The More Halving Advances, the More Rational Double Spending Attack is

Taishi Nakai
Kyoto University
Kyoto, Japan

Akira Sakurai
Kyoto University
Kyoto, Japan

Kazuyuki Shudo
Kyoto University
Kyoto, Japan

***Abstract*—Several blockchains, such as Bitcoin, feature an event known as a ”halving,” where the reward obtained by miners for mining a block is halved at regular intervals. As halving progresses, the reward for newly issued cryptocurrency per block will decrease, potentially making double-spending attacks more profitable than mining honestly. A double spending attack involves an attacker creating a longer chain to overwrite a transaction that has been included in the main chain, thereby reusing the transaction. This attack was introduced in the Bitcoin paper by Satoshi Nakamoto, the originator of the blockchain concept. However, there has not been sufficient quantitative analysis of double-spending attacks following a halving. This study employs a simulator to calculate the profits from double spending attacks under various parameters in the context of halving. The results show that, 20 years from now, conducting a double spending attack could be more profitable than regular Bitcoin mining if the attacker controls more than 10% of the hash rate. This poses a significant challenge to the foundation of Bitcoin. Furthermore, this research analyzes the causes of this situation and reveals that the resale value ratio of the goods purchased with the transactions used in the double spending attack has a significant impact on the economic rationality of the attacks.**

***Index Terms*—cryptocurrency, security, bitcoin, double spending attack, blockchain, halving**

I. Introduction

Bitcoin. Bitcoin [1] is a decentralized digital currency that operates without reliance on central banks or a single governing authority. It was proposed by Satoshi Nakamoto in 2008 and implemented in 2009. The Bitcoin network uses a peer-to-peer system and a public distributed ledger known as a blockchain to process, validate, and record transactions. One of the most defining characteristics of Bitcoin is its predetermined supply limit, which is set to eventually reach 21 million bitcoins.

Halving. The Bitcoin halving event refers to the reduction of the block reward given to miners by half. This occurs approximately every four years, specifically after every 210,000 blocks. The halving mechanism controls the issuance rate of new bitcoins, thereby mitigating inflation. This process will continue until the maximum supply is reached.

Double-spending attack. A double-spending attack (DSA) is a method in which an attacker attempts to spend the same bitcoin more than once. The attacker sends two conflicting transactions simultaneously and attempts to invalidate one after the other has been confirmed. This attack is particularly effective against transactions with a low number of confirmations and poses a significant security threat to blockchain networks. The concept of double-spending was first addressed in Nakamoto's white paper on Bitcoin. It is generally considered that a transaction achieves finality once six blocks, including the block containing the transaction, have been added to the main chain. This is commonly referred to as the “six-block finality” rule.

Challenge. As the halving events reduce mining rewards, performing a double-spending attack might become more economically appealing to certain miners compared to regular mining activities. However, there has been limited quantitative analysis of this possibility.

As previously mentioned, Satoshi Nakamoto calculated the probability that an attacker would catch up with honest miners during a double-spending attack, but this calculation assumes that the attacker has unlimited resources, and it does not consider the profitability of the attacker at all. Gervais et al. [2] and Suliyanti [3] simulated double-spending attacks using a simulator and calculated the rewards. Cyril et al. [4] theoretically calculated the number of blocks required for finality, taking into account the profitability of double-spending attacks, rather than the traditional 6-block finality. Additionally, Jehyuk et al. [5] theoretically demonstrated that an attacker could execute a double-spending attack within a finite time. Moroz et al. [6] evaluated double-spending attacks economically, considering the costs associated with such attacks. However, Gervais et al., Suliyanti, Cyril et al., Jehyuk et al., and Moroz et al. did not sufficiently consider the impact of halving periods. Auer [7] showed that the time required for finality increases when considering the profitability of double-spending attacks in relation to halving periods. However, Auer did not consider the resale price ratio of assets obtained through double-spending attacks or the attack resources that the attacker needs to prepare. Additionally, his study only considers cases where 51% of the hash rate is rented, without accounting for the possibility that existing miners could conduct a double-spending attack precisely. Budish [8] investigated the economic incentives for 51% attacks in cases where attackers rent hash power, as well as cases where existing miners turn into attackers. However, his study does not consider the resale price ratio of assets obtained through double-spending attacks, nor does it model

This work was supported by JSPS KAKENHI Grant Numbers JP21H04872 and JP24H00691, JST ACT-X Grant Number JPMJAX24M9, and JST BOOST Grant Number JPMJBS2407.

Proc. IEEE 43rd Int'l Conf. on Consumer Electronics
(IEEE ICCE 2025), January 2025

the probability of successful attacks when less than 51% of the hash rate is prepared. Rosenfeld [9] calculated the rewards of double-spending attacks while considering the resale price ratio. However, his study assumes that attackers have unlimited financial resources and does not take halving periods into account.

Contributions. In this study, we analyze the economic feasibility of double-spending attacks in the context of Bitcoin halving, assuming attackers have limited resources and a constrained attack duration. Using a simulator, we show that the resale price ratio significantly contributes to the profitability of double-spending attacks. We also find that under certain conditions, it becomes more profitable to engage in double-spending attacks than to continue regular mining as halving progresses. Specifically, in non-bubble periods, if an attacker spends 15 BTC on a double-spending attack, it would be economically rational to perform the attack 20 years after the halving, provided the resale price ratio is 0.99 and the attacker controls at least 30% of the hashrate, 1.00 with at least 25%, or 1.01 with at least 10%.

II. Experiments

We conducted simulations of double-spending attacks under various parameter settings. We then calculated the attacker's profit based on different sets of parameters and compared it to the profits from regular mining activities.

First, in Section II-A, we describe the double-spending attack strategy used in our simulations. Section II-B details the execution of the double-spending attack simulation. In Section II-C, we define several parameters and calculate the attacker's profit based on the simulation results. Finally, Section II-D analyzes the profitability of double-spending attacks. Table I summarizes the variables and constants used in both the simulation and profitability calculations for the double-spending attacks.

A. Double-Spending Attack Strategy

The transaction used for the double-spending attack is referred to as the DSA transaction. The attacker is assumed to be an existing miner. We consider a time limit for the attacker because their resources for carrying out the attack are limited. First, the attacker broadcasts the DSA transaction to the network, purchasing goods with it. Once honest miners include the transaction in a block, the attacker initiates the attack, starting the countdown for the attack duration. The attacker wins if the number of blocks they generate exceeds the number of blocks generated by honest miners, after at least z blocks containing the DSA transaction have been added to the main chain. If the attack duration exceeds the attacker's time limit, the attacker loses. The purchased goods are converted into currency after the DSA transaction achieves z-block finality, and the value is measured in Bitcoin.

Algorithm 1 calculates the attacker's win condition, the time taken for the attack to conclude, and the number of blocks generated by the attacker during the DSA.

Algorithm 1 Simulate Double Spending Attack

```
Require: $\beta$: attacker's hash rate ratio, $at$: attacker's time limit
Ensure: Returns tuple of win flag, end time, and block height
$T \leftarrow 600$ {Average time between blocks (seconds)}
$z \leftarrow 6$ {Number of blocks required for finality}
$currentTime \leftarrow 0.0$
$finTime \leftarrow 0$
$attackerBlockHeight \leftarrow 0$
$honestBlockHeight \leftarrow 1$
$winFlag \leftarrow$ false
while true do
    $timeForBlock \leftarrow$ GenerateBlockTime($T$)
    if $currentTime + timeForBlock > at$ then
        $winFlag \leftarrow$ false
        $finTime \leftarrow at$
        break
    end if
    if $\beta \geq$ rand()/RAND_MAX then
        $currentTime \leftarrow currentTime + timeForBlock$
        $attackerBlockHeight \leftarrow attackerBlockHeight + 1$
    else
        $currentTime \leftarrow currentTime + timeForBlock$
        $honestBlockHeight \leftarrow honestBlockHeight + 1$
    end if
    if $attackerBlockHeight \geq z$ and $attackerBlockHeight > honestBlockHeight$ then
        $winFlag \leftarrow$ true
        $finTime \leftarrow currentTime$
        break
    end if
end while
return ($winFlag, finTime, attackerBlockHeight$)
```

B. Simulation

We first set the attacker's hash rate β and time limit t_{limit}, then performed $1,000,000$ simulations, measuring the outcome w_i, the attack duration $t_{attack,i}$, and the number of blocks generated by the attacker a_{Blocks}. We ran simulations with eight values for β (0.1, 0.15, 0.2, 0.25, 0.3, 0.35, 0.4, 0.45) and 24 values for t_{limit} (from 1 to 24 hours, in 1-hour increments), resulting in 192 total simulations. The finality parameter z was set to 6, and the average block generation interval T was set to 600 seconds, based on actual Bitcoin settings.

Figure 1 shows a graph plotting the attacker's win rate as a function of the attack time limit. Figure 2 shows the expected number of blocks generated by the attacker, conditional on a win, as a function of the attack time limit. Figure 3 plots the expected duration of successful attacks against the attack time limit.

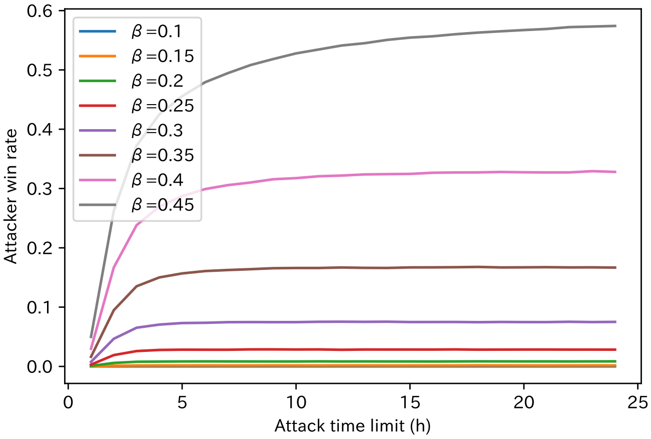

Fig. 1. Attacker win rate as a function of the attack time limit.

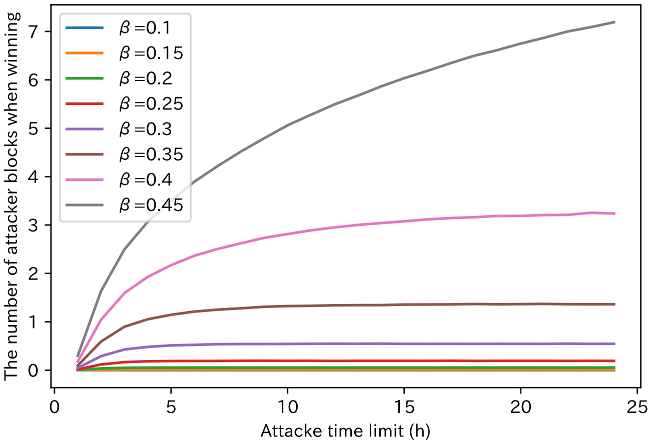

Fig. 2. Expected number of blocks generated by the attacker upon a win as a function of the attack time limit.

C. Profit Calculation

Based on the attacker's hash rate ratio β, the time limit of the attack t_{limit}, the outcome w_i for each attempt, the end time of the game $t_{attack,i}$, and the number of blocks generated by the attacker a_{Blocks}, we calculate the profit. The profit is derived by solving the system of equations from Eq. (1) to Eq. (4).

$$\begin{aligned} E_{dsa} = \frac{1}{n}\sum_{i=1}^{n} w_i(R_B \cdot a_{Blocks,i} + R_{dsa}) \\ + R_{dsa} \cdot Rate_{resell} \\ - \frac{1}{n}\sum_{i=1}^{n} t_{attack,i} \cdot c \cdot \beta - R_{dsa} \end{aligned} \tag{1}$$

$$R_B = R_{base} + R_{tx} \tag{2}$$

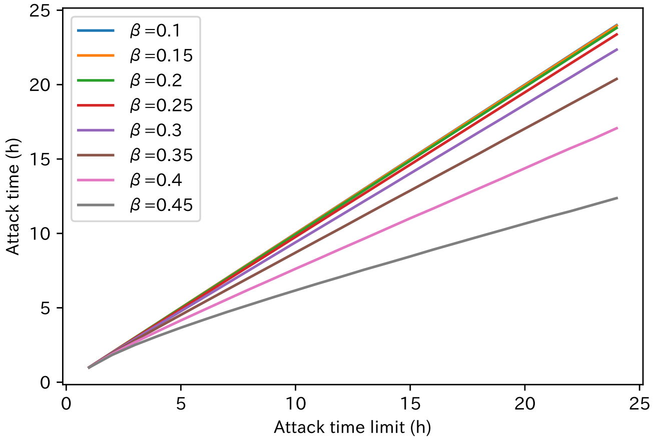

Fig. 3. Expected attack duration as a function of the attack time limit.

$$R_{base} = \frac{R_{standard}}{2^{n_{halving}}} \tag{3}$$

$$c = \frac{R_B \cdot c_{btc}}{T} \tag{4}$$

The equation for the attacker's profit, Eq. (1), represents the total reward per block R_B when a double-spending attack succeeds, plus the reward from the double-spending attack transaction R_{dsa}, and the value of goods purchased through the attack $R_{dsa} \cdot Rate_{resell}$, from which the mining cost incurred during the attack and the double-spending transaction R_{dsa} are subtracted. Eq. (3) calculates the reward for newly issued bitcoins included in one block, considering the halving period. Eq. (4) shows the mining cost per second (BTC/s) for the entire network's hash rate.

Furthermore, by combining Eq. (1) and Eq. (4), it can be expressed as follows:

$$\begin{aligned} E_{dsa} = \{Blocks_{win}(\beta, t_{limit}) - \frac{\beta \cdot c_{btc}}{T} \cdot t_{attack}(\beta, t_{limit})\} \cdot R_B \\ + \{Rate_{win}(\beta, t_{limit}) - 1 + Rate_{resell}\} \cdot R_{dsa} \end{aligned} \tag{5}$$

where $Rate_{win}(\beta, t_{limit})$, $Blocks_{win}(\beta, t_{limit})$, and $t_{attack}(\beta, t_{limit})$ are expressed by the following equations. These are also illustrated in the graphs shown in Figures 1, 2, and 3, respectively.

$$Rate_{win}(\beta, t_{limit}) = \frac{1}{n}\sum_{i=1}^{n} w_i \tag{6}$$

$$Blocks_{win}(\beta, t_{limit}) = \frac{1}{n}\sum_{i=1}^{n} w_i \cdot a_{Blocks,i} \tag{7}$$

$$t_{attack}(\beta, t_{limit}) = \frac{1}{n}\sum_{i=1}^{n} t_{attack,i} \tag{8}$$

TABLE I
VARIABLES AND DESCRIPTIONS USED IN THE SIMULATION AND PROFIT CALCULATION FOR DSA.

Symbols	Description
β	The attacker's hash rate as a proportion of the total network hash rate. The proportion of the hash rate for honest miners is $1 - \beta$.
t_{limit}	The attacker's time limit for the attack. The attacker has a limited budget, which restricts the duration of the attack.
$t_{attack,i}$	The actual attack time (s) in the i-th simulation. If the attack duration exceeds t_{limit} and the double-spending attack is unsuccessful, the game ends, and t_{attack} is set to t_{limit}.
z	The number of additional blocks required for a transaction to be considered final once it is included in the main chain. The block containing the transaction is also included in this count.
E_{dsa}	The expected profit from the double-spending attack (BTC).
R_{dsa}	The amount of the DSA transaction (BTC), representing the reward specific to the success of the double-spending attack.
$Rate_{resell}$	The resale price ratio for goods obtained via the DSA transaction.
R_B	The reward per block (BTC), given by $R_B = R_{base} + R_{tx}$.
R_{base}	The reward for newly minted bitcoins included in a block (BTC).
R_{tx}	The average transaction fee reward per block (BTC).
$n_{halving}$	The number of halving events.
$R_{standard}$	The standard block reward for newly minted bitcoins (BTC). For example, if the period from 2020.5 to 2024.3 is the standard, $R_{standard}$ is 6.25 BTC, and for the period 2024.4 to 2028, it is 3.125 BTC.
w_i	The outcome of the i-th simulation. 1 if the attacker wins, 0 if the attacker loses.
$a_{Blocks,i}$	The number of blocks generated by the attacker in the i-th simulation.
c	The cost per second of mining with the total network hash rate (BTC/s).
c_{btc}	The cost of mining 1 bitcoin.
T	The average block generation interval (s).
n	The number of simulations executed.

Varying the attacker's hash rate β and the attack time limit t_{limit}, we calculate the expected profit of the attacker Eq. (1). Since the profit from regular mining is 0, a double-spending attack is economically viable if the attacker's profit exceeds 0.

The parameters used to calculate the profit are set to the following values. There are a total of 54 parameter combinations used to calculate the profit.

TABLE II
MINIMUM ATTACKER'S HASH RATE RATIO AND ATTACK TIME LIMIT WHEN $E_{dsa} > 0$ FOR $n_{halving} = 0$, $R_{tx} = 0$.

R_{dsa} $Rate_{resell}$	15	30	150
0.99	\	\	0.35, 2
1.00	\	\	0.35, 2
1.01	\	\	0.35, 2

- Parameters to vary:
  - $n_{halving}$
    Three values are set: 0, 1, and 5. A halving period in Bitcoin occurs every four years, where 0 represents the recent state from 2020.5 to 2024.3, 1 represents the next halving period from 2024.3 to 2028, and 5 represents the situation 20 years from now.
  - R_{dsa}
    Three values are set: 15, 30, and 150 BTC. 15 BTC is approximately ¥100,000,000 (as of February 8, 2024, where 1 BTC = ¥6,403,062, $1 = ¥148.15 [10]). The values were set at 2 times and 10 times the base amount of 15 BTC.
  - R_{tx}
    Two values are set: 0 and 7.40 BTC. The value of 7.40 was set based on the peak value during the bubble (December 23, 2017). As described by Raphael [7], when there is no bubble, the value tends to approach 0, so we also set it to 0.
  - $Rate_{resell}$
    Three values are set: 0.99, 1.00, and 1.01. The values of 0.99 and 1.00 represent cases where the spread for purchasing (exchanging) non-Bitcoin currencies at a centralized exchange is 1% or nearly 0%, respectively. The value of 1.01 represents a case where the price of the non-Bitcoin currency rises by 1%.
- Fixed parameters:
  - $R_{standard}$
    Set at 6.25 BTC based on the recent state from 2020.5 to 2024.3.
  - c_{btc}
    A miner will not spend more than 1 BTC to mine 1 BTC, so this is set to 1 BTC.

For each parameter combination, we calculate the profit. We record the minimum attacker hash rate at which the profit becomes non-negative, and the combination of the lowest necessary attack resources, that is, the combination with the shortest attack time limit. The results are summarized in Tables II to VII. The number on the left of the comma represents the attacker's hash rate ratio, and the number on the right represents the attack time limit (in hours h). If there is no minimum attacker hash rate at which the profit becomes non-negative, a slash is drawn in the table. An example of how to fill out the table is shown. Figures 4 and 5 show the expected profit for the attacker in relation to the attack time limit when $n_{halving} = 0$, $R_{tx} = 0$, $R_{dsa} = 30$, and $Rate_{resell} = 1.00$, and when $n_{halving} = 5$, $R_{tx} = 0$, $R_{dsa} = 30$, and $Rate_{resell} = 1.00$, respectively. For Figure 4, none of the attacker's hash rates result in a profit greater than 0. Therefore, a slash is drawn in the $R_{dsa} = 30$, $Rate_{resell} = 1.00$ row of Table II. In contrast, for Figure 5, an attacker hash rate of 25% or more results in a profit greater than 0, and the shortest attack time limit is 2 hours. Hence, $0.25, 2$ is entered in the $R_{dsa} = 30$, $Rate_{resell} = 1.00$ row of Table VI.

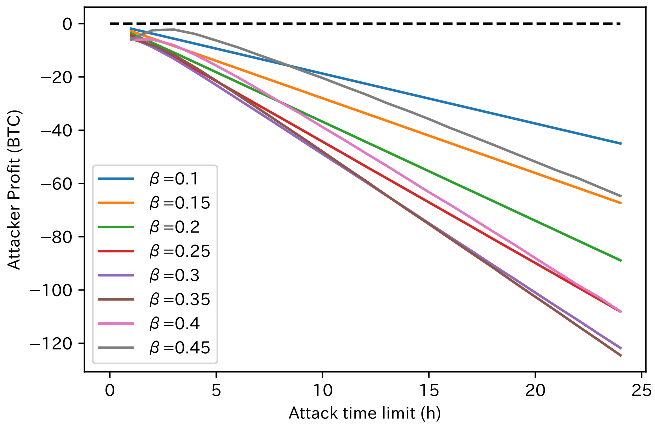

Fig. 4. Expected attacker's profit versus attack time limit when $n_{halving} = 0$, $R_{tx} = 0$, $R_{dsa} = 30$, $Rate_{resell} = 1.00$

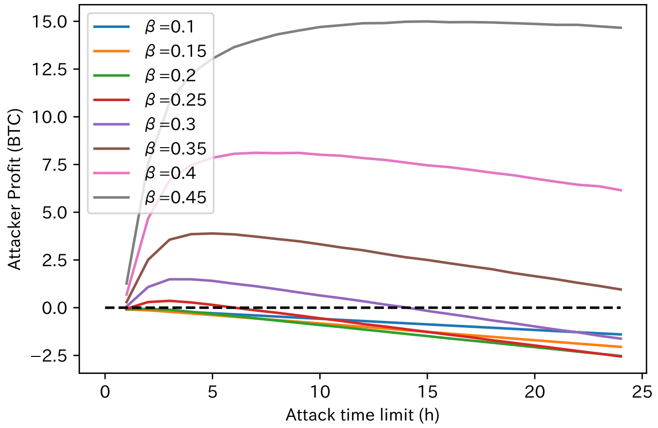

Fig. 5. Expected attacker's profit versus attack time limit when $n_{halving} = 5$, $R_{tx} = 0$, $R_{dsa} = 30$, $Rate_{resell} = 1.00$

D. Analysis of Results

The following three points can be inferred from Tables II to VII. We analyze each point:

- The economic rationality of conducting double-spending attacks increases as the halving progresses.
- Lower transaction fee rewards enhance the economic rationality of conducting double-spending attacks.
- As the halving progresses, the impact of the resell price ratio on the profitability of double-spending attacks increases.

TABLE III
MINIMUM ATTACKER'S HASH RATE RATIO AND ATTACK TIME LIMIT WHEN $E_{dsa} > 0$ FOR $n_{halving} = 0$, $R_{tx} = 7.40$.

R_{dsa} $Rate_{resell}$	15	30	150
0.99	\	\	0.45, 2
1.00	\	\	0.45, 2
1.01	\	\	0.45, 2

TABLE IV
MINIMUM ATTACKER'S HASH RATE RATIO AND ATTACK TIME LIMIT WHEN $E_{dsa} > 0$ FOR $n_{halving} = 1$, $R_{tx} = 0$.

R_{dsa} $Rate_{resell}$	15	30	150
0.99	\	0.45, 2	0.3, 2
1.00	\	0.45, 2	0.3, 2
1.01	\	0.45, 2	0.1, 1

TABLE V
MINIMUM ATTACKER'S HASH RATE RATIO AND ATTACK TIME LIMIT WHEN $E_{dsa} > 0$ FOR $n_{halving} = 1$, $R_{tx} = 7.40$.

R_{dsa} $Rate_{resell}$	15	30	150
0.99	\	\	0.45, 2
1.00	\	\	0.45, 2
1.01	\	\	0.45, 2

1) Economic Rationality of Double-Spending Attacks with Halving Progression: Comparing Tables II, IV, and VI, we observe that as the halving progresses, the attacker's hash rate required for the double-spending attack's profit to become greater than or equal to zero decreases, making double-spending attacks easier to execute.

As per Equation (3), R_{base} decreases with each halving. Since $R_{tx} = 0$, R_B also approaches zero with each halving. Figure 6 shows the coefficient of R_B in Equation (5) against the attack time limit when $T = 600(s)$ and $c_{btc} = 1.0$. As it is always negative, when R_B decreases, the influence of this coefficient diminishes, improving the profitability of the attack. Consequently, the economic incentive for double-spending attacks increases as the halving progresses.

2) Economic Rationality of Double-Spending Attacks Due to Low Transaction Fee Rewards: Comparing Tables VI and VII, we observe that when transaction fee rewards are lower, the attacker's hash rate required for the double-spending attack's profit to become greater than or equal to zero decreases, making double-spending attacks easier to execute.

TABLE VI
MINIMUM ATTACKER'S HASH RATE RATIO AND ATTACK TIME LIMIT WHEN $E_{dsa} > 0$ FOR $n_{halving} = 5$, $R_{tx} = 0$.

R_{dsa} $Rate_{resell}$	15	30	150
0.99	0.3, 2	0.25, 3	0.25, 2
1.00	0.25, 2	0.25, 2	0.15, 2
1.01	0.1, 1	0.1, 1	0.1, 1

TABLE VII
MINIMUM ATTACKER'S HASH RATE RATIO AND ATTACK TIME LIMIT WHEN $E_{dsa} > 0$ FOR $n_{halving} = 5$, $R_{tx} = 7.40$.

R_{dsa} $Rate_{resell}$	15	30	150
0.99	\	\	0.45, 2
1.00	\	\	0.45, 2
1.01	\	\	0.4, 2

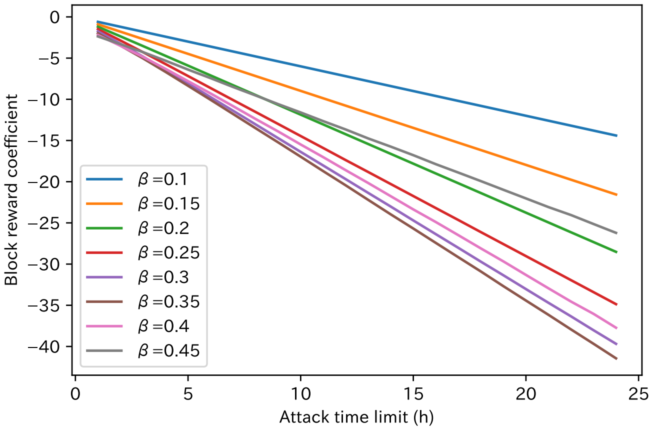

Fig. 6. Coefficient of R_B in Equation (5) against the attack time limit

From Equation (2), when R_{tx} decreases, R_B also decreases. As R_B decreases, the same mechanism as in Section II-D1 applies, making double-spending attacks easier. Consequently, lower transaction fee rewards increase the economic incentive for double-spending attacks.

3) Impact of Resell Price Ratio on Profitability of Double-Spending Attacks with Halving Progression: In Tables II, III, IV, V, and VII, changes in the value of $Rate_{resell}$ have little impact on the profitability of double-spending attacks. On the other hand, in Table VI, where the halving has progressed and transaction fee rewards are low due to the absence of a cryptocurrency bubble, we observe that as $Rate_{resell}$ increases, the attacker's hash rate required for the double-spending attack's profit to become greater than or equal to zero decreases, making double-spending attacks easier.

In Equation (5), the term $Rate_{win}(\beta, t_{limit}) - 1$ in the coefficient of R_{dsa} is always negative, as seen from the values in Figure 1. Therefore, unless $Rate_{resell}$ is such that $Rate_{win}(\beta, t_{limit}) - 1 + Rate_{resell}$ becomes greater than zero, the attacker's profit E_{dsa} will not be positive regardless of how large R_{dsa} is. Moreover, not only must $Rate_{win}(\beta, t_{limit}) - 1 + Rate_{resell}$ be positive, but it must also be larger than $\{Blocks_{win}(\beta, t_{limit}) - \frac{\beta \cdot c_{btc}}{T} \cdot t_{attack}(\beta, t_{limit})\} \cdot R_B$.

If the halving has not progressed or the transaction fee reward R_{tx} is large, as analyzed in Sections II-D1 and II-D3, R_B does not decrease, and the influence of the negative coefficient of R_B in Equation (5) becomes significant. Therefore, unless the R_{dsa} is large, the profit from the double-spending attack will not be positive. However, if the halving has progressed and the transaction fee reward R_{tx} is small, the profit from the double-spending attack may become positive even if R_{dsa} is not so large.

Furthermore, focusing on the term $Rate_{win}(\beta, t_{limit}) - 1 + Rate_{resell}$ in the coefficient of R_{dsa} in Equation (5), when the attacker's hash rate ratio is small, $Rate_{win}(\beta, t_{limit})$ takes a value close to zero (Figure 1). Therefore, depending on the value of $Rate_{resell}$, the attacker's hash rate ratio required for the DSA's profit to become greater than or equal to zero can vary significantly

III. Conclusion

During the recent cryptocurrency bubble period, it is not economically rational to conduct a double-spending attack unless the attacker prepares a double-spending transaction of 150 BTC and holds a hash rate share of 45%. On the other hand, during non-bubble periods, it was found that preparing a double-spending transaction of only 15 BTC would be economically rational if the attacker has a hash rate share of at least 30% with a resale price ratio of 0.99, at least 25% with a resale price ratio of 1.00, or at least 10% with a resale price ratio of 1.01, compared to regular mining. This is because:

- As the halving progresses, R_B becomes smaller, reducing the influence of the negative coefficient of R_B in Equation (5).
- Lower transaction fee rewards make R_B smaller, reducing the influence of the negative coefficient of R_B in Equation (5).
- The profitability of DSAs cannot become positive unless the coefficient of R_{dsa} in Equation (5), $Rate_{win}(\beta, t_{limit}) - 1 + Rate_{resell}$, becomes positive. Therefore, the value of the resale price ratio $Rate_{resell}$ is crucial. In particular, when the attacker has only a small hash rate, the win rate of the DSA is close to 0, so changes in the value of $Rate_{resell}$ around 1.00 greatly affect the profitability of the DSA, determining the threshold of the attacker's hash rate at which double-spending becomes economically rational.

The fact that conducting a double-spending attack can be more economically rational than regular mining is a fundamental issue for Bitcoin. Future research will focus on developing methods to address this incorrect economic rationality of double-spending attacks.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 3–16, 2016.

[3] Widya Nita Suliyanti and Riri Fitri Sari. Evaluation of hash rate-based double-spending based on proof-of-work blockchain. In *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 169–174, 2019.

[4] Cyril Grunspan and Ricardo Pérez-Marco. On profitability of nakamoto double spend. *Probability in the Engineering and Informational Sciences*, 36(3):732–746, 2022.

[5] Jehyuk Jang and Heung-No Lee. Profitable double-spending attacks. *Applied Sciences*, 10(23):8477, 2020.

[6] Daniel J Moroz, Daniel J Aronoff, Neha Narula, and David C Parkes. Double-spend counterattacks: Threat of retaliation in proof-of-work systems. *arXiv preprint arXiv:2002.10736*, 2020.

[7] Raphael Auer. Beyond the doomsday economics of'proof-of-work'in cryptocurrencies. 2019.

[8] Eric Budish. The economic limits of bitcoin and the blockchain. Technical report, National Bureau of Economic Research, 2018.

[9] Meni Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.

[10] MUFG. The exchange rate on february 8, 2024. https://www.murc-kawasesouba.jp/fx/past/index.php?id=240208 (access on 10/16/2024).