An Alternative Approach to Blockchain Mining Work for Making Blockchain Technologies Fit to Ubiquitous and Mobile Computing Environments

Yuki Kano
Department of Computer Science and Engineering
Waseda University
Tokyo, Japan
konayuki@dcl.cs.waseda.ac.jp

Tatsuo Nakajima
Department of Computer Science and Engineering
Waseda University
Tokyo, Japan
tatsuo@dcl.cs.waseda.ac.jp

***Abstract*—The *mining work concentration problem*, whereby machine power is monopolized when supporting its operation, is becoming a serious problem in virtual currency using the *blockchain technology* that has drawn significant attention in recent years. The paper presents a new solution to solve the problem by using a simple virtual currency service that allows a user to operate the service by giving the user a new incentive based on gamification, not traditional economic incentives. We conducted experiments that show the feasibility of adopting the alternative incentive.**

Keywords—Cryptcurrency; Gamification; Human Crowd's Power; Mining Work Centralization

I. INTRODUCTION

Blockchain technology, which prevents duplicate trading and tampering of data, has recently drawn a significant amount of attention due to its ability to make our society more robust and efficient. Blockchain technology is actually a part of a cryptcurrency system named Bitcoin proposed in 2008; the technology makes it possible to carry out reliable commercial transactions that do not go through third parties on the Internet, which was difficult to realize before [8]. The blockchain technology not only issues its own currency [10]; the blockchain technology has also been used for domain name service [9], smart contracts [7], etc. The blockchain technology will become an important infrastructure to support almost all information services in the future.

While the blockchain technology is expected to be a next-generation technology, some problems have also been pointed out. Since the operation of the network system is carried out by distributing the machine power through peer-to-peer communication, it is possible to be able to selfishly manipulate transaction data by monopolizing more than 51% of the total machine power. Taking Bitcoin as an example, incentives for the Bitcoin operation are to earn its virtual currency. Because only economic incentives are used to obtain the currency, some users aim at obtaining the currency by preparing a huge amount of machine power, and the machine power has been centralized [5]. Such a problem is referred to as the *mining work concentration problem*.

Many techniques have been studied to solve the mining work concentration problem by suggesting an alternative mining algorithm, but no research has given a new incentive to the user. In this study, therefore, by using a method called gamification to motivate people through psychological factors [6], the paper investigates whether the mining work concentration problem can be solved by providing incentives based on psychological factors through gamification rather than offering economic incentives.

II. MINING WORK BASED ON GAMIFICATION

A. An Overview of Our Approach

We design a gamified service to justify our approach and focus on the mining work centralization problem. It is a customized and simplified virtual currency system based on the blockchain technology developed for justifying this research, giving incentives based on psychological factors using gamification against mining work and allowing users to perform approval work.

The developed service consists of the following elements.

Currency Unit: In this service, the unit of virtual currency used is expressed by [coin].

Communication protocol: For the sake of simplicity, the client/server model was used for developing the service. Although the blockchain technology is typically used in the P2P method, since the purpose of this experiment is only to give incentives for psychological factors to mining work, adopting the client/server method would not affect the results.

Account: The service needs to create an account for each participating user. The account is provided with the fields. In order to mine virtual curency, it is necessary to generate a block.

Transaction: The service exchanges virtual currency between users. For sending coins to others, the remittance account name and the amount of coins can be registered. When the transaction is performed normally, the transaction data is added to the transaction data list, and the user can confirm the contents of the transaction added to the data list at any time.

Block: The service generates blocks storing multiple transaction. The creation of the block is done in the visualized

978-1-5090-6226-3/17/$31.00 ©2017 IEEE

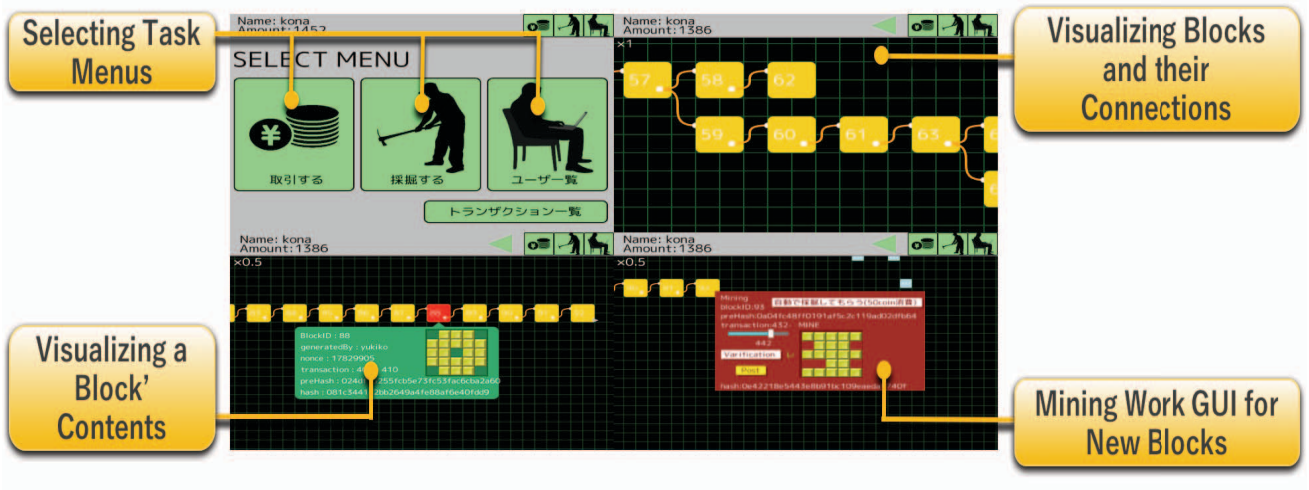

Fig. 1. A GUI Screenshot of the Proposed Service

state by a user. The user stores the hash value of one block in the newly generated block. Blocks can be connected like unidirectional chains. When the approval work succeeds by the mining work to be described later, the block is added to the block data list. Block information and blocks are added to the preceding and succeeding blocks, and the service can check how it is connected in a visualized state.

Mining Work: In order for a user to generate blocks and to add them to the block list, the block approval work is required. When blocks are approved and the chain extends from the block for the longest time, the block creator is given a reward. The mining work in this service is performed by manipulating visualized values by a user. In the game design, the value of the nonce in the block is made to correspond to the shape of the puzzle on the 5 × 5 board surface. The purpose is to make the user voluntarily perform a series of tasks of changing the value of nonce and performing approval work.

B. Service Design

In this service, a server/client model is adopted as presented above. The server mainly deals with data; account, transaction, and block. In a client, the service to offer the functions necessary for mining work and exchange of virtual currency is provided to a user.

All operations by the user are performed through a Graphic User Interface (GUI) and provide six modes according to the necessary functions. The explanation of each mode is listed below, and the execution screen of the application is shown in Fig. 1.

Account Registration and Login: The service registers a new account or logs in with an existing account.

Menu: It is possible to change to the transaction generation mode, the account list confirmation mode, the mining mode, (automatic or manual) and the transaction list confirmation mode, respectively.

Transaction Publication: The service can create a transaction for coin remittance from the account the current user is using, for any existing account.

List Up Account: The service can check the list of account names in the registered account list.

List Up Transaction: The service can check the list of transaction lists.

Mining Work: The service allows a user to check the list of block lists visually. The blocks are connected by hash value. It can generate a new block from the existing latest block. In order to generate a new block, mining work is necessary, and let this user do this work on the GUI.

III. An Experiment Method and Results

In order to evaluate whether the developed service gives users enough incentives for psychological factors caused by gamification, we run the service and conduct experiments using a questionnaire based on users' answers and an interview.

A. Overview

This experiment was carried out by distributing client software for a total of 44 people (Age: 10-20) offering the service described in the previous section. The experiment period is one week. The evaluation was carried out using the statistical data obtained after the experiment and the questionnaire result of the optional answer.

In addition to manually performing mining work to evaluate whether mining work was done as a result of incentives for psychological motivation, the function of automatically mining work with a certain probability by consuming coins held. This approach imitates the mining work in conventional Bitcoin whereby the problem is solved using machine power. If there are users who manually perform mining work even under this circumstance, within the game, it can be said that the incentive of the psychological factor through gamification is meaningful.

B. About Motivating Factors

The section considers what a participant felt motivated to mining work. Focusing on the answer to Q1 (What is the reason for thinking about mining work ?), 52.9% participants

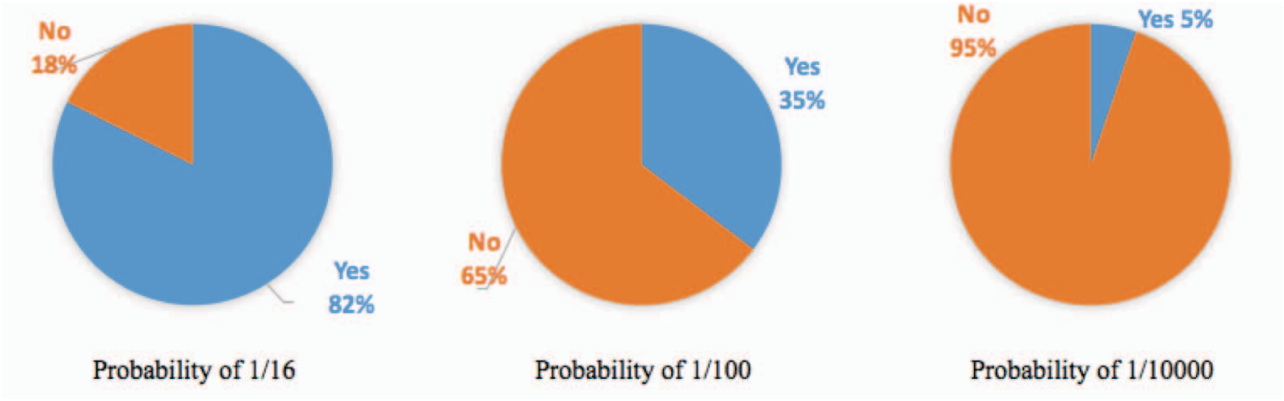

Fig. 2. Proportion trying to continue manual mining work, with probability of (a)1/16, (b)1/100, and (c)1/10000

accounted for "*Mining work itself was fun*.". Also, 47.1% of participants said "*I wanted to build my own block and wanted to join the block. Because I wanted a reward*.", and "*It was told to me to do the mining work.*" for 35.3% of participants. This means that roughly half of the participants were motivated to do mining work through gamification. Similarly, some participants were motivated through economic rewards like Bitcoin, or the intrinsic motivation to contribute the service's operation. However, 35.3% of participants responded that "*I was told to do the mining work*", which can be inferred as a participant who could not have motivated the mining work through gamification. In addition, 5.9% of participants answered "*I wanted to win the mining work competition*." This means that there are a few participants who were motivated through social incentives like the competition to solve a puzzle.

Since the virtual currency used in this service is the currency generated for the experiment, and it was not accompanied by actual monetary value, the difference caused by the design decision is also necessary to be taken into account. In the free interview, some were answers such as "*Because there was no value of coin"; the motivation to collect coin did not rise so much.*", or *"I thought that motivation would change if the reward was directly returned to participants."*

If the currency used here is a currency with monetary value, it can be inferred that the options that can affect the answer result of Q1 include "*I wanted a reward.*", "*Because I was told to do the mining work.*" Since these options are all related to the incentive by an external factor based on "currency", it can be considered that it is independent of the incentives by internal factors using gamification.

C. *Effects of Gamification*

This section discusses whether the game elements offered by gamification used for the service were given incentives from psychological factors to participants. The game element used in the service was to associate the nonce value in the block with the shape of the puzzle. Focusing on the answer to Q2 (Have you had fun in mining work ?), the percentage of participants who actually felt pleasure with mining work was 65%, and the percentage of participants who did not feel fun was 35%. In other words, it can be said that more than half of the participants had motivation for the game elements in the service.

We also try to perform a comparison between automatic and manual mining work. From Table I, the number of total blocks generated during the experiment was 819, among which 542 blocks by manual mining work and 277 blocks by automatic mining work were found. That is, 66% of the blocks are manually created. This ratio generally agrees with the proportion of participants who felt pleasure with respect to the mining work incorporating game elements. Looking at the answer to Q2, half of the participants answered "*Because I wanted to do mining work in my hand*." This is the reason why they did not use automatic mining work. Also, looking at the answer to Q3 (This is a question to the person who performed automatic mining work. What is the reason why you did it ?) , 80% of participants answered "*I used it just as a trial.*" as the reason for using automatic mining work. On the other hand, since 20% of participants answered that "*Mining work was troublesome.*" It can be inferred that most participants accounted for mining work as games instead of monotonous work.

TABLE I. THE NUMBER OF BLOCKS GENERATED

Manual	Auto
542	277

In summary, it is concluded that it is effective to give incentives due to internal factors using gamification to mining work.

D. *Application to Cryptcurrency*

This section considers whether the mining work using gamification can be applied to realistic cryptographic currency using the blockchain technology. In the service used This paper defines the success probability to do mining work as 1/16. According to this probability, if a participant can continue using the service or looking at the answer to Q4 (The probability of mining work success this time was 1/16. Do you think you would continue mining work with this probability ?), 82% of participants answered "*I think I can continue*." from Fig. 2 (a). On the other hand, if looking at the answer to Q5 (If the probability of mining work had reached 1/100, would you decide to continue mining work ?), whether a participant seems to continue mining work when the probability to do mining work successfully is 1/100, 35% of participants from Fig. 2 (b) replied "*I think I can continue.*" Also, if looking at the answer

to Q6 (If the probability of mining work success is 1/10000, would you decide to continue mining work ?), whether a participant seems to continue mining work when the probability to do mining work has become 1/10000, only 5% of participants answered "*I think I can continue*." from Fig. 2 (c).

From these answers, it was found that the lower the success probability of mining work, the less motivated a participant to do mining work. For example, since the success probability of performing mining work in Bitcoin is $1/10^{21}$ as of January 2017 [2], it can be said that it may be impractical to apply the game element of this service applied to mining work in Bitcoin. However, as mentioned above, the service can be used by "fun by game" as a motivational factor; it seems likely to be able to provide machine power using gamification without direct mining work. In other words, it seems to be effective when giving participants mining work as puzzles or games as incentives to provide machine power.

We still need to consider how to make puzzles and game designs more effective and what kind of design you should not get bored with in order to keep participants providing machine power, and we will conduct more experiments to justify the proposed approach.

IV. Related Work

A. Bitcoin Mining

The most notable blockchain technology is the virtual currency named Bitcoin, invented in the paper written by Nakamoto in 2008 [9]. He claimed "*To implement a distributed blockchain server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash*". Hashcash refers to data and nonce, and it is a mechanism that does not allow transactions to be approved until the hash value becomes less than a certain value [1]. By making hassle-free calculation to confirm the transaction using the hash value, it requires huge machine power for preventing illegal transactions.

The mechanism that requires machine power for the approval of a transaction like the approach is called *Proof-of-Work* (PoW). In order for Bitcoin to operate stably, a large number of users need to perform PoW in their computers, so incentives for the users to provide the machine power are required. Nakamoto also said in his paper "*By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them*" [8] Such a mechanism that obtains Bitcoin as a reward using the machine power is represented as *mining* by analogy to digging out gold at a mine.

B. Mining Work Centralization Problem

When the machine power concentrates on one entity, it is pointed out that the entity can modify the chain, which makes it impossible to maintain the legitimacy of the system. For example, as presented in [3], the authors claimed "*Too much hash power controlled by one entity can cause Bitcoin to become similar to the payment systems and currencies it was meant to improve upon. A pool with more than 51% of the network hash power can block transactions, double spend, and change other consensus rules.*"

As shown in [4], the authors claimed "*By using the latency of the network such as deliberately shifting the disclosure timing of block information, we can create a situation where block generation can be monopolized without holding 51% of machine power*". In [7], the author indicated that the Bitcoin mining algorithm has vulnerability to a single concentration and is no longer dispersed; then he proposed solving the problem where it creates random data based on the state of the blockchain, computes randomly chosen transactions from the last N blocks of the blockchain, and returns the resulting hash.

V. Conclusion

In this paper, we proposed encouraging participation in mining work activities by incentivizing users through psychological factors made available by gamification; the objective was to solve the mining work concentration problem. When it comes to make a user perform mining work directly, since the probability of the approval work succeeding is deeply related to motivation, it does not work on such a design. However, the extracted insights show that it is beneficial to use ubiquitous machine power by giving the user a gaming element.

Acknowledment

This work was supported in part by the Program for Leading Graduate Schools, "Graduate Program for Embodiment Informatics" of the Ministry of Education, Culture, Sports, Science and Technology (MEXT) of Japan.

References

[1] A. Back. (2017, April 10). *Hashcash - A Denial of Service Counter-Measure*, [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf.

[2] BLOCKCHAIN.info. (2017, April 10). *difficulty*. [Online]. Avaiable: https://blockchain.info/ja/charts/difficulty.

[3] M. Draupnir. (2017, April 10). *Bitcoin Mining Centralization*, [Online]. Avaiable: https://www.bitcoinmining.com/bitcoin-mining-centralization/.

[4] I. Eyal, and E. G. Sirer, "*Majority is not Enough: Bitcoin Mining is Vulnerable*", Proc. Financial Cryptography and Data Security Conf. (FC'14). 2014.

[5] I. Eyal, and and E. G. Sirer. *How to Disincentivize Large Bitcoin Mining Pools*, (2017, April 10). [Online]. Avaiable: http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools/.

[6] K.Huotari, and J.Hamari, "*A definition for gamification: anchoring gamification in the service marketing literature*", Electronic Markets vol.27, no.1, 2017.

[7] P. Maltsev. (2017, April 10). *A Next-Generation Smart Contract and Decentralized Application Platform*, [Online]. Avaiable: https://github.com/ethereum/wiki/wiki/White-Paper.

[8] S. Nakamoto. (2017, April 10). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[9] Namecoin Project. (2017, April 10). *Namecoin*. [Online]. Avaiable: https://www.namecoin.org.

[10] B. Vitalik, and R. Meni. (2017, April 10). *Colored Coins*, 2015. [Online]. Avaiable: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification.