International Journal of Mathematical, Engineering and Management Sciences
Vol. 8, No. 4, 547-559, 2023
https://doi.org/10.33889/IJMEMS.2023.8.4.031

System-Level Dependability Analysis of Bitcoin under Eclipse and 51% Attacks

Chencheng Zhou
Department of Electrical and Computer Engineering,
University of Massachusetts, Dartmouth, MA, USA.
E-mail: czhou@umassd.edu

Liudong Xing
Department of Electrical and Computer Engineering,
University of Massachusetts, Dartmouth, MA, USA.
Corresponding author: lxing@umassd.edu

Qisi Liu
Department of Electrical and Computer Engineering,
University of Hartford, Hartford, CT, USA.
E-mail: qliu@hartford.edu

Yuzhu Li
Department of Decision and Information Sciences,
University of Massachusetts, Dartmouth, MA, USA.
E-mail: yuzhu.li@umassd.edu

(Received on April 14, 2023; Accepted on June 07, 2023)

Abstract
Bitcoin is an electronic cryptocurrency developed based on Blockchain technology. With its decentralized feature, it has become incredibly popular since its invention. However, the Bitcoin network suffers from 51% attacks, where if malicious attackers' control over half of the computing power, they are able to rewrite the network. The attackers are capable of doing so by initiating the Eclipse attack first, which aims to monopolize all communications from and to a controlled Bitcoin node. In this paper, we model and analyze the dependability of the Bitcoin network subject to the Eclipse and 51% attacks. We propose a hierarchical model that encompasses a continuous-time Markov chain method for the node-level dependability analysis and a multi-valued decision diagram method for the system-level dependability analysis. Detailed case studies on Bitcoin systems with homogeneous and heterogeneous nodes are conducted to demonstrate the proposed model and investigate the impacts of several critical parameters on Bitcoin network dependability.

Keywords- Bitcoin, Dependability, Eclipse attack, Hierarchical modeling, 51% attack.

1. Introduction

As a blockchain-based peer-to-peer cryptocurrency system (Ferrag et al., 2018; Kang et al., 2018; Frizzo-Barker et al., 2020; Xing, 2020), Bitcoin has the decentralized property of enabling users to trade freely without involving any intermediate agents (Nakamoto, 2008). However, Bitcoin can be vulnerable to various cyberattacks.

For example, by taking advantage of Bitcoin's open network, an attacker may track the addresses of transactions and their relationships, putting users' privacy in danger (Reid and Harrigan, 2013). A malicious miner can attack the blockchain consensus mechanism to tamper with Bitcoin's data (Bag et al., 2016). In addition, Bitcoin may be subject to other attacks like selfish mining (Eyal and Sirer, 2014), Sybil attacks

(Zhang and Lee, 2019), 51% attacks (Bastiaan, 2015; Novoa et al., 2021), and Eclipse attacks (Heilman et al., 2015; Zhou et al., 2021a). To defend Bitcoin against those attacks, different strategies have been suggested. For example, Eyal and Sirer (2014) suggested a mitigation strategy based on modifying the Bitcoin protocol to cope with selfish mining attacks. Gervais et al. (2015) suggested several countermeasures based on dynamic timeouts, updating block advertisements, and penalizing non-responding nodes for enhancing Bitcoin security. Monaco (2015) suggested a decentralized anonymous payment scheme to protect users' privacy. Göbel et al. (2016) applied Markov Chains for detecting selfish mining attacks by monitoring orphan blocks' production rate. Existing studies (as exemplified above) have mostly concentrated on detecting threats and examining the impacts of malicious behaviors.

Some recent efforts have been made for the quantitative analysis of dependability in Bitcoin. Specifically, in Zhou et al. (2021a), a continuous-time Markov chain (CTMC)-based method was proposed to model the behavior of a Bitcoin node under the Eclipse attack and further quantify the node-level dependability of Bitcoin with exponentially distributed state transition times. In Zhou et al. (2021b), a semi-Markov process-based approach was proposed to analyze the steady-state dependability of a Bitcoin node with general state transition time distributions. In Zhou et al. (2022), another CTMC-based analytical method was suggested to evaluate the dependability of the Bitcoin system, considering selfish mining behavior. Based on this work, two network-wide defense strategies were put forward to disincentivize malicious selfish miners and improve the system's dependability in Zhou et al. (2023). The existing works have mostly focused on node-level dependability analysis or considered a single type of attack. In practice, the Bitcoin network may be vulnerable to more than one type of attack at the same time.

In this paper, we contribute by modeling and analyzing the system-level dependability of the Bitcoin network subject to the combined Eclipse and 51% attacks. We propose a hierarchical modeling approach that encompasses the CTMC-based method suggested by Zhou et al. (2021a) for modeling the node-level behavior under the Eclipse attack, and a multi-valued decision diagram (MDD)-based method for modeling the system-level dependability of the Bitcoin system considering the 51% attack. Numerical case studies are carried out to demonstrate the proposed model under both homogeneous and heterogeneous node situations. The effects of critical parameters on Bitcoin dependability are also evaluated.

The rest of the paper is arranged as follows: Section 2 examines the working mechanism of the Eclipse attack and the 51% attack. Section 3 introduces the hierarchical modeling approach to analyze system-level dependability. Section 4 investigates the effects of user behavior parameters on both node-level and system-level dependability using case studies. Section 5 summarizes our research results and points out the future study plan.

Below are major notations used in the paper:

t	Mission time.
λ_{ij}	Transition rate from state i to state j.
μ_{ji}	Recovery transition rate from state j to state i.
$P_j(t)$	Probability of the system being in state j at time t.
$D_{\text{node}}(t)$	Dependability of a Bitcoin node at time t.
$D_{\text{system}}(t)$	Dependability of a Bitcoin system at time t.
$P_{m,j}$	Probability of Bitcoin node m being in state j.
$P_{Sk}(t)$	Probability of Bitcoin system being in state Sk.
n	Number of nodes in the considered Bitcoin network.

2. Attack Models

This work considers two types of attacks: the Eclipse attack (Heilman et al., 2015) and the 51% attack (Novoa et al., 2021). While an Eclipse attacker has the objective of gaining control of the information flow of a victim node (making the victim node lose connections with other legitimate nodes), a 51% attacker tries to control over 50 percent of the network nodes to gain the power to alter the blockchain.

Specifically, for a successful Eclipse attack, the attacker maliciously fills the routing table of the victim node (VN) before a restart. The VN may be forced to restart, or the attacker may simply wait for the VN's restart. Following the restart, the VN builds an outgoing connection with the attack address in the routing table while the attacker's node continuously builds an incoming connection with the VN. Eventually, the VN's information flow channel is monopolized. Consequently, the VN can only receive malicious information transmitted from the attacker's node (Heilman et al., 2015).

Successful Eclipse attacks on multiple nodes may lead to other attacks like the 51% attack (Novoa et al., 2021). The 51% attack targets digit currency by a malicious miner or a group of them who aim to control over 50 percent of the network's computing power. Once the attackers own 51% of the nodes, they are capable of halting payment, preventing confirmation of new transactions, and reversing transactions to double-spend by altering the blockchain. In this work, we use the 51% attack to define the system-level dependability measure of the Bitcoin network.

3. Proposed Hierarchical Modeling Approach

The hierarchical modeling approach proposed in this work encompasses the CTMC-based node-level dependability analysis considering the Eclipse attack (Section 3.1) and the MDD-based method for the system-level dependability analysis of the Bitcoin system considering the 51% attack (Section 3.2).

3.1 Node-Level Modeling

To model and analyze the node-level dependability under the Eclipse attack, we utilize the CTMC-based method developed in the previous work (Zhou et al., 2021a). To make the paper self-contained, a brief review of the method is provided below.

Five states can be distinguished for a Bitcoin node under the Eclipse attack: original state (0), table hacked state (1), restart state (2), connected state (3), and monopolized state (4). Figure 1 shows the possible transitions among those five states. The transition from state 0 to state 1 (with transition rate λ_{01}) is caused by the attack node that sends the ADDR message including many forged IP addresses to gradually overwrite all legal addresses of the VN's routing table.

The transition from state 1 to state 2 (with rate λ_{12}) is caused by the VN's restart while the transition from state 1 back to state 0 (with rate μ_{10}) is caused by the victim's detecting and deleting suspicious message containing the forged addresses.

The transition from state 2 to state 3 (with rate λ_{23}) is caused by the VN being connected to the attack addresses, while the transition from state 2 back to state 1 (with rate μ_{21}) is caused by the victim's cleaning its routing table.

The transition from state 3 to state 4 (with rate λ_{34}) is caused by the VN being forced to pick a forged address from the hacked routing table to build an outgoing connection, while the transition from state 3 back to state 0 (with rate μ_{30}) is caused by the victim's successfully restoring healthy connections via maintenance.

The transition from state 4 back to state 3 (with rate μ_{43}) is caused by the victim's detecting adversary connections and re-establishing partial connections with legal nodes. Once state 4 is reached, the attacker is able to control all incoming connections to the VN, and the Eclipse attack is successful.

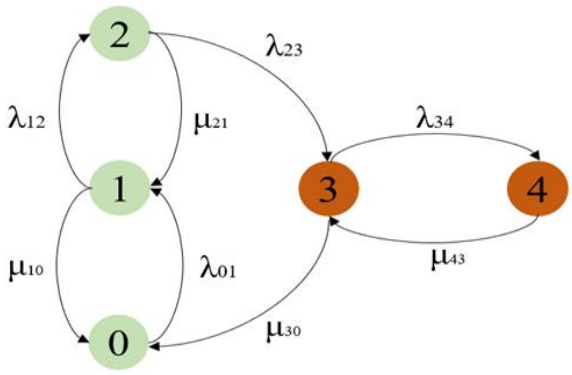

Figure 1. The state transition diagram of the Bitcoin node under the Eclipse attack.

Refer to Zhou et al. (2021a) for the Laplace transform-based solution to solve the Markov model of Figure 1 to derive all the state probabilities $P_j(t)$ (j=0,1,2,3,4). The dependability of the Bitcoin node is computed as $D_{\text{node}}(t) = P_0(t) + P_1(t) + P_2(t)$.

3.2 System-Level Modeling

The entire Bitcoin system has three states: stable (state *S*0), exposed (state *S*1), and dominated/failed (state *S*2). Specifically, when over fifty percent of the nodes are controlled by the Eclipse attacker, the 51% attack is successful. In this case, the entire Bitcoin system is considered to be in the dominant state (*S*2). Consider a Bitcoin network with n nodes. The dominated state occurs when at least ω (defined in (1)) nodes are in the monopolized state 4.

$$\omega = \begin{cases} \frac{n}{2} + 1, & \text{if } n \text{ is an even number} \\ \frac{n+1}{2}, & \text{if } n \text{ is an odd number} \end{cases} \quad (1)$$

The Bitcoin system is considered in the stable state (*S*0) when at least ω nodes are in the stable state 0. We consider any state other than stable and dominated states as the exposed state (*S*1) for the Bitcoin system in this work. The system dependability is defined as the probability that the Bitcoin system is in a non-dominated state, i.e.,

$$D_{\text{system}}(t) = P_{S0}(t) + P_{S1}(t) = 1 - P_{S2}(t) \quad (2)$$

We analyze the three system state probabilities and dependability for Bitcoin systems with homogeneous nodes (Section 3.2.1) and heterogeneous nodes (Section 3.2.2).

3.2.1 Homogeneous Nodes

In the case of all the nodes being homogeneous (i.e., having the same state probabilities $P_{mj} = P_j$), the probability of the system being in the dominated state (*S*2) can be obtained using (3).

$$P_{S2}(t) = C_n^{\omega}(P_4)^{\omega}(1\text{-}P_4)^{n-\omega} + \ldots + C_n^{n-1}(P_4)^{n-1}(1\text{-}P_4) + (P_4)^n$$
$$= \sum_{x=0}^{n-\omega} C_n^{\omega+x}(P_4)^{\omega+x}(1-P_4)^{n-\omega-x} \quad (3)$$

The probability of the system being in the stable state ($S0$) can be obtained using (4).

$$P_{S0}(t) = \sum_{x=0}^{n-\omega} C_n^{\omega+x} (P_0)^{\omega+x} (1 - P_0)^{n-\omega-x} \quad (4)$$

Thus, the probability of the system being in the exposed state ($S1$) can be obtained as

$$P_{S1}(t) = 1 - P_{S0}(t) - P_{S2}(t) \quad (5)$$

3.2.2 Heterogeneous Nodes

To analyze the system-level Bitcoin dependability when the nodes are heterogeneous, each node is modeled as a five-state component, and the MDD model (Xing and Dai, 2009; Xing and Amari, 2015) is applied to represent the system-level behavior of the Bitcoin system.

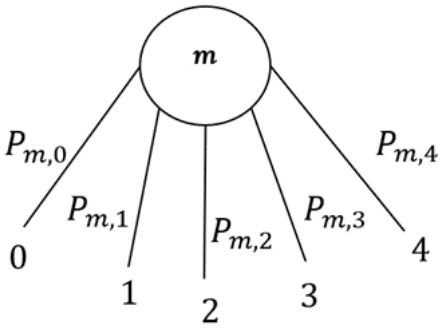

Figure 2. An MDD non-sink node modeling Bitcoin node *m*.

Specifically, as illustrated in Figure 2, each Bitcoin node *m* is modeled as a non-sink node with five outgoing edges, representing the node being in the original (0), table hacked (1), restart (2), connected (3), and monopolized (4) states, respectively. Each edge is associated with its corresponding state probability, denoted by $P_{m,0}$, $P_{m,1}$, $P_{m,2}$, $P_{m,3}$, $P_{m,4}$, respectively. Those node-level state probabilities are evaluated using the CTMC-based method presented in Section 3.1.

Based on the state definitions presented at the beginning of Section 3.2, lattice-structured MDD models may be constructed, as illustrated by a specific example below.

Consider a Bitcoin network with n=4 nodes labeled by $N1$, $N2$, $N3$, and $N4$, respectively. They are miners with different levels of user sense of system protection. In this example, the normal, above-average, and strong levels are differentiated. Among the four nodes, $N1$ and $N2$ have the normal level, whose state probabilities are analyzed using the CTMC-based method under parameter set *a*. Node $N3$ has the above-average level, whose state probabilities are analyzed using parameter set *b*. Node $N4$ has the strong level, whose state probabilities are analyzed using parameter set *c*.

To analyze the probability of the system being in the dominant state $P_{S2}(t)$, we construct the MDD model in the 3-out-of-4 lattice structure as shown in Figure 3, where sink node '1' means the system is in the dominated state ($S2$) and sink node '0' means the system is not in the dominated state.

According to the MDD evaluation method (Xing and Amari, 2015; Xing and Dai, 2009), $P_{S2}(t)$ can be obtained as the sum of the probabilities of all paths from root node $N1$ to sink node '1':

$$P_{S2}(t) = P_{N1,4} * P_{N2,4} * P_{N3,4} + P_{N1,4} * P_{N2,4} * (1- P_{N3,4}) * P_{N4,4} + P_{N1,4} * (1- P_{N2,4}) * P_{N3,4} * P_{N4,4} + (1- P_{N1,4}) * P_{N2,4} * P_{N3,4} * P_{N4,4}. \quad (6)$$

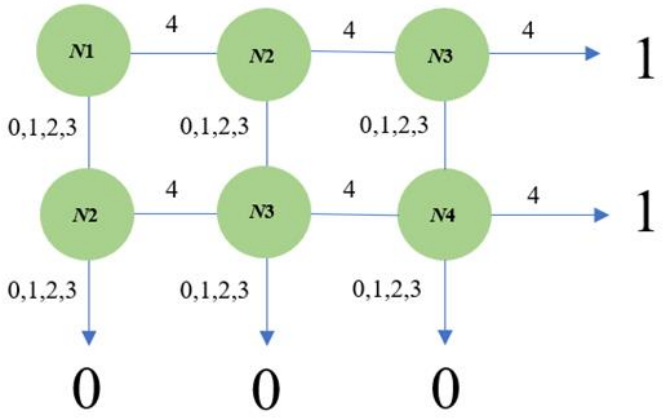

Figure 3. MDD for the Bitcoin network in the dominated state.

To analyze the probability of the system being in the stable state $P_{S0}(t)$, we construct the MDD model in the 3-out-of-4 lattice structure as shown in Figure 4, where sink node '1' means the system is in the stable state ($S0$) and sink node '0' means the system is not in the stable state.

Based on the MDD of Figure 4, $P_{S0}(t)$ can be obtained as the sum of the probabilities of all paths from root node $N1$ to sink node '1':

$$P_{S0}(t) = P_{N1,0} * P_{N2,0} * P_{N3,0} + P_{N1,0} * P_{N2,0} * (1- P_{N3,0}) * P_{N4,0} + P_{N1,0} * (1- P_{N2,0}) * P_{N3,0} * P_{N4,0} + (1- P_{N1,0}) * P_{N2,0} * P_{N3,0} * P_{N4,0}. \quad (7)$$

After $P_{S0}(t)$ and $P_{S2}(t)$ are evaluated, the probability of the system being in the exposed state ($S1$) can be obtained as $P_{S1}(t) = 1- P_{S0}(t) - P_{S2}(t)$.

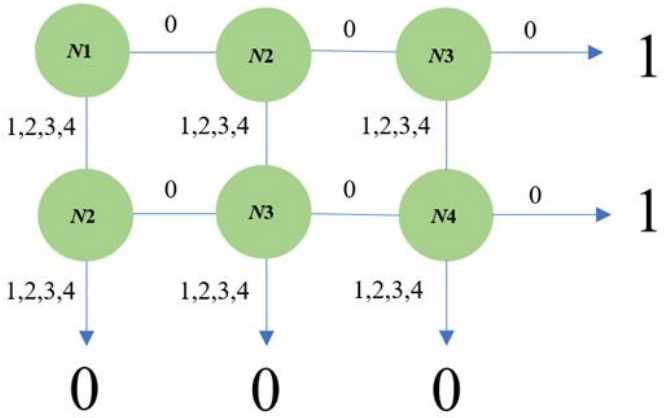

Figure 4. MDD for the Bitcoin network in the stable state.

4. Numerical Results and Analysis

Table 1 lists the parameter sets used in the case studies. The parameter values are designed based on the statistics and studies from Sapirshtein et al. (2016). Among the three sets *a*, *b*, and *c*, parameters (μ_{21}, μ_{30}, μ_{43}), which model the user's sense of system protection, are different while the other parameters are the same.

Table 1. Eclipse attack model transition rate parameters (per hour).

Rate	*Set a*	*Set b*	*Set c*	*Set d*	*Set e*
μ_{10}	0.05	0.05	0.05	0.05	0.05
μ_{21}	0.01	0.12	0.38	0.12	0.12
μ_{30}	0.05	0.18	0.53	0.18	0.18
μ_{43}	0.02	0.16	0.45	0.16	0.16
λ_{01}	0.03	0.03	0.03	0.03	0.03
λ_{12}	0.25	0.25	0.25	0.05	0.65
λ_{23}	0.34	0.34	0.34	0.34	0.34
λ_{34}	0.16	0.16	0.16	0.16	0.16

Specifically, sets *a*, *b*, and *c* model miners with the normal level, above-average level, and strong level of system protection sense, respectively. The analysis results using those three parameter sets should reveal the effects of the user's sense of system protection on node dependability and further on system dependability.

Among the three sets *d*, *b*, and *e*, the parameter λ_{12} that models the user's restart habit, is different, while the other parameters are the same. Specifically, sets *d*, *b*, and *e* model miners with increasing restarting frequencies. The analysis results using those three parameter sets should reveal the effects of the user's restart habit on node dependability and further on system dependability.

4.1 Node-Level Dependability Analysis Results

Table 2 summarizes the numerical analysis results for the Bitcoin node-level dependability under the different parameter sets. It is revealed that a node is more likely to stay in the dependable state when the miner has a higher sense of system protection, and a node has a higher probability of being compromised if its user shuts down and restarts the node with higher frequency because the Eclipse attack requires the system's reboot to complete the attack.

Table 2. Node-level dependability results.

t(hrs)	Set *a*	Set *b*	Set *c*	Set *d*	Set *e*
12	0.864533	0.923578	0.976648	0.975726	0.891195
18	0.755948	0.883587	0.971561	0.957196	0.849035
24	0.657072	0.857726	0.969674	0.941810	0.824199
30	0.570580	0.842074	0.969004	0.93030	0.809803
36	0.495490	0.832862	0.968770	0.922198	0.801483
42	0.430359	0.827513	0.945121	0.916718	0.796677

Table 3 presents the monopolized state (i.e., state 4) probabilities of the Bitcoin node under different parameter sets, which are used for the system-level dependability analysis in Section 4.2.

Table 3. The monopolized state probability for the Bitcoin node.

t (hrs)	Set *a*	Set *b*	Set *c*	Set *d*	Set *e*
12	0.059353	0.025932	0.006814	0.007778	0.038901
18	0.144560	0.048030	0.009339	0.016714	0.064551
24	0.240354	0.064309	0.010367	0.025116	0.081221
30	0.332884	0.074752	0.010738	0.031831	0.091178
36	0.416866	0.081067	0.010863	0.036757	0.096984
42	0.491129	0.084784	0.010904	0.040182	0.100346

4.2 System-Level Dependability Analysis Results

In Section 4.2.1, we further investigate the effects of the level of system protection sense and restart habit on system-level dependability using homogeneous Bitcoin networks. In Section 4.2.2, we present the numerical analysis results of a heterogenous Bitcoin network.

4.2.1 Homogeneous Nodes

Consider three networks with 10, 20, and 30 nodes, respectively. Based on the node state 4 probability obtained for sets *a*, *b*, and *c* in Table 3 and Equations (2) and (3), the system-level dependability results under those three sets are evaluated and presented in Table 4. Figures 5 and 6 demonstrate the results graphically.

Table 4. Dependability of Bitcoin with homogeneous nodes.

Set	Size	12hrs	18hrs	24hrs	30hrs	36hrs	42hrs
a	10	0.99985585	0.99158042	0.93263511	0.78779143	0.59027820	0.39896848
	20	0.99999994	0.99981840	0.98956610	0.90883467	0.70364223	0.44340978
	30	0.99999999	0.99999556	0.99819102	0.95701572	0.77101774	0.46649799
b	10	0.99997772	0.99994746	0.99978935	0.99957302	0.99937713	0.99923336
	20	0.99999999	0.99999999	0.99999987	0.99999952	0.99999894	0.99999841
	30	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999
c	10	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999
	20	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999
	30	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999

Figure 5 illustrates that system-level dependability *D* for Bitcoin with 30 nodes is the highest and decreases with the lowest speed as time proceeds; *D* for Bitcoin with 10 nodes is the lowest and decreases with the highest speed as time proceeds. It can be concluded that a larger Bitcoin network is more resilient against the 51% attack.

Figure 6 illustrates that the system-level dependability *D* for Bitcoin with 20 nodes under set *c* is the highest and decreases with the lowest speed as time proceeds, while *D* under set *a* is the lowest and decreases sharply as time proceeds. It is intuitive that a network tends to be dependable when all its nodes/miners have higher protection awareness.

Based on the node state probability obtained for sets *d*, *b*, and *e* in Table 3 and Equations (2)-(3), the system-level dependability results under those three sets are evaluated and presented in Table 5. Figure 7 demonstrates the results graphically.

Based on the comparisons illustrated in Figure 7, we can make the inference that the Bitcoin system is more likely to stay in a dependable state when its miners restart rarely after the mining.

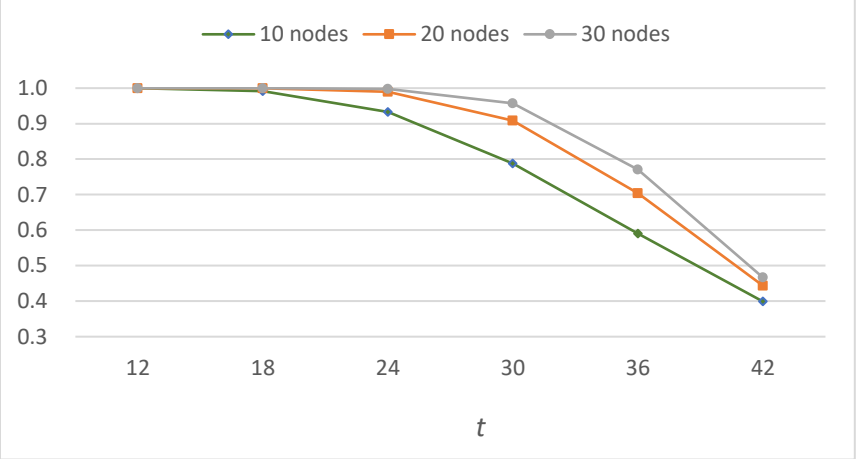

Figure 5. System-level dependability with homogeneous nodes under set *a*.

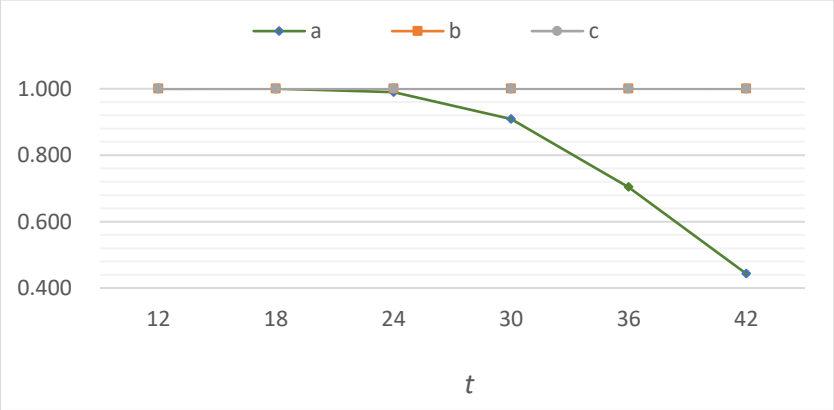

Figure 6. System-level dependability for Bitcoin with 20 homogeneous nodes under sets *a*, *b*, *c*.

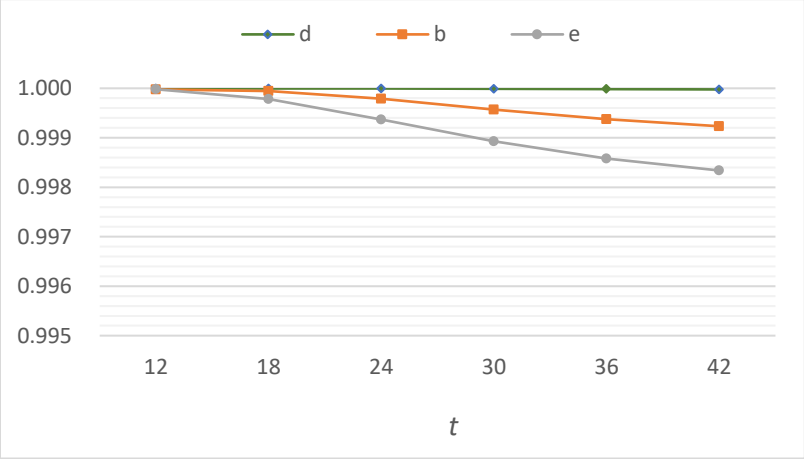

Figure 7. System-level dependability for Bitcoin with 10 homogeneous nodes under sets *d*, *b*, and *e*.

Table 5. Dependability of Bitcoin with homogeneous nodes.

Set	Size	12hrs	18hrs	24hrs	30hrs	36hrs	42hrs
d	10	0.99999999	0.99999969	0.99999771	0.99999279	0.99998552	0.99997772
	20	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999
	30	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999
b	10	0.99997772	0.99994746	0.99978935	0.99957302	0.99937713	0.99923336
	20	0.99999999	0.99999999	0.99999987	0.99999952	0.99999894	0.99999841
	30	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999	0.99999999
e	10	0.99998095	0.99978560	0.99937165	0.99892821	0.99857806	0.99833909
	20	0.99999999	0.99999987	0.99999892	0.99999691	0.99999457	0.99999262
	30	0.99999999	0.99999999	0.99999999	0.99999998	0.99999997	0.99999996

4.2.2 Heterogenous Nodes

To further illustrate the effects of restarting habits on the dependability of heterogeneous Bitcoin networks (HBN), we compare three networks with different restarting frequencies. Specifically, HBN-A contains four nodes, respectively, characterized by parameter sets *aabc*, where λ_{12} =0.25 models the average restart frequency. HBN-L contains four nodes, respectively, characterized by parameter sets *a′a′b′c′*, which share the same parameter values with *aabc* except λ_{12} =0.05 modeling the low restart frequency. HBN-H contains four nodes, respectively, characterized by parameter sets *a″a″b″c″*, which also share the same parameter values with *aabc* except λ_{12} =0.65 modeling the high restart frequency.

Based on Section 3.1, Table 6 presents the monopolized state probability of a Bitcoin node under each parameter set.

Based on the node-level state 4 probabilities in Table 6 and Equations (2) and (6), Table 7 shows the system-level dependability results of the three HBNs with different restart habits. Figure 8 demonstrates the graphical results.

Table 6. The monopolized state probability for Bitcoin nodes.

t (hrs)	Set *a′*	Set *a*	Set *a″*	Set *b′*	Set *b*	Set *b″*	Set *c′*	Set *c*	Set *c″*
12	0.018028	0.059353	0.088107	0.007778	0.025932	0.038900	0.001958	0.006814	0.010642
18	0.051419	0.144560	0.191790	0.016714	0.048030	0.064550	0.003026	0.009339	0.013198
24	0.097067	0.240354	0.298296	0.025116	0.064309	0.081220	0.003661	0.010367	0.013912
30	0.148811	0.332884	0.396010	0.031831	0.074752	0.091178	0.004012	0.010738	0.014078
36	0.202267	0.416866	0.481828	0.036757	0.081067	0.096984	0.004202	0.010863	0.014111
42	0.254860	0.491129	0.555872	0.040182	0.084784	0.100347	0.004304	0.010904	0.014117

Based on Table 7 and Figure 8, we can conclude that the Bitcoin network with miners having a higher restart frequency has a relatively lower resilience against the Eclipse and 51% attacks. This result is consistent with that obtained for the homogeneous network in Figure 7. Therefore, the miners are recommended to lower the restart frequency to reduce the chance of being exposed to the Eclipse threats.

Table 7. Bitcoin system-level dependability and comparisons.

t (hrs)	HBN-L	HBN-A	HBN-H
12	0.999486	0.995046	0.974593
18	0.996382	0.970478	0.888651
24	0.990735	0.933354	0.791052
30	0.983527	0.892441	0.700741
36	0.975478	0.851532	0.620233
42	0.967005	0.811891	0.548892

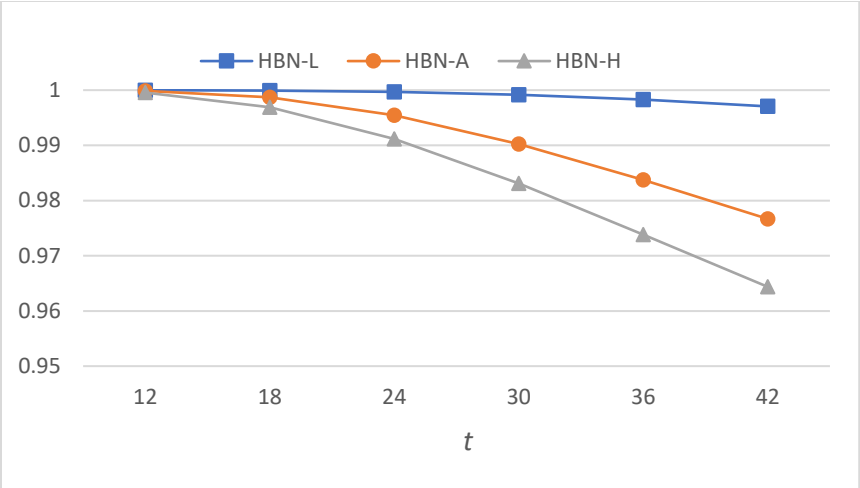

Figure 8. Impacts of restart habits on system-level dependability of heterogeneous network.

5. Conclusions and Future Research Plan

Blockchain technology forms the basis of the Bitcoin network, renowned for its reliable and secure nature due to its decentralized, distributed, and immutable properties. Meanwhile, the Bitcoin network is still vulnerable to various cyberattacks, including the 51% attack, which occurs when malicious miners gain control of more than 50% of the computing power, enabling them to alter the network's transactions. The Eclipse attack is one tactic that can be used by the 51% attackers to achieve control.

In this work, we make contributions by putting forward a hierarchical model that encompasses a CTMC-based node-level dependability analysis and an MDD-based system-level dependability analysis for Bitcoin systems under the Eclipse attack and the 51% attack. Both homogenous and heterogeneous situations are discussed. The effects of several parameters related to miners' behaviors are examined through case studies. It is revealed that the Bitcoin system's dependability is positively correlated with the degree of security awareness exhibited by its miners. Moreover, to minimize the risk of being exposed to Eclipse threats, it is advisable for miners to decrease the frequency of regular restarts and avoid unnecessary restarts. Other suggestions include maintaining a vigilant watch on network activity and looking out for suspicious or abnormal patterns or behaviors using network monitoring tools, monitoring connections established by the mining system, and reviewing incoming and outgoing traffic.

In the future, we are interested in extending the hierarchical MDD-based model to analyze other Bitcoin-oriented attacks like the block withholding attack and the jumping mining attack.

Conflict of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Acknowledgments

This research was supported by the Cybersecurity Graduate Research Fellowship from the University of Massachusetts Dartmouth Cybersecurity Center.

References

Bag, S., Ruj, S., & Sakurai, K. (2016). Bitcoin block withholding attack: Analysis and mitigation. *IEEE Transactions on Information Forensics and Security*, *12*(8), 1967-1978.

Bastiaan, M. (2015). Preventing the 51%-attack: A stochastic analysis of two phase proof of work in Bitcoin. https://fmt.ewi.utwente.nl/media/175.pdf, Accessed in June 2023.

Eyal, I., & Sirer, E.G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *International Conference on Financial Cryptography and Data Security* (pp. 436-454). Springer, Berlin, Heidelberg.

Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the Internet of Things: Research issues and challenges. *IEEE Internet of Things Journal*, *6*(2), 2188-2204.

Frizzo-Barker, J., Chow-White, P.A., Adams, P.R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, *51*, 102029. https://doi.org/10.1016/j.ijinfomgt.2019.10.014

Gervais, A., Ritzdorf, H., Karame, G.O., & Capkun, S. (2015). Tampering with the delivery of blocks and transactions in Bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 692-705). Denver, United States.

Göbel, J., Keeler, H.P., Krzesinski, A.E., & Taylor, P.G. (2016). Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay. *Performance Evaluation*, *104*, 23-41.

Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on Bitcoin's peer-to-peer network. In *24th USENIX Security Symposium* (pp. 129-144). Washington D.C., United States.

Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., & Zhang, Y. (2018). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal*, *6*(3), 4660-4670.

Monaco, J.V. (2015). Identifying Bitcoin users by transaction behavior. In *Biometric and Surveillance Technology for Human and Activity Identification XII* (Vol. 9457, pp. 945704). International Society for Optics and Photonics. Baltimore, United States. https://doi.org/10.1117/12.2177039.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Consulted*, *1*(2012), 28, https://bitcoin.org/bitcoin.pdf.

Novoa, F., Orozco, A., Polanco, R., & Wightman, A. (2021). The 51% attack on blockchains: A mining behavior study. *IEEE Access*, *9*, 140549-140564. https://doi.org/10.1109/ACCESS.2021.3119291.

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the Bitcoin system. In *Security and Privacy in Social Networks* (pp. 197-223). Springer, New York, United States.

Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2016). Optimal selfish mining strategies in Bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 515-532). Springer, Berlin, Heidelberg.

Xing, L. (2020). Reliability in internet of things: Current status and future perspectives. *IEEE Internet of Things Journal*, *7*(8), 6704-6721. https://doi.org/10.1109/JIOT.2020.2993216.

Xing, L., & Amari, S.V. (2015). *Binary decision diagrams and extensions for system reliability analysis*. Scrivener Publishing LLC, Beverly, MA. https://doi.org/10.1002/9781119178026.

Xing, L., & Dai, Y. (2009). A new decision-diagram-based method for efficient analysis on multistate systems. *IEEE Transactions on Dependable and Secure Computing*, *6*(3), 161-174.

Zhang, S., & Lee, J.H. (2019). Double-spending with a sybil attack in the Bitcoin decentralized network. *IEEE Transactions on Industrial Informatics*, *15*(10), 5715-5722.

Zhou, C., Xing, L., & Liu, Q. (2021a). Dependability analysis of Bitcoin subject to eclipse attacks. *International Journal of Mathematical, Engineering and Management Sciences*, *6*(2), 469-479.

Zhou, C., Xing, L., Guo, J., & Liu, Q. (2022). Bitcoin selfish mining modeling and dependability analysis. *International Journal of Mathematical, Engineering and Management Sciences*, *7*(1), 16-27.

Zhou, C., Xing, L., Liu, Q., & Wang, H. (2021b). Semi-Markov based dependability modeling of Bitcoin nodes under eclipse attacks and state-dependent mitigation. *International Journal of Mathematical, Engineering and Management Sciences*, *6*(2), 480-92.

Zhou, C., Xing, L., Liu, Q., & Wang, H. (2023). Effective selfish mining defense strategies to improve Bitcoin dependability. *Applied Sciences*, *13*(1), 422, https://doi.org/10.3390/app13010422.