The Trailer of Blockchain Governance Game*

SONG-KYOO KIM

ABSTRACT

This paper deals with design of the secure blockchain network framework to prevent damages from an attacker. The design is based on the hybrid theoretical approaches which is named as the Blockchain Governance Game. The framework of this game finds the best strategy towards preparation for preventing attacker a network malfunction. Analytically tractable results are obtained by using hybrid of the fluctuation theory and the mixed strategy game theory which enables to predict the moment for operations and deliver the optimal portion of backup nodes to protect the blockchain network.

Keywords: Blockchain, Bitcoin, mixed game; stochastic model; fluctuation theory; network security, 51 percent attack

AMS Classification: 60K30, 60K99, 90B60, 90B50, 91A35, 91A55, 91A80

1. INTRODUCTION

The cryptocurrencies (coins and tokens) are the collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called coins (or tokens) are used to store and transmit value among participants in the blockchain network. A blockchain is a growing list of records, called blocks, which are linked using cryptography. Blockchains which are readable by the public are widely used by cryptocurrencies. Though blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system. One of strength of blockchain is the decentralized peer-to-peer network which eliminates a number of security risks that come with data being held centrally. Decentralized consensus has therefore been claimed with a blockchain. In the other hand, we have observed the intensive attacks which are dedicated for blockchain networks and the 51 percent attack is one of typical attacks by generating blocks with false information (transactions) because of this genion strength of the blockchain. A private blockchain which is permission has been proposed for business or government uses. This type of blockchains can be considered a middle-ground for companies that are interested in the blockchain technology in general but are not comfortable with a level of control offered by public networks (Kim, 2018a). It is noted that the network control even for private blockchains should be minimal to avoid all security matters what the typical centralized networks have.

*) This paper is the abridged summary of the working paper which is targeting an international journal in the applied mathematics area.
The Blockchain Governance Game is proposed in this paper and it is basically a stochastic game model with the fluctuation and the mixed strategies. The model is targeted to prevent blockchain based attacks (i.e., the 51 percent attack) and keep the network decentralized. We consider the case that an attacker to trying to build an alternative block chains faster than regular miners (Nakamoto, 2009). The defender (or controller) only manages the small percentage of nodes which are released prior the attack is happened. The results are given as joint functionals between two players of the predicted time of the first observed threshold which is crossing the half of the total nodes (i.e., 51 percents) along with values of each component upon this time.

2. Stochastic Model For Blockchain Network

2.1 Basic Stochastic Model
The antagonistic game of two players (called "A" and "H") are introduced to describe the blockchain network between a defender and an attacker. Both players compete to build the blocks either for honest or false ones. Let \((\Omega, \mathcal{F}(\Omega), P)\) be probability space \(\mathcal{F}_A, \mathcal{F}_H, \mathcal{F}_\tau \subseteq \mathcal{F}(\Omega)\) be independent \(\sigma\)-subalgebras. Suppose:

\[
\mathcal{A} := \sum_{k \geq 0} X_k \xi_{s_k}, \quad s_0(= 0) < s_1 < s_2 < \cdots, \text{ a.s.} \quad (2.1)
\]

\[
\mathcal{H} := \sum_{j \geq 0} Y_j \xi_{t_j}, \quad t_0(= 0) < t_1 < t_2 < \cdots, \text{ a.s.} \quad (2.2)
\]

are \(\mathcal{F}_A\)-measurable and \(\mathcal{F}_H\)-measurable marked Poisson processes \((\xi_a)\) is a point mass at \(a\) with respective intensities \(\lambda_A\) and \(\lambda_H\) and point independent marking. These two values are related with the computing performance for generating blocks for attackers and honest nodes in the blockchain network. They will represent the actions of player A (an attacker) and H (an honest node). Player A builds the blocks with false transactions (e.g., double spend) at times \(s_1, s_2, \ldots\) and sustain respective build the blocks of magnitudes \(X_1, X_2, \ldots\) formalized by the process \(\mathcal{A}\). The building blocks to player H are described by the process \(\mathcal{H}\) similarly. Player H will generate the blocks which contain the correct transactions. Both players races to build their blocks (either honest or false). The processes \(\mathcal{A}\) and \(\mathcal{H}\) are specified by their transforms

\[
\mathbb{E}[g^{\mathcal{A}(s)}] = e^{\lambda_A(s)(g-1)}, \quad \mathbb{E}[z^{\mathcal{H}(t)}] = e^{\lambda_H(t)(g-1)}. \quad (2.3)
\]

The game is observed at random times in accordance with the point process which is equivalent with the duration of PoW (Proof-of-Work) completion (around 10 minutes in the Bitcoin) in the blockchain network (Kim, 2018a):

\[
T := \sum_{i \geq 0} \xi_{\tau_i}, \quad \tau_0(> 0)), \tau_1, \ldots, \quad (2.4)
\]

which is assumed to be delayed renewal process. If

\[
(A(t), H(t)) := \mathcal{A} \otimes \mathcal{H}([0, \tau_k]), \quad k = 0, 1, \ldots, \quad (2.5)
\]
forms an observation process upon \( A \otimes H \) embedded over \( T \), with respective increments
\[
(X_k, Y_k) := A \otimes H([\tau_k-1, \tau_k]), \quad k = 1, 2, \ldots,
\]
and
\[
X_0 = A_0, \quad Y_0 = H_0.
\]
The observation process could be formalized as
\[
A_T \otimes H_T := \sum_{k \geq 0} (X_k, Y_k) \varepsilon_{\tau_k},
\]
where
\[
A_T = \sum_{i \geq 0} X_i \varepsilon_{\tau_i}, \quad H_T = \sum_{i \geq 0} Y_i \varepsilon_{\tau_i},
\]
and it is with position dependent marking and with \( X_k \) and \( Y_k \) being dependent with the notation
\[
\Delta_k := \tau_k - \tau_{k-1}, \quad k = 0, 1, \ldots, \tau_{-1} = 0,
\]
and
\[
\gamma(g, z) = \mathbb{E}[g^{X_k} \cdot z^{Y_k}], \quad g > 0, \quad z > 0.
\]
By using the double expectation,
\[
\gamma(g, z) = \delta(\lambda_A(1 - g) + \lambda_H(1 - z))
\]
and
\[
\gamma_0(g, z) = \mathbb{E}[g^{A_0} z^{H_0}] = \delta_0(\lambda_A(1 - g) + \lambda_H(1 - z))
\]
where
\[
\delta(\theta) = \mathbb{E}[e^{-\theta \Delta_i}], \quad \delta_0(\theta) = \mathbb{E}[e^{-\theta \tau_0}]
\]
are the magical transform of increments \( \Delta_1, \Delta_2, \ldots \). The game in this case is a stochastic process \( A_T \otimes H_T \) describing the evolution of a conflict between players A and H known to an observation process \( T = \{\tau_0, \tau_1, \ldots \} \). The game is over when on the \( k \)th observation epoch \( \tau_k \), the collateral building blocks to player A exceeds more than the half of the total nodes \( M \). To further formalize the game, the exit index is introduced:
\[
\nu := \inf \{k : A_k = A_0 + X_1 + \cdots + X_k \geq \left( \frac{M}{2} \right) \},
\]
\[
\mu := \inf \{j : H_j = H_0 + Y_1 + \cdots + Y_j \geq \left( \frac{M}{2} \right) \}.
\]
Since, an attacker is win at time \( \tau_\nu \), otherwise an honest node generates the correct blocks. We shall be targeting the confined game in the view point of player A. The first
passage time $\tau_\nu$ is the associated exit time from the confined game and the formula (2.6) will be modified as

$$\overline{A}_\tau \otimes \overline{H}_\tau := \sum_{k \geq 0} (X_k, Y_k) \in \tau_k$$ (2.16)

which the path of the game from $\mathcal{F}(\Omega) \cap \{ \nu < \mu \}$, which gives an exact definition of the model observed until $\tau_\nu$. The joint functional of the blockchain network model is as follows:

$$\Phi_{[\frac{\nu}{\mu}]} = \Phi_{[\frac{\nu}{\mu}]}(\xi, g_0, g_1, z_0, z_1) = \mathbb{E}[\xi^{\nu} \cdot g_0^{A_{v-1}} \cdot g_1^{A_{v}} \cdot z_0^{H_{v-1}} \cdot z_1^{H_{v}} 1_{\nu < \mu}]$$ (2.17)

where $M$ indicates the total number of nodes (or ledgers) in the blockchain network. This functional will represent the status of attackers and honest nodes upon the exit time $\tau_\nu$. The latter is of particular interest, we are interested in not only the prediction of catching up the blocks by attackers but also one observation prior to this. The Theorem 1 establishes an explicit formula for $\Phi_{\frac{\nu}{\mu}}$ with (2.11) and (2.13):

$$\begin{align*}
\gamma &:= \gamma(g_0 g_1 u, z_0 z_1 v), \\
\gamma_0 &:= \gamma_0(g_0 g_1 u, z_0 z_1 v), \\
\Gamma &:= \gamma(g_1 u, z_1 v) \\
\Gamma_0 &:= \gamma_0(g_1 u, z_1 v) \\
\Gamma^1 &:= \gamma(g_1, z_1 v) \\
\Gamma^1_0 &:= \gamma_0(g_1, z_1 v)
\end{align*}$$ (2.18) - (2.23)

The first exceed model by Dshahalow and the operator is defined as follows:

$$\mathcal{D}_{(x,y)}[f(x,y)](u,v) := (1-u)(1-v)\sum_{x \geq 0} \sum_{y \geq 0} f(x,y) u^x v^y,$$ (2.24)

then

$$f(x,y) = \mathcal{D}_{(u,v)}[\mathcal{D}_{(x,y)} \{ f(x,y) \}]$$

where $\{ f(x,y) \}$ is a sequence, with the inverse

$$\mathcal{D}_{(u,v)}^{(m,n)}(\bullet) = \begin{cases} 
(\frac{1}{m!n!}) \lim_{(u,v) \to 0} \frac{\partial^m \partial^n f}{\partial u^m \partial v^n} (1-u)(1-v)(\bullet), & m \geq 0, n \geq 0 \\
0, & \text{otherwise}
\end{cases}$$ (2.25)

Theorem 1: the functional $\Phi_{\frac{\nu}{\mu}}$ of the process of (2.17) satisfies following expression:

$$\Phi_{[\frac{\nu}{\mu}]} = \mathcal{D}_{(u,v)}^{(\frac{\nu}{\mu},[\frac{\nu}{\mu}])} \left[ \Gamma^1_0 - \Gamma_0 + \frac{\xi \cdot \gamma_0}{1 - \xi \gamma} (\Gamma^1 - \Gamma) \right]$$ (2.26)
From (2.32), we can find the LST of $\tau_{\nu-1}$ (or $\tau_{\nu}$) and the generating function of $A_{\nu-1}$ (or $A_{\nu}$):

$$E[\xi^\nu] = \Phi[\xi^\nu](\xi, 1, 1, 1, 1).$$  \hspace{1cm} (2.27)

$$E[g_{0_{\nu-1}}^A] = \Phi[g_{0_{\nu-1}}^A](1, g_0, 1, 1, 1),$$  \hspace{1cm} (2.28)

$$E[g_{1_{\nu}}^A] = \Phi[g_{1_{\nu}}^A](1, 1, g_1, 1, 1),$$  \hspace{1cm} (2.29)

The decision parameters such as the first exceed observation index $\nu$ and the moment of making a decision $\tau_{\nu-1}$ could be found from (2.34)-(2.38):

$$E[\nu] = \left. \frac{\partial}{\partial \xi} \Phi[\xi^\nu](\xi, 1, 1, 1, 1) \right|_{\xi=1}$$  \hspace{1cm} (2.30)

$$E[\tau_{\nu-1}] = E[\tau_0] + E[\Delta_1](E[\nu] - 1)$$  \hspace{1cm} (2.31)

3. Blockchain Governance Mixed Game Strategy

3.1 Preliminaries

Let us consider a two-person mixed strategy game, and the player H (i.e., a defender) is the person who has two strategies at the observation moment, one step before attackers complete to generate alternative chains with dishonest transactions (i.e., double spending). Player H has the following strategies (1) DoNothing – doing nothing, which implicates that the blockchain networks are running as usual, and (2) Action – taking the preliminary action for avoiding attacks by adding honest nodes. In the view of player A (an attacker), he might succeed to catch the blocks or fail to catch (i.e., the blockchain network has been defended). So, the responses of player A would be either "Not burst" or "Burst." Let us assume that the cost for reserving the additional honest nodes is $c_\alpha$ where $\alpha$ is the portion to reserve the blocks for blockchain defense. The token provider might reserve the certain portion of nodes for protecting the values and the network. If the attacks succeed to generate alternative blocks, the network is bursted and the whole value of the tokens (or coins) $B$ will be lost and this value might be equivalent with the value by ICO (Initial Coin Offering). It still has the chance to be bursted even if the defender (or the provider) adds the honest nodes before catching blocks by an attacker. In this case, the cost will be not only the token value but also the reservation cost for additional honest nodes. The normal form of games is as follows:

- Players: $N = \{A, H\}$.
- Strategy sets:
  $$s_A = \{"NotBurst", "Burst"\},$$
  $$s_H = \{"DoNothing", "Action"\},$$

Based on the above conditions, the general cost matrix at the prior time to be burst $\tau_{\nu-1}$ could be composed as follows:
Table 1. Cost matrix

|                | NotBurst \((1 - q(s_H))\) | Burst \(q(s_H)\) |
|----------------|---------------------------|-----------------|
| **DoNothing**  | 0                         | \(B\)           |
| **Action**     | \(c_\alpha\)              | \(c_\alpha + B\)|

where \(q(s_H)\) is the probability of bursting blockchain network (i.e., an attacker wins the game) and it depends on the strategic decision of player H (a defender):

\[
q(s_H) = \begin{cases} 
\mathbb{E}\left[ \mathbf{1}\{A_H \geq \frac{M}{2}\} \right], & s_H = \{\text{DoNothing}\}, \\
\mathbb{E}\left[ \mathbf{1}\{A_H \geq \frac{M(1 + \alpha)}{2}\} \right], & s_H = \{\text{Action}\}.
\end{cases}
\tag{3.2}
\]

It is noted that the payoffs for the reserved nodes (i.e., "Action" strategy of player H) should be better than the other strategy. Otherwise, player H does not have to spend the cost of the governance. The portion of reserved nodes for protecting a blockchain network \(\alpha\) depends on the payoff function and the optimal portion for the blockchain governance \(\alpha^*\) could be found as follows:

\[
\alpha^* = \inf\{\alpha \geq 0 : \mathcal{C}_{\text{NoA}}(q^0) \geq \mathcal{C}_{\text{Act}}(\alpha)\},
\tag{3.3}
\]

where (at the moment \(\tau_{\nu-1}\)),

\[
\mathcal{C}_{\text{NoA}}(q^0) = B \cdot q^0,
\tag{3.4}
\]

\[
\mathcal{C}_{\text{Act}}(\alpha) = c_\alpha \left(1 - q^1_\alpha\right) + (c_\alpha + B) q^1_\alpha,
\tag{3.5}
\]

\[
q^0 = \mathbb{E}\left[ \mathbf{1}\{A_H \geq \frac{M}{2}\} \right], q^1_\alpha = \mathbb{E}\left[ \mathbf{1}\{A_H \geq \frac{M(1 + \alpha)}{2}\} \right].
\tag{3.6}
\]

### 3.2 Blockchain Governance Game

We would like to design the enhanced blockchain network governance that can take the action at the decision making moment \(\tau_{\nu-1}\). The governance in the blockchain is followed by the decision making parameter. It also means that we will not take any action until the time \(\tau_{\nu-1}\) and it still have the chance that all nodes are governed by an attacker if the attacker catches more than the half of nodes at \(\tau_{\nu-1}\) (i.e., \(\{A_{\nu-1} \geq \frac{M}{2}\}\)). If the attacker catches the less than half of all nodes at \(\tau_{\nu-1}\) (i.e., \(\{A_{\nu-1} < \frac{M}{2}\}\)), then the defender could take the action to avoid the attack at \(\tau_{\nu}\). The total cost for developing the enhanced blockchain network is as follows:

\[
\mathcal{C}(q^0, \alpha)_{\text{Total}} = \mathbb{E}\left[ \mathcal{C}_{\text{Act}}(\alpha) \cdot \mathbf{1}\{A_{\nu-1} \geq \frac{M}{2}\} + \mathcal{C}_{\text{NoA}}(q^0) \cdot \mathbf{1}\{A_{\nu-1} < \frac{M}{2}\} \right] \tag{3.7}
\]

\[
= (c_\alpha (1 - q^1_\alpha) + (c_\alpha + B) q^1_\alpha) p_{A_{\nu-1}} + B \cdot q^0 (1 - p_{A_{\nu-1}})
\]

where
Because \( \Phi(1, g_0, 1, 1, 1) \) from (2.17) is the probability generating function of \( A_{\nu-1} \), the probability mass could be found as follows:

\[
P\{A_{\nu-1} = k\} = \lim_{g_0 \to 0} \frac{1}{k!} \frac{\partial^k}{\partial g_0^k} \Phi(1, g_0, 1, 1, 1), \quad k = 0, \ldots, \left\lfloor \frac{M}{2} \right\rfloor
\]

(3.9)

### 3.3 Simulated Results in Practice

You may consider the private blockchain based services with offering the tokens. Even though the network is designed for controlling by the provider, the network should have at least enough power to avoid attacks not only from outsiders but also from insiders. The 51% attack still could be happened enough though the network designed based on the private blockchain. The way of manage the reliability of the network is supporting the additional nodes to give the less chance that an attacker catches the blocks with false transactions. The initial conditions of the network and the related costs could be given by gathering the data but the values in the paper (see Table 2) are artificially given only for demonstration purposes.

| Name   | Value                        | Description                                      |
|--------|------------------------------|--------------------------------------------------|
| \( M \) | 100,000 [User]               | Total number of the nodes in the network         |
| \( B \) | 50,000,000 [USD]             | (Target) total value of tokens (or coins) offered by ICO |
| \( c_{\alpha} \) | \( 3\alpha \cdot M [USD] \) | Cost for reserving additional nodes to avoid attacks |
| \( E[A_0] \) | 100 [Blocks]                | Total number of blocks that changed by an attacker at \( \tau_0(=0) \) |
| \( E[H_0] \) | 150 [Blocks]                | Total number of blocks that changed by an honest node at \( \tau_0(=0) \) |

Table 2. Initial conditions for the cost function

Since, the model has been analytically analyzed, the values for the cost function and the probability distributions could be calculated straight forward (see Table 3) but, again, the values are artificially given.

| Name   | Value | Equations | Description                                      |
|--------|-------|-----------|--------------------------------------------------|
| \( q^0 \) | 0.019 | (2.28), (3.6) | Probability that an attacker catches the blocks more than half |
| \( q^1_{\alpha} \) | \( \frac{3\alpha}{1+\alpha} \) | (3.6) | Probability that an attacker catches after adding reserved nodes |
| \( \alpha \) | – | (3.7) | The portion of additional nodes for blockchain protection |
| \( \alpha^* \) | – | – | The condition of the reserved nodes for minimizing the cost |
| \( p_{A_{\nu-1}} \) | 0.8 | (2.28), (3.8) | The probability that an honest node catches the blocks at \( \tau_{\nu-1} \) |
| \( \mathcal{C}(\alpha)_{Total} \) | – | (3.7) | The total cost function for enhanced blockchain network |

Table 3. Calculated values from the equations

The above condition is directly applied to the optimization model and described by the following mathematical programming style:

\[
\text{Objective (3.7)} \\
\min U = \mathcal{C}(\alpha)_{Total}
\]

(3.10)
Subject to (3.3)

\[ \alpha \geq \frac{c_n}{B q^b - c_a} \]  

(3.11)

and Table 2 and 3 are mapping the values for the optimization practice. We take the parameters from the above tables and calculate the total cost \( C(\alpha)_{\text{Total}} \) and \( \alpha \) that gives the minimal for \( C(\alpha)_{\text{Total}} \). As it mentioned, \( \alpha \) is the portion that a defender reserves nodes to protect the network from an attackers. As an illustration (see Figure 1), the calculation using MS-Excel yields, that result in making the minimum cost 7,129,333 [USD] when the portion of 13.4%. It means that the service provider should keep 13,400 nodes additionally for managing the risk from attackers.

![Block Chain Optimization](image)

**Figure 1.** Optimization for Blockchain Network Security

The moment of releasing the additional nodes will be the time \( t_{\nu-1} \) (2.31) when is one step prior than the time that an attacker catches more than half of the whole blocks (i.e., \( t_{\nu} \)).

### 4. Conclusion

The objective of this paper is establishing the theoretical framework of the blockchain governance game with the explicit equations for developing the blockchain network security for avoid the attacks for decentralized networks. As it said on the title, the paper is the condensed summary for only introducing the concept of blockchain governance game for the secured decentralized network security. The core parts of the research including the proof of the Theorem 1, the actual calculation of the probabilities for the decision making parameters and the demonstration based on the analysis are not included in this trailer but these will be fully deployed in the final paper. The blockchain governance game could be designed by gathering all related data from real networks without calculating mathematical functions. This research (even this trailer) will be helpful for whom considers the initial coin offering (ICO) or launching new blockchain based services with the enhanced security features.
REFERENCES

Armknecht, F., Karame, G. and et. al. (2015), Ripple: Overview and Outlook, Lecture Notes in Computer Science 9229, Springer, Berlin, Germany, pp. 163-180.

Andrychowicz, M., Dziembowski, S. and et. al. (2015), On the Malleability of Bitcoin Transactions, Lecture Notes in Computer Science 8976, pp. 1-18.

Antonopoulos, A. M. (2017), Mastering Bitcoin: Programming the Open Blockchain, 2nd Ed., O'Reilly, Sebastopol, CA.

Beikverdi, A. and Song, J. (2015), Trend of centralization in Bitcoin’s distributed network, Proceedings of The 16th IEEE/ACIS International Conference, pp. 1-6.

Decker, C. and Wattenhofer, R. (2013). Information propagation in the Bitcoin network, IEEE P2P 2013 Proceedings, pp. 1-10

Dshalalow, J. H. (1995), "First excess level process", Advances in Queueing, CRC Press, Boca Raton, FL, pp 244-261.

Dshalalow, J. H. and Ke, H.-J. (2009), "Layers of noncooperative games", Nonlinear Analysis 71, pp.283-291.

Eyal, I., Gencer, A. E. and et. al. (2016), Bitcoin-NG: A Scalable Blockchain Protocol, The 13th USENIX Symposium on Networked Systems Design and Implementation, March 16-18, CA, pp. 45-59

Eyal, I. and Sirer, E. (2014), Majority Is Not Enough: Bitcoin Mining Is Vulnerable. Lecture Notes in Computer Science 8437, Springer, Berlin, Germany, pp. 436-454.

Garay, J., Kiayias. A. and Leonardos. N. (2015), The Bitcoin Backbone Protocol: Analysis and Applications, Lecture Notes in Computer Science 9057, Springer, Berlin, Germany, pp. 281-310.

Kim, W. (2018), Bitcoin, Blockchain Mechanism and Its Evolution (Korean), retrieved from http://www.itf2nd.or.kr/publication/regular/weeklytrend/weekly/list.do?selectedId=1032

Kim, Y. (2018), Blockchain: Ideal and Reality, retrieved from https://www.blockchainhub.kr/bbs/board.php?bo_table=lecture&wr_id=1879

Luu L, Teutsch J, Kulkarni R, Saxena P. Demystifying Incentives in the Consensus Computer. In: Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security. CCS’15. New York, NY, USA: ACM; 2015. p. 706-719.

Nakamoto, S. (2009), Bitcoin: A Peer-to-Peer Electronic Cash System, retrieved from http://www.bitcoin.org

Weiss, M. and Corsi, E. (2018), Bitfury: Blockchain for Government, HBP Case 9-818-031, 29 pages.

Yli-Huumo, J., Ko, D. and et. al. (2016), Where Is Current Research on Blockchain Technology?-A Systematic Review, PLoS ONE 11:10, 27 pages.