mathematics

Article

Enhanced IoV Security Network by Using 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: This paper deals with the design of the secure network in an Enhanced Internet of Vehicles by using the Blockchain Governance Game (BGG). The BGG is a system model of a stochastic game to find best strategies towards preparation of preventing a network malfunction by an attacker and the paper applies this game model into the connected vehicle security. Analytically tractable results for decision-making parameters enable to predict the moment for safety operations and to deliver the optimal combination of the number of reserved nodes with the acceptance probability of backup nodes to protect a connected car. This research helps for whom considers the enhanced secure IoV architecture with the BGG within a decentralized network.

Keywords: IoT security; Internet of Vehicles; IoV; connected car; Blockchain Governance Game; mixed game; stochastic model; fluctuation theory; 51 percent attack

check for updates

Citation: Kim, S.-K. Enhanced IoV Security Network by Using Blockchain Governance Game. *Mathematics* **2021**, *9*, 109. https://doi.org/10.3390/math9020109

Received: 8 December 2020
Accepted: 29 December 2020
Published: 7 January 2021

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

1. Introduction

A connected car transfers data to others based on vehicle-to-vehicle (V2V) communication technologies and it typically means that cars are equipped for Internet access usually with wireless local area networks (WLANs). Cars have been evolved to support enhanced driving aids for full autonomous driving by using the artificial intelligence (AI) and its maneuvers [1]. The Internet of Vehicles (IoV) is a superset of a connected car which contains sensors, GPS, entertainment systems, brakes and throttles. The IoV is a moving network which is made up of IoT enabled cars through the usage of modern electronics and the integrated information to maintain traffic flow. Cars have evolved from mechanical transportation to the smart vehicles with varieties of communication and sensing capabilities. The IoV has developed over time from the conventional vehicular networks that connect the smart vehicles to the smart city with the development of Internet of Things (IoT) [2]. The IoV is designed to perform more effective fleet management and accident avoidance [3,4]. An ad-hoc network is applied to connect IoT components as nodes in a connected car [4]. Adapting the Blockchain technologies into IoV networks brings huge attentions from researchers and developers because of decentralization, anonymity, and trust characteristics [5–7]. Additionally, data sharing among vehicles is critical to improve driving safety and to enhance vehicular services in IoV networks. The studies in the security and the tractability of data sharing indicate that utilizing consensus schemes are as hard as establishing Blockchain enabled IoV (BIoV) [6]. Some other studies have proposed a decentralized trust management system for vehicle data credibility assessment using Blockchain with joint Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus schemes [7–9]. Vehicle manufacturers Volkswagen and Ford have filed the patents that enable secure inter-vehicle communication through Blockchain technologies [10,11]. In the view point of the IoT securities, several studies are dealing with similar topics regarding the Blockchain based IoT securities [6,12–14]. Most studies are surveys [12] but none of them are mathematically approached for developing a network architecture for a Blockchain based IoT [13,14].

The Enhanced BIoV (EBIoV) network, which has been conceptually introduced on public [15], is reloaded in this paper. The EBIoV is an IoV network architecture based on the Edge computing [16,17] with enabling the Blockchain Governance Game (BGG) [18,19] for improving network securities [15]. Although a public Blockchain is designed for empowering their decentralization [20], current public Blockchain based services including cybercurrencies are not fully safe from attacks especially based on the mining computation [18]. Hence, a private Blockchain which is a permission-based Blockchain [20] has been proposed for business or government usage [21,22]. Many peoples are interested in a private Blockchain technology even in a consortium Blockchain technology [20] but they are not comfortable with a level of control compared to the offered control level in a public decentralized network. More importantly, the control levels in a Blockchain network should be balanced to retain the strengths of a decentralized network to avoid all security matters what atypical centralized network contains [18]. By adapting the BGG, we do not need to concern about the computation power for mining (i.e., generating ledgers) without losing the strength from fully decentralized networks. A conventional BIoV model could be applied to trace the provenance of spare parts back through every step of the supply chain to its original manufacture date and location [15,23]. Car manufacturers concern that service centers and garages are knowingly fitting counterfeit spare parts to their vehicles of customers. Counterfeit parts shall damage a brand reputation when the parts become causes of accidents. Identifying genuinity of car parts by using the EBIoV has been studied and the network within car components shall be considered as an Edge network [16,17,24].

The Fog computing pushes information to the neighborhood area network amount of community knowledge at an IoT gateway and it could be combined with the Blockchain technology for enhancing security matters [17]. In the EBIoV network architecture, diagnosis equipment in car service centers is in a Fog network and the database in a headquarter (HQ) is positioned the level of the cloud network (see Figure 1). This paper provides the mathematical functional of the EBIoV network architecture for enhancing security particularly from counterfeits of car parts. The EBIoV security regarding counterfeits of car parts has already been studied [15] and this research is focused on avoiding conventional IoV attack in a decentralized network. The BGG is the game model that an attacker and a defender compete each other by building blocks in private and public chains as a sequence of stages to generate ledgers [18,19]. The historical strategies and the probabilistic stage transitions can be observed by both an attacker and a defender. Hence, the interaction between an attacker and a defender can be modeled as a stochastic game [18,19,25]. This joint functional between two players of the predicted time of the first observed threshold to cross the half of the total nodes along with values of each component upon this time. The defender (a car company) could take a preliminary action (i.e., request to add honest nodes as a safety mode) for protecting the Blockchain in a vehicle.

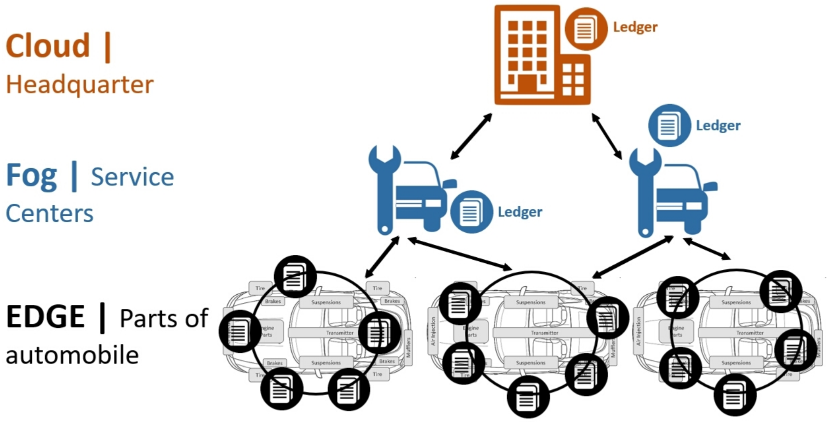

Figure 1. Adapting Fog Computing in Auto Services in Blockchain [15].

This paper is organized as follows: Section 2 presents the Enhanced BIoV (EBIoV) network and it describes how to construct EBIoV architecture by using the BGG model which is a stochastic game between an attacker and a defender. Once a dishonest blocks are generated, the model predicts how many blocks will be generated and finds the moment when more than the half of nodes are covered by an attacker. The framework for setting up the mixed strategic game is provided in Section 3. The optimal values of an EBIoV network for the memoryless case are analytically calculated in Section 4. The memoryless property implies that a defender does not spend additional resources to store past information. Lastly, Section 5 provides the conclusion of the paper.

2. Stochastic Game for BIOV Network Security

The Blockchain Governance Game (BGG) [18,19] has been adapted the BIoV network architecture to defend against the attacks [15]. This system model consists of one attacker (i.e., the miner which intends to fork a private chain) and one defender (the miner which honestly mines on the public chain) [25]. This explicit function (Theorem BGG-1) from the BGG (Blockchain Governance Game) gives the predicted moment of one step prior to an attack [18].

2.1. Enhanced IoV Network Structure

The proposed BIoV network structure [15] is explored in detail in this section. The components in a vehicle, the equipment of a service center and a HQ database are hooked up as one Blockchain network (see Figure 2). Each smart components in a connected car could mechanically or electronically generate random values and share these values with other smart components. Tires, brakes, an engine, a transmitter in a car could be the smart components which shall be capable to communicate with other components and to construct ledgers. Connected car components beside a CPU (smart controller) generate values based on their mechanical actions and these generated values are sharing with all other components including assigned service centers and a company headquarter. Each values from car components is unique and randomly generated. And sharing these generated number is a transaction in a conventional Blockchain network. A service center has a database which contains information from cars which are served by service centers. The unique value based on a registered car database are generated and sharing with other nodes including a company headquarter.

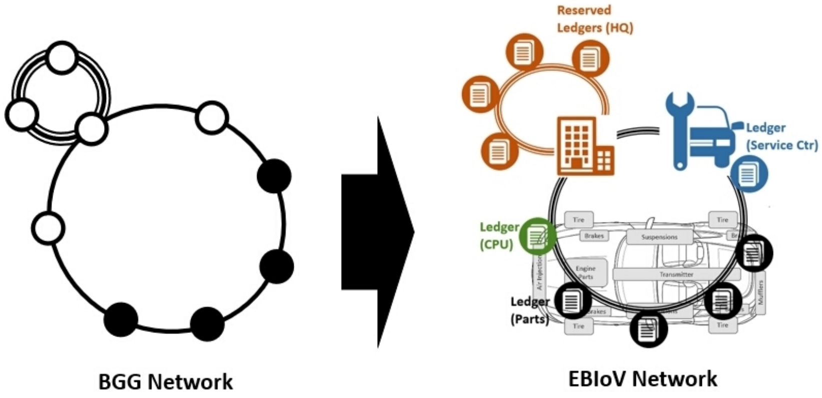

Figure 2. Adapting BGG for the EBIoV architecture [18].

Unlike conventional Blockchain networks, an EBIoV network does not have any reward system which requires a heavy computational power for being a miner to generate ledgers. All nodes even in a service center and a HQ have same contribution power and the equal chance to be a miner. For instance, a node of a CPU is same as nodes of other car parts although a CPU controls other car parts. The verifiable random function (VRF) which maps inputs to verifiable pseudorandom outputs is applied to select a node for generating ledgers [26,27]. The VRF has been applied to perform secret cryptographic solution to select committees to run the consensus protocol [28,29]. By applying the VRF, all nodes in the EBIoV network shall have the equal chance to become a miner who generates ledgers without requiring heavy computational powers. The mechanism for protecting an EBIoV network is exactly same as the mechanism of the BGG. The governance in a Blockchain network is followed by the decision making parameters which include the prior time before catching more than half of total nodes by an attacker. Any action shall not be taken until one step prior to the time when it passes the first passage time. It still has the chance that all nodes are governed by an attacker although an attacker catches less than the half of nodes.

2.2. BGG Model for Enhanced BIoV Network

To apply the BGG model into the BIoV network structure, the antagonistic game of two players (called "A" and "H") are introduced to describe the Blockchain network in a connected car as a defender and an attacker. Both players compete to build the blocks either for honest or false nodes. Let $(\Omega, \mathcal{F}(\Omega), P)$ be probability space $\mathcal{F}_A, \mathcal{F}_H, \mathcal{F}_\tau \subseteq \mathcal{F}(\Omega)$ be independent σ-subalgebras. Suppose:

$$\mathcal{A} := \sum\nolimits_{k\geq 0} X_k \varepsilon_{s_k},\ s_0(=0) < s_1 < s_2 < \cdots, \text{a.s.} \tag{1}$$

$$\mathcal{H} := \sum\nolimits_{j\geq 0} Y_j \varepsilon_{t_j},\ t_0(=0) < t_1 < t_2 < \cdots,\ \text{a.s.} \tag{2}$$

are $\mathcal{F}_A$-measurable and $\mathcal{F}_H$-measurable marked Poisson processes (ε_w is a point mass at w) with respective intensities λ_a and λ_h. 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 (a defender). Player A builds the blocks with fake information and sustain respective build the blocks of magnitudes X_1, $X_2, \ldots$ formalized by the process. Similarly, player H generates the blocks with authorized information with the blocks of magnitudes Y_1, $Y_2, \ldots$ Both players compete each other to build their blocks (either genuine or fake). The processes $\mathcal{A}$ and $\mathcal{H}$ are specified by their transforms

$$\mathbb{E}\left[g^{\mathcal{A}(s)}\right] = e^{\lambda_a s(g-1)}, \mathbb{E}\left[z^{\mathcal{H}(t)}\right] = e^{\lambda_h t(z-1)}. \tag{3}$$

The game is observed at random times in accordance with the point process and it is equivalent with the duration of the PoW (Proof-of-Work) completion in a Blockchain based network:

$$\mathcal{T} := \sum\nolimits_{i\geq 0} \varepsilon_{\tau_i},\ \tau_0(>0)), \tau_1, \ldots, \tag{4}$$

which is assumed to be delayed renewal process. The observation process could be formalized as

$$\mathcal{A}_\tau \otimes \mathcal{H}_\tau := \sum\nolimits_{k\geq 0} (X_k, Y_k)\varepsilon_{\tau_k}, \tag{5}$$

and it is with position dependent marking and with X_k and Y_k being dependent with the notation

$$\Delta_k := \tau_k - \tau_{k-1},\ k = 0, 1, \ldots, \tau_{-1} = 0, \tag{6}$$

and

$$\gamma(g, z) = \mathbb{E}\left[g^{X_k} \cdot z^{Y_k}\right], \|g\| \leq 1, \|z\| \leq 1. \tag{7}$$

By using the double expectation,

$$\gamma(g, z) = \delta(\lambda_A(1-g) + \lambda_H(1-z)), \tag{8}$$

$$\gamma_0(g, z) = \delta_0(\lambda_A(1-g) + \lambda_H(1-z)), \tag{9}$$

where

$$\delta(\theta) = \mathbb{E}\Big[e^{-\theta\Delta_1}\Big], \delta_0(\theta) = \mathbb{E}\Big[e^{-\theta\tau_0}\Big], \tag{10}$$

are the magical transform of increments $\Delta_1, \Delta_2, \ldots$. This game contains a stochastic process $\mathcal{A}_\tau \otimes \mathcal{H}_\tau$ which describes the evolution of a conflict between players A and H known to an observation process $\mathcal{T}$={$\tau_0, \tau_1, \ldots$}. The process ends when on the k-th observation epoch τ_k, the collateral building blocks to player H (or A) exceeds more than the half of the total nodes M in the regular operation or player A exceeds more than $\Big(\frac{M}{2}\Big) + B$ nodes under the safety mode. To further formalize the game, the exit indexes [18] are as follows:

$$\nu := \inf\bigg\{k : A_k = A_0 + X_1 + \cdots + X_k \geq \bigg(\frac{M}{2}\bigg) + B\bigg\}, \tag{11}$$

$$\mu := \inf\bigg\{j : H_j = H_0 + Y_1 + \cdots + Y_j \geq \bigg(\frac{M}{2}\bigg)\bigg\} \tag{12}$$

where B is the number of the reserved honest nodes from a headquarter (HQ) which is depends on the availability from the HQ. Since, an attacker is win at time τ_ν, otherwise an honest node generates the correct blocks to share with others nodes. We are targeting the confined game in the view point of player A. The joint functional of the BIoV network model is as follows:

$$\Phi\bigg(\zeta; \bigg\lceil\frac{M}{2}\bigg\rceil + B, \bigg\lceil\frac{M}{2}\bigg\rceil\bigg) = \mathbb{E}\bigg[\mathbb{E}\bigg[\zeta^\nu \cdot g_0^{A_{\nu-1}} \cdot g_1^{A_\nu} \cdot z_0^{H_{\nu-1}} \cdot z_1^{H_\nu}\mathbf{1}_{\{\nu<\mu\}}\bigg|B\bigg]\bigg], \tag{13}$$

$$\|\zeta\| \leq 1, \|g_0\| \leq 1, \|g_1\| \leq 1, \|z_0\| \leq 1, \|z_1\| \leq 1,$$

where M indicates the total number of nodes (or ledgers) in the BIoV network for each car (see Figure 2). The BGG-1 Theorem [18] establishes an explicit formula $\Phi\Big(\xi, \Big\lceil\frac{M}{2}\Big\rceil + B, \Big\lceil\frac{M}{2}\Big\rceil\Big)$ and the functional (13) satisfies following expression:

$$\Phi\bigg(\zeta; \bigg\lceil\frac{M}{2}\bigg\rceil + B, \bigg\lceil\frac{M}{2}\bigg\rceil\bigg) = \mathfrak{D}_{(u,v)}^{(\lceil\frac{M}{2}\rceil+B,\lceil\frac{M}{2}\rceil)}\bigg[\Gamma_0^1 - \Gamma_0 + \frac{\xi \cdot \gamma_0}{1-\xi\gamma}\Big(\Gamma^1 - \Gamma\Big)\bigg] \tag{14}$$

$$\gamma := \gamma(g_0g_1u, z_0z_1v), \gamma_0 := \gamma_0(g_0g_1u, z_0z_1v), \tag{15}$$

$$\Gamma := \gamma(g_1u, z_1v), \Gamma_0 := \gamma_0(g_1u, z_1v), \tag{16}$$

$$\Gamma^1 := \gamma(g_1, z_1v), \Gamma_0^1 := \gamma_0(g_1, z_1v). \tag{17}$$

Additionally, the operator $\mathfrak{D}_{(x,y)}^{(m,n)}$ in (14) is defined as follows [18]:

$$\mathfrak{D}_{(x,y)}^{(m,n)}(\bullet) = \begin{cases} \Big(\frac{1}{m!\cdot n!}\Big)\lim_{(x,y)\to 0}\frac{\partial^m\partial^n}{\partial x^m\partial y^n}\frac{1}{(1-x)(1-y)}(\bullet), & m,n \geq 0, \\ 0, & \text{otherwise}, \end{cases} \tag{18}$$
$$||x|| < 1, ||y|| < 1,$$

then we can find

$$g(m,n) = \mathfrak{D}_{(x,y)}^{(m,n)}\Big[\mathcal{D}_{(m,n)}\left\{g(m,n)\right\}\Big], \tag{19}$$

where

$$\mathcal{D}_{(m,n)}\left[g(m,n)\right](x,y) := (1-x)(1-y)\sum_{m\geq 0}\sum_{n\geq 0}g(m,n)x^my^n, ||x|| < 1, ||y|| < 1. \tag{20}$$

It is noted that both operators $\mathfrak{D}$, $\mathcal{D}$ are originated from the first exceed theory [30,31]. We can find the PGFs (probability generating functions) of the exit index ν from (14):

$$\mathbb{E}[\zeta^{\nu}] = \mathbb{E}\left[\Phi\left(\zeta; \left\lceil \frac{M}{2} \right\rceil + B, \left\lceil \frac{M}{2} \right\rceil\right) \middle| B\right]\Bigg|_{(g_0,g_1,z_0,z_1)\to 1} \tag{21}$$

3. Strategies in Blockchain Governance Game

Let us consider a two-person mixed strategy game which is played by player H as a defender and player A as an attacker. Player H, who is mostly a car company in an EBIoV network, has two strategies at the observation moment when one step prior to complete for generating alternative chains with fake information. Basically, player H has the following strategies (i.e., operation modes): (1) Regular−regular operations which implicates that the BIoV network in a connected car are running as usual, and (2) Safety−the network is running under the safety mode for avoiding attacks by adding honest nodes from a HQ. Alternatively, player A (an attacker) might succeed to catch the blocks or fail to catch the honest nodes. Therefore, the response of player A would be either "Not Burst" or "Burst." Let us assume that the cost for reserving additional honest nodes is c_b where b is a set of the factors that related with the reserved nodes from a HQ and these related factors could be one or multiple values.

The headquarter of a car company reserves a certain portion of nodes for protecting the BIoV network integrity. If an attacker succeeds to generate alternative blocks within car parts, the network in a car is burst and the whole car value V is lost. It still has a chance to burst a car network although a defender (or a car company) adds honest nodes before catching blocks of an attacker. In this case, the lost cost includes not only a full car value but also a cost for additional reserved honest nodes. The normal form of a game is as follows:

$$\begin{array}{ll} .\ \text{Players:} & \boldsymbol{N} = \{\text{A}, H\}, \\ .\ \text{Strategy sets:} & \\ & \boldsymbol{s_a} = \{\text{“NotBurst”}, \text{“Burst”}\}, \\ & \boldsymbol{s_h} = \{\text{“Regular”}, \text{“Safety”}\} \end{array} \tag{22}$$

Based on the above conditions, the general cost matrix at $\tau_{\nu-1}$ when is the prior time just before bursting could be composed as shown in Table 1 where $q(s_h)$ is the probability of bursting a blockchain network (i.e., an attacker wins a game) and it depends on a strategic choice of player H:

$$q(s_h) = \begin{cases} \mathbb{E}\left[\mathbf{1}_{\left\{A_\nu \geq \frac{M}{2}\right\}}\right], & s_h = \{\text{“Regular”}\}, \\ \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}_{\left\{A_\nu \geq \frac{M}{2} + B\right\}} \middle| B\right]\right], & s_h = \{\text{“Safety”}\}. \end{cases} \tag{23}$$

Table 1. Cost matrix.

	NotBurst $(1 - q(s_h))$	**Burst $(q(s_h))$**
Regular	0	V
Safety	c_b	$c_b + V$

It is noted that the cost for reserved nodes (i.e., the cost of "Safety" operation strategy by player H) should be smaller than the whole cost of the other strategy. Additionally, the number of reserved honest nodes from the HQ is random and this variable B shall have a certain probability distribution. Let us consider the number of reserved honest nodes has the binomial distribution with the success probability ρ and the number of trial n. The PGF of the binomial distribution is as follows:

$$\sigma_n = \mathbb{E}\left[b^B\right] = (\rho b - (1-\rho))^n. \tag{24}$$

The optimal number of reserved nodes n^* which supported by the HQ depends on the cost function and the optimal value ρ^* is the acceptance rate when the reserved honest nodes are requested to a HQ. The best combination (n^*, ρ^*) could be found as follows:

$$(n^*, \rho^*) = \inf\left\{(n, \rho) \geq 0 : \mathfrak{S}_{\text{Reg}}\left(q^0\right) \geq \mathfrak{S}_{\text{Safe}}(n, \rho)\right\}, \tag{25}$$

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

$$\mathfrak{S}_{\text{Reg}}\left(q^0\right) = V \cdot q^0, \tag{26}$$

$$\mathfrak{S}_{\text{Safe}}(n, \rho) = c_{(n,\rho)}\left(1 - q^1_\eta\right) + \left(c_{(n,\rho)} + V\right) q^1_{(n,\rho)}, \tag{27}$$

$$q^0 = \mathbb{E}\left[\mathbf{1}_{\left\{A_\nu \geq \lceil \frac{N}{2} \rceil\right\}}\right], \tag{28}$$

$$q^1_{(n,\rho)} = \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}_{\left\{A_\nu \geq \lceil \frac{N}{2} \rceil + B\right\}} \middle| B\right]\right]. \tag{29}$$

We would like to design the BGG adapted BIoV network that is capable to take the safety operation at the decision making moment $\tau_{\nu-1}$. The governance of the Blockchain network is driven by the BGG decision making parameters. It is noted that no safety actions are required until the time $\tau_{\nu-1}$. Additionally, it still has 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., $\left\{A_{\nu-1} \geq \frac{M}{2}\right\}$). If the attacker catches less than half of all nodes at $\tau_{\nu-1}$ (i.e., $\left\{A_{\nu-1} < \frac{M}{2}\right\}$), then the defender could run the safety mode to avoid the burst at τ_ν. The total cost for developing the enhanced BIoV network is as follows:

$$\begin{aligned} \mathfrak{S}\left(q^0; n, \rho\right)_{\text{Total}} &= \mathbb{E}\left[\mathfrak{S}_{\text{Safe}}(n, \rho) \cdot \mathbf{1}_{\left\{A_{\nu-1} < \frac{M}{2}\right\}} + \mathfrak{S}_{\text{Reg}}\left(q^0\right) \cdot \mathbf{1}_{\left\{A_{\nu-1} \geq \frac{M}{2}\right\}}\right] \\ &= \left\{c_{(n,\rho)}\left(1 - q^1_{(n,\rho)}\right) + \left(c_{(n,\rho)} + n\rho\right) q^1_{(n,\rho)}\right\} p_{A_{-1}} + B \cdot q^0\left(1 - p_{A_{-1}}\right) \end{aligned} \tag{30}$$

where

$$p_{A_{-1}} = \boldsymbol{P}\left\{A_{\nu-1} < \frac{M}{2}\right\} = \sum_{k=0}^{\lfloor \frac{M}{2} \rfloor} \boldsymbol{P}\{A_{\nu-1} = k\}. \tag{31}$$

3.1. Memoryless BGG Observation Process for EBIoV Networks

It is assumed that the observation process has the memoryless properties. This might be a special condition but very practical for actual implementation of a Blockchain Governance Game [18]. It implies that a defender does not spend additional cost for storing past information. After building a cost function of a BGG network, we could find explicit solutions of q^0, $p_{A_{-1}}$ and the moment of decision making after finding the closed form (PGF) of the first exceed index ν, each probability (generating function) of the number of blocks at the moment τ_ν $\left(\text{i.e., } \mathbb{E}\left[g_1^{A_\nu}\right]\right)$ and $\tau_{\nu-1}$ $\left(\text{i.e., } \mathbb{E}\left[g_0^{A_{\nu-1}}\right]\right)$. The functional $\mathfrak{D}$ is defined on the space of all analytic functions at 0. Recalling from (7)–(10), we have:

$$\gamma(g, z) = \delta(\lambda_a(1-g) + \lambda_h(1-z)) = \gamma_a(g) \cdot \gamma_h(z), \tag{32}$$

$$\gamma_a(g) = \delta(\lambda_a(1-g)), \gamma_h(z) = \delta(\lambda_h(1-z)), \tag{33}$$

and

$$\gamma_0(g, z) = \delta_0(\lambda_a(1-g) + \lambda_h(1-z)) = \gamma^0_a(g) \cdot \gamma^0_h(z), \tag{34}$$

$$\gamma^0_a(g) = \mathbb{E}\left[g^{A_0}\right] = \delta_0(\lambda_a(1-g)), \tag{35}$$

$$\gamma_h^0(z) = \mathbb{E}\left[z^{H_0}\right] = \delta_0(\lambda_h(1-z)), \tag{36}$$

from (15)–(17),

$$\gamma = \gamma_a \cdot \gamma_h := \gamma_a(g_0 g_1 u)\gamma_h(z_0 z_1 v), \tag{37}$$

$$\gamma_0 = \gamma_a^0 \cdot \gamma_h^0 := \gamma_a^0(g_0 g_1 u)\gamma_h^0(z_0 z_1 v), \tag{38}$$

$$\Gamma := \gamma_a(g_1 u)\gamma_h(z_1 v), \Gamma_0 := \gamma_a^0(g_1 u)\gamma_h^0(z_1 v), \tag{39}$$

$$\Gamma^1 := \gamma_a(g_1)\gamma_h(z_1 v), \Gamma_0^1 := \gamma_a^0(g_1)\gamma_h^0(z_1 v). \tag{40}$$

The exit index (aka, the first exceed level index) is the most important factor to be fully analyzed because the decision making parameters including the marginal mean of $\tau_{\nu-1}$, A_ν and $A_{\nu-1}$ could be calculated easily once the exit index is explicitly determined from (18) and (37)–(40):

$$\mathbb{E}[\zeta^\nu] := L^1 + L^2 - L^3 \tag{41}$$

where

$$L^1 = \mathfrak{D}_{(u,v)}^{\left(\frac{M}{2}+B,\frac{M}{2}\right)}\left[\gamma_h^0(v) - \gamma_a^0(u)\gamma_h^0(v)\right], \tag{42}$$

$$L^2 = \mathfrak{D}_{(u,v)}^{\left(\frac{M}{2}+B,\frac{M}{2}\right)}\left[\frac{\zeta \cdot \gamma_a^0(u)\gamma_h^0(v)\gamma_h(v)}{1-\zeta\gamma_a(u)\gamma_h(v)}\right], \tag{43}$$

$$L^3 = \mathfrak{D}_{(u,v)}^{\left(\frac{M}{2}+B,\frac{M}{2}\right)}\left[\frac{\zeta \cdot \gamma_a^0(u)\gamma_h^0(v)\gamma_a(u)\gamma_h(v)}{1-\zeta\gamma_a(u)\gamma_h(v)}\right]. \tag{44}$$

Since the observation process has the memoryless properties, the inter-arrival time for observation is exponentially distributed and the functionals (37)–(40) could be reconstructed as follows:

$$\gamma_a^0(u) = \frac{\beta_a^0}{1-\alpha_a^0 \cdot u}, \gamma_a(u) = \frac{\beta_a}{1-\alpha_a \cdot u}, \gamma_h^0(v) = \frac{\beta_h^0}{1-\alpha_h^0 \cdot v}, \gamma_h(v) = \frac{\beta_h}{1-\alpha_h \cdot v}, \tag{45}$$

$$\beta_a^0 = \frac{1}{\left(1+\widetilde{\delta}_0\lambda_a\right)}, \alpha_a^0 = \frac{\widetilde{\delta}_0 \cdot \lambda_a}{\left(1+\widetilde{\delta}_0 \cdot \lambda_a\right)}, \beta_a = \frac{1}{\left(1+\widetilde{\delta} \cdot \lambda_a\right)}, \alpha_a = \frac{\widetilde{\delta}_0 \cdot \lambda_a}{\left(1+\widetilde{\delta} \cdot \lambda_a\right)}, \tag{46}$$

$$\beta_h^0 = \frac{1}{\left(1+\widetilde{\delta}_0 \cdot \lambda_h\right)}, \alpha_h^0 = \frac{\widetilde{\delta}_0 \cdot \lambda_h}{\left(1+\widetilde{\delta}_0 \cdot \lambda_h\right)}, \beta_h = \frac{1}{\left(1+\widetilde{\delta} \cdot \lambda_h\right)}, \alpha_h = \frac{\widetilde{\delta}_0 \cdot \lambda_h}{\left(1+\widetilde{\delta} \cdot \lambda_h\right)}, \tag{47}$$

where

$$\widetilde{\delta}_0 = \mathbb{E}[\tau_0], \widetilde{\delta} = \mathbb{E}[\Delta_k]. \tag{48}$$

From (42),

$$\begin{aligned} L^1 &= \mathfrak{D}_{(u,v)}^{\left(\frac{M}{2}+B,\frac{M}{2}\right)}\left[\gamma_h^0(v)\right] - \mathfrak{D}_{(u,v)}^{\left(\frac{M}{2}+B,\frac{M}{2}\right)}\left[\gamma_a^0(u)\gamma_h^0(v)\right] \\ &= \beta_h^0\left[\frac{1-\left(\alpha_h^0\right)^{\frac{M}{2}+1}}{1-\left(\alpha_h^0\right)}\right]\left(1-\beta_A^0\left[\frac{1-\left(\alpha_a^0\right)^{\frac{M}{2}+B+1}}{1-\left(\alpha_a^0\right)}\right]\right) \end{aligned} \tag{49}$$

and, from (43),

$$\begin{aligned} L^2 &= \mathfrak{D}_{(u,v)}^{\left(\frac{M}{2}+B,\frac{M}{2}\right)}\left[\frac{\zeta\cdot\gamma_a^0(u)\gamma_a^0(v)\gamma_h(v)}{1-\zeta\gamma_a(u)\gamma_h(v)}\right] \\ &= \textstyle\sum_{n\geq 0}\zeta^{n+1}\left\{\left(\beta_a^0\cdot(\beta a)^n\right)\cdot\sum_{j=0}^{\frac{M}{2}+B}\left\{(\alpha_a)^j\psi_{n-1}^a(j)\right\}\right\}\cdot\left\{\left(\beta_h^0\cdot(\beta_h)^{n+1}\right)\cdot\sum_{k=0}^{\frac{M}{2}}\left\{(\alpha_h)^k\psi_n^h(k)\right\}\right\} \end{aligned} \tag{50}$$

and, from (44),

$$\begin{aligned} L^3 &= (\zeta\beta_a^0\beta_h^0\beta_a\beta_h)\left[\textstyle\sum_{n\geq 0}(\zeta\beta_a\beta_h)^n\,\Xi_n^a\left(\frac{M}{2}+B\right)\cdot\Xi_n^h\left(\frac{M}{2}\right)\right] \\ &= \textstyle\sum_{n\geq 0}\zeta^{n+1}\left\{\left(\beta_a^0\cdot(\beta a)^{n+1}\right)\cdot\sum_{j=0}^{\frac{M}{2}+B}\left\{(\alpha_a)^j\psi_n^a(j)\right\}\right\}\cdot\left\{\left(\beta_h^0\cdot(\beta_h)^{n+1}\right)\cdot\sum_{k=0}^{\frac{M}{2}}\left\{(\alpha_h)^k\psi_n^h(k)\right\}\right\} \end{aligned} \tag{51}$$

where

$$\Xi_n^a(m)=\textstyle\sum_{j=0}^{m}\left\{(\alpha_a)^j\psi_n^a(j)\right\},\Xi_n^h(m)=\sum_{k=0}^{m}\left\{(\alpha_h)^k\psi_n^h(k)\right\}, \tag{52}$$

$$\psi_n^a(j)=\left(\sum_{i=0}^{j}\binom{n+i}{i}\left(\frac{\alpha_a^0}{\alpha_a}\right)^i\right),\psi_n^h(k)=\left(\sum_{i=0}^{k}\binom{n+i}{i}\left(\frac{\alpha_h^0}{\alpha_h}\right)^i\right). \tag{53}$$

From (49)–(53), the PGF of the exit index ν satisfies the following formula from the lemma in the BGG [18]:

$$\begin{aligned} \mathbb{E}[\zeta^\nu] &= \beta_h^0\left[\frac{1-\left(\alpha_h^0\right)^{\frac{M}{2}+1}}{1-\left(\alpha_h^0\right)}\right]\left(1-\beta_A^0\cdot\mathbb{E}\left[\frac{1-\left(\alpha_a^0\right)^{\frac{M}{2}+B+1}}{1-\left(\alpha_a^0\right)}\right]\right) \\ &+\textstyle\sum_{n\geq 0}\zeta^{n+1}\left[(\beta_a^0\beta_h^0\beta_h)(\beta_a\beta_h)^n\,\Xi_n^h\left(\frac{M}{2}\right)\cdot\mathbb{E}\left[\Xi_{n-1}^a\left(\frac{M}{2}+B\right)-\Xi_n^a\left(\frac{M}{2}+B\right)\beta_a\right]\right] \end{aligned} \tag{54}$$

and

$$\mathbb{E}[\nu]=\left(\beta_a^0\beta_h^0\beta_h\right)\textstyle\sum_{n\geq 1}n\left\{(\beta_a\beta_h)^n\,\Xi_{n-1}^h\left(\dfrac{M}{2}\right)\mathbb{E}\left[\Xi_{n-2}^a\left(\dfrac{M}{2}+B\right)-\Xi_{n-1}^a\left(\dfrac{M}{2}+B\right)\beta_a\right]\right\} \tag{55}$$

where

$$\Xi_{-1}^a(m)=0,\Xi_{-2}^a(m)=0,\Xi_{-1}^h(m)=0. \tag{56}$$

3.2. Marginal Means of EBIoV Decision Making Parameters

In the EBIoV network, conventional decision making parameters are ν, $\tau_{\nu-1}$, A_ν and $A_{\nu-1}$. Although all decision making parameters could be fully analyzed, using a marginal mean of each parameter is occasionally more efficient than finding the explicit PGFs of parameters. The marginal means of EBIoV decision making parameters could be found as follows:

$$\mathbb{E}[\nu]=\frac{\partial}{\partial\zeta}\mathbb{E}\left[\Phi\left(\zeta;\left\lceil\frac{M}{2}\right\rceil+B,\left\lceil\frac{M}{2}\right\rceil\right)\middle|B\right]\Bigg|_{(\zeta,g_0,g_1,z_0,z_1))\to 1}, \tag{57}$$

$$\mathbb{E}[\tau_{\nu-1}]=\mathbb{E}[\tau_0]+\mathbb{E}[\Delta_1](\mathbb{E}[\nu]-1), \tag{58}$$

$$\mathbb{E}[A_\nu]=\mathbb{E}[A_0]+\mathbb{E}[\nu-1]\mathbb{E}[X_k], \tag{59}$$

$$\mathbb{E}[A_{\nu-1}]=\mathbb{E}[A_0]+\mathbb{E}[\nu-2]\mathbb{E}[X_k]. \tag{60}$$

Recalling from (23), the probability of bursting a Blockchain network (i.e., an attacker wins a game) under the memoryless properties becomes a Poisson compound process:

$$q(s_h)=\textstyle\sum_{k>\frac{M}{2}}\mathbb{E}\left[\mathbf{1}_{\{A_\nu=k\}}\right],s_h=\{\text{“Regular”}\}, \tag{61}$$

or

$$q(s_h)=\mathbb{E}\left[\textstyle\sum_{k>\frac{M}{2}+B}\mathbb{E}\left[\mathbf{1}_{\{A_\nu=k\}}\right]\middle|B\right],s_h=\{\text{“Safety”}\}, \tag{62}$$

where

$$\mathbb{E}\left[\mathbf{1}_{\{A_\nu=k\}}\right]=\mathbb{E}\left[\frac{\lambda_a\tau_\nu}{k!}\cdot e^{-\lambda_a\tau_\nu}\right]. \tag{63}$$

4. The EBIoV Optimization Practice

This section deals with the BIoV network security optimization practice in a connected car. The strategy for protecting the EBIoV network is supporting additional nodes to give the less chance that an attacker catches blocks with false control requests. The example in this paper is targeting a connected car which consists 16 IoV components in a BIoV network (15 nodes from car parts and 1 node from a service center) and the estimated car value is around 50,000 USD (see Table 2).

Table 2. Initial conditions for the cost function.

Name	Value	Description
M	16 [Component]	Total number of the nodes in each BIoV network
V	50,000 [USD]	Average value of a BIoV enabled connected car
$c(n,\rho)$	$=25 \cdot n \cdot \rho$ [USD]	Cost for reserving nodes to avoid attacks per each car
$\mathbb{E}[A_0]$	2 [Blocks]	Total number of blocks that changed by an attacker at $\tau_0(=0)$
B_M	32 [Nodes]	Maximum number of honest nodes supported from the HQ

It is noted that the values on Table 2 are artificially made up for demonstration purposes only. Since the BGG adapted IoV network (EBIoV) has been analytically solved, finding optimal values of a cost function and calculating a probability distribution of a model are straight forward. However, software implementation by using a programming language is still required for solving a LP (Linear Programming) problem. Based on the above conditions, a LP model could be described as follows from (25) and (28):

$$\begin{array}{c}\text{Objective:}\\ G = min\ \mathfrak{S}(n,\rho)_{\text{Total}}\end{array} \tag{64}$$

$$\begin{array}{c}\text{Subject to:}\\ n \geq \frac{c_{(n,\rho)}}{V \cdot q^0 - c(n,\rho)};\end{array} \tag{65}$$

From (28), the total cost $\mathfrak{S}(n,\rho)_{Total}$ is as follows:

$$\mathfrak{S}(n,\rho)_{Total} = \Big\{c(n,\rho)\Big(1 - q^1_{(n,\rho)}\Big) + \Big(c(n,\rho) + V\Big)q^1_{(n,\rho)}\Big\}p_{A_{-1}} + Vq^0 \cdot (1 - p_{A_{-1}}) \tag{66}$$

where

$$\begin{aligned} p_{A_{-1}} &= \boldsymbol{P}\Big\{A_{\nu-1} < \tfrac{M}{2}\Big\} \simeq \boldsymbol{P}\Big\{A_\nu < \tfrac{M}{2} - \lambda_a\widetilde{\delta}\Big\} \\ &= \textstyle\sum_{k=0}^{\{\frac{M}{2}-\lambda_a\widetilde{\delta}\}} \left(\frac{\{\lambda_a(\widetilde{\delta_0}+\mathbb{E}[\nu-1]\widetilde{\delta})\}^k}{k!} \cdot e^{-\lambda_a(\widetilde{\delta_0}+\mathbb{E}[\nu-1]\widetilde{\delta})} \right), \end{aligned} \tag{67}$$

$$q^0 \simeq 1 - \textstyle\sum_{k=0}^{\frac{M}{2}} \left(\dfrac{\Big\{\lambda_a\Big(\widetilde{\delta_0} + \mathbb{E}[\nu-1]\widetilde{\delta}\Big)\Big\}^k}{k!} \cdot e^{-\lambda_a(\widetilde{\delta_0}+\mathbb{E}[\nu-1]\widetilde{\delta})} \right), \tag{68}$$

$$q^1_{(n,\rho)} = \textstyle\sum_{j=0}^{n} \qquad \sum_{\{k \geq \frac{M}{2}+B+j\}} \left(\dfrac{\lambda_a\Big(\widetilde{\delta_0} + \mathbb{E}[\nu-1]\widetilde{\delta}\Big)}{k!} \cdot e^{-\lambda_a(\widetilde{\delta}+\mathbb{E}[\nu-1]\widetilde{\delta})} \right) P_j, \tag{69}$$

$$P_j = \binom{n}{j}\rho^j(1-\rho)^{n-j}. \tag{70}$$

The total cost $\mathfrak{S}(n,\rho)_{\text{Total}}$ could be minimized by the given parameter set (n,ρ) and the parameter set (n^*,ρ^*) is the optimal combination of an acceptance rate and the number of total backup nodes which are supported from the HQ. The below illustration in Figure 3 is the conventional graph that shows the optimal result of the BGG based BIoV (EBIoV) network based on the given initial conditions in Table 2.

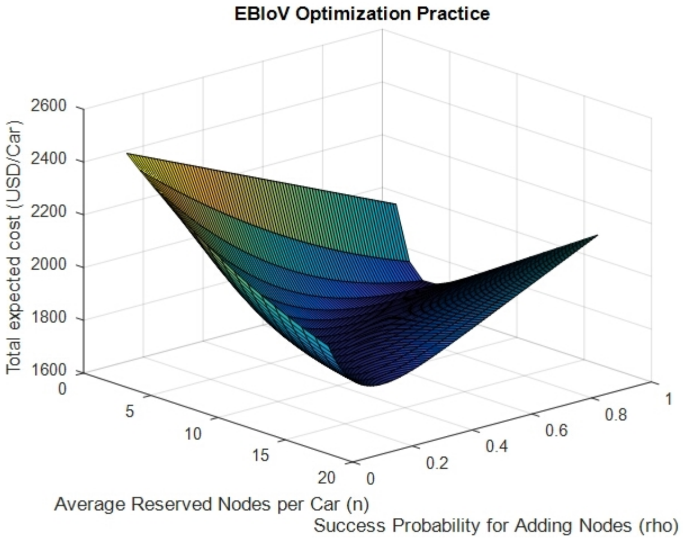

Figure 3. Optimization Example for the EBIoV.

It is noted that the total cost for reserving backup nodes should be more than the car value when an EBIoV network is burst. Hence, the limitation of the success probability for adding nodes is as follows:

$$\frac{V \cdot q^0}{c(n,\rho) \cdot (B_M - 1)} \leq 1, \tag{71}$$

where B_M is the maximum available reserved nodes per a connected car. According to this demonstration (based on Table 2), the optimal cost is 1700 USD (per a car) when the defender reserves 4 additional nodes per each car with the 82.6% acceptance rate for managing the risk from attackers (i.e., $n^* = 4$, $\rho^* = 0.826$). The moment of requesting the additional nodes will be the time $\tau_{\nu-1}$ when is one step prior to the moment when an attacker catches more than the half of whole blocks.

5. Conclusions

This paper establishes the enhanced Blockchain based IoV network architecture by bringing a theoretical model in stochastic modeling. The Enhanced Blockchain enabled Internet of Vehicles (EBIoV) is an advanced secure IoT network architecture for protecting a connected car from attackers. This new architecture has been designed for a decentralized network by adapting the Blockchain Governance Game (BGG) to improve the connected car security. The BGG is a mathematically proven game model to develop optimal defense strategies to protect systems from attackers. The practical case in the paper demonstrates how an EBIoV network could be implemented for connected car securities. The EBIoV network is the first research that applies a BGG model into the IoV security domain. The BGG model shall be extended to various Blockchain based cybersecurity areas including IoT security and secured decentralized service network design.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: There are no available data to be stated.

Acknowledgments: Special thanks to the Guest Editor, Nicu Bizon, who guides the author to submit the proper topic of the journal and also thankful to the referees whose comments are very constructive.

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

References

1. Rouse M. Internet of Vehicles. 2018. Available: https://whatis.techtarget.com/definition/Internet-of-Vehicles (accessed on 1 May 2019).
2. Kim S.; Shrestha, R. Internet of Vehicles, Vehicular Social Networks, and Cybersecurity. In *Automotive Cyber Security*; Springer: Singapore, 2020; pp. 149–181.
3. 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.
4. 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, Germany, 2018; pp. 137–157.
5. 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]
6. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; In Kim, D.; Zhao, J. Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]
7. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [CrossRef]
8. Steger, M.; Dorri, A.; Kanhere, S.S.; Römer, K.; Jurdak, R.; Karner, M. Secure wireless automotive software updates using blockchains: A proof of concept. In *Advanced Microsystems for Automotive Applications*; Springer: Cham, Germany, 2017; pp. 137–149.
9. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57. [CrossRef]
10. Blockchain News. Available online: https://www.ccn.com/volkswagen-seeks-patent-for-inter-vehicular-blockchain-communications-system/ (accessed on 1 May 2019).
11. Haig, S. Ford to Use Cryptocurrency for Inter-Vehicle Communication System. 2018. Available online: https://news.bitcoin.com/ford-cryptocurrency-inter-vehicle-communication-system/ (accessed on 1 May 2019).
12. Conoscenti, M.; Vetrò, 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.
13. Restuccia, F. Blockchain for the Internet of Things: Present and Future. Available online: https://arxiv.org/abs/1903.07448 (accessed on 1 May 2019).
14. Jesus, E.F.; Chicarino, V.R.L.; de Albuquerque, C.V.N.; Rocha, A.A.D.A. Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. *Secur. Commun. Netw.* **2018**, *2018*, 9675050. [CrossRef]
15. Kim, S.-K.; Yeun, C.Y.; Damiani, E.; Al-Hammadi, Y.; Lo, N.-W., New Blockchain Adoptation For Automotive Security by Using Systematic Innovation. In Proceedings of the 2019 IEEE Transportation Electrification Conference and Expo Asia-Pacific, Jeju, Korea, 8–10 May 2019; pp. 1–4.
16. Baker, J.; Edge Computing—The New Frontier of the Web. Available online: https://hackernoon.com/edge-computing-a-beginners-guide-8976b6886481 (accessed on 1 May 2019).
17. ERPINNEW. Fog Computing vs Edge Computing. 2017. Available online: https://erpinnews.com/fog-computing-vs-edge-computing (accessed on 1 May 2019).
18. Kim, S.-K. Blockchain Governance Game. *Comput. Ind. Eng.* **2019**, *136*, 373–380. [CrossRef]
19. Kim, S.-K. Strategic Alliance for Blockchain Governance Game. *Probab. Eng. Inf. Sci.* **2020**, 1–17. doi:10.1017/s0269964820000406. [CrossRef]
20. Hammoud, A.; Sami, H.; Mourad, A.; Otrok, H.; Mizouni, R.; Bentahar, J. AI, Blockchain, and Vehicular Edge Computing for Smart and Secure IoV: Challenges and Directions. *IEEE Internet Things Mag.* **2020**, *3*, 68–73. [CrossRef]
21. Narayanan, A.; Clar, J. Bitcoin's Academic Pedigree. *Mag. Commun. ACM* **2017**, *60*, 36–45. [CrossRef]
22. Weiss, M.; Corsi, E. *Bitfury: Blockchain for Government*; HBP Case 9—818-031; Harvard University: Cambridge, MA, USA, 2018; 29p.
23. Jones, M. Blockchain for Automotive: Spare Parts and Warranty. 2017. Available online: https://www.ibm.com/blogs/internet-of-things/iot-Blockchain-automotive-industry/ (accessed on 1 May 2019)
24. Bonomi, F.; Milito, R. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012; pp. 13–16.
25. Liu, Z.; Luong, N.C.; A Survey on Applications of Game Theory in Blockchain. *arXiv* **2019**, arXiv:1902.10865.
26. Micali, S.; Rabin, M.; Wang, W.; Niyato, D.; Wang, P.; Liang, Y.C.; In Kim, D. Verifiable random functions. In Proceedings of the 40th IEEE Symposium on Foundations of Computer Science, New York, NY, USA, 17–19 October 1999; pp. 120–130.
27. Dodis, Y.; Yampolskiy, A. A Verifiable Random Function with Short Proofs and Keys. In *Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3386, pp. 416–431.
28. Gorbunov, S. Algorand Releases First Open-Source Code: Verifiable Random Function. 2018. Available online: https://medium.com/algorand/ (accessed on 1 May 2019).

29. Zhao, W. MIT Professor's Blockchain Protocol Nets 62 Million in New Funding. 2018. Available online: https://www.coindesk.com/mit-professors-Blockchain-protocol-nets-62-million-in-new-funding (accessed on 1 May 2019).
30. Dshalalow, J.H. *First Excess Level Process, Advances in Queueing*; CRC Press: Boca Raton, FL, USA, 1995; pp. 244–261.
31. Dshalalow, J.H.; Ke, H.-J. Layers of noncooperative games. *Nonlinear Anal.* **2009**, *71*, 283–291. [CrossRef]