

Intuitively, the reason why “selfish mining” fails is that even if an adversary tries to “erase” some block mined by an honest player (which contains some honest fruits), by the chain growth and chain quality properties of the underlying blockchain, eventually an honest player will mine a new block which is stable and this honest player will include the fruit in it—in fact, the time before such an “honest block” arrives is short enough for the fruit to still be “recent” at the time of the honest block arriving.