How much is the fork? Fast Probability and Profitability Calculation during Temporary Forks

Aljosha Judmayer
aljosha.judmayer@univie.ac.at
University of Vienna and SBA Research

Nicholas Stifter
nicholas.stifter@univie.ac.at
University of Vienna and SBA Research

Philipp Schindler
pschindler@sba-research.org
University of Vienna and SBA Research

Edgar Weippel
edgar.weippl@univie.ac.at
University of Vienna

ABSTRACT

Estimating the probability, as well as the profitability, of different attacks is of utmost importance when assessing the security and stability of prevalent cryptocurrencies. Previous modeling attempts of classic chain-racing attacks have different drawbacks: they either focus on theoretical scenarios such as infinite attack durations, do not account for already contributed blocks, assume honest victims which immediately stop extending their chain as soon as it falls behind, or rely on computationally heavy approaches which render them ill-suited when fast decisions are required. In this paper, we present a simple yet practical model to calculate the success probability of finite attacks, while considering already contributed blocks and victims that do not give up easily. Hereby, we introduce a more fine grained distinction between different actor types and the sides they take during an attack. The presented model simplifies assessing the profitability of forks in practical settings, while also enabling fast and more accurate estimations of the economic security grantees in certain scenarios. By applying and testing our model in the context of bribing attacks, we further emphasize that approaches where the attacker compensates already contributed attack-chain blocks are particularly cheap. Better and more realistic attack models also help to spot and explain certain events observed in the empirical analysis of cryptocurrencies, or provide valuable directions for future studies. For better reproducibility and to foster further research in this area, all source code, artifacts and calculations are made available on GitHub.

KEYWORDS

Cryptocurrency, Forks, Attack Probability, Attack Profitability

1 INTRODUCTION

Whenever a miner in a permissionless Proof-of-Work (PoW) cryptocurrency detects a fork, this miner has to make a decision which chain to extend, i.e, where to best utilize her hashrate. As a profit-oriented and economically rational miner, she would want to select the chain which offers the higher expected profit for the next block as fast as possible. Optimizing for maximum profit, other revenue opportunities besides the block reward of the next block, such as a *bribe* [1], or some other way to increase the miner extractable value (MEV) [2, 3, 12], also have to be taken into account. We present and apply a simple model, that is precisely tailored towards the question of selecting the most profitable branch of a fork, as well as assessing the probability of this branch becoming canonical.

Modeling the security of PoW cryptocurrencies has been addressed from several different angles. One of the first approaches by Rosenfeld [13] highlights that successful double-spending is possible with any attacker hashrate (no majority is needed), assuming that all non-attacking nodes are honest and accept the attack chain as soon as it becomes the longest/heaviest chain. Thereby, an infinite attack duration is implicitly assumed from the perspective of the attacker. Moreover, potential incentives of participants are ignored. Liao and Katz [8] extend the analysis from Rosenfeld [13] in the context of chain forks incentivized by whale transactions, i.e., transactions which carry an exceptionally high fee which can be viewed as a bribe. Their model is simple and specifically tailored for bribing, but does not account for already contributed blocks, finite attacks, and victims that do not accept longer chains immediately. In this paper, we build upon the model of Liao and Katz [8] and extend it through finite Markov chains. In context of cryptocurrencies, Markov chains have mainly been used to model selfish-mining [4, 11], however, to the best of our knowledge, not directly to model double-spending or bribing attacks.

Markov decision processes (MDP) were successfully used in the past to model certain security aspects of PoW cryptocurrencies such as selfish-mining [5, 14], or double-spending [5, 18]. The double-spending MDP in [5] is quite versatile and incorporates a lot of parameters (for example stale block rate and network connectivity). On the down side, it assumes that the *exit* state is reached as soon as the adversarial chain is ahead of the main chain. This assumption though may not hold in practice, in particular when economically rational victims are considered. Moreover, adapting existing MDP based approaches to account for already contributed blocks to the fork/main chain regarding the profitability is not straight forward, as it would require a substantial change in the design of currently available MDPs. We avoid this issue, by using a Markov chain solely to calculate the required probabilities and embed these in a formula that accounts for already contributed blocks to each chain. Last but not least, evaluating finite complex MDPs and applying binary search to find the maximum reward is more time consuming than evaluating a finite Markov chain. As the run time heavily depends on the chosen model and concrete parameterization, an accurate comparison is of course impossible if the underlying model is not exactly the same, but to give the reader some intuition we provide an approximation assuming a current desktop computer as underlying hardware: in this case, a broadly used MDP [5, 18] for finding optimal strategies has a runtime in the range of multiple minutes,

whereas our approach provides results within milliseconds, parameterized for practical fork ranges of around 6 blocks. Even when parameterized for forks that are multiple thousand blocks long, our approach still provides results within seconds. This is possible since the required calculations consist mainly of matrix multiplications and closed form formulas. In summary, our approach complements established MDPs used to find optimal strategies, as it does not incorporate network latency or stale block rate, but it provides a practically oriented and quickly computable model that also takes economically rational victims and already contributed blocks into account. Therefore, our approach poses a viable alternative, especially for scenarios where the overhead imposed by MDPs is undesired or unacceptable. All source code as well as all generated artefacts can be found on GitHub[1].

Also from an empirical analysis point of view, better models for attacks on prevalent cryptocurrencies are helpful, as they might offer explanations for observed fork patterns, or provide valuable directions for future studies and measurements which aim to detect forking patterns related to malicious activities of miners.

1.1 Related Work

As we discussed previously in the beginning of this introduction, in the context of cryptocurrencies, Markov chains have mainly been used to model selfish-mining [4, 11]. More complex, Markov decision processes have been used to model selfish-mining [5, 14] as well as double-spending [5, 18]. Closest to our approach is the line of research regarding the analysis of double-spending starting with Rosenfeld [13], which was extended by Liao and Katz [8] to incorporate a basic notion of bribing/incentives. This is also the model which we extend upon in the paper at hand.

Lately, a series of works has empirically analyzed and automated the discovery and possible exploitation of MEV opportunities [2, 16, 19, 20]. Our work is orthogonal to this line of research and may best be compared by elaborating on the question whether or not to join/or initiate a blockchain fork to hunt a missed MEV opportunity. At the end of Zhou et al. [18] this question has also been raised and was briefly addressed using the MDP from Gervais et al. [5], to derive thresholds for the required minimum MEV value and hashrate required to justify a fork. Our work can be seen as an extension to this question from a different angle, without the previously mentioned drawbacks of an MDP based approach, while accounting for already contributed blocks to a fork and economically rational victims.

1.2 Structure of this Paper

In this paper, we aim to model and analyze a range of different attacks from the perspective of an individual miner. These include classical longest chain races [13], but also bribing [1] and other attacks involving additional income, such as MEV opportunities [2, 18] and algorithmic incentive manipulation attacks [7]. In Section 2 we first extend the system model provided by Judmayer et al. [6, 7], for example by allowing the victims to have hashrate. In Section 3 we build up and extend the calculation approach presented by Liao and Katz [8]. In Section 3.1 we first describe their original approach using our newly introduced notation from Section 2. We consider already contributed blocks in Section 3.2, economically rational victims as well as finite attacks with different pain thresholds for actors in Section 3.3 and economically incentivized attacks with effort-related compensation approaches in Section 3.4.

2 ROLES, TYPES AND SIDES OF PLAYERS

In this work, the focus of our analysis is soly on miners, nevertheless to increase the extensibility of our model and to offer a defintion for further discussions, we differentiate between two player *roles* (*miner* and *user*) and three player *types* (*altruistic*, *Byzantine* and *rational*). Each player must have *one* role and at the same time fall into *one* of three types of actors[2]. In general, roles define the capabilities of a player, whereas player types define their overall strategic behaviour. Additionally, during an attack the actors of the type *rational player* can be on one of three *sides* (*extractors*, *victim* and *indifferent*). On which side a rational player will be during an attack depends on various factors which influence the value at stake for the respective player, for example already contributed blocks to a chain. The set of all players is denoted $\mathcal{P}$ and the number of players is $|\mathcal{P}|$. The sets of players are denoted in calligraphic letters, e.g., $\mathcal{A}, \mathcal{B}, \mathcal{R}, \mathcal{M}, \mathcal{U}$, where $\mathcal{P} = \mathcal{M} \cup \mathcal{U} = \mathcal{A} \cup \mathcal{B} \cup \mathcal{R}$.

2.1 Player Roles

The roles define the capabilities of a player. If player i controls some hashrate p_i, where $\sum_{i=1}^{|\mathcal{P}|} p_i = 1$, he is part of the set of miners $\mathcal{M}$ and thus termed a miner. The number of miners in $\mathcal{P}$ is denoted with $|\mathcal{M}|$. If a player does not control any hashrate, he is part of the set of users $\mathcal{U}$ and thus termed a user. The number of users in $\mathcal{P}$ is denoted with $|\mathcal{U}|$. It holds that $\sum_{i=1}^{|\mathcal{M}|} p_i = 1$, whereas $\sum_{i=1}^{|\mathcal{U}|} p_i = 0$.

2.2 Player Types

The different types define the general strategic behaviour of a player. For our analysis, we uniquely assign a player $i \in \mathcal{P}$ to one of three mutually disjoint actor types, s.t. $\mathcal{P} = \mathcal{A} \cup \mathcal{B} \cup \mathcal{R}$.

Altruistic players ($\mathcal{A}$): The set of players which act altruisticly. They always follow the rules of the protocol and hence do not deviate even if this would offer higher profits. The accumulated hashrate of these players is denoted by $p_{\mathcal{A}}$.

Byzantine players ($\mathcal{B}$): The set of players or a single player, which acts Byzantine and thereby in the most destructive way possible e.g., by executing an attack. The accumulated hashrate of these players is denoted by $p_{\mathcal{B}}$. For most of our attack analysis in this paper we set $p_{\mathcal{B}} = 0$.

Rational players ($\mathcal{R}$): The set of players which act rational under economic considerations. They follow the rules of the initial protocol as long as there is no other strategy which yields higher profits. The accumulated hashrate of these players is denoted by $p_{\mathcal{R}} = 1 - (p_{\mathcal{A}} + p_{\mathcal{B}})$. The number of players that are rational is denoted by $|\mathcal{R}|$, where each player controls some fraction of the total hashrate s.t. $p_{\mathcal{R}} = \sum_{i=1}^{|\mathcal{R}|} p_{\mathcal{R}_i}$ holds. An example for a rational actor is Rachel (R). Rational players are the only type of player which can be further divided into different *sides* during an attack

[1] https://github.com/kernoelpanic/howmuchisthefork_artefacts

[2] In this work, the word actor and player are used interchangeably.

(see 2.3). Rationality always depends on a certain optimization criteria in question, i.e., the parameter which should be optimized by acting rational. In this paper the rationally criteria is *short term* maximization of funds, under the assumption that the exchange rate remains constant, analogous to most analysis approaches [8]. So the question rational players face is: "What is the next best block?", i.e., the most profitable chain to extend.

2.3 Player Sides

During an attack a rational player can also be categorized depending on the side she is taking in the respective attack. This is only relevant for rational players, as they might change their strategy if this promises higher profits, while altruistic players for example never change their strategy. At any point, it holds that $\mathcal{R} = \mathcal{E} \cup \mathcal{V} \cup \mathcal{I}$.

Extractor(s)/ Exploiter(s) ($\mathcal{E}$): The set of players which does not follow the prescribed rules of the protocol to gain a financial advantage. They seek to exploit an additional value extraction opportunity, such as a front running, arbitrage, a censorship, double-spend, or any other attack vector to increase their MEV beyond what they would get by block rewards and fees. Therefore, they might be willing to share some of their reward in order to bribe other miners, to aid in their attack. This set of players has hashrate $p_{\mathcal{E}}$. They join (or are assumed to join) an attack to gain a profit.

Victim(s) ($\mathcal{V}$): The set of players which would lose funds if a described attack is successful, e.g., a merchant who is the victim of a double-spend. This set of players has hashrate $p_{\mathcal{V}}$. Vicitims certainly work against an ongoing attack and even might launch a counter-attack if this is economically rational.

Indifferent ($\mathcal{I}$): The set of players which follows the prescribed rules of the protocol, although an attack is ongoing. This party does neither profit nor lose when the attack is successful. The difference between these actors and altruistic miners is that these indifferent rational miners would change their strategy as soon as they are positively, or negatively, affected by an attack. Therefore, as long as the situation for them does not change, they can also be modelled as being part of $p_{\mathcal{A}}$, which was implicitly done in previous modelling approaches. In this work, we explicitly define the hashrate of these actors by $p_{\mathcal{I}}$, s.t., $p_{\mathcal{R}} = p_{\mathcal{E}} + p_{\mathcal{V}} + p_{\mathcal{I}}$.

To illustrate that the separation of economically rational actors into the mentioned sides is dependent on the viewpoint, we now provide an example.

2.4 Example: (Unindented) Fork

When a miner Alice (A) does not receive the latest block b_{n_B} from miner Bob (B) timely, she keeps on trying to extend an old block b_{n-1}. If now Alice finds a block b'_{n_A} and publishes it, this results in a unindented fork where Bob would build up on his block b_{n_B} and Alice would continue to mine on her block b'_{n_A}, even after receiving Bob's block for the same height. Although, such situations can be expected to happen during normal protocol operation, at that point Bob and Alice have no way to tell if this was a coincidence or happened because of malicious activity. Only if this pattern persists for a prolonged period of time, it would be possible to detect a skew in the distribution of blocks and the occurrence of forks, which would indicate malicious mining activity in retrospect. However, for a singular event this distinction between attack and normal operation is difficult.

Therefore, at that point Alice as well as Bob could also be viewed as adversarial from the perspective of the other party. From the perspective of Bob, Alice would be the aggressor, i.e., $A \in \mathcal{E}$, and he is the victim $B \in \mathcal{V}$, as he would lose his rewards from block b_{n_B} if b'_{n_A} becomes part of the longest chain. From the perspective of Alice, Bob would be the aggressor, i.e., $B \in \mathcal{E}$, and she is the victim $A \in \mathcal{V}$, as she would lose her funds from block b'_{n_A} if b_{n_B} becomes part of the longest chain. Under the assumption that the transactions in both blocks are equal, all other rational miners are indifferent from both viewpoints as they do not have any preference regarding one of the two blocks, i.e., $\big(\mathcal{R} \cap (A \cup B)\big) \in \mathcal{I}$.

If now a new block $b_{(n+1)_C}$ is found and published by Carol, which builds up on the block of Alice (b'_{n_A}) the situation changes again, depending on which type of Actor Bob is. If Bob is altruistic ($B \in \mathcal{A}$) he switches to the longer chain and the fork is over. If Bob is Byzantine then his actions can be modelled as the worst response without considering his individual losses or gains, i.e., in this case continue mining on top of b_{n_B}. If Bob is economically rational his choice which chain to adopt will depend on his expected profits and thus also on his hashrate and the resulting chance of winning the race. Also the set of indifferent miners changes: Carol now clearly has an interest in keeping the longest chain containing her block. Moreover, all other miners have a higher chance to gain rewards on the longest chain than on a shorter chain, therefor their expected reward will be higher on the longest chain as well.

3 PROBABILITY AND PROFITABILITY CALCULATION

In this section we focus on the question which chain to extend in case of a fork, i.e., which next block provides the most expected profit. We address this question from the perspective of an individual rational miner m with hahsrate p_m. Therefore, we build up on the model from Liao and Katz [8], which we first translate into the notations used in this work and then extend it. Thereby, we consider already contributed blocks, finite attack durations and individual pain thresholds of players, as well as economically rational victims.

3.1 Basic Model for Calculating Expected Profit

An inherent requirement for calculating the expected profit of the next block in any scenario where there is more than one chain that can be extended, is that the total hashrate which will work towards each individual chain has to be guessed, as also done in [8]. Considering the setting, where all players are economically rational ($p_{\mathcal{R}} = 1$), the miner m has to estimate $p_{\mathcal{E}}$, $p_{\mathcal{V}}$ and $p_{\mathcal{I}}$, in order to calculate the expected payoffs for the next blocks(s). Hereby, $\mathcal{E}$ is assumed to work on the attack chain, and $\mathcal{V}$ is assumed to work on the main chain, as these chains provide more individual profit for them. The players in $\mathcal{I}$ are indifferent because they will neither lose nor profit from the attack and thus always work on the currently longest chain. A possible explanation for such a situation (considering imperfect information available to the parties) might be, that indifferent miners have not yet recognized that a profitable attack is

going on. Another explanation would be, that their potential gains from the attack exactly cancel out their expected losses on the main chain.

The probability of an attack chain, or fork, to ever catch-up given an unlimited number of tries/blocks ($N = \infty$), if it is z blocks behind, was defined in [10, 13] and is given by Equation 1.

$$\mathbb{P}(\text{succ. attack}) \coloneqq \begin{cases} \left(\frac{\text{hashrate on fork chain}}{\text{hashrate on main chain}}\right)^{z+1} = \left(\frac{\text{p}}{\text{1-p}}\right)^{z+1} & \text{if } z \geq 0 \text{ and } p \leq 0.5 \\ 1 & \text{if } z < 0 \text{ or } p > 0.5 \end{cases} \tag{1}$$

In case of a fork/attack the miner m has two options: Either m *joins* the attack and extends the fork, or m *abstains* from the attack and thus extends the main chain. Depending on this decision, the resulting success probability of the attack changes as p_m is added to the hashrate working on the respective chain and thus against the other. The resulting success probabilities of the fork in both scenarios are as follows in our verbose notation.

$$\mathbb{P}(\text{success join}) \coloneqq \begin{cases} \left(\frac{p_{\mathcal{B}}+p_{\mathcal{E}}+p_m}{p_{\mathcal{A}}+p_{\mathcal{V}}+p_{\mathcal{I}}}\right)^{z+1} & \text{if } z \geq 0 \text{ and } p_{\mathcal{B}} + p_{\mathcal{E}} + p_m \leq 0.5 \\ 1 & \text{if } z < 0 \text{ or } p_{\mathcal{B}} + p_{\mathcal{E}} + p_m > 0.5 \end{cases} \tag{2}$$

$$\mathbb{P}(\text{success abstain}) \coloneqq \begin{cases} \left(\frac{p_{\mathcal{B}}+p_{\mathcal{E}}}{p_{\mathcal{A}}+p_{\mathcal{V}}+p_{\mathcal{I}}+p_m}\right)^{z+1} & \text{if } z \geq 0 \text{ and } p_{\mathcal{B}} + p_{\mathcal{E}} \leq 0.5 \\ 1 & \text{if } z < 0 \text{ or } p_{\mathcal{B}} + p_{\mathcal{E}} > 0.5 \end{cases} \tag{3}$$

Since we aim to compare the profitability of mining on different chains of the same cryptocurrency, the costs for mining are the same regardless on which chain the hashrate is p_m is mining on. Therefore, as in [8] we can ignore the operational costs of mining in our calculation as it is the same on all chains. Moreover, we do not include the costs of acquiring the mining hardware in our calculation, as we assume that this has already been done and was based on an economically rational decision that mining in general can be executed profitably.

To now compare the expected profits of extending two different chains, we normalize the reward to 1 ($r_{block} = r_{blockreward} + r_{fee} = 1$) and assume that the exchange rate and thus the value gain from a block remains constant. Then the expected reward of m for one new block on the main chain if a fork/attack fails is given by Equation 4.

$$\rho_{main} \coloneqq \frac{\left(1 - \mathbb{P}(\text{success abstain})\right) \cdot p_m}{p_{\mathcal{A}} + p_{\mathcal{V}} + p_{\mathcal{I}} + p_m} \tag{4}$$

Conversely, the expected reward of m for one new block on the attack chain if a fork/attack succeeds is given by Equation 5.

$$\rho_{fork} \coloneqq \frac{\mathbb{P}(\text{success join}) \cdot p_m}{p_{\mathcal{B}} + p_{\mathcal{E}} + p_m} \cdot (\epsilon + 1) \tag{5}$$

Equation 5 already contains a potential bribe ϵ, which is paid out on per block basis in the competing attack chain. Thereby, also the expected profit for miners participating in bribing [1] or algorithmic incentive manipulation [7] attacks can be modelled. If an unintentional fork without any bribes should be modeled, ϵ can be set to zero.

To derive the required bribe ϵ, as done in [8], the expected reward on the fork/attack chain has to be larger than the expected reward on the main chain. This means Equation 5 has to be larger than 4, i.e., $\rho_{fork} > \rho_{main}$. Rearranging this inequality yields.

$$\epsilon > \frac{\left(1 - \left(\frac{p_{\mathcal{B}}+p_{\mathcal{E}}}{p_{\mathcal{A}}+p_{\mathcal{V}}+p_{\mathcal{I}}+p_m}\right)^{z+1}\right)}{p_{\mathcal{A}} + p_{\mathcal{V}} + p_{\mathcal{I}} + p_m} \cdot \frac{p_{\mathcal{B}} + p_{\mathcal{E}} + p_m}{\left(\frac{p_{\mathcal{B}}+p_{\mathcal{E}}+p_m}{p_{\mathcal{A}}+p_{\mathcal{V}}+p_{\mathcal{I}}}\right)^{z+1}} - 1 \tag{6}$$

A briber can use this formula to estimate the required amount of the bribe to convince other economically rational miners to join the attack.

When analysing the case of an infinite attack duration (i.e., Equation 1) an interesting observation regarding an artefact of this approach can be made. If the hashrate of the attacker exceeds $0.381966\ldots$, then in forks of length one ($z = 1$) the expected profitability of the next block while staying on the fork is higher than it would be on the main chain i.e., in the case where the equivalent hashrate participates in honest mining. This particular hashrate value already occurred in some publications [9, 15] in the context of cryptocurrencies, but was never discussed in detail. Appendix A outlines why this bound in hashrate of exactly $1/\phi^2$ exists and where it comes from.

We now will build upon this model form Liao and Katz [8] and enhance it by considering the effects of *already contributed blocks* and then consider finite attack durations and economically rational victims.

3.2 Considering Already Contributed Blocks

To the best of our knowledge all previous attempts of calculating the attack success probability implicitly assume that all non-attacking miners immediately switch to the attack chain as soon as it gets ahead of the honest chain. An assumption which is unlikely to hold in practise, as it ignores blocks which have already been appended by those miners to a competing chain. Therefore, if miners should be modeled as economically rational, already mined blocks have to be taken into account. We therefore, enhance the proposed model from [8] to account for rational miners and already contributed blocks. As a first step, we extend the model from [8] and also consider blocks already contributed by m to the respective chain. For example, if m has already contributed two blocks to the main chain, which would not be rewarded if the attack succeeds, this is denoted by $\eta_{main} = 2$. The number of blocks m has already contributed to the attack chain (if any) is denoted by η_{attack}. It is possible that there are cases where both values ($\eta_{main}, \eta_{attack}$) are greater than 0, so we have to account for that in our calculation. This might happen when m has first worked on the main chain and then switched to an attack. Then, while the attack is still ongoing, m evaluates if it makes sense from her perspective to pursue the progressed attack. The expected reward in number of block rewards (normalized) for one new block in the main chain if the fork/attack fails, is thus given by Equation 7. For space reasons we abbreviate

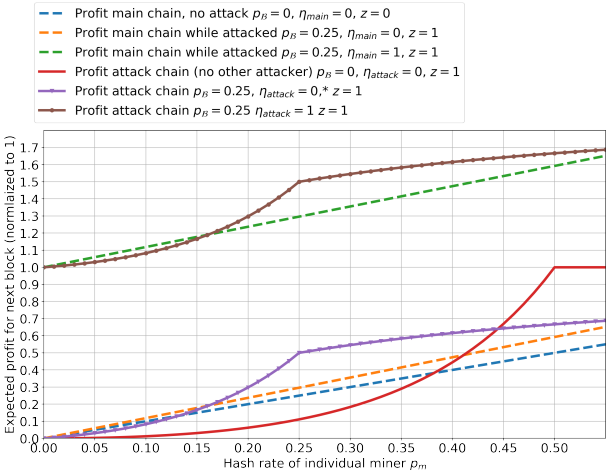


Figure 1: The expected reward (ρ) for the next block is given on the y-axis, while the hashrate p_m of the miner under consideration is given on the x-axis. The figures shows a comparison of the profitability of different scenarios for mining on the main chain, versus mining on the attack chain.

$\mathbb{P}$(success abstain) by $\mathbb{P}$(abstain).

$$\rho_{main\ bl.} := \frac{\big(1 - \mathbb{P}(\text{abstain})\big) \cdot p_m}{p_{\mathcal{A}} + p_{\mathcal{V}} + p_{\mathcal{I}} + p_m} + \big(\eta_{main} \cdot (1 - \mathbb{P}(\text{abstain}))\big) + \big(\mathbb{P}(\text{abstain}) \cdot \eta_{fork}\big) \tag{7}$$

Conversely, the reward in number of block rewards (normlized to 1) for one new block on the attack chain if the attack succeeds is given by Equation 8. This assumes that the bribe ϵ is paid for every contributed block on the attack chain, but other variants are also possible. To evaluate an unintentional fork without bribes, ϵ can be set to zero. For space reasons we again abbreviate $\mathbb{P}$(success join) by $\mathbb{P}$(join).

$$\rho_{fork\ bl.} := \left(\frac{\mathbb{P}(\text{join}) \cdot p_m}{p_{\mathcal{B}} + p_{\mathcal{E}} + p_m} \cdot (\epsilon + 1)\right) + \big(\eta_{fork} \cdot (\epsilon + 1) \cdot \mathbb{P}(\text{join})\big) + \big(\eta_{main} \cdot (1 - \mathbb{P}(\text{join}))\big) \tag{8}$$

Given these Equations, a rational miner now can compare the achievable rewards on both chains and pick the most profitable one. In this way, also the case in which a miner has contributed blocks to two or more chains can be captured and compared. Figure 1 shows a comparison for different hashrates and already contributed blocks. It can be observed that, as soon as a miner has already contributed a block to a chain, his expected profit increases significantly on that chain. This makes it unlikely, that rational players in such a situation will readily switch to the attack chain as soon as it takes the lead. Moreover, it can be observed that, if there is another attacker ($p_{\mathcal{B}} > 0$), joining an attack becomes more profitable than staying on the main chain sooner, i.e., with lower hashrate p_m. Although, staying on the main chain is slightly more profitable if somebody else with low chances of success is working on an attack chain, as in this case less hashrate is concentrated on the main chain. The same holds true, in the other direction, but since the overall hashrate on the attack chain is lower, the potential gains are higher as they have to be divided amongst fewer players.

As the probability calculation in this case implicitly still assumes that victims will switch immediately as soon as their chain falls behind and that attackers will stick to their chain infinitely long, we now augment the model to account for rational victims and finite attacks.

3.3 Considering Economically Rational Victims and Finite Attacks

We now want to model rational miners, who do not immediately switch to the attack chain once it has taken the lead, e.g., because they have already contributed blocks to the main chain which they would lose in this case. The miners who keep on mining on the main chain can be viewed as *victims* ($\mathcal{V}$) with hashrate $p_{\mathcal{V}}$, whereas miners who switch to the attack chain as soon as it takes the lead can either be viewed as *altruistic* ($\mathcal{A}$) with hashrate $p_{\mathcal{A}}$, or as *indifferent* ($\mathcal{I}$) with hashrate $p_{\mathcal{I}}$. Miners who start working on a fork/attack chain can be viewed as *Byzantine* ($\mathcal{B}$) with hashrate $p_{\mathcal{B}}$, or if they are economically rational as *extractor* ($\mathcal{E}$) with hashrate $p_{\mathcal{E}}$. Those last two sets of miners would profit if the attack chain wins.

We model an attack, which is not immediately over as soon as the attack chain takes the lead, using a finite Markov chain. Since we are only interested in modelling practical and thus finite attacks, it is sufficient to use a finite Markov chain for the practically plausible range in which both chains will grow relative to each other.

Thereby, the set of victims ($\mathcal{V}$) will work against the attack, even if their (previous main) chain is behind already. They will only give up if a configurable lead ($\overrightarrow{k}$), in terms of blocks, is reached. In opposition to that, the attacker and bribable rational miners work on the attack chain ($\mathcal{B} \cup \mathcal{E}$) of the fork. The third fraction of miners consisting of altruistic, as well as indifferent rational miners, work either for, or against the attack, depending on which chain is currently the longest ($\mathcal{A} \cup \mathcal{I}$). The difference between the last two groups is, that altruistic miners will never support a shorter chain, while the decision of indifferent miners can be subject to change depending on their expected profit[3].

As we are only interested in practical attacks, they have a certain finite maximum duration. This is the number of blocks (N) the fork is assumed to last, i.e., the period it can be financed by the involved parties. In our model this is the number of steps that are taken in the Markov chain (see Figure 2). Moreover, each of the two opposing parties ($\mathcal{V}$ against $\mathcal{B} \cup \mathcal{E}$) has a certain pain threshold in terms of blocks that their chain can fall behind until they deem it unlikely that they will ever catch up again. For $\mathcal{V}$ this number in terms of blocks is defined by $\overrightarrow{k}$, whereas for $\mathcal{B} \cup \mathcal{E}$ this value is $\overleftarrow{k}$. The winning condition, from the perspective of the attackers, for this kind of race can be defined in two ways:

[3]For the analysis presented here, these two groups ($\mathcal{A}$ and $\mathcal{I}$) are treated similarly. If this should not be the case, the Markov chain can be augmented. For example the hashrate $p_{\mathcal{I}}$ can be modelled to work for, or against the attack, if a chain is in the lead for a sufficiently large number of blocks.

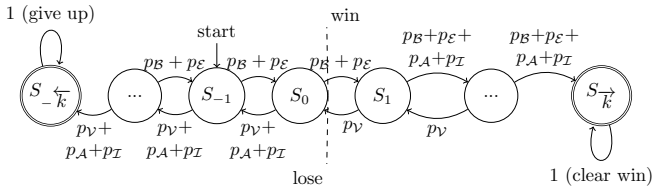


Figure 2: Markov chain for modelling finite attacks and persistent victims ($p_{\mathcal{V}}$).

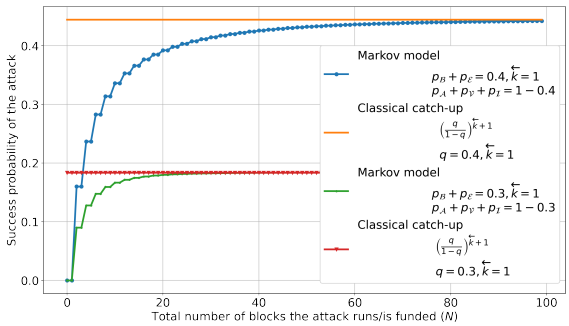


Figure 3: Comparison of the infinite attack success probability to our finite Markov chain model for increasing attack duration $N = \overrightarrow{k}$ (x-axis).

- **Win:** The sum of all probabilities of the states on the right hand side, where the attack chain is the longest chain after a total of N blocks i.e., steps taken in the Markov chain.
- **Clear win:** The success probability of the *clear win* state at which the attack chain has an advantage of $\overrightarrow{k}$ s.t., the victims will give up.

Every other state is a lose state for the attackers. The start state is defined by the initial disadvantage for the attackers z. Usually for block exclusion (also known as censorship) attacks, and missed MEV opportunities, $z = 1$, thus S_{-1} is the start state.

To validate our approach, we now want to use our Markov chain model to approximate the success probability of a classical infinite attack[4], in which the defenders are not rational and give up as soon as they are behind. Therefore, we have to configure our Markov chain model as follows: Set $\overrightarrow{k} = 1$ and increase N as well as $\overleftarrow{k}$ to approach the success probability of the infinitely running attack. Figure 3 shows that our Markov model approaches the maximum success probability of an infinitely running attack as N grows.

We now use the probability of all success states after N iterations of our Markov chain, to replace the probability calculation in Equation 7 and 8 with the success probability of the attack computed via the Markov chain, instead of using the infinite success probability calculation. Thereby, we can also compute the profitability using the same formula, but now with a different probability calculation. Before we compare some example scenarios using this new model, we extend it to also account for attacks in which a briber compensates participating bribees for contributed blocks, even if the attack as a whole is not successful.

3.4 Effort-Related Compensation for Contributed Blocks

Previous works indicate that paying bribes even if the attack as a whole is not successful is a viable strategy. In paper [17] the authors describe effective transaction censorship attacks which operate by paying for complacent blocks. In paper [6] a double-spend attack is described in which an attacker compensates already contributed blocks to the attack branch, even if the attack as a whole is not successful. To evaluate the costs of the overall attack the authors in paper [6] simulated different scenarios and thereby focused on the perspective of the briber.

In this paper we want to illustrate the economic feasibility in such a scenario from the perspective of an individual bribee, i.e., an economically rational miner m. Therefore, we augment the expected profitability calculation for the next bock on either chain in a way that ensures that already contributed blocks are compensated even if the attack is not successful.

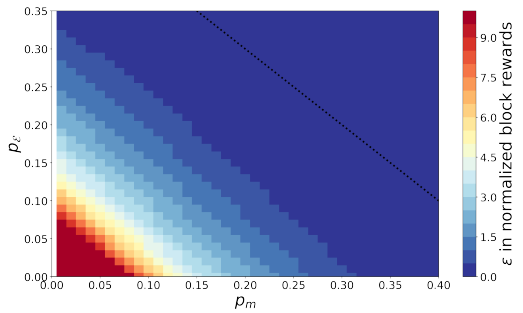
To calculate the expected profit for the next block on the main chain in this case, Equation 7 is extended to also include compensations for blocks contributed to the fork. At first this might seem counter intuitive, but this captures the case where a miner m has already contributed blocks to a fork and considers switching back to the main chain. In this case m would unconditionally receive the compensation for already contributed attack blocks even if the main chain wins, plus a bribe for the attack chain blocks if the fork happens to be successful and the main chain loses.

$$\rho_{main\ comp.} :=$$

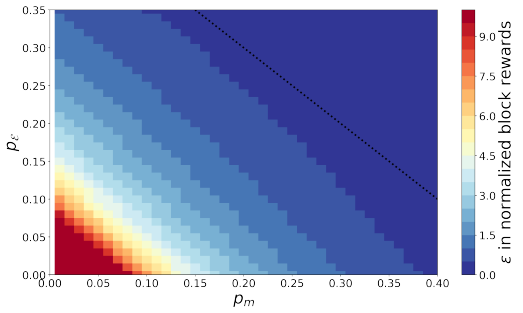
$$\frac{\big(1 - \mathbb{P}(\text{abstain})\big) \cdot p_m}{p_{\mathcal{A}} + p_{\mathcal{V}} + p_{\mathcal{I}} + p_m} + \big(\eta_{main} \cdot (1 - \mathbb{P}(\text{abstain}))\big) \tag{9}$$

$$+ \eta_{fork} + \Big(\eta_{fork} \cdot \epsilon \cdot \mathbb{P}(\text{abstain})\Big) \tag{10}$$

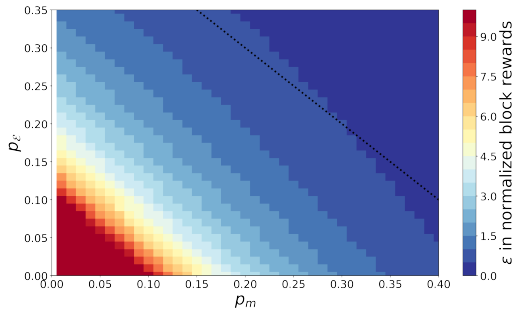
[4]Where q is the attacker hashrate s.t. $\left(\frac{q}{1-q}\right)^{z+1}$, as defined in [10, 13]



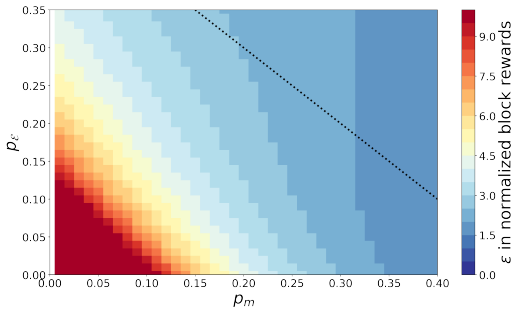
(a) ***Model:*** **Min.** ϵ **for** $\rho_{fork} > \rho_{main}$**, with classic infinite probability calculation (Equation 6).** ***Conf.:*** $z = 1, N = \infty$



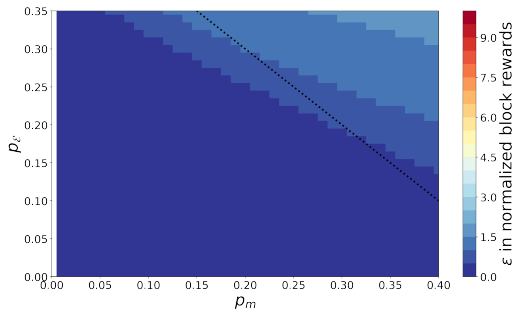
(b) ***Model:*** **Min.** ϵ **for** $\rho_{fork} > \rho_{main}$**, with probabilities from Markov chain** ***Conf.:*** $p_\mathcal{V} = 0, z = 1, \overrightarrow{k} = 1, \overleftarrow{k} = 6, N = 6$



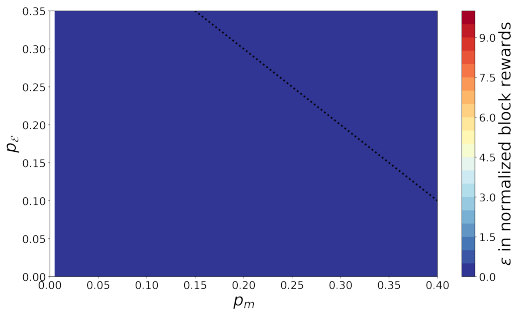
(c) ***Model:*** **Min.** ϵ **for** $\rho_{fork} > \rho_{main}$**, with probabilities from Markov chain** ***Conf.:*** $p_\mathcal{V} = 0.25, z = 1, \overrightarrow{k} = 3, \overleftarrow{k} = 6, N = 6$



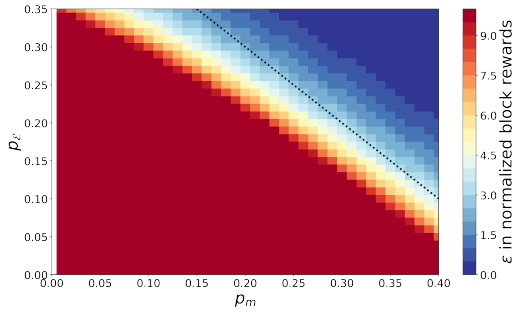
(d) ***Model:*** **Min.** ϵ **for** $\rho_{\textit{fork bl.}} > \rho_{\textit{main bl.}}$**, with probabilities from Markov chain** ***Conf.:*** $p_\mathcal{V} = 0.25, z = 1, \overrightarrow{k} = 3, \overleftarrow{k} = 6, N = 6, \eta_{main} = 1$



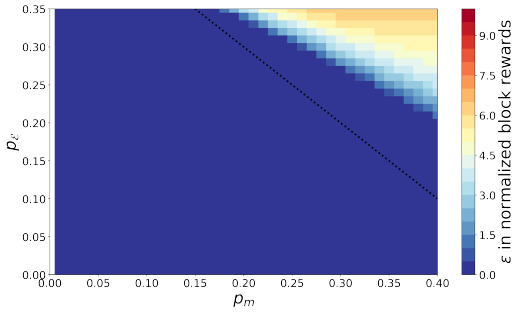
(e) ***Model:*** **Min.** ϵ **for** $\rho_{\textit{fork comp.}} > \rho_{\textit{main comp.}}$**, with probabilities from Markov chain** ***Conf.:*** $p_\mathcal{V} = 0.25, z = 1, \overrightarrow{k} = 3, \overleftarrow{k} = 6, N = 6, \eta_{main} = 1$



(f) ***Model:*** **Min.** ϵ **for** $\rho_{\textit{fork comp.}} > \rho_{\textit{main comp.}}$**, with probabilities from Markov chain** ***Conf.:*** $p_\mathcal{V} = 0.25, z = 1, \overrightarrow{k} = 3, \overleftarrow{k} = 6, N = 6$



(g) ***Model:*** **Min.** ϵ **for** $\rho_{\textit{fork bl.}} > \rho_{\textit{main bl.}}$**, with probabilities from Markov chain** ***Conf.:*** $p_\mathcal{V} = 0.25, z = 6, \overrightarrow{k} = 3, \overleftarrow{k} = 9, N = 10, \eta_{attack} = 3$



(h) ***Model:*** **Min.** ϵ **for** $\rho_{\textit{fork comp.}} > \rho_{\textit{main comp.}}$**, with probabilities from Markov chain** ***Conf.:*** $p_\mathcal{V} = 0.25, z = 6, \overrightarrow{k} = 3, \overleftarrow{k} = 9, N = 10, \eta_{main} = 3$

Figure 4: Minimum bribe value per block ϵ**, given in normalized block rewards, for different models and configurations. Thereby,** ϵ **reaches from** 0 **(blue) to** 10 **or higher (red). The y-axis shows** $p_\mathcal{E}$**, while the x-axis shows** p_m**. The dashed line marks** $p_\mathcal{E} + p_m = 0.5$**.**

To calculate the expected profit for the next block on the attack chain in this case, Equation 8 is extended to also include compensations for blocks contributed to the fork. In this case, there additionally exists the probability to also get a normalized block reward (excluding bribe ϵ) for the next block if the attack is not successful. Additionally, all already contributed blocks are compensated even if the attack fails (without additional ϵ per block). In case the attack is successful, an additional bribe ϵ is paid per block.

$$\rho_{\textit{fork comp.}} := \frac{\mathbb{P}(\text{join}) \cdot p_m}{p_{\mathcal{B}} + p_{\mathcal{E}} + p_m} \cdot (1+\epsilon) + \frac{(1-\mathbb{P}(\text{join})) \cdot p_m}{p_{\mathcal{B}} + p_{\mathcal{E}} + p_m} + \eta_{fork} + \big(\eta_{fork} \cdot \epsilon \cdot \mathbb{P}(\text{join})\big) + \big(\eta_{main} \cdot (1-\mathbb{P}(\text{join}))\big) \tag{11}$$

3.5 Comparison

We now want to compare different attack scenarios regarding the required minimum bribe ϵ for an attack. To calculate the min. bribe s.t. switching to the attack chain becomes more profitable for m compared to mining on the main chain, we again set $\rho_{fork^*} > \rho_{main^*}$ and solve for ϵ.

Figure 4 shows color map plots of the minimum bribe ϵ required such that contributing the next block to the attack chain is more profitable for a miner with hashrate p_m (x-axis) than extending the main chain. The y-axis shows the hashrate ($p_{\mathcal{E}}$) of other economically rational attackers. The dashed black line marks $p_m + p_{\mathcal{E}} > 0.5$, at which point the attackers would be able to overtake the system when attacking infinitely long. The required minimum bribe ϵ is denominated in normalized block rewards in a range from 0 to 10, where 0 is blue, and a bribe of 10 (or more) times the normalized block reward is red.

Figure 4a to Figure 4f show various models and configurations for the case $z = 1$. This resembles the case of a one-block fork as it might happen when certain transactions ought to be censored, or a missed MEV opportunity should be exploited although a block has already been mined. Figure 4a depicts the case where no compensations for already contributed blocks to the attack chain are paid (Equations 7 and 8 are used in the inequality). Furthermore, in Figure 4a the probability is calculated using the classic infinite model from Equation 1. In comparison, Figure 4b uses our Markov chain with an attack duration of $N = 6$ and $\overrightarrow{k} = 1$, which resembles the case that the attack is over as soon as the attack chain takes the lead. In both figures no compensations for already contributed blocks are paid. It can be observed that in this comparable scenario, the required bribes are slightly higher in the Markov chain model, as in this case the attack does not run infinitely long (although the infinite case can be approximated by increasing N).

Figure 4c shows the same situation in our Markov chain model, but now the victim has hashrate $p_{\mathcal{V}} = 0.25$. It can be seen that in this case the required bribes are of course higher as now the victim is working against the attack even after the attack chain has become the longest chain. The bribe further increases in Figure 4d as now m has contributed already one block to the main chain.

Figure 4e suddenly does require hardly any bribes as now the Equations 9 and 11 for effort-related compensation are used. In this case, even though m has already contributed one block to the main chain ($\eta_{main} = 1$), no extra direct bribe per block (despite of course the compensations) is required. This effect is further amplified in Figure 4f, where effort-related compensation is used as well, but no blocks have been contributed by m to any chain in this case. Here we see that no extra bribes per block are require such that extending the attack chain is more profitable for m than extending the main chain. Therefore, it would make sense to combine the exploitation of a missed MEV opportunity, with a bribing attack that compensates already mined blocks, as hardly any additional bribe per block is needed to incentivize economically rational miners to participate.

Figure 4g shows a classical double-spend scenario where the attack chain is $z = 6$ blocks behind. In this case the required bribe is very high although m has already contributed $\eta_{attack} = 3$ blocks to the fork. This is because in this case no effort-related compensation is paid for already contributed blocks. As soon as effort-related compensation is paid for contributed blocks the required bribe again becomes 0 even for longer range forks like that. Figure 4h shows such a case even in a scenario where m has already contributed blocks to the main chain ($\eta_{main} = 3$). Even in this case no extra bribe is required to incentivize m to mine on the attack chain if effort-related compensation is used. Observe that in Figure 4h, bribes are required as soon as the hashrate of $p_m + p_{\mathcal{E}}$ is high enough. The reason for this is that the probability to find a block on the main chain gets better compared to the attack chain. Moreover, the stakes are higher on the main chain as 3 blocks have already been contributed which would be lost in case the main chain loses.

4 LIMITATIONS AND FUTURE WORK

An interesting direction for future work is to investigate the long term consequences of successful attacks. For example, a drop in the exchange rate which reduces the profitability of the attack. Such considerations have to to be taken into account by economically rational miners as well. If the exchange rate is not static, then also the amount of funds players are currently holding becomes relevant.

5 CONCLUSION

We have presented an improved model for calculating the probability and profitability of chain forks, i.e., attacks, form the perspective an individual miner m. Our model considers, configurable finite attack durations, already contributed blocks to the respective chains, as well as victims which do not immediately switch to the attack chain as soon as it takes the lead. We have applied the model to more accurately investigate forks of length 1, which are the relevant case for exploiting missed MEV opportunities. Furthermore we have described approaches which allow modeling bribing attacks which compensate miners for already contributed blocks, even if the overall attack is unsuccessful. We have shown that bribing attacks, which can plausibly ensure that blocks contributed by bribees are compensated, require hardly any additional bribe per block to incentivize economically rational miners to participate in the attack. This further emphasizes the risk such bribing attacks pose to the overall stability of the underlying system, especially for short range forks.

REFERENCES

[1] Joseph Bonneau. 2016. Why buy when you can rent? Bribery attacks on Bitcoin consensus. In *BITCOIN '16: Proceedings of the 3rd Workshop on Bitcoin and Blockchain Research*. http://fc16.ifca.ai/bitcoin/papers/Bon16b.pdf

[2] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 910–927. https://par.nsf.gov/servlets/purl/10159474

[3] Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. 2019. SoK: Transparent Dishonesty: front-running attacks on Blockchain. In *arXiv preprint arXiv:1902.05164*. https://arxiv.org/pdf/1902.05164.pdf

[4] Ittay Eyal and Emin Gün Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security*. Springer, 436–454. http://arxiv.org/pdf/1311.0243

[5] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdo rf, and Srdjan Capkun. 2016. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC*. ACM, 3–16. https://pdfs.semanticscholar.org/8b32/309a7730de87a02e38c7262307245dca5274.pdf

[6] Aljosha Judmayer, Nicholas Stifter, Alexei Zamyatin, Itay Tsabary, Ittay Eyal, Peter Gaži, Sarah Meiklejohn, and Edgar Weippl. 2019. Pay-To-Win: Cheap, Crowdfundable, Cross-chain Algorithmic Incentive Manipulation Attacks on PoW Cryptocurrencies. Cryptology ePrint Archive, Report 2019/775. https://eprint.iacr.org/2019/775

[7] Aljosha Judmayer, Nicholas Stifter, Alexei Zamyatin, Itay Tsabary, Ittay Eyal, Peter Gaži, Sarah Meiklejohn, and Edgar Weippl. 2020. SoK: Algorithmic Incentive Manipulation Attacks on Permissionless PoW Cryptocurrencies. Cryptology ePrint Archive, Report 2019/775. https://eprint.iacr.org/2019/775

[8] Kevin Liao and Jonathan Katz. 2017. Incentivizing blockchain forks via whale transactions. In *International Conference on Financial Cryptography and Data Security*. Springer, 264–279. http://www.cs.umd.edu/jkatz/papers/whale-txs.pdf

[9] Patrick McCorry, Alexander Hicks, and Sarah Meiklejohn. 2018. Smart Contracts for Bribing Miners. In *5th Workshop on Bitcoin and Blockchain Research, Financial Cryptography and Data Security 18 (FC). Springer*. http://fc18.ifca.ai/bitcoin/papers/bitcoin18-final14.pdf

[10] Satoshi Nakamoto. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

[11] Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi. 2016. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *1st IEEE European Symposium on Security and Privacy, 2016*. IEEE. http://eprint.iacr.org/2015/796.pdf

[12] Kaihua Qin, Liyi Zhou, and Arthur Gervais. 2021. Quantifying Blockchain Extractable Value: How dark is the forest? *arXiv preprint arXiv:2101.05511* (2021). https://arxiv.org/pdf/2101.05511

[13] M. Rosenfeld. 2014. *Analysis of Hashrate-Based Double Spending*. Vol. abs/1402.2009. https://arxiv.org/pdf/1402.2009.pdf Publication Title: CoRR.

[14] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. 2016. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*. Springer, 515–532. https://fc16.ifca.ai/preproceedings/30_Sapirshtein.pdf

[15] Jason Teutsch, Sanjay Jain, and Prateek Saxena. 2016. When cryptocurrencies mine their own business. In *Financial Cryptography and Data Security (FC 2016)*. https://www.comp.nus.edu.sg/prateeks/papers/38Attack.pdf

[16] Christof Ferreira Torres, Antonio Ken Iannillo, Arthur Gervais, and Radu State. 2021. *The Eye of Horus: Spotting and Analyzing Attacks on Ethereum Smart Contracts*. https://arxiv.org/pdf/2101.06204 _eprint: 2101.06204.

[17] Fredrik Winzer, Benjamin Herd, and Sebastian Faust. 2019. *Temporary Censorship Attacks in the Presence of Rational Miners*. https://eprint.iacr.org/2019/748 Published: Cryptology ePrint Archive, Report 2019/748.

[18] Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. 2021. *On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols*. https://arxiv.org/pdf/2103.02228 _eprint: 2103.02228.

[19] Liyi Zhou, Kaihua Qin, and Arthur Gervais. 2021. A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. *arXiv:2106.07371 [cs]* (June 2021). http://arxiv.org/abs/2106.07371 arXiv: 2106.07371.

[20] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V. Le, and Arthur Gervais. 2020. High-Frequency Trading on Decentralized On-Chain Exchanges. *arXiv preprint arXiv:2009.14021* (2020). https://arxiv.org/pdf/2009.14021.pdf

ACKNOWLEDGMENTS

This material is based upon work partially supported by (1) the Christian-Doppler-Laboratory for Security and Quality Improvement in the Production System Lifecycle; The financial support by the Austrian Federal Ministry for Digital and Economic Affairs, the Nation Foundation for Research, Technology and Development and University of Vienna, Faculty of Computer Science, Security & Privacy Group is gratefully acknowledged; (2) SBA Research; the competence center SBA Research (SBA-K1) funded within the framework of COMET Competence Centers for Excellent Technologies by BMVIT, BMDW, and the federal state of Vienna, managed by the FFG; (3) the FFG Industrial PhD projects 878835 and 878736. (4) the FFG ICT of the Future project 874019 dIdentity & dApps. (5) the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078 (FeatureCloud). We would also like to thank our anonymous reviewers for their valuable feedback and suggestions.

A THE $1/\phi^2$ BOUND

If no fork, or attack, occurs the hashrate p_m of a miner and thus the probability to find a new block, is directly correlated with the expected profit for a new block (if normalized to one). Let's assume that $p_{\mathcal{E}} = p_{\mathcal{V}} = p_{\mathcal{I}} = 0$, and there is only one rational miner p_m. In case of an unintentional, or malicious fork, where p_m is one block behind ($z = 1$) and tries to catch-up infinitely long as defined in equation 1 from [10, 13], his profitability on the fork increases beyond his expected profit for staying on the main chain, when the miner has a hahsrate greater than $\approx 38.2\%$ of the total hashrate. This value already occurred in the following publications in the context of cryptocurrencies [9, 15], but was not discussed in great detail there, nor related to $1/\phi^2$. We now show how this value is derived and where it comes from.

Corollary A.1 (The $1/\phi^2$ bound). *When $p_{\mathcal{E}} = p_{\mathcal{V}} = p_{\mathcal{I}} = 0$, then in case of a fork of the only rational miner m with hashrate p_m, the expected normalized reward for the next block of m, who is one block behind ($z = 1$), is higher when trying to catch-up, as defined in equation 1 from [10, 13], compared to switching to the main chain when $p_m > \frac{1}{\phi^2}$, where ϕ is the golden ratio defined as $\phi = \frac{1+\sqrt{5}}{2} = 1.618033988749895\ldots$ s.t. $\frac{1}{\phi^2} = 0.38196601125010515\ldots$.*

The reason for this lies in the calculation of the success probability for infinitely running attacks as defined in equation 1. The parameters for this attack are $p_{\mathcal{B}} = p_{\mathcal{E}} = p_{\mathcal{V}} = p_{\mathcal{I}} = 0$ and p_m, which leads to $p_{\mathcal{A}} = 1 - p_m$. If we insert these parameters into our equations for ρ_{main} and ρ_{fork} we get:

$$\rho_{main} = \frac{\left(1 - \left(\frac{0}{(1-p_m)+p_m}\right)^2\right) \cdot p_m}{(1-p_m)+p_m} = p_m \tag{12}$$

This basically describes a linear relationship between hashrate and profit if no attack occurs. In case p_m decides to attack and is one block behind, the profitability translates to equation 1 from [10, 13]:

$$\rho_{fork} = \frac{\left(\frac{p_m}{1-p_m}\right)^2 \cdot p_m}{p_m} \cdot (0+1) = \left(\frac{p_m}{1-p_m}\right)^2 \tag{13}$$

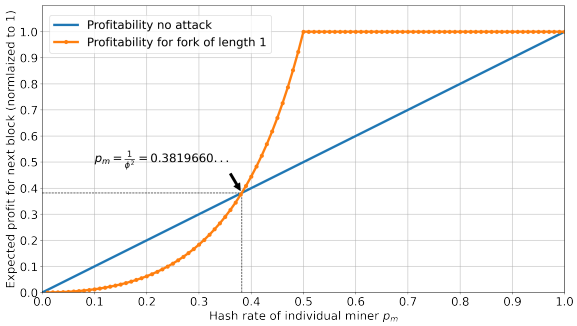


Figure 5: The expected reward for the next block ρ is given on the y-axis, while the hashrate p_m of the miner under consideration is given on the x-axis. The figures shows a comparison of the profitability of mining on the main chain without any forks/attack and mining on a fork/attack with $p_{\mathcal{B}} = p_{\mathcal{E}} = p_{\mathcal{V}} = 0$ and $z = 1$.

Finding the intersection (see Figure 5) yields.

$$p_m = \left(\frac{p_m}{1-p_m}\right)^2 = \frac{3}{2} - \frac{\sqrt{5}}{2} = \frac{3-\sqrt{5}}{2} = \frac{\sqrt{5}-3}{2} = 1 - \frac{1}{\phi} = \frac{1}{\phi^2} \tag{14}$$

Therefore, as soon as the hashrate of the attacking miner p_m surpasses $\frac{1}{\phi^2}$, his chance of winning the infinite race increases beyond his fraction of the total hashrate. □

Although, theoretically correct, corollary A.1 assumes that the attack runs infinitely long, an assumption which is unlikely to hold in practice.

B COMPARISON TABLES

In this section we want to list and compare concreate values of different models and configurations. To aid reproducability and allow readers to spot small changes in values which are not observable in figures, we provide tables for some parameterizations. If the required bribe ϵ in a cell is 0 the cell is colored blue. The code that generates all tables and figures can be found on GitHub[5].

[5] https://github.com/kernoelpanic/howmuchisthefork_artefacts

	$p_m = 0.05$	$p_m = 0.1$	$p_m = 0.2$	$p_m = 0.3$	$p_m = 0.33$	$p_m = 0.382$	$p_m = 0.4$
$p_{\mathcal{E}} = 0.00$	$p_{\mathcal{A}} = 0.950$ $\rho = 0.050$ $\epsilon = 17.054$ $\rho' = 0.050$ $\mathbb{P} = 0.003$	$p_{\mathcal{A}} = 0.900$ $\rho = 0.100$ $\epsilon = 7.125$ $\rho' = 0.100$ $\mathbb{P} = 0.012$	$p_{\mathcal{A}} = 0.800$ $\rho = 0.200$ $\epsilon = 2.321$ $\rho' = 0.200$ $\mathbb{P} = 0.060$	$p_{\mathcal{A}} = 0.700$ $\rho = 0.300$ $\epsilon = 0.883$ $\rho' = 0.300$ $\mathbb{P} = 0.159$	$p_{\mathcal{A}} = 0.670$ $\rho = 0.330$ $\epsilon = 0.649$ $\rho' = 0.330$ $\mathbb{P} = 0.200$	$p_{\mathcal{A}} = 0.618$ $\rho = 0.382$ $\epsilon = 0.353$ $\rho' = 0.382$ $\mathbb{P} = 0.282$	$p_{\mathcal{A}} = 0.600$ $\rho = 0.400$ $\epsilon = 0.275$ $\rho' = 0.400$ $\mathbb{P} = 0.314$
$p_{\mathcal{E}} = 0.05$	$p_{\mathcal{A}} = 0.900$ $\rho = 0.052$ $\epsilon = 7.529$ $\rho' = 0.052$ $\mathbb{P} = 0.012$	$p_{\mathcal{A}} = 0.850$ $\rho = 0.105$ $\epsilon = 4.126$ $\rho' = 0.105$ $\mathbb{P} = 0.031$	$p_{\mathcal{A}} = 0.750$ $\rho = 0.210$ $\epsilon = 1.556$ $\rho' = 0.210$ $\mathbb{P} = 0.103$	$p_{\mathcal{A}} = 0.650$ $\rho = 0.315$ $\epsilon = 0.596$ $\rho' = 0.315$ $\mathbb{P} = 0.230$	$p_{\mathcal{A}} = 0.620$ $\rho = 0.346$ $\epsilon = 0.430$ $\rho' = 0.346$ $\mathbb{P} = 0.279$	$p_{\mathcal{A}} = 0.568$ $\rho = 0.401$ $\epsilon = 0.216$ $\rho' = 0.401$ $\mathbb{P} = 0.373$	$p_{\mathcal{A}} = 0.550$ $\rho = 0.420$ $\epsilon = 0.159$ $\rho' = 0.420$ $\mathbb{P} = 0.408$
$p_{\mathcal{E}} = 0.10$	$p_{\mathcal{A}} = 0.850$ $\rho = 0.055$ $\epsilon = 4.359$ $\rho' = 0.055$ $\mathbb{P} = 0.031$	$p_{\mathcal{A}} = 0.800$ $\rho = 0.110$ $\epsilon = 2.645$ $\rho' = 0.110$ $\mathbb{P} = 0.060$	$p_{\mathcal{A}} = 0.700$ $\rho = 0.219$ $\epsilon = 1.067$ $\rho' = 0.219$ $\mathbb{P} = 0.159$	$p_{\mathcal{A}} = 0.600$ $\rho = 0.329$ $\epsilon = 0.399$ $\rho' = 0.329$ $\mathbb{P} = 0.314$	$p_{\mathcal{A}} = 0.570$ $\rho = 0.362$ $\epsilon = 0.278$ $\rho' = 0.362$ $\mathbb{P} = 0.369$	$p_{\mathcal{A}} = 0.518$ $\rho = 0.419$ $\epsilon = 0.122$ $\rho' = 0.419$ $\mathbb{P} = 0.471$	$p_{\mathcal{A}} = 0.500$ $\rho = 0.439$ $\epsilon = 0.081$ $\rho' = 0.439$ $\mathbb{P} = 0.508$
$p_{\mathcal{E}} = 0.20$	$p_{\mathcal{A}} = 0.750$ $\rho = 0.059$ $\epsilon = 1.860$ $\rho' = 0.059$ $\mathbb{P} = 0.103$	$p_{\mathcal{A}} = 0.700$ $\rho = 0.117$ $\epsilon = 1.212$ $\rho' = 0.117$ $\mathbb{P} = 0.159$	$p_{\mathcal{A}} = 0.600$ $\rho = 0.235$ $\epsilon = 0.497$ $\rho' = 0.235$ $\mathbb{P} = 0.314$	$p_{\mathcal{A}} = 0.500$ $\rho = 0.352$ $\epsilon = 0.157$ $\rho' = 0.352$ $\mathbb{P} = 0.508$	$p_{\mathcal{A}} = 0.470$ $\rho = 0.388$ $\epsilon = 0.095$ $\rho' = 0.388$ $\mathbb{P} = 0.569$	$p_{\mathcal{A}} = 0.418$ $\rho = 0.449$ $\epsilon = 0.017$ $\rho' = 0.449$ $\mathbb{P} = 0.672$	$p_{\mathcal{A}} = 0.400$ $\rho = 0.470$ $\epsilon = 0.000$ $\rho' = 0.471$ $\mathbb{P} = 0.706$
$p_{\mathcal{E}} = 0.30$	$p_{\mathcal{A}} = 0.650$ $\rho = 0.060$ $\epsilon = 0.827$ $\rho' = 0.060$ $\mathbb{P} = 0.230$	$p_{\mathcal{A}} = 0.600$ $\rho = 0.120$ $\epsilon = 0.531$ $\rho' = 0.120$ $\mathbb{P} = 0.314$	$p_{\mathcal{A}} = 0.500$ $\rho = 0.240$ $\epsilon = 0.183$ $\rho' = 0.240$ $\mathbb{P} = 0.508$	$p_{\mathcal{A}} = 0.400$ $\rho = 0.360$ $\epsilon = 0.020$ $\rho' = 0.360$ $\mathbb{P} = 0.706$	$p_{\mathcal{A}} = 0.370$ $\rho = 0.396$ $\epsilon = 0.000$ $\rho' = 0.398$ $\mathbb{P} = 0.760$	$p_{\mathcal{A}} = 0.318$ $\rho = 0.459$ $\epsilon = 0.000$ $\rho' = 0.472$ $\mathbb{P} = 0.843$	$p_{\mathcal{A}} = 0.300$ $\rho = 0.480$ $\epsilon = 0.000$ $\rho' = 0.496$ $\mathbb{P} = 0.867$
$p_{\mathcal{E}} = 0.33$	$p_{\mathcal{A}} = 0.620$ $\rho = 0.060$ $\epsilon = 0.626$ $\rho' = 0.060$ $\mathbb{P} = 0.279$	$p_{\mathcal{A}} = 0.570$ $\rho = 0.119$ $\epsilon = 0.390$ $\rho' = 0.119$ $\mathbb{P} = 0.369$	$p_{\mathcal{A}} = 0.470$ $\rho = 0.239$ $\epsilon = 0.112$ $\rho' = 0.239$ $\mathbb{P} = 0.569$	$p_{\mathcal{A}} = 0.370$ $\rho = 0.358$ $\epsilon = 0.000$ $\rho' = 0.362$ $\mathbb{P} = 0.760$	$p_{\mathcal{A}} = 0.340$ $\rho = 0.394$ $\epsilon = 0.000$ $\rho' = 0.405$ $\mathbb{P} = 0.810$	$p_{\mathcal{A}} = 0.288$ $\rho = 0.456$ $\epsilon = 0.000$ $\rho' = 0.474$ $\mathbb{P} = 0.883$	$p_{\mathcal{A}} = 0.270$ $\rho = 0.478$ $\epsilon = 0.000$ $\rho' = 0.495$ $\mathbb{P} = 0.904$
$p_{\mathcal{E}} = 0.38$	$p_{\mathcal{A}} = 0.568$ $\rho = 0.058$ $\epsilon = 0.345$ $\rho' = 0.058$ $\mathbb{P} = 0.373$	$p_{\mathcal{A}} = 0.518$ $\rho = 0.116$ $\epsilon = 0.187$ $\rho' = 0.116$ $\mathbb{P} = 0.471$	$p_{\mathcal{A}} = 0.418$ $\rho = 0.232$ $\epsilon = 0.006$ $\rho' = 0.232$ $\mathbb{P} = 0.672$	$p_{\mathcal{A}} = 0.318$ $\rho = 0.348$ $\epsilon = 0.000$ $\rho' = 0.371$ $\mathbb{P} = 0.843$	$p_{\mathcal{A}} = 0.288$ $\rho = 0.383$ $\epsilon = 0.000$ $\rho' = 0.409$ $\mathbb{P} = 0.883$	$p_{\mathcal{A}} = 0.236$ $\rho = 0.444$ $\epsilon = 0.000$ $\rho' = 0.468$ $\mathbb{P} = 0.937$	$p_{\mathcal{A}} = 0.218$ $\rho = 0.464$ $\epsilon = 0.000$ $\rho' = 0.487$ $\mathbb{P} = 0.951$
$p_{\mathcal{E}} = 0.40$	$p_{\mathcal{A}} = 0.550$ $\rho = 0.057$ $\epsilon = 0.262$ $\rho' = 0.057$ $\mathbb{P} = 0.408$	$p_{\mathcal{A}} = 0.500$ $\rho = 0.114$ $\epsilon = 0.126$ $\rho' = 0.114$ $\mathbb{P} = 0.508$	$p_{\mathcal{A}} = 0.400$ $\rho = 0.229$ $\epsilon = 0.000$ $\rho' = 0.235$ $\mathbb{P} = 0.706$	$p_{\mathcal{A}} = 0.300$ $\rho = 0.343$ $\epsilon = 0.000$ $\rho' = 0.372$ $\mathbb{P} = 0.867$	$p_{\mathcal{A}} = 0.270$ $\rho = 0.377$ $\epsilon = 0.000$ $\rho' = 0.408$ $\mathbb{P} = 0.904$	$p_{\mathcal{A}} = 0.218$ $\rho = 0.437$ $\epsilon = 0.000$ $\rho' = 0.465$ $\mathbb{P} = 0.951$	$p_{\mathcal{A}} = 0.200$ $\rho = 0.457$ $\epsilon = 0.000$ $\rho' = 0.482$ $\mathbb{P} = 0.963$

Table 1: Comparison of minimum bribe required per block ϵ for $\rho_{\textbf{fork bl.}} > \rho_{\textbf{main bl.}}$ with probabilities calculated using our Markov chain. The axis iterate the hashrate of an individual miner p_m, and other attackers $p_{\mathcal{E}}$. The table also shows the expected reward of miner m, if p_m would be directed towards the attack chain $\rho' = \rho_{\textbf{fork bl.}}$, as well as the expected reward $\rho = \rho_{\textbf{main bl.}}$, if p_m would be directed towards the main chain. All attacks start with a disadvantage of $z = 1$, a duration of $N = 8$ and the following configuration of the Markov chain $\overrightarrow{k} = 1$, $\overleftarrow{k} = 10, \eta_{attack} = 0, \eta_{main} = 0, p_{\mathcal{V}} = 0.000000$.

	$p_m = 0.05$	$p_m = 0.1$	$p_m = 0.2$	$p_m = 0.3$	$p_m = 0.33$	$p_m = 0.382$	$p_m = 0.4$
$p_{\mathcal{E}} = 0.00$	$p_{\mathcal{A}} = 0.850$ $\rho = 1.050$ $\epsilon = 20.157$ $\rho' = 1.050$ $\mathbb{P} = 0.002$	$p_{\mathcal{A}} = 0.800$ $\rho = 1.100$ $\epsilon = 9.004$ $\rho' = 1.100$ $\mathbb{P} = 0.011$	$p_{\mathcal{A}} = 0.700$ $\rho = 1.200$ $\epsilon = 3.617$ $\rho' = 1.200$ $\mathbb{P} = 0.055$	$p_{\mathcal{A}} = 0.600$ $\rho = 1.300$ $\epsilon = 2.015$ $\rho' = 1.300$ $\mathbb{P} = 0.149$	$p_{\mathcal{A}} = 0.570$ $\rho = 1.330$ $\epsilon = 1.755$ $\rho' = 1.330$ $\mathbb{P} = 0.188$	$p_{\mathcal{A}} = 0.518$ $\rho = 1.382$ $\epsilon = 1.429$ $\rho' = 1.382$ $\mathbb{P} = 0.267$	$p_{\mathcal{A}} = 0.500$ $\rho = 1.400$ $\epsilon = 1.342$ $\rho' = 1.400$ $\mathbb{P} = 0.298$
$p_{\mathcal{E}} = 0.05$	$p_{\mathcal{A}} = 0.800$ $\rho = 1.050$ $\epsilon = 10.039$ $\rho' = 1.050$ $\mathbb{P} = 0.011$	$p_{\mathcal{A}} = 0.750$ $\rho = 1.103$ $\epsilon = 6.021$ $\rho' = 1.103$ $\mathbb{P} = 0.028$	$p_{\mathcal{A}} = 0.650$ $\rho = 1.208$ $\epsilon = 2.988$ $\rho' = 1.208$ $\mathbb{P} = 0.095$	$p_{\mathcal{A}} = 0.550$ $\rho = 1.314$ $\epsilon = 1.856$ $\rho' = 1.314$ $\mathbb{P} = 0.217$	$p_{\mathcal{A}} = 0.520$ $\rho = 1.346$ $\epsilon = 1.659$ $\rho' = 1.346$ $\mathbb{P} = 0.264$	$p_{\mathcal{A}} = 0.468$ $\rho = 1.401$ $\epsilon = 1.404$ $\rho' = 1.401$ $\mathbb{P} = 0.356$	$p_{\mathcal{A}} = 0.450$ $\rho = 1.420$ $\epsilon = 1.336$ $\rho' = 1.420$ $\mathbb{P} = 0.390$
$p_{\mathcal{E}} = 0.10$	$p_{\mathcal{A}} = 0.750$ $\rho = 1.045$ $\epsilon = 6.781$ $\rho' = 1.045$ $\mathbb{P} = 0.028$	$p_{\mathcal{A}} = 0.700$ $\rho = 1.100$ $\epsilon = 4.630$ $\rho' = 1.100$ $\mathbb{P} = 0.055$	$p_{\mathcal{A}} = 0.600$ $\rho = 1.212$ $\epsilon = 2.639$ $\rho' = 1.212$ $\mathbb{P} = 0.149$	$p_{\mathcal{A}} = 0.500$ $\rho = 1.325$ $\epsilon = 1.786$ $\rho' = 1.325$ $\mathbb{P} = 0.298$	$p_{\mathcal{A}} = 0.470$ $\rho = 1.358$ $\epsilon = 1.630$ $\rho' = 1.358$ $\mathbb{P} = 0.352$	$p_{\mathcal{A}} = 0.418$ $\rho = 1.417$ $\epsilon = 1.424$ $\rho' = 1.417$ $\mathbb{P} = 0.453$	$p_{\mathcal{A}} = 0.400$ $\rho = 1.437$ $\epsilon = 1.369$ $\rho' = 1.437$ $\mathbb{P} = 0.489$
$p_{\mathcal{E}} = 0.20$	$p_{\mathcal{A}} = 0.650$ $\rho = 1.007$ $\epsilon = 4.355$ $\rho' = 1.007$ $\mathbb{P} = 0.095$	$p_{\mathcal{A}} = 0.600$ $\rho = 1.069$ $\epsilon = 3.398$ $\rho' = 1.069$ $\mathbb{P} = 0.149$	$p_{\mathcal{A}} = 0.500$ $\rho = 1.196$ $\epsilon = 2.319$ $\rho' = 1.196$ $\mathbb{P} = 0.298$	$p_{\mathcal{A}} = 0.400$ $\rho = 1.326$ $\epsilon = 1.777$ $\rho' = 1.326$ $\mathbb{P} = 0.489$	$p_{\mathcal{A}} = 0.370$ $\rho = 1.365$ $\epsilon = 1.673$ $\rho' = 1.365$ $\mathbb{P} = 0.550$	$p_{\mathcal{A}} = 0.318$ $\rho = 1.433$ $\epsilon = 1.534$ $\rho' = 1.433$ $\mathbb{P} = 0.653$	$p_{\mathcal{A}} = 0.300$ $\rho = 1.457$ $\epsilon = 1.496$ $\rho' = 1.457$ $\mathbb{P} = 0.688$
$p_{\mathcal{E}} = 0.30$	$p_{\mathcal{A}} = 0.550$ $\rho = 0.918$ $\epsilon = 3.365$ $\rho' = 0.918$ $\mathbb{P} = 0.217$	$p_{\mathcal{A}} = 0.500$ $\rho = 0.987$ $\epsilon = 2.827$ $\rho' = 0.987$ $\mathbb{P} = 0.298$	$p_{\mathcal{A}} = 0.400$ $\rho = 1.129$ $\epsilon = 2.160$ $\rho' = 1.129$ $\mathbb{P} = 0.489$	$p_{\mathcal{A}} = 0.300$ $\rho = 1.277$ $\epsilon = 1.805$ $\rho' = 1.277$ $\mathbb{P} = 0.688$	$p_{\mathcal{A}} = 0.270$ $\rho = 1.322$ $\epsilon = 1.737$ $\rho' = 1.322$ $\mathbb{P} = 0.743$	$p_{\mathcal{A}} = 0.218$ $\rho = 1.402$ $\epsilon = 1.652$ $\rho' = 1.402$ $\mathbb{P} = 0.828$	$p_{\mathcal{A}} = 0.200$ $\rho = 1.430$ $\epsilon = 1.631$ $\rho' = 1.430$ $\mathbb{P} = 0.854$
$p_{\mathcal{E}} = 0.33$	$p_{\mathcal{A}} = 0.520$ $\rho = 0.880$ $\epsilon = 3.153$ $\rho' = 0.880$ $\mathbb{P} = 0.264$	$p_{\mathcal{A}} = 0.470$ $\rho = 0.950$ $\epsilon = 2.692$ $\rho' = 0.950$ $\mathbb{P} = 0.352$	$p_{\mathcal{A}} = 0.370$ $\rho = 1.096$ $\epsilon = 2.112$ $\rho' = 1.096$ $\mathbb{P} = 0.550$	$p_{\mathcal{A}} = 0.270$ $\rho = 1.249$ $\epsilon = 1.803$ $\rho' = 1.249$ $\mathbb{P} = 0.743$	$p_{\mathcal{A}} = 0.240$ $\rho = 1.296$ $\epsilon = 1.745$ $\rho' = 1.296$ $\mathbb{P} = 0.794$	$p_{\mathcal{A}} = 0.188$ $\rho = 1.379$ $\epsilon = 1.676$ $\rho' = 1.379$ $\mathbb{P} = 0.870$	$p_{\mathcal{A}} = 0.170$ $\rho = 1.408$ $\epsilon = 1.660$ $\rho' = 1.408$ $\mathbb{P} = 0.892$
$p_{\mathcal{E}} = 0.38$	$p_{\mathcal{A}} = 0.468$ $\rho = 0.801$ $\epsilon = 2.818$ $\rho' = 0.801$ $\mathbb{P} = 0.356$	$p_{\mathcal{A}} = 0.418$ $\rho = 0.873$ $\epsilon = 2.464$ $\rho' = 0.873$ $\mathbb{P} = 0.453$	$p_{\mathcal{A}} = 0.318$ $\rho = 1.023$ $\epsilon = 2.011$ $\rho' = 1.023$ $\mathbb{P} = 0.653$	$p_{\mathcal{A}} = 0.218$ $\rho = 1.183$ $\epsilon = 1.775$ $\rho' = 1.183$ $\mathbb{P} = 0.828$	$p_{\mathcal{A}} = 0.188$ $\rho = 1.233$ $\epsilon = 1.735$ $\rho' = 1.233$ $\mathbb{P} = 0.870$	$p_{\mathcal{A}} = 0.136$ $\rho = 1.321$ $\epsilon = 1.693$ $\rho' = 1.321$ $\mathbb{P} = 0.927$	$p_{\mathcal{A}} = 0.118$ $\rho = 1.352$ $\epsilon = 1.685$ $\rho' = 1.352$ $\mathbb{P} = 0.943$
$p_{\mathcal{E}} = 0.40$	$p_{\mathcal{A}} = 0.450$ $\rho = 0.771$ $\epsilon = 2.706$ $\rho' = 0.771$ $\mathbb{P} = 0.390$	$p_{\mathcal{A}} = 0.400$ $\rho = 0.842$ $\epsilon = 2.383$ $\rho' = 0.842$ $\mathbb{P} = 0.489$	$p_{\mathcal{A}} = 0.300$ $\rho = 0.993$ $\epsilon = 1.968$ $\rho' = 0.993$ $\mathbb{P} = 0.688$	$p_{\mathcal{A}} = 0.200$ $\rho = 1.155$ $\epsilon = 1.757$ $\rho' = 1.155$ $\mathbb{P} = 0.854$	$p_{\mathcal{A}} = 0.170$ $\rho = 1.206$ $\epsilon = 1.722$ $\rho' = 1.206$ $\mathbb{P} = 0.892$	$p_{\mathcal{A}} = 0.118$ $\rho = 1.296$ $\epsilon = 1.689$ $\rho' = 1.296$ $\mathbb{P} = 0.943$	$p_{\mathcal{A}} = 0.100$ $\rho = 1.328$ $\epsilon = 1.685$ $\rho' = 1.328$ $\mathbb{P} = 0.956$

Table 2: Comparison of minimum bribe required per block ϵ for $\rho_{\textbf{fork bl.}} > \rho_{\textbf{main bl.}}$ with probabilities calculated using our Markov chain. The axis iterate the hashrate of an individual miner p_m, and other attackers $p_{\mathcal{E}}$. The table also shows the expected reward of miner m, if p_m would be directed towards the attack chain $\rho' = \rho_{\textbf{fork bl.}}$, as well as the expected reward $\rho = \rho_{\textbf{main bl.}}$, if p_m would be directed towards the main chain. All attacks start with a disadvantage of $z = 1$, a duration of $N = 8$ and the following configuration of the Markov chain $\overrightarrow{k} = 3$, $\overleftarrow{k} = 10, \eta_{attack} = 0, \eta_{main} = 1, p_{\mathcal{V}} = 0.100000$.

	$p_m = 0.05$	$p_m = 0.1$	$p_m = 0.2$	$p_m = 0.3$	$p_m = 0.33$	$p_m = 0.382$	$p_m = 0.4$
$p_{\mathcal{E}} = 0.00$	$p_{\mathcal{A}} = 0.850$ $\rho = 0.050$ $\epsilon = 0.000$ $\rho' = 1.000$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.800$ $\rho = 0.100$ $\epsilon = 0.000$ $\rho' = 1.000$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.700$ $\rho = 0.200$ $\epsilon = 0.000$ $\rho' = 1.000$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.600$ $\rho = 0.300$ $\epsilon = 0.000$ $\rho' = 1.000$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.570$ $\rho = 0.330$ $\epsilon = 0.000$ $\rho' = 1.000$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.518$ $\rho = 0.382$ $\epsilon = 0.000$ $\rho' = 1.000$ $\mathbb{P} = 0.001$	$p_{\mathcal{A}} = 0.500$ $\rho = 0.400$ $\epsilon = 0.000$ $\rho' = 1.000$ $\mathbb{P} = 0.001$
$p_{\mathcal{E}} = 0.05$	$p_{\mathcal{A}} = 0.800$ $\rho = 0.053$ $\epsilon = 0.000$ $\rho' = 0.500$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.750$ $\rho = 0.105$ $\epsilon = 0.000$ $\rho' = 0.667$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.650$ $\rho = 0.211$ $\epsilon = 0.000$ $\rho' = 0.800$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.550$ $\rho = 0.316$ $\epsilon = 0.000$ $\rho' = 0.857$ $\mathbb{P} = 0.001$	$p_{\mathcal{A}} = 0.520$ $\rho = 0.347$ $\epsilon = 0.000$ $\rho' = 0.868$ $\mathbb{P} = 0.001$	$p_{\mathcal{A}} = 0.468$ $\rho = 0.402$ $\epsilon = 0.000$ $\rho' = 0.884$ $\mathbb{P} = 0.003$	$p_{\mathcal{A}} = 0.450$ $\rho = 0.421$ $\epsilon = 0.000$ $\rho' = 0.889$ $\mathbb{P} = 0.003$
$p_{\mathcal{E}} = 0.10$	$p_{\mathcal{A}} = 0.750$ $\rho = 0.056$ $\epsilon = 0.000$ $\rho' = 0.333$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.700$ $\rho = 0.111$ $\epsilon = 0.000$ $\rho' = 0.500$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.600$ $\rho = 0.222$ $\epsilon = 0.000$ $\rho' = 0.667$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.500$ $\rho = 0.333$ $\epsilon = 0.000$ $\rho' = 0.750$ $\mathbb{P} = 0.001$	$p_{\mathcal{A}} = 0.470$ $\rho = 0.367$ $\epsilon = 0.000$ $\rho' = 0.767$ $\mathbb{P} = 0.002$	$p_{\mathcal{A}} = 0.418$ $\rho = 0.424$ $\epsilon = 0.000$ $\rho' = 0.793$ $\mathbb{P} = 0.005$	$p_{\mathcal{A}} = 0.400$ $\rho = 0.444$ $\epsilon = 0.000$ $\rho' = 0.800$ $\mathbb{P} = 0.007$
$p_{\mathcal{E}} = 0.20$	$p_{\mathcal{A}} = 0.650$ $\rho = 0.062$ $\epsilon = 0.000$ $\rho' = 0.200$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.600$ $\rho = 0.125$ $\epsilon = 0.000$ $\rho' = 0.333$ $\mathbb{P} = 0.000$	$p_{\mathcal{A}} = 0.500$ $\rho = 0.250$ $\epsilon = 0.000$ $\rho' = 0.500$ $\mathbb{P} = 0.001$	$p_{\mathcal{A}} = 0.400$ $\rho = 0.375$ $\epsilon = 0.000$ $\rho' = 0.600$ $\mathbb{P} = 0.007$	$p_{\mathcal{A}} = 0.370$ $\rho = 0.412$ $\epsilon = 0.000$ $\rho' = 0.623$ $\mathbb{P} = 0.011$	$p_{\mathcal{A}} = 0.318$ $\rho = 0.477$ $\epsilon = 0.000$ $\rho' = 0.656$ $\mathbb{P} = 0.020$	$p_{\mathcal{A}} = 0.300$ $\rho = 0.500$ $\epsilon = 0.000$ $\rho' = 0.667$ $\mathbb{P} = 0.025$
$p_{\mathcal{E}} = 0.30$	$p_{\mathcal{A}} = 0.550$ $\rho = 0.071$ $\epsilon = 0.000$ $\rho' = 0.143$ $\mathbb{P} = 0.001$	$p_{\mathcal{A}} = 0.500$ $\rho = 0.143$ $\epsilon = 0.000$ $\rho' = 0.250$ $\mathbb{P} = 0.001$	$p_{\mathcal{A}} = 0.400$ $\rho = 0.286$ $\epsilon = 0.000$ $\rho' = 0.400$ $\mathbb{P} = 0.007$	$p_{\mathcal{A}} = 0.300$ $\rho = 0.429$ $\epsilon = 0.000$ $\rho' = 0.500$ $\mathbb{P} = 0.025$	$p_{\mathcal{A}} = 0.270$ $\rho = 0.471$ $\epsilon = 0.000$ $\rho' = 0.524$ $\mathbb{P} = 0.035$	$p_{\mathcal{A}} = 0.218$ $\rho = 0.546$ $\epsilon = 0.000$ $\rho' = 0.560$ $\mathbb{P} = 0.062$	$p_{\mathcal{A}} = 0.200$ $\rho = 0.571$ $\epsilon = 0.000$ $\rho' = 0.571$ $\mathbb{P} = 0.074$
$p_{\mathcal{E}} = 0.33$	$p_{\mathcal{A}} = 0.520$ $\rho = 0.075$ $\epsilon = 0.000$ $\rho' = 0.132$ $\mathbb{P} = 0.001$	$p_{\mathcal{A}} = 0.470$ $\rho = 0.149$ $\epsilon = 0.000$ $\rho' = 0.233$ $\mathbb{P} = 0.002$	$p_{\mathcal{A}} = 0.370$ $\rho = 0.298$ $\epsilon = 0.000$ $\rho' = 0.377$ $\mathbb{P} = 0.011$	$p_{\mathcal{A}} = 0.270$ $\rho = 0.448$ $\epsilon = 0.000$ $\rho' = 0.476$ $\mathbb{P} = 0.035$	$p_{\mathcal{A}} = 0.240$ $\rho = 0.492$ $\epsilon = 0.000$ $\rho' = 0.500$ $\mathbb{P} = 0.049$	$p_{\mathcal{A}} = 0.188$ $\rho = 0.570$ $\epsilon = 0.748$ $\rho' = 0.570$ $\mathbb{P} = 0.083$	$p_{\mathcal{A}} = 0.170$ $\rho = 0.597$ $\epsilon = 0.898$ $\rho' = 0.597$ $\mathbb{P} = 0.099$
$p_{\mathcal{E}} = 0.38$	$p_{\mathcal{A}} = 0.468$ $\rho = 0.081$ $\epsilon = 0.000$ $\rho' = 0.116$ $\mathbb{P} = 0.003$	$p_{\mathcal{A}} = 0.418$ $\rho = 0.162$ $\epsilon = 0.000$ $\rho' = 0.207$ $\mathbb{P} = 0.005$	$p_{\mathcal{A}} = 0.318$ $\rho = 0.323$ $\epsilon = 0.000$ $\rho' = 0.344$ $\mathbb{P} = 0.020$	$p_{\mathcal{A}} = 0.218$ $\rho = 0.485$ $\epsilon = 1.664$ $\rho' = 0.485$ $\mathbb{P} = 0.062$	$p_{\mathcal{A}} = 0.188$ $\rho = 0.534$ $\epsilon = 1.813$ $\rho' = 0.534$ $\mathbb{P} = 0.083$	$p_{\mathcal{A}} = 0.136$ $\rho = 0.618$ $\epsilon = 1.722$ $\rho' = 0.618$ $\mathbb{P} = 0.137$	$p_{\mathcal{A}} = 0.118$ $\rho = 0.647$ $\epsilon = 1.644$ $\rho' = 0.647$ $\mathbb{P} = 0.161$
$p_{\mathcal{E}} = 0.40$	$p_{\mathcal{A}} = 0.450$ $\rho = 0.083$ $\epsilon = 0.000$ $\rho' = 0.111$ $\mathbb{P} = 0.003$	$p_{\mathcal{A}} = 0.400$ $\rho = 0.166$ $\epsilon = 0.000$ $\rho' = 0.200$ $\mathbb{P} = 0.007$	$p_{\mathcal{A}} = 0.300$ $\rho = 0.333$ $\epsilon = 0.000$ $\rho' = 0.333$ $\mathbb{P} = 0.025$	$p_{\mathcal{A}} = 0.200$ $\rho = 0.500$ $\epsilon = 2.233$ $\rho' = 0.500$ $\mathbb{P} = 0.074$	$p_{\mathcal{A}} = 0.170$ $\rho = 0.549$ $\epsilon = 2.168$ $\rho' = 0.549$ $\mathbb{P} = 0.099$	$p_{\mathcal{A}} = 0.118$ $\rho = 0.636$ $\epsilon = 1.878$ $\rho' = 0.636$ $\mathbb{P} = 0.161$	$p_{\mathcal{A}} = 0.100$ $\rho = 0.666$ $\epsilon = 1.760$ $\rho' = 0.666$ $\mathbb{P} = 0.189$

Table 3: Comparison of minimum bribe required per block ϵ for $\rho_{\textit{fork comp.}} > \rho_{\textit{main comp.}}$ with effort-related compensation and probabilities calculated using our Markov chain. The axis iterate the hashrate of an individual miner p_m, and other attackers $p_{\mathcal{E}}$. The table also shows the expected reward of miner m, if p_m would be directed towards the attack chain $\rho' = \rho_{\textit{fork comp.}}$, as well as the expected reward $\rho = \rho_{\textit{main comp.}}$, if p_m would be directed towards the main chain. All attacks start with a disadvantage of $z = 6$ and a duration of $N = 8$ and the following configuration of the Markov chain $\overrightarrow{k} = 3, \overleftarrow{k} = 10, \eta_{attack} = 0, \eta_{main} = 0, p_{\mathcal{V}} = 0.100000$.