

Incentive Compatible and Anti-Compounding of Wealth in Proof-of-Stake

Yilei Wang^{*1}, Guoyu Yang¹, Andrea Bracciali¹, Ho-fung Leung¹, Haibo Tian¹,
Man Ho Au¹, Xiaomei Yu¹

^a*School of Information Science and Engineering, Qufu Normal University, China*

^b*Department of Computing Science and Mathematics, University of Stirling, UK*

^c*Department of Computer Science and Engineering, The Chinese University of Hong Kong,
Hong Kong*

^d*School of Electronics and Information Technology, Sun Yat-Sen University, China*

^e*Department of Computing, Hong Kong Polytechnic University, Hong Kong*

^f*Department of Information and Engineer, Shandong Normal University, China*

Abstract

The reward functions are essential ingredients of consensus mechanism in Blockchain, which may bias the wealth distributions due to various incentives. Generally, constant reward function in proof of stakes (PoS) may incur the phenomenon of compounding, where rich get richer. That is, the wealth distribution is not so equitable in proof of stakes than that in proof of works (PoW). In the sequel, geometric reward function is proposed as an alternative choice to circumvent this problem. However, it's not so desirable since no parties have incentives to participate in the consensus mechanism, which does not capture the concern of incentive compatability. In this paper, we tailor a new bonus reward function by adding random salts to the geometric reward function. The new reward function is a tradeoff between equitablity and incentive compatability. We conclude that the quitability of the new reward function is optimal compared with others. Beyond that, we present Gini coefficients to fine-evaluate euqitability of reward functions. We propose a new metric (aka. reward ratio) to quantify the level of incentive compability. Our simulation results show that the new reward function performs better than others in both incentive compatability and anti-compounding.

Keywords: Proof of stake, Gini coefficient, wealth distribution, Incentive

compatible

1. Introduction

Cryptocurrency, represented by bitcoin, has the conspicuous virtue of “decentralization”, which transforms the manners of value transmission and wealth distribution in cyber space. Recently blockchain, the underlining technology of bitcoin, has been broadly discussed and applied in various fields, such as finance, healthcare, Internet of Things (IoT) and cloud computing [? ?]. As is well known, the basic regime in blockchain is consensus mechanism, which may keep in functional order if all participants have enough incentives [?]. Otherwise, the blockchain system is going to be on the verge of collapse. Generally, economy measures (i.e. reward function) are taken to provide incentives sustaining the stability of blockchain system. Constant reward function, where the reward function is constant in a certain period, is widely used in many consensus mechanisms due to easy implementation. However, the usage of constant reward function may cause compounding of wealth (i.e. equitability) in PoS. Geometric reward function, where the reward function dynamically changes according to some fixed parameters, may dwarf the phenomenon of wealth compounding. While it’s proved to be not incentive compatible, which impedes the awareness of taking part in consensus mechanism. In effect, any perfect looking reward functions are of limited value to both practice and research if wealth compounding and incentives absence cannot be settled. There should be a tradeoff between equitability and incentive compatibility.

Therefore, we propose a new reward function based on geometric reward function by introducing random bonus mechanism. More concretely, each participant who has the privilege to create a new block may get extra bonus except for his rewards. We meticulously design positive bonus to assign enough incentives at the beginning of system so that participants are willing to take part into the consensus mechanism. Note that the expectation of the whole bonus is zero. That means there exist some negative bonus, which will not impede

the incentives since the rewards derived from reward function are large enough
30 to neutralize the negative bonus. Our new reward function performs well in
both world restraining the compounding phenomenon and guaranteeing incen-
tive compatibility to acceptable extents.

1.1. Related works

On the contrary to “ASIC-resistance” coins, which seem more “egalitarian”,
35 PoS is easy to make rich richer. Some empirical analyses indicate that PoS
system has poor equitability [?]. However, there is a lack of formal discussion
with respect to equitability issue. Azouvi et al. define the notion of egalitar-
ianism to measure the equitability of most popular cryptocurrencies including
Bitcoin, Ethereum, Litecoin and Monero [?]. Their simulation results show
40 that “ASIC-resistance” performs well in decreasing egalitarianism. As an unex-
pected outcome, the stake-based cryptocurrencies can be perfectly egalitarian
by elaborately selected parameters. Fanti et al. quantify the phenomenon of
compounding by a new metric named equitability [?]. They claim that the
equitability of existing reward functions used in PoW and PoS is not acceptable
45 and therefore they propose a geometric rewards function. They prove that the
new reward function performs better in equitability and may resist selfish mining
attacks. The downside is that geometric reward function guarantee little incen-
tives for parties at the beginning of the system. Leonardos et al. implement
Oceanic games in blockchain mining, which is normally used to analyze decision
50 making in corporate settings [?]. They also reveal incentives to form mining
pools in order to increase their resources. At the last part of their paper, they
declare that their strategic interactions can be directly applied in blockchain
equitability.

The work of [?] neglects an important ingredient in blockchain economic
55 ecosystem–incentives. As we mentioned above, parties should have enough in-
centives to sustain the consensus mechanism. Brünjes et al. [?] address
the problem of stake formation without mention of compounding. Solidus is
an incentive compatible cryptocurrency on the basis of permissionless Byzan-

tine consensus [?]. It injects incentives for almost each phase of the practical
60 Byzantine consensus like get-epoch phase, elect phase, prepare phase and ac-
cept phase. The incentives also consist of negative ones such as penalties for
malicious actions. On the other hand, Solidus can also mitigate selfish min-
ing attacks. Ouroboros also considers incentives by rewarding nodes, who are
members of a committee generating a new block [?]. FruitChains is a new
65 blockchain protocol, which introduce a notion of fairness [?]. It manages to
reach optimal fairness level under the scenario of selfish mining attack since it
undermines incentive compatibility [?]. They prove that, given proper pa-
rameters, δ - approximate fairness can be reached. Both [?] and [?] are
incentive compatibility for block proposers. However, they fail to eliminate the
70 variance of rewards. Luu et al. demystify incentives in blockchain toward the
view of game theory [?]. They formalize the attacks as verifier’s dilemma game
and propose a solution for this game. Their formalization is practical since it’s
implemented in real cryptocurrency networks [? ?].

The last problem is how to evaluate equitability and incentive compatibility.
75 The existing works propose lots of solutions as mentioned above. In effect, Gini
coefficient is a mature metric to measure inequality in economics [?] and
blockchain is really an economic ecosystem [? ? ?]. Therefore, it’s natural to
evaluate the wealth (i.e. stakes) distribution by Gini coefficient [? ? ?]. Kondor
et al. analyze the bitcoin transaction network toward the view of complex
80 network by measuring degree distribution, degree correlations and clustering
coefficient [?]. They also study the money flow in the network and the wealth
accumulation with Gini coefficient. The Gini coefficient is approximate 0.985,
which means a high inequality in wealth for the transaction network. Maesa
et al. [?] construct a users graph instead of transaction network in the work
85 of [?]. They define three properties of richness for the network and evaluate
them with Gini coefficient. The Gini coefficient of the mining power is studied
in [?], which utilizes practical bitcoin data between 2013-12-21 and 2018-12-19.
Another case study of the wealth distribution with respect to bitcoin network is
conducted in [?]. It collects more than 36 million transactions and a list of all

90 users including their wealth. The authors prove that rich have becoming richer since the Gini coefficient is very close to 1. Again, the egalitarianism of bitcoin peer-to-peer network is mentioned in [?], where Gini coefficient is analyzed with network degree distribution.

1.2. Motivations and contributions

95 As can be seen in existing works, equitability is an essential feature. Gini coefficient is one of metrics to evaluate the equitability for Blockchain-based systems. Previous empirical works demonstrate that Gini coefficient is pretty high in bitcoin networks, which may be inclined to centralization, contrary to the original intention of blockchain. For example, rich may get richer. Note that
100 the stake accumulation is closely related to the definition of reward function. Another problem, worthy of being paid attention to, but easily being ignored, is incentive mechanism. Any reward function, even with low Gini coefficient (high equitability), is an empty promise if parties has no incentives to be involved in the blockchain system. However, the existing works are less than satisfactory
105 in both equitability and incentive mechanism. Therefore, a new bonus reward function based on geometrical reward function is proposed to make a tradeoff between equitability and incentive compatibility. Our main contribution are as follows.

- We revisit the geometric reward function r_g in [?] and find that it is
110 not incentive compatibility especially at the outset of blockchain system. Therefore, we propose a metric (aka. reward ratio), which is defined as the ratio between the initial and the i^{th} block reward with respect to specific reward function r . The ratio of geometric reward function is far below that of constant reward function r_c . However, the latter has undesirable
115 equitability.
- We propose a new bonus reward function r_b as a trade off between incentive compatibility and equitability. We prove, given proper parameters, it suffices that the bonus reward function is optimal reward ratio compared

Table 1: The comparison on incentive compatibility and equitability (\checkmark denotes desirable property and \times on the contrary)

Reward function	Incentive compatibility	Equitability
Constant reward	\checkmark	\times
Geometric reward	\times	\checkmark
Bonus reward	\checkmark	\checkmark

with the geometric reward function. Table ?? presents the comparison
 120 with respect to incentive compatibility and equitability.

- We analyze the compounding of wealth in PoS with gini coefficient instead
 of equitability since the former is the most commonly used measurement
 of inequality in economics. We simulate the Gini coefficients for constant
 reward function, geometric reward function and bonus reward function
 125 respectively. To visually demonstrate the differences of Gini coefficients
 of these reward function, we simulate them with respect to various distri-
 butions (e.g. Pareto distribution, Weibul distribution). The results show
 that the wealth distribution is acceptable under proper parameters.

1.3. Road map

130 Some preliminaries are present in section 2, consisting of Gini coefficient,
 various distributions and incentive compatibility etc. Section 3 first delineates
 the definitions of constant reward function and geometric reward function, then
 proposes the new bonus reward function based on geometric reward function.
 We revisit the evaluation of equitability used in [?] and compare this metric of
 135 bonus reward function with others. It's proved that, given proper parameters,
 bonus reward function is most equitable among these reward function. Finally,
 we propose a new concept (aka. reward ratio) to evaluate the metric of incentive
 compatability and prove that bonus reward function is optimal with respect to
 reward ratio. Section 4 presents the pseudo codes of simulation programs and
 140 compare reward function, geometric reward function and bonus reward function

under various fixed parameters. The simulation results show that bonus reward function performs well in both equitability and incentive compatibility, which is consistent with the theoretical analysis.

2. Preliminaries

2.1. Gini coefficient

Generally, Gini coefficient is an index usually adopted to measure the degree of inequality in a distribution. Gini coefficient is widely used in economics to evaluate how equality of income distributions. Therefore, we borrow this convention to analyze the equality for wealth distributions of cryptocurrencies under the influences of specific reward functions. Normally, Gini coefficient is defined based on Lorenz curve. An alternative but equivalent definition for Gini coefficient G is shown in Equation (??).

$$G = \frac{\sum_{i=1}^n \sum_{j=1}^n |x_i - x_j|}{2 \sum_{i=1}^n \sum_{j=1}^n x_j} = \frac{\sum_{i=1}^n \sum_{j=1}^n |x_i - x_j|}{2n^2 \bar{x}}. \quad (1)$$

Here, x_i is the income of party i ($i \in [1, 2, \dots, n]$) and \bar{x} is the average absolute difference of all pairs of items for all parties.

2.2. Related distributions

Pareto distributions. The Pareto distribution, is a power-law probability distribution found in a large number of real-world phenomena. Its most significant representativeness rule is ‘‘Pareto principle’’ (or, the 80-20 rule), which means that about 80% of the wealth is held by 20% of its population. Therefore, it’s natural to assume that the wealth distribution for cryptocurrencies is Pareto distribution at least in the initial stage of the wealth. The probability density function of a Pareto distribution is as follows.

$$f_X(x) = \begin{cases} \frac{\alpha x_m^\alpha}{x^{\alpha+1}} & x \geq x_m, \\ 0 & x < x_m. \end{cases} \quad (2)$$

Here X is a random variable with Pareto distribution, x is a specific number, x_m is the minimum possible value of X , and α is a positive parameter.

Weibull distributions. Weibull distribution is a continuous probability distribution, which is widely used in the reliability engineering processing life test data. Here, we use the distribution to denote the life-span of cryptocurrencies. 160 The probability density function of a Weibull distribution is as follows.

$$f(x; \lambda, k) = \begin{cases} \frac{k}{\lambda} \left(\frac{x}{\lambda}\right)^{(k-1)} e^{-(x/\lambda)^k} & x \geq 0, \\ 0 & x < 0. \end{cases} \quad (3)$$

Here $k > 0$ denotes the shape parameter and $\lambda > 0$ denotes the scale parameter of the distribution. Both are parametric families of probability distributions.

Exponential distribution. Exponential distributions describe that events occur independently in a mean speed. It's used to sample random values for our proposed reward functions since it is memoryless. The probability density function of an exponential distribution is as follows. 165

$$f(x; \gamma) = \begin{cases} \gamma e^{-\gamma x} & x \geq 0, \\ 0 & x < 0. \end{cases} \quad (4)$$

Here x denotes the fixed time and γ denotes the number of events occurrence in unit time.

170 2.3. Incentive compatibility

Incentive compatibility is a mechanism, where parties may achieve optimal incomes when they act according to their true preferences. Here the true preferences may denote the decided principles in cryptocurrency ecosystems. The basic idea for removing the phenomenon of compounding is the reward therein due to incentives for parties. Therefore, the reward function must be incentive 175 compatible. Otherwise, the reward function is of no use, no matter how perfect it is.

3. Reward function and equitability

3.1. Reward functions

180 Reward function is an essential part in cryptocurrencies since it provides incentives for parties to act by following the specific consensus mechanisms (e.g. PoW, PoS). The reward functions should first satisfy the property of incentive compatibility and then equitability. In this paper, we still adopt the reward functions as previous works, where the total reward coins is fixed to be about 21 million. Parties (aka. miners) manage to mine a block and win a specific reward for mining the block. The reward is halved every 210,000 blocks in the Nakamoto consensus mechanism, which is also the commonly used reward function in most consensus mechanism. However, this kind of constant reward function may lead to the phenomenon of compounding when it's implemented in proof of stake. 190 Geometric reward function [?] is lack of incentives especially at the first few blocks even if it can cripple compounding to some extent. Therefore, we propose a new bonus reward function, which makes a trad off between compounding and incentives. Here, we inherit the notations in [?] to facilitate the illustration of their relationships. Let $T = 210,000$ denote the interval, $R = 50 \cdot \frac{1}{2^{\lceil \frac{T}{2} - 1 \rceil}}$ · T denote the total rewards. Similar to [?], R and T are fixed as above. 195

- Constant reward function $r_c(t) = \frac{R}{T}$ (r_c for simplicity), where $t = [1, 2, 3, \dots]$ the t^{th} block.
- Geometric reward function $r_g(t) = (1+R)^{\frac{t}{T}} - (1+R)^{\frac{t-1}{T}}$ (r_g for simplicity).
- Bonus reward function $r_b(t) = (1+R)^{\frac{t}{T}} - (1+R)^{\frac{t-1}{T}} + c_t$ (r_b for simplicity), 200 where c_t obeys exponential distribution with 0 expectation. The main role for c_t is to add random slats to the reward function such that a trad off between equitability and incentive compatibility can be made.

The reward functions are shown in Figure ???. The constant reward function and the geometric reward function are the same to the work of [?]. The bonus 205 reward function is a composition of geometric reward function and random cost

as shown in Figure ???. Here the block height is divided into 5 periods, each of which consists of 210,000 blocks. For example, the first period denotes 0-210,000 blocks and the the second period denotes 210,001-420,000 and so on.

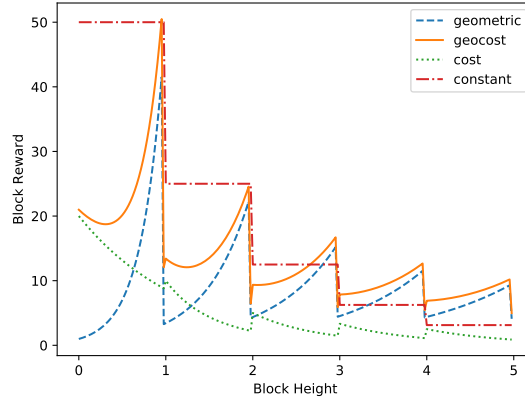


Figure 1: The constant, geometric and bonus reward functions. Here constant denotes the constant reward function, geometric denotes the geometric reward function, cost denotes the random salts used in bonus reward function and geocost denotes bonus reward function.

3.2. Evaluation of equitability

210 The notion of equitability is define identically to [?]. Here, we only present the equitability of our bonus reward function and prove that, given proper parameters, the equitability of bonus reward function is optimal than geometric reward function.

215 **Theorem 1** Given $c_i > \frac{S_i}{S_{i-1}}c_{i-1}$ ($i = 1, 2, \dots, T$), the bonus reward function r_b is the most equitable among the constant reward function, geometric reward function and the bonus reward function.

Proof: Since it's proved that the equitability of geometric reward function r_g is better than that of the constant reward function r_c . So we only prove that the equitability of bonus reward function r_b is optimal compared with that of the geometric reward function r_g . The conclusion can be established.

220

Let $S(n) = r_g = (1 + R)^{\frac{n}{T}} - (1 + R)^{\frac{n-1}{T}}$, $S'(n) = r_b = r_g + c_i$. According to Lemma 1 in [?], we have,

$$Var(v_{A,r_g}(T)) = (v_{A,r_g}(0) - v_{A,r_g}(0)^2) \left(1 - \frac{S(0)^2}{S(T)^2} \prod_{i=1}^T (2e^{\theta_n} - 1)\right). \quad (5)$$

Recall that Equations ?? and ?? establish in this paper with respect to random salts.

$$e^{\theta_n} = \frac{S'(n)}{S'(n-1)} = \frac{S'(n) - c_n}{S'(n-1) - c_{n-1}} \quad (6)$$

$$r'(n) = S'(n+1) - S'(n) = S(n+1) - S(n) + (c_{n+1} - c_n). \quad (7)$$

The equitability of r_b is in Equation ?? when we combine Equations ?? and ?? into Equation ??.

$$Var(v_{A,r_b}(T)) = (v_{A,r_b}(0) - v_{A,r_b}(0)^2) \left(1 - \frac{S'(0)^2}{S'(T)^2} \prod_{i=1}^T (2e^{\theta_n} - 1)\right) \quad (8)$$

Let $c_T = 0$, the difference between Equation ?? and ?? is the part of $\prod_{i=1}^T (2e^{\theta_n} - 1)$. Therefore, we only need to compare this part. Let,

$$E_{r_g} = E_g^1 * E_g^2 * \dots * E_g^T = \left(\frac{2S_0}{S_1} - 1\right) * \left(\frac{2S_1}{S_2} - 1\right) * \dots * \left(\frac{2S_{T-1}}{S_T} - 1\right),$$

$$E_{r_b} = E_p^1 * E_p^2 * \dots * E_p^T = \left(\frac{2(S_0 + c_0)}{S_1 + c_1} - 1\right) * \left(\frac{2(S_1 + c_1)}{S_2 + c_2} - 1\right) * \dots * \left(\frac{2(S_{T-1} + c_{T-1})}{S_T + c_T} - 1\right).$$

Here, we relax the condition by only comparing each pair of E_g^i and E_p^i ($i = 1, 2, \dots, T$) independently. So we have,

$$\begin{aligned} E_g^i - E_p^i &= \left(\frac{2(S_i + c_i)}{S_{i-1} + c_{i-1}} - 1\right) - \left(\frac{2S_i}{S_{i-1}} - 1\right) \\ &= \frac{[2(S_i + c_i) - (S_{i-1} + c_{i-1})]S_{i-1} - (2S_i - S_{i-1})(S_{i-1} + c_{i-1})}{(S_{i-1} + c_{i-1})S_{i-1}} \\ &= 2 \frac{S_{i-1}c_i - S_i c_{i-1}}{(S_{i-1} + c_{i-1})S_{i-1}} \end{aligned}$$

225 In conclusion, given $c_i > \frac{S_i}{S_{i-1}} c_{i-1}$, we have $E_g^i > E_p^i$ and thus $Var(v_{A,r_b}(T)) < Var(v_{A,r_g}(T))$.

□

3.3. Incentive compatibility

Incentive compatibility is another metric for cryptocurrencies except for equitability. Sometimes, it's especially important compared with equitability since any reward function is good for nothing with no incentives. Therefore, in this paper, we introduce the incentive compatibility to illustrate the incentives such that parties are willing to take part into the consensus mechanism. In the following, we present the definition for evaluating the performance of incentive compatibility within cryptocurrency content.

Definition 1 The reward ratio for one specific reward function is defined as:

$$rat_{r_x}^{inv^i} = r_x(t_{inv_1^i})/r_x(t_j) \quad (9)$$

Here, x denotes different reward functions, inv^i denotes the i^{th} interval. t_j denotes the $(t_j)^{th}$ block, which suffices that $\lceil \frac{t_j}{T} \rceil = inv^i$ and $t_{inv_1^i}$ (t_{inv} for simplicity) denotes the first block inside the i^{th} interval.

Definition 2 The reward ratio for reward function r_x is optimal compared with another reward function $r_{x'}$, if it satisfied: $rat_{r_x}^{inv^i} > rat_{r_{x'}}^{inv^i}$.

Theorem 2 Given positive $\frac{ct_{inv}}{ct_j} > \frac{r_g(t_{inv})}{r_g(t_j)}$, The bonus reward function r_b is optimal reward ratio compared with the geometric reward function.

Proof Scheme: It's obvious that $rat_{r_c}^{inv^i} = 1$, $rat_{r_g}^{inv^i} = 1$, $rat_{r_g}^{inv^i} = \frac{r_g(t_{inv})}{r_g(t_j)}$ and $rat_{r_b}^{inv^i} = \frac{r_g(t_{inv}) - ct_{inv}}{r_g(t_j) - ct_j}$. We can easily prove that there always exist proper parameters such that $\frac{ct_{inv}}{ct_j} > \frac{r_g(t_{inv})}{r_g(t_j)}$ suffices. Note that the designer for the consensus mechanism can arbitrarily choose the parameters.

□

4. Simulations and comparisons

In this section, we simulate the Gini coefficients for three reward functions mentioned above. In fact, the wealth distribution is affected not only by the reward function but also by the consensus mechanism. Therefore, we simulate Gini coefficients based on the reward function and consensus mechanism (e.g. PoS and PoW). More concretely, (1) each party is assumed to own some initial

stakes, which are sampled by specific distributions like Pareto distribution and
255 Weibull distribution. Meanwhile, the computational power is also initialed ac-
cording to the same distributions if PoW is used. (2) The algorithm decides the
winner for the current block according to their ratio of stakes or computational
power. (3) The algorithm updates the stakes and enters into the next block. (4)
Gini coefficient is computed according to Equation ???. The algorithm is shown
260 in Algorithm 1.

We present the Gini coefficient of constant reward function under PoW con-
sensus mechanism in Figure ???. There are some subtle differences in Gini coeffi-
cient (close to 1) when the distribution parameter is lower than 1. Note that the
distributions are normalized to fall into $[0, 1, 2, 3, 4, 5]$. In fact, the parameters
265 are magnified 100 times in Algorithm 1. The Gini coefficient decrease dramati-
cally when the initial stakes are sampled according to Pareto distribution. On
the other hand, the Gini coefficients keep the trend with the distribution param-
eters grow when the initial stakes are sampled according to random and Weibull
distributions. In other words, the initial samplings affect the wealth distribution
270 under PoW consensus mechanism and Pareto distribution facilitate to impair
the compounding phenomenon compared with the other two distributions.

In the sequel, we demonstrate the Gini coefficients of different reward func-
tions under PoS consensus mechanism in Figures ??, ??, ?? respectively. Fur-
thermore, we also present Gini coefficients with different initial stake distribu-
275 tions since they affect the wealth distributions as mentioned above. Note that
the general trends of Gini coefficients for PoS are similar to that of PoW except
that the Gini coefficients are relatively low under PoS consensus mechanism.
That is, PoS performs better than PoW with respect to wealth distribution,
which is a little bit contradict to the existing result with equitability in [?].
280 Therefore, Gini coefficient is a better metric to measure the wealth distribution
compared to equitability. As can be seen in Figures ??, ??, ??, the Gini coeffi-
cients tend to be stable. Take the coefficients under Pareto distribution as an
example, the Gini coefficients of geometric and bonus-random reward functions
are close to 0, which denote absolutely fair within the scope of wealth distribu-

Algorithm 1 *Gini Coefficient*

```
1: function Gini(Wealths[ ])
2:    $len \leftarrow Length(Wealths[ ])$ 
3:    $Sorted\_Wealths[ ] \leftarrow Sort(Wealths[ ])$ 
4:   for  $i = 1 \rightarrow len$  do
5:      $Sum\_Wealths[i] \leftarrow Sorted\_Wealths[i] + Sum\_Wealths[i - 1]$ 
6:   end for
7:    $Last\_Wealth \leftarrow Sum\_Wealths[len - 1]$ 
8:    $Nor\_Wealths[i] \leftarrow \frac{Sum\_Wealths[i]}{Last\_Wealth}$ 
9:    $B \leftarrow \int_0^1 Nor\_Wealths[ ] dx$ 
10:   $A \leftarrow \int_0^1 dx \int_{Nor\_Wealths[ ]}^x dy$ 
11:   $G \leftarrow \frac{A}{A+B}$ 
12:  return  $G$ 
13: end function
14:
15: function main(void)
16:   while  $Gini\_Coefficient \geq \xi$  do
17:      $R \leftarrow Gen\_BTC(self, *args)$ 
18:      $Reward[ ] \leftarrow Calculate\ block\ reward$ 
19:     for  $i = 1 \rightarrow Length(R)$  do
20:       if POW model then
21:          $C \leftarrow Gen\_POW(self, *args)$ 
22:       end if
23:       if POW model then
24:          $k \leftarrow Selection(C[ ])$ 
25:       else
26:          $k \leftarrow Selection(R[ ])$ 
27:       end if
28:        $R[k] \leftarrow R[k] + Reward[t]$ 
29:     end for
30:      $Gini\_Coefficient \leftarrow Gini(R)$ 
31:   end while
32: end function
```

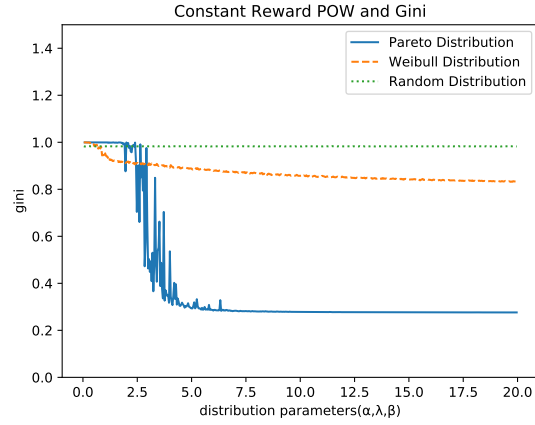


Figure 2: The Gini coefficient of constant reward function under PoW consensus mechanism. Here α , γ and β are distribution parameters in Pareto distribution, Weibull distribution and random distribution respectively.

285 tion. That is, geometric reward function and bonus-random geometric reward function perform better than constant reward function.

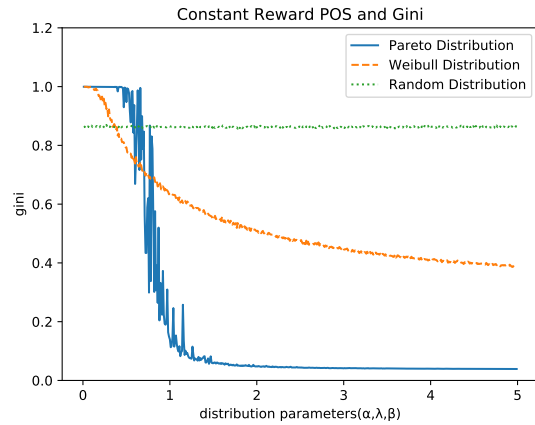


Figure 3: The Gini coefficient of constant reward function under PoS consensus mechanism.

Finally, we compare the Gini coefficients of three rewards functions with identical initial stake distributions in Figure ?? and ?? respectively. Similar to previous results, the Gini coefficients have little difference when the distribution

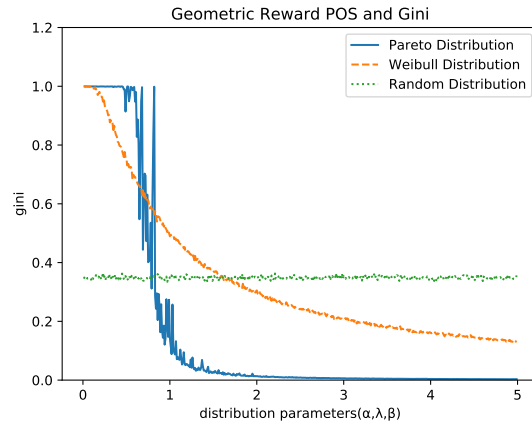


Figure 4: The Gini coefficient of geometric reward function under PoS consensus mechanism.

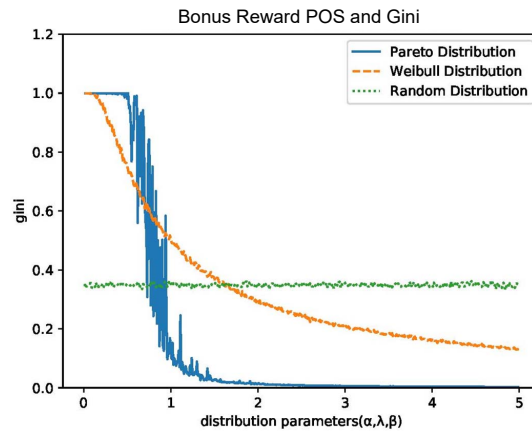


Figure 5: The Gini coefficient of bonus reward function under PoS consensus mechanism.

290 parameters are lower than 1 and fork afterwards. However, it's obvious that the Gini coefficients of bonus reward function is minimum among three reward functions. That is, our proposed reward function performs best with respect to the wealth distribution, which coincides with the theoretical analysis.

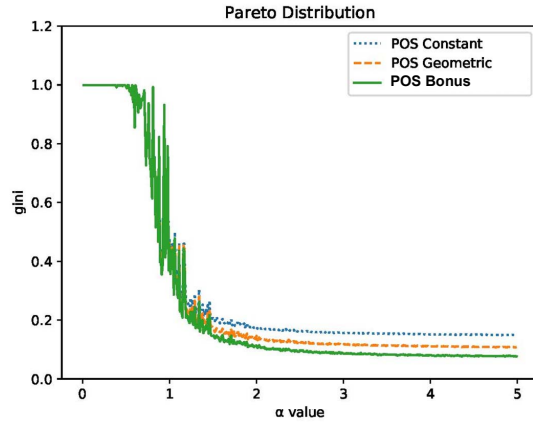


Figure 6: The Gini coefficient of reward functions under Pareto distribution.

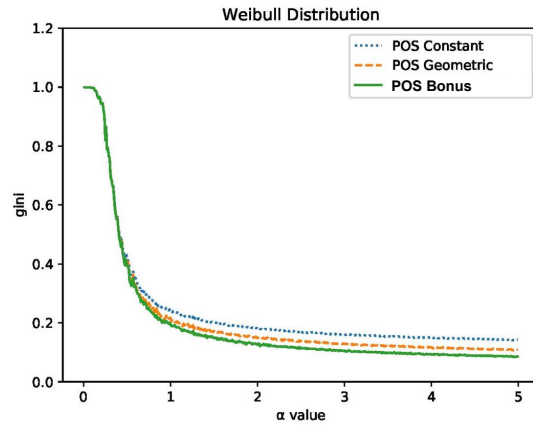


Figure 7: The Gini coefficient of reward functions under Weibull distribution.

5. Conclusions and future works

295 Recently, there's a great concern over cryptocurrencies, which may overturn
the value transformation model. The wealth is reallocated in cryptocurrency
economic environment according to the consensus mechanism. More specifically,
certain incentive mechanism is implemented to inspire miners by rewarding them
to mine new blocks. One of the highlights therein is the wealth distribution
300 under the reward functions. Bonus reward function is proposed based on geo-
metric reward function by adding random salts. We prove that bonus reward
function is the most equitable function compared with constant and geometric
reward functions. Furthermore, equitability is not the unique metric to evalu-
ate the fairness of wealth distributions. We borrow Gini coefficient as a metric
305 to evaluate the wealth distribution over cryptocurrencies. The simulation re-
sults show that bonus reward function has a lower Gini coefficient, which can
cripple compounding to some extent. The future works should consider other
reward functions except for the proposed ones to leverage the incentives and
equitability.

310 Acknowledgments

This study was funded by Foundation of National Natural Science Foun-
dation of China (grant number:61771231, 6150028), Natural Science Shandong
Province (grant number: ZR2016FM23, ZR2017MF010, ZR2017MF062), Key
Research and Development Program of Shandong Province NO. 2019GGX101025).