Intuitively, the reason why we require fruits to be recent is to prevent a different kind of attack: without it, an attacker could *withhold fruits*, and suddenly release lots of them at the same time, thereby creating an very high fraction of adversarial fruit in some segment of the (fruit) chain. By requiring the fruits to be recent, we prevent the adversary from squirreling away (too many of) its fruits: since the underlying blockchain has a guaranteed chain growth, we can upperbound the extra amount of time the attacker can withold fruits and thus upperbound the number of extra fruits it can release in any window.