Information Sciences 530 (2020) 85–94

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Incentive compatible and anti-compounding of wealth in proof-of-stake

Yilei Wang[a,b,*], Guoyu Yang[a], Andrea Bracciali[c], Ho-fung Leung[d], Haibo Tian[e], Lishan Ke[b], Xiaomei Yu[f]

[a] School of Information Science and Engineering, Qufu Normal University, China
[b] School of Computer Science and Cyber Engineering, Guangzhou University, China
[c] Department of Computing Science and Mathematics, University of Stirling, UK
[d] Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong
[e] School of Electronics and Information Technology, Sun Yat-Sen University, China
[f] Department of Information and Engineer, Shandong Normal University, China

ARTICLE INFO

Article history:
Received 12 November 2019
Revised 16 January 2020
Accepted 27 March 2020
Available online 25 April 2020

Keywords:
Proof of stake
Gini coefficient
Wealth distribution
Incentive compatible

ABSTRACT

Geometric reward function is proposed as an alternative choice to circumvent the problem of compounding. However, it's not so desirable since no parties have incentives to participate in the consensus mechanism. 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 compatibility. 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 compatibility. Our simulation results show that the new reward function performs better than others in both incentive compatibility and anti-compounding.

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 [1–4]. As is well known, the basic regime in blockchain is consensus mechanism, which may keep in functional order if all participants have enough incentives [5–8]. 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

* Corresponding author at: School of Information Science and Engineering, Qufu Normal University, China.
E-mail addresses: wang_yilei2019@qfnu.edu.cn (Y. Wang), yangguoyu1020@163.com (G. Yang), andrea.bracciali@stir.ac.uk (A. Bracciali), lhf@cuhk.edu.hk (H.-f. Leung), tianhb@mail.sysu.edu.cn (H. Tian), kelishan@gzhu.edu.cn (L. Ke), yxm0708@126.com (X. Yu).

https://doi.org/10.1016/j.ins.2020.03.098
0020-0255/© 2020 Elsevier Inc. All rights reserved.

are of limited value to both practice and research if wealth compounding and incentives absence cannot be settled [9–11]. 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 to neutralize the negative bonus. Our new reward function performs well in both world restraining the compounding phenomenon and guaranteeing incentive compatibility to acceptable extents.

1.1. Related works

On the contrary to “ASIC-resistance” coins, which seem more “egalitarian”, PoS is easy to make rich richer. Some empirical analyses indicate that PoS system has poor equitability [12]. However, there is a lack of formal discussion with respect to equitability issue. Azouvi et al. define the notion of egalitarianism to measure the equitability of most popular cryptocurrencies including Bitcoin, Ethereum, Litecoin and Monero [13]. Their simulation results show that “ASIC-resistance” performs well in decreasing egalitarianism. As an unexpected 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 [14]. They claim that the equitability of existing reward functions used in PoW and PoS is not acceptable 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 incentives for parties at the beginning of the system. Leonardos et al. implement Oceanic games in blockchain mining, which is normally used to analyze decision making in corporate settings [15,16]. 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. Fuzzy theory is also utilized to optimize the decision making problems [17,18].

The work of [14] neglects an important ingredient in blockchain economic ecosystem–incentives. As we mentioned above, parties should have enough incentives to sustain the consensus mechanism. Brünjes et al. [19] address the problem of stake formation without mention of compounding. Solidus is an incentive compatible cryptocurrency on the basis of permissionless Byzantine consensus [20]. It injects incentives for almost each phase of the practical Byzantine consensus like get-epoch phase, elect phase, prepare phase and accept phase. The incentives also consist of negative ones such as penalties for malicious actions. On the other hand, Solidus can also mitigate selfish mining attacks. Ouroboros also considers incentives by rewarding nodes, who are members of a committee generating a new block [21]. FruitChains is a new blockchain protocol, which introduce a notion of fairness [22]. It manages to reach optimal fairness level under the scenario of selfish mining attack since it undermines incentive compatibility [23]. They prove that, given proper parameters, δ- approximate fairness can be reached. Both [21] and [22] are incentive compatibility for block proposers. However, they fail to eliminate the variance of rewards. Luu et al. demystify incentives in blockchain toward the view of game theory [24]. 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 [25,26].

The last problem is how to evaluate equitability and incentive compatibility. The existing works propose lots of solutions as mentioned above. In effect, Gini coefficient is a mature metric to measure inequality in economics [27] and blockchain is really an economic ecosystem [28–30]. Therefore, it’s natural to evaluate the wealth (i.e. stakes) distribution by Gini coefficient [31–33]. Kondor et al. analyze the bitcoin transaction network toward the view of complex network by measuring degree distribution, degree correlations and clustering coefficient [34]. 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. [35] construct a users graph instead of transaction network in the work of [34]. 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 [36], 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 [37]. It collects more than 36 million transactions and a list of all 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 [38], where Gini coefficient is analyzed with network degree distribution.

1.2. Motivations and contributions

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 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 in both equitability and incentive mechanism. Therefore, a new bonus

Table 1
The comparison on incentive compatibility and equitability (✓ denotes desirable property and × on the contrary).

Reward function	Incentive compatibility	Equitability
Constant reward	✓	×
Geometric reward	×	✓
Bonus reward	✓	✓

reward function based on geometrical reward function is proposed to make a tradeoff between equitablity and incentive compatibility. Our main contribution are as follows.

- We revisit the geometric reward function r_g in [14] and find that it is 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 ith 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 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 with the geometric reward function. Table 1 presents the comparison 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 respectively. To visually demonstrate the differences of Gini coefficients of these reward function, we simulate them with respect to various distributions (e.g. Pareto distribution, Weibul distribution). The results show that the wealth distribution is acceptable under proper parameters.

1.3. Road map

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 [14] and compare this metric of 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 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 crptocurrencies 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 Eq. (1).

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

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.

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

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. Weibul 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. The probability density function of a Weibull distribution is as follows.

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

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.

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

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

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 compatible. Otherwise, the reward function is of no use, no matter how perfect it is.

3. Reward function and equitability

3.1. Reward functions

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. Geometric reward function [14] 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 [14] to facilitate the illustration of their relationships. Let $T = 210,000$ denote the interval, $R = 50 \cdot \frac{1}{2^{\lceil \frac{t}{T} - 1 \rceil}} \cdot T$ denote the total rewards. Similar to Fanti et al. [14], R and T are fixed as above.

- Constant reward function $r_c(t) = \frac{R}{T}$ (r_c for simplicity), where $t = [1, 2, 3, \ldots\ldots]$ the tth 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), 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 Fig. 1. The constant reward function and the geometric reward function are the same to the work of [14]. The bonus reward function is a composition of geometric reward function and random cost as shown in Fig. 1. 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 second period denotes 210,001-420,000 and so on.

3.2. Evaluation of equitability

The notion of equitability is define identically to [14]. 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.

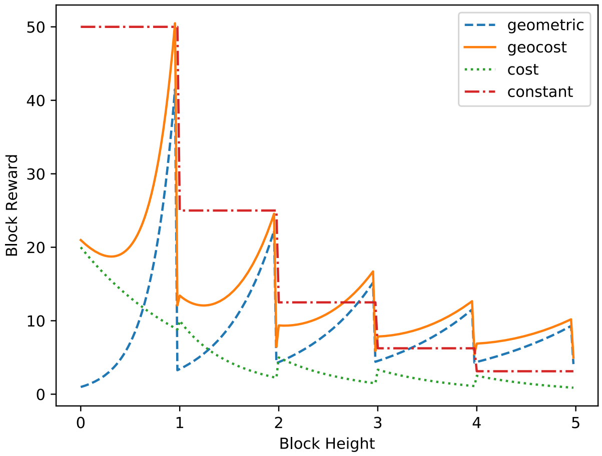

Fig. 1. The constant, geometric and bonus reward functions. Here constant denotes the constant reward function, geometric denotes the geometric reward function, cost denotes the random salts used in bonus reward function and geocost denotes bonous reward function.

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.

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 [14], we have,

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

Recall that Eqs. (6) and (7) establish in this paper with respect to random salts.

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

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

The equitability of r_b is in Eq. (8) when we combine Eqs. (6) and (7) into Eq. (5).

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

Let $c_T = 0$, the difference between Eq. (5) and (8) is the part of $\prod_{i=1}^{T}(2e^{\theta_n} - 1)$. Therefore, we only need to compare this part. Let,

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

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

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,

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

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

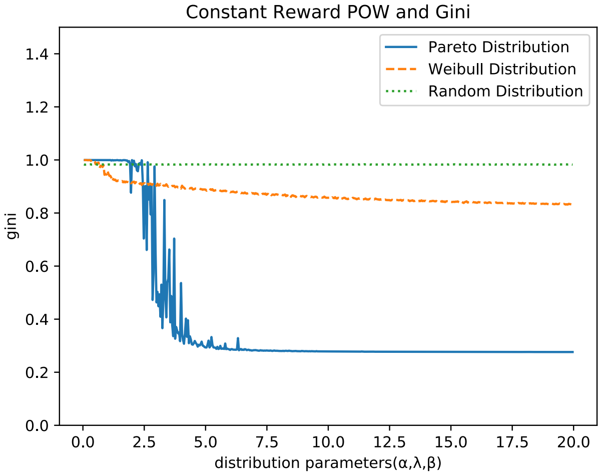

Fig. 2. The Gini coefficient of constant reward function under PoW consensus mechanism. Here α, γ and β are distribution parameters in Pareto distribution, Weibull distribution and random distribution respectively.

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 crytocurrency content.

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

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

Here, x denotes different reward functions, inv^i denotes the ith 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 ith 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* $\frac{c_{t_{inv}}}{c_{t_j}} > \frac{r_g(t_{inv})}{r_g(t_j)}$, *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 $rat_{r_b}^{inv^i} = \frac{r_g(t_{inv}) - c_{t_{inv}}}{r_g(t_j) - c_{t_j}}$. We can easily prove that there always exist proper parameters such that $\frac{c_{t_{inv}}}{c_{t_j}} > \frac{r_g(t_{inv})}{r_g(t_j)}$ 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 Weibull distribution. Meanwhile, the computational power is also initialed according 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 Eq. (1). The algorithm is shown in Algorithm 1.

We present the Gini coefficient of constant reward function under PoW consensus mechanism in Fig. 2. There are some subtle differences in Gini coefficient (close to 1) when the distribution parameter is lower than 1. Note that the distri-

Algorithm 1 Gini coefficient.

```
function $Gini(Wealths[\ ])$
    $len \leftarrow Length(Wealths[\ ])$
    $Sorted\_Wealths[\ ] \leftarrow Sort(Wealths[\ ])$
    for $i = 1 \rightarrow len$ do
        $Sum\_Wealths[i] \leftarrow Sorted\_Wealths[i] + Sum\_Wealths[i-1]$
    end for
    $Last\_Wealth \leftarrow Sum\_Wealths[len-1]$
    $Nor\_Wealths[i] \leftarrow \frac{Sum\_Wealths[i]}{Last\_Wealth}$
    $B \leftarrow \int_0^1 Nor\_Wealths[\ ]\ dx$
    $A \leftarrow \int_0^1\ dx \int_{Nor\_Wealths[\ ]}^{x}\ dy$
    $G \leftarrow \frac{A}{A+B}$
    $return\ G$
end function

function $main(void)$
    while $Gini\_Coefficient \geq \xi$ do
        $R \leftarrow Gen\_BTC(self, *args)$
        $Reword[\ ] \leftarrow Calculate\ block\ reward$
        for $i = 1 \rightarrow Length(R)$ do
            if $POW\ model$ then
                $C \leftarrow Gen\_POW(self, *args)$
            end if
            if $POW\ model$ then
                $k \leftarrow Selection(C[\ ])$
            else
                $k \leftarrow Selection(R[\ ])$
            end if
            $R[k] \leftarrow R[k] + Reward[t]$
        end for
        $Gini\_Coefficient \leftarrow Gini(R)$
    end while
end function
```

butions are normalized to fall into [0,1,2,3,4,5]. In fact, the parameters are magnified 100 times in Algorithm 1. The Gini coefficient decrease dramatically when the initial stakes are sampled according to Pareto distribution. On the other hand, the Gini coefficients keep the trend with the distribution parameters grow when the initial stakes are sampled according to random and Weibull distributions. In other words, the initial samplings affect the wealth distribution 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 functions under PoS consensus mechanism in Figs. 3–5 respectively. Furthermore, we also present Gini coefficients with different initial stake distributions 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 that PoW with respect to wealth distribution, which is a little bit contradict to the existing result with equitability in [14]. Therefore, Gini coefficient is a better metric to measure the wealth distribution compared to equitability. As can be seen in Figs. 3–5, the Gini coefficients 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 distribution. That is, geometric reward function and bonus-random geometric reward function perform better than constant reward function.

Finally, we compare the Gini coefficients of three rewards functions with identical initial stake distributions in Figs. 6 and 7 respectively. Similar to previous results, the Gini coefficients have little difference when the distribution 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.

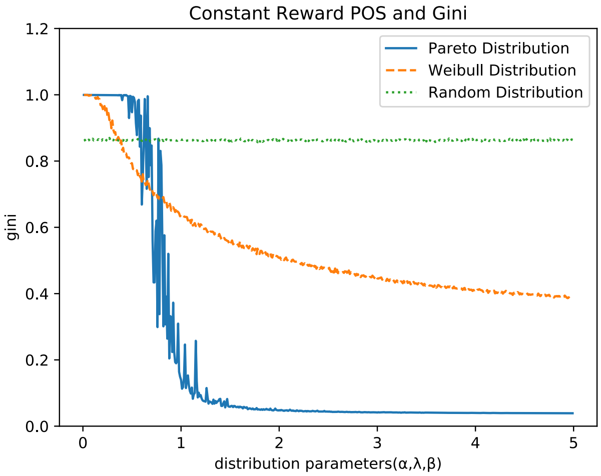

Fig. 3. The Gini coefficient of constant reward function under PoS consensus mechanism.

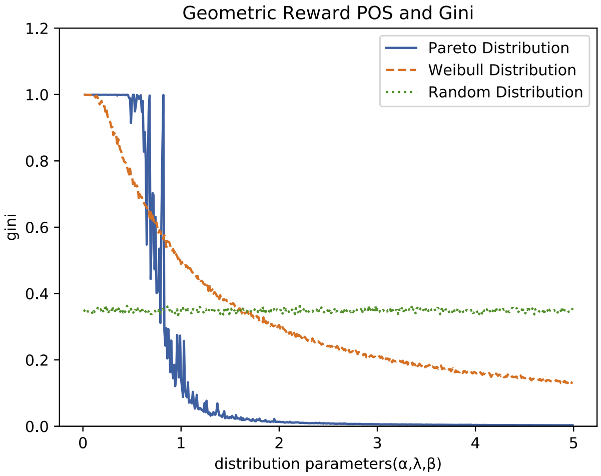

Fig. 4. The Gini coefficient of geometric reward function under PoS consensus mechanism.

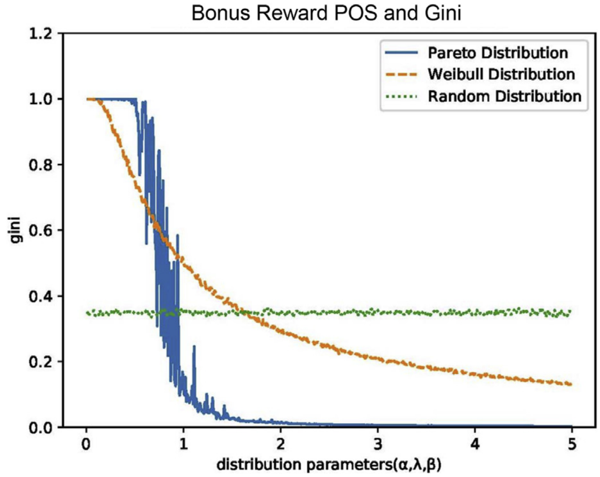

Fig. 5. The Gini coefficient of bonus reward function under PoS consensus mechanism.

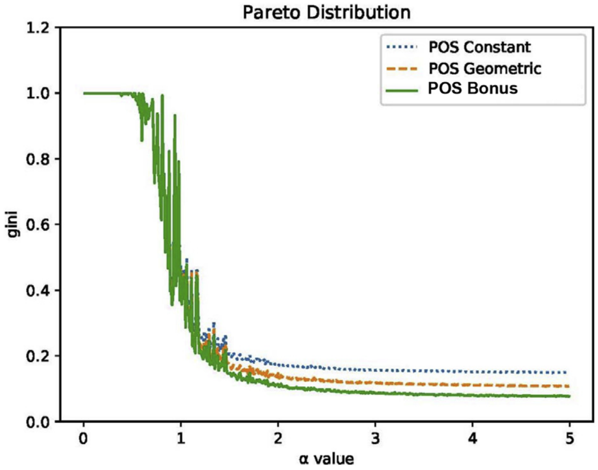

Fig. 6. The Gini coefficient of reward functions under Pareto distribution.

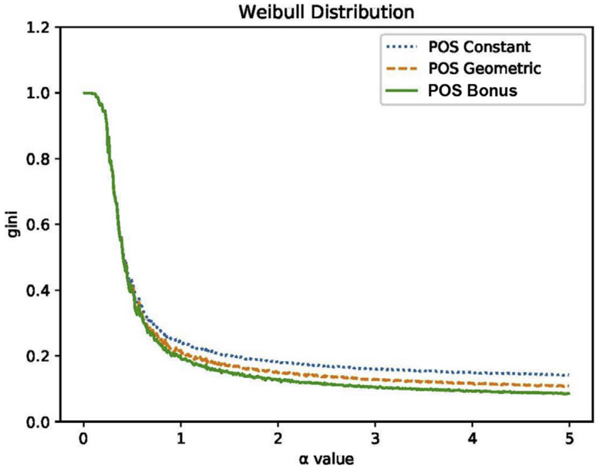

Fig. 7. The Gini coefficient of reward functions under Weibull distribution.

5. Conclusions and future works

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 under the reward functions. Bonus reward function is proposed based on geometric 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 evaluate the fairness of wealth distributions. We borrow Gini coefficient as a metric to evaluate the wealth distribution over cryptocurrencies. The simulation results show that bonus reward function has a lower Gini coefficient, which can cripple compounding to some extend. The future works should consider other reward functions except for the proposed ones to leverage the incentives and equitability.

Declaration of Competing Interest

None.

Acknowledgments

This study was funded by Foundation of National Natural Science Foundation 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).

References

[1] H. Wang, D. He, J. Shen, Z. Zheng, C. Zhao, M. Zhao, Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing, Soft Comput. 21 (24) (2017) 7325–7335.
[2] H. Wang, Z. Zheng, L. Wu, P. Li, New directly revocable attribute-based encryption scheme and its application in cloud storage environment, Cluster Comput. 20 (3) (2017) 2385–2392.
[3] Y. Wang, A. Bracciali, T. Li, F. Li, X. Cui, M. Zhao, Randomness invalidates criminal smart contracts, Inf. Sci. 447 (2019) 291–301.
[4] L. Zhang, Y. Wang, F. Li, Y. Hu, M.H. Au, A game-theoretic method based on q-learning to invalidate criminal smart contracts, Inform. Sci. 498 (2019) 144–153.
[5] X. Zheng, H. Liu, A scalable coevolutionary multi-objective particle swarm optimizer, Int. J. Comput. Intell.Syst. 3 (5) (2010) 590–600.
[6] Y. Wang, M. Zhao, Y. Hu, Y. Gao, X. Cui, Secure computation protocols under asymmetric scenarios in enterprise information system, Enterp. Inform. Syst. (2019) 1–21.
[7] X. Chen, C. Li, D. Wang, S. Wen, J. Zhang, S. Nepal, Y. Xiang, K. Ren, Android HIV: a study of repackaging malware for evading machine-learning detection, IEEE Trans. Inf. Forensics Secur. 15 (2019) 987–1001.
[8] R. Coulter, Q.-L. Han, L. Pan, J. Zhang, Y. Xiang, Data-driven cyber security in perspective–intelligent traffic analysis, IEEE Trans. Cybern. (2019).
[9] T. Li, X. Li, X. Zhong, N. Jiang, C.-z. Gao, Communication-efficient outsourced privacy-preserving classification service using trusted processor, Inf. Sci. 505 (2019) 473–486.
[10] A. Hassan, R. Hamza, H. Yan, P. Li, An efficient outsourced privacy preserving machine learning scheme with public verifiability, IEEE Access 7 (2019) 146322–146330.
[11] N. Jiang, D. Xu, J. Zhou, H. Yan, T. Wan, J. Zheng, Toward optimal participant decisions with voting-based incentive model for crowd sensing, Inf. Sci. 512 (2020) 1–17.
[12] A. Miller, M. Möser, K. Lee, A. Narayanan, An empirical analysis of linkability in the Monero blockchain, 2017.
[13] S. Azouvi, A. Hicks, SoK: tools for game theoretic models of security for cryptocurrencies, arXiv:1905.08595(2019).
[14] G. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, G. Wang, Compounding of wealth in proof-of-stake cryptocurrencies, arXiv:1809.07468(2018).
[15] N. Leonardos, S. Leonardos, G. Piliouras, Oceanic games: centralization risks and incentives in blockchain mining, arXiv:1904.02368(2019).
[16] X.-F. Ding, H.-C. Liu, A new approach for emergency decision-making based on zero-sum game with pythagorean fuzzy uncertain linguistic variables, Int. J. Intell. Syst. 34 (7) (2019) 1667–1684.
[17] H. Garg, R. Arora, Generalized intuitionistic fuzzy soft power aggregation operator based on t-norm and their application in multicriteria decision–making, Int. J. Intell. Syst. 34 (2) (2019) 215–246.
[18] P. Mandal, A.S. Ranadive, Pythagorean fuzzy preference relations and their applications in group decision-making systems, Int. J. Intell. Syst. 34 (7) (2019) 1700–1717.
[19] L. Brünjes, A. Kiayias, E. Koutsoupias, A.-P. Stouka, Reward sharing schemes for stake pools, arXiv:1807.11218(2018).
[20] I. Abraham, D. Malkhi, K. Nayak, L. Ren, A. Spiegelman, Solidus: an incentive-compatible cryptocurrency based on permissionless byzantine consensus, CoRR (2016) abs/1612.02916.
[21] C. Badertscher, P. Gaži, A. Kiayias, A. Russell, V. Zikas, Ouroboros genesis: composable proof-of-stake blockchains with dynamic availability, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2018, pp. 913–930.
[22] R. Pass, E. Shi, FruitChains: a fair blockchain, in: Proceedings of the ACM Symposium on Principles of Distributed Computing, ACM, 2017, pp. 315–324.
[23] O. Schrijvers, J. Bonneau, D. Boneh, T. Roughgarden, Incentive compatibility of bitcoin mining pool reward functions, in: International Conference on Financial Cryptography and Data Security, Springer, 2016, pp. 477–498.
[24] L. Luu, J. Teutsch, R. Kulkarni, P. Saxena, Demystifying incentives in the consensus computer, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM, 2015, pp. 706–719.
[25] X. Xiao, X. Zheng, Y. Zhang, A multidomain survivable virtual network mapping algorithm, Secur. Commun. Netw. 2017 (2017).
[26] H. Wang, D. He, J. Shen, Z. Zheng, X. Yang, M.H. Au, Fuzzy matching and direct revocation: a new CP-ABE scheme from multilinear maps, Soft Comput. 22 (7) (2018) 2267–2274.
[27] R. Dorfman, A formula for the Gini coefficient, Rev. Econ. Stat. (1979) 146–149.
[28] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc., 2015.
[29] R. Beck, C. Müller-Bloch, J.L. King, Governance in the blockchain economy: a framework and research agenda, J. Assoc. Inform. Syst. 19 (10) (2018) 1020–1034.
[30] R. Qin, Y. Yuan, S. Wang, F.-Y. Wang, Economic issues in bitcoin mining and blockchain research, in: 2018 IEEE Intelligent Vehicles Symposium (IV), IEEE, 2018, pp. 268–273.
[31] S. Yitzhaki, et al., On an extension of the Gini inequality index, Int. Econ. Rev. 24 (3) (1983) 617–628.
[32] S.R. Chakravarty, Extended Gini indices of inequality, Int. Econ. Rev. (1988) 147–156.
[33] E.N. Wolff, Changing inequality of wealth, Am. Econ. Rev. 82 (2) (1992) 552–558.
[34] D. Kondor, M. Pósfai, I. Csabai, G. Vattay, Do the rich get richer? An empirical analysis of the bitcoin transaction network, PLoS ONE 9 (2) (2014) e86197.
[35] D.D.F. Maesa, A. Marino, L. Ricci, Data-driven analysis of bitcoin properties: exploiting the users graph, Int. J. Data Sci.Anal. 6 (1) (2018) 63–80.
[36] Y. Yu, J. Deng, Y. Tang, J. Liu, W. Chen, Decentralized ensemble learning based on sample exchange among multiple agents, in: Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, ACM, 2019, pp. 57–66.
[37] M. Gupta, P. Gupta, Gini coefficient based wealth distribution in the bitcoin network: a case study, in: International Conference on Computing, Analytics and Networks, Springer, 2017, pp. 192–202.
[38] F. Caccioli, G. Livan, T. Aste, Scalability and egalitarianism in peer-to-peer networks, in: Banking Beyond Banks and Money, Springer, 2016, pp. 197–212.