DeFi Protocol Compound Suffers a $90m Reverse Rugpull After “1 Letter Bug”

Posted on Oct 12, 2021 | [BLOG](https://www.cybavo.com/blog/)



DeFi interest protocol [Compound Finance](https://compound.finance/) has given its users an unintended early Christmas to the tune of $90 million, all thanks to a single letter bug in its code that caused it to issue more COMP tokens than it should.

The incident, which shocked the network and the cryptoverse at large due to Compound’s industry stature and the size of the loss, has seen users receive more COMP tokens as a result of the bug. The decentralized staking protocol is looking to recover the tokens by appealing to recipients’ conscience, issuing a taxation threat, and incentivized compliances.

Some developers and analysts are calling the COMP mistake the biggest-ever fund loss in a smart contract incident, with as much as [$162 million “up for grabs”](https://www.cnbc.com/2021/10/03/162-million-up-for-grabs-after-bug-in-defi-protocol-compound-.html), according to its founder.

**What is Compound Finance?**

Compound is an algorithmic, autonomous interest rate protocol built for developers that unlocks a large selection of open financial applications. It made headlines in June 2020 when its pioneering governance token COMP skyrocketed in value and created a slew of copycat governance tokens.

**Compound founder threatens community with “doxxing”**

Q4 started off with fireworks for the DeFi space, after this 1 October tweet from Compound chief Robert Leshner:

<https://twitter.com/rleshner/status/1443730726751506432>

After community outcry over the veiled threats in his tweet, including the big crypto taboo of  [“doxxing](https://hackernoon.com/doxxing-the-ultimate-crypto-taboo-3c19ce278d72)” (the practice of revealing the real identity behind a pseudonymous crypto address), Leshner was quick to walk back the tweet, admitting it was “bone-headed”.

Then, it was time to dissect what went wrong.

**What went wrong with Compound’s $90 million distribution?**

Compound Finance was to implement [Proposal 062](https://compound.finance/governance/proposals/62), an upgrade to split COMP token rewards to users and aid in bug fixes. Due to Compound Finance’s approach as a community-based project, the upgrade was written by a community member, and went through regular checks before implementation, but an undetected fault remained.

Hours after approval and implementation of the upgrade, the development team noticed an issue with the distribution, with some users getting much more than they were due. Compound Labs and concerned community members traced the glitch to an undetected error in the upgrade.

Protocol users flocked to social media to claim that they received more tokens. One particular user claimed that he received [70 million COMP tokens](https://etherscan.io/tx/0xf4bfef1655f2092cf062c008153a5be66069b2b1fedcacbf4037c1f3cc8a9f45) which is worth roughly $20 million. Another user reported about $29 million worth of COMP tokens. Unfortunately, the losses kept coming in, with few options available to the team. At first glance, the total loss was recorded at around $70 million, but later it was revised to $90 million worth of tokens.

As disastrous as this was for Compound Finance, the development team has reiterated that no funds supplied or borrowed in its interest program are at risk. This was a huge relief, because a scenario where supplied or borrowed funds get affected would have caused chaos amongst the community, potentially leading to a mass exodus of the protocol.

**Governance settings works against Compound**

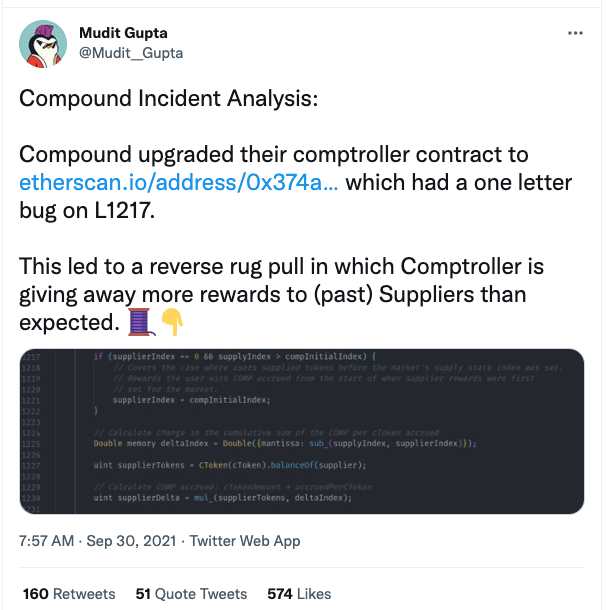
Unfortunately, the team couldn’t stop the error because a change would require a seven-day governance period.

“There are no admin controls or community tools to disable the COMP distribution; any changes to the protocol require a 7-day governance process to make their way into production”   
[Leshner](https://twitter.com/rleshner/status/1443380518498848768?t=f82oM1P0uIPlHi9neBpb9w&s=19), founder, Compound

**How a “one letter bug” caused a costly “reverse rugpull”**

A developer at SushiSwap, Mudit Gupta, explained in a tweet that this whole incident occurred due to a “one letter bug” in the code that caused a reverse [“rugpull”.](https://coinmarketcap.com/alexandria/glossary/rug-pull)

According to Gupta, Compound [upgraded their comptroller contract](https://t.co/mgLGKCywxf?amp=1) which contained a one letter bug on L1217, leading to a reverse rugpull in which Comptroller ended up giving away more rewards to previous suppliers than it should have.



[In a tweetstorm](https://twitter.com/Mudit__Gupta/status/1443454935639609345?t=sznwoTmp3KMDffaI1vpINA&s=19) on 30 September, Gupta explained in great technical detail how the bug happened:

*The bug happens when someone supplies tokens for a market with zero comp rewards like cSUSHI, and cTUSD before the market is initialized or migrated. `supplyIndex` for such tokens remains equal to `compInitialIndex` which means that the if block on L1217 is not triggered.*

*The check there should have been >= rather than >. Since the if block is not triggered, `supplierIndex` remains 0 while `supplyIndex` is 1e36. The delta of the indexes becomes 1e36 and the protocol pays out rewards for 1e36 indexes rather than the intended zero rewards.*

*The last version of comptroller had the same checks but it was fine then because the initial value of `supplyIndex` was 0 rather than 1e36. Logically, the check should have been `>=` even then but since the default was 0, `>` was functionally equivalent but a bit more optimal.*

*In the latest version, changes happened to the default values which meant that this optimization became invalid. If someone only reviewed the delta of the upgraded contract, they might have missed this. A small change at one place can introduce a vulnerability at another.*

*This is why reviewing deltas is dangerous and no matter how small the upgrade, full audits are essential for critical contracts.*

**Will Compound Recover The COMP Tokens?**

Robert Leshner, founder of Compound Labs, stated that there’s a [capped amount](https://twitter.com/rleshner/status/1443380518498848768?t=KCeDJ3x6FpIloB0fBfX91Q&s=19) of COMP in the contract address, but all have already been handed out. While this is a huge blow for the platform, users who earn a passive income through DeFi interest protocols had a field day.

While DeFi protocols have been booming and challenging traditional finance, its decentralization and limited regulation often lead to a reduced recovery rate in cases like this. Bugs such as the one faced by Compound Finance occur in the cryptoverse and pose a huge threat to the protocol.

One thing is certain though, Compound Finance needs its tokens back, and Robert Leshner is taking a two-phase approach.

First off, he has appealed to users who benefited from this windfall to [voluntarily return](https://twitter.com/rleshner/status/1443730726751506432?t=iaviRU4VPwX6Yg8QPWhkEw&s=19) the tokens. A return may seem unlikely, but when incentivized, users may be urged to comply for ethical reasons, plus they are getting rewarded for it. Stranger things have happened in DeFi, where white hat hackers often return funds for bounties and even [not-so-white hackers (see Poly Network hack)](https://www.cybavo.com/blog/poly-network-hack-defi-security/) might do the same when they run out of options.

Compound Finance has asked users to return the tokens and keep 10% as a white hat. This happened in the case of Alchemix, another DeFi protocol that also distributed more tokens than intended. Most Alchemix users returned the excess, but the [Alchemix](https://www.google.com/amp/s/finance.yahoo.com/amphtml/news/free-money-bug-hits-defi-181236746.html) case was about $4 million while Compound’s case is up to $90 million, making the chances of return even slimmer.

Secondly, Robert Leshner is not simply going to rely on the goodwill of users to return the tokens. In a [tweet](https://twitter.com/rleshner/status/1443730726751506432), (which he has since said was wrong) he threatened users that they will be reported to the IRS. If Compound reports its users to the IRS, they would have to pay income tax on the excess tokens. This tactic is unlikely to work because users can simply pay the tax rather than return the money to Compound. Nevertheless, it may spur some users to return the tokens.

Doxxing users is an extremely excessive approach that has been walked back by the owner of Compound. [Doxxing](https://en.m.wikipedia.org/wiki/Doxing) would entail exposing what was ordinarily meant to be private, a no-go area in the cryptoverse(人肉搜索需要暴露通常被认为是隐私的东西，这是加密领域的禁区。). If Compound decides to move forward with doxxing, its reputation may never recover from it.

**What can DeFi protocols like Compound do to avoid these costly mistakes?**

Although its token price has since recovered, Compound’s losses sent COMP’s price down by [13%](https://coinmarketcap.com/currencies/compound/). It also damaged the company’s reputation in the eyes of DeFi users who are looking for better protection against [DeFi hacks, scams and mistakes](https://www.cybavo.com/blog/defi-hacks-2021/).

DeFi meltdowns like this can be avoided by extra checks before upgrades and a more fluid governance system to nip it in the bud(防患于未然). Protocols can also outsource these functions to third-party service providers to scrutinize and audit proposed upgrades before they are implemented(在实施建议的升级之前仔细检查和审计). For DeFi to be above centralized finance, these glitches have to stop occurring.