{h-1} \frac{R - f_{i,h'}}{R} \right) + \frac{R - f_{i,H}}{f_{i,H}} \prod_{h'=1}^{H-1} \frac{R - f_{i,h'}}{R}}, \qquad h = 1. \tag{9}$$

Consequently, $\pi(h)$ can be derived with (5), (7) and (9) for any awaiting gap h in the cases with $1 < h \leq H$, $h > H$, and $h = 1$.

3.3.4. Relation between the total per-slot mining probability R and the per-slot mining probability of an individual node $f_{i,h}$

Recall the mining probability of the entire network per slot, R, as given in (2). It can be interpreted as the steady mining rate of the whole network. R is given by

$$R = \lim_{h\to\infty} \sum_{i=1}^{N} \sum_{x=1}^{h} f_{i,x} \pi_i(x), \tag{10}$$

where $\pi_i(x)$ denotes the steady-state probability of Node-i with the awaiting gap x, and $\pi_i(x)$ can be obtained by substituting (3) into (5) and (7).

By using (5) and (7), the total per-slot mining probability R can be expanded to the following form:

$$R = \sum_{i=1}^{N} f_{i,1}\pi_i(1) \tag{11a}$$

$$+ \sum_{i=1}^{N}\sum_{h=2}^{H} f_{i,h}\pi_i(1)\left(\prod_{h'=1}^{h-1}\frac{R - f_{i,h'}}{R}\right) \tag{11b}$$

$$+ \sum_{i=1}^{N} f_{i,h}\pi_i(1)\frac{R - f_{i,H}}{f_{i,H}}\left(\prod_{h'=1}^{H-1}\frac{R - f_{i,h'}}{R}\right). \tag{11c}$$

Therefore, R can be calculated with (11), where $\pi_i(1)$ is the corresponding steady-state for Node-i with awaiting gap-1; therefore, $\pi_i(1) = \pi(1)$. $\pi(1)$ is given in (9).

3.3.5. Generalization of $\mathcal{P}_{i,\gamma}^{win}$

Recall that $\mathcal{P}_{i,\gamma}^{win}$ is the probability of Node-i being elected as the block generator. We derive $\mathcal{P}_i$ which generalizes $\mathcal{P}_{i,\gamma}^{win}$ in terms of $f_{i,h}$ for PoX schemes. By using such generalized form, γ is abstracted into the configurable functions (Fairness function and/or Degree function) of $f_{i,h}$ for any Node-i. As such, any miners can obtain the probability being elected as the block generator by calculating $f_{i,h}$.

We define $\mathcal{T}_i$ as the block generation rate of Node-i. It is measured by the average number of awaiting gaps required for the miner to be elected again. For simplicity of notation, we let $f_{i,h} = \alpha\Upsilon(\omega_i)\Phi(h,H) = \alpha_i\Phi(h,H)$, where $\alpha_i = \alpha\Upsilon(\omega_i)$ and α is a network parameter normalizing the probability. This operation is reasonable as the *Degree function* $\Phi(\cdot)$ can equal to 1 and be ignored for some PoX schemes (e.g., PoW), while we can realize α_i is (non-)Fairness-

oriented by observing whether $\Upsilon(\omega_i) = \omega_i$ holds. Then, $\mathcal{T}_i$ can be given by

$$\begin{aligned}\mathcal{T}_i &= \lim_{h\to\infty}\sum_{x=1}^{h} x\frac{\pi(x)}{\pi(1)}f_{i,x} \times \lim_{k\to\infty}\sum_{x=0}^{k}(1-R)^x \\ &= \left(\sum_{x=1}^{H} x\frac{\pi(x)}{\pi(1)}f_{i,x} + f_{i,H}\lim_{h\to\infty}\sum_{x=H+1}^{h} x\frac{\pi(x)}{\pi(1)}\right)\times\frac{1}{R} \\ &= \frac{\sum_{x=1}^{H} x\frac{\pi(x)}{\pi(1)}f_{i,x}}{R} + \frac{f_{i,H}\left(\prod_{h'=1}^{H-1}\frac{R-f_{i,h'}}{R}\right)}{R} \times \lim_{h\to\infty}\left[\sum_{x=H+1}^{h} x\left(\frac{R-f_{i,H}}{R}\right)^{x-H}\right].\end{aligned} \tag{12}$$

As a result, $\mathcal{P}_i$ can be given by

$$\mathcal{P}_i = \frac{1}{\mathcal{T}_i}. \tag{13}$$

Note that $\lim_{k\to\infty}\sum_{x=0}^{k}(1-R)^x = 1/R$, and it indicates that no new block has been finalized in the last k slots of the current round. $\frac{\pi(x)}{\pi(1)}f_{i,x}$ is the probability that the awaiting gap of Node-i starts at the height of x. Here, $\pi(x)$ is divided by $\pi(1)$ to eliminate the effect of the initial state (i.e., $h = 1$).

As a result, $\mathcal{T}_i$ can be calculated based on (5) to (11), and the given $\{\alpha_i, \Upsilon(\cdot), \Phi(\cdot)\}$. Since $\mathcal{T}_i$ is the generation rate of Node-i (i.e., how many awaiting gaps on average a miner needs to wait until it can be elected as the block generator since the last time it was elected), the generalized form of $\mathcal{P}_{i,\gamma}^{win}$ in (1), $\mathcal{P}_i = 1/\mathcal{T}_i$.

3.4. Proposed Evaluation Metrics

Based on the proposed analytical model and the resulting $\mathcal{P}_i$ in (12) and (13), we propose three important metrics to evaluate PoX schemes, i.e., *Resource Sensitivity*, *System Convergence*, and *Resource Fairness*. Currently popular PoX-based consensus algorithms, as summarized in Table 1, can all be evaluated by using the proposed metrics.

3.4.1. Resource sensitivity

The proposed *Resource Sensitivity* evaluates *the correlation between the system resource ratio* $\frac{\omega_i}{\sum\omega_i}$*, and the average probability of Node-i being the elected as*

the block generator, $\mathcal{P}_i$.

For any PoX scheme, we have $\mathcal{P}_i = f(z)$, where $z = \omega_i / \sum \omega_i$. The gradient g of any point and the corresponding area $E(g)$ bounded by $f(z)$ can be defined as

$$g = \frac{\mathrm{d}(f(z))}{\mathrm{d}z};$$

$$E(z) = \int_0^{50\%} f(z)\mathrm{d}z, \quad \forall g \geq 0.$$

We define *Zero-Resource-Sensitivity* if $g = 1$; *Positive-Resource-Sensitivity* if $g > 1$; and *Negative-Resource-Sensitivity* if $0 \geq g < 1$. *Zero-Resource-Sensitivity* indicates the mining probability $\mathcal{P}_i$ is proportional to the resource ratio in a 1:1 ratio. The 50% is the resource ratio with which this node can launch the double-spending attack in a *Zero-Resource-sensitive* context (1:1 ratio). A positive sensitivity leads to a larger impact to $\mathcal{P}_i$ by the resource ratio, while a negative one leads to a smaller impact to $\mathcal{P}_i$. We also assert the relationship between *Resource Sensitivity* and the security of a PoX scheme, i.e., the smaller $E(z)$ is, the less Resource-sensitive it can achieve, thus a more secure PoX scheme that has better performance on *Resource sensitivity*.

By referring to the security model proposed in Bitcoin's whitepaper [1], security is specified to be the probability that an attacker could catch up with loyal miners in some consecutive rounds. It is closely dependent on the probability that an attacker potentially wins the puzzle race and generates a malicious block, as captured by our proposed $\mathcal{P}_i$. For example, $\mathcal{P}_i$ of traditional PoX schemes, e.g., PoW and PoS, leads to a *Zero-Resource-Sensitivity* with $f_{i,h} = \alpha\omega_i$, $\Upsilon(\omega_i) = \omega_i$, and $\Phi(\cdot) = 1$ (which is the identity line illustrated as the dark blue solid line in Fig. 6). This consequently indicates that $\mathcal{P}_i$ increases along with the system resource in a 1:1 ratio, i.e., $E(z) = \mathbf{1}$ (i.e., an isosceles right triangle. Here "$\mathbf{1}$" represents a normalized area.), hence more Resource-sensitive and less secure than those with $E(z) < \mathbf{1}$.

Resource Sensitivity is complementary to the Bitcoin's security model, in terms of the correlation between the system resource ratio and the average

probability of any node being the block generator. Such definition of *Resource Sensitivity* based on the resource distribution is reasonable, as influential attack strategies (e.g., selfish mining and double-spending attack) depend on the resource distribution.

3.4.2. System convergence

The entire system takes rounds to reach the steady-state, while the steady-state is satisfied if both (4) and (6) hold. Thus, *System Convergence* is evaluated by *the number of rounds needed to reach steady-state.*

Here, the gap between the theoretical value of $\mathcal{T}_n$ (driven by (12)), and the simulation one (obtained by the Monte Carlo-based simulation) is upper bounded by a chosen tolerance (the steady-state is reached if the tolerance is satisfied). The tolerance is chosen as $\sim 3\%$ (see Fig. 4). This is because the PoX schemes considered in Table 1 have a margin of error of 3% (the y-axis of Fig. 4) while the ratio of system resource owned by an arbitrary node $f_{i,h} \simeq 50\%$ (the x-axis of Fig. 4). This satisfies the requirement of the fault tolerance (FT) of PoX-based consensus algorithms, $N > 2\mathrm{f} + 1$ (N denotes the total number of participating miners; f denotes the number of malicious miners).

A stable $\mathcal{P}_i$ can be useful for each individual miner to estimate the profits more accurately, while an unstable consensus algorithm does not provide such benefits in the absence of a steady-state. As a result, *System Convergence* can be an important metric for rational users who tend to run more controllable PoX schemes. They will be able to observe how much longer they need to wait until the entire system becomes stable and predictable with high precision, so that a more controllable cost-risk assessment can be conducted. Here, a more controllable cost-risk assessment implies that, the faster a system becomes stable, the earlier users obtain an accurate profit estimation, thus the users can be more thoroughly prepared for all possible financial challenges. Moreover, we prove the model realistic with *System Convergence* in a real-world system based on the simulation in Section 5.2.1. The simulation reveals that our model

can provide reasonably accurate estimation of the number of rounds in the real world, especially in a well-connected network with low latency.

3.4.3. Resource fairness

Resource Fairness [22] is defined as *an indicator that indicates (in the case of* $E(z) < \mathbf{1}$*) whether there exists a threshold* η *with respect to the resource ratio, to the right-hand-side of which* $g \to 0$ *based on the corresponding Fairness function* $\Upsilon(\cdot)$.

The asymptotically zero gradient ($g \to 0$) provides *Resource Fairness* against a wealthy, resourceful node (i.e., Fairness-orientation). Here, a wealthy node has at least 50% resource ratio, with which this node can launch the double-spending attack in a *Zero-Resource-sensitive* context (1:1 ratio).

Resource Fairness is a specific requirement of a PoX-based consensus algorithm. It prevents monopolization of wealthy miners, and incentivizes all miners to participate in the mining process. The miners are expected to voluntarily apply *Fairness function* because of the similar reason how miners remain decentralized among centralized mining pools [23][1]. *Resource Fairness* has an impact on *Resource Sensitivity* by narrowing down the gap between the lowest and highest $\mathcal{P}_n$ with an unchanged value of H. *Resource Fairness* also affects *System Convergence* by introducing a many-to-one function with respect to h, e.g., a partition function $\zeta(\cdot)$ in Section 5. As such, the Fairness function $\Upsilon(\cdot) = \zeta(\cdot)$ can significantly decrease the number of rounds to reach the steady-state; see Fig. 7 for further details.

[1]The loss caused by a double-spending attack launched by a centralized mining pool will make the participated miners migrated out. Similarly, miners are expected to voluntarily prevent the monopoly by restricting the wealthy when they are rich enough.

4. Consideration on Network Setting

4.1. Sparse Blockchain Networks

Our model, using the similar assumption of [20] , i.e., a well-connected network with a small $\frac{t}{T}$, and $\frac{\sum \omega_i^{\text{forked}}}{\omega}$ is also negligible with a constant $\sum \omega$. A small $\frac{t}{T}$ also contributes to a negligible orphan rate, giving attackers no opportunities to exploit any attack strategies on the orphans; refer to [8, Section IX-A].

Forking is purposely prevented when every miner mines on a new block with the same block height, and the assumption of a zero propagation time t is subject to the following reasons.

For the PoW schemes, the de facto probability that a forked block is mined and inserted is also (apart from $\mathcal{P}_{i,\gamma}^{win}$) directly proportional to,

1. the ratio between t and T, i.e., $\frac{t}{T}$;
2. the ratio of computation resource $\sum \omega_i^{\text{forked}}$ working on a block that would be an orphan one, to the total resource ω; i.e., $\frac{\sum \omega_i^{\text{forked}}}{\omega}$ (the *chain quality* proposed in [20, 13]).

The upper bound of time consumption to finalize a new block, δ, becomes unpredictable as $\frac{t}{T} \to 1$. This means the synchronization becomes looser so that the performance and security of PoW deteriorates. Thus, as we consider

1. $\frac{t}{T}$ approaches zero (the throughput is not considered here);
2. rational miners are incentivized to wait until the finalized block of the current round is consistently accepted across the whole network before mining the next block, [2]

$\frac{\sum \omega_i^{\text{forked}}}{\omega}$ can be negligible in our model.

[2] In this paper, we consider that the attackers do not behave maliciously at the time when the honor miners are waiting for the consistency while T becomes large. When $\frac{t}{T} \to 0$, $T > \delta$, the partially synchronous network can be thought to be completely synchronous, in turn, satisfies the proposed small-slotted mechanism.

For the PoS and other PoX schemes without the computation resource, punishment mechanisms (such as the Slashers in Ethereum 2.0 [24] or the Verifiable Delay Function (VDF) [25]) are applied to miners who mine multiple blocks on the same height to prevent Nothing-at-stake and long-range attacks. In the case that $\frac{t}{T}$ approaches zero, $\frac{\sum \omega_i^{\text{forked}}}{\omega}$ is also negligible.

4.2. Large-scale Blockchain Networks

The proposed model is designed for a large-scale Blockchain network with N potential miners competing for the role of block generator. We define a finite scale of an upper bound of the awaiting gap h, i.e., $N > H$. This is reasonable and usually implemented in PoS-Velocity [19]. Similar designs have also been implemented to prevent coins hoarding. This is a critical issue of traditional coinage-based PoS. Attackers hoard the coins on multiple accounts with infinite H to boost the success probability [3]. On the other hand, it is practical to implement an upper bound so that the physical operation can be more affordable due to the worst-case searching complexity of $O(NH)$ for traversing the awaiting gaps of all N miners in the entire network.

5. Simulation and Evaluation

In this section, we present the simulation and evaluation, based on *Resource Sensitivity*, *System Convergence*, *Resource Fairness* of our proposed analytical model of the considered PoX schemes listed in Table 1.

5.1. Framework

The simulation setting is presented in the following.

Hardware setting: A 2017 iMac with 10.13.3 macOS High Sierra, a processor of 2.3GHz Intel Core i5 and 16 GB 2133 MHz DDR4 memory are used.

Software setting: We carry out a Monte Carlo simulation using Python-2.7 to conduct the mining process given N, H, and $\alpha = \frac{1}{2H\sum \omega_i}$, to obtain the simulated value of $\mathcal{P}_i$ for Node-i. The calculated value of $\mathcal{P}_i$ for Node-i based on (13) is obtained by using Matlab-2017. Here, the values of N, H, and α are

set based on the hardware performance.

Samples setting: The parameter $f_{i,h}$ for each of the PoX-based consensus algorithms is described in Table 1, given the distribution of $\{\alpha_i\}$. Here, a coinage-based PoS with a strong restriction implies that the awaiting gap of an elected generator starts from 0 (zero probability of being elected consecutively), while a weak restriction starts from non-zero.

In this simulation, we use a normal distribution and a Pareto distribution for the resource distribution among the miners, with normal-distributed wealth inequality and 80/20-rule-based wealth inequality, respectively. Any PoX scheme where miners need to put great efforts, e.g., computational power and token values, in winning the race results in a Pareto Distribution [26], while it is normal-distributed if the system resource becomes less costly to the system resource among the miners, e.g., PoP. As such, we assume that $\{\alpha_i\}$ of PoW, PoS, and PoA follow the Pareto distribution; PoP follows the normal distribution. To be specific, we implement Proof-of-Collaboration (PoC) [5][3], for the simulation of both strongly restricted and weakly restricted coinage-based PoS consensuses.

We implement a typical type of Fairness-oriented PoS-Velocity with a Pareto distribution in the simulation, where the Fairness function $\Upsilon(\omega_i) = \zeta(\omega_i)$ and the Degree function $\Phi(\cdot) = \mu(\min\{\cdot\})$ are used[4]. Here, we use the definition

[3]This consensus defines two new parameters, $\mathcal{CC}$ and $\mathcal{P}_{PoC}$. The winner of each round of generating the new block will earn $\mathcal{CC}$, while $\mathcal{P}_{PoC}$ is defined as the time since the last $\mathcal{CC}$ changes. On the other hand, $\mathcal{P}_{PoC} \in [\mathcal{L}, \mathcal{R}]$, where $\mathcal{L}$ can be constant during a long-term period and $\mathcal{R} = 3\mathcal{L}$. Also, $\mathcal{P}_{PoC}$ of the winner is set to 0 for the next single round (so that $\mathcal{P}_{PoC}$ starts from 0). Therefore, the PoC consensus can be regarded as a variant of strongly restricted coinage-based PoS and $f_{n,h} = \alpha_n \min\{h-1, H\}$, where $1 \leq h \leq H$, $h = \mathcal{P}_{PoC}$, $h = 1 = \mathcal{L}$, $h - 1 = 0$, $H = \mathcal{R}$. In addition, the PoC consensus can be with a weak restriction if we set $\mathcal{P}_{PoC}$ to $\mathcal{L}$ instead of 0.

[4]An example is that, $\zeta(\cdot)$ can be a partition function where the lower and upper bound are pre-defined to avoid the monopoly and starvation; $\mu(\cdot)$ can be a non-linear function where the gradient g remains flat from the beginning up to a threshold, followed by a sharp increase after the threshold (so that the poor miners can be more likely to win).

in [3] of PoS-Velocity. That is the linear $\Phi(\cdot)$ is substituted by other forms of Degree functions, e.g., a non-linear function $\mu(\cdot)$; the Fairness function is set to the form of a partition function, e.g., $\zeta(\cdot)$.

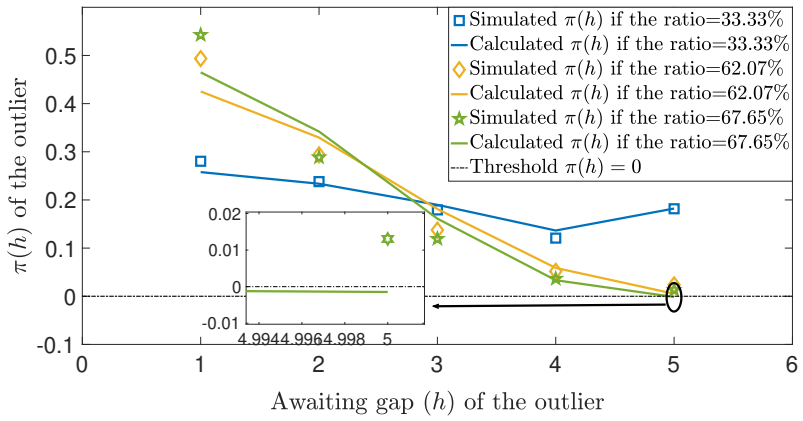
5.2. Simulation Result

First, the scope of our proposed model in terms of the margin of error is discussed. After that, the proposed metrics, *Resource Sensitivity*, *System Convergence*, and *Resource Fairness* are simulated among the (non-)Fairness-oriented PoX schemes listed in Table 1. Finally, we deliver the implicit findings for miners to evaluate PoX schemes in different scenarios based on the proposed model.

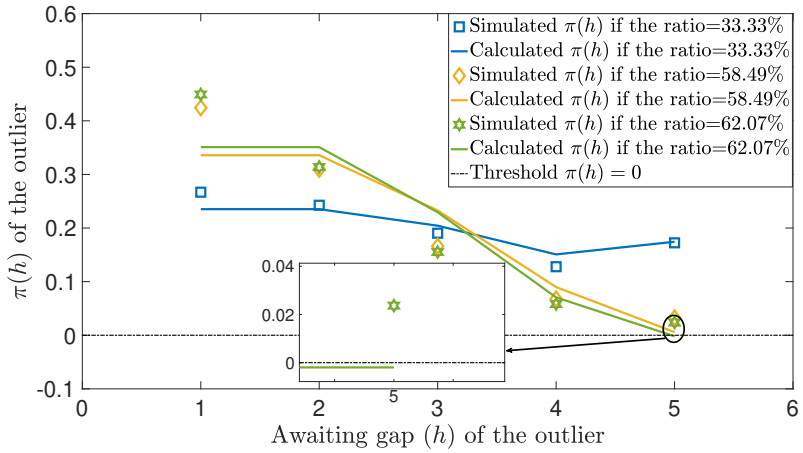
5.2.1. Accuracy of the proposed model - margin of error

To investigate the accuracy of the estimation derived from our model and possible factors impacting on such accuracy, we consider two types of margin of errors in this section.

- **Standard Error** (S). It is also known as the standard error of the estimate, representing the average distance between the estimated values and observed values. Smaller S implies a better fitted model.
- **Adjusted R-squared** ($ARSQ$) [27]. $ARSQ$ is known as the adjusted coefficient of determination in statistics, representing the ratio of the variance in the dependent variable that is predictable from the independent variable(s) with considering the number of independent variable(s). It is often used to assess how good the estimated model fit the observed values, the closer to 1 the better. Note that, in our simulation $ARSQ$ is a complemented metrics to S as a non-linear model may imply an inaccuracy due to the unexpected over-fitting. A high-$ARSQ$ indicates a good fitting only if S is within the acceptable range. In contrast, we can still reliably approximate the trend with a high-$ARSQ$ when S is slightly higher than the range.



(a) $f_{i,h} = \alpha \min\{h, H\}$



(b) $f_{i,h} = \alpha \min\{h - 1, H\}$

Figure 3: $\pi(h)$ of the outlier with a Pareto distributed system resource for coinage-based PoS and Non-Fairness-oriented PoS-Velocity respectively, where $N = 10$, $H = 5$, $\alpha = \frac{1}{2H\sum\omega_i}$. An invalid $\pi(H)$ that is negative appears when $h = H$.

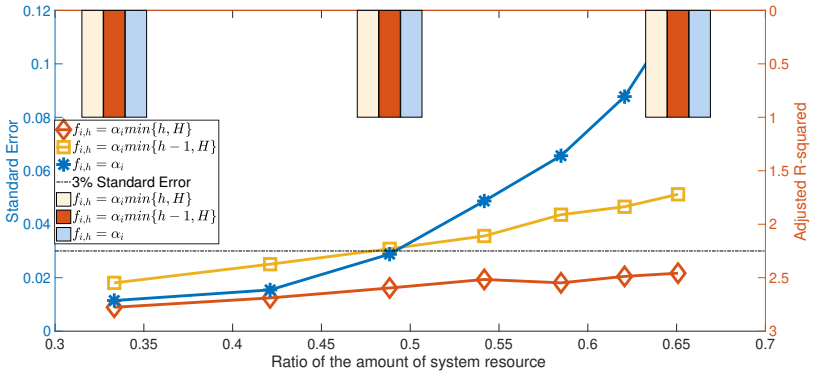


Figure 4: The margin of error with the growth of the resource ratio owned by an arbitrary miner that is the outlier, where $N = 10$, $H = 5$, $\alpha = \frac{1}{2H\sum\omega_i}$, in terms of both S and $ARSQ$. Here, the system resource is Pareto distributed. Note that the ratio is the system resource ratio that a specific outlier miner owns.

Our analytical model is applicable to Pareto distributions (that is the worst case), where the outlier owns up to 50% of the system resource that is equal to the FT of all PoX schemes. An outlier denotes Node-i that owns the majority of the Pareto-distributed system resource. For example, in the following list if $N = 10$,

$$\boldsymbol{\omega} = [0.01, 0.02, 0.03, 0.04, 0.05, 0.06, 0.07, 0.08, 0.09, 0.55],$$

where the n-th element in the list is the ratio of the amount of system resource of Node-i. The node with $\omega = 0.55$ is defined as the outlier.

According to Fig. 3, when $f_{i,h} = \alpha_i \min\{h, H\}$ (see Fig. 3(a)) and $\alpha_i \min\{h-1, H\}$ (see Fig. 3(b)), the invalid negative $\pi(i, H)$ appears at $h = H$, as the ratio of system resource owned by Node-i increases.

Fig. 4 shows the correlation of the resource ratio owned by the outlier, with the two types of margin of error between the estimated and simulated values. It shows that $ARSQ$ of all considered $f_{i,h}$ remains closed to 1, which results in a good fitting if S is within the acceptable range. S remains low when the ratio of the amount of system resource is less than 50% for all considered $f_{i,h}$. Also, S increases exponentially as the ratio increases for $f_{i,h} = \alpha_i$ (the blue

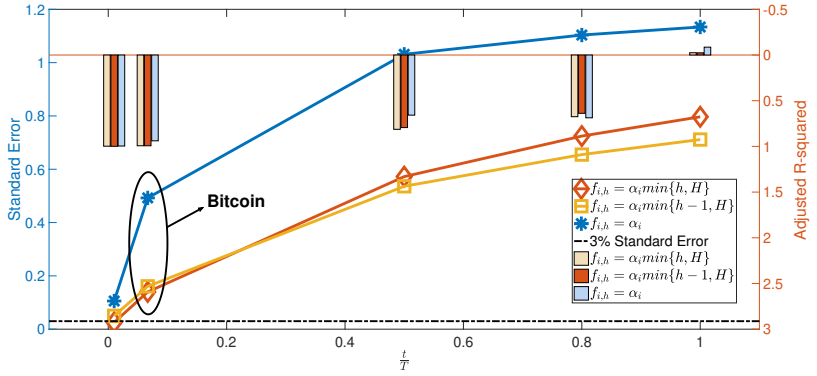


Figure 5: The margin of error with the growth of $\frac{t}{T}$, where $N = 10$,$H = 5$,$\alpha = \frac{1}{2H\sum\omega_i}$, in terms of both S and $ARSQ$. Here, the system resource is Pareto distributed with the ratio of the amount of system resource owned by a specific outlier miner is 33%.

line). Thus, it can be concluded that, the proposed model suits in the Pareto distribution with an outlier owning up to $\sim$ 50% resource, but does not suit an accurate prediction for a Pareto-distributed system with an outlier that is too fart apart (greater than $\sim$ 50%), except for algorithms satisfying *Resource Fairness* (referring to the example of PoS-Velocity shown in Table 1). In spite of this, the proposed model can still be reliable on approximating the trend. Note that the smallest outlier has satisfied the required FT ($N \geq 2f + 1$), where f is the number of faulty miners. This consequently leads to an acceptable range of S for the accuracy of the proposed model, i.e., 3%.

Fig. 5 shows the correlation of $\frac{t}{T}$ with the two types of margin of error between the estimated and simulated values. By investigating what range of $\frac{t}{T}$ the margin of error can be acceptable, we can subsequently determine the upper bound of $\frac{t}{T}$ which can tolerate the possible deviation in (2). It shows that the values of $ARSQ$ of all considered $f_{i,h}$ remain closed to 1 when $\frac{t}{T} \leq \frac{40}{600}$ (Bitcoin point, 95% confident interval) [1, 28], decrease smoothly when $\frac{t}{T} \leq 0.8$, and incur a sharp decrease onwards. S of $f_{i,h} = \alpha_i \min\{h, H\}$ and $f_{i,h} = \alpha_i \min\{h-1, H\}$ remain closed to the 3% range when $\frac{t}{T}$ falls around the Bitcoin point, which still results in a reliable trend-approximation. However, S

of $f_{i,h} = \alpha_i$ (the blue line) supports the reliable trend-approximation only if $\frac{t}{T}$ stands around the Bitcoin point, and incurs a sharp increase onwards. The same circumstance happens for $f_{i,h} = \alpha_i \min\{h, H\}$ and $f_{i,h} = \alpha_i \min\{h-1, H\}$ if $\frac{t}{T}$ is greater than the Bitcoin point. Thus, it can be concluded that, the proposed model supports a reliable trend-approximation for $\frac{t}{T}$ that is smaller than the Bitcoin point.

Validated by Figs. 3 to 5, it can be further concluded that

- the model is accurate if the FT of PoX schemes is satisfied with either Pareto-distributed or normal-distributed resource;
- the model can provide a reliable trend-approximation when $\frac{t}{T}$ is sufficiently small (the network latency is comparatively negligible to the block period), which corresponds to the circumstance of a well-connected network with low latency in the real world.

5.2.2. Resource sensitivity

We simulate the process ranging from PoW to PoP, and both of the coinage-based PoS with strong and weak restrictions, as shown in Table 1. Also, the corresponding calculated values are obtained by calculating (13) under different settings of $f_{i,h}$.

Finding 1: The coinage-based PoS (Strong restriction) [18, 5] has the best performance on Resource Sensitivity among our considered non-Fairness-oriented PoX schemes.

This finding is revealed in Fig. 6, where $\mathcal{P}$ is subject to the ratio of the amount of system resource. An identity line regardless of the distribution type is obtained for $f_{i,h} = \alpha_i$ (the dark blue line), i.e., zero-Resource-sensitive. Note that $\mathcal{P}_i$ is collectively generalized as $\mathcal{P}$ among the miners. The light blue curve of $f_{i,h} = \alpha_i \min\{h-1, H\}$ appears to have a better performance on *Resource Sensitivity* than that of $f_{i,h} = \alpha_i \min\{h, H\}$ (the purple line) due to the setting

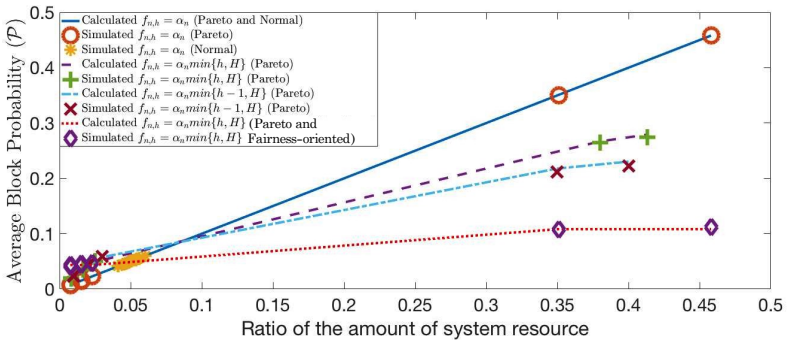


Figure 6: The correlation between the resource ratio and the average block probability $\mathcal{P}$, where $N = 20$, $H = 10$, $\alpha = \frac{1}{2H\sum \omega_i}$.

of strong restriction rather than weak restriction. Referring to Section 2.1, it can be concluded that the cost for attackers to catch up with the honest miners can be higher with $f_{i,h} = \alpha_i \min\{h-1, H\}$ or $f_{i,h} = \alpha_i \min\{h, H\}$ than only $f_{i,h} = \alpha_i$.

Finding 2: The poor (i.e., the less resourceful miners) can gain more profit with a positive Degree function (that increases the mining probability by multiplying the resource ratio and the awaiting gap) [19, 18, 5]. In contrast, the obtained profit becomes lower for the rich with the increased ratio of resource owned.

Based on Fig. 6, it is conceivable that poor miners can obtain a greater gradient g than wealthy miners (positive-Resource-sensitivity), in the case of $f_{i,h} = \alpha_i \min\{h-1, H\}$ (the light blue line) and $\alpha_i \min\{h, H\}$ (the purple line) with a Pareto-distributed resource. There exists a threshold intercepting the identity line, to the left of which the gradient m is greater so that poor miners can obtain a larger $\mathcal{P}$ than they used to deserve with only $f_{i,h} = \alpha_i$ (the dark blue line). Likewise, wealthy miners, i.e., the outliers, can only obtain a smaller g than that of $f_{i,h} = \alpha_i$. This implies a mechanism that taking from the wealthy to help the poor to balance the profits among the whole participated miners.

5.2.3. System convergence

We proceed to evaluate *System Convergence* of the considered PoX schemes, where each of them runs for 1,000 tries. In each of the schemes, the system starts from the same initial state. We name the number of rounds required to reach the steady-state *system convergence period*. During this simulation, we set that the steady-state is reached once the gap between the calculated and the simulation value of $\mathcal{T}_i$ decreases down to 3% (the explanation of 3% refers to the definition of *System Convergence* in Section 3.4).

Finding 3: For PoX schemes disabling the Fairness function, 80/20-rule-based wealth inequality deteriorates System Convergence, compared to normal-distributed wealth inequality.

This finding is shown in Fig. 7, where a Pareto distribution applying to $f_{i,h} = \alpha_i$ (the brown box) takes the longest time to reach the steady-state, while it converges the most quickly with a normal-distributed resource (the purple box). Thus, PoP resulting in a normal-distributed resource has the lowest number of rounds to reach the steady-state, compared with those with a Pareto-distributed resource. This is because of the outlier of Pareto-distributed resource overwhelmingly dominates the mining process.

Finding 4: The system convergence period can be reduced by enabling Resource Fairness and applying a positive Degree function (that increases the mining probability by multiplying the resource ratio and the awaiting gap).

According to Fig. 7, it can be found that $f_{i,h} = \alpha_i \min\{h, H\}$ (the green box) with an active Fairness function needs fewer rounds to reach the steadstate than that of $f_{i,h} = \alpha_i \min\{h, H\}$ (the blue box) with an inactive Fairness function. On the other hand, $f_{i,h} = \alpha_i$ (the brown box) with Degree function $\Phi(\cdot) = 1$ has longer *system convergence period* than the blue box with a positive Degree function. This is because the active Fairness function and positive Degree

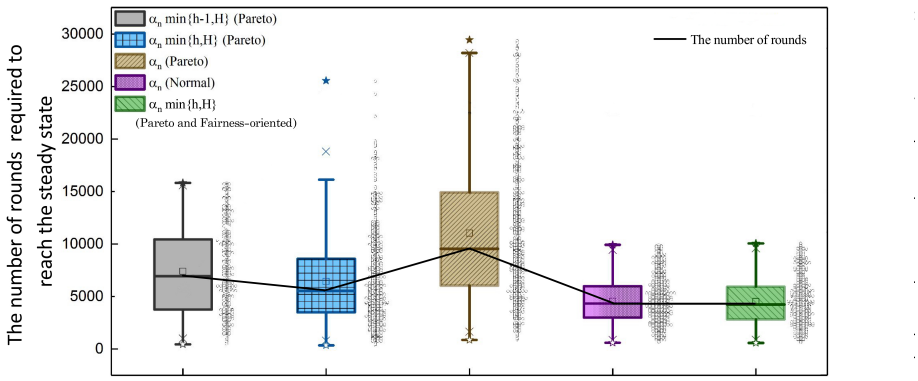


Figure 7: The comparison among the four different PoX schemes in terms of *System Convergence*, where $N = 10$, $H = 5$, $\alpha = \frac{1}{2H\sum \omega_i}$.

function apply a stronger restriction to the Monte Carlo variables, compared to those without an inactive Fairness function.

5.2.4. Resource fairness

Fig. 6 shows that none of the considered PoX schemes (except the red dot line) is upper bounded and Fairness-oriented, as the $\mathcal{P}_i$ of wealth miners remain a linear increasing based on the resource ratio owned by each miner. In other words, *Resource Fairness* is inactive for these PoX schemes, while *Resource Fairness* holds in some circumstances (i.e., $\Upsilon(\omega_i) \neq \omega_i$, to meet different requirements) for the Fairness-oriented PoS-Velocity listed in Table 1, referring to the red dot line in Fig. 6 and green box in Fig. 7. In this section, we show how *Resource Fairness* "encourages" such kind of PoX schemes to achieve better performance of *Resource Sensitivity* and *System Convergence*.

Recall that we implement a typical type of PoS-Velocity (see Section 5.1) as an example of a Fairness-oriented PoX scheme. It is revealed in Fig. 6, where the considered PoS-Velocity has the best performance on *Resource Sensitive* (i.e.,

the smallest $E(g)$) among all of the considered PoX schemes. In addition to the better performance of *Resource Sensitivity*, $\mathcal{P}$ remains constant when the upper bound is met with a partition function $\zeta(\omega)$. In other words, *Resource Fairness* can be satisfied with a simple linear $\Upsilon(\omega_i)$ being substituted by the design of a partitioned $\Upsilon(\omega_i) = \zeta(\omega)$. Thus, the considered PoS-Velocity prevents wealthy miners from monopolizing the entire network and incentivizes all miners to participate in the mining process and getting rewards.

Furthermore, the 80/20-rule-based wealth inequality can be addressed by the considered PoS-Velocity. Fig. 7 shows that *System Convergence* of the considered PoS-Velocity with a Pareto distribution (the green box) performs as good as that of PoP, i.e., $f_{i,h} = \alpha_i$ with a normal-distributed resource (the purple box).

It turns out that by enabling *Resource Fairness* with the designed $\Upsilon(\cdot)$ and $\Phi(\cdot)$, the considered PoS-Velocity achieves,

- **best** *Resource Sensitivity*: the best performance on *Resource Sensitivity* among any other non-Fairness-oriented PoX schemes listed in Table 1, based on the red dot line in Fig. 6;
- **improved** *System Convergence*: a performance on *System Convergence* that is as good as that of PoP with a normal-distributed resource, based on the comparison between the purple and green boxes shown in Fig. 7.

5.2.5. Summary

To sum up, apart from the considered PoS-Velocity scheme (defined in Section 5.1), other Fairness-oriented PoS-Velocity schemes can also reveal their optimized *Resource Sensitivity* and *System Convergence* by using our model. This can be achieved as long as the proper $\Upsilon(\cdot)$ and $\Phi(\cdot)$ are set (e.g., partition $\Upsilon(\cdot)$ and non-linear $\Phi(\cdot)$). By using the proposed model, we reveal that carefully designed *Resource Fairness* is particularly important to balance *Resource Sensitivity*, and *System Convergence* of PoX-based consensus algorithms in the

long-term steady-state. Such steady-state analysis and findings have not been possible without our model.

6. Related Work

There have been several studies proposing analytical models to evaluate the consensus engine of Nakamoto protocol, focusing on PoW from the beginning. Garay et al. proposed a model with negligible network delay and constant total mining power [20] for PoW. Miller and LaViola proposed an analytical model for PoW in terms of the faulty tolerance within a reliant synchronization network [10]. [29] proposes a specific security model regarding the adversarial strategies (selfish mining) considered in [30]. Also, in [31], a security analysis of PoW based on a partially synchronous network is proposed in terms of both the consistency and network partition. On top of that, [13] thoroughly discussed the security issue of PoW, which mainly focuses on natural/malicious consistency problems due to the considerable block propagation time. Apart from a few papers claiming the randomized consensus [12] and the PoX schemes [3, 4] from which the concept of PoX-based consensus algorithms originate, there are not as many as papers generalizing the PoW/PoS consensus algorithms. They tend to be a model where only PoW, PoS, or any other variants are compared [32, 33, 34].

The above models focus on attacks based on the weakness of incentive schemes due to natural/malicious network partitions caused by the considerable block propagation time, such as the selfish-mining-attack, eclipse-attack and computational double-spending attack in PoW [13], and nothing-at-stake attack and long-range attack in PoS [33]. None of them focuses on the resource distribution, to evaluate how much different settings of the weighted system resource distribution will impact the long-term steady-state, and provides an analytical model to each individual miner for a long-term risk assessment, i.e., the amount of profits can be earned if being a miner to pay the system resource.

It is worth noting that, [13] proposed the pitfalls in existing security models that the unrealistic parameters range may prevent the vulnerabilities from being

discovered in the first place and mislead researches into only focusing on a single attack strategy and incentive. This is indeed acceptable, nevertheless, the resource distribution can be analyzed separately from all the other parameters caused by the network delay and non-zero block propagation time; refer to Algo. 4 in [20]. In our model, we simplify our scenario and focus on the security only impacted by the resource distribution without taking the network delay ([20] considers the same assumption) and any corresponding attack strategies and incentives caused by the delay into account. Such a model we proposed can still allow miners to estimate the profits by the proposed metric, *Resource Sensitivity*, as shown in Section 3.4.1.

7. Conclusions and Future Work

We developed a new infinite-dimensional Markov model to unify the steady-state analysis for weighted resource distribution of different PoX-based Blockchains in large-scale networks. The probability of an arbitrary node being elected as the block generator was derived. Based on the analytical model, we evaluated PoW, balance-based and coinage-based PoS, PoA and PoP, in terms of *Resource Sensitivity*, *System Convergence*, and *Resource Fairness*. We also assessed a typical PoS-Velocity scheme with a weight consisting of the proper set Fairness function and Degree function, and showed the balanced performance of the scheme in regards to all the three metrics. Extensive simulation results also prove that the applicability and generality of the model. This can significantly encourage the adoption of Blockchain in large-scale networks that provide public services to the communities.

In the future, we will optimize the margin of error of the model and study the short-term impact of the accumulated resource of each miner upon the entire system. Our model can potentially provide an effective benchmark to evaluate and compare different PoX-based consensus algorithms from a broader aspect.

8. Acknowledgement

This project was partially supported by funding from Food Agility CRC Ltd, funded under the Commonwealth Government CRC Program. The CRC Program works with University of Technology Sydney, and supports industry-led collaborations between industry, researchers and the community.

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008). URL https://bitcoin.org/bitcoin.pdf

[2] L. Lamport, R. Shostak, M. Pease, The Byzantine Generals Problem, ACM Trans. Program. Lang. Syst. 4 (3) (1982) 382–401. doi:10.1145/357172.357176.
URL http://doi.acm.org/10.1145/357172.357176

[3] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Commun. Surveys Tuts. 18 (3) (2016) 2084–2123. doi:10.1109/COMST.2016.2535718.

[4] W. Wang, et al., A Survey on Consensus Mechanisms and Mining Management in Blockchain Networks, arXiv preprint arXiv:1805.02707.

[5] C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, M. Guo, Making big data open in edges: A resource-efficient blockchain-based approach, IEEE Transactions on Parallel and Distributed Systems (2018) 1–1doi:10.1109/TPDS.2018.2871449.

[6] O. Leiba, Y. Yitzchak, R. Bitton, A. Nadler, A. Shabtai, Incentivized delivery network of iot software updates based on trustless proof-of-distribution, CoRR abs/1805.04282. arXiv:1805.04282.
URL http://arxiv.org/abs/1805.04282

[7] M. Vukolić, The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, in: International workshop on open problems in network security, Springer, 2015, pp. 112–125.

[8] Z. Zheng, S. Xie, H.-N. Dai, H. Wang, Blockchain challenges and opportunities: A survey, in: Work Pap., 2016.

[9] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, Computer Communications 136 (2019) 10 – 29. doi:https://doi.org/10.1016/j.comcom.2019.01.006.
URL http://www.sciencedirect.com/science/article/pii/S0140366418306881

[10] A. Miller, J. J. LaViola Jr, Anonymous byzantine consensus from moderately-hard puzzles: A model for Bitcoin (2014).
URL http://nakamotoinstitute.org/research/anonymous-byzantine-consensus

[11] R. Pass, L. Seeman, A. Shelat, Analysis of the Blockchain Protocol in Asynchronous Networks, in: Annu. Inte. Conf. on the Theory and Appl. of Cryptographic Techn. (EUROCRYPT '17), Springer, Cham, 2017, pp. 643–673.

[12] V. Gramoli, From blockchain consensus back to byzantine consensus, Future Generation Comput. Syst.doi:https://doi.org/10.1016/j.future.2017.09.023.
URL http://www.sciencedirect.com/science/article/pii/S0167739X17320095

[13] R. Zhang, B. Preneel, Lay down the common metrics: Evaluating proof-of-work consensus protocols' security, in: 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019.

[14] S. Lo, J. C. Wang, Bitcoin as money?, Current Policy Perspectives 14-4,

Federal Reserve Bank of Boston (2014).
URL https://EconPapers.repec.org/RePEc:fip:fedbcq:2014_004

[15] I. Bentov, C. Lee, A. Mizrahi, M. Rosenfeld, Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]Y, SIGMETRICS Perform. Eval. Rev. 42 (3) (2014) 34–37. doi:10.1145/2695533.2695545.
URL http://doi.acm.org/10.1145/2695533.2695545

[16] D. Hopwood, S. Bowe, T. Hornby, N. Wilcox, Zcash Protocol Specification, Tech. rep., Zerocoin Electric Coin Company, Lakewood, CO, USA (Jan. 2016).

[17] H. Kopp, C. Bösch, F. Kargl, Koppercoin–a distributed file storage with financial incentives, in: The 12th Int. Conf. on Inform. Security Practice and Experience (ISPEC 2016), Springer, Cham, 2016, pp. 79–93.

[18] S. King, S. Nadal, PPcoin: peer-to-peer crypto-currency with proof-of-stake.
URL https://pdfs.semanticscholar.org/0db3/8d32069f3341d34c35085dc009a85ba13c13.pdf

[19] Reddcoin (2018).
URL https://wiki.reddcoin.com/Main_Page

[20] J. Garay, A. Kiayias, N. Leonardos, The Bitcoin Backbone Protocol: Analysis and Applications, in: Annu. Int. Conf. on the Theory and Appl. of Cryptographic Techn. (EUROCRYPT '15), Springer, Berlin, Heidelberg, 2015, pp. 281–310.

[21] G. Wood, Ethereum: A secure decentralised generalised transaction ledger (Apr. 2014).
URL http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf

[22] S. Marco Colino, The antitrust f word: Fairness considerations in competition law, Journal of Business Law, Forthcoming.

[23] S. R. Danning Sui, J. Pfeffer, Are Miners Centralized? A Look into Mining Pools, accessed on 22.10.2019 (2018).
URL https://media.consensys.net/are-miners-centralized-a-look-into-mining-pools-b594425411dc

[24] V. Buterin, V. Griffith, Casper the friendly finality gadget, arXiv preprint arXiv:1710.09437.

[25] D. Boneh, J. Bonneau, B. Bünz, B. Fisch, Verifiable delay functions, Cryptology ePrint Archive, Report 2018/601, https://eprint.iacr.org/2018/601 (2018).

[26] N. Van Saberhagen, Cryptonote v 2.0 (2013).

[27] J. Miles, R Squared, Adjusted R Squared, American Cancer Society, 2014. arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118445112.stat06627, doi:10.1002/9781118445112.stat06627.
URL https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118445112.stat06627

[28] C. Decker, R. Wattenhofer, Information propagation in the bitcoin network, in: IEEE P2P 2013 Proceedings, 2013, pp. 1–10.

[29] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, ACM, New York, NY, USA, 2016, pp. 3–16. doi:10.1145/2976749.2978341.
URL http://doi.acm.org/10.1145/2976749.2978341

[30] A. Sapirshtein, Y. Sompolinsky, A. Zohar, Optimal selfish mining strategies in bitcoin, in: International Conference on Financial Cryptography and Data Security, Springer, 2016, pp. 515–532.

[31] R. Pass, L. Seeman, A. Shelat, Analysis of the blockchain protocol in asynchronous networks, in: J.-S. Coron, J. B. Nielsen (Eds.), Advances in Cryptology – EUROCRYPT 2017, Springer International Publishing, Cham, 2017, pp. 643–673.

[32] G. BitFury, Proof of stake versus proof of work, White paper, Sep.

[33] J. Debus, Consensus Methods in Blockchain Systems, Tech. rep., Frankfurt School of Finance & Management, Blockchain Center, Frankfurt am Main, Germany (2017).

[34] W. Li, S. Andreina, J.-M. Bohli, G. Karame, Securing proof-of-stake blockchain protocols, in: Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, 2017, pp. 297–315.