axioms

MDPI

Article

Multi-Layered Blockchain Governance Game

Song-Kyoo (Amang) Kim

School of Applied Sciences, Macao Polytechnic Institute, R. de Luis Gonzaga Gomes, Macao; amang@ipm.edu.mo; Tel.: +853-8599-6455

Abstract: The research designs a new integrated system for the security enhancement of a decentralized network by preventing damages from attackers, particularly for the 51 percent attack. The concept of multiple layered design based on Blockchain Governance Games frameworks could handle multiple number of networks analytically. The Multi-Layered Blockchain Governance Game is an innovative analytical model to find the best strategies for executing a safety operation to protect whole multiple layered network systems from attackers. This research fully analyzes a complex network with the compact mathematical forms and theoretically tractable results for predicting the moment of a safety operation execution are fully obtained. Additionally, simulation results are demonstrated to obtain the optimal values of configuring parameters of a blockchain-based security network. The Matlab codes for the simulations are publicly available to help those whom are constructing an enhanced decentralized security network architecture through this proposed integrated theoretical framework.

Keywords: blockchain governance game; mixed game; stochastic model; fluctuation theory; network security; 51 percent attack; IoT; network architecture

check for updates

Citation: Kim, S.-K. Multi-Layered Blockchain Governance Game. *Axioms* **2022**, *11*, 27. https://doi.org/10.3390/axioms11010027

Academic Editors: Ana Meca and Carlos Gutierrez-Hita

Received: 11 November 2021
Accepted: 6 January 2022
Published: 9 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

The blockchain is a hashed digital ledger by accomplishing authenticity of all nodes in a typical peer-to-peer decentralized network which could remove various security threats caused by a centralized network [1–3]. The basic blockchain data structure could evaluate data transactions in each chain which grows in an append-only permission on the top of latest verified blocks [1,4]. This mechanism is secure because a single node cannot govern more than half of the computational power in the network [5–8]. Through the distributed consensus of networks nodes, the blockchain network security is enhanced. If an attacker invests more than 50 percent of the computational power (i.e., governs more than half of the total nodes), he could conquer a whole blockchain network. To avoid majority matters, Verifiable Random Functions (VRFs) are adapted into blockchain-based security applications to remove heavy computation power for mining [9,10]. The VRF is capable to select a miner randomly, and each node has the same chance to be a miner [9]. This technique has been adapted for selecting a miner to map inputs to verifiable pseudorandom outputs [10].

Blockchain technologies have been widely adapted into cyber-security matters including the Internet of Things [11,12], the Internet of Vehicles [13–19] and Edge-Fog computing [20–22] because blockchain-based network architectures (i.e., decentralized networks) are secured to avoid practically any attacks which are dedicated on conventional network architectures (i.e., centralized networks). These attacks on centralized networks include DoS (Denial-of-Service), phishing, spoofing and server hacking attacks. Therefore, the securities based on the blockchain protocol level have been widely studied [2,4,23], but these studies are limited because the configuring parameters for security protocols are arbitrarily chosen. Hence, the Blockchain Governance Game (BGG) and the Strategic Alliance for Blockchain Governance Game (SABGG) are alternatively designed to break through the limitations by constructing a new network architecture. On the other hand, game theoretic approaches

for improving securities have also been widely applied into various telecommunication networks [24,25], communication protocols [26] and trustworthy data [27,28]. It is even applied into designing blockchain-based services and securities [29]. The stochastic game executes stochastic transitions among the states of the game, and players in a stochastic game could change their strategies based on the past actions and randomness of behaviors of the other players. Several kinds of stochastic games have been adapted to avoid the 51 percent attack, and a stochastic game has been used for analyzing the selection between honest mining and making the decision of the proper time for adding and releasing mined blocks [2]. The BGG and the SABGG are the mixed model of the fluctuation and the mixed strategy game for analyzing a single layered network to provide the decision making moment for taking preliminary security actions before attacks [30,31]. The SABGG is a variant of BGG, which is designed for strategically allying nodes instead of keeping hidden nodes [31]. These BGG frameworks find optimal decision-making parameters and the strategic choices of a defender are either taking a preliminary action (i.e., a safety mode) or doing nothing. Taking a preliminary action for security operations shall not be optimal until the game reaches one step prior to pass the Nash equilibrium [29]. Once corrupted blocks are generated, all models independently predict the number of blocks to be generated and the moment until more than half of the total nodes are corrupted by an attacker. The techniques deliver the results under a composition of the $\mathcal{D}$–operator and its inverse $\mathfrak{D}$–operator, which have been introduced in the BGG models [30,31]. In this paper, the extended blockchain governance game framework is newly designed for improving complex decentralized network securities. The *Multi-Layered Blockchain Governance Game* (MLBGG) is a combined stochastic game model based on the BGG frameworks. The main contributions of this research are the following:

- Mathematically analyzing a complex network management;
- An analytical solution that can support optimal values of configuring parameters for network securities;
- A complicated decentralized network can be securely designed and managed by using this innovative theoretical framework.

The layer 1 is a set of multiple BGG-based networks, and the other layer (i.e., layer 0) is single SABGG-based network (see Figure 1). This multiple layer framework makes the BGG more flexible to applying various hierarchical system architectures, including Edge-Fog computing [20,21], hierarchical network systems [18,22] and IoT-Server networks (see Section 3).

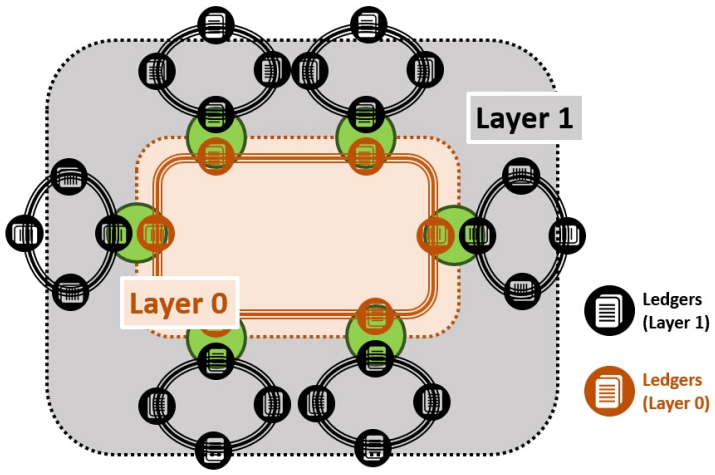

Figure 1. Multi-Layered Blockchain Governance Game structure.

The paper is organized as follows: Stochastic models of MLBGG architecture with some key analytical techniques are introduced in Section 2. This section also explains how the multi-layered model is connected with the BGG for layer 1 and the SABGG for layer 0. The modeled processes of the accumulated corrupted blocks of each node mathematically predict both the time and size of the nodes and which are governed by attackers. In Section 3, the MLBGG framework is applied into a practical IoT (Internet of Things) network architecture. This section shows how the MLBGG could be adapted into an IoT-Server combined network system. This is a typical way to construct a blockchain-based network architecture by adapting the MLBGG. Various simulations for the MLBGG determine configuring parameters in Section 4. Although theoretical approaches without simulated results still helps computer programming, these simulation are practically optimizing configuring parameters of an IoT-Server combined network system.

2. Multi-Layered Blockchain Governance Game

A multi-layered blockchain governance game (MLBGG) combines a set of multiple BGG networks and single SABGG network which are hierarchically connected. Each system in layer 1 is exactly mapped with the BGG, and layer 0 is mapped with the SABGG (see Figure 2).

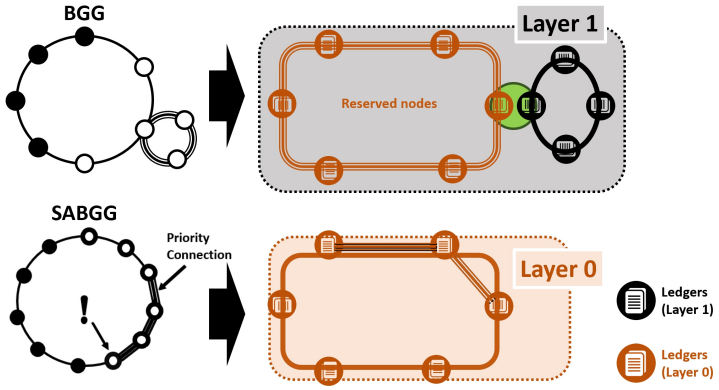

Figure 2. BGG and SABGG mapping into MLBGG.

2.1. Layer 1: BGG Stochastic Modelling

Layer 1 is a set of $\eta + 1$ BGG networks, and the l-th BGG network has M_l nodes with B^0 ($\leq \eta$) reserved nodes for executing a safety operation. In layer 1 (i.e., the second layer), each BGG network between an attacker and a defender are described the antagonistic game. Two players (A: an attacker, H: a defender) in the l-th BGG network in layer 1 compete to build the blocks either for honest or false ones. It is noted that one particular BGG network in layer 1 (i.e., l-th network) is firstly analyzed and combining whole BGG networks as a single set will be covered later in this section.

Let $(\Omega, \mathcal{F}(\Omega), P)$ be probability space $\mathcal{F}_{A^l}, \mathcal{F}_{H^l}, \mathcal{F}_\tau \subseteq \mathcal{F}(\Omega)$ and layer 1 be independent σ-subalgebras in the l-th network ($l = 0, 1 \ldots, \eta$). Let us consider $\mathcal{F}_{A^l}$-measurable and $\mathcal{F}_{H^l}$-measurable marked Poisson processes as follows:

$$\mathcal{A}^l := \sum_{k \geq 0} X_k^l \varepsilon_{s_k^l}, s_0^l (= 0) < s_1^l < s_2^l < \cdots, \tag{1}$$

$$\mathcal{H}^l := \sum_{j \geq 0} Y_j^l \varepsilon_{t_j^l}, t_0^l (= 0) < t_1^l < t_2^l < \cdots, \tag{2}$$

where $l = 0, 1, \ldots, \eta$ with respective intensities λ_A^l and λ_H^l of l-th network in layer 1 and ε_a is a point mass at a. These two values are related with block generating performances of an

attacker and a defender [30]. In the l-th BGG network in layer 1, the processes $\mathcal{A}^l$ and $\mathcal{H}^l$ are specified by their transforms:

$$\mathbb{E}\left[g^{\mathcal{A}^l(s)}\right] = e^{\lambda_A^l(s)(g-1)}, l = \{0, 1, \ldots, \eta\}, \tag{3}$$

$$\mathbb{E}\left[z^{\mathcal{H}^l(t)}\right] = e^{\lambda_H^l(t)(z-1)}, l = \{0, 1, \ldots, \eta\}, \tag{4}$$

where η is the total number of allied nodes in layer 0, and the observation process for all systems in layer 1 is:

$$\mathcal{T} := \sum_{i \geq 0} \varepsilon_{\tau_i},\ \tau_0(>0), \tau_1, \ldots, \tag{5}$$

which is assumed to be delayed renewal process. If

$$\left(A^l(t), H^l(t)\right) :=\ \mathcal{A}^l \otimes \mathcal{H}^l\left(\left[0, \tau_k^l\right]\right), k = 0, 1, \ldots, \tag{6}$$

forms an observation process upon $\mathcal{A}^l \otimes \mathcal{H}^l$ embedded over $\mathcal{T}$, with respective increments

$$\left(X_k^l, Y_k^l\right) := \mathcal{A}^l \otimes \mathcal{H}^l([\tau_{k-1}, \tau_k]), k = 1, 2, \ldots, \tag{7}$$

and

$$X_0^l = A_0^l,\ Y_0^l = H_0^l, l = \{0, 1, \ldots, \eta\}. \tag{8}$$

The observation process of the l-th BGG network could be formalized as

$$\mathcal{A}_\tau^l \otimes \mathcal{H}_\tau^l := \sum_{k \geq 0} \left(X_k^l, Y_k^l\right)\varepsilon_{\tau_k}, l = \{0, \ldots \eta\}, \tag{9}$$

with position-dependent marking in the l-th blockchain network and with X_k^l and Y_k^l could be defined with the notation

$$\Delta_k := \tau_k - \tau_{k-1}, k = 0, 1, \ldots, \tau_{-1} = 0, \tag{10}$$

and

$$\gamma^l(g, z) = \mathbb{E}\left[g^{X_k^l} \cdot z^{Y_k^l}\right],\ \|g\| \leq 1, \|z\| \leq 1. \tag{11}$$

Due to the double expectation,

$$\gamma^l(g, z) = \delta\left(\lambda_a^l(1-g) + \lambda_h^l(1-z)\right), l = \{0, 1, \ldots, \eta\}, \tag{12}$$

and

$$\gamma_0^l(g, z) = \delta_0\left(\lambda_a^l(1-g) + \lambda_h^l(1-z)\right), \tag{13}$$

where

$$\delta(\theta) = \mathbb{E}\left[e^{-\theta\Delta_1}\right],\ \delta_0(\theta) = \mathbb{E}\left[e^{-\theta\tau_0}\right] \tag{14}$$

are the marginal transform of increments $\Delta_1, \Delta_2, \ldots$. In the l-th system, the stochastic process $\mathcal{A}_\tau^l \otimes \mathcal{H}_\tau^l$ analyzes a conflict between players with an observation process for the l-th system in the layer 1. This game is over when the collateral building blocks by either one of player exceeds the threshold ($>\frac{M_l}{2}$) on the k-th observation epoch τ_k. The exit indices for each network are:

$$\nu^l := inf\left\{k : A_k^l = A_0^l + X_1^l + \cdots + X_k^l \geq \left(\frac{M_l}{2}\right)\right\}, \tag{15}$$

$$\mu^l := inf\left\{j : H_j^l = H_0^l + Y_1^l + \cdots + Y_j^l \geq \left(\frac{M_l}{2}\right)\right\}, \tag{16}$$

where $l = \{0, 1, \ldots, \eta\}$, and η is the number of backup nodes, which are equivalent with the number of nodes in layer 0. Player A (an attacker) wins at time τ_{ν^l}; otherwise, player H (a defender) generates the correct blocks. At this moment, the confined game in the view point of player A^l for each BGG network in layer 1 is targeted. The Formula (6) will be modified as:

$$\overline{\mathcal{A}_\tau^l} \otimes \overline{\mathcal{H}_\tau^l} := \sum_{k\geq 0}^{\nu^l} \left(X_k^l, Y_k^l\right) \varepsilon_{\tau_k} \tag{17}$$

which is the path of the game from $\mathcal{F}(\Omega) \cap \left\{\nu^l < \mu^l\right\}$, which gives an exact definition of the model observed until τ_{ν^l}. The joint functional of the l-th BGG model in layer 1 is as follows:

$$\begin{aligned} \Phi^l_{\left\lceil \frac{M_l}{2} \right\rceil} &= \Phi^l_{\left\lceil \frac{M_l}{2} \right\rceil}(\xi, g_0, g_1, z_0, z_1) \\ &= \mathbb{E}\left[\xi^{\nu^l} \cdot g_0^{A^l_{\nu^l-1}} \cdot g_1^{A^l_{\nu^l}} \cdot z_0^{H^l_{\nu^l-1}} \cdot z_1^{H^l_{\nu^l}} \mathbf{1}_{\left\{\nu^l < \mu^l\right\}}\right], l = \{0, \ldots, \eta\}. \end{aligned} \tag{18}$$

This functional represents the status of an attacker and honest nodes upon the exit time τ_ν^l, $l = \{0, 1, \ldots, \eta\}$. For the BGG-1 theorem [30], the operators for the first exceed model [32,33] are defined as follows:

$$\mathcal{D}_{(x,y)}\left[f(x,y)\right](u,v) := (1-u)(1-v) \sum_{x\geq 0} \sum_{y\geq 0} f(x,y) u^x v^y, ||u|| < 1, ||v|| < 1, \tag{19}$$

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

$$\mathfrak{D}^{(m,n)}_{(u,v)}(\bullet) = \left(\frac{1}{m! \cdot n!}\right) \lim_{(u,v)\to 0} \frac{\partial^m \partial^n}{\partial u^m \partial v^n} \frac{1}{(1-u)(1-v)}(\bullet), m \geq 0, n \geq 0. \tag{20}$$

Additionally, the new operators for dealing with the matrix calculations are introduced. Let us consider the matrix of a function set $\boldsymbol{f}_{(x,y)}$ as follows:

$$\boldsymbol{f}_{(x,y)} = \begin{bmatrix} f_0(x,y) \\ f_1(x,y) \\ \vdots \\ \vdots \\ f_n(x,y) \end{bmatrix} \tag{21}$$

and the matrix operations for $\mathcal{D}_{(x,y)}\{\bullet\}$ and $\mathfrak{D}^{(m,n)}_{(u,v)}\{\bullet\}$ are defined as follows:

$$\mathbb{D} \odot \boldsymbol{f}_{(x,y)} := \mathcal{D}_{(x,y)}\{\boldsymbol{f}\} = \begin{bmatrix} (1-u)(1-v)\sum\sum f_0(x,y)u^x v^y \\ (1-u)(1-v)\sum\sum f_1(x,y)u^x v^y \\ \vdots \\ (1-u)(1-v)\sum\sum f_l(x,y)u^x v^y \\ \vdots \\ (1-u)(1-v)\sum\sum f_n(x,y)u^x v^y \end{bmatrix} \tag{22}$$

and

$$\mathbb{D}_{\boldsymbol{M_r}}^{-\mathbf{1}} \odot \boldsymbol{G}_{(u,v)} := \begin{bmatrix} \mathfrak{D}_{(u,v)}^{(m_0,n_0)}\{G_0(u,v)\} \\ \mathfrak{D}_{(u,v)}^{(m_1,n_0)}\{G_1(u,v)\} \\ \vdots \\ \mathfrak{D}_{(u,v)}^{(m_l,n_l)}\{G_l(u,v)\} \\ \vdots \\ \mathfrak{D}_{(u,v)}^{(m_n,n_n)}\{G_r(u,v)\} \end{bmatrix}, \tag{23}$$

where

$$\boldsymbol{M_r} = \begin{bmatrix} m_0 & n_0 \\ m_1 & n_1 \\ \vdots & \vdots \\ \vdots & \vdots \\ m_r & n_r \end{bmatrix} \tag{24}$$

From the BGG-1 Theorem [30], we can set up the matrix of the functional and the functional matrix for all blockchain networks in layer 1 as follows:

$$\boldsymbol{\Phi}_{\boldsymbol{M_\eta}}^{\mathbf{1}} = \mathbb{D}_{\boldsymbol{M_\eta}}^{-\mathbf{1}} \odot \boldsymbol{G}_{(u,v)}, \tag{25}$$

where

$$\boldsymbol{G}_{(u,v)} = \begin{bmatrix} G_0(u,v) \\ \vdots \\ G_l(u,v) \\ \vdots \\ G_\eta(u,v) \end{bmatrix}, \boldsymbol{M_\eta} = \left\{ \begin{matrix} \left\lceil \frac{M_0}{2} \right\rceil & \left\lceil \frac{M_0}{2} \right\rceil \\ \vdots & \vdots \\ \left\lceil \frac{M_l}{2} \right\rceil & \left\lceil \frac{M_l}{2} \right\rceil \\ \vdots & \vdots \\ \left\lceil \frac{M_\eta}{2} \right\rceil & \left\lceil \frac{M_\eta}{2} \right\rceil \end{matrix} \right\}, \tag{26}$$

and $\boldsymbol{M_\eta}$ indicates the vector form of all blockchain networks in layer 1. From (18):

$$\Phi_{\left\lceil \frac{M_l}{2} \right\rceil}^{l} = \mathfrak{D}_{(u,v)}^{\left(\left\lceil \frac{M_l}{2} \right\rceil, \left\lceil \frac{M_l}{2} \right\rceil\right)}[G_l(u,v)],\ l = \{0,\ldots,\eta\}, \tag{27}$$

where

$$G_l(u,v) = \left[\Gamma_0^1 - \Gamma_0 + \frac{\xi \cdot \gamma_0}{1 - \xi\gamma} \left(\Gamma^1 - \Gamma \right) \right],$$

and

$$\begin{aligned} \gamma &:= \gamma^l(g_0 g_1 u, z_0 z_1 v), && (28)\\ \gamma_0 &:= \gamma_0^l(g_0 g_1 u, z_0 z_1 v), && (29)\\ \Gamma &:= \gamma^l(g_1 u, z_1 v), && (30)\\ \Gamma_0 &:= \gamma_0^l(g_1 u, z_1 v), && (31)\\ \Gamma^1 &:= \gamma^l(g_1, z_1 v), && (32)\\ \Gamma_0^1 &:= \gamma_0^l(g_1, z_1 v). && (33) \end{aligned}$$

From (18) and (27), the probability generating functions (PGFs) for $A_{\nu^l-1}^l$ (and also $A_{\nu^l}^l$) and the exit index ν^l of the l-th BGG network in the layer 1 are determined as follows:

$$\mathbb{E}\left[\xi^{\nu^l}\right] = \Phi_{\left\lceil \frac{M_l}{2} \right\rceil}^{l}(\xi, 1, 1, 1, 1), \tag{34}$$

$$\mathbb{E}\left[g_0^{A_{\nu^l-1}^l}\right] = \Phi^l_{\lceil \frac{M_l}{2} \rceil}(1, g_0, 1, 1, 1), \tag{35}$$

$$\mathbb{E}\left[g_1^{A_{\nu^l}^l}\right] = \Phi^l_{\lceil \frac{M_l}{2} \rceil}(1, 1, g_1, 1, 1), l = \{0, \ldots, \eta\}. \tag{36}$$

From (5), (10) and (34), the moments of making a decision $\tau_{\nu-1}$ are:

$$\mathbb{E}\left[\nu^l\right] = \frac{\partial}{\partial \xi} \Phi^l_{\lceil \frac{M}{2} \rceil}(\xi, 1, 1, 1, 1)\Big|_{\xi=1}, \tag{37}$$

$$\mathbb{E}\left[\tau_{\nu^l-1}\right] = \mathbb{E}[\tau_0] + \mathbb{E}[\Delta_1]\left(\mathbb{E}\left[\nu^l\right] - 1\right), l = \{1, \ldots, \eta\}. \tag{38}$$

In a conventional BGG [30], the probability of bursting the l-th blockchain network $q^l(s_H)$ is determined as follows:

$$q^l(s_H) = \begin{cases} \mathbb{E}\left[\mathbf{1}_{\left\{A_\nu^l \geq \frac{M}{2}\right\}}\right], & s_H = \{\text{DoNothing}\}, \\ \mathbb{E}\left[\mathbf{1}_{\left\{A_\nu^l \geq \left(\frac{M}{2} + B^1\right)\right\}}\right], & s_H = \{\text{Action}\} \end{cases} \tag{39}$$

where $B^1 (\leq \eta)$ is the number of backup nodes, which are hooked as in layer 0 (see Figure 2), and the reserved nodes depend on the availability of other blockchain networks in the same layer. When the reserved nodes are realized during a safety mode, the bursting probability of the l-th blockchain network in the layer 1 is revised as follows:

$$\mathbb{E}\left[\mathbf{1}_{\left\{A_\nu^l \geq \left(\frac{M_l}{2} + B^1\right)\right\}}\right] = \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}_{\left\{A_\nu \geq \left(\frac{M_l}{2} + B^1\right)\right\}} \middle| B^1\right]\right] \tag{40}$$

where

$$P\left\{B_\eta^1 = j\right\} = \binom{\eta}{j}\left(\rho^{\mathbf{1}}\right)^j\left(1 - \rho^{\mathbf{1}}\right)^{\eta - j}, \tag{41}$$

$$\rho^{\mathbf{1}} = \left(\frac{1}{\eta + 1}\right)\mathbb{E}\left[\sum_{k=0}^{\eta} \mathbf{1}_{\left\{H_\nu^k \geq \frac{M_k}{2}\right\}}\right]. \tag{42}$$

2.2. Layer 0: SABGG Stochastic Modelling

The SABGG network with $\eta + 1$ nodes are considered in the layer 0 (i.e., the first layer) and two persons (called "Corrupted" and "Genuine") play a game by governing blocks which are either genuine or corrupted ledgers. For layer 0, let us assume:

$$\mathcal{C} := \sum_{j \geq 0} J_j \varepsilon_{u_j}, u_0 (= 0) < u_1 < u_2 < \cdots, \tag{43}$$

$$\mathcal{G} := \sum_{k \geq 0} K_k \varepsilon_{v_k}, v_0 (= 0) < v_1 < v_2 < \cdots, \tag{44}$$

are also marked Poisson processes (i.e., $\mathcal{F}c$ and $\mathcal{F}_g$ measures) and position-independent marking with respective intensities λ_c and λ_g. Similar to (5), a third-party observation point process is determined as follows:

$$\mathcal{U} := \sum_{i \geq 0} \varepsilon_{t_i}, t_0 (> 0)), t_1, \ldots. \tag{45}$$

Similarly, player C (corrupted; a layer 0 attacker) builds the blocks which contain false transactions at the times $u_1, u_2, \ldots$. In the other hand, player G (genuine; a layer 0 defender) generates the blocks which contain the correct transactions. The transforms of the processes $\mathcal{C}$ and $\mathcal{G}$ are:

$$\mathbb{E}\left[y^{\mathcal{C}(u)}\right] = e^{\lambda_c(u)(y-1)}, \mathbb{E}\left[z^{\mathcal{G}(v)}\right] = e^{\lambda_g(v)(z-1)}. \tag{46}$$

Unlike layer 1, layer 0 has one single SABGG network. The observation process upon $\mathcal{C} \otimes \mathcal{G}$ with respective increments:

$$(J_i, K_i) := \mathcal{C} \otimes \mathcal{G}([t_{i-1}, t_i]), i = 1, 2, \ldots, \tag{47}$$

and

$$J_0 = C_0, K_0 = G_0. \tag{48}$$

The observation process of layer 0 is formalized as:

$$\mathcal{C}_t \otimes \mathcal{G}_t := \sum_{i \geq 0} (J_i, K_i)\varepsilon_{t_i}, \tag{49}$$

where

$$\mathcal{C}_t = \sum_{i \geq 0} J_i \varepsilon_{t_i}, \ \mathcal{G}_t = \sum_{i \geq 0} K_i \varepsilon_{t_i}, \tag{50}$$

with position-dependent marking. We can find the functional

$$\alpha(y, z) = \mathbb{E}\left[y^{J_i} \cdot z^{K_i}\right], \|y\| \leq 1, \|z\| \leq 1 \tag{51}$$

with the notation

$$U_i := t_i - t_{i-1}, i = \{0, 1, \ldots\}, t_{-1} = 0. \tag{52}$$

Similarly, from the previous section, we have:

$$\alpha(y, z) = \alpha\big(\lambda_c(1 - y) + \lambda_g(1 - z)\big), \tag{53}$$

$$\alpha_0(y, z) = \alpha_0\big(\lambda_c(1 - y) + \lambda_g(1 - z)\big), \tag{54}$$

where

$$\alpha(\theta) = \mathbb{E}\left[e^{-\theta U_1}\right], \ \alpha_0(\theta) = \mathbb{E}\left[e^{-\theta t_0}\right]. \tag{55}$$

The exit indices are formalized as follows:

$$\nu := inf\left\{j : C_j \, (= C_0 + J_1 + \cdots + J_j) \geq \left(\frac{\eta}{2}\right)\right\}, \tag{56}$$

$$\nu_2 := inf\left\{j : C_j \, (= C_0 + J_1 + \cdots + J_j) - B^0 \geq \left(\frac{\eta}{2}\right)\right\}, \tag{57}$$

$$\mu := inf\left\{l : G_l (= G_0 + K_1 + \cdots + K_l) \geq \left(\frac{\eta}{2}\right)\right\}, \tag{58}$$

where B^0 ($\leq \eta$) is the number of available nodes by the strategic alliance. The game in the layer 0 is over at $\min\{\nu, \nu_2, \mu\}$. The first passage time t_ν is the associated exit time from the confined game, and Formula (49) is modified as:

$$\overline{\mathcal{C}_t} \otimes \overline{\mathcal{G}_t} := \sum_{n \geq 0}^{\nu} (J_n, K_n)\varepsilon_{t_n}, \tag{59}$$

which gives an exact definition of the model observed until t_ν without the strategic alliance action. The explicit formula of the SABGG [31] is as follows:

$$\begin{aligned} \Theta_{\frac{\eta}{2}} &= \Theta_{\{\nu, \nu_2, \mu\}}(\zeta, y_0, y_1, b, z_0, z_1) \\ &= \mathbb{E}\left[\zeta^\nu \cdot y_0^{C_{\nu-1}} \cdot y_1^{C_\nu} \cdot b^{C_\nu - B_\eta} \cdot z_0^{G_{\mu-1}} \cdot z_1^{G_\mu} \mathbf{1}_{\{\nu < \nu_2 < \mu\}}\right], \end{aligned} \tag{60}$$

and the extended first exceed theory [32,33] has been applied, and the operator $\mathcal{D}^{(q,r,s)}_{(a,b,c)}$ is defined as:

$$\mathcal{D}_{(a,b,c)}^{(q,r,s)}\left[g(a,b,c)\right] := (1-q)(1-r)(1-s)\cdot\left\{\sum_{a\geq 0}\sum_{b\geq 0}\sum_{c\geq 0} g(a,b,c)q^a r^b s^c\right\}, \tag{61}$$

and $||q|| < 1$, $||r|| < 1$, $||s|| < 1$. Then, we have:

$$g(a,b,c) = \mathfrak{D}_{(q,r,s)}^{(a,b,c)}\left[\mathcal{D}_{(a,b,c)}\left\{g(a,b,c)\right\}(q,r,s)\right], \tag{62}$$

where $\{g(a,b,c)\}$ is a sequence, with the inverse:

$$\mathfrak{D}_{(q,r,s)}^{(a,b,c)}(\bullet) = \left(\frac{1}{a!\cdot b!\cdot c!}\right)\lim_{(q,r,s)\to 0}\left\{\frac{\partial^a\partial^b\partial^c}{\partial q^a\partial r^b\partial s^c}\frac{1}{(1-q)(1-r)(1-s)}(\bullet)\right\}. \tag{63}$$

From the BGG-2 Theorem [31]:

$$\Theta_{\lceil\frac{N}{2}\rceil} = \mathfrak{D}_{(q,r,s)}^{(\lceil\frac{\eta}{2}\rceil,\lceil\frac{\eta}{2}\rceil,\lceil\frac{\eta}{2}\rceil)}\left\{\sigma_\eta\cdot\beta\left(\frac{1-\beta^1}{1-\beta}\right)\cdot\left(\alpha_0^1-\alpha_0+\frac{\zeta\Phi_0}{1-\zeta\Phi}\left(\alpha^1-\alpha\right)\right)\right\}, \tag{64}$$

where

$$\begin{aligned}
\Phi &:= \alpha(y_0y_1bqr, z_0z_1s), && (65)\\
\Phi_0 &:= \alpha_0(y_0y_1bqr, z_0z_1s), && (66)\\
\alpha &:= \alpha(y_1bq, z_1), && (67)\\
\alpha_0 &:= \alpha_0(y_1bq, z_1), && (68)\\
\alpha^1 &:= \alpha(y_1b, z_1), && (69)\\
\alpha_0^1 &:= \alpha_0(y_1b, z_1), && (70)\\
\beta &:= \alpha(br, s), && (71)\\
\beta^1 &:= \alpha(r, 1), && (72)\\
\sigma_\eta &:= \mathbb{E}\left[b^{-B_\eta}\right]. && (73)
\end{aligned}$$

The moment of making a decision $t_{\nu-1}$ could be found as follows:

$$\mathbb{E}[\nu] = \frac{\partial}{\partial\zeta}\Theta_{\lceil\frac{\eta}{2}\rceil}(\zeta,1,1,1,1,1)\Big|_{\zeta=1}, \tag{74}$$

$$\mathbb{E}[t_{\nu-1}] = \mathbb{E}[t_0] + \mathbb{E}[U_1](\mathbb{E}[\nu]-1). \tag{75}$$

In layer 0, the probability of bursting the blockchain network $q^0(s_H)$ is determined as follows:

$$q^0(s_g) = \begin{cases}\mathbb{E}\left[\mathbf{1}_{\left\{C_\nu\geq\frac{\eta}{2}\right\}}\right], & s_g = \{\text{DoNothing}\},\\ \mathbb{E}\left[\mathbf{1}_{\left\{C_\nu\geq\frac{\eta(1+\alpha)}{2}\right\}}\right], & s_g = \{\text{Action}\}.\end{cases} \tag{76}$$

where α is an overhead portion for protecting the layer 0 (i.e., $B^0 = \left(\frac{\eta}{2}\right)\cdot\alpha$). The probability of bursting a SABGG network by an attacker is as follows:

$$q(s_g) = \begin{cases}\sum_{k>\frac{\eta}{2}}\mathbb{E}\left[\mathbf{1}_{\{C_\nu=k\}}\right], & s_g = \{\text{DoNothing}\},\\ \mathbb{E}\left[\sum_{k>\frac{\eta}{2}+B^0}\mathbb{E}\left[\mathbf{1}_{\{C_\nu=k\}}\right]\right], & s_g = \{\text{Action}\},\end{cases} \tag{77}$$

where

$$\mathbb{E}\left[\mathbf{1}_{\{C_\nu=k\}}\right] = \mathbb{E}\left[\mathbb{E}\left[\frac{(\lambda_c t_\nu)^k}{k!}\cdot e^{-\lambda_c t_\nu}\Big|t_\nu\right]\right]. \tag{78}$$

3. Multiple Layered IoT-Server Network Design

The MLBGG framework is suitable to adapt any type of hierarchical networks, including computer networks and management systems. A typical IoT-Server network architecture is connected cars (i.e., IoT connection) which are controlled by agent servers which are decentralized and equally contributed. The Internet of Vehicles or EBIoV (Enhanced Blockchain-based Internet of Vehicles) [19] are widely known frameworks for connecting smart components in each car. Although the application in this paper deals with smart components in a connected car as IoT elements, this model could be applied to drones as IoT elements for improving their security. Basically, any IoT component could consider the MLBGG model for enhancing its security without centralized authentication systems.

3.1. Multiple Layered IoT-Server Network Architecture

The networks which combines IoT networks and a server network could adapt the MLBGG. The set of IoT networks is one layer and one set with management servers is the other layer. The BGG is adapted into IoT networks as layer 1 and the SABGG is applied into the network of management servers (see Figure 3).

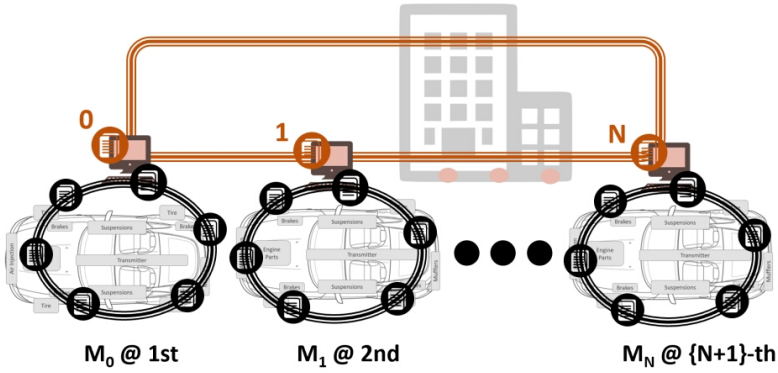

Figure 3. IoT-Server network architecture in the MLBGG. M_k (k = 0, 1, 2, ... N) is the index which is started from 0 and N + 1 is the total count of cars.

Layer 1 contains $\eta + 1$ IoT systems, and each IoT system has $M_l, l = \{0, 1, \ldots, \eta\}$ components which are fully connected. The l-th IoT system should have at least one (agent) server as a component within M_l components. These servers, which have higher control levels, become the components in layer 0, and the $\eta + 1$ elements in layer 0 are the backup nodes for all IoT systems in layer 0 (i.e., shared backup nodes). Since $\eta + 1$ servers in layer 0 can keep multiple ledgers, each server has all ledgers from the IoT systems in layer 0. It is noted that up to η nodes might allay one node in layer 0. The blockchain ledger for the agent system (i.e., layer 0) is different than the ledgers for IoT systems (i.e., layer 1) and is only shared within layer 0.

3.2. Stochastic Optimization

In layer 1, the reserving costs for backup nodes (i.e., "Action" strategy of a defender in layer 1) should be cheaper than the network bursting costs; otherwise, player H would choose the other strategy ("DoNothing" strategy). The number of nodes for protecting $\eta + 1$ BGG networks in layer 1 depends on the cost function. Available reserved nodes are equally applied to every BGG networks in layer 1, and the optimal portion for the blockchain governance B^1 could be found as follows:

$$B^1 = \inf\left\{\eta \geq 0 : \mathfrak{C}^{\mathbf{1}}\left(B^1\right)\right\}, B^1 \leq \eta, \tag{79}$$

where

$$\mathfrak{C}^{\mathbf{1}}\left(B^1\right) = \sum_{l=0}^{\eta} \mathbb{E}\left[\mathfrak{C}_{\mathbf{1}}^{l}\left(B_{\eta}^{1}\right)_{\text{Total}}\right]. \tag{80}$$

The governance cost function for governance for the l-th BGG networks in the layer 1 is as follows:

$$\mathfrak{C}^{l}_{\mathbf{1}}(B)_{\text{Total}} = \mathfrak{C}^{l}_{\text{Act}}(B) \cdot \mathbb{E}\left[\mathbf{1}_{\left\{A^{l}_{\nu-1} < \frac{M_l}{2}\right\}}\right] + \mathfrak{C}^{l}_{\text{NoA}} \cdot \mathbb{E}\left[\mathbf{1}_{\left\{A^{l}_{\nu-1} \geq \frac{M_l}{2}\right\}}\right] \tag{81}$$

and

$$\rho^{\mathbf{1}} = \left(\frac{1}{\eta+1}\right)\mathbb{E}\left[\sum_{l=0}^{\eta} \mathbf{1}_{\left\{H^{l}_{\nu} \geq \frac{M_l}{2}\right\}}\right], l = \{0.\ldots,\eta\}. \tag{82}$$

For each blockchain network in layer 1, no action for the l-th blockchain network will be taken until the moment τ_{ν^l-1}. If the attacker catches less than half of all nodes at $\tau^{l}_{\nu-1}$ (i.e., $\left\{A^{l}_{\nu-1} < \frac{M_l}{2}\right\}$), then the defender could take the action to avoid the attack at τ^{l}_{ν}, $l = 0, 1, \ldots, \eta$.

In layer 0, the acceptance rate of a strategic alliance in a blockchain network α depends on the cost function and the optimal portion $\alpha^{\mathbf{0}}$ for the SABGG could be found as follows (where $B := B^{0}_{\eta} = \left(\frac{\eta}{2}\right) \cdot \alpha$):

$$\alpha^{\mathbf{0}} = \inf\left\{\alpha \geq 0 : \mathfrak{C}^{0}_{\text{NoA}}\left(r^{0}\right) \geq \mathfrak{C}^{0}_{\text{Act}}(\alpha)\right\}, \tag{83}$$

where (at the moment $t_{\nu-1}$)

$$\mathfrak{C}^{\mathbf{0}}_{\text{NoA}}\left(r^{0}\right) = U_0 \cdot r^{0}, \tag{84}$$

$$\mathfrak{C}^{\mathbf{0}}_{\text{Act}}(\alpha,\eta) = c^{0}_{\eta}(\alpha)\left(1 - r^{1}_{\alpha}\right) + \left(c^{0}_{\eta}(\alpha) + U_0\right)r^{1}_{\alpha}, \tag{85}$$

$$r^{0} = \mathbb{E}\left[\mathbf{1}_{\left\{C_{\nu} \geq \frac{\eta}{2}\right\}}\right],\ r^{1}_{\alpha} = \mathbb{E}\left[\mathbf{1}_{\left\{C_{\nu} \geq \frac{\eta}{2}+B\right\}}\right]. \tag{86}$$

From (82) and (83), the optimal acceptance rate for layer 0 is determined as follows:

$$\alpha^{*} = \min\left\{\rho^{\mathbf{1}}, \alpha^{\mathbf{0}}\right\}, \tag{87}$$

and the defender will not take any action until the time $t_{\nu-1}$ for layer 0. If the attacker catches less than half of all nodes at $t_{\nu-1}$ (i.e., $C_{\nu-1} < \lceil \frac{\eta}{2} \rceil$), then the defender could take the action to avoid the attack at t_{ν}. The total cost for developing the enhanced blockchain network is as follows:

$$\mathfrak{C}^{\mathbf{0}}(\alpha,\eta)_{\text{Total}} = \mathfrak{C}^{\mathbf{0}}_{\text{Act}}(B) \cdot \mathbb{E}\left[\mathbf{1}_{\left\{C_{\nu-1} < \frac{\eta}{2}\right\}}\right] + \mathfrak{C}^{\mathbf{0}}_{\text{NoA}} \cdot \mathbb{E}\left[\mathbf{1}_{\{C_{\nu-1} \geq B\}}\right], \tag{88}$$

and the optimal portion for the blockchain governance $\eta^{\mathbf{0}}$ could be found as follows:

$$\eta^{0} = \inf\{\eta \geq 0 : \mathfrak{C}^{\mathbf{0}}(\eta)\}. \tag{89}$$

Since $\Theta_{\lceil \frac{\eta}{2} \rceil}(1, y_0, 1, 1, 1, 1)$ from (2.64) is the probability generating function of $C_{\nu-1}$, the probability mass could be found as follows:

$$\boldsymbol{P}\{C_{\nu-1} = k\} = \lim_{y_0 \to 0} \frac{1}{k!}\frac{\partial^{k}}{\partial y_0^{k}}\Theta_{\lceil \frac{N}{2} \rceil}(1, y_0, 1, 1, 1, 1), k = 0, \ldots, \left\lfloor \frac{\eta}{2} \right\rfloor. \tag{90}$$

From (79) and (89), the optimal number of the reserved nodes for layer 0 in layer 1 could be found as follows:

$$\eta^{*} = \max\left\{B^{1}, \eta^{0}\right\}. \tag{91}$$

Based on the conditions, the LP (Linear Programming) model could be described as follows:

Objective:

$$min\boldsymbol{G} = \mathbb{E}\left[\mathfrak{C}^{\mathbf{0}}\left(B^0\right)_{\text{Total}} + \mathfrak{C}^{\mathbf{1}}\left(B^1\right)_{\text{Total}}\right] \tag{92}$$

Subject to:

$$\alpha^* \geq \frac{c_\eta}{U_0 \cdot r^0 - c_\eta}. \tag{93}$$

4. Model Simulations

The safety mode is considered for protecting a network. Theoretically, the BGG-based network takes a preliminary action to avoid a 51 percent attack by an attacker. The simulations in this section are targeted to find optimal values of the configuring parameters, including an optimal number of reserved nodes in the layer 1 and the acceptance rate for the SABGG-based network in layer 0. The first simulation is finding the optimal value of reserved nodes for IoT networks in layer 1 (Section 4.2). The second one is designed to evaluate the optimal acceptance rate of the SABGG which is adapted in layer 0 (Section 4.3). Lastly, an overall cost comparison with a conventional network without adapting the BGG is discussed on Section 4.4.

4.1. Preliminaries

The safety mode is considered for protecting a multi-layered network. Theoretically, a BGG based network takes a preliminary action to avoid a 51 percent attack by an attacker. The action may actually happen before governing more than half of the nodes by an attacker or after. Two points of the Proof-Of-Work (POW) are considered as action points: One is the moment that passes more than a half of the nodes in the networks which are more than $\frac{M_l}{2}, l = 0, 1, \ldots \eta$ for layer 1 and more than $\frac{\eta}{2}$ for the layer 0. The other is one step prior to passing more than half the nodes in both layers. The best situation shall be that the safety mode is executed when an attacker takes more than half of the nodes, but the network is protected by releasing additional backup nodes. However, it is noted that attempting to govern more than a half of the nodes may happen even after exiting the safety mode (see Figure 4).

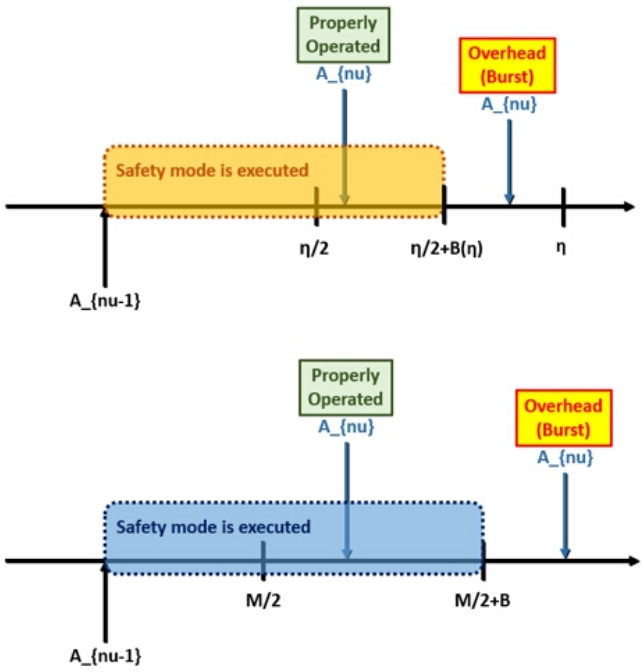

Figure 4. Operation of the safety mode of layer 0 (**top**) and layer 1 (**bottom**).

The simulation is processed by the following strategies:

- Two cases (one is with the BGG, the other is without the BGG) per each layer are simulated;
- Simulating the 51 percent attack to evaluate whether the nodes in the network are protected by the BGG or not;
- If the number of nodes governed by the attack is more than half at τ_v^l (i.e., $A_v^l \geq \frac{M_l}{2}$, $l = \{0, 1, \ldots, \eta\}$), the networks in layer 1 are burst;
- If the number of nodes governed by the attack is more than half at t_v (i.e., $C_v \geq \frac{\eta}{2}$), the network of layer 0 is burst;
- The safety modes for each layer are randomly executed based on the Binomial random variables;
- The observation (i.e., the duration of the proof-of-work) are the same within the same layer.

The strategy for protecting each network in layer 1 is for supporting the additional nodes to give the less chance that an attacker catches blocks with false control requests. The IoT-connected network is considered as a BGG network in the layer, and the estimated mean value of each network in layer 1 is around USD 10,000 each. The reserved nodes for a safety mode are the same for main nodes in the layer 0. All nodes in the layer 0 contains multiple ledgers of all network in the layer 1 (i.e., the number of reserved nodes η for a safety mode is same for all network in the layer 1). The details of other setups are described in Table 1.

Table 1. Initial conditions for layer 1.

Name	Value	Description
$\mathbb{E}\left[M^l\right]$	250	Average number of nodes of each network in layer 1 ($l = \{1, \ldots, N\}$)
$\mathbb{E}[V_l]$	10,000 [USD]	Average value of each network in layer 1
$c_1(B)$	–	The cost for reserving nodes to avoid attacks in layer 1
λ_A^l	–	The rate of attacking in layer 1
B	–	The number of backup nodes supported from layer 0 ($B \leq \eta$)

The setups for layer 0 could be similarly described in Table 2. It is noted that the overall loss value by the burst layer 0 network is higher than the average loss values of networks in layer 1 because the components in layer 1 are mainly IoT sensors, which are cheaper than the components in layer 0, which are typically servers and workstations.

Table 2. Initial conditions for layer 0.

Name	Value	Description
α (or p)	–	Acceptance rate for strategic alliance in layer 0
U_0	120,000 [USD]	Total value of the layer 0 network
$c_0(\alpha)$	–	The cost for reserving nodes to avoid attacks in layer 0
λ_c	–	The rate of governing nodes by attackers in layer 0
N	41 [Nodes]	Total number of nodes in layer 0 ($N = \eta + 1$)

4.2. Optimizing Backup Nodes for the Layer 1

This simulation considers that 41 (i.e., $\eta + 1$) IoT networks (as layer 1) are hooked up as a single network (as layer 0), and each IoT network has up to 40 backup nodes for security modes. The simulation goes for 1000 trials and finds the optimal number of backup nodes based on the cost efficiency. It has been executed 4 times with 1000 trials, and the optimal values vary (see Figure 5).

It shows that the optimal number of backup nodes are ranged between 35 and 45 nodes. The cost efficiency is around 46 percent, which indicates 250 BGG-based IoT networks are 46 percents cheaper than conventional IoT networks in terms of overall operating costs.

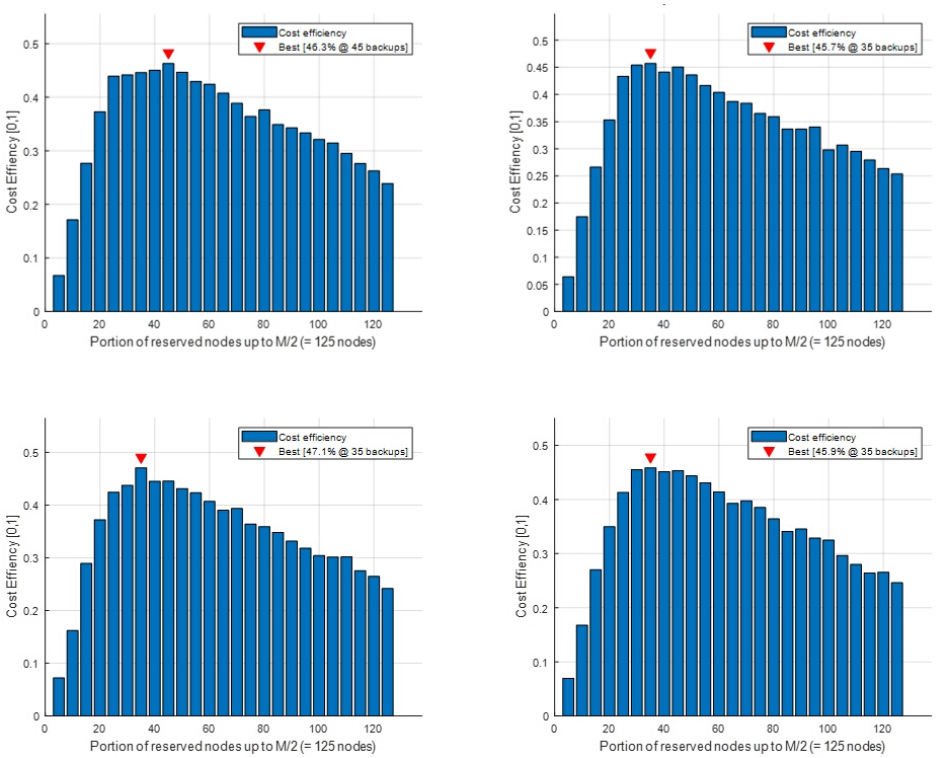

Figure 5. Simulation results to find the optimal value of the backup node.

4.3. Acceptance Rate of Strategic Alliance in the Layer 0

In layer 0, the acceptance rate is a vital matter because the layer 0 network adapts the SABGG [31]. This simulation robustly finds the optimal acceptance rate with correspond to number of nodes in layer 0. The simulation shows that around a 46 percent acceptance rate will give the best effort regardless of the number of nodes in layer 0 (see Figure 6).

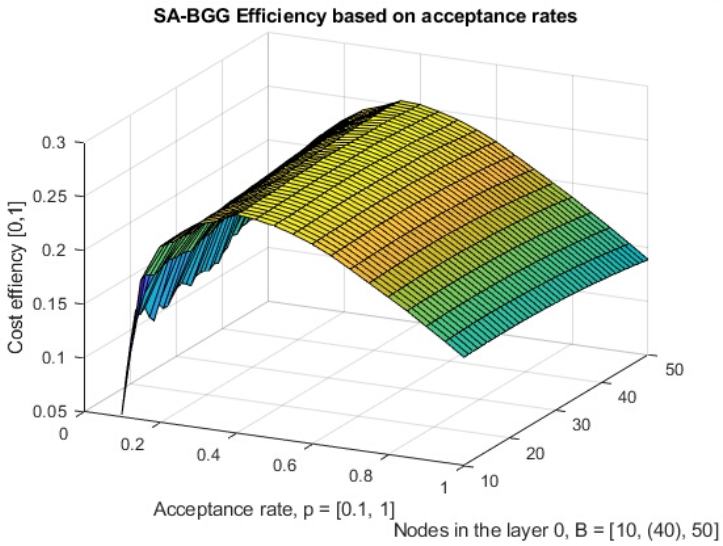

Figure 6. Acceptance rate optimization in layer 0.

4.4. Overall Performance Discussion of a Multi-Layered BGG

This session shows the comparison between a Multi-Layered BGG (MLBGG) and a blockchain network without BGG. The simulation calculates the average operating costs of both networks (layer 0 and 1) based on 1000 trials with the given conditions (Tables 1 and 2). The result shows that the average operating costs for the safety mode are USD 286,916 for the MLBGG adapted network (USD 115,400 in layer 0 and USD 171,516 in layer 1) and the network without the MLBGG costs USD 520,000 (i.e., USD 120,000 + USD 400,000).

The average cost efficiency of the MLBGG-adapted network ε that compares to the safety operation cost of conventional IoT networks can be solved as follows [34]:

$$\varepsilon = \frac{|C_b - C_r|}{C_r} \tag{94}$$

where C_b (=USD 286,916) is the average safety operation costs with the MLBGG and C_r (=USD 520,000) is the cost of an atypical IoT network without the BGG adaptation. From (94), the MLBGG cost efficiency is 0.4482 (in Figure 7), which means that about 45 percent of the costs are saved by adapting an MLBGG. Since the testing values are randomly generated in each simulation, the results from other trials might not be the same as the current ones in this section.

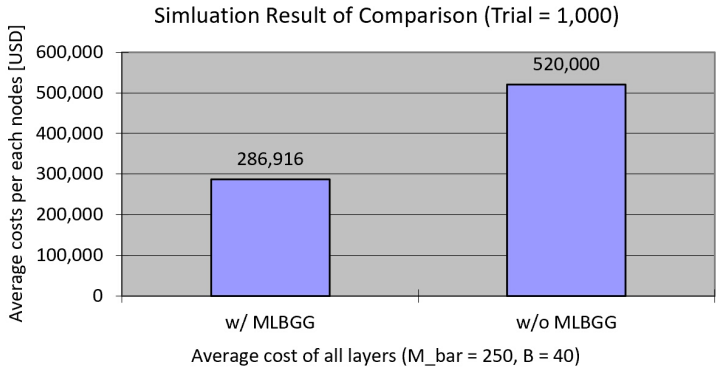

Figure 7. Performance comparison graph.

5. Conclusions

The major target of this paper has established explicit formulas of the Multi-Layered Blockchain Governance Game, and the set of IoT networks are combined with secure management network systems as a higher hierarchy. This hybrid network architecture directly adapts the blockchain governance game for enhancing the security. An analytic approach supports the theoretical background of decision-making factors to design the enhanced network architecture. The several simulations are executed to find various hyper-parameters, which also impacts the network performance. This innovative architecture is targeted to improve the security only based on network architectural perspectives. This new proposed model is still theoretical, and actual implementations on real blockchain networks shall be developed to see how this theory is actually working. Other technical perspectives for improving blockchain security are out of scope in this paper, but combining these technical perspectives and the MLBGG might be considered as future research topics. The MLBGG model shall be extended to various blockchain-based cybersecurity network frameworks for connected cars and smart drone swarms.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Special thanks to the Guest Editor, Ana Meca, who has guided the author to submit the proper topic of the journal. The Matlab codes for the simulations are publicly available on GitHub (https://github.com/amangkim/mlbgg (accessed on 10 November 2021)) for users to try the demonstrations of the Multi-Layered Blockchain Governance Game.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available online: http://www.bitcoin.org (accessed on 10 November 2021).
2. Beikverdi, A.; Song, J. Trend of centralization in Bitcoin's distributed network. In Proceedings of the 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015; pp. 1–6.
3. Yli-Huumo, I.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology? A Systematic Review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef] [PubMed]
4. Decker, C.; Wattenhofer, R. Information propagation in the Bitcoin network. In Proceedings of the IEEE P2P 2013 Proceedings, Trento, Italy, 9–11 September 2013; pp. 1–10.
5. Kim, W. Bitcoin, Blockchain Mechanism and Its Evolution. 2018. Available online: http://www.itfind.or.kr/publication/ (accessed on 10 November 2021). (In Korean)
6. Narayanan, A.; Clar, J. Bitcoin's Academic Pedigree. *Mag. Commun. ACM* **2017**, *60*, 36–45. [CrossRef]
7. Weiss, M.; Corsi, E. Bitfury: Blockchain for Government. *HBP Case* **2018**, *12*, 818-031.
8. Armknecht, F.; Karame, G.O.; Mandal, A.; Youssef, F.; Zenner, E. Ripple: Overview and Outlook. In *Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2015; Volume 9229, pp. 163–180.
9. Micali, S.; Rabin, M.O.; Vadhan, S.P. Verifiable random functions. In Proceedings of the 40th IEEE Symposium on Foundations of Computer Science, New York, NY, USA, 17–18 October 1999; pp. 120–130.
10. Goldberg, S.; Reyzin, L.; Papadopoulos, D.; Vcelak, J. Verifiable Random Functions. IETF. 2021. Available online: https://datatracker.ietf.org/doc/draft-irtf-cfrg-vrf/09/ (accessed on 10 November 2021).
11. Restuccia, F.; D'Oro, S.; Kanhere, S.S.; Melodia, T.; Das, S.K. Blockchain for the Internet of Things: Present and Future. 2018. Available online: https://arxiv.org/abs/1903.07448 (accessed on 1 May 2019).
12. Bolton, T.; Dargahi, T.; Belguith, S.; Al-Rakhami, M.S.; Sodhro, A.H. On the Security and Privacy Challenges of Virtual Assistants. *Sensors* **2021**, *21*, 2312. [CrossRef] [PubMed]
13. Rouse, M. Internet of Vehicles. 2018. Available online: https://whatis.techtarget.com/definition/Internet-of-Vehicles (accessed on 1 May 2019).
14. Dandala, T.T.; Krishnamurthy, V.; Alwan, R. Internet of Vehicles (IoV) for traffic management. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 10–11 January 2017; pp. 1–4.
15. Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 13th IEEE/ACS International Conference of Computer Systems and Applications (AICCSA 2016), Agadir, Morocco, 29 November–2 December 2016.
16. Haig, S. Ford to Use Cryptocurrency for Inter-Vehicle Communication System. 2017. Available online: https://news.bitcoin.com/ford-cryptocurrency-inter-vehicle-communication-system/ (accessed on 1 May 2019).
17. Hamid, U.Z.A.; Zamzuri, H.; Limbu, D.K. Internet of Vehicle (IoV) Applications in Expediting the Implementation of Smart Highway of Autonomous Vehicle: A Survey. In *Performability in Internet of Things*; Springer: Cham, Switzerland, 2018; pp. 137–157.
18. Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Commun. Mag.* **2017**, *55*, 119–125. [CrossRef]
19. Kim, S.-K. Enhanced IoV Security Network by Using Blockchain Governance Game. *Mathematics* **2021**, *9*, 109. [CrossRef]
20. Baker, J. Edge Computing—The New Frontier of the Web. 2017. Available online: https://hackernoon.com/edge-computing-a-beginners-guide-8976b6886481 (accessed on 10 November 2021).
21. ERPINNEW. Fog Computing vs. Edge Computing. 2017. Available online: https://erpinnews.com/fog-computing-vs-edge-computing (accessed on 1 May 2019).
22. Cisco Networking Academy. *Connecting Networks Companion Guide*; Cisco Press: Indianapolis, IN, USA, 2014.
23. Eyal, I.; Sirer, E. Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In *Lecture Notes in Computer Science*; Springer: Berlin, Germany, 2014; Volume 8437, pp. 436–454.
24. Abdalzaher, M.S.; Seddik, K.; Elsabrouty, M.; Muta, O.; Furukawa, H.; Abdel-Rahman, A. Game Theory Meets Wireless Sensor Networks Security Requirements and Threats Mitigation: A Survey. *Sensors* **2016**, *16*, 1003. [CrossRef]
25. Hu, J.; Reed, M.; Thomos, N.; AI-Naday, M.F.; Yang, K. Securing SDN-Controlled IoT Networks Through Edge Blockchain. *IEEE Internet Things* **2021**, *8*, 2102–2115. [CrossRef]
26. Wang, T.; Bai, X.; Wang, H.; Liew, S.C.; Zhang, S. Game-Theoretical Analysis of Mining Strategy for Bitcoin-NG Blockchain Protocol. *IEEE Syst.* **2021**, *15*, 2708–2719. [CrossRef]

27. Abdalzaher, M.S.; Muta, O. A Game-Theoretic Approach for Enhancing Security and Data Trustworthiness in IoT Applications. *IEEE Internet Things* **2020**, *7*, 11250–11261. [CrossRef]
28. Abdalzaher, M.S.; Seddik, K.; Muta, O. An effective Stackelberg game for high-assurance of data trustworthiness in WSNs. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 1257–1262.
29. Liu, Z.; Luong, N.C.; Wang, W.; Niyato, D.; Wang, P.; Liang, Y.C.; Kim, D.I. A Survey on Applications of Game Theory in Blockchain. *arXiv* **2019**, arXiv:1902.10865.
30. Kim, S.-K. Blockchain Governance Game. *Comput. Ind. Eng.* **2019**, *136*, 373–380. [CrossRef]
31. Kim, S.-K. Strategic Alliance for Blockchain Governance Game. *Probab. Eng. Inf. Sci.* **2021**, 1–17. [CrossRef]
32. Dshalalow, J.H.; Ke, H.-J. Layers of noncooperative games. *Nonlinear Anal.* **2009**, *71*, 283–291. [CrossRef]
33. Dshalalow, J.H. *First Excess Level Process, Advances in Queueing*; CRC Press: Boca Raton, FL, USA, 1995; pp. 244–261.
34. Kim, S.-K. Design of stochastic hitless-prediction router by using the first exceed level theory. *Math. Methods Appl. Sci.* **2003**, *28*, 1481–1490. [CrossRef]