Bitcoin's security relied on the assumption that a majority of the network, as measured by computational resources, would honestly run the default reference client. Among the most well-known are "selfish-mining"-style attacks that exploit weaknesses in the distributed consensus protocol, and network-level attacks that seek to create network partitions between mining powers, referred to as the "eclipse attack" . Although we significantly expand the strategy space considered by the selfish mining paper, we do not claim to study the full possible strategy space. Under the strategy space we consider, we show dominant strategies for different regions of the parameter space.

However, we do not preclude the possibility of other strategies outside our strategy space that perform better. First, we show that the space of viable mining strategies is complicated, and that selfish mining is not optimal in general. Second, we show that the possibility of combining mining attacks with network-level attacks further complicate the space of possible strategies. A notable challenge that we pose is the task of designing a consensus protocol whose security is formally founded under rationality assumptions rather than honest majority – the latter was adopted by Garay et al.

in their proof of the Bitcoin backbone protocol . The findings of our paper demonstrate that achieving this could be difficult – especially if one also wishes to take into account realistic models of network formation and propagation. Bitcoin's re ference implementation mandates that, whenever some miner produces a valid block, it distributes this to the rest of the network. Eyal and Sirer show selfish miners can gain an unfair share of the block reward by deviating from the reference client.

Specifically, a miner with more than 33%computational power can attain disproportionate gains by maintaining a private blockchain and withholding blocks that have been mined. This forces honest miners to perform wasted computations on a stale public branch. Selfish mining works because honest miners are forced to spend their computation cycles on blocks that are destined to not be on the public chain. The peerto-peer connections between these nodes can be inferred through various techniques.

This way the eclipsing node can filter the eclipsed node's view of the blockchain. Their paper describes elaborate techniques to achieve eclipse attacks on the Bitcoin network. Although a few proposed counter-measures have been implemented that reduce the feasibility of carrying out an eclipse attack by a single node, multiple nodes can collude and still succeed in eclipsing – in particular, in Section 7, we argue that it may in fact be incentive compatible for selfish players to collude in launching eclipsing attacks. Furthermore, we provide a basis for understanding how an attacker could exploit an eclipsed node to profit and analyze the gains that can be achieved.

Knowledge of the Bitcoin network can further help a network-level attacker. For example, Coinscope proposes non-trivial techniques to map out the Bitcoin network topology as well as the hashpower of various nodes. Such knowledge would enable an attacker to make targeted attacks to eclipse mining entities. Concurrent and independent work.

Concurrent to and independent of our work, Sapirshtein et al. also observe 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 from

this space. One way is by observing the stale block rate – a stale block is one that has valid transactions and proof-of-work, but is ultimately excluded from the main chain .

4 Stale blocks occur by chance in ordinary operation, even when every miner is honest. When all miners are honest, the relative rate of stale blocks is the same for all miners. Stimulated by the selfish mining attack's publication, the Bitcoin community has deployed various services to monitor for evidence of the attack occurring. Despite this widespread awareness, the selfish mining attack has not been observed in practice.

Recall that selfish mining has not been shown to be an equilibrium strategy – in fact our models assume that the rest of the network is compliant with the reference protocol. In reality, the members of the Bitcoin network may react and change their strategy or upgrade the protocol itself . Another explanation is that potential selfish miners may consider it risky to get caught. Since it takes two weeks for the Bitcoin difficulty to adjust, a stubborn mining attack must be sustained this long before any extra revenue comes in.

A "brief" stubborn mining attack, or one that is detected before the difficulty adjusts, would not be profitable. The governance structure of the Bitcoin network is uncertain , so adaptive responses may be difficult to coordinate. Eyal has recently shown that scenarios where one pool attacks another lead to an equilibrium where pools have limited size, suggesting that this property may be self-enforcing. Eclipse attacks can benefit the victim.

As it turns out, the "victim" of an eclipse attack can sometimes even profit from the attack, even when the attacker uses the optimal strategy . In such cases, Alice and Lucy effectively have a mutually beneficial relationship and share their increased revenue relative to Bob.