sustainability

Article

A Scalable IoT Protocol via an Efficient DAG-based Distributed Ledger Consensus

Bumho Son [1], Jaewook Lee [1] and Huisu Jang [2,*]

[1] Department of Industrial Engineering, Seoul National University, Seoul 08826, Korea; andymogul@snu.ac.kr (B.S.); jaewook@snu.ac.kr (J.L.)

[2] School of Finance, Soongsil University, 369 Sangdo-ro, Dongjak-gu, Seoul 06978, Korea

* Correspondence: yej523@ssu.ac.kr; Tel.: +82-10-3872-7798

Received:15 January 2020; Accepted: 14 February 2020; Published: 18 February 2020

Abstract: The Internet of Things (IoT) suffers from various security vulnerabilities. The use of blockchain technology can help resolve these vulnerabilities, but some practical problems in terms of scalability continue to hinder the adaption of blockchain for application in the IoT. The directed acyclic graph (DAG)-based Tangle model proposed by the IOTA Foundation aims to avoid transaction fees by employing a different protocol from that used in the blockchain. This model uses the Markov chain Monte Carlo (MCMC) algorithm to update a distributed ledger. However, concerns about centralization by the coordinator nodes remain. Additionally, the economic incentive to choose the algorithm is insufficient. The present study proposes a light and efficient distributed ledger update algorithm that regards only the subtangle of each step by considering the Bayesian inference. Experimental results have confirmed that the performance of the proposed methodology is similar to that of the existing methodology, and the proposed methodology enables a faster computation time. It also provides the same resistance to possible attacks, and for the same reasons, as does the MCMC algorithm.

Keywords: blockchain; cryptocurrency; MCMC algorithm; Bayesian inference; distributed system; IoT system

1. Introduction

The Internet of Things (IoT) is currently used in various fields and is expected to play a more important role in our lives [1,2]. However, security issues are increasing because of the heterogeneity and large number of objects in the IoT system [3,4]. Attacks such as the Denial of Service (DoS) can be made on the applications layer, the network layer, and the system level since smart devices constantly interact with various systems that control them [5]. These possible attacks can provide unlimited access to personal information or disruptions in service [6]. Therefore, designing an IoT system that can guarantee a high level of security is a critical priority.

Classic blockchain structures like Bitcoin and Ethereum solve a similar security problem by constructing a Proof-of-Work (PoW) consensus between users. Recently, several studies have shown that introducing the blockchain structure into the IoT system can improve the security and efficiency of the IoT network [7]. For instance, Huh et al. [8] and Zhang and Wen [9] proposed using a smart contract on the blockchain to control IoT devices and facilitate e-business transactions.

However, there are some practical problems to be solved before the blockchain can be used in this way. IoT differs from other blockchain-related fields because of its small devices [10]. IoT nodes continuously generate a large amount of data and send it through the network. Thus, it becomes necessary for devices with small resources and capacities to utilize the entire blockchain (which is one of the blockchain's main properties) and actively issue transactions on the chain [11]. The most popular blockchain platforms, like Bitcoin and Ethereum, cannot handle such a high volume of transactions because their transaction processing ability is directly affected by the block size [12]. Increasing the block size can lead to an increase in the processed transactions per second, but it also causes a data burden on all nodes.

The most widely known solution for these problems has been provided by Popov [13]. Popov [13] has proposed the Tangle for the cryptocurrency IOTA, which is a directed acyclic graph (DAG)-based distributed ledger, in which the group issuing transactions is identical to the group confirming transactions; this helps address the high transaction fee problem in micropayments. The DAG-based blockchain offers a higher level of scalability by creating blocks that do not contain whole transactions [14]. However, it still has some limitations.

The Tangle's consensus algorithm operates by issuing a new transaction to verify two other existing transactions that have never been previously verified, which are referred to as "tips". Currently, a light node in the Tangle receives the results of the Markov chain Monte Carlo (MCMC)-based tip selection algorithm from a node operated by the Foundation, known as a "coordinator," by calling the tip selection API to select the tips to approve. To choose the tips, a coordinator node considers a reliable transaction (a "milestone") issued by a coordinator node to implement an MCMC algorithm. However, the presence of transactions with a trustworthy status granted by the Foundation's coordinator node gives rise to a centralization issue with regard to IOTA. Additionally, there is no reason to enforce a suggested tip selection method for general users.

Popov et al. [15] separated nodes complying with the default tip selection algorithm from the selfish nodes pursuing their own profits. However, it is plausible that every node behaves "selfishly" in a way that minimizes its cost. General participants want their transactions' cumulative confirmation to become sufficiently large in the Tangle. Therefore, they may want to develop a strategy that allows their transaction weight to accumulate quickly. Hence, at this point, the only strategy they can take is to choose tips that can quickly increase their cumulative weight.

As seen from the above discussion, there is a need to present the tip selection algorithm, which can be voluntarily followed by participating nodes. In other words, all nodes should be able to maximize their interests by following the algorithm. Our research focuses on an efficient tip selection algorithm that can be adapted to the current IoT system consisting of devices with a computational limit.

In the following discussion, we propose a more efficient and light tip selection algorithm that allows users to maximize their confirmation probability by selecting adequate tips that can be applied to limited capacity IoT systems. In addition, we discuss the resistance of the proposed algorithm to possible attack scenarios, and finally present recommendations for future research.

2. Related Works

2.1. Blockchain Adaptation for IoT

Starting from the peer-to-peer payment system, blockchain is gaining interest to be adopted in various fields because of its transparency and ability to mainatain privacy [16]. Many researches have investigated the possibility of applying the blockchain system in many fields, including energy systems, IoT, and voting. Wu and Tran [17], Yang et al. [18] showed the possible attempts for applying blockchain to energy systems and claimed that the blockchain can be the solution for managing distributed energy network. Kshetri and Voas [19] proposed that using cryptocurrency coin as voting mean can make e-voting system. The blockchain system enables security of voting by authorizing that no vote has been changed and that each vote belongs to proper person. These works have shown blockchain, which can gain trust by its decentralized structure, can be applied to almost every field which needs distributed system.

The blockchain is well known for its ability to solve security and privacy issues. However, the authors of Dorri et al. [10] suggest that there still exist several challenges to be addressed before the blockchain can be adapted to the IoT. First, IoT devices do not have enough resources and capacity to maintain the classic blockchain. Second, the current blockchain technology's block creation process is too slow to handle transactions between IoT devices (a scalability problem).

To handle the first issue, Dorri et al. [10], Dorri et al. [20], Yang et al. [21] proposed architectures that enable high-computational objects besides IoT devices to maintain the blockchain. Dorri et al. [10] and Dorri et al. [20] suggest a cluster-based blockchain to make cluster heads with a sufficient calculation ability to handle the blockchain in the case of a smart home. Similarly, Yang et al. [21] used a blockchain between roadside units (RSUs) to handle implementation in a vehicular network system.

Since the most crucial benefit of adapting the blockchain to the IoT is security, some loss of scalability will be necessary; although minimizing the increasing processing time is still a critical issue. Blockchain's scalability problem comes from the trade-off between the block creation speed and the security of the chain [22]. The greedy heaviest-observed sub-tree (GHOST) protocol suggests that the whole chain maintains several uncle blocks that fail to generate a new block because they take a longer time do so compared with the first block maker. The GHOST protocol considers the blockchain as a tree. It can be used as a solution to the network security problem, which is caused by the faster block generation time leading to a higher stale rate [23]. The idea of allowing a block to designate uncle blocks is also applied in constructing blockDAG structure SPECTRE and Conflux [24], where blockDAG structure is a DAG that allows each block to direct more than two blocks. The SPECTRE protocol constructs the set of accepted transactions by making every block vote for deciding which block defeats another between two conflicting blocks. It enables high transaction throughput and security level at the same time. However, this voting system does not guarantee linear order of blocks. The PHANTOM protocol offers linear order of blocks by using a greedy algorithm to select honest blocks among blockDAG [25]. Confirmed linear order of blocks allows functioning of smart contracts on the PHANTOM system, but only can provide smaller transaction throughput than the SPECTRE protocol because of its need to reach consensus.

Other DAG-based cryptocurrencies like DagCoin, Byteball, Raiblock, and IOTA constructed DAG with transactions, not blocks. Raiblock made each user maintain their own DAG without one global chain, while Dagcoin/Byteball and IOTA constructed one global transaction DAG. They proposed various consensus as a way to increase the security of the DAG. Dagcoin/Byteball identified main chain relying on witnesses, the trustable honest nodes, to achieve consensus [26,27]. IOTA achieved consensus through the concept of cumulative weight of each transactions and Markov Chain Monte Carlo (MCMC) algorithm while Raiblock used balance-weighted voting system for conflicting transactions [13,28]. Even though the IOTA Foundation's Tangle structure is designed for the IoT system directly, this structure still suffers from some drawbacks with regard to widespread use in terms of scalability and centralization.

2.2. IOTA and the Tangle

Bitcoin technology entails the provision of an incentive to "miners" to confirm transactions on the block. This incentive is called a transaction fee, and is applied on every transaction; in some situations, the transaction fee may be larger than the original transaction size. The imposition of the transactions fee poses significant problems for the IoT industry, since the IoT relies on rapid micropayments. To address these concerns, the authors of Popov [13] designed a cryptocurrency ledger named IOTA, whose central concept is the use of a DAG-based ledger called the Tangle, instead of the blockchain, to record transactions.

The Tangle differs from the existing blockchain in two ways. It uses a structure where nodes, instead of the network's participators, represent transactions. In blockchain terminology, the Tangle is made up of blocks that only contain one transaction each, which we now refer to as "sites". When a new transaction is issued, it has to solve a cryptographic hash puzzle similar to that of Bitcoin blockchain. Subsequently, it approves two tips, which are previous transactions that have never been approved by other transactions. The transaction checks if two approved transactions conflict by examining the Tangle history, and if it discovers a conflict between them, it will not approve those transactions.

The approval becomes the edge of the Tangle. When site i approves site j, it becomes a directed edge $i \rightarrow j$ in the Tangle. In this way, every user who issues a transaction automatically contributes to the Tangle's security.

Direct and indirect approval are defined as follows: if there is an edge $i \rightarrow j$, site i directly approves site j. If there is an edge $i \rightarrow k \rightarrow j$, i indirectly approves j. As a transaction gets more direct or indirect approvals, it achieves a higher level of confidence. Popov [13] showed that if a large number of nodes follow a particular reference rule, other nodes will be in Nash equilibrium in following the same reference rule. This kind of assumption makes sense in the IoT system where nodes have similar pre-installed firmware.

Each transaction's weight determines its importance in the Tangle. The Tangle defines a transaction's cumulative weight as the sum of the weights of other nodes that directly or indirectly approve the transaction, including itself. In practice, every node's weight is 1. Therefore, the number of nodes that directly or indirectly approve the node represents the cumulative weight. As such, a transaction's cumulative weight will grow with speed λw where w is the mean weight of proven transactions.

One of the main concerns of blockchain security is the malicious node issue. For the Tangle, parasite chains that attempt to approve its double-spending transaction can exist. In this scenario, the parasite chain would reference the main Tangle to obtain a high score. Additionally, it might generate numerous tips to force the new honest sites to reference its tips. The use of a tip selection algorithm utilizing MCMC algorithm has been proposed as one way to avoid this issue. The MCMC algorithm consists of four steps. First, the new site considers the subTangle between the time interval $[W, 2W]$, where W is a sufficiently large number. Second, it randomly selects N particles in that interval. Third, it progresses the random walk beginning from each of the particles. In this random walk, the algorithm can only progress to the sites that have approved its transactions. Finally, it progresses the random walk until it ends up in tips. The two tips that have arrived first will be the two tips that the new site approves. However, to avoid the lazy tip issue, any tips that have arrived too quickly are discarded. Through the random walk, the transition probability is defined as below average. If y approves x ($y \rightarrow x$), the transition probability from x to y can be expressed as follows:

$$P_{xy} = exp(-\alpha(H_x - H_y))(\sum_{z:z \rightarrow x} exp(-\alpha(H_x - H_z)))^{-1} \tag{1}$$

where H_x denotes the cumulative weight of site x.

Using this tip selection algorithm, the parasite chain's tips will not be selected as approved tips since its sites have less cumulative weight than the main Tangle (because the parasite chain references the main Tangle and the main Tangle does not).

However, the current IOTA system's stability relies on a particular type of node, called the coordinator node. The IOTA Foundation authorizes this type of node and issues the transaction, which is called a milestone. The above tip selection algorithm starts from the milestone while every other node in the Tangle recognizes the milestone (and not the collection of random sites described above) as a valid transaction. Therefore, IOTA's system is highly centralized, which means that an attack on the coordinator node can turn into an attack on the whole system. Furthermore, the tip selection algorithm would take a longer time as the Tangle grows, which will cause a scalability problem.

The above studies tried to adapt blockchain systems to the IoT. However, these studies cannot provide a sufficient level of scalability for the IoT system. For fast transaction processing, we need a new algorithm that is appropriate for the IoT.

3. Proposed Algorithm

Before we make a statement of the proposed method, we would give a brief description of Bayesian inference. Bayesian inference, a kind of statistical inference, uses the Bayes' rule to update the unknown objective probability density as more evidence or information becomes available. Apart from being widely applied in the fields of science, engineering, and philosophy, Bayesian inference has been employed especially in the dynamic analysis of data sequences [29–32].

In Bayesian inference, the posterior distribution can be deduced from two antecedent probabilities, a prior and likelihood, according to Bayes' rule expressed as

$$P(H|E) = \frac{P(E|H)P(H)}{P(E)}, \tag{2}$$

where H means any hypothesis affected by the data, E, which is the evidence corresponding to new data; $P(H|E)$ is a probability that we ultimately want to know after the evidence E is observed; $P(E|H)$ is the probability of observing the evidence when the hypothesis or the model is given; and $P(H)$ is a prior density, that is, a probability of the objective hypothesis or model before the evidence is given.

In this study, we also restrict the network structure as a Tangle of the IOTA and develop the argument by accepting the underlying assumptions and related definitions in IOTA's white paper. We approximate a discrete probability density for the existing tip set, as the original tip selection algorithm does [13]. The difference from the conventional algorithm is that we project the probabilistic distribution of the tip set into the space of the node set consisting of nodes issued on a site in the subtangle. The reason why the cumulative weight of the node selects the tip set is that a node with a high cumulative weight would want to maintain its high cumulative weight by carrying out confirmations quickly. We describe the proposed algorithm below.

1 If the node participates in the network for the first time, two of the currently available tips are randomly selected.
2 In subsequent tip selections, each node selects a new tip set from the prior density based on the precedence subtangle, wherein all sites are directly or indirectly confirmed by the tip set recently confirmed by each node.
3 Based on the updated subtangle, the discrete likelihood distribution can be suggested for the nodes issuing a transaction in the updated subtangle. The value of the likelihood distribution of each node should be approximated in order to reflect the principle that malicious nodes have a smaller probability than typical participant nodes based on the already known information of the preceding subtangle.
4 The posterior distribution is updated given the likelihood and a prior distribution.

While the existing MCMC methodology discusses the probability density over the tips itself, the current study deals with the probability density over the nodes that issued sites. Hereafter, we shall update the probability density only for the moments when the user should select the tips and the moment at which a transaction is issued. For the sake of brevity, the moment of issuing the t-th transaction and selecting the t-th tips is referred to as the t-th phase. We address the modeling of the discrete posterior density transition over time by deploying the Bayes' rule. In other words, a discrete posterior density at the t-th phase is determined by the t-th prior and the t-th likelihood distribution, which is created based on the t-th subtangle consisting of sites approved by the tips selected at the t-th phase.

The posterior distribution obtained in the immediately preceding phase becomes the prior distribution at the present phase. Using the Markov chain structure, it is assumed that the present prior distribution contains cumulative information according to the subtangle at each precedent phase. Before becoming the t-th state, a node has a discrete posterior distribution for the nodes and participants in the network based on the $(t-1)$-th subtangle. Assuming that the set of participating nodes known by this node at the $(t-1)$-th phase is K, the equation below is established,

$$\sum_{i \in K} p_i = 1, \quad i \in K, \tag{3}$$

where p_i is the prior density of the i-th node.

Before updating the posterior distribution, we first propose a probability distribution for choosing tips in the t-th phase based on the t-th prior distribution. We defined an additional set M and K' at the t-th phase. Set M contains new nodes, which are not contained in the set K and newly appear in the t-th subtangle. Set K has a subset K' which contains the nodes excluded from the tip issuing node set at the t-th phase. Each k, k' and m means the number of elements in the set K, K' and M.

Based on the above assumptions and Equation (3), we can derive a probability distribution for tip selection as follows,

$$p_x^{tip} = \begin{cases} \frac{k-k'}{k-k'+m} \frac{p_x}{\sum_{i \in K \setminus K'} p_i}, & x \in K \setminus K' \\ \frac{1}{k-k'+m}, & x \in M \end{cases} \tag{4}$$

In the t-th phase, the new information we can obtain is the subtangle created after selecting a set of tips based on the probability distribution given above. We need an appropriate likelihood distribution to estimate the posterior probability density for the union of the known set of nodes K and the set of new nodes L from the subtangle. For the sake of the argument, we classify the entire node set into three subset to propose a proper likelihood distribution. The characteristics of each subset and the estimates of the likelihood distribution are described in each subsection.

3.1. ***Set A***: *Only Included in the Prior Distribution*

Since the set A consists of nodes that are included in the prior distribution but are excluded when forming the subtangle, the new information relevant to set A can not be obtained from the subtangle. Therefore, the likelihood distribution is obtained from the average cumulative weight held in the prior density in a manner similar to the existing tangle. The nodes included in set A can be considered as two cases as follows: the number of issued transactions, and the average cumulative weight are small or large nodes. The second case is more likely to be a malicious, intentional node. Despite the fact that a node issued a large number of transactions, if a node can only be observed in the restricted subtangle, it is likely that the node intentionally attempted to be malicious. Therefore, it is reasonable to provide a likelihood distribution in inverse proportion to the average cumulative weight. We have proposed the following likelihood distribution for set A, taking into account the case of the other subsets:

$$p_x^A = \frac{N_A}{N_A + N_B + N_C} \frac{exp(-\alpha_1 w_x)}{\sum_{i \in A} exp(-\alpha_1 w_i)}, \quad x \in A, \tag{5}$$

where N_S is the number of elements in set S, w_x is the average cumulative weight of node i based on the $(t-1)$-th subtangle, and α_1 is the parameter for the distribution. Sets B and C are defined in each subsequent subsection.

3.2. ***Set B***: *Both Included in the Prior Distribution and the t-th Subtangle*

Set B covers nodes that are observed in both consecutive phases. When a normal node is observed in successive phases, it is assumed that transactions are issued, on average, λ times between the two phases depending on the Poisson process assumption. It can be expected that the average cumulative weight of a typical node will increase by about λ between the two consecutive phases.

Consider the case where the average cumulative weight change is noticeably larger than lambda. Regardless of the direction of the change, this means that the corresponding node is unusual. For example, an abnormal average cumulative weight increase may be a signal that the node has started a malicious attack. A remarkable reduction in the average cumulative weight may also be a signal that the $(t-1)$-th subtangle contained the parasite tangle of a malicious node. In other words, it is reasonable that a likelihood distribution is presented based on the extreme change in the average cumulative weight. With our proposed algorithm, we employ a step function for implementing the corresponding likelihood distribution. If the absolute value of the difference of the node's average cumulative weight between the $(t-1)$ and t-th phases is greater than the sum of λ

and the parameter α_3, then the likelihood that a transaction generated by the node will be selected as a tip is reduced. Therefore, the likelihood distribution of set B can be approximated as follows:

$$p_x^B = \begin{cases} \frac{n_1}{n_1+n_2} p, \quad if & |w_x^{(t-1)} - w_x^t| \geq \lambda + \alpha_3 \\ \frac{n_2}{n_1+n_2}(1-p), \quad if & |w_x^{(t-1)} - w_x^t| < \lambda + \alpha_3, \end{cases} \tag{6}$$

n_1 is the number of nodes satisfying the first condition, and n_2 is the number of nodes satisfying the second condition in set B, p is the threshold probability, and α_3 is the parameter for the model.

3.3. ***Set C**: Only Included in the t-th Subtangle*

Set C consists of newly observed nodes in the t-th subtangle. In other words, it is possible to estimate the likelihood distribution with the same principle as in the case of the set A. The only difference between the two cases is that set C uses node information of the t-th subtangle unlike set A, which investigates the node information of the $(t-1)$-th subtangle.

$$p_x^C = \frac{N_C}{N_A + N_B + N_C} \frac{exp(-\alpha_3 w_x)}{\sum_{i \in C} exp(-\alpha_1 w_i)}, \quad x \in C, \tag{7}$$

where N_S is the number of elements in set S, w_x is the average cumulative weight of node i based on the t-th subtangle, and α_3 is the parameter for the distribution.

Assuming that a sincere node and a malicious node each issued a total of n transactions, the transaction issued by the sincere one would cumulate its weight independently from other sincere participants. After the adaptation period, the cumulative weight of each transaction issued by a sincere node would increase linearly and assume that the value is w. Under the same conditions, all the n transactions issued by a malicious node would inevitably have different cumulative weights that are dependent on each other's transactions. In order to hide its malicious intent, a node must approve only its transactions. In this case, the cumulative weight of the first issued transaction is w, the cumulative weight of the following transactions would be bound to $w-1, w-2, w-3,$ etc.

4. Empirical Study

In order to evaluate the stability of the system for each method, we performed simulation studies where λ is 20 or 50, and the number of iterations is 1000, and 3000, respectively.

Figure 1 shows that the cumulative weight increases with the slope of the lambda without any difference for each methodology. Figure 1 also confirms that each methodology reliably increases the cumulative weight of any transaction under usual circumstances and that the slope depends on the volume of transactions issued on average per unit of time. There exists a remarkable difference in the average cumulative weight between the empirical result and the original paper [13]. While Popov [13] have mentioned that there is an adaptation period in which a cumulative weight is exponentially increased, this simulation study confirms that the cumulative weight is linearly increased according to the number of iterations.

The simulation results show that each methodology's number of tips is concentrated around a λ, which is slightly different from Popov [13]'s assumption the number of tips remains roughly stationary in time and in concentrated around a number $L_0 = 2\lambda h$. We have also found that the number of tips of the proposed algorithm becomes roughly stationary in time around the λ, as in other algorithms. Figure 2 presents the number of tips according to λ.

Figure 3 shows the elapsed time of each iteration for the MCMC and the proposed algorithm, respectively. Unlike the MCMC algorithm of extracting particles from the main tangle and performing MCMC simulations, the proposed method considers only the subtangle calculated at each time step, so that the elapsed time of each step is shorter than the MCMC algorithm.

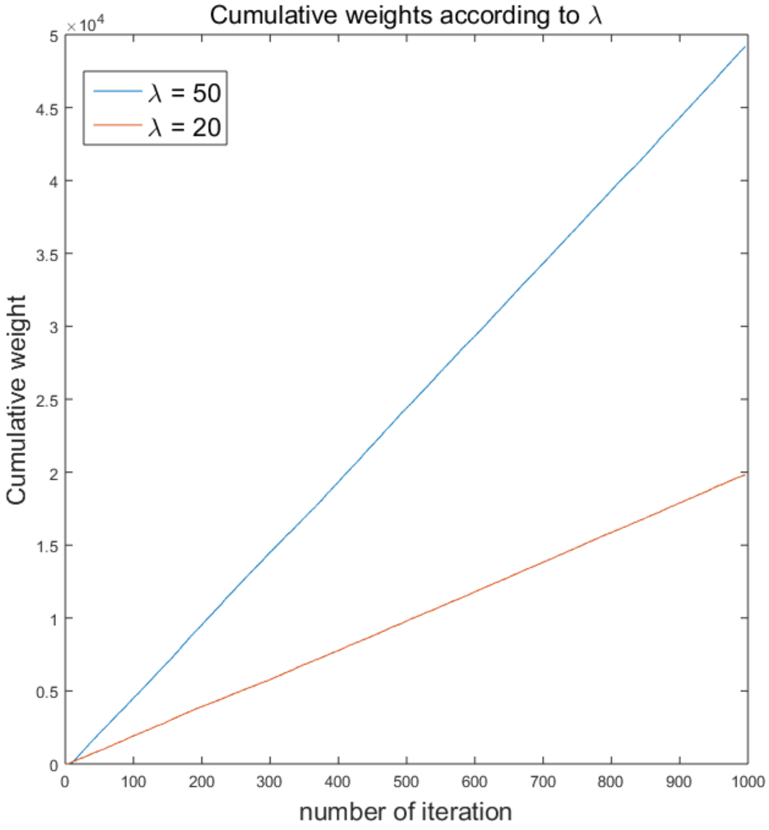

Figure 1. Cumulative weights according to λ with random selection algorithm.

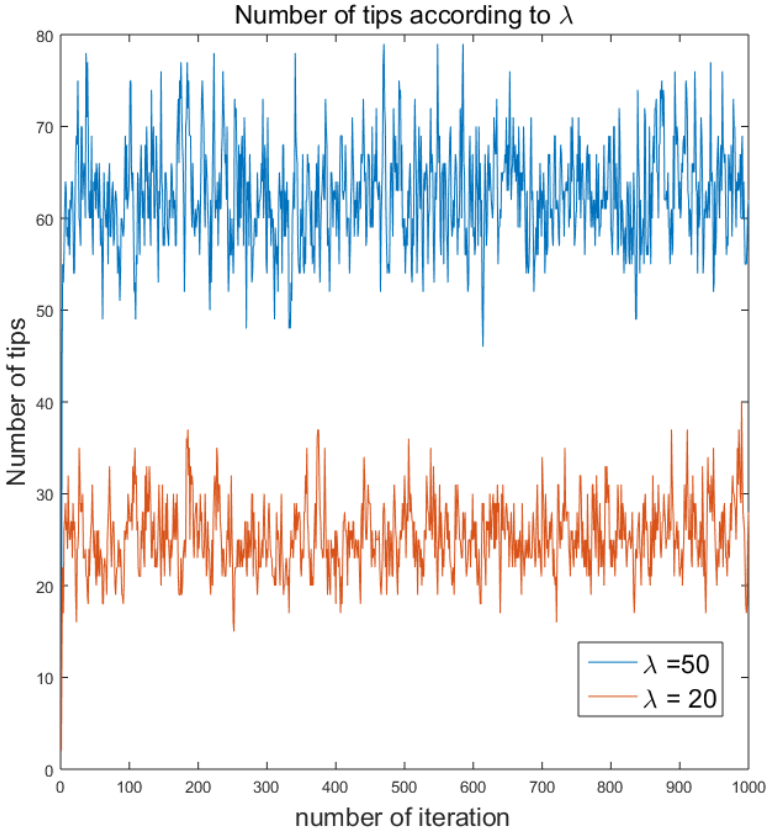

Figure 2. Number of tips according to λ with random selection algorithm.

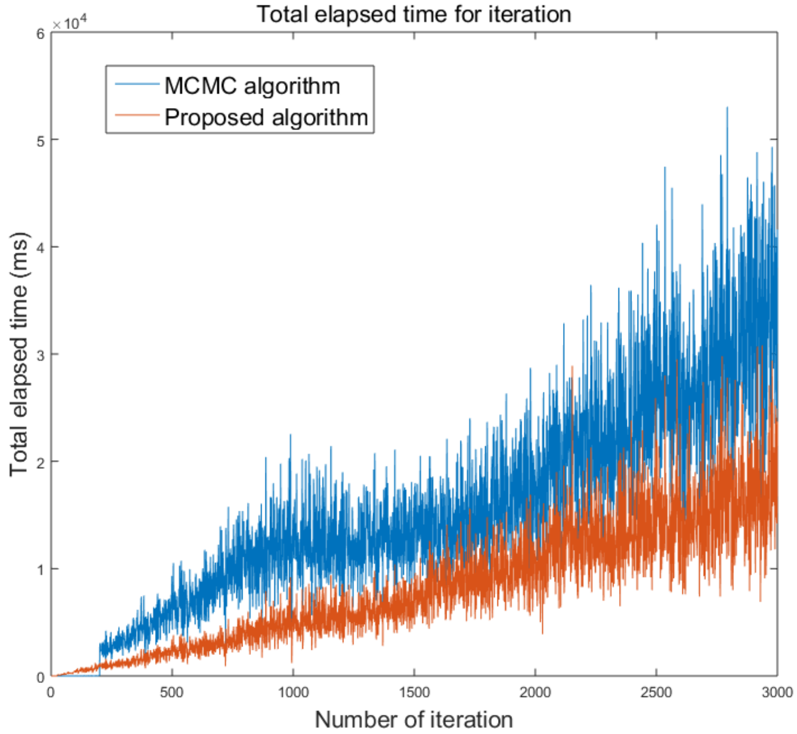

Figure 3. Total elapsed time for iteration with two algorithms.

The proposed and MCMC algorithms have the same principle to prevent malicious node attacks. Both methods attempt to minimize the probability of attack by reducing the probability that a malicious node is selected as a tip. A significant difference between the two algorithms is revealed in the way by which a node's maliciousness is determined. The two algorithms consider different criteria to determine whether a node is malicious. While MCMC algorithm determines site's maliciousness by only considering the cumulative weight, the proposed algorithm also considers the change in the cumulative weight. The proposed algorithm estimates the likelihood distribution of nodes included only in prior distribution, vice versa, by average cumulative weight which is similar to MCMC algorithm. In the case of nodes both included in the prior distribution and the t-th subtangle, the proposed methodology evaluates the probability of the node being malicious based on the sudden increase or decrease in the cumulative weight of any node (i.e., a large variability in the cumulative weight). Given the fact that many types of network attacks are made through the sudden appearance of specific parasite subtangles, the proposed algorithm attempts to impose a penalty, by using Bayesian inference, for the sudden volatility of cumulative weight over time. For instance, if a parasite subtangle appears and disappears between consecutive states, the proposed algorithm in the previous section will exponentially decrease the probability of selecting that node as a tip. Therefore, the proposed algorithm is also resistant to possible attack scenarios for the same reasons discussed in [13].

The main advantage of the proposed methodology is that it is light and efficient. Each node is supposed to retain only its subtangle at each time step and the advanced posterior (or prior) information according to the time. Each node needs to refer to the information of the subtangle to confirm the validity of the transactions directly or indirectly approved by the selected tips to issue a transaction. In other words, the subtangle's information is essential for every time step, irrespective of the proposed algorithm. Thus, the proposed algorithm is expected to help mitigate the problem of centralization issues by coordinators present in the tangle because the proposed algorithm is very light and efficient when utilizing information.

5. Conclusions

The proposed algorithm constructs the entire network by calculating the probability that the network participant node is malicious, and we are currently studying with a consensus algorithm suitable for this ledger expansion method. This algorithm can also be applied to various scenarios considered in the IoT system. For example, it is possible to utilize the proposed algorithm as a fast and efficient storage method for an image data stream that requires continuous data transmission, such as closed-circuit television (CCTV) data. The development of these algorithms is expected to contribute to improving IoT systems' future security.

Author Contributions: Methodology, H.J.; Project administration, J.L.; Writing–original draft, B.S.; Writing–review and editing, B.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Research Foundation of Korea Grant through the Korean Government (MEST) under Grant No. 2019R1F1A1058061 and No. 2019R1A2C2002358

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Singh, S.; Singh, N. Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In Proceedings of the 2015 IEEE International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, India, 8–10 October 2015; pp. 1577–1581.
2. Wu, J.; Feng, Y.; Sun, P. Sensor fusion for recognition of activities of daily living. *Sensors* **2018**, *18*, 4029. [CrossRef] [PubMed]
3. Zhang, Z.K.; Cho, M.C.Y.; Wang, C.W.; Hsu, C.W.; Chen, C.K.; Shieh, S. IoT security: ongoing challenges and research opportunities. In Proceedings of the 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA), Matsue, Japan, 17–19 November 2014; pp. 230–234.
4. Farooq, M.U.; Waseem, M.; Khairi, A.; Mazhar, S. A critical analysis on the security concerns of internet of things (IoT). *Int. J. Comput. Appl.* **2015**, *111*, 1–6.
5. Amoozadeh, M.; Raghuramu, A.; Chuah, C.N.; Ghosal, D.; Zhang, H.M.; Rowe, J.; Levitt, K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132. [CrossRef]
6. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
7. Casado-Vara, R.; Chamoso, P.; De la Prieta, F.; Prieto, J.; Corchado, J.M. Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management. *Inf. Fusion* **2019**, *49*, 227–239. [CrossRef]
8. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th IEEE International Conference on Advanced Communication Technology (ICACT), Bongpyeong, South Korea, 19–22 February 2017; pp. 464–467.
9. Zhang, Y.; Wen, J. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 983–994. [CrossRef]
10. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an optimized blockchain for IoT. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, USA, 18–21 April 2017; pp. 173–178.
11. Reilly, E.; Maloney, M.; Siegel, M.; Falco, G. A Smart City IoT Integrity-First Communication Protocol via an Ethereum Blockchain Light Client. In Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019), Montreal, QC, Canada, 27 May 2019; pp. 15–19.
12. Vujičić, D.; Jagodić, D.; Ranđić, S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In Proceedings of the 2018 17th IEEE International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia-Herzegovina, 21–23 March 2018; pp. 1–6.
13. Popov, S. The Tangle. Available online: https://iota.org/IOTA_Whitepaper.pdf (accessed on 15 February 2015).

14. Kotilevets, I.; Ivanova, I.; Romanov, I.; Magomedov, S.; Nikonov, V.; Pavelev, S. Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions. *IFAC-PapersOnLine* **2018**, *51*, 693–696. [CrossRef]
15. Popov, S.; Saa, O.; Finardi, P. Equilibria in the Tangle. *arXiv* **2017**, arXiv:1712.05385.
16. Giungato, P.; Rana, R.; Tarabella, A.; Tricase, C. Current trends in sustainability of bitcoins and related blockchain technology. *Sustainability* **2016**, *9*, 2214. [CrossRef]
17. Wu, J.; Tran, N.K. Application of blockchain technology in sustainable energy systems: An overview. *Sustainability* **2018**, *10*, 3067. [CrossRef]
18. Yang, T.; Guo, Q.; Tai, X.; Sun, H.; Zhang, B.; Zhao, W.; Lin, C. Applying blockchain technology to decentralized operation in future energy internet. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017, pp. 1–5.
19. Kshetri, N.; Voas, J. Blockchain-enabled e-voting. *IEEE Softw.* **2018**, *35*, 95–99. [CrossRef]
20. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
21. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-based Decentralized Trust Management in Vehicular Networks. *IEEE Internet Things J.* **2019**, *6*, 1495–1505. [CrossRef]
22. Herrera-Joancomartí, J.; Pérez-Solà, C. Privacy in bitcoin transactions: new challenges from blockchain scalability solutions. In Proceedings of the International Conference on Modeling Decisions for Artificial Intelligence, Sant Julià de Lòria, Andorra, 19–21 September 2016; Spriner: Cham, Switzerland, 2016; pp. 26–44.
23. Sompolinsky, Y.; Zohar, A. *Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains*; Cryptology ePrint Archive, Report 2013/881; IACR: Lyon, France, 2013.
24. Sompolinsky, Y.; Lewenberg, Y.; Zohar, A. *SPECTRE: Serialization of Proof-of-Work Events: Confirming Transactions via Recursive Elections*; no 1159, Cryptology ePrint Archive; IACR: Lyon, France, 2016.
25. Sompolinsky, Y.; Zohar, A. *Phantom: A Scalable Blockdag Protocol*; IACR Cryptology ePrint Archive: Lyon, France, 2018.
26. Churyumov, A. Byteball: A Decentralized System for Storage and Transfer of Value. Available online: https://byteball.org/Byteball.pdf (accessed on 25 November 2018).
27. Lerner, S.D. *DagCoin: A Cryptocurrency without Blocks*; White Paper, 11 September 2015. Available online: https://bitslog.com/2015/09/11/dagcoin/ (accessed on 11 November 2018).
28. LeMahieu, C. RaiBlocks: A Feeless Distributed Cryptocurrency Network. Available online: https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf (accessed on 11 November 2018).
29. Bardwell, L.; Fearnhead, P. Bayesian detection of abnormal segments in multiple time series. *Bayesian Anal.* **2017**, *12*, 192–218. [CrossRef]
30. Sanchez-Castillo, M.; Blanco, D.; Tienda-Luna, I.; Carrion, M.; Huang, Y. A Bayesian framework for the inference of gene regulatory networks from time and pseudo-time series data. *Bioinformatics* **2018**, *34*, 964–970. [CrossRef] [PubMed]
31. Brodersen, K.H.; Gallusser, F.; Koehler, J.; Remy, N.; Scott, S.L. Inferring causal impact using Bayesian structural time-series models. *Ann. Appl. Stat.* **2015**, *9*, 247–274. [CrossRef]
32. Dong, L.; Sui, P.; Sun, P. Novel naive Bayes classification algorithm based on semi-supervised learning. *J. Jilin Univ. (Eng. Technol. Ed.)* **2016**, *46*, 884–889.