



Incident Report

Time: 6am GMT, Friday Mar 12, 2021

Tokens affected: BDP seed pools only. bALPHA and liquidity pools unaffected

Summary: An unexpected behavior/bug in the reward mechanism in our smart contract prevented users from unstaking from the seed pools and claiming their BDP rewards once mining was completed. To resolve, the team deployed an API that used a snapshot of the blockchain and allowed users to use the emergency withdrawal function to unstake their funds from the seed pools. Users could not claim their BDP rewards. The result is that approximately 5.7 million BDP tokens (over 7% of the total supply) are effectively burned. Users who farmed BDP will be airdropped their reward tokens in the coming days.

What happened:

~6am GMT: On Friday, Mar 12, 2021, mining for the initial circulating supply of BDP tokens was completed, with a total of 24 million BDP distributed among the seed pools. At the end of the mining period, users who had staked assets in seed pools expected to reclaim their assets plus the BDP tokens they had farmed.

The issue was caused by a bug in the BDPToken contract that caused BDP rewards to not be claimable by anybody after the rewards period ended.

The root cause of the issue is the following function in the BDPToken contract:

```
function mint(address _to, uint256 _amount) public {
    require(msg.sender == BDPMaster, "BDPToken: only master farmer can mint");
    require(seedPoolAmount > 0, "BDPToken: cannotmint for pool");
    require(seedPoolAmount >= _amount, "BDPToken:amount greater than limitation");
    seedPoolAmount = seedPoolAmount.sub(_amount);
    _mint(_to, _amount);
}
```

Specifically this line:

```
require(seedPoolAmount > 0, "BDPToken: cannotmint for pool");
```

Intended to prevent minting of additional BDP tokens at the end of the initial rewards distribution period, the logic checks if the amount of BDP to be distributed is *greater than 0* instead of *greater than or equal to 0*. Reward distribution period end returned `seedPoolAmount == 0`, causing the mint function to always fail. Since no other BDP tokens will be distributed in this manner and `seedPoolAmount == 0` will always be true, the mint function can never be called again. This effectively burned the ~5.7 million BDP tokens that were not claimed prior to the end of the reward distribution period.

~6:30am GMT: Users begin to report that they are not able to unstake from their seed pools

~7:30am GMT: BDP advises users that their funds are safe, and that while the “emergency withdrawal” function is available, to hold off from unstaking until we have reviewed available options.

~8:00am GMT: After investigation of the contract with partners, BDP advises users that we will be able to use a snapshot to deliver farmed rewards to respective users via airdrop, and that they can safely use the “emergency withdrawal” function written into the smart contract to extract their staked funds from seed pools.

~10:00am GMT: BDP verifies that the minting process for bALPHA works differently than the minting process for BDP due to the changing distribution rates. bALPHA rewards will be claimable after the end of rewards distribution.

What are we doing to make this right:

1. In the coming days, we will use a blockchain snapshot taken at the end of the initial rewards distribution period to airdrop the community their correct BDP reward.
2. We have confirmed that this bug does not affect any other smart contracts in our protocol and reviewed our smart contracts for issues.

What are we doing to prevent this in the future:

1. Ensure that this part of the contract will never be used again
2. Reviewing and updating our testing protocols to ensure that key elements of our deployment timeline are fully challenged and stress-tested.
3. Growing our team to allocate additional resources to development, review of code infrastructure, and testing.

We thank BDP supporters for their patience and continued confidence in us, our mission and our vision.



-The BDP Team