Evaluation of Energy Consumption in Block-Chains with Proof of Work and Proof of Stake

Rong Zhang\textsuperscript{1,a} and Wai Kin (Victor) Chan\textsuperscript{1,b}

\textsuperscript{1}Environmental Science and New Energy Technology Engineering Laboratory, Tsinghua-Berkeley Shenzhen Institute, Tsinghua University, Shenzhen 518055, P.R. CHINA

\textsuperscript{a}zr17@mails.tsinghua.edu.cn; \textsuperscript{b}chanw@sz.tsinghua.edu.cn

Abstract. Although there are several special features in block-chain technology such as machine trust, traceability, and security, high energy consumption remains an issue in broadening the applications of block-chain technology. Some researchers proposed the use of proof of stake (PoS) mechanism rather than proof of work (PoW) mechanism to reduce energy consumption of block-chain. However, because PoS cannot guarantee fairness, mixed consensus mechanisms could be a solution and has been adopted in many studies. This paper aims to evaluate the performances of PoW, PoS and mixed consensus mechanisms from three aspects: energy consumption, fairness, and reliability. An agent-based model of a typical block-chain system equipped with different consensus mechanisms is created in NetLogo. This model simulates and evaluates the performances of different consensus mechanisms in the block-chain system.

1. Introduction
In 2008, Nakamoto [1] introduced the concept, structure, and operation mechanism of block-chain. Since then, people began to pay attention to block-chain and identified many useful characteristics, such as machine trust, traceability, and data immutability. Researchers have studied applications of block-chain technology in different domains [2]. A remarkable characteristic of block-chain is the ability to build machine trust through a consensus mechanism. Nakamoto proposed a Proof-of-Work (PoW) mechanism to address the consensus problem. PoW requires nodes to compete to solve a mathematical puzzle, and the winner of which will obtain the right to update the block-chain [3]. The probabilities of success greatly depend on the computing power. Therefore, the competitive mechanism and incentive structure of PoW have led to huge energy consumption [4]. It is estimated that the energy consumption of Bitcoin may overtake that of Denmark by 2020 [5].

King and Nadal [6] proposed a new mechanism, Proof-of-Stake (PoS), which can replace PoW to provide consensus and security. PoS can reduce the mining difficulty of each node and speed up the mining process based on the proportion and time of possessing coins (the reward from block-chain to miners) of each node. However, on the other hand PoS has a fairness problem. This makes rich nodes richer, and reduces the attraction of other nodes [7]. Therefore, some researchers have put forward a combination of PoW and PoS to avoid the drawbacks of both. The theoretical feasibility of such combination method has also been verified [8-10]. This paper develops an agent-based model of block-chain system to simulate its energy consumption, fairness, and reliability. The performances of PoS, PoW and mixed consensus mechanisms are evaluated and compared by using this model.
2. Model description

We created an agent-based model for the block-chain system. This model can be configured to mimic different consensus mechanisms. It consists of node agents and block agents, denoted by sets X and Y, respectively. There are three modules in this model: 1) node generating module, 2) block generating module, and 3) evaluation module. These agents and modules as well as their relationships are described in the following.

2.1. Agents and variables

Node agents: A node agent, \( x \in X \), is generated from node generating module. A node agent is a participant in the block-chain system. Each node agent keeps three variables: computing power \( (C_i) \), reliability index \( (R_i) \), and coinage \( (CA_i) \). Node agents mine with computing power and can get rewards when it creates a block. Reliability index is used to indicate the loyalty of each node agent to the system. Coinage is simply defined as the quantity of coins \( (CO_i) \), multiplied by the holding time \( (ht_i) \). Holding time utility declines as time passes.

Block agents: A block agent \( (y \in Y) \), represents a block generated from the block-chain system. Each block agent owns two variables: timestamp \( (T_j) \) and difficulty degree index \( (d_j) \). Timestamp ensures the traceability of the chain, and the difficulty degree index indicates the difficulty of mining.

2.2. Modules

Node generating module: This module determines the generation of nodes. We define an increment index \( (I_i) \), to signify the attraction of a node to the rest of the nodes in the market.

Blocks generating module: This module is responsible for the generation of blocks. Block agents determine the difficulty degree index. Each node provides its solution \( (S_i) \) to the puzzle \( (P_j) \). A node’s solution is expressed by Eq. 1 under the PoW mechanism and Eq. 2 under the PoS mechanism. The node, which presents the minimum solution, will be the creator of the block and obtain a coin reward.

\[
S_{i-pow} = \frac{p_j \cdot d_j}{C_i} \tag{1}
\]

\[
S_{i-pos} = \frac{p_j \cdot d_j}{C_i \cdot CA_i} \tag{2}
\]

Evaluation module: The computing power results in energy consumption \( (E_i) \) of this node in this block generation period under the PoW mechanism, and it needs to be divided by coinage under PoS mechanism. The fairness \( (F_s) \) can be expressed as the variance of the number of coins owned by the nodes. The reliability function is defined as the reliability index of a node times the weight of that node. We can use Eqs.3-7 to evaluate the energy consumption \( (E_{pow}/E_{pos}) \), fairness \( (F_s) \), and reliability, \( (R_{s-pow}/R_{s-pos}) \), of the block-chain system from start time \( (ST) \) till end time \( (ET) \).

\[
E_{pow} = \sum_{t=ST}^{ET} (C_i) \tag{3}
\]

\[
E_{pos} = \sum_{t=ST}^{ET} \left(\frac{C_i}{CA_i}\right) \tag{4}
\]

\[
F_s = \frac{D(CO_i)}{N} = \frac{\sum(CO_i - AVG(CO_i))^2}{N} \tag{5}
\]

\[
R_{s-pow} = \sum_i(R_i \cdot \frac{C_i}{\sum C_i}) \tag{6}
\]

\[
R_{s-pos} = \sum_i(R_i \cdot \frac{CA_i \cdot C_i}{\sum CA_i \cdot \sum C_i}) \tag{7}
\]

2.3. Model structure

This model consists of nodes generating, block generating and evaluation modules. The system first generates some initial nodes, and then runs the node generation module every 1,440 minutes. A block
is generated every ten minutes and then, the system would be evaluated. The model structure is shown in Figure 1.

![Figure 1](image)

**Figure 1.** The structure of the agent-based model.

3. Simulation experiments

3.1. Parameter setting

We consider a fixed market with 100 participants. The simulation length of each experiment is 300,000 minutes (i.e., 30,000 cycles). The computing power, reliability index of nodes and the difficulty degree of blocks are generated randomly.

3.2. Simulation modes

Based on the above description, six experiments (called “modes”) are considered. Mode 1 execute PoS mechanism entirely. The following modes increase 20% period one after another to adopt PoW mechanism. And mode 6 execute PoS mechanism in whole period. The simulation modes setup is shown in Table 1 and each mode is simulated for ten times.

| Mode   | PoW period | PoS period |
|--------|------------|------------|
| Mode 1: PoS | 0%         | 100%       |
| Mode 2: 0.2PoW | 20%        | 80%        |
| Mode 3: 0.4PoW | 40%        | 60%        |
| Mode 4: 0.6PoW | 60%        | 40%        |
| Mode 5: 0.8PoW | 80%        | 20%        |
| Mode 6: PoW   | 100%       | 0%         |

4. Results and analysis

By running these six experiments, we obtained the performance of the block-chain system under these consensus mechanisms.

4.1. Energy consumption

The first performance index is the energy consumption. Figure 2 shows that the energy consumption of each mode is relatively stable. Typically, the longer the period of PoW mechanism, the more energy was consumed. However, Mode 2 had the minimum energy consumption instead of Mode 1. Adopting the PoW mechanism in the initial 20% period consumes less energy than adopting PoS mechanism entirely. The statistics of energy consumption of each consensus mode are shown in the box chart in Figure 3.
Figure 2. Energy consumption of different consensus modes.

Figure 3. Box chart statistics of energy consumption.

Figure 4. Energy consumption process.

Figure 5. Current total coinage statistics.

To understand the reason why the energy consumption of Mode 2 is lower than that of Mode 1, we explore the process of energy consumption in various consensus modes. As shown in Figure 4, although Mode 2 consumes more energy than Mode 1 in the initial 20% period, Mode 1 depletes energy quicker than Mode 2 in the remaining period. Furthermore, we find that the current total coinage of Mode 2 is larger than that of Mode 1 in the rest 80% period as shown in Figure 5. The current total coinage is an effective way to reduce energy consumption. The more decentralized the coins, the more the total coinage is due to the coinage utility decreasing in time and it will be clear when mining successfully. Moreover, this can be explained as the PoW process in the initial stage making the resource allocation more reasonable and increasing the total coinage, which is much more conducive to the overall energy consumption reduction.
4.2. Fairness
The distribution of coins owns by nodes is used to measure the fairness index of the system. As shown in Figure 6, most nodes own a few coins while some nodes acquire a huge amount of coins in Mode 1. The longer the PoW mechanism is adopted, the distribution of the coins will be more fair. We found out that the variance of the PoS mechanism is particularly large compared with PoW and the mixed mechanism.

![Distribution of coins](image)

**Figure 6.** Distribution of coins.

4.3. Reliability index
We use the reliability function to evaluate the reliability of the system. The reliability index of Mode 1 fluctuates greatly, while other modes are relatively stable as shown in Figure 7. This is because the initial nodes have advantages under the PoS mechanism, and the reliabilities of these initial nodes directly determine the reliability of the whole system. This finding is also verified by the variation of reliability index in individual experiments shown in Figure 8.

![Reliability index of the system](image)

**Figure 7.** The reliability index of whole system.

![The variation of reliability index in individual runs of Mode 1](image)

**Figure 8.** The variation of reliability index in individual runs of Mode 1.

5. Conclusion
We created an agent-based model of a block-chain system equipped with PoW, PoS, and mixed consensus mechanisms using NetLogo. We carried out simulation experiments under six consensus modes. Results from simulation experiments show that energy consumption can be reduced by more
than 75% by the pure PoS mechanism. The lowest energy consumption situation is achieved by the mixed consensus mechanism. For fairness, it was found that the longer the POW mechanism is used for, the more equitable the system will be. As for reliability, the reliability of the PoS mechanism fluctuates greatly because of the influence of initial members. We found that block-chain systems with PoW and mixed mechanisms both have a high reliability. Through the simulation results under different consensus mechanism modes, the following observations are obtained: 1) PoW mechanism provides high reliability and fairness, but also causes high energy consumption, 2) PoS mechanism can significantly reduce energy consumption, but is low in reliability and fairness, and 3) a combination of PoW and PoS mechanisms not only effectively solves the fairness and reliability problems, but also significantly reduces energy consumption.

Acknowledgments

This paper was partially funded by Shenzhen Municipal Development and Reform Commission, Shenzhen Environmental Science and New Energy Technology Engineering Laboratory, Grant Number: SDRC [2016]172.

References

[1] Nakamoto S 2008 Bitcoin: A peer-to-peer electronic cash system
[2] Czepluch J S, Lollike N Z, and Malone S O 2015 The use of block chain technology in different application domains (Copenhagen: The IT University of Copenhagen Press) p 59
[3] Crosby M, Pattanayak P, Verma S, and Kalyanaraman 2016 Blockchain technology: Beyond bitcoin Applied Innovation 2 11
[4] Saleh F 2019 Blockchain without waste: Proof-of-stake SSRN 3183935
[5] Athey S, Parashkevov I, Sarukkai V, and Xia J 2016 Bitcoin pricing, adoption, and usage: Theory and evidence SSRN 2826674
[6] King S and Nadal S 2012 Ppcoin: Peer-to-peer crypto-currency with proof-of-stake (self-published paper)
[7] Poelstra A 2014 Distribution consensus from proof of stake is impossible (self-published paper)
[8] Bentov I, Lee C, Mizrahi A, and Rosenfeld M 2014 Proof of activity: Extending bitcoin’s proof of work via proof of stake (IACR Cryptology ePrint Archive) p 452
[9] Duong T, Chepurnoy A, Fan L, and Zhou H S 2018 Twinscoin: a cryptocurrency via proof-of-work and proof-of-stake Proc. The 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts (ACM press) pp 1-13
[10] Duong T, Fan L, and Zhou H S 2016 2-hop blockchain: Combining proof-of-work and proof-of-stake securely (IACR Cryptology ePrint Archive) p 716