#Description: vault inflation mechanism

Inflation Attack

ERC 2646 basic calculation

deposit()

```
*/
function deposit(uint _amount) public {
    uint256 _pool = balance();
    uint256 _before = token.balanceOf(address(this));
    token.safeTransferFrom(msg.sender, address(this), _amount);
    uint256 _after = token.balanceOf(address(this));
    _amount = _after.sub(_before); // Additional check for deflationary tokens
    uint256 shares = 0;
    if (totalSupply() == 0) {
      shares = _amount;
    } else {
      shares = (_amount.mul(totalSupply())).div(_pool);
    }
    _mint(msg.sender, shares);

    earn();
}
```

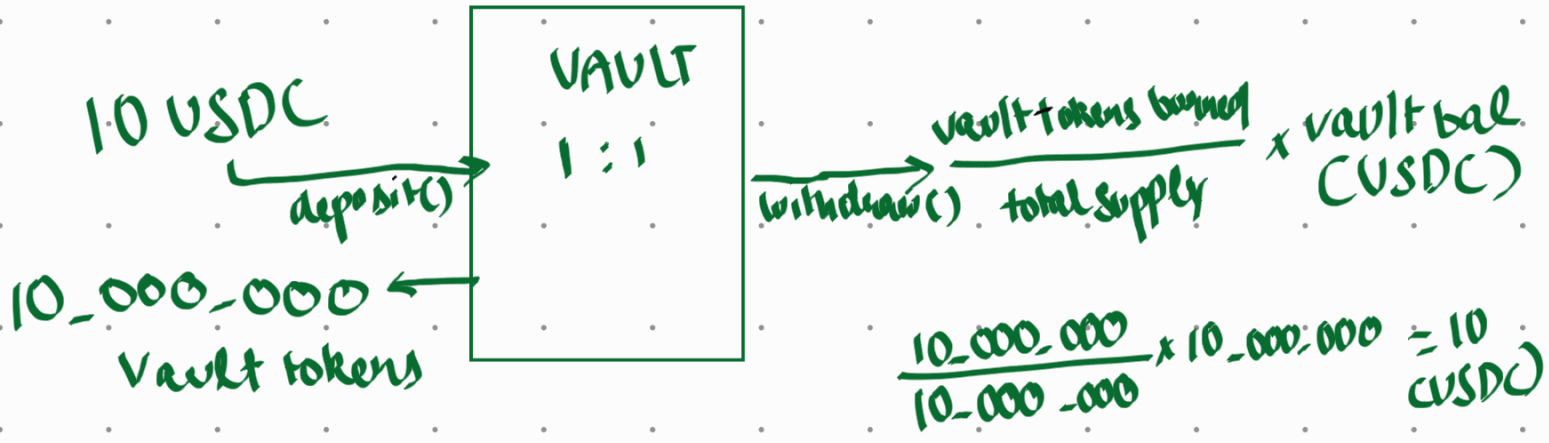
withdraw()

```
*/
function withdraw(uint256 _shares) public {
    uint256 r = (balance().mul(_shares)).div(totalSupply());
    _burn(msg.sender, _shares);

    uint b = token.balanceOf(address(this));
    if (b < r) {
        uint _withdraw = r.sub(b);
        IStrategy(strategy).withdraw(_withdraw);
        uint _after = token.balanceOf(address(this));
        uint _diff = _after.sub(b);
        if (_diff < _withdraw) {
            r = b.add(_diff);
        }
    }
```

1 USDC = 1_000_000

For 1st deposit:



Attack

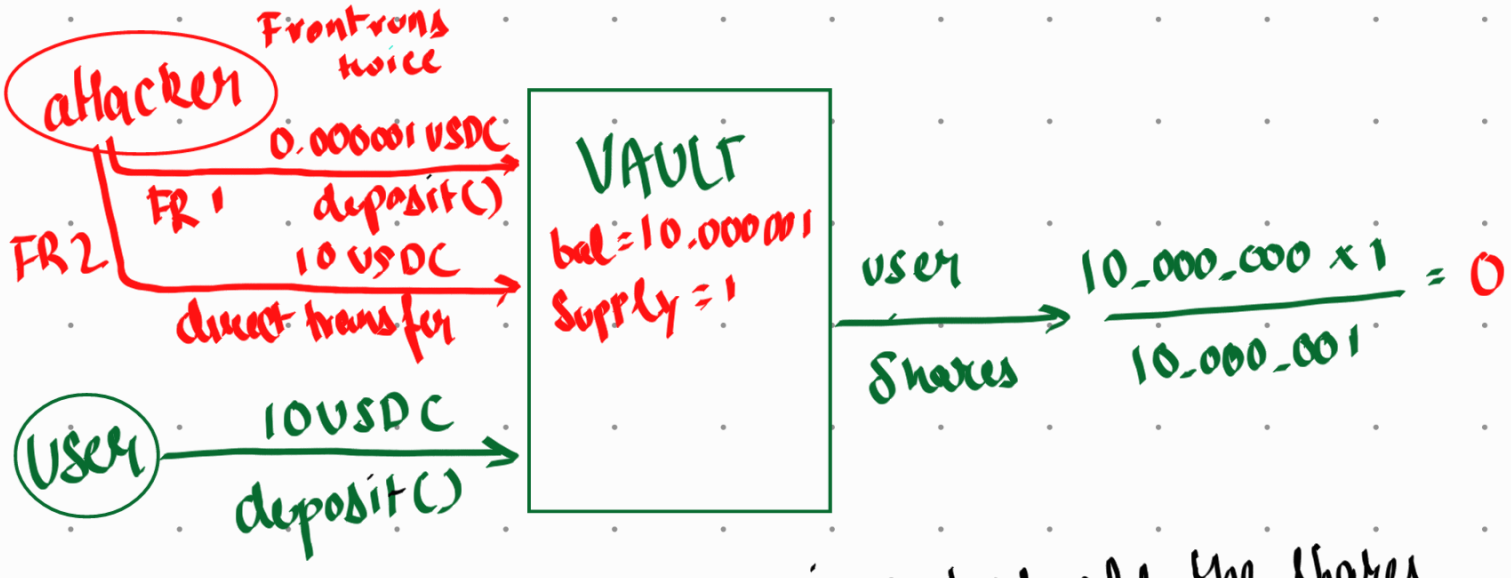
If an attacker is somehow able to increase vault balance without increasing

'total supply' then

$$\text{amount deposited} \times \frac{\text{total supply}}{\text{contract balance}}$$

for 10 USDC deposited.

$$1\_000\_000 \times \frac{1}{1\_000\_001} = 0$$



Attacker at this time has all the shares and can run away with vault balance.

Mitigation (Openzeppelin):

- Virtual Offset
  - more decimals in total supply than balance
- Use virtual shares to virtual balance on first deposit to make the attack non profitable

deposit to

Canonical

$$\text{amount deposited} \times \frac{\text{total supply}}{\text{balance}}$$

Openzeplin

$$\text{amount deposited} \times \frac{\text{total supply} + 1}{\text{balance} + 1}$$

$$10\_000\_000 \times \frac{2}{10\_000\_001} = 1$$

Attacker 10_000_001 = 1VT

User 10_000_000 = 1VT

Scenario:

Attacker	20_000_001	1 VT
User	10_000_000	0 VT

$$\frac{\text{VT Burned}}{1 + \text{Total Supply}} \times \text{Vault balance}$$

$$\frac{1}{2} \times 30\_000\_001 = 15\_000\_000$$

$15 < 20$ attacker lost money