Nama : Diah Aisyah

NIM : 1103184023

Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack

a well-known attack where a selfish miner, under In this paper, we expand the mining strategy space to parameters, earn the miner more revenue. Show that the selfish mining attack is not (in general) optimal. By non-trivially composing mining attacks with network-level eclipse attacks. Best strategy, in some cases victims of an eclipse attack can blockchain technology, where miners reach consensus about a majority of the network, as measured by computational Since cryptocurrencies carry monetary value, they naturally become a valuable target of attacks.

A secure-by-design cryptocurrency, an attacker controlling is able to obtain only α fraction of the mining reward. Attacks to gain an unfair share of the mining reward. Refer to such attacks generically as mining attacks., and network-level attacks that seek to create network partitions between mining powers, referred to as the “eclipse In this paper, we take an in-depth look at the mining attack strategy space, and make several interesting revelations.

Selfish mining is not optimal for a large parameter space. We introduce a new family of alternative “stubborn mining” strategies that generalize and outperform the selfish For a large fraction of the interesting parameter space, our new strategies significantly increase the Depending on the environment parameters, stubborn mining strategies can beat selfish mining In one of our mining strategies, called trail-stubbornness, the attacker keeps mining on her private fork even if more of the public’s mining power. cases, a trail-stubborn strategy can result in 13% gains in

An attacker’s revenue is increased by non-trivial combinations of stubborn mining and network-level attacks. stubborn miner can additionally exploit network-level attacks to further increase its gains. the rest of its peers at the network-level, by controlling its of non-trivial strategies exist when combining stubborn mining with eclipse attacks. these strategies can sometimes result in 30% gains in attacker’s best strategy actually helps the eclipsed nodes,

Systematic exploration of strategy space. to systematically explore the space of strategies combining selfish-mining-style attacks with network-level eclipse her strategy based on estimated parameters including the network it can potentially eclipse and the fraction of the Although we significantly expand the strategy space considered by the selfish mining paper,

we do not claim to study the full possible strategy space. space we consider, we show dominant strategies for different that the space of viable mining strategies is complicated, and that selfish mining is not optimal in general. we show that the possibility of combining mining attacks with network-level attacks further complicate the space of Mining attacks. Mining attacks. proved certain security properties of the Bitcoin consensus protocol under highly idealized assumptions about the network propagation, and more However, it has been shown that the security of the consensus protocol can be broken when nodes are rational rather Bitcoin's reference implementation mandates that, whenever some miner produces a valid block, it distributes this to Eyal and Sirer show selfish miners can gain an unfair share of the block reward by deviating gains by maintaining a private blockchain and withholding Selfish mining works because honest miners are forced to members of a mining pool can launch a block withholding At the network layer, each Bitcoin demonstrated a network-level eclipse attack where a single node monopolizes all possible connections to a victim and eclipses it from the network. achieve eclipse attacks on the Bitcoin network. reduce the feasibility of carrying out an eclipse attack by a in launching eclipsing attacks. eclipsed node to profit and analyze the gains that can be Knowledge of the Bitcoin network can further help a network-level attacker. network-level attacker. For example, Coinscope proposes non-trivial techniques to map out the Bitcoin network knowledge would enable an attacker to make targeted attacks to eclipse mining entities. that selfish mining is suboptimal.

They define a broad strategy space and use a combination of analytic bounds and numeric solvers to compute approximately-optimal strategies Their strategy space is a generalization of our stubborn mining strategies; however, they do not consider how to compose mining attacks with eclipse attacks.

We begin by defining the basic model of Bitcoin mining extend the model to include eclipse attacks as well. the attacker's) block when Alice and Bob have released We represent the attacker and the rest of the network only in in mining pools where they join efforts in solving computational puzzles and share block rewards. pools account for 75% of the network. Mining pools the Bitcoin network using the timestamps and proofs-ofwork published in the blockchain itself. hashpower among mining pools and other entities can be inferred using several heuristics the largest mining pool was when the attacker controls over 50% of the hashpower, the of the mining reward, and can revert or delay transactions). compromise of a large mining pool the prior known selfish mining In a nutshell, all known deviant mining strategies work by selectively withholding blocks mined by the attacker always loses the race

between public miners i to j. attacker, causing the rest of the network to waste its hashpower on redundant blocks.