

Inside Qubic’s Selfish Mining Campaign on Monero: Evidence, Tactics, and Limits

Suhyeon Lee ✉ 

ShardLab, Seoul, Republic of Korea

Hashed Open Research, Seoul, Republic of Korea

Hyeongyeong Kim 

Korea University, Seoul, Republic of Korea

Abstract

In 2025, the blockchain network Qubic conducted a mining campaign on Monero, a privacy-focused cryptocurrency. It publicly presented the campaign as a “51% takeover” and a demonstration of selfish mining. The episode provides a rare opportunity to test such claims in a privacy-preserving proof-of-work network, where pool attribution and private release decisions are difficult to observe. We combine Monero node measurements, Qubic pool observations, community-shared artifacts, and disclosed view keys to attribute blocks and identify candidate withholding periods. Rather than sustained majority control, we observe elevated orphaning and deeper reorganizations. Qubic did not follow a single optimized selfish mining strategy, instead varying between standard selfish mining and more defensive block-release decisions. Across the campaign, it gained no reward advantage over honest mining. Community monitoring and Qubic’s countermeasures reveal how real-world mining campaigns evolve in response to an active ecosystem. Overall, the campaign disrupted Monero without exhibiting a stable profit-maximizing strategy, leaving open disruptive incentives beyond direct mining rewards.

2012 ACM Subject Classification Security and privacy → Distributed systems security; Computer systems organization → Peer-to-peer architectures; Networks → Network measurement

Keywords and phrases Blockchain, Proof-of-Work, Selfish Mining, Monero

Digital Object Identifier 10.4230/LIPIcs.AFT.2026.28

Related Version *Full Version:* <https://arxiv.org/abs/2512.01437>

Supplementary Material *Dataset (Data and Source Code):* <https://github.com/shlee-lab/Qubic-selfish-mining-study>, archived at `swh:1:dir:0abc35958926898433f7dd17c43e31a822a4378e`

Funding *Suhyeon Lee:* Suhyeon Lee received support from ShardLab.

Acknowledgements We are grateful to the Monero community for sharing artifacts and empirical observations that complemented our measurements. We especially thank DataHoarder (<https://github.com/WeebDataHoarder>) and Sergei Chernykh (sech1) for providing access to supplemental datasets and answering technical questions that helped us validate and refine parts of our analysis. We thank the anonymous reviewers for their thoughtful feedback, which helped improve the paper.

1 Introduction

Selfish mining can undermine the incentive compatibility of proof-of-work systems [2]. By withholding and strategically releasing blocks, a miner can orphan competing blocks and waste other miners’ resources. Despite extensive theoretical study [10, 16], large-scale deployments have rarely been documented on live networks.

In August 2025, Qubic, a blockchain network built around redirecting mining resources to external computations, launched a high-profile mining campaign on Monero (XMR). Qubic reported selling the mined XMR to fund buybacks and burns of its native QUBIC token and to pay miner bonuses, tying the operation to its own token economy [14, 15]. It publicly



© Suhyeon Lee and Hyeongyeong Kim;

licensed under Creative Commons License CC-BY 4.0

8th Conference on Advances in Financial Technologies (AFT 2026).

Editors: Aggelos Kiayias and Maria Kyrpoulou; Article No. 28; pp. 28:1–28:19

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

■ **Table 1** Research questions and main findings.

Research question	Main finding
RQ1. Can Qubic activity be reliably identified despite Monero’s privacy design?	Yes. Community-observed data, extra-nonce patterns, pool observations, and disclosed view keys jointly support Qubic labels and interval-level aggregate measurements.
RQ2. Did Qubic sustain majority mining power, and what direct chain-level impact did its activity have?	We do not observe sustained majority control. Qubic’s share rose sharply in identified periods, but the clearer impact is elevated orphaning and deeper reorganizations.
RQ3. Do static selfish mining models explain Qubic’s observed main-chain share?	No single fixed strategy explains all periods. Qubic’s observed behavior generally fell between standard selfish mining and a more conservative release strategy, while its execution did not appear consistently optimized.
RQ4. Did Qubic gain mining rewards from this behavior, and what execution factors shaped gains or losses?	The withholding intervals do not show consistent reward gains over honest mining. Later difficulty-adjustment spillovers mitigated the shortfall, but Qubic remained below the honest mining baseline across the identified periods and subsequent gaps.
RQ5. How did the Monero ecosystem respond, and how should those responses affect interpretation of the incident?	The community monitored Qubic’s mining activity and relayed reconstructed blocks when possible. Qubic treated this exposure as an operational risk and progressively strengthened its countermeasures, reducing visibility into its internal mining activity over time.

described the campaign as a “51% takeover” and a demonstration of selfish mining. The incident therefore raised practical questions that public dashboards could not answer. We ask what occurred on chain, how the campaign was executed operationally, and whether it was economically effective or primarily disruptive.

This framing also raises a question that block-reward profitability alone cannot answer. Kroll et al. describe a *Goldfinger attack* as an attack whose utility comes from weakening the target cryptocurrency rather than from earning native mining rewards. We restrict our profitability analysis to mining rewards and revisit the available market-price evidence in Section 9.

Answering these questions is especially challenging in Monero. Blocks do not carry explicit pool identifiers, and key signals of selfish mining are off-chain by design. We therefore study the campaign by combining multiple vantage points: blocks on the main chain and orphan blocks from Monero nodes, Qubic pool job notifications, and Qubic-network artifacts shared by the Monero community. Table 1 summarizes the five research questions and our main findings.

We make four contributions:

- **Multi-source attribution and dataset.** We combine node-observed blocks, Qubic pool signals, and community-observed data, and validate the resulting attribution against disclosed view keys while quantifying its coverage limits.
- **Empirical campaign measurement.** We reconstruct Qubic’s mining activity, assess its public claim of majority mining, and measure its effects on orphaning and chain reorganizations.
- **Strategy and economic evaluation.** We compare the observed behavior with the standard selfish mining model and a conservative-release variant, analyze race outcomes, and account for delayed difficulty-adjustment spillovers when evaluating mining rewards.
- **Operational response and inference limits.** We examine community monitoring and Qubic’s countermeasures as operational factors that affected block observability and limit what can be inferred about Qubic’s intended release strategy.

Organization

Section 2 reviews related work. Section 3 describes the data sources, block attribution, and coverage limits. Section 4 measures Qubic’s mining share and its effects on orphaning and chain reorganizations. Sections 5–7 analyze Qubic’s selfish mining behavior and its immediate and delayed effects on mining rewards. Section 8 analyzes community monitoring, Qubic’s countermeasures, and the resulting limits on strategy inference. Section 9 discusses the broader economic interpretation and mitigation implications, and Section 10 concludes.

2 Related Work

Selfish mining and strategy variants

Selfish mining was formalized as a profitable deviation under specific network and propagation assumptions [2]. Follow-on work generalized the attacker’s strategy space, including eclipse variants [10]. Other work studied optimal and efficiently computable selfish mining strategies using Markov decision processes [16, 24], and examined how profitability and thresholds change across protocols such as Ethereum [4]. Intermittent selfish mining has also been studied in the context of difficulty adjustment [11]. Our work builds on these foundations but focuses on what can be validated in a real campaign where internal attacker state is not observable and attribution is difficult. Recent work has also provided statistical and empirical tools for detecting behavior resembling selfish mining in real PoW systems [9].

Propagation, forks, and difficulty dynamics

Propagation delays and network asymmetries shape stale blocks and tie-breaking, and are central to selfish mining performance [1, 3]. Beyond generic propagation effects, Monero’s network-layer attack surface has been studied in the context of eclipse-style isolation [17]. Prior work further showed that difficulty adjustment can interact with variable hash power and adversarial strategies to create unstable throughput or cyclic effects [6].

Defenses and mitigations

A diverse set of defense approaches have been proposed, including Fresh Bitcoins [5], Zeroblock [18], and Publish-or-Perish style mechanisms [23]. Alternative designs such as Frutchains [12] and StrongChain [20] explore fairness and transparency in PoW consensus. In parallel, operational discussions in the Monero community have proposed pool-level detective mining and Publish-or-Perish-inspired mitigations [19, 21]. Finally, work on Monero mining-pool data publication shows that pool-published data can expose otherwise hidden information, illustrating why operational data can matter for incident validation [22].

3 Data Collection and Qubic Block Attribution

This section describes the data sources and processing steps used in the analysis. The dataset and analysis code are available as supplementary material.

3.1 Block and mining information collection

We combine three data sources: Monero block data from nodes, mining job data from Qubic pool job-notification traffic, and Qubic-related block data collected by the Monero community from Qubic network traffic.

Monero block information

We operated a pruned Monero full node, which validates the blockchain while retaining only a subset of prunable transaction data to reduce storage. This node let us collect main-chain blocks and locally observable orphan blocks that are not available from public explorers. We operated it from September 29 to October 17, 2025. For earlier periods, we queried public Monero full nodes via RPC for historical block and coinbase data. To improve orphan coverage, we probed 20 public nodes, selected the five most responsive nodes, and periodically synchronized their orphan observations. Public-node collection still does not guarantee complete orphan coverage, and some pool-specific orphan blocks may remain unobserved.

Qubic mining pool

Qubic distinguishes consensus nodes called *Computors* from miners that receive tasks and return solutions [13]. Our observations cover the public pool API and community-collected job and solution traffic, not Qubic’s full internal network. Because we initiated this study after the campaign was already underway, the job-notification data cover its later phase, from September 26 to October 17, 2025. During this period, we queried the RPC API of the Qubic mining pool at 5-second intervals. The API has a structure similar to the Stratum protocol, which is widely used by PoW mining pools, and is openly accessible. Specifically, the `job_notify` method returns multiple values, including the mining block height and the previous block hash, enabling miners to obtain the most recent mining jobs. These records show which block tip Qubic instructed miners to work on.

Monero community observations

We also obtained an additional dataset of Qubic-related blocks from Monero community users Sergei Chernykh and DataHoarder, who collected it by monitoring Qubic-related activity. We refer to these records as *community-observed Qubic blocks*. The community used multiple observation channels, including Qubic network traffic and related artifacts, but we do not treat the dataset as a complete Qubic-provided ground truth. We use it as an independent view of Qubic-related blocks, especially orphan blocks that may be missed by Monero-node observation. Merging the community and node-derived datasets by block hash adds 93 community-observed orphan blocks that are absent from the node-derived block table, suggesting limited propagation.

3.2 Qubic block attribution

View-key verification

Monero transaction outputs, including coinbase rewards, use one-time addresses that cannot be publicly linked to the recipient’s address. Blocks therefore do not reveal which miner controls a reward output. A disclosed view key allows the corresponding reward outputs to be identified retrospectively. Qubic disclosed its view keys only after each weekly epoch ended, so they could not support real-time attribution. This verification was also limited for periods before our node began operating because we could not fully collect historical orphan-block data. The full version lists the disclosed view keys used in this study.

Initial heuristic attribution

Before obtaining the community dataset and without using the view keys disclosed by Qubic, we constructed an initial seed set from orphan-fork blocks attributed to Qubic. We examined the extra-nonce area of their coinbase transactions and iteratively refined two structural regex patterns to identify additional candidate blocks in the node data. These patterns extended attribution coverage but were not treated as independent proof of ownership. The full version provides representative examples and the two patterns.

Cross-source validation and final labels

We compared the initial labels with the community dataset over the overlapping observation period. Of the 13,000 initially attributed Qubic blocks, 12,989 also appear in the community dataset, corresponding to a 99.92% confirmation rate among the initial positive labels. We observe no disagreement in chain or orphan status among the matched blocks. We retain the remaining 11 node-observed orphan candidates because each matches a Qubic extra-nonce pattern and shares the relevant prefix with a verified Qubic main-chain block at the same height. Their coinbase data were not preserved, however, so they cannot be verified directly with a view key.

The community dataset contains 13,771 Qubic blocks in the study period, 782 of which were missed by our initial heuristic attribution. Of these, 689 were present but unlabeled in our pruned-node dataset, while 93 were absent from it. We relabel the former and add the latter community-only orphan blocks. The resulting union contains 58,944 observed blocks, of which 13,782 are attributed to Qubic. Our final labels therefore follow the community-observed hash set, supplemented by the 11 node-observed orphan candidates.

Coverage and parent-block checks

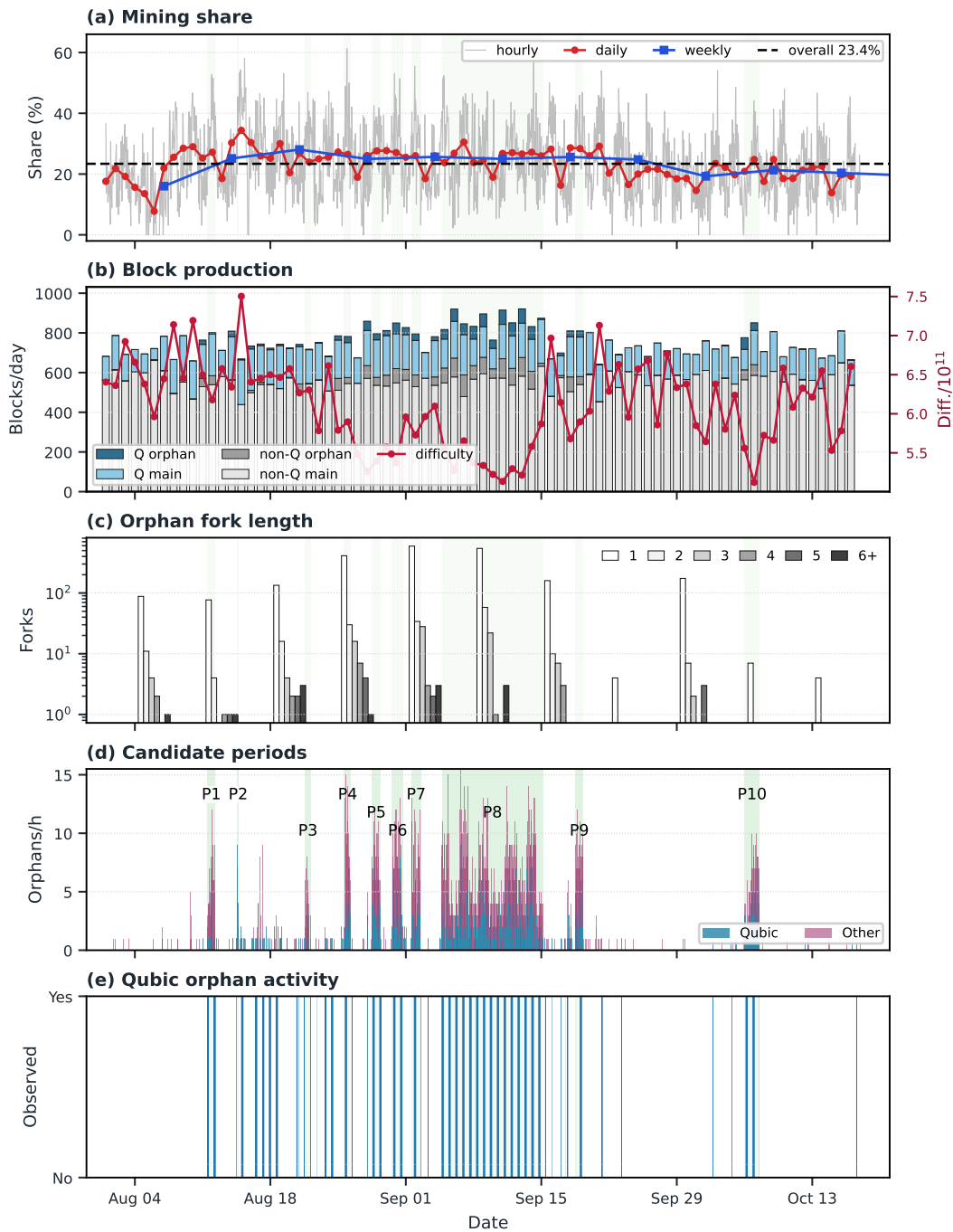
The 93 community-only orphans were observable in the Qubic network and verifiable with disclosed view keys, but absent from observations from our Monero node. Excluding them changes the reported quantities only slightly and does not alter our conclusions. Separately, for community-observed Qubic orphans with raw block blobs, we parse the Monero header `prev_id` and check whether the parent hash appears in either dataset. This identifies the parent for 1,218 of 1,228 such orphans overall and for 1,213 of 1,216 within our observation window. Because the global node-observed table does not preserve raw blobs or parent hashes for every non-Qubic orphan, this check does not establish complete parent coverage for all observed forks. The full version reports the detailed results.

4 Qubic's Mining Share and Network Impact

This section examines Qubic's mining activity on Monero during the measurement period. We first quantify its mining power based on attributed blocks, and then examine its impact on orphan blocks and reorganizations. A focused analysis of Qubic's selfish mining strategy follows in Section 5.

4.1 Observed mining share

Figure 1(a) shows Qubic's observed block-production share in the Monero network, computed as the ratio of Qubic-attributed blocks to all observed main-chain and orphan blocks over weekly, daily, and hourly windows. Because the pool's physical hashrate is difficult both to



■ **Figure 1** Overview of Qubic's mining activity and selfish mining indicators on a common timeline. Panels show (a) Qubic's observed block-production share, (b) daily block production and average difficulty, (c) weekly orphan-fork length distribution, (d) hourly orphan counts and candidate selfish mining periods, and (e) hours containing observed Qubic orphan blocks. Lightly shaded bands denote the ten candidate periods used in the selfish mining analysis.

measure directly and to reconstruct retrospectively, we use this quantity as an empirical estimate of its relative hashrate α in our selfish mining models. This calculation uses the combined attribution set described in Section 3.2, including community-observed Qubic labels. Across the measurement period, the resulting estimate averages 23.38%.

A central point in public discussions was Qubic’s claim, echoed by several media outlets, that it had achieved a 51% mining position on Monero [15]. However, the notion of a “51% attack” is often left ambiguous, and our measurements do not support a persistent majority. In the hourly series, we observe several short intervals where Qubic’s share approaches or briefly exceeds 50%. In contrast, the corresponding daily and weekly aggregates never reach 51%, and Qubic does not maintain a stable majority at any point in our dataset. These results indicate that while Qubic temporarily concentrated substantial mining power, it did not achieve the sustained control typically associated with a practical 51% attack on the Monero network.

4.2 Orphaning and reorganizations

Although Qubic did not sustain majority mining power, periods of elevated Qubic activity coincided with a marked increase in orphaning and deeper forks on Monero.

Figure 1(b) presents the daily counts of main-chain and orphan blocks, separated into Qubic-attributed and non-Qubic blocks, alongside the average network difficulty. During periods of elevated Qubic activity, both Qubic and non-Qubic orphan counts increase markedly. The resulting forks contain blocks from other miners as well as Qubic’s own blocks that failed to enter the main chain.

Among the cases for which raw block blobs are available, we directly verify eleven heights at which at least two distinct blocks attributed to Qubic share the same parent. At nine heights, one Qubic block entered the main chain and another was orphaned. At two additional heights in P2, both Qubic sibling blocks were orphaned in favor of a non-Qubic block. Nine of the eleven cases occurred between August 14 and 17, including six in P2. Mining a second block on the same parent does not extend a private chain, so this behavior wastes the pool’s own work and is inconsistent with a rational mining strategy. We suspect that these events resulted from an early job coordination failure in Qubic’s selfish mining operation. Because our job telemetry begins later, we cannot directly confirm the internal cause.

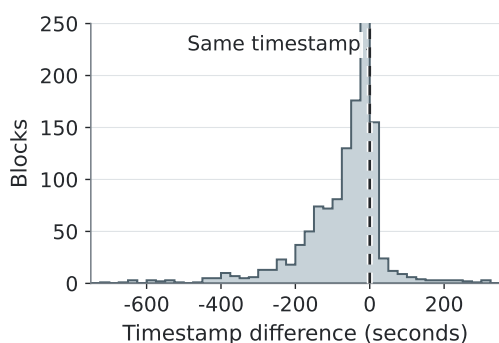
Figure 1(c) shows the distribution of orphan fork lengths over time. Outside periods of elevated Qubic activity, orphan forks are almost exclusively of length one. During high-activity periods, the distribution shifts toward longer orphan chains and more frequent multi-block forks. This pattern shows that the campaign coincided with deeper reorganizations rather than only more isolated one-block orphans.

5 Qubic’s Selfish Mining Strategy and Revenue

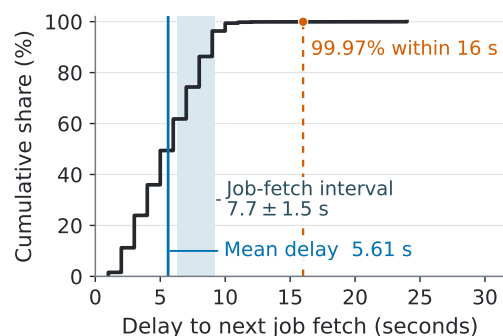
We examine how Qubic’s selfish mining behavior varied over time and compare its observed mining revenue with model predictions and honest mining baselines.

5.1 Selfish mining strategies

Selfish mining, introduced by Eyal and Sirer [2] and later optimized by Sapirshtein et al. [16], describes how a rational miner (or pool) withholds blocks and selectively publishes a private chain to seek a revenue share exceeding its relative hashrate. We use the original Eyal–Sirer strategy as our standard selfish mining model. In practice, miners face uncertainty due to



■ **Figure 2** Qubic blocks’ timestamp difference distribution with same-height competing blocks, including orphan blocks.



■ **Figure 3** Empirical CDF of the delay between Qubic block timestamps and the first subsequent job-fetch record that references the block. The mean delay is 5.61 seconds. 86.3% of matched blocks fall within 8 seconds and 99.97% within 16 seconds.

network asynchrony and incomplete information, and may adapt their withholding and release rules accordingly. Qubic’s observed behavior suggests that its withholding and release rules differed from the standard strategy, although its exact internal strategy remains unobservable.

We use the following terminology throughout the analysis. The attacker’s relative hashrate is denoted by α . A *private chain* is a sequence of valid blocks that the attacker has mined but has not yet broadcast. The *lead* is the number of blocks by which this private chain is ahead of the public chain. For example, if the public chain is at height 100 and the attacker privately holds blocks up to height 102, the lead is 2. In the state-machine figures below, state i means that the attacker has lead i . State 0 means there is no private lead. State $0'$ is the tie-breaking event that occurs when the attacker publishes a withheld block at the same height as an honest block. The parameter γ is defined only for this state $0'$ tie-breaking event: it is the probability that honest miners who find the next block extend the attacker’s branch rather than the competing honest branch. Thus, γ is not an orphan rate and is not estimated from arbitrary non-tip orphan blocks.

Because Qubic’s internal block-discovery times and private-chain states are unavailable, we infer its behavior from Monero main-chain and orphan data, Qubic attribution labels, and block timestamps. We first assess whether the timestamps can approximate event ordering, then use orphan activity to identify sustained selfish mining periods.

5.2 Reliability of Qubic block timestamps

We assess whether Qubic’s block timestamps approximate discovery and release timing. To do so independently of the fork patterns analyzed below, we measure the delay between each timestamp and the first subsequent job-fetch record that references the block as its predecessor.

The mining client is configured to fetch new jobs approximately every 7 seconds, and the observed average fetch interval in our logs is 7.74 ± 1.46 seconds. The mean delay is 5.61 seconds, with 86.3% of matched blocks falling within 8 seconds and 99.97% within 16 seconds (Fig. 3). This delay distribution is consistent with timestamps being generated within Qubic’s normal mining workflow. Although the comparison cannot rule out selective manipulation,

we find no evidence of systematic timestamp shifts large enough to invalidate relative temporal comparisons. Additionally, community observers who monitored Qubic-network traffic reported no indications of systematic timestamp manipulation.¹

Using these timestamps, Fig. 2 shows that most Qubic blocks competing at the same height have timestamps earlier than or comparable to those of their competitors. This timing pattern supports early block discovery followed by selective withholding. The small number of unusually late timestamps occurs predominantly among orphaned Qubic blocks.

We therefore use Qubic’s timestamps, together with orphan dynamics, as approximate indicators of relative event ordering and selfish mining activity. This interpretation assumes that Qubic did not systematically alter timestamps to conceal private-chain lead lengths or release decisions.

5.3 Periods of sustained selfish mining activity

Qubic’s strategy may vary over time, and selfish mining, if present, is unlikely to be applied uniformly across the entire observation window. To separate periods of sustained abnormal orphan activity from the rest of the observation window, we use the heuristic in Alg. 1. We treat such activity as an indicator of potential selfish mining.

■ **Algorithm 1** Selfish Mining Period Heuristic.

Require: Blocks B with timestamps and orphan flags, thresholds $\tau_{\min}$, $d_{\min}$, $g_{\max}$

Ensure: Valid period spans M

```

1: Step 1: Construct the complete hourly series
2:  $H \leftarrow$  complete hourly range covered by  $B$ 
3: for all  $h \in H$  do
4:    $C[h] \leftarrow |\{b \in B : b.\text{is\_orphan} \wedge \lfloor b.\text{timestamp} \rfloor_{\text{hour}} = h\}|$ 
5: end for
6: Step 2: Find maximal contiguous segments
7:  $S \leftarrow$  maximal segments of  $\{h \in H : C[h] \geq \tau_{\min}\}$ 
8:  $S \leftarrow \{(s_i, e_i) \in S : |e_i - s_i| \geq d_{\min}\}$ 
9: Step 3: Merge segments with gaps  $\leq g_{\max}$  hours
10:  $M \leftarrow \text{merge}(S, g_{\max})$ 
11: return  $M$ 

```

The heuristic operates in three steps. First, we construct a complete hourly series over the observation window and compute the orphan count $C[h]$ for each hour, assigning zero to hours with no observed orphan blocks. Second, we identify maximal contiguous segments in which every hour satisfies a minimum orphan-count threshold $\tau_{\min}$ and the total segment length exceeds a minimum duration $d_{\min}$. Third, we merge neighboring segments separated by gaps shorter than $g_{\max}$ hours to tolerate brief fluctuations in activity. The result is a set M of candidate selfish mining periods.

For Fig. 4, we distinguish fork runs involving Qubic and other miners from Qubic self forks in which two blocks attributed to Qubic share the same parent and height. The latter do not identify a private chain lead and are excluded from inference about Qubic’s release strategy.

¹ Personal communication with Monero community observers.

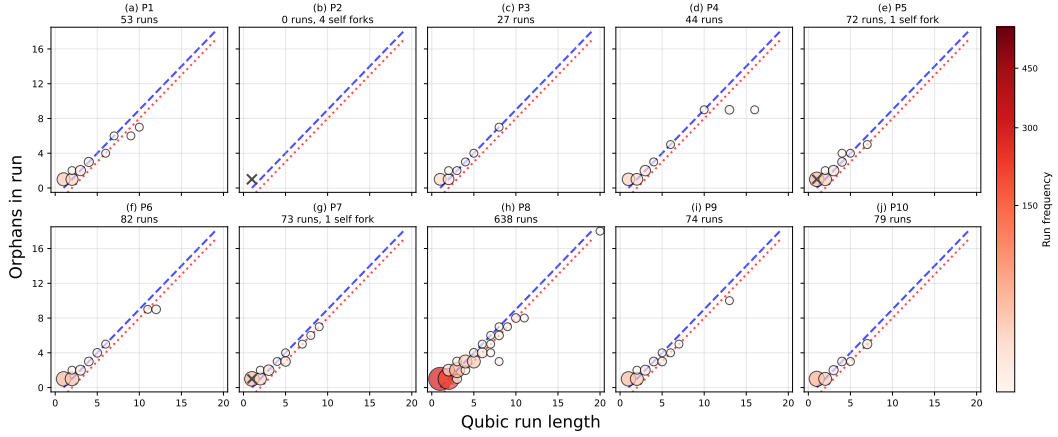


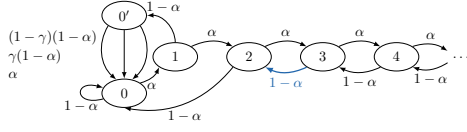
Figure 4 Distribution of orphan blocks per Qubic run length across ten candidate periods, shown in panels (a) through (j). Red circles visualize the frequency of fork runs involving Qubic and other miners. Gray crosses mark Qubic self forks associated with an accepted Qubic block, which are excluded from inference about Qubic’s release strategy because they do not identify a private chain lead. Same-parent Qubic pairs in which both blocks were orphaned fall outside this run-based plot. Reference lines show $y = x - 1$ (blue dashed) and $y = x - 2$ (red dotted).

In our evaluation, we set $\tau_{\min} = 2$ orphan blocks per hour, $d_{\min} = 4$ hours, and $g_{\max} = 6$ hours. These settings capture sustained orphan activity while preventing short gaps from splitting a continuous span of activity into multiple periods. Our heuristic captures sustained, observable phases of Qubic’s selfish mining operation and may miss brief or sporadic activity. The resulting P1–P10 candidate periods form the basis of the focused analyses that follow. To check robustness to the threshold choices, we repeat the analysis over all 80 parameter combinations. In every setting, Qubic’s target-rate-normalized yield remains below the corresponding estimated α , so the aggregate underperformance is not specific to our default parameters. The full version provides the detailed sensitivity analysis, and the artifact includes the full grid.

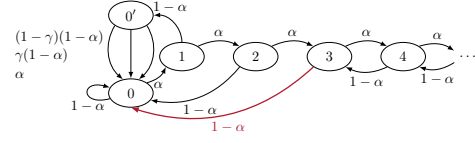
Figure 1(d) shows the resulting candidate periods on the timeline, while Fig. 1(e) shows the hours in which Qubic orphan blocks were observed. Applying this heuristic yields ten periods (P1–P10) during which Qubic’s block share and involvement in orphan blocks are noticeably higher than their global averages. Qubic’s estimated share averages 28.33% across these periods, compared with 23.38% over the full measurement window. This association suggests that sustained, observable selfish mining activity was more common when Qubic’s estimated share was relatively high.

Figure 4 further illustrates how Qubic’s behavior varies across the identified periods by plotting the lengths of runs controlled by Qubic against the number of associated orphan blocks. In P1, P3, and P4, most runs that provide release information lie close to the blue line ($y = x - 1$), corresponding to release at lead 1. P2 instead contains four plotted Qubic self forks, two additional same-parent Qubic pairs that were both orphaned, and no run that provides release information.

During P8, where Qubic’s activity is most intensive, we observe many runs aligned with patterns indicative of release at lead 2, suggesting a more conservative release strategy that avoids exposing the pool to tie situations when the lead is only one block. This shift supports the view that Qubic adapted its release rule over time, motivating the need for an analytical model that captures this conservative release behavior.



■ **Figure 5** Standard selfish mining state machine. State i is the attacker's private lead, and state $0'$ denotes the tie-breaking event.



■ **Figure 6** State machine for the conservative strategy. At lead 3, an honest discovery triggers full publication and a return to state 0.

5.4 Standard and conservative selfish mining models

To interpret the observed periods, we compare them against analytical models of selfish mining. We first recall the standard selfish mining revenue function $R_{\text{selfish}}(\alpha, \gamma)$, which gives the pool's expected main-chain revenue share as a function of its relative hashrate α and the tie-breaking parameter γ . Figure 5 shows the corresponding state machine. When the selfish miner has a private lead, it keeps mining privately. When the honest network catches up, the selfish miner publishes withheld blocks to create or win a race. In state $0'$, the race can resolve in three ways. An honest miner may extend the honest branch with probability $(1-\alpha)(1-\gamma)$, an honest miner may extend the selfish branch with probability $(1-\alpha)\gamma$, or the selfish miner may find the next block with probability α . Equation 1 gives the Eyal-Sirer revenue expression [2].

$$R_{\text{selfish}}(\alpha, \gamma) = \frac{\alpha(1-\alpha)^2(4\alpha + \gamma(1-2\alpha)) - \alpha^3}{1 - \alpha(1 + (2-\alpha)\alpha)} \quad (1)$$

We then consider a conservative-release variant of selfish mining, which we call the conservative strategy. The conservative strategy follows the Eyal-Sirer state transitions except at private lead 3, as shown in Fig. 6. If the honest network finds a block in that state, the attacker fully publishes its three-block private chain and returns to state 0 instead of retaining a private lead. This additional transition represents a more conservative release decision motivated by Qubic's observed behavior. We compare Qubic's observations with both models without assuming that either model captures its exact time-varying strategy.

Using this model, we derive a closed-form expression for the expected revenue under the conservative strategy as a function of α and γ .

► **Proposition 1.** *Let $R_{\text{mod}}(\alpha, \gamma)$ denote the selfish pool's long-run fraction of accepted blocks under the conservative strategy encoded by the state machine in Fig. 6, where $\alpha \in (0, \frac{1}{2})$ is the pool's relative hashrate and $\gamma \in [0, 1]$ is the tie-breaking parameter. Then*

$$R_{\text{mod}}(\alpha, \gamma) = \frac{\alpha(-2\alpha^3\gamma + 3\alpha^3 + 5\alpha^2\gamma - 9\alpha^2 - 4\alpha\gamma + 4\alpha + \gamma)}{1 - \alpha - 2\alpha^2 + \alpha^3 - \alpha^4}. \quad (2)$$

The proof is given in the full version.

5.5 Model predictions and observed revenue

We now apply the analytical model using parameters inferred from the identified selfish mining periods. For each period, we estimate Qubic's relative hashrate α from its share of main-chain and orphaned blocks. We estimate γ only from resolved state $0'$ tie-breaking events: cases where exactly one Qubic block competes with a block attributed to another miner at the same height and the next main-chain block reveals which branch the network extended. If the next block is mined by an honest miner and extends Qubic's branch, we

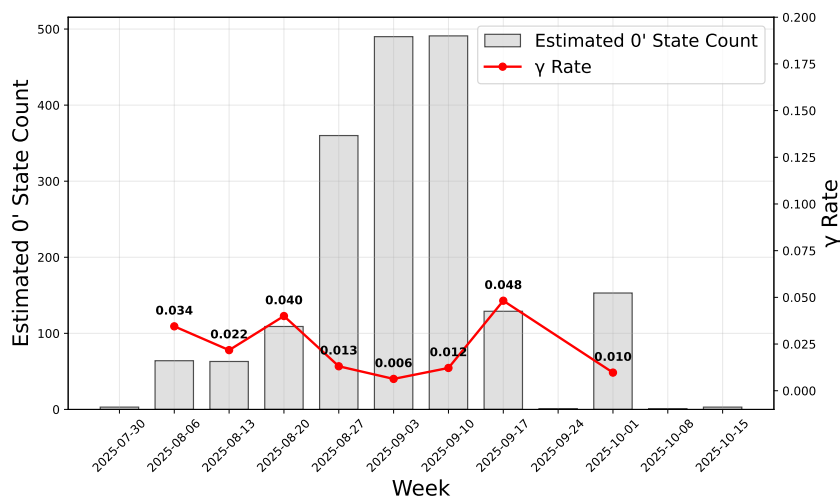


Figure 7 Weekly estimates of the tie-breaking parameter γ and the number of observed state 0' tie-breaking events. We use only resolved races containing exactly one Qubic block and a competing block attributed to another miner. Heights containing multiple Qubic blocks and non-tip orphan blocks are excluded because they do not reveal a binary tie-breaking choice.

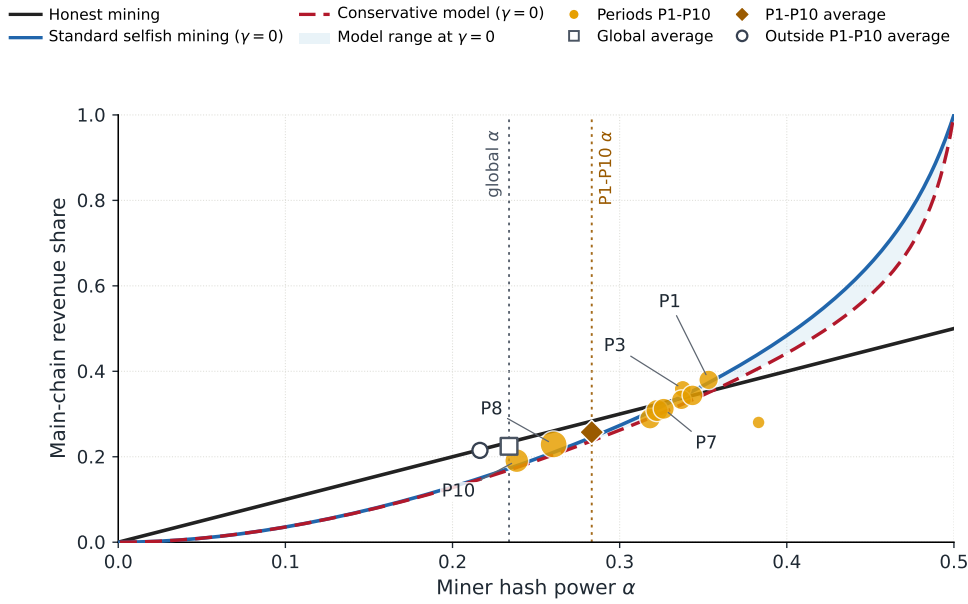
count it as a γ success. If it extends the honest branch, we count it as a failure. We exclude non-tip orphan blocks from this calculation, because they may be discovered after the race has already been resolved and therefore do not measure tie-breaking behavior. Figure 7 shows that the weekly estimates of γ are close to zero. We attribute this to delayed propagation because Qubic blocks tend to arrive at nodes after competing blocks despite having earlier timestamps.

At the average hashrate share of 28.33% during the identified selfish mining periods and $\gamma \approx 0$, the standard selfish mining model yields an expected revenue ratio of $R_{\text{selfish}} \approx 24.56\%$, while the conservative model yields $R_{\text{mod}} \approx 23.71\%$. Both are below the honest mining baseline at the same α . Qubic’s P1–P10 main-chain share is 25.75%, also below the honest mining baseline. The same relation holds without P8, with a main-chain share of 29.88% against an estimated α of 31.53%. Separately, its share of the blocks expected at Monero’s target rate is 25.11%, a 3.22 percentage-point shortfall from α that measures the active-period economic opportunity cost. The net contribution of transaction fees was below 3% of realized block rewards and did not materially affect our conclusions.

The period-level points, however, do not align cleanly with either reference-model prediction. Some periods lie closer to the standard model, some are closer to the conservative model, and P1 and P3 outperform the honest baseline despite the aggregate underperformance. The full version reports the detailed period values. The next section examines observed tie-breaking outcomes as one direct reason why period-level shares can depart from the corresponding $\gamma \approx 0$ model predictions.

6 Race Outcomes and Limits of Static Models

The preceding comparison treats the standard and conservative models as fixed reference strategies. We next examine Qubic’s outcomes in state 0' tie-breaking events as one directly observable source of deviation.



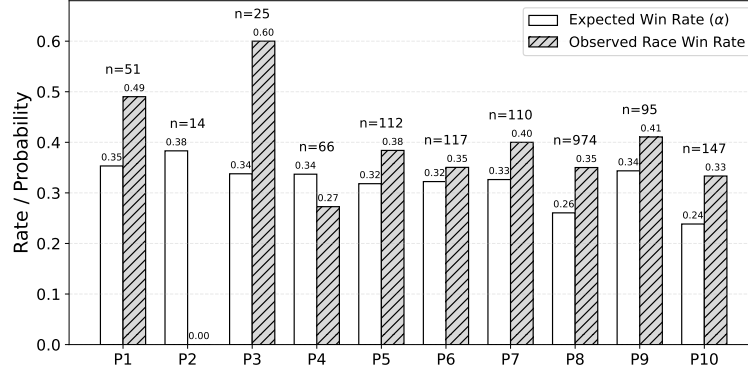
■ **Figure 8** Theoretical main-chain revenue shares predicted by the standard and conservative models at $\gamma \approx 0$, compared with Qubic’s observed main-chain shares. The shaded area shows the revenue range obtained by mixing the two fixed strategies in different proportions. Period markers show P1–P10, with marker size proportional to period scale. The filled diamond shows the P1–P10 average, while hollow markers show the global average and the average outside P1–P10.

The reference-model predictions use the global estimate $\gamma \approx 0$. Local race outcomes can nevertheless differ across periods, and Qubic sometimes won observed state $0'$ tie-breaking events at rates above its period-level mining share. These are cases where exactly one Qubic block competes with a block attributed to another miner at the same height and the next accepted block reveals which branch the network extended. We exclude heights containing multiple Qubic blocks because these self forks do not represent a binary tie-breaking event.

As illustrated in Fig. 9, Qubic’s winning rate in these race conditions was higher than its period-level estimated share α in eight of the ten periods. For example, P1 has an observed race winning rate of 0.49 against $\alpha = 0.35$, P3 has 0.60 against $\alpha = 0.34$, and P7 has 0.40 against $\alpha = 0.33$.

By contrast, P2 recorded no Qubic-branch wins (0/14) and contained six parent-linked Qubic self forks within roughly 95 minutes, suggesting temporary operational instability. P4 also remained below α . More broadly, these results show that period-average α does not fully capture the local conditions under which Qubic released withheld blocks.

These local advantages can help explain why some observed main-chain shares exceed the corresponding $\gamma \approx 0$ model predictions. They do not explain the aggregate target-rate shortfall or establish consistently profitable execution. Race counts are limited in some periods, and high win rates can coexist with orphan losses and missed honest mining rewards. The next section therefore examines whether lower difficulty following the identified periods increased Qubic’s rewards during the subsequent gaps and offset its active-period losses.



■ **Figure 9** Qubic’s winning ratio in observed state $0'$ tie-breaking events. The reference win probability is $\alpha + (1 - \alpha)\gamma$, which reduces to the period-level block share α under the global estimate $\gamma \approx 0$. The observed rate counts events in which the next main-chain block extends Qubic’s branch. Heights containing multiple Qubic blocks are excluded.

7 Intermittent Mining and Difficulty-Adjustment Spillovers

Qubic earned fewer blocks than the honest mining baseline in most of the identified selfish mining periods. Evaluating only these periods may miss a delayed benefit because slower main-chain growth can lower Monero’s sliding-window difficulty in the intervals that follow. Intermittent selfish mining has been studied as a difficulty-adjustment phenomenon [11]. To capture both the immediate and delayed effects, we pair each identified period P_k with its following gap G_k and analyze them as a single accounting sequence.

7.1 Accounting model

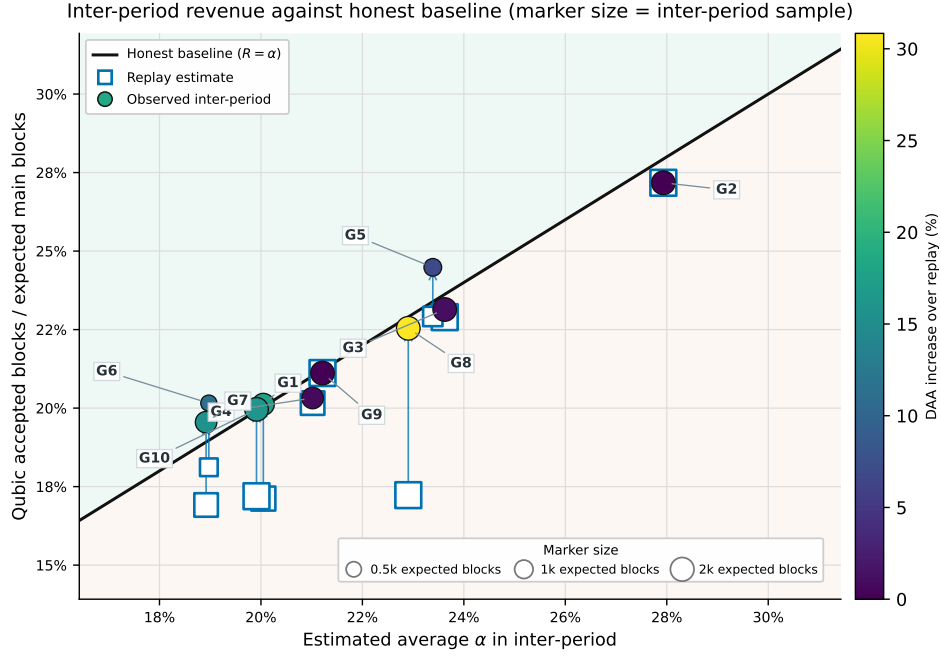
Each G_k begins after P_k and ends when the next identified period starts. For each P_k , we define the signed balance relative to honest mining as

$$\Delta_{\text{active}}(P_k) = B_Q^{\text{main}}(P_k) - \alpha_k N_{\text{target}}(P_k), \quad (3)$$

where $N_{\text{target}}(P_k)$ is the number of blocks expected at Monero’s target rate. A negative value indicates that Qubic obtained fewer accepted blocks than expected from honest mining at its estimated hashrate. This target-rate accounting expresses the period’s effect in block-equivalents, allowing direct comparison with the subsequent DAA effect.

7.2 Estimating delayed effects on gap rewards

If selfish mining reduces main-chain production during P_k , Monero’s sliding-window DAA can leave the following gap with lower difficulty. To estimate this delayed effect, we add synthetic main-chain slots to restore target-rate production during each P_k , then replay Monero’s sliding-window DAA over the reconstructed timeline. This replay estimates the difficulty path that would have followed if main-chain production during P_k had remained at the target rate. We then compare the observed difficulty at each Qubic-attributed accepted block in G_k with the corresponding replayed difficulty. The full version discusses the time-scale implications of Monero’s sliding-window DAA.



■ **Figure 10** Qubic’s gap revenue under the observed and replayed difficulty paths. Each G_k denotes the gap after identified period P_k . The black line is the honest mining baseline $R = \alpha$. Hollow squares show the replay estimate, filled circles show observed gap revenue, and vertical arrows show the DAA spillover. Marker size encodes gap sample size, capped at the 2k expected-block guide for readability.

Let D_i be the observed difficulty at a Qubic-attributed accepted block in G_k , and let $\hat{D}_i$ be the corresponding replayed difficulty. The block-equivalent DAA spillover is

$$\Delta_{\text{DAA}}(G_k) = \sum_{i \in Q(G_k)} \left(1 - \frac{D_i}{\hat{D}_i} \right), \quad (4)$$

where $Q(G_k)$ is the set of Qubic-attributed accepted blocks in the gap. If the observed difficulty is lower than the replayed difficulty, the block contributes a positive fractional block-equivalent.

7.3 Empirical spillover

Figure 10 compares Qubic’s observed gap rewards with the replay estimates. We measure the DAA effect as the increase from the replay estimate to the observed outcome. This comparison is distinct from whether the observed point lies above the honest mining line. Across all gaps, Qubic obtained 7,806 accepted blocks, while the replay yields 7,344.2 block-equivalents. The difference is +461.8 block-equivalents, or +6.3% relative to the replay estimate. Against a target-rate honest mining expectation of 7,855.3 blocks, the observed gap total remains 49.3 blocks lower. Summed across P1–P10, the period balance is −410.7 block-equivalents. Across the identified periods and subsequent gaps, Qubic obtained 11,045 accepted blocks against a target-rate honest mining expectation of 11,505.0, a shortfall of 460.0 block-equivalents, or 4.0%.

P8 and its following gap provide a representative example. During P8, Qubic’s estimated hashrate was 26.05%. It obtained 1,700 accepted blocks, compared with an honest mining expectation of 1,961.5, giving $\Delta_{\text{active}}(P_8) = -261.5$ block-equivalents. During G_8 (P8→P9),

Qubic obtained 541 accepted blocks, while the replay estimate was 413.5 block-equivalents. The resulting $\Delta_{\text{DAA}}(G_8) = +127.5$ block-equivalents substantially raised gap rewards. However, the target-rate honest mining expectation for G_8 was 549.7 blocks, leaving the gap 8.7 blocks lower and the P8– G_8 pair 270.2 block-equivalents below the corresponding honest mining baselines.

The estimated DAA spillover increased Qubic’s rewards in the later gaps. Even with this increase, its combined reward across the identified periods and subsequent gaps remained 4.0% below the target-rate honest mining baseline.

8 Community Monitoring and Qubic Countermeasures

The preceding sections analyzed Qubic’s campaign on Monero quantitatively, using observed data and theoretical mining models. The campaign, however, was a real-world operation in which one blockchain project targeted another live network, with active communities on both sides. The Monero community responded quickly by monitoring Qubic’s mining activity and relaying observations and reconstructed blocks to Monero nodes. Qubic, in turn, introduced countermeasures. This section examines how that interaction affected block observability and informs our interpretation of Qubic’s observed release behavior.

8.1 Community monitoring and block relay

To detect Qubic’s private mining activity, Monero community members deployed monitoring nodes across the network. By connecting to Qubic’s low-level mining network from multiple observation nodes, collecting packet-level data, and analyzing local logs, these community observers reconstructed the timing of mining jobs and their corresponding solution messages on Qubic’s *Computor* network.

Each job encodes a block template, a candidate block assembled for mining that specifies the header and the set of transactions. This allowed the community observers to track which template Qubic used at a given time and when the corresponding solution was observed. They checked the origin and integrity of the collected messages using the digital signatures of Qubic’s dispatcher and *computor* nodes and matched each job to its corresponding solution. They then used the PoW hash in the Result field of each solution message to match the solution to a reconstructed Monero block. Reception-log timestamps provided the timing information.

When these records were sufficient to reconstruct a valid Monero block, community members attempted to propagate it before Qubic’s intended release. The relay was not integrated with a protocol-level mechanism for coordinating Monero nodes, making it difficult to translate these efforts into a reliable chain-level response.

The processed records also helped the community identify Qubic-related blocks and assemble the dataset used in our analysis. We assessed the resulting dataset against observable block patterns and Qubic’s later-disclosed view keys, obtaining the strong agreement reported in Section 3.2.

8.2 Qubic countermeasures

Qubic nevertheless appears to have regarded the possibility of early private-block exposure as an operational risk and soon introduced countermeasures.² First, to prevent leakage of mining-solution data, it introduced encryption for solution messages circulating on its *Computor* network. Initially, Qubic applied a simple XOR-based scheme. Because the messages contained fixed or readily inferable fields, we infer that the key could be recovered through known-plaintext analysis. Community observers also reported recovering the key. Qubic then changed its encryption method and keys multiple times, rotated keys regularly, and adjusted message-routing paths, making real-time observation increasingly difficult. These measures reduced the community's access to solution data, although the open *Computor*-network architecture continued to expose some activity to external observers. Over time, Qubic's network appeared to shift toward a more controlled and centralized configuration, with tighter control over task dissemination and increasing reliance on a small set of dispatching points.

As a more fundamental countermeasure, Qubic began withholding transactions from block templates shared on its network. The missing transactions were revealed only when Qubic later published or relayed the block, preventing observers from reconstructing the complete Monero block in real time. Once the missing transactions became available, community observers reconstructed past blocks and relayed them for retrospective verification. Because this reconstruction occurred only after disclosure, it did not provide a timely mechanism for influencing chain selection.

8.3 Operational impact and inference limits

This sequence shows that Qubic's operation was shaped by more than hashrate dynamics. The community's relay efforts were not part of a coordinated Monero protocol response, so their direct effect on chain selection or Qubic's realized rewards cannot be established. Qubic responded with encryption, routing changes, and withheld transactions. These countermeasures progressively reduced the observability of its later activity.

Observed orphan lengths and release patterns may therefore reflect a mixture of Qubic's intended strategy, network propagation, monitoring pressure, and Qubic's own countermeasures. Our analysis describes the behavior visible in the data rather than reconstructing Qubic's exact internal strategy. The reference strategies therefore serve as benchmarks for interpreting release behavior that changed over time, not as exact descriptions of individual forks.

9 Discussion

Economic interpretation

Qubic's campaign may not have been motivated solely by mining revenue. In the Goldfinger model, an attacker may benefit by undermining confidence in the target cryptocurrency [7]. Qubic's promotional framing and token-linked reward structure suggest incentives beyond Monero block rewards [14, 15]. However, daily CoinGecko prices do not indicate a lasting effect on Monero. From August 1 to October 17, XMR ranged from \$235.58 to \$343.44 and

² The operational details in this subsection are based primarily on personal communication with Monero community observers.

ended at \$293.15, 1.0% below its initial price. QUBIC ranged from USD 1.38×10^{-6} to USD 3.27×10^{-6} and ended at USD 1.47×10^{-6} , 43.2% below its initial price. Price data alone cannot determine whether the campaign produced broader benefits. The attention it brought to Qubic may itself have provided promotional value beyond mining rewards.

Mitigation implications

Freshness-aware chain-selection rules, including Publish-or-Perish-style mechanisms discussed after the campaign, could reduce the value of late withheld blocks [5, 18, 23, 21]. Their effectiveness depends on assumptions about timing and propagation. Detective mining could use information exposed by a public selfish mining pool to mine on its leading private branch [19, 8]. In practice, transaction withholding creates operational risks, and intentionally extending the attacker's branch raises social concerns. Both responses address specific tactics, while systems with modest and concentrated hash power remain exposed because of limits in decentralization, propagation, and observability.

10 Conclusion

Qubic's campaign neither sustained majority control nor consistently followed a textbook selfish mining strategy. It increased orphaning and reorganization depth. Nevertheless, across the identified periods and subsequent gaps, Qubic remained 4.0% below the target-rate honest mining baseline despite occasional tie-breaking advantages and later DAA spillovers. Community monitoring and Qubic's countermeasures further show that real-world campaigns evolve with changing observability and operational responses. Evaluating such campaigns requires considering their on-chain effects, underlying incentives, public claims, and ecosystem responses.

References

- 1 Christian Decker and Roger Wattenhofer. Information propagation in the Bitcoin network. In *13th IEEE International Conference on Peer-to-Peer Computing (P2P)*, pages 1–10. IEEE, September 2013. doi:10.1109/P2P.2013.6688704.
- 2 Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security*, pages 436–454. Springer, 2014. doi:10.1007/978-3-662-45472-5_28.
- 3 Julius Fechner, Balakrishnan Chandrasekaran, and Marc X. Makkes. Calibrating the performance and security of blockchains via information propagation delays: revisiting an old approach with a new perspective. In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing (SAC '22)*, pages 282–289. ACM, 2022. doi:10.1145/3477314.3507003.
- 4 Chen Feng and Jianyu Niu. Selfish mining in ethereum. In *IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 1306–1316. IEEE, 2019. doi:10.1109/ICDCS.2019.00131.
- 5 Ethan Heilman. One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner (poster abstract). In *Financial Cryptography and Data Security*, pages 161–162. Springer, 2014. doi:10.1007/978-3-662-44774-1_12.
- 6 Dragos I. Ilie, Sam M. Werner, Iain Stewart, and William J. Knottenbelt. Unstable throughput: When the difficulty algorithm breaks. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–5. IEEE, 2021. doi:10.1109/ICBC51069.2021.9461086.
- 7 Joshua A. Kroll, Ian C. Davey, and Edward W. Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *Workshop on the Economics of Information Security*, 2013. URL: <https://econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf>.

- 8 Suhyeon Lee and Seungjoo Kim. Rethinking selfish mining under pooled mining. *ICT Express*, 9(3):356–361, 2023. doi:10.1016/j.ictex.2022.03.003.
- 9 Sheng-Nan Li, Carlo Campajola, and Claudio J. Tessone. Statistical detection of selfish mining in proof-of-work blockchain systems. *Scientific Reports*, 14(1):6251, 2024. doi:10.1038/s41598-024-55348-3.
- 10 Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 305–320. IEEE, 2016. doi:10.1109/EUROSP.2016.32.
- 11 Kevin Alarcón Negy, Peter R. Rizun, and Emin Gün Sirer. Selfish mining re-examined. In Joseph Bonneau and Nadia Heninger, editors, *Financial Cryptography and Data Security*, pages 61–78, Cham, 2020. Springer International Publishing. doi:10.1007/978-3-030-51280-4_5.
- 12 Rafael Pass and Elaine Shi. FruitChains: A fair blockchain. In *Proceedings of the ACM Symposium on Principles of Distributed Computing*, pages 315–324. ACM, 2017. doi:10.1145/3087801.3087809.
- 13 Qubic Docs. Node types in the qubic network. URL: <https://docs.qubic.org/learn/nodes/>.
- 14 retrodrive. Epoch 172 recap - the monero experiment. <https://qubic.org/blog-detail/epoch-172-recap-the-monero-experiment>, August 2025. Accessed: 2025-10-25.
- 15 retrodrive. Qubic performs 51% monero network takeover demonstration. <https://qubic.org/blog-detail/historic-takeover-complete-qubic-miners-now-secure-monero-network>, August 2025. Accessed: 2025-10-25.
- 16 Ayelet Sapirshstein, Yonatan Sompolinsky, and Aviv Zohar. Optimal selfish mining strategies in Bitcoin. In *Financial Cryptography and Data Security*, pages 515–532. Springer, 2017. doi:10.1007/978-3-662-54970-4_30.
- 17 Ruisheng Shi, Zhiyuan Peng, Lina Lan, Yulian Ge, Peng Liu, Qin Wang, and Juan Wang. Eclipse attacks on monero’s peer-to-peer network. In *Network and Distributed System Security Symposium (NDSS 2025)*, 2025. doi:10.14722/ndss.2025.240095.
- 18 Siamak Solat and Maria Potop-Butucaru. Brief announcement: ZeroBlock: Timestamp-free prevention of block-withholding attack in Bitcoin. In *Stabilization, Safety, and Security of Distributed Systems*, pages 356–360. Springer, 2017. doi:10.1007/978-3-319-69084-1_25.
- 19 Riccardo Spagni. (github issue #140) implement detective mining (pool software change, no protocol change required). <https://github.com/monero-project/research-lab/issues/140>, August 2025. Accessed: 2025-10-25.
- 20 Pawel Szalachowski, Daniël Reijbergen, Ivan Homoliak, and Siwei Sun. StrongChain: Transparent and collaborative Proof-of-Work consensus. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 819–836. USENIX Association, 2019. URL: <https://www.usenix.org/conference/usenixsecurity19/presentation/szalachowski>.
- 21 tevador. (github issue #144) selfish mining mitigations (publish or perish). <https://github.com/monero-project/research-lab/issues/144>, August 2025. Accessed: 2025-10-25.
- 22 Dimaz Ankaa Wijaya, Joseph K. Liu, Ron Steinfeld, and Dongxi Liu. Transparency or anonymity leak: Monero mining pools data publication. In *Information Security and Privacy (ACISP 2021)*, volume 13083 of *Lecture Notes in Computer Science*, pages 433–450. Springer, 2021. doi:10.1007/978-3-030-90567-5_22.
- 23 Ren Zhang and Bart Preneel. Publish or perish: A backward-compatible defense against selfish mining in Bitcoin. In *Topics in Cryptology – CT-RSA 2017*, pages 277–292. Springer, 2017. doi:10.1007/978-3-319-52153-4_16.
- 24 Roi Bar Zur, Ittay Eyal, and Aviv Tamar. Efficient MDP analysis for selfish-mining in blockchains. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT)*, pages 113–131. ACM, 2020. doi:10.1145/3419614.3423264.