2022

Bitcoin Selfish Mining Modeling and Dependability Analysis

Chencheng Zhou

Liudong Xing

Jun Guo

Qisi Liu
Electrical and Computer Engineering, q1liu@odu.edu

Original Publication Citation

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. https://doi.org/10.33889/IJMEMS.2022.7.1.002

International Journal of Mathematical, Engineering and Management Sciences
Vol. 7, No. 1, 16-27, 2022
https://doi.org/10.33889/IJMEMS.2022.7.1.002

Bitcoin Selfish Mining Modeling and Dependability Analysis

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

Jun Guo
College of Software,
Northeastern University, China.
E-mail: guojun@mail.neu.edu.cn

Qisi Liu
Department of Electrical and Computer Engineering,
Old Dominion University, VA, USA.
E-mail: q1liu@odu.edu

(Received on November 04, 2021; Accepted on December 21, 2021)

Abstract
Blockchain technology has gained prominence over the last decade. Numerous achievements have been made regarding how this technology can be utilized in different aspects of the industry, market, and governmental departments. Due to the safety-critical and security-critical nature of their uses, it is pivotal to model the dependability of blockchain-based systems. In this study, we focus on Bitcoin, a blockchain-based peer-to-peer cryptocurrency system. A continuous-time Markov chain-based analytical method is put forward to model and quantify the dependability of the Bitcoin system under selfish mining attacks. Numerical results are provided to examine the influences of several key parameters related to selfish miners' computing power, attack triggering, and honest miners' recovery capability. The conclusion made based on this research may contribute to the design of resilience algorithms to enhance the self-defense and robustness of cryptocurrency systems.

Keywords- Bitcoin, Blockchain, Selfish mining, Continuous-time Markov chain, Dependability.

1. Introduction

Intensive research and development efforts from academia, industries and governments have been devoted to blockchain technology in the last decade (Ferrag et al., 2018; Kang et al., 2018; Dai et al., 2019; Bhushan et al., 2021). It has been applied to diverse applications, such as smart contracts, financial services, voting, supply chains, Internet of Things, energy trading, etc. (Akbari et al., 2017; Frizzo-Barker et al., 2020; Wongthongtham et al., 2021; Xing, 2020, 2021). Due to the safety-critical and security-critical nature of these applications, it is crucial to model the dependability attribute of the blockchain-based systems. In this work, we focus on the dependability modeling and analysis of Bitcoin, a blockchain-based peer-to-peer cryptocurrency network (Nakamoto, 2008).

In contrast to the traditional fiat currency, Bitcoin is a decentralized system where individuals can freely trade without engaging banks (Tschorsch and Scheuermann, 2016). Bitcoin is now widely utilized in diverse fields with a market cap of over $1trillion (Best, 2021). Due to its business-critical nature, the Bitcoin network has become the target of many cyber-attacks. For instance, a malicious attacker may compromise the blockchain data availability by generating illegal or incorrect access to the data through tracking correspondences of different addresses like the Bitcoin and IP addresses (Koshy et al., 2014). An attacker may also temper the data by attacking the blockchain's consensus mechanism (Bag et al., 2016). Through tracking relationships between addresses of transactions in the Bitcoin open network, an attacker may access users' personal information (Reid and Harrigan, 2013). Other examples of security attacks launched to the Bitcoin system include but are not limited to selfish mining attacks (Eyal and Sirer, 2014), sybil attacks (Zhang and Lee, 2019), mining pool attacks (Bahack, 2013; Qin et al., 2020), miner attacks (Rosenfeld, 2011), re-identification attacks (Meiklejohn et al., 2013), eclipse attacks (Zhou et al., 2021a), and CryptoLocker-based attacks (Liao et al., 2016).

Many research efforts have been dedicated to defending the Bitcoin system against those security attacks. For instance, a mitigation approach based on modifying the Bitcoin protocol was proposed in Eyal and Sirer (2014) to defend Bitcoin against colluding selfish mining attacks. Several countermeasures (updating block advertisements, dynamic timeouts, penalizing non-responding nodes) were investigated in Gervais et al. (2015) to improve the Bitcoin network security. A hardware token was suggested in Bamert et al. (2014) to secure Bitcoin transactions. The weakness of Bitcoin in protecting privacy was first studied and an anonymous, decentralized payment mechanism was then suggested for privacy protection in Monaco (2015). The threat to Bitcoin from the pool mining was first discussed and Markov chains were then applied for stochastic analysis of a two-phase proof-of-work in Bastiaan (2015). Markov chains were utilized in Göbel et al. (2016) for possibly detecting block-hiding attacks through monitoring orphan blocks' production rate.

While existing works have mostly centered on studying impacts of the malicious behaviors or detecting and defending threats, some of the recent efforts have been expended in the quantitative performance evaluation of Bitcoin. For example, in Wang et al. (2020), a mathematical model was proposed to estimate the performance and effectiveness of selfish attacks quantitatively and investigated the relationship between the extra mining gain and computational power. In Motlagh et al. (2021), an analytical model was proposed for studying the effects of selfish mining on the Bitcoin network connectivity, node response time, block delivery time, and block arrival rate. In Zhou et al. (2021a), a continuous-time Markov Chain-based approach was suggested for assessing the dependability of a Bitcoin node subject to Eclipse attacks; this work was extended in Zhou et al. (2021b) through semi-Markov models for accommodating non-exponential state transition time distributions. In Yang et al. (2020), a Markov model was applied to evaluate the mining revenue, and potential risk of the Bitcoin system under selfish mining. In Xia et al. (2021), the impacts of multiple miners and propagation delay on selfish mining were studied, which found that the Bitcoin network with a higher orphan rate is more vulnerable. To the best of our knowledge, no works have been done to study the selfish mining behavior from the perspective of the Bitcoin network dependability and identify the attacking or defending parameters as well as their effects on the Bitcoin network dependability attribute.

In this paper, we advance the state of the art by examining the selfish mining behavior and considering this attack behavior in the quantitative dependability analysis of the Bitcoin network. We also investigate the impacts of several key parameters related to selfish miners' computing

power, attack triggering and honest miners' recovery capability on the Bitcoin dependability through numerical results.

The rest of the paper is structured as follows: Section 2 presents the functioning mechanism of the selfish mining attack. Section 3 presents the state transition diagram of the Bitcoin system under the selfish mining attack. Section 4 derives the state probabilities and the Bitcoin dependability using the continuous-time Markov chain (CTMC)-based approach. Section 5 carries out a numerical analysis of several key model parameters and discusses their impacts on the Bitcoin dependability. Section 6 concludes our study results and discusses future research plans.

2. The Selfish Mining Attack

In the selfish mining attack (also known as the block withholding attack), selfish miners intentionally withhold the newly mined blocks. Instead of broadcasting the new blocks immediately, the selfish miners keep these blocks secretly and build their own branches. At a certain point, the selfish miners publish their private branch and gain unfair revenue.

In this research, we focus on the three-block strategy. Due to the limitation of computing power, it is often extremely hard to expand the lead. To realize the attack, an attacker always withholds the mined blocks and keeps mining on the private branch until the private branch is exactly three blocks longer than the main branch. When the honest miner finds the next block, the attacker publishes their private branch immediately. Because of the proof-of-work protocol, the attacker can successfully claim the rewards while the honest miner's computing power is wasted. Figure 1 shows the flowchart of a successful selfish mining attack.

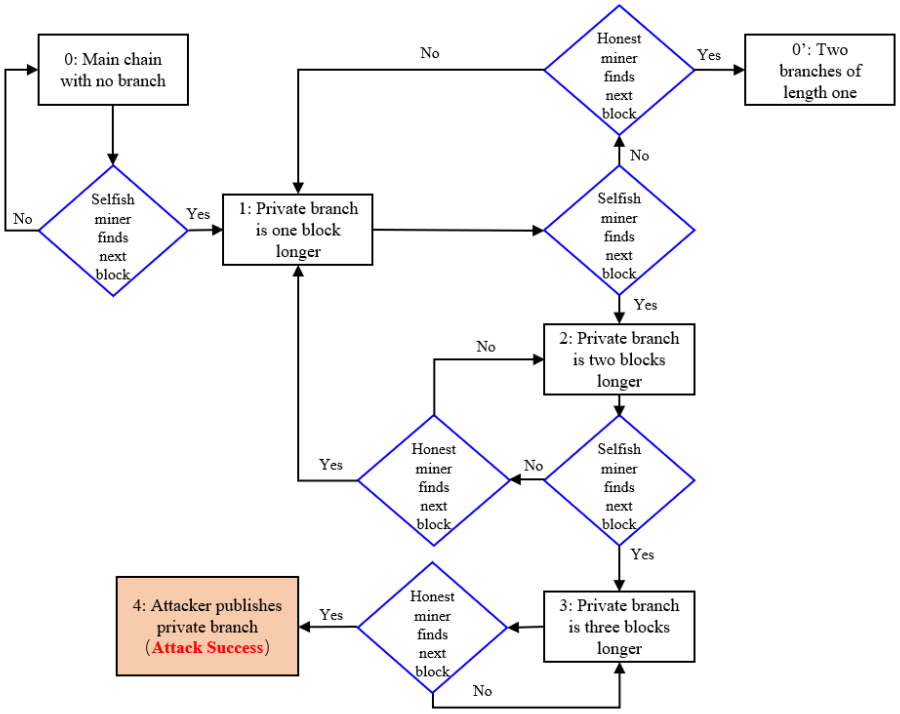

Figure 1. Flowchart of a successful selfish mining attack.

The realization of the selfish mining attack highly depends on the computing power. Some blockchain attacks like Eclipse attacks are capable of controlling the blockchain channels and information flows of more nearby nodes, and gradually controlling most of the blockchain network. Thus, a successful Eclipse attack can reinforce the selfish mining attack (Heilman et al., 2015).

3. State-Transition Diagram

Based on the working mechanism of the selfish attack presented in Section 2, we illustrate the state transition diagram of the Bitcoin system under the attack in Figure 2. Six major states are differentiated and defined: 0 (original or initial state), 0' (double branches), 1 (one block lead), 2 (two-block lead), 3 (three-block lead), and 4 (attack success).

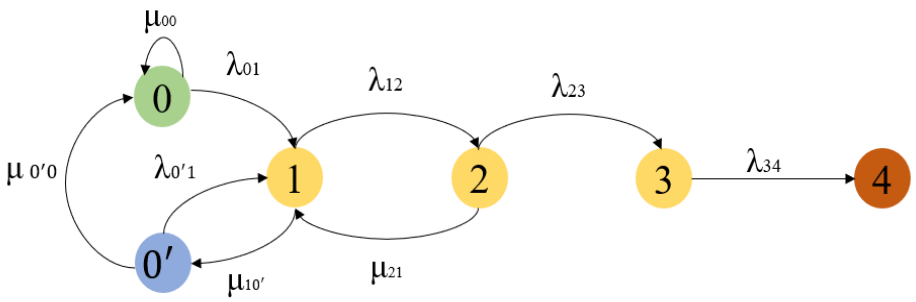

Figure 2. State transition diagram of the bitcoin under the selfish mining attack.

In the original state 0, there is only one main chain every miner is mining on. There is no branch. Under state 0, the malicious miner mines a block and keeps it secretly. As a result, a private branch is built and the system transits from state 0 to state 1 with transition rate of λ_{01}. Under state 0, if the honest miner finds the block first, then the system remains in state 0 with μ_{00}.

Under state 1, if the malicious miner successfully finds the next block on their private branch, then the system transits to state 2 with transition rate of λ_{12}. Under state 1, if the honest miner finds the next block before the malicious miner, then the system transits to state 0' with transition rate of $\mu_{10'}$.

Under state 0' (the chain has two branches of length one), if the malicious miner finds the new block with rate $\lambda_{0'1}$, the system transits to state 1 where the selfish miner's private branch is one block longer. If the honest miner finds the new block first, the system can transit back to the initial state 0 with rate $\mu_{0'0}$.

Under state 2, the malicious miner can be the first one to find the next block with rate λ_{23}, causing the system to transit to state 3. Under state 2, if the honest miner discovers the next block, the system can transit back to state 1 with rate μ_{21}.

Under state 3, when the honest miner successfully finds the next block with rate λ_{34}, the system transits to state 4. Under state 4, the selfish miner broadcasts their private branch, which becomes the main branch. Consequently, the selfish mining attack completes.

Based on the state transition diagram, Section 4 derives the state probabilities and further the Bitcoin dependability based on the continuous-time Markov chain (CTMC) approach. Section 5 investigates the effects of some representative state transition rates on the Bitcoin dependability.

4. CTMC-based Dependability Evaluation

Based on the state transition diagram of Figure 2, we present the state equations in Eq. (1), which consists of a transition rate matrix, a state probability vector, and a vector of the derivative of the state probability. Particularly, $P_j(t)$ denotes the probability that the Bitcoin is in state j (j = 0, 0', 1, 2, 3, 4), and $\dot{P}_j(t)$ denotes the derivative of the state j probability.

$$\begin{bmatrix} -\lambda_{01} & \mu_{0'0} & 0 & 0 & 0 & 0 \\ 0 & -(\mu_{0'0}+\lambda_{0'1}) & \mu_{10'} & 0 & 0 & 0 \\ \lambda_{01} & \lambda_{0'1} & -(\mu_{10'}+\lambda_{12}) & \mu_{21} & 0 & 0 \\ 0 & 0 & \lambda_{12} & -(\mu_{21}+\lambda_{23}) & 0 & 0 \\ 0 & 0 & 0 & \lambda_{23} & -\lambda_{34} & 0 \\ 0 & 0 & 0 & 0 & \lambda_{34} & 0 \end{bmatrix} \begin{bmatrix} P_0(t) \\ P_{0'}(t) \\ P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \end{bmatrix} = \begin{bmatrix} \dot{P}_0(t) \\ \dot{P}_{0'}(t) \\ \dot{P}_1(t) \\ \dot{P}_2(t) \\ \dot{P}_3(t) \\ \dot{P}_4(t) \end{bmatrix} \quad (1)$$

Eqs. (2)-(7) are separate differential equations based on Eq. (1).

$$\dot{P}_0(t) = -\lambda_{01}P_0(t) + \mu_{0'0}P_{0'}(t), \quad (2)$$

$$\dot{P}_{0'}(t) = \mu_{10'}P_1(t) - (\mu_{0'0} + \lambda_{0'1})P_{0'}(t), \quad (3)$$

$$\dot{P}_1(t) = \lambda_{01}P_0(t) + \lambda_{0'1}P_{0'}(t) - (\mu_{10'} + \lambda_{12})P_1(t) + \mu_{21}P_2(t), \quad (4)$$

$$\dot{P}_2(t) = \lambda_{12}P_1(t) - (\mu_{21} + \lambda_{23})P_2(t), \quad (5)$$

$$\dot{P}_3(t) = \lambda_{23}P_2(t) - \lambda_{34}P_3(t), \quad (6)$$

$$\dot{P}_4(t) = \lambda_{34}P_3(t). \quad (7)$$

Applying the Laplace transform-based method, we solve Eqs. (2)-(7) to obtain the system state probabilities (Xing et al., 2019). The initial state probabilities used are $P_0(0) = 1$ and $\sum_{i=0,0'}^{4} P_i(t) = 1$. Specifically, the Laplace transforms of the six Bitcoin system state probabilities $P_i^*(s)$ (j = 0, 0', 1, 2, 3, 4), are

$$P_{0'}^*(s) = \left(\frac{1}{s} - \frac{1}{s+\lambda_{01}}\right)/\left(1 + \frac{\mu_{0'0}}{s+\lambda_{01}} + \frac{A}{\mu_{10'}} + \frac{\lambda_{01}*A}{\mu_{10'}*B} + \frac{\lambda_{23}*\lambda_{12}*A}{\mu_{10'}*B*(s+\lambda_{34})} + \frac{\lambda_{23}*\lambda_{12}*\lambda_{34}*A}{\mu_{10'}*B*(s+\lambda_{34})*s}\right), \quad (8)$$

$$P_0^*(s) = \frac{\mu_{0'0}*P_{0'}^*(s)+1}{s+\lambda_{01}}, \quad (9)$$

$$P_1^*(s) = \frac{A*P_{0'}^*(s)}{\mu_{10'}}, \quad (10)$$

$$P_2^*(s) = \frac{\lambda_{12}*A*P_{0'}^*(s)}{\mu_{10'}*B}, \quad (11)$$

$$P_3^*(s) = \frac{\lambda_{23}*\lambda_{12}*A*P_{0'}^*(s)}{\mu_{10'}*B*(s+\lambda_{34})}, \quad (12)$$

$$P_4^*(s) = \frac{\lambda_{23}*\lambda_{12}*\lambda_{34}*A*P_{0'}^*(s)}{\mu_{10'}*B*(s+\lambda_{34})*s}, \quad (13)$$

where, $A = s + \mu_{0'0} + \lambda_{0'1}$, and $B = s + \mu_{21} + \lambda_{23}$.

Applying the inverse Laplace transform to $P_i^*(s)$ in Eqs. (8)-(13) (conducted by MATLAB in our work), we obtain the Bitcoin system state probabilities $P_j(t)$ (j = 0, 0', 1, 2, 3, 4) in the time domain. Further, the Bitcoin dependability (the probability that the Bitcoin system performs correctly) is evaluated as $D(t) = P_0(t) + P_{0'}(t) + P_1(t) + P_2(t) + P_3(t)$. Thus, $\overline{D}(t) = P_4(t)$ (the Bitcoin is not dependable since the selfish mining attack is successful under state 4).

5. Numerical Results and Impacts of Model Parameters

In this section, the effects of several key parameters on the Bitcoin dependability are investigated through numerical results. These results could help us gain a better understanding of the selfish mining mechanism.

Based on statistics and survey from Sapirshtein et al. (2016), seven sets of parameter values are designed in Table 1 for the transition rates in Figure 2, including rates related to the selfish miner's attacking behavior or power (λ_{01}, $\lambda_{0'1}$, λ_{12}, λ_{23}, λ_{34}), and rates related to the honest miner's recovery capability ($\mu_{0'0}$, $\mu_{10'}$, and μ_{21}).

In particular, we study the impacts of parameters λ_{01}, λ_{12}, λ_{34}, $\mu_{10'}$, and μ_{21} on the Bitcoin dependability using parameter sets of Table 1. Specifically, (λ_{01}, λ_{12}) reflect the selfish miner's computing power; their impacts are studied via parameter sets *a*, *b*, and *c* in Table 1. λ_{34} models the Bitcoin system's trigger rate; its impacts are examined via parameter sets *d*, *b* and *e*. ($\mu_{10'}$, μ_{21}) reflect the honest miner's recovery capability; their impacts are examined using sets *f*, *b*, and *g* in Table 1.

Table 1. State transition rate (per hour) values used for numerical analysis.

Rate	*Set a*	*Set b*	*Set c*	*Set d*	*Set e*	*Set f*	*Set g*
λ_{01}	0.03	0.12	0.34	0.12	0.12	0.12	0.12
$\lambda_{0'1}$	0.11	0.11	0.11	0.11	0.11	0.11	0.11
λ_{12}	0.06	0.18	0.56	0.18	0.18	0.18	0.18
λ_{23}	0.04	0.04	0.04	0.04	0.04	0.04	0.04
λ_{34}	0.36	0.36	0.36	0.14	0.58	0.36	0.36
$\mu_{0'0}$	0.24	0.24	0.24	0.24	0.24	0.24	0.24
$\mu_{10'}$	0.12	0.12	0.12	0.12	0.12	0.06	0.24
μ_{21}	0.31	0.31	0.31	0.31	0.31	0.15	0.48

5.1 Impacts of Selfish Miner's Computing Power Parameters $\lambda_{01}, \lambda_{12}$

The impacts of the selfish attacker's computing power are examined via parameter sets *a*, *b*, and *c* in Table 1, which model the selfish miner who has relatively low, medium, and high computing power, respectively. These malicious miners sometimes incorporate other attack methods like Eclipse attacks to reinforce their computing power dramatically. Table 2 presents the Bitcoin dependability under sets *a*, *b*, and *c* for several values of mission time. Figure 3 demonstrates the dependability results graphically.

It can be observed from Figure 3 that the Bitcoin dependability decreases with time. The Bitcoin system under set *a* (low computing power of the selfish miner) has the highest dependability *D* and the lowest decreasing speed. The Bitcoin system under set *c* (high computing power of the selfish

miner) has the lowest dependability *D* and decreases with the highest speed. The Bitcoin dependability *D* under set *b* (average computing power of the selfish miner) has values between the former two cases. The above results are intuitive since it is more difficulty for the Bitcoin system to stay in the dependable state when the selfish attacker has a higher computing power. As time proceeds, the difference in the Bitcoin dependability between the low and high computing power cases becomes more significant due to the different declination speeds under these two cases.

Table 2. The bitcoin dependability under sets *a*, *b*, *c*.

***t* (hrs)**	**Set *a***	**Set *b***	**Set *c***
6	0.999486	0.995046	0.974593
12	0.996382	0.970478	0.888651
18	0.990735	0.933354	0.791052
24	0.983527	0.892441	0.700741
30	0.975478	0.851532	0.620233
36	0.967005	0.811891	0.548892

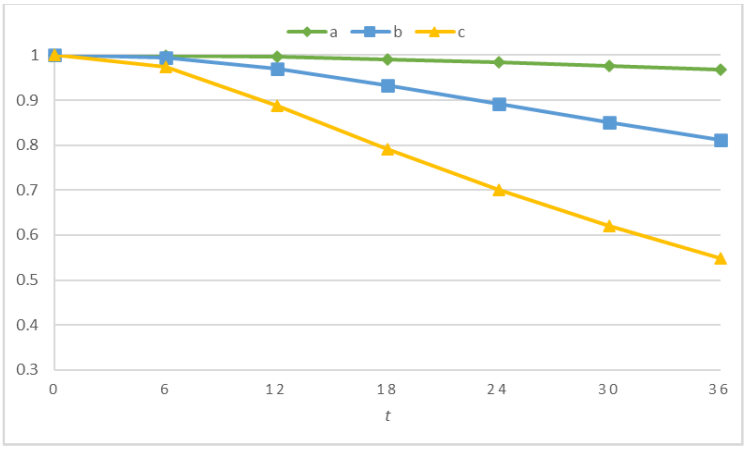

Figure 3. Impacts of parameters $\lambda_{01}, \lambda_{12}$ on the Bitcoin dependability.

5.2 Impacts of Trigger Parameter λ_{34}

In Table 1, the impacts of the attack trigger parameter λ_{34} are examined via parameter sets *d*, *b*, and *e* with low, medium, and high trigger rates, respectively. Table 3 presents the Bitcoin dependability results computed using those three parameter sets. Figure 4 demonstrates the Bitcoin dependability results graphically.

Table 3. The bitcoin dependability under sets *d*, *b*, and *e*.

***t* (hrs)**	**Set *d***	**Set *b***	**Set *e***
6	0.997539	0.995046	0.993512
12	0.982237	0.970478	0.965505
18	0.953978	0.933354	0.926607
24	0.918293	0.892442	0.885231
30	0.879581	0.851531	0.844381
36	0.840341	0.811892	0.804993

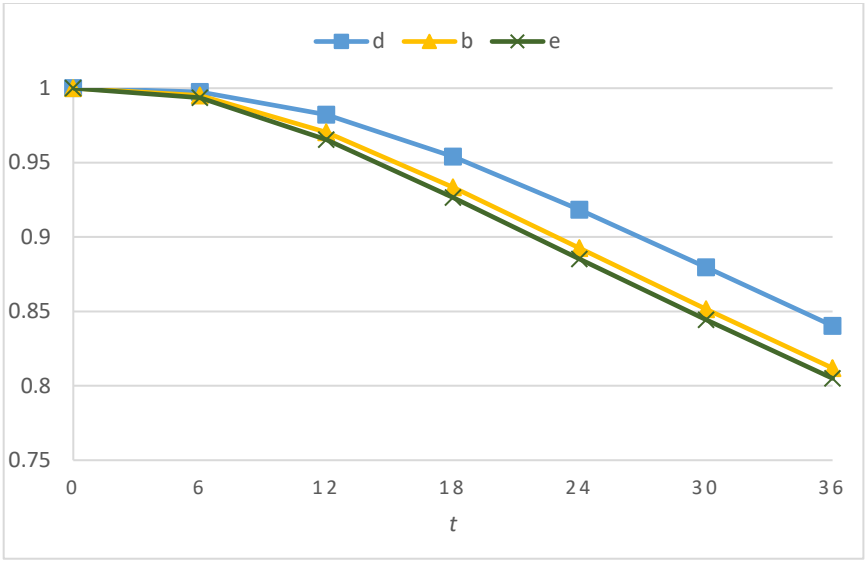

Figure 4. Impacts of parameters λ_{34} on the Bitcoin dependability.

It can be observed from Figure 4 that the Bitcoin system under set *d* (low trigger rate) has the highest dependability *D* and the lowest decreasing speed as time proceeds; the Bitcoin under set *e* (high trigger rate) has the lowest dependability *D* and the highest decreasing speed as time proceeds; the values of *D* under set *b* (medium trigger rate) are between the former two cases. These numerical results are intuitive since the higher trigger rate means it is more likely to realize the last attack step, which eventually leads to the successful selfish mining attack, and hence lower the system dependability. As time proceeds, the difference in the Bitcoin dependability between the low and high trigger rate cases becomes more noticeable at the beginning and then tends to become stable for the considered parameter settings.

5.3 Impacts of Recovery Capability Parameters μ_{10}, μ_{21}

The impacts of the recovery capability parameters μ_{10}, μ_{21} on the Bitcoin dependability are examined via parameter sets *f*, *b*, and *g* in Table 1, where an honest miner has low, average/medium, and high recovery capability, respectively. Table 4 presents the Bitcoin system dependability results under sets *f*, *b* and *g*. Figure 5 demonstrates the results graphically.

Table 4. The Bitcoin dependability under sets *f*, *b*, and *g*.

***t* (hrs)**	**Set *f***	**Set *b***	**Set *g***
6	0.993886	0.995046	0.996187
12	0.958601	0.970478	0.980332
18	0.899313	0.933354	0.959003
24	0.830612	0.892441	0.936624
30	0.761233	0.851531	0.914432
36	0.695032	0.811892	0.892744

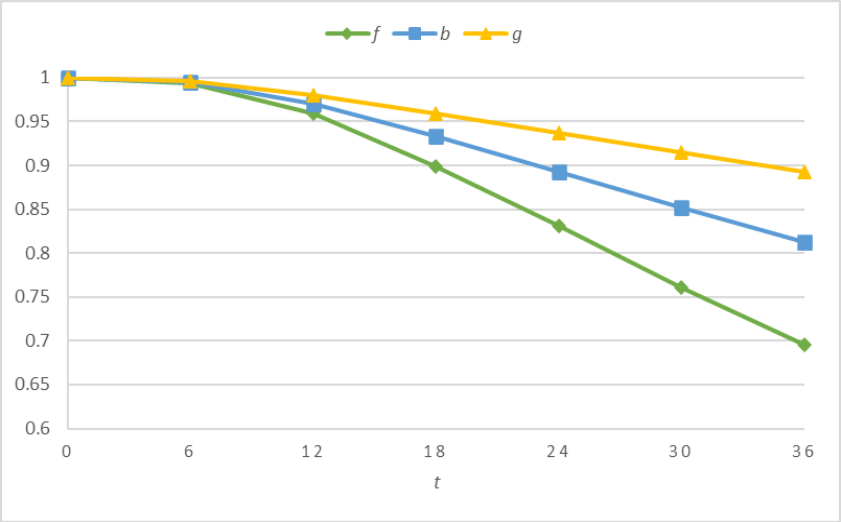

Figure 5. Effects of parameters μ_{10},, μ_{21} on the Bitcoin dependability.

It can be observed from Figure 5 that the Bitcoin system under set *f* (honest miner with low recovery capability) has the lowest system dependability *D* and the highest decreasing speed as time proceeds; the Bitcoin under set *g* (honest miner with high recovery capability) has the highest values of *D* and the lowest decreasing speed among the three cases; the Bitcoin under set *b* (honest miner with average recovery capability) has values of *D* between the former two cases. From the above intuitive results, we can conclude that the Bitcoin system with honest miners having higher recovery capability is more dependable. Moreover, as time proceeds, the difference in the Bitcoin dependability between the low and high recovery capability cases becomes more notable due to the different declination speeds under these two cases.

6. Conclusion and Future Directions

The Bitcoin network is vulnerable to selfish mining attacks, during which a malicious miner withholds the mined block and mines on its own private chain secretly. The existing studies on selfish mining have mostly focused on cryptography and protocol designs, risk detection and damage estimation caused by the adversaries. To defend against selfish mining, it is crucial to study the behavior of selfish mining from the Bitcoin network dependability's perspective. This paper makes contributions to the state of the art by building an analytical dependability model based on the CTMC for the Bitcoin system subject to the selfish mining attack. Numerical results are provided to assess the impacts of several model factors (including selfish miners' computing power, the attack triggering parameter, and honest miners' recovery capability) on the overall Bitcoin dependability. The findings include 1) it is more unlikely that the Bitcoin system stays in the dependable state when the selfish attacker has a higher computing power; 2) the Bitcoin system tends to fail more quickly as the trigger rate increases; and 3) the Bitcoin system tends to be more dependable when its honest miners have better recovery capability.

While the findings from this research are mostly intuitive, the quantitative results and comparisons will provide effective guidance for us to develop resilience algorithms and protocols. Such algorithms can enhance the robustness of the current blockchain-based cryptocurrency network models, improving their self-defense capability against various malicious attacks. In the future

study, we are also interested in extending our dependability analysis to non-exponential state transition times through exploring methods such as semi-Markov models (Zhou et al., 2021b) and multi-integral-based analytical methods (Zeng et al., 2019).

Conflict of Interest

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

Acknowledgments

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

References

Akbari, E., Wu, Q., Zhao, W., Arabnia, H.R., & Yang, M.Q. (2017, December). From blockchain to internet-based voting. In *2017 International Conference on Computational Science and Computational Intelligence* (pp. 218-221). IEEE. Las Vegas, United States.

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.

Bahack, L. (2013). Theoretical Bitcoin attacks with less than half of the computational power (draft). *arXiv preprint arXiv:1312.7013*, https://eprint.iacr.org/2013/868.pdf, Accessed in September 2020.

Bamert, T., Decker, C., Wattenhofer, R., & Welten, S. (2014, September). Bluewallet: The secure bitcoin wallet. In *2014 International Workshop on Security and Trust Management* (pp. 65-80). Springer. Cham, Switzerland.

Bastiaan, M. (2015, January). 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 August 2020.

Best, R. (2021, October). Daily bitcoin market cap history up until October 24, 2021.

Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2021). Unification of blockchain and internet of things (BIoT): requirements, working model, challenges and future directions. *Wireless Networks 27*(1), 55-90.

Dai, H.N., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: a survey. *IEEE Internet of Things Journal*, *6*(5), 8076-8094.

Eyal, I., & Sirer, E.G. (2014, March). Majority is not enough: Bitcoin mining is vulnerable. In *2014 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.

Gervais, A., Ritzdorf, H., Karame, G.O., & Capkun, S. (2015, October). Tampering with the delivery of blocks and transactions in Bitcoin. In *2015 Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 692-705). ACM. Denver, Colorado, 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 *2015 24th USENIX Security Symposium* (pp. 129-144). USENIX Association. Washington D.C., United States. https://www.statista.com/statistics/377382/bitcoin-market-capitalization, Accessed in October 2021.

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.

Koshy, P., Koshy, D., & McDaniel, P. (2014, March). An analysis of anonymity in bitcoin using p2p network traffic. In *2014 International Conference on Financial Cryptography and Data Security* (pp. 469-485). Springer. Berlin, Heidelberg.

Liao, K., Zhao, Z., Doupé, A., & Ahn, G.J. (2016, June). Behind closed doors: measurement and analysis of cryptolocker ransoms in Bitcoin. In *2016 APWG Symposium on Electronic Crime Research* (pp. 1-13). IEEE. Toronto, Canada.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., & Savage, S. (2013, October). A fistful of Bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 Conference on Internet Measurement Conference* (pp. 127-140). ACM. Barcelona, Spain.

Monaco, J.V. (2015, May). Identifying Bitcoin users by transaction behavior. In: Kakadiaris, I.A., Kumar, A., Scheirer, W.J. (eds) *Biometric and Surveillance Technology for Human and Activity Identification XII*. SPIE, Baltimore, Maryland, United States, pp. 25-39.

Motlagh, S.G., Mišić, J., & Mišić, V.B. (2021). The impact of selfish mining on bitcoin network performance. *IEEE Transactions on Network Science and Engineering*, *8*(1), 724-735.

Qin, R., Yuan, Y., & Wang, F.Y. (2020). Optimal block withholding strategies for blockchain mining pools. *IEEE Transactions on Computational Social Systems*, *7*(3), 709-717. doi: 10.1109/TCSS.2020.2991097.

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the Bitcoin system. In: Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A. (eds) *Security and Privacy in Social Networks*. Springer, New York, United States, pp. 197-223.

Rosenfeld, M. (2011). Analysis of Bitcoin pooled mining reward systems. *arXiv preprint arXiv:1112.4980*, Accessed in September 2020.

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

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. *Consulted*, *1*(2012), 28.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084-2123.

Wang, S., Yin, B., Zhang, S., Cheng, Y., Cai, L.X., & Cao, X. (2020). A selfish attack on chainweb blockchain. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference* (pp. 1-6). IEEE. Taipei, Taiwan. doi: 10.1109/GLOBECOM42002.2020.9322246.

Wongthongtham, P., Marrable, D., Abu-Salih, B., Liu, X., Morrison, G. (2021). Blockchain-enabled 2 peer-to-peer energy trading. *Computers & Electrical Engineering*, *94*, 107299.

Xia, Q., Dou, W., Xi, T., Zeng, J., Zhang, F., Wei, J., Liang, G. (2021). The impact analysis of multiple miners and propagation delay on selfish mining. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference* (pp. 694-703). IEEE. Madrid, Spain.

Xing, L. (2020). Reliability in internet of things: current status and future perspectives. *IEEE Internet of Things Journal*, *7*(8), 6704-6721.

Xing, L. (2021). Cascading failures in internet of things: review and perspectives on reliability and resilience. *IEEE Internet of Things Journal*, *8*(1), 44-64.

Xing, L., Levitin, G., & Wang, C. (2019). *Dynamic system reliability: modeling and analysis of dynamic and dependent behaviors*. John Wiley & Sons. Hoboken, New Jersey.

Yang, R., Chang, X., Mišić, J., & Mišić, V.B. (2020). Assessing blockchain selfish mining in an imperfect network: honest and selfish miner views. *Computers & Security*, *97*, 101956.

Zeng, Y., Xing, L., Zhang, Q., & Jia, X. (2019). An analytical method for reliability analysis of hardware-software co-design system. *Quality and Reliability Engineering International*, *35*(1), 165-178.

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., 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), 480-492.