Forbidden periods for slashed bakers

To keep bakers honest, Tezos doesn't allow them to overuse their baking rights by baking or attesting twice when it's their turn to do so, referred to in general as "double-signing." Bakers who double-sign are penalized by "slashing" (losing part of their security deposit) and by being prevented from baking or attesting for a certain amount of time. Slashing is a rarely used but necessary feature to keep the chain honest.

People worry about being slashed for double-signing, and Tezos-related sites warn about it for transparency, but in reality, double-signing is extremely rare. The main cause of double-signing is having two baking daemons running at the same time, such as if a baker is migrating from one computer to another and leaves the old baking daemon running for too long.

However, a baker did get slashed for double-signing and the result was confusing even to many people who are intimately aware of how the Tezos consensus mechanism works. This document is a detailed explanation of what happened when this baker was slashed.

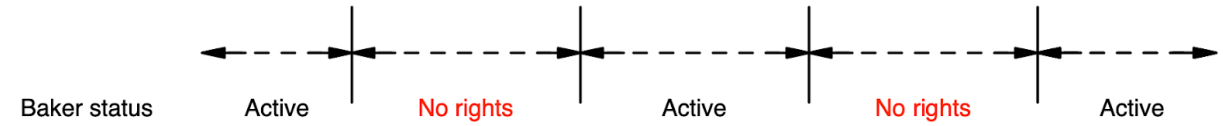
> Note: the explanation here is based on activity in the current Rio protocol. Behaviors, constants, and time periods may change in future protocol upgrades.

The baker in question made an honest mistake of migrating their setup to a new system while leaving the baking daemon running on the old system. When it was the baker's turn to bake and attest, both daemons did so, and an accuser immediately denounced them for double-signing.

Fortunately, thanks to adaptive slashing, the penalty for a first offense is very small – a fraction of a percent of the baker's total stake. This light penalty reflects the fact that double-signing is almost certainly a mistake and not an attempt to increase baking rewards, because the potential gain is very small.

There's another effect of slashing involved: a baker that double-signs is prevented from baking or attesting for a certain number of cycles, known as the forbidden period. This period is in part penalty to the baker, and it does have a financial effect because they miss out on rewards, but more importantly, it prevents them from suffering larger penalties if they have a faulty setup and double-sign repeatedly. The forbidden period gives them time to find and shut down the second baking daemon before it double-signs again.

However, something surprising happened after this last instance of slashing: the baker was locked out for two non-contiguous periods of time. Their baking rights looked like this:



Why did the slashed baker have no attestation rights for two separate periods of time? The answer has to do with how rights are calculated. Calculating bakers' rights is complicated, but for the purposes of this situation, these are the relevant details:

- A baker's rights are relative to their baking power, which is the amount that they have staked plus the amount that delegators have staked to them.
- Baking rights are calculated a certain number of cycles in advance, determined by the CONSENSUS_RIGHTS_DELAY protocol constant, which is currently 2 cycles. For example, a baker's rights for cycle 10 are calculated at the end of cycle 7 based on their baking power at the end of cycle 7.
- Bakers cannot bake if the current amount they have staked is less than the amount that the protocol calculated their rights on. Normally this isn't a problem, because staked funds are locked for CONSENSUS_RIGHTS_DELAY cycles and therefore bakers and stakers can't withdraw funds that were used to calculate rights for a future cycle. However, slashing penalties decrease baking power immediately and therefore the current baking power might not match the baking power that was calculated two cycles ago.
- When a baker is denounced for double-signing, they are forbidden from signing for the rest of the current cycle and for one more full cycle.

Based on these details, can you calculate how many cycles a slashed baker loses rights for? Don't feel bad if you can't; it took engineers at TriliTech and Nomadic Labs a week of research to feel confident about what had happened here. Here's a cycle-by-cycle scenario of what happened, in general terms:

Cycle 10: A baker double signs. The baker is immediately denounced for double-signing. As a result, the baker is forbidden from signing for the remainder of the cycle.

Cycle 11: The baker is still prevented from signing as part of the forbidden period. At the end of this cycle, the baker is slashed, which reduces their stake.

Cycle 12: The forbidden period is over at the beginning of this cycle. However, the baker is still forbidden from signing because their rights for this cycle were calculated based on their stake at the end of cycle 9. Because the slashing penalty reduced their stake, the baker's current stake is less than the stake that was used to calculate their rights for this cycle. Thus the baker is prevented from signing during this cycle.

Cycle 13: Similar to the previous cycle, the baker has no rights because their current stake is lower than the stake that was used to calculate their rights for this cycle.

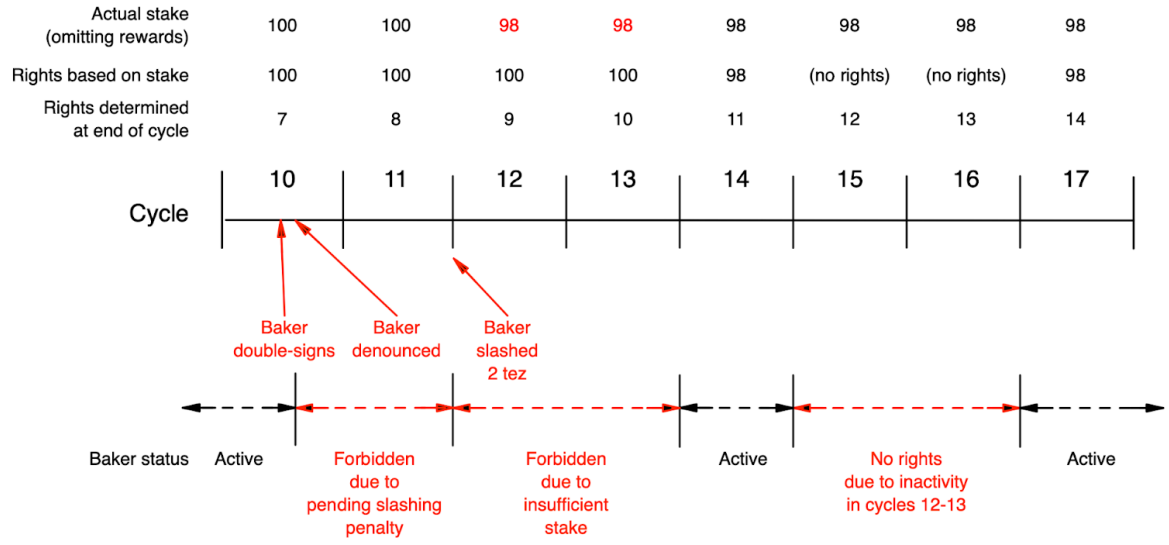
Cycle 14: The baker becomes active again because their current stake matches the stake that was used to calculate rights for this cycle at the end of cycle 11, which includes the deduction from the slashing penalty.

Cycle 15: The baker has no rights because they were forbidden in cycle 12.

Cycle 16: Similar to the previous cycle, the baker has no rights because they were forbidden in cycle 13.

Cycle 17: The baker becomes active again with rights based on their stake at the end of cycle 14 and they continue to be active.

In this way, being slashed can stop a baker from baking and attesting for five full cycles plus part of the cycle in which they were denounced. Here's a diagram that shows what happened, with hypothetical amounts for the stake and slashing penalty:



One interesting thing we learned during this investigation was that bakers can reduce the number of cycles that they miss out on baking in. Read on to see how.

Being forbidden from signing for two full cycles (11 and 12 in the example above) is unavoidable: the first is due to the slashing penalty and the second is due to having insufficient stake. But the baker can avoid being forbidden in the next cycle (13) by staking more tez before that cycle starts to make up for the slashing penalty. Then they have sufficient stake in cycle 13 to bake. How many cycles does the baker miss out on now?

Here's a scenario that includes the baker topping up their stake to replace the slashing penalty:

Cycle 10: A baker double signs. The baker is immediately denounced for double-signing. As a result, the baker is forbidden from signing for the remainder of the cycle.

Cycle 11: The baker is still forbidden as part of the penalty. At the end of this cycle, the baker is slashed, which reduces its stake.

Cycle 12: The penalty for double-signing is over at the beginning of this cycle. However, the baker is still forbidden because their rights for this cycle were calculated based on their stake at the end of cycle 10.

Unlike the previous scenario, the baker stakes more tez in cycle 12 to make up for the slashed amount before the end of cycle 12. (They could not have done so any earlier than cycle 12 because being forbidden due to double-signing prevents them from staking.)

Cycle 13: Unlike the previous scenario, the baker has baking rights because the tez they added in cycle 12 makes up for the slashed tez. Because they added tez, their current stake is at least as large as the stake that their rights were calculated on at the end of cycle 10.

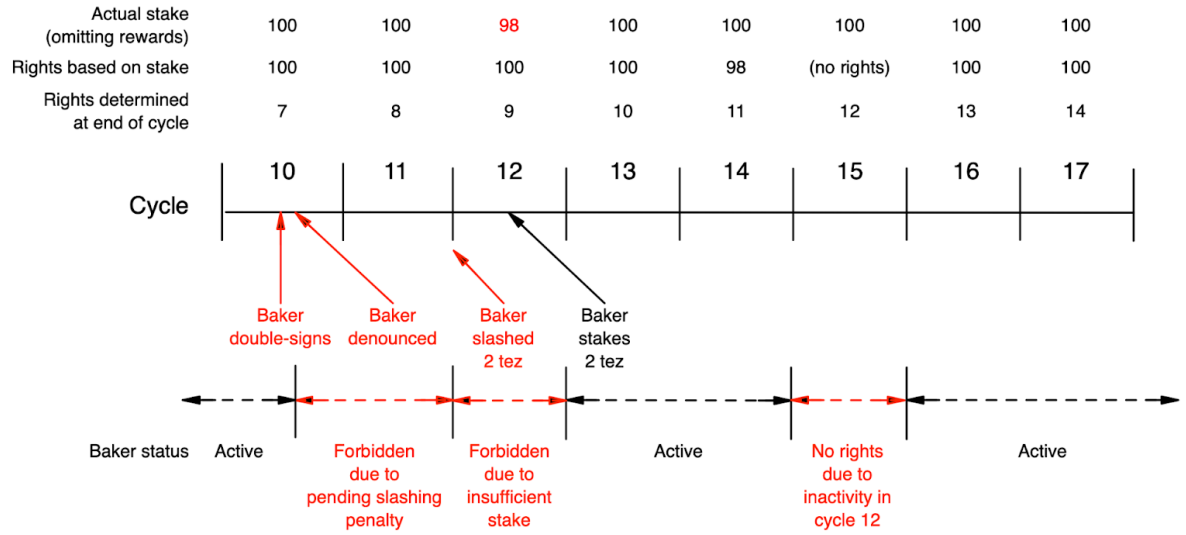
Cycle 14: The baker becomes active again because its current stake matches the stake that was used to calculate rights for this cycle at the end of cycle 11, which includes the deduction from the slashing penalty.

Cycle 15: The baker has no rights because they were forbidden in cycle 12.

Cycle 16: The baker becomes active again with rights based on their stake at the end of cycle 13.

Cycle 17: The baker is active and continues to be active.

In this scenario, adding tez to replace the slashing penalty reduced the number of cycles that the baker was inactive by two. Here's a diagram of this new scenario:



Bakers should check their baking setups and migrations to avoid double signing. For questions, contact the Tezos or baking Discord servers.

Thanks to Germán Delbianco, who helped sort out these technical details to explain what happened.