What Is Selfish Mining?

Selfish mining is a deceitful cryptocurrency mining strategy in which one miner or a group solves a hash, opens a new block, and withholds it from the public blockchain. This action creates a fork, which is then mined to get ahead of the public blockchain.

If the group's blockchain gets ahead of the honest blockchain, it can introduce its newest block to the network. The network is geared to recognize the most recent block, so the group's fork would overwrite the original blockchain. The miners could effectively steal cryptocurrency from other users by altering the blockchain.

How Does Selfish Mining Work?

"Mining" is the process in which nodes in the blockchain's network validate and confirm transactions. Miners earn newly minted tokens in return for their computational effort. With selfish mining, the cartel obscures newly created blocks from the main chain, revealing them at a later point in time.

Selfish mining was first identified by Cornell researchers Emin Gün Sirer and Ittay Eyal in a 2013 paper.1 They proved that it was possible to earn more bitcoins by hiding newly-generated blocks from the main blockchain, creating a blockchain fork. Theoretically, the miners could introduce it to the network at the right time and alter the blockchain.

The Bitcoin and other cryptocurrency networks using the proof-of-work consensus mechanism rely on miners whose mining software discovers the solution to the randomly-generated encrypted hash number. When the hash is solved, a new block opens up on the blockchain, and the miner who solved it receives a transaction fee and a reward.

In their 2013 paper, Sirer and Eyal demonstrated that miners can increase their overall revenue share by hiding new blocks and making them available to systems within their private network. This practice speeds up the discovery process and irons out infrastructure problems related to mining, such as network latency and electricity costs.

Initially, the forked blockchain will be shorter than the public blockchain. The private chain mines new blocks within its pool and hides any newly-generated blocks. The mining process is repeated until the private blockchain reaches a block height greater than that of the public blockchain.

Selfish miners then strategically time the introduction of their new blocks to the honest blockchain such that the public blockchain joins the newly introduced chain. The public network mines the new blockchain, and the selfish miners receive the cryptocurrency rewards and transaction fees for their newly accepted blocks.

Sirer and Eyal analyzed resources wasted for both chains. They postulated that selfish miners possessed a competitive advantage over miners on the public blockchain because their rewards are comparatively greater after accounting for wasted resources.

Is Selfish Mining a Threat?

Sirer and Eyal presented compelling evidence for altering a blockchain by creating a fork and getting ahead of honest miners. They also state that rational miners, upon observing the group's profits, will join the group because they will be attracted to the increased rewards. However, other researchers disagree on the incentives, practicality, and threats posed by selfish miners and groups.

In 2017, Craig Wright demonstrated that selfish miners would not create more blocks—and thus earn more rewards—than they were already entitled to if they were honest miners.

In 2018, Jake Gober theorized that if selfish mining were more profitable than honest mining, many miners would be doing it. Jake demonstrated that while selfish mining is more profitable than honest mining, multiple selfish miners or groups on a network would create a race between the forks and reduce profitability.

Interestingly, Zhaojie Wang et al. observe in their research that as of the end of 2021, there were no known instances of a selfish mining attack in the real world.

The arguments for both sides suggest that while selfish mining attacks can happen, they may be purely academic. Another possibility is that a selfish mining attack has occurred in the past, and it hasn't been observed.

What's more likely, however, is that the majority of cryptocurrency miners have honest intentions, and the mathematical modeling is being used to push blockchain technology development.

What Is a Selfish Mining Attack?

A selfish mining attack is an deliberate alteration of a blockchain to increase rewards to one miner or a group of miners.

Is Bitcoin Dependant on Miners?

The Bitcoin network uses miners to validate block and transaction information. Without miners, verification and validation couldn't happen, and the network wouldn't function.

What Is Self Mining Bitcoin?

The community-accepted term for mining on your own is solo mining. To solo mine, you use an application specific integrated circuit (ASIC) miner or one of your devices that is capable of mining cryptocurrency to attempt to mine. Unfortunately, the computational power needed to mine Bitcoin is well outside the scope of a solo miner—unless that miner owns a large Bitcoin mining operation.