

Forum:[Hack Forums](#)

Thread: [Qubic attack on XMR monero: No 51% attack has happened](#)

Rsynced - August 17, 2025, 3:04 pm

<https://riat.at/qubic-attack-on-xmr-monero-no-51-attack-proven/>

Quote:Qubic attack on XMR monero: No 51% attack has happened
Aug 17, 2025

—

by parasew

in Blog

Based on the numbers at the time (2.6 GH/s peak vs ~6.71 peak GH/s total Monero network), Qubic's actual share was nowhere near majority

If factoring in their selfish mining strategy, their best so far was around 28%

Hashpower is self-reported, as demonstrated by fastpool and visible through the delta of network hashrate and pool reported hashrate

Multiple outlets amplified Qubic's press/PR without independent verification; independent researchers and data sources dispute the ">51%" narrative.

Reorgs != proof of sustained 51% control and 6 blocks is far from the 10-11 blocks needed for double spends.

Potential evidence for XMR price suppression and similarities to problems outlined in the Monerun. Verifiable Data

We have proof that Qubic has misrepresented their own hashrate, and have posted misleading numbers of the total network hashrate in their post¹ about their alleged "51% takeover" on the Monero network. Sadly a lot of online blogs and self-proclaimed "journalists" have re-posted the numbers without doing their own diligence. The information of recent posts by Coindesk² and Cointelegraph just echoed original marketing information sent out by Qubic. The Defiant³ at least have reached out to exchanges, and to developers, which has provided a more nuanced view of the situation.

In a writeup titled "Reaction to Coindesk's poorly researched article about an alleged 51% attack on the Monero Network" we (RIAT) already discussed why the original article of Coindesk did just echo wrong and partial information. It is important to precisely look at verifiable data – in order not to fall for this orchestrated media stunt by Qubic, a small actor that has economic incentive to push their own coin and interests.

The reported numbers have been already debunked by theblock.co⁴, BitMEX Research⁵, Shai Wyborski from Kaspas⁶, and by the Monero community⁷.

Current hashrates can be observed by looking at mining pool stats (for example [miningpoolstats.stream](#)). The numbers of the network hashrate can be calculated from the difficulty – but the pool hashrate numbers are reported from the individual pools. The pool hashrate can easily be manipulated, as was already demonstrated by fastpool, and has been discussed by tuxsudo and other members of Monero community. Look at the total network hashrate and compare it to the reported hashrate. There is a visible difference! The many solo miners (and botnets) are not even counted in the sum of pool hashrates. This means the actual network hashrate is likely higher

than what's reflected on pool stats sites.

We urge any news media outlet to not re-publish marketing data without first validating it. The data from Qubic could have been validated by demanding they published their view key. This would be the only way to provably verify their claim of controlling over 51% of the Monero network's hashrate. It would provide verifiable, on-chain evidence of their mining activity and allow the community to independently confirm or debunk their numbers, without giving them the ability to spend the funds. But even if their numbers would be high, it would not qualify for a 51% attack.

There was no 51% attack

As of today (Sunday August 17) Qubic had a maximum hashpower of 2.6 Gh/S, which was self-reported by them. The (proven) Monero Network Hashrate was at 6.25 Gh/s – which places Qubic at far below 50%. This still sounds like a lot, but shows that any claims of a 51% attack are provably wrong: there was no 51% attack, and more importantly: it was very far from being a successful 51% attack.

A 51% attack is when a single entity or a group of colluding entities gains sustained control of more than 50% of the network's total hashrate on a proof-of-work (PoW) blockchain. This majority control allows the attacker to manipulate the network's consensus. While a double-spend is the most common and financially devastating outcome, a successful attack can also involve transaction censorship or a denial-of-service against the network.

Qubic had 51% of the last 100 blocks at a specific time. But this does not equal to a hashrate being 51%! It only tells us that it allows Qubic to build six blocks faster than the rest of the network by getting lucky. It does not mean a '51% attack' happened, or was successful! They would have needed much more hashpower than they have (self) reported. Researchers have estimated that they would have to have had an extra 4.25Gh/s, which would be more than double the hashrate they had at this time.

But even these 6 blocks are not a lot, which makes the claims for a "takeover" even more absurd. Monero wallets and major exchanges require a transaction to have 10 confirmations, which takes approximately 20 minutes, before the funds are considered spendable. While a chain reorganization (reorg) of a few blocks can occur due to network latency or other factors, it is not sufficient to reverse a transaction that has already received 10 confirmations. Therefore, a 6-block reorg does not prove a successful and sustained 51% attack, as it is far short of the 10-11 blocks needed to invalidate a fully confirmed transaction.

Qubic has further also used a strategy called "selfish mining". This is a malicious strategy to withhold blocks your pool has found, and then later publish them in order to "penalize" the other miners (because they have lost the time going forward on the wrong blocks). This strategy again makes it possible for Qubic to have "an appearance of higher hash-rate than they already have" (see this extensively described in the The Qubic Minority Report). Even with this strategy they only could secure 6 blocks, which sounds like a lot – but ultimately is far from being a successful demonstration.

Exchanges and price

Some researchers have voiced the theory that the ultimate goal of the FUD campaign spearheaded by Qubic is to artificially suppress the price of Monero. A potential reason is the recent price spikes in the past months, and thus a campaign like this could make the exchanges be able to stack up on their Monero cheaply.

Historical events such as the Monerun have already shown that exchanges rarely hold full reserves of XMR. If users demanded large-scale withdrawals simultaneously, many exchanges would need to purchase Monero externally to cover liabilities.

As of writing, XMR withdrawals remain disabled on most major exchanges. The decision by the Kraken cryptocurrency exchange to temporarily halt Monero deposits was a precautionary measure in response to the public claims of a potential attack. This was not a confirmation that an attack had actually occurred.

In summary, the claims of a Qubic 51% attack on the Monero network were false. The situation serves as a powerful reminder of the need for critical analysis of public data and the ongoing importance of decentralized mining to maintain the integrity of a cryptocurrency network. The Monero Project officially encourages the use of P2Pool. It's a decentralized, trustless, and permissionless peer-to-peer mining pool. It offers the frequent payouts of a traditional pool without the need to trust a centralized server. This helps to increase the robustness and decentralization of the Monero network.

"So my nintendo wii can 51% attack bitcoin? Just unsuccessfully?" (DastardlyWarthog, Reddit)

retrodrive. "Qubic Performs 51% Monero Network Takeover Demonstration | Qubic." Qubic.org, 12 Aug. 2025,

qubic.org/blog-detail/historic-takeover-complete-qubic-miners-now-secure-monero-network. Accessed 16 Aug. 2025. ?

Naga Avan-Nomayo. "Monero Faces Chain Reorganization Fears after Qubic Says It Controls 51% of Hashrate." The Block, 12 Aug. 2025, www.theblock.co/post/366535/monero-faces-chain-reorganization-fears-after-qubic-says-it-controls-51-of-hashrate. Accessed 16 Aug. 2025. ?

Wyborski, Shai. "The Qubic Minority Report | Parallel Thoughts." Gitbook.io, 16 Aug. 2025, shai-deshe.gitbook.io/parallel-thoughts/proof-of-work/the-qubic-minority-report. Accessed 16 Aug. 2025. ?

"/R/Monero." Reddit.com, 2025, www.reddit.com/r/Monero/comments/1mod130/psa_qubic_is_lying_they_dont_have_50_hash_rate/. Accessed 16 Aug. 2025. ?

Behnke, Rob. "Explained: The Monero 51% Attack (August 2025)." Halborn.com, 12 Aug. 2025, www.halborn.com/blog/post/explained-the-monero-51-percent-attack-august-2025. Accessed 16 Aug. 2025. ?

Knight, Oliver. "XMR News: Inside Qubic's Controversial 51% Takeover of the Monero Blockchain." CoinDesk, 12 Aug. 2025, [coindesk.com/business/2025/08/12/monero-s-51-attack-problem-inside-qubic-s-controversial-network-takeover](https://www.coindesk.com/business/2025/08/12/monero-s-51-attack-problem-inside-qubic-s-controversial-network-takeover). Accessed 16 Aug. 2025. <https://archive.is/wdX5c> ?

Omelchenko, Denis. "Monero Faces Network Reorg as Community Split over Qubic's Role." Thedefiant.io, The Defiant, 14 Aug. 2025, thedefiant.io/news/blockchains/monero-faces-network-reorg-community-split-over-qubic-role. Accessed 16 Aug. 2025. ?