A survey note on difficulty adjustments using LWMA for crypto currency c0ban

Noritaka Kobayashi, Ph.D, *Blockchain specialist* and Makoto Fujio

contact : nkobayashi88@gmail.com

***Abstract*—We have heard news of coin hopping attack in 2018 several times on PoW. Some case caused leak out of coin and others lead big issues on double spending at exchange market etc. The attack was made by big mining firm or a group who uses cloud mining services a lot. Especially the attack can be made easily on lower than second tier coins because its hash rate is not enough big. In addition, hash rate on cloud mining services became extremely big, any user could have very large hash rate promptly as long as they have enough big fund. Since we see big issues on difficulty adjustment of PoW consensus, we have conducted simulations of LWMA (*Linear Weighted Moving Average*) on c0ban which is the largest crypto currency in Japan. In this paper, we have concluded what type of LWMA would be ideal against hopping attack.We propose the difficulty algorithm would be applied on c0ban.**

***Index Terms*—blockchain, difficulty adjustment, coin hopping attack, LWMA, consensus algorithm, proof of work, PoW, Bitcoin, c0ban**

I. Issues on existing mining industry for crypto currency

BITCOIN was bubble? Price of Bitcion hit the highest record on January 2018 as of July 2018. It was higher than USD 20,000. Meanwhile we have lots of miners since summer in 2017. It is because Bitcoin and almost all crypto currency's price were increasing. We personally began to mining Bitcoin aggressively since summer in 2017. It was relatively easy to mine it and keep profit from there. However, we see the number of miners is growing rapidly from the end of 2017. It became very difficult to keep profit by mining. The world reached to have huge hashpower to keep decentralized network.

Consensus algorithm such as Proof-of-Work could be said invention. It provided us independent and self-growing system for authorizing transaction. Incentive for miners make people start it. It is enough appealing. We often call it *decentralization*. What is decentralization? It is the reason that blockchain is called revolution. Decentralization means that anyone can start to gain profit from the consensus world as they wish without any permission. For example, people does not need authorization to start mining Bitcoin. It is free to start as long as they have knowledge to do it. It is called decentralization.

As one know, prices of crypto currency dropped dramatically after incident of NEM leak out on 26th January 2018 in Japan. It led miner difficulty to gain profit from mining. Mining hashpower trend to be left over this year. Cloud mining providers where people are able to purchase any hashpower instantly by bit become influential. It is because miners who have huge hashpower tend to sell their power on the cloud services. As a result, liquidity of hashpower is increasing. Trend of sharing economy came to mining industry as well. It can be said it is good trend. Because electricity fee for mining is not small. Electricity which mining Bitcion is used for just mining itself. Although the machine calculate /it something to gain Bitcoin, its calculation does not contribute any knowledge activities at all. Someone say it wastes resources. The technology goes against the time. Since we are looking for eco-society and sustainability world in 21st century, we see bit contradiction in this industry. Although decentralized consensus system itselt is invention, its infrastructure especially mining for Bitcoin looks like technology in very early stage of industrial revolution.

In such situation, coins which have the following three features could be attacked by cloud mining users. Firstly, coins which adopt popular hash algorithm It is because it is relatively easy to gain its hashpower from cloud mining providers. Secondly, coins which run less flexibility algorithm for difficulty adjustment. It ie because attackers can take advantage of achieving hopping attack as described later. We see lots of coins who suffer from such attack recently. Lastly, if coins are ranked in second tier group, it would be tended to be attacked than others. It is because market cap of a second tier coin is enough big. It is attractive for attacker to hack it. Since its market cap is second tier, its total hashpower is also second tier. It means attacker could have hugh ratio of whole hashpower of the coins easily. Approximately market cap of second tier is around USD 50 million to 1000 million.

In this paper, we simulate advance difficulty adjustment for coins which could be attacked. We have investigated several algorithm for the simulation. Of all, LWMA (*Linear Weighted Moving Average*) is adopted for the simulation. The result in this paper will be applied to any coin which has the above two features.

II. Attack on mining

A. Coin hopping attack

COIN hopping attack was one of the biggest issues in blockchain industry in 2018. It is because anyone could have made 51% attack on coins easier than before. A good

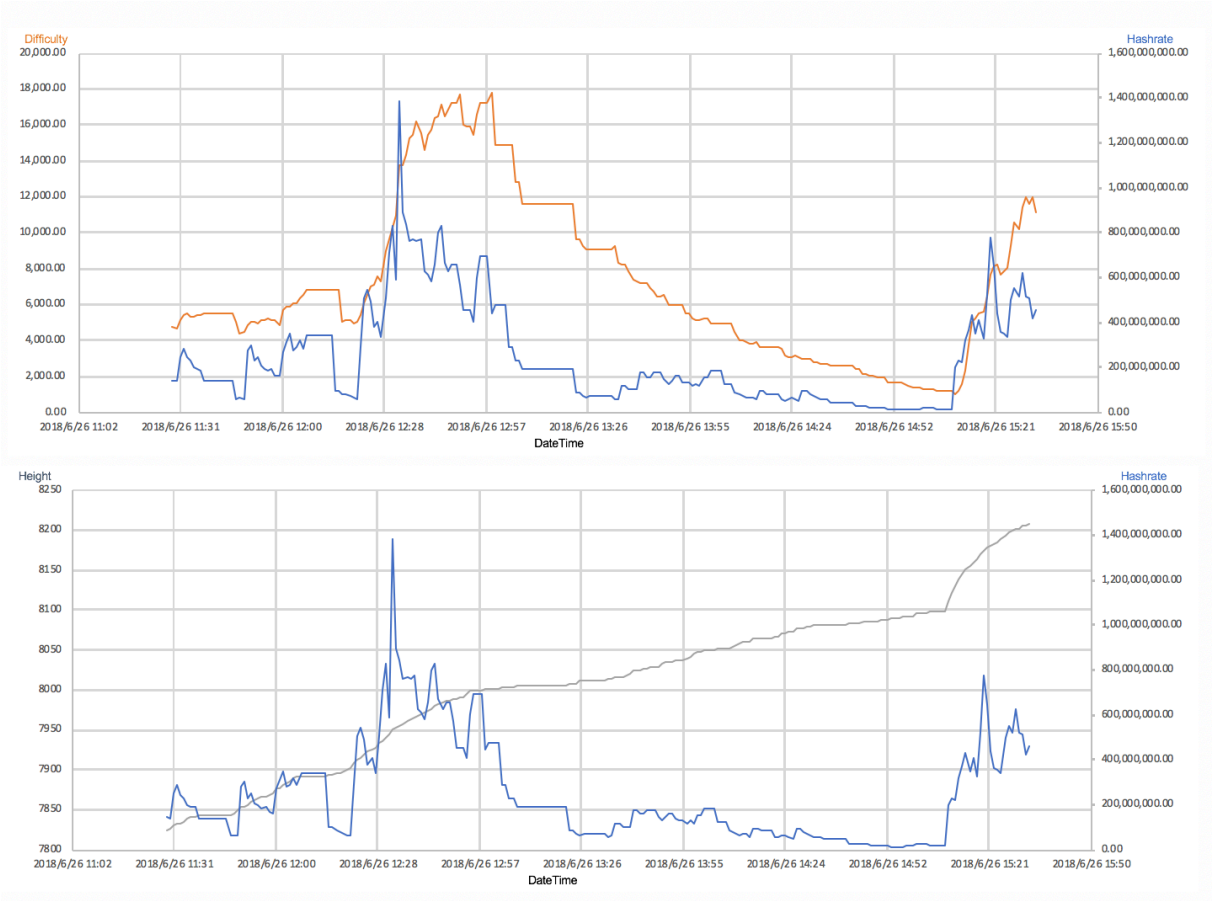

Fig. 1. Simulation result (w=60)

research note[5] for difficulty control by IOHK research was published in July 2017.

Coin hopping attack by an adversarial miner A is described as below according to [5].

- There are at least 2 possible coins (C_1, C_2) A can contribute to. Without a loss of generality, we assume that each of them provides about the same profitability of the mining activity.
- A is mining coin C_2 before the beginning of an epoch a. At the beginning of a he is switching to mine coin C_1.
- Without the contribution of miner A the total mining power of the C_2 network for the epoch decreases.
- For an epoch b right after epoch a, the difficulty of C_2 is to be readjusted to a lower value. So A starts mining C_2 again with a lower difficulty.

The profit the adversarial miner gains from this attack can be calculated as below where we assume Bitcoin's difficulty recalculation function and a constant network hashrate with respect to the rest of network, without the adversarial miner.

Assume that R_0 is hashrate of miners where no miner is participates in the coin hopping attack in both C_1 and C_2 and assume that $R_a = R_0 \cdot p$ is hashrate of the adversarial miner where $0 < p < 1$. Before epoch a the adversary is mining coin C_2, thus the difficulty of the C_2 network is $D_0 = (R_0 + R_a) \cdot \mid \Delta \mid$ as described in Section 3.1 in [6]. During epoch a, the difficulty of the C_2 network is still D_0, and A switches to mine coin C_1 at a difficulty $D_1 = R_0 \cdot \mid \Delta \mid$ calculated from honest miners hashrate R_0 only. During the epoch b the adversary starts mining of C_2, now at difficulty D_1, while honest miners on chain C_1 continute to mine it with higher difficulty D_0. After that A continues to switch between chains C_1 and C_2 always mining on the chain with lower difficulty D_1, spending $R_0 \cdot \mid \Delta \mid$ computational power per block, whereas honest miners spend $(R_0 + R_a) \mid \Delta \mid$ computational power per block. That is how the adversarial miner A will generate profits. Its calculation is described in Section 3, in [5].

B. *Maximizing cloud hashrate attack*

From beginning of 2018, we sometimes see advanced model of coin hopping attack. We call it *Maximizing cloud hashrate attack*.

In this attack, an adversarial miner A_c does not need to mining 2 possible coins. All they need is only one, that is their target coin only. Maximizing cloud hashrate attack is described as below.

- There is a coin C_3 that an adversarial miner A_c is targeting.

Fig. 2. Simulation result (w=32)

- Difficulty adjustment of C_3 is recalculated by every M blocks like Bitcoin's one.
- Hash algorithm of C_3 is general. A miner is able to purchase its hashrate on some cloud mining services.
- Total hashrate of C_3 is not large very much comparing to Bitcoin or Ethereum etc.
- Hashrate more than 10% of total hashrate for C_3 are available on the cloud services.
- The adversarial miner A_c will purchase hashrate on cloud for block M.

If difficulty adjustment of a coin is dynamic one as described in [6], effect of maximizing cloud hashrate attack may not be enough big as the adversarial miner. However the attack can be done by a miner who does not have any mining firm. They could be able to do attack anytime and anywhere as long as they could purchase mining power to the target coins on cloud services.

The attack is very effective to coins of second tier group. Features of second tier coins is that we have exchange market, good volume of trade, its total hashrate is not huge. It is relatively easy to attack such coins for adversarial miners. In addition, cloud mining players became very large in 2018. It lead to provide an environment where an adversarial miner could attack easier than ever.

Some incident was already happened like attack to Monacoin in Russia exchange. In terms of Bitcoin gold, it was in 51% attack [7]. We could say decentralized consensus algorithm is unstable because it is decentralized world. In this paper, we will try to provide meaningful simulation date for coins which could have possibilities to be suffered attack.

III. Simulation target

In this paper, we have conducted several simulations on c0ban in appendix A. C0ban is the first crypto currency for advertisement and entertainment. Its specification is described in table I. It is traded on c0ban exchange market in Japan operated by LastRoots Co., Ltd. We had 16 players of semi-authorized exchange market in Japan on January 2018. Now only 3 players survived, LastRoots is one of three as of July 2018. c0ban is available only on c0ban exchange market now. Its market cap is around USD 100 million to 300 million for the last one year. Difficulty adjustment of c0ban is recalculated by every 2700 blocks which is about one day. The reason why we choice c0ban for the simulation is that we developed it on December 2016. It was released and be open chain crypto currency. As of now, the number of holders is more than 50K. It is like one of the typical second tier coins.

C0ban can be a good target of maximizing cloud hashrate attack. In fact, it was attacked for months in 2018. We have research on which adjustment algorithm would be ideal against the attack. In [5], linear least squares method[8] is introduced and simulated. It is applied on real Bitcoin data as well. They assume that an adversarial miner possesses 20% of total computational power of network and assume that the adversarial miner repeatedly turns on and then off their mining to manipulate difficulty and produce more blocks described in Figure 2 in [5]. Based on the simulation, the profit of the attacker then is two times lower. Thus the linear difficulty control algorithm is better than one used in Bitcoin for coin-hopping attack scenario.

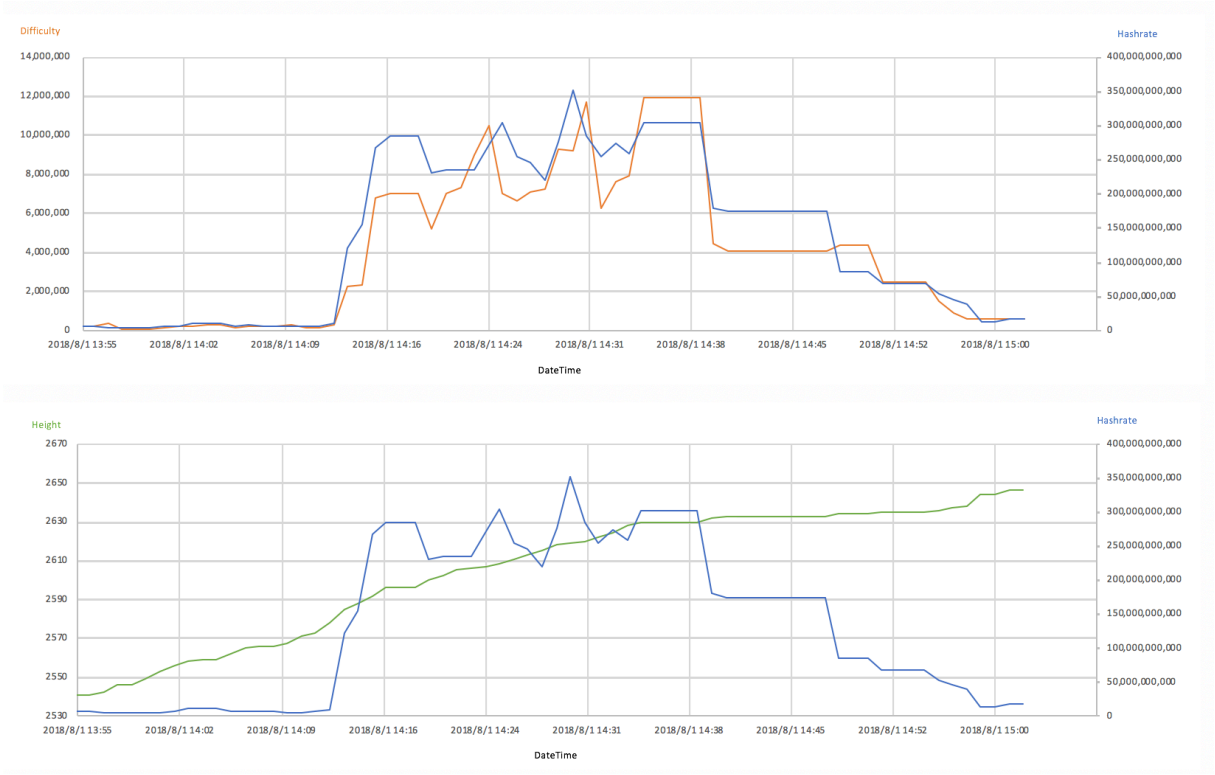

Fig. 3. Simulation result (w=8)

A. LWMA

In this paper, we focus on Maximizing cloud hashrate attack. The attacker could possess more than 20% or more of total computational network. In addition, they could increase their hashrate as they wish as long as hashrate is available on cloud mining services. We need to consider more drastic attack than coin hopping attack. Flexible conformability is required on difficulty algorithm against such attack. On the way to research on difficulty algorithm to find fit the situation, we referred LWMA, Linear Weighted Moving Average, history[9] and its application data[10]. We considered the algorithm might be one possible choice.

On LWMA, difficulty is recalculated based on the last w blocks' difficulty. We have conducted four types of simulation on real data of c0ban. On the simulation, parameters $w = 60, 32, 8, and 4$ are selected.

B. Simulation 1 w=60

We describe two type of simulation graphs for each four cases. The first one is graph of relation between difficulty (dot line) and hashrate. The latter is relation between block hight (dot line) and hashrate.

Although we could see conformability of difficulty while hashrate is increasing, conformability is lost when hashrate was dropped as shown in Figure1. In terms of block generation interval, its speed seems to be stable. Such stability might be enough for network. Since more importance is stability of difficulty, w=60 is not ideal for the situation.

C. Simulation 2 w=32

If we set w=32, we could also see conformability of difficulty while hashrate is increasing as shown in Figure 2. However when hashrate was dropped, difficulty was still remain high. Since it take time to generate new block, difficulty adjustment is not calculated sooner. It is not the one we are looking for the situation.

D. Simulation 3 w=8

In case of w=8, conformability of difficulty seems very good for whole situation as shown in Figure 3. While hashrate is increaseing, conformability of difficulty looks good. When hashrate is dropped, difficulty seems to be kept on conformability.

In terms of block generation interval, it looks it take time a little bit. But it is within the range of acceptable.

E. Simulation 4 w=4

If w is 4, stability of difficulty was lost. It looks it has conformability at a glance, however it is not stable after dropping hashrate as shown in Figure 4.

IV. Conclusion

BASED on the simulation, we believe that parameter w=8 is the best of all. c0ba is going very well since its launch. It is the first crypto currency tied up with advertisements and entertainments. After its ICO on July 2016, the coins was

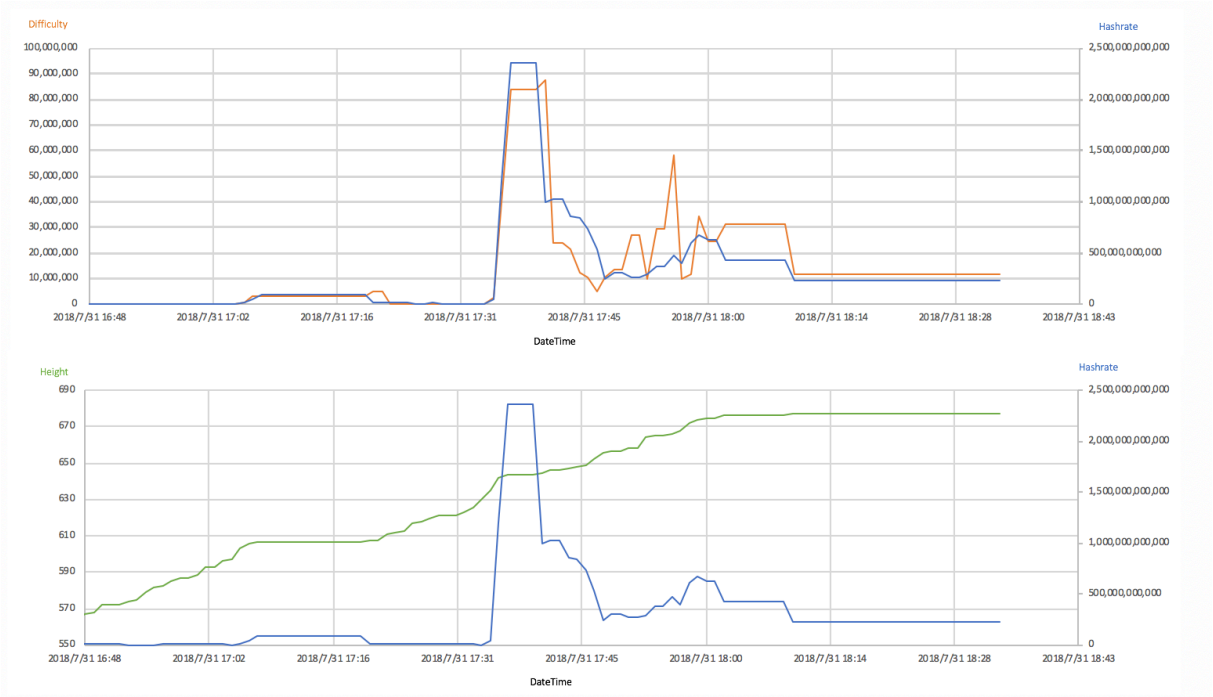

Fig. 4. Simulation result (w=4)

activated on December 2016, its application was released on February 2017, on the list of exchange on March 2018. Its users are increasing gradually. As of now, its market cap is enough big which is around USD 150 million to 200 million. Its difficulty adjustment is recalculated by every 2,700 blocks. It is one of the simple method. We believe that we will propose to the community that LWMA described in this paper should be applied on the real network of c0ban for protection of users assets. As one of the main contributors for c0ban community, we will keep on monitoring not only situation of mining for c0ban but also overall status of mining and cryptocurrency industry.

We believe that concept of decentralized consensus is truly invention. We could say it is miracle. Imagine that we have now more than 10K nodes across the world for Bitcoin mining. It is providing security network and maintain assets more than USD 100 billion for 24/365. From the simple algorithm of decentralized network, it took only for 9 years to build this hash network. We did not have any leader. No manager tried to make it growth. Self-growing system has established the decentralized network. Millions of engineers and business person came this industry to be part of the revolution.

We think we have lots of issues on blockchain, crypto currency, and decentralized algorithm. Although it is invention, it is still very early stage of changing era. Even though LWMA or other method is applied on c0ban or other second tier coins, it is not enough for stability. New type of attack will be created. The important thing that we should keep in mind is continue to improve. Decentralized network would be evolved by decentralized speculation of people. Since it is decentralized, we do not have center of it. We should not have it. We believe that decentralized network will accelerate the evolution of technology and management. Attack never ends. If you give up then it all ends here.

ACKNOWLEDGMENT

I want to thank you for technical advisory comments, and support simulation to Takashi Matsukaze, Masakazu Yano, Hiroaki Mizuno and Jun Hamada. Their valuable comments and support helped us to achieve result of the simulation especially.

APPENDIX A
SPECIFICATION OF C0BAN IN DETAILS

C0BAN is designed based on Bitcoin, the following two issues will be tackled to solve. Firstly, it is increasing the number of transactions per seconds, the other is speeding up of authorization time. The two enhancements could be achieved by adjusting both block size and block generation interval simultaneously. We have done whole experiments to decided what block size and block generation interval would be the best for c0ban.

In this paper, installation of *segwit* is described in detail to achieve the above two enhancements. Consensus algorithm is discussed at section A-F. Detailed specifications such as the number of total coins issued, etc. are referenced in Appendix A. Other basic technologies could be referenced from Bitcoin white paper[12].

A. Block size

Average size of transaction on blockchain is mostly fixed size as shown in TABLE **??** and **??**. All transaction are stored

in a block of blockchain. Hence if a size of block is large, more transaction could be processed in the block. Simply but, the bigger the size of block, the more transaction could be done.

To increase the number of transactions per second, the best way would be to make the block size large. 4MB to 20MB of block size are considered for c0ban and its demonstration experiment has been conducted. As known, 2MB of block size is being used for Bitcoin. Although larger size of block was tried for Bitcoin before, it was stopped due to security reasons. It is also crucial to increase block size for Bitcoin engineers. It has been attempted several times but not be finalized yet [13]. c0ban could be improved so that secure transactions could be done which would be proved by the experiment we have conducted. In conclusion, 4MB is applied for c0ban. It is explained in section of experiments.

B. Block generation interval

A Block on blockchain consists of several transactions. Once the block is authorized, whole transactions stored are authorized as well. Block generation interval is also described as an interval of block authorization. It is ten minutes in general on Bitcoin blockchain. As described, c0ban would be used at cashiers of shops, 30 to 60 seconds are set as block generation interval. Although the adjustment would be extremely difficult, it should be solved for becoming general payment method.

If block generation interval is set from X to Y where $X > Y$, the number of transactions per second could become X/Y times larger.

In conclusion, 32 seconds is selected for c0ban block generation interval. Experiments result will be described later.

C. The number of blocks for authorization

As mentioned, we are seeking for crypto currency which could authorize transfer faster. That is why 32 seconds are chosen for block generation interval. As known, authorization of block chain is not decided by generation interval only. It depends on the number of blocks needed to confirm transaction. The current bitcoin uses 6 blocks which means about one hour for authorization because block generation interval of bitcoin is 10 minutes. one hour is too slow for c0ban usage. On the other hand, 32 seconds is 19 times faster than bitcoin. In terms of final block authorization, we set 15 blocks (= 8 minutes) which means c0ban is 7.5 times faster authorization than bitcoin.

D. Difficulty adjustment

If term of difficulty adjustment is d day(s) and block generation interval is g day(s), the number of blocks generated until the next difficulty adjustment is described as follow.

$$d/g$$

Assume that bitcoin of d and g are d_b and g_b, respectively. Assume that c0ban of d and g are d_c and g_c, respectively. If the below formula is true, we could say we have enough terms for difficulty adjustment.

$$d_c > d_b g_c / g_b$$

Since d_c is 0.74 days where d_b is 14 days, g_b is 10 minutes, and g_c is 32 seconds, 1 day is selected for c0ban difficulty adjustment for further security. By taking further security into consideration, 1 day is chosen for difficulty adjustment for c0ban. Regarding to the number of blocks for authorization and difficulty adjustment, the setting is for the early stage of c0ban. These may be adjusted at right timing in the near future.

E. SegWit (Segregated Witness)

An input field of transaction includes a signature information, called Unlocking-Script, for certifying ownership of the balance, as shown in Table **??**. The SegWit (Segregated Witness) separates this Unlocking-Script into another data region, called witness.

The field size of Unlocking-Script can be reduced to one-fourth by only storing pointer to the witness instead of storing whole Unlocking-Script data. As a result, transaction size is also reduced, so that the number of transactions which are included in a block are increased. SegWit is installed on c0ban and was confirmed that it work well.

F. Hash calculation algorithm

Establishing secure and stable system are the most important requirements. The reason why we take advantage of Bitcoin technologies is its reliability. Drastic modification of Bitcoin should be avoided as it provides safe and stable operation. It is our basic stance.

Regarding to selecting consensus algorithm, we follow the stance. Although *PoS (Proof of Stake)*, *PoC(Proof of Capacity)* or *PoI(Proof of Importance)*, etc are introduced on new crypto currencies recently, those algorithm have not yet achieved stable enough performance. Besides, tremendous labor would be needed to improve source codes despite its uncertainty of stability. *PoW(Proof of Work)* was applied as consensus algorithm for c0ban out of such consideration. Then, selection of hash calculation algorithm has been discussed in our team. As stated earlier, demonstration experiment has been conducted including performance check of hash calculation algorithm.

We basically believe that mining itself does not have any social value other than gaining crypto currency after huge calculation. Since gaining currency such as mining gold should be extremely difficult, mining mechanism of blockchain was invented. It would work for decentralized authorization system very well, however its electricity spending on the mining activities face lack of economic rationality. Electricity consumption would be crucial issues because necessity of nuclear plant for electricity is discussed very actively in Japan since 3.11 in 2011. The future technology of blockchain should be improved as Earth-friendly manner. The points would be considered on c0ban 2.0 described in section **??**. Regarding to hash calculation algorithm for c0ban, the following two hash algorithms are examined.

- SHA256: It is a hash calculation algorithm which is applied on Bitcoin. ASIC(application specific integrated circuit) is already supported. All mining machine will be replaced to ASIC in the near future.
- Ethash: It is a hash calculation algorithm which is applied on Ethereum. It is said that it would be difficult to produce ASIC because of utilizing a large amount of memory. That is why CPU or GPU mining are major now.

In conclusion, SHA256 was selected after discussion for months. Our decision was not made by performance of algorithm. It was made by business and stable operation points of view. We could expect lots of c0ban app users in a short term, hashing power would be needed as much as quickly for stable and secured operation. If new kinds of algorithm is selected, we have to wait for miners who have capability of using the new one. It could become a crucial issue to c0ban business. That is why the most common algorithm, which is SHA256, should be fit for c0ban.

G. Mining

The first 1,000 blocks are used for pre-mining. Although c0ban is a public block chain, block rewards for mining is set zero for the first 739,125th blocks which means 273.7 days $((738,125block * 32seconds)/(24hours * 60minutes * 60seconds))$. On the other hand, transaction fee is set from the beginning.

The reason of the algorithm designed is to aim performance stability. We have conducted demonstration experiments for months. We have confirmed its operation check. For its last step, we concluded that performance check should be run on real market inside our highly reliable data center configuration as described in table II. Since it is the first challenge in the world to launch new block chain combined advertisement solution, we have to figure out what revision should be made to update c0ban. Prompt revision should be beneficial to all c0ban users.

After 739,126 blocks, block rewards is set two RYO from 739,126th to 985,500th blocks. Two RYO will be added every 246,375th blocks until rewards become eight RYO. From 1,478,251th blocks, block rewards is set eight RYO towards 9,608,625th block which is the last block with block rewards. Block rewards on c0ban will be terminated sometime in 2025.

As known, block rewards on bitcoin decrease every four years. Its miner can not expect enough rewards from 2020 July which is the next reward halving [20]. Since SHA256 is selected for c0ban, we could expect bitcoin miners could switch to c0ban miners. Their hashing power will make c0ban safety strengthening. We hope that c0ban could be a stable reward platform for miners until 2025.

H. The number of transaction per second

From the whole specifications mentioned in this section, the number of transaction per second could be increased. Ideally speaking, its maximum is 700 transaction per second. It means about 60 million transactions per day. It would be quite enough for our business model. However to achieve the maximum power, a huge number of nodes will be required. The speed is not confirmed on demonstration experiments. As described in table II, transaction speed c0ban would depends on c0band which is a node for transfer transaction to c0ban block chain from our own iDC. Increasing of amount of transaction could be monitored. It has proportional relation with the number of c0ban app or exchange market users. Investment on facility would be proceeded to fit the number of users. Transaction speed needed could be achieved.

APPENDIX B
SPECIFICATIONS OF C0BAN

Basic and program specifications of c0ban are shown in Table I and Table II respectively. These are as of end of September and may be changed.

APPENDIX C
HISTORY OF C0BAN DEVELOPMENT

LastRoots Co., Ltd was set on June 2nd 2016. Only 6 months have passed to develop whole system since founding.

REFERENCES

[1] Noritaka Kobayashi, and Yoshinobu Shijo, *c0ban: a crypto currency is for advertisements and entertainment apps*, c0ban white paper, v0.1, Sep. 2016.

[2] Noritaka Kobayashi, and Yoshinobu Shijo, *c0ban: a crypto currency is for advertisements and entertainment apps*, c0ban white paper, v0.2, Dec. 2016.

[3] Noritaka Kobayashi, Tatsuhiro Tsuchiya, and Tohru Kikuno, *MinimizingtheMean Delay of Quorum-Based Mutual Exclusion Schemes*, The Journal of Systems and Software, Vol.58, No.1, pp.1-9, Sep. 2001.

[4] Noritaka Kobayashi, *Design and Evaluation of Automatic Test Generation Strategies for Functional Testing of Software*, Ph.D thesis, Osaka university March, 2002.

[5] Dmitry Meshkov, Alexander Chepurnoy, Marc Jansen, IOHK Research *Revisiting Difficulty Control for Blockchain Systems*.

[6] D. Kraft,, *Difficulty control for blockchain-based consensus systems, Peer-to-Peer networking and applications*, in 2015 1-17.

[7] http://fortune.com/2018/05/29/bitcoin-gold-hack/

[8] C.L. Lawson, R.J. Hanson, *Solving least squares problems*, Vol. 161, SIAM, 1974.

[9] https://github.com/zawy12/difficulty-algorithms/issues/24

[10] https://github.com/zawy12/difficulty-algorithms/issues/3

[11] The DAO attack: Code Issue Leadvertisements to $60 Million Ether Theft, June, 2016. http://www.coindesk.com/dao-attacked-code-issue-leadvertisements-60-million-ether-theft/

[12] Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, conculted January, 2012, 2008.

[13] Roger Ver Is Still Determined to Increase the Bitcoin Block Size Limit via a Hard Fork, September, 2016. https://Bitcoinmagazine.com/articles/roger-ver-is-still-determined-to-increase-the-Bitcoin-block-size-limit-via-a-hard-fork-1474550552

[14] Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Crypto-Currencies,* published by O'Reilly Media, Inc., 2014.

[15] Reference information from the URL, https://bitcoin.org/en/development

[16] Reference information from the https://github.com/bitcoin/bitcoin

[17] World Community Grid Welcomes Ripple Labs as a Partner, https://ripple.com/insights/world-community-grid-welcomes-ripple-labs-as-a-partner/ Dec. 2013.

[18] Gavin Wood, *Ethereum : A secure decentralised generalised transaction ledger homestead revision*, August, 2015.

[19] W. Feller, *An introduction to probability theory and its applications*, 1957.

[20] Bitcoin Block Reward Halving Countdown, estimated that July 2nd, 2020. *http://www.bitcoinblockhalf.com/*.

[21] Inoue Takehiko. *Slam Dunk, Anzai sensei*.

Noritaka Kobayashi, Ph.D He received Ph.D in Computer Science from Osaka University, 2002. His major was distributed computing and software test efficiency. He skipped two grades to receive Ph.D. After graduation, he worked as a business consultant at Nomura Research Institute, Ltd. for nine years and business development executive at GREE Inc. for two years. He was engaged in starting up new businesses in IT & mobile as well as M&A. He established Diixi Pte.Ltd in 2012 and Yourwifi Pte.Ltd. in 2013 both in Singapore to acquire Asian market. The CHAOS ASIA which is an innovative pitch event, was produced by him in 5 cities world wide. He was selected as Asian entrepreneur by AsianEntrepreneur.org in 2015. Certified from Columbia business school, executive education program in 2008. He is also an associate professor at Business Breakthrough university since 2010. He will give lectures of ”block chain and Fintech” there from April, 2017. Yourwifi was received 292nd rank at Technology Fast Asia 500 in December 2017.

Makoto Fujio He graduated of Department of Engineering Science of Osaka Univeristy in 2011. After that, he joined Fuji Xerox Co., Ltd as an engineer. He encountered blockchain and bitcoin by chance in 2017. Since then he focused on its research and development. Since he see forecast of c0ban appealing, he joined in 2018. He supported the simulation in this paper.

TABLE I
APPENDICES B-1 : BASIC SPECIFICATIONS OF C0BAN

a	Release date	December 15th, 2016
b	Coin name	c0ban
c	Unit	RYO
d	minimum Unit	0.00000001 RYO = 1 k0bayash1
e	Consensus algorithm	PoW (Proof of Work)
f	Hash algorithm	SHA256
g	Single signature address format for public key	34-digit starting with “8”
h	Multi signature address format for public key	34-digit starting with “C”
i	Address format for private key	52-digit starting with “M”(WIFC) or 51-digit starting with “5” (WIF)
j	Block generation interval	32 seconds
k	Total amount of c0ban	88,000,000 RYO
l	Amount of c0ban for pre-mining	22,000,000 RYO where the first 1000 blocks are used
m	Amount of c0ban for normal mining	66,000,000 RYO
	others	block generation interval and coinbase (reward for miners) will be determined as normal mining will be finished for 10 years.
n	block reward	0 RYO from block 1,001 to block 739,125
o	block reward	2 RYO from block 739,126 to block 985,500
p	block reward	4 RYO from block 985,501 to block 1,231,875
q	block reward	6 RYO from block 1,231,876 to block 1,478,250
r	block reward	8 RYO from block 1,478,251 to block 9,358,687
s	block reward	4 RYO for block 9,358,688

TABLE II
APPENDICES B-2 : PROGRAM SPECIFICATIONS OF C0BAN

a	Name	c0band, c0ban-qt
b	Port number for P2P connection	3881
c	Port number for RPC	3882
d	Port number for TEST P2P connection	13881
e	Port number for TEST RPC	13882
f	DNS seed configuration	none
g	Initial connection node address	4 (fixed)
h	Magic number	0x6330626e(c0bn)
i	Maximum block size	4MB
j	Transaction compression	SegWit
k	Multilingual support	YES
l	Version number	v0.15.1.1
m	Additional RPC	Outputs Packaging

TABLE III
APPENDICES C : HISTORY OF C0BAN DEVELOPMENT

June 5th 2016	Started to develop block chain c0ban
June 14th 2016	Run press release about c0ban concept
July 21st 2016	Launched ICO for c0ban development
September 26th 2016	c0ban white paper v0.1 was released
December 15th 2016	Genesis block of c0ban was started
December 15th 2016	c0ban white paper v0.2 (this paper) was released
December 15th 2016	c0ban web wallet was released. c0ban explorer was released
February 23rd 2017	c0ban apps was released
March 28th 2017	c0ban exchange market was released
December 2017	market cap of c0ban exceeded USD 300 million