

BUG REPORT

Missing check for total staking limit per epoch



Mundus

04 Dec 2025

Bug Report: QVE-2025-0009

Bug ID	QVE-2025-0009
Finder	<i>Mundus team</i>
Date (reported)	<i>04.12.2025</i>
Status	<i>Found bug</i>
Bug Description	
URL	https://github.com/qubic/core/blob/v1.269.0/src/contracts/QBond.h#L305-L386
Summary	QBond uses an address to stake/lock on QEarn QEarn limits 1T qu staking per address per epoch QBond performs staking on behalf of users via QEarn. Currently, the staking procedure lacks a check for the total staking limit per address per epoch.
Consequences	Stakers incur a loss of accrued rewards. In the worst-case scenario, this results in a partial loss of the staked principal.
Solution	Check total amount staking before submitting to QEarn; or handle response from QEarn after calling lock() api.
Priority	Medium
Severity	Medium

Additional Notes, step-by-step Description:

- For an epoch, in which total amount staking in QBond exceeds the limitation of QEarn staking cap (1T qu) per address; then total amount actually locked on QEarn $\leq 1T$ qu (**real_locked_amount**). When maturity:
 - QEarn will send back to QBond amount [_qearnIncomeAmount](#) = rewards + **real_locked_amount**
 - QBond still be recording total: **totalStaked * QBOND_MBOND_PRICE** $> 1T$ qu
 - **totalReward** = [_qearnIncomeAmount](#) - **totalStaked * QBOND_MBOND_PRICE**
- So, the [totalReward](#) can be negative as computation [here](#), leading to users receiving less than the staked principal as [here](#).