

Forum:[Hack Forums](#)

Thread: [Omnicoon Problem](#)

Omniscient - February 10, 2015, 2:31 pm

Earlier today at the coin exchange AllCrypt there has been an episode. We're not even sure what to call it exactly as it's still under investigation by both AllCrypt and the Omnicoin Dev Team.

For the immediate future I've disabled the purchase of the OMC award as well as the 3P1C upgrade. I won't at this time halt the auction of the group for OMC. Since the auction doesn't end for about 3 weeks I think there is time to figure this out before making any additional decisions.

Just a few facts that I know. Here are some of the OMC addresses that were part of the issue:

ofquhkd2UbzqL7QgbzzYghcQwm9KYAc5WT Current Balance: -1,056,549.99920000

<http://explorer.coinpayments.net/address.php?chain=5&addr=ofquhkd2UbzqL7QgbzzYghcQwm9KYAc5WT>

oQNwHSamQTJi7bVfaz8hUoBLYadu93bRyF Current Balance: 37,456.64261370

<http://explorer.coinpayments.net/address.php?chain=5&addr=oQNwHSamQTJi7bVfaz8hUoBLYadu93bRyF>

oThxvSbjKTivXF6EppFc2HycuiLwxVLv4 Current Balance: -1,305,725.66601370

<http://explorer.coinpayments.net/address.php?chain=5&addr=oThxvSbjKTivXF6EppFc2HycuiLwxVLv4>

Official statements by the dev team are being made but please respect that they are already busy working to not only figure out what happened but to also work on correcting it as best as possible.

The suspicion is a 51% attack because it is indeed a smaller alt-coin chain. There are things that can be done though to help fix this and being a small alt-coin actually helps make that possible.

In any case it's being worked on. Please be patient and more info will be released when it's necessary for members to know. Let's not go all dramatic about this either until we know the full-extent of the damage and what can or can't be fixed.

Thank you.

Abraham Lincoln - February 10, 2015, 2:35 pm

The OMC team is working to resolve this situation. It is our hope to try to recover the stolen OMC and get it back in the right hands, but there are no guarantees.

If all goes well, we hope to have this cleaned up within a few days, although again we cannot make any promises.

In the mean time we highly recommend that you do not make any trades or deals with other users using OMC.

Justin Timberlake - February 10, 2015, 2:36 pm

I, among many other members, lost a considerable amount of money. I'm sure it's in everyone's best interest to help the coin recover, and hopefully we can do just that.

Random - February 10, 2015, 2:37 pm

(Feb 10, 2015 03:36 PM)Justin Timberlake Wrote: [\[CITE\]](#) I, among many other members, lost a considerable amount of money. I'm sure it's in everyone's best interest to help the coin recover, and hopefully we can do just that.Same.

Hoping something can be done about this

Mix - February 10, 2015, 2:37 pm

So Thats Whats Going On I Have Seen Alot of people Noticing The Omc Sides Were missing I thought U Were Thinking of Removing The Alt-coin but im glad to see that its not that bad Hope Too See The Best From This problem And I Will Carry On Supporting Omc As Much As I Can.

bandors - February 10, 2015, 2:55 pm

If 51% was achieved, is all of OMC ruined?

c x y k - February 10, 2015, 2:58 pm

So, what exactly has happened?

Has the 'coin' been stolen, as such?

Abraham Lincoln - February 10, 2015, 3:05 pm

(Feb 10, 2015 03:55 PM)Bandors Wrote: [\[CITE\]](#) If 51% was achieved, is all of OMC ruined? From what I can tell, yes it was. Otherwise the attack wouldn't have worked.

No, OMC isn't ruined. We're working on a solution to this issue.

(Feb 10, 2015 03:58 PM)qonda? Wrote: [\[CITE\]](#) So, what exactly has happened?

Has the 'coin' been stolen, as such?

According to AllCrypt 2.5 million OMC were stolen from their wallets via an exploit in the network.

Thee Coin as a whole is still alive and we are as in control of it as we where before.

Raz3d - February 10, 2015, 3:08 pm

I hope it's getting fixed soon. Thanks.

bandors - February 10, 2015, 3:16 pm

This is pretty upsetting. I hope it doesn't happen again.

Omniscient - February 10, 2015, 3:18 pm

Quote:According to AllCrypt 2.5 million OMC were stolen from their wallets via an exploit in the network.

I think more accurately they say that they had a 2.5m OMC deposit which was then sold for BTC and the BTC was withdrawn. So under that scenario they wiped out about 2 BTC from buyers. If the OMC chain is reversed then it's those specific buyers of the fraudulent OMC who paid BTC that are the losers here. It doesn't in my view appear that any actual OMC was stolen. Just that AllCrypt was tricked into accepting fake block of OMC.

That's just my point of view at face value of what I'm being told. It's not any technical analysis based on the chain itself or the AllCrypt site.

Jason™ - February 10, 2015, 3:21 pm

Omni, If this isn't reversed, do you think these people with the OMC will have the balls to place a bid?

I saw the other thread that you made but I wasn't sure if you planned on changing the group requirements or canceling it all in all.

FRANKIE - February 10, 2015, 3:26 pm

(Feb 10, 2015 03:35 PM)Abraham Lincoln Wrote: [\[CITE\]](#) In the mean time we highly recommend that you do not make any trades or deals with other users using OMC.

Is it unreasonable to attempt to buy at maximum 2000 OMC or something near that amount?

beslim - February 10, 2015, 3:26 pm

Abraham Lincoln Wrote: [\[CITE\]](#) The OMC team is working to resolve this situation. It is our plan to fully refund all those who were affected by this.

If all goes well, we hope to have this cleaned up within a few days, although we cannot make any promises.

In the mean time we highly recommend that you do not make any trades or deals with other users using OMC.

I'm glad at least that you have a plan to fully refund all those who were affected by this.

Raoul Duke - February 10, 2015, 3:26 pm

According to the allcrypt statement in the other thread there is only 12k OMC left in their wallet so I think they tried to sell as much "fake OMC" they can then withdraw the rest (deposit fake OMC withdraw true OMC)

#Merky - February 10, 2015, 3:27 pm

Hope you get this fixed soon omni I'm looking to get ep1c ?

Raoul Duke - February 10, 2015, 3:29 pm

(Feb 10, 2015 04:26 PM)FRANKIE Wrote: [\[CITE\]](#) Is it unreasonable to attempt to buy at maximum 2000 OMC or something near that amount?

"IF" there is a rollback your 2000 OMC will disappear and the money you used to buy it will not come back...

Nobody should make any move or deal with OMC until we know more.

Abraham Lincoln - February 10, 2015, 3:31 pm

(Feb 10, 2015 04:21 PM)Jason™ Wrote: [\[CITE\]](#) Omni, do you suppose this has something to do with the group you are selling?

If this isn't reversed, do you think these people with the OMC will have the balls to place a bid?

Yes, this most likely does. Someone wanted a quick way to get enough OMC to buy the group.

(Feb 10, 2015 04:26 PM)FRANKIE Wrote: [\[CITE\]](#) Is it unreasonable to attempt to buy at maximum 2000 OMC or something near that amount?

No. You should not buy any OMC at all. Zero. If you do you are at risk of losing it.

Jason™ - February 10, 2015, 3:36 pm

(Feb 10, 2015 04:31 PM)Abraham Lincoln Wrote: [\[CITE\]](#) Yes, this most likely does. Someone wanted a quick way to get enough OMC to buy the group.

No. You should not buy any OMC at all. Zero. If you do you are at risk of losing it.

I edited my post the second you quoted me haha, but yeah I agree.

Pretty stupid though because I doubt Omni would allow a bid with stolen coins.

Abraham Lincoln - February 10, 2015, 3:41 pm

(Feb 10, 2015 04:36 PM)Jason™ Wrote: [\[CITE\]](#) I edited my post the second you quoted me haha, but yeah I agree.

Pretty stupid though because I doubt Omni would allow a bid with stolen coins.
Well if no one known about it they might have been able to get away with it.

FRANKIE - February 10, 2015, 3:42 pm

(Feb 10, 2015 04:31 PM)Abraham Lincoln Wrote: [\[CITE\]](#) Yes, this most likely does. Someone wanted a quick way to get enough OMC to buy the group.

No. You should not buy any OMC at all. Zero. If you do you are at risk of losing it.
All right, thank you for the warning. I will hold them until this blows over.

Aceman - February 10, 2015, 3:44 pm

(Feb 10, 2015 04:18 PM)Omniscient Wrote: [\[CITE\]](#) I think more accurately they say that they had a 2.5m OMC deposit which was then sold for BTC and the BTC was withdrawn. So under that scenario they wiped out about 2 BTC from buyers. If the OMC chain is reversed then it's those specific buyers of the fraudulent OMC who paid BTC that are the losers here. It doesn't in my view appear that any actual OMC was stolen. Just that AllCrypt was tricked into accepting fake block of OMC.

That's just my point of view at face value of what I'm being told. It's not any technical analysis based on the chain itself or the AllCrypt site. Yeah that's spot on from what I understand. I'm pretty crushed considering the amount that was lost and while the OMC can be recovered I'm still pretty upset about the BTC that was lost from the buy orders. Especially since a large part of that would have been mine. Since it was an attack by 51% attack I don't see AllCrypt reimbursing anybody.

Abraham Lincoln - February 10, 2015, 3:49 pm

(Feb 10, 2015 04:44 PM)Aceman Wrote: [\[CITE\]](#) Yeah that's spot on from what I understand. I'm pretty crushed considering the amount that was lost and while the OMC can be recovered I'm still pretty upset about the BTC that was lost from the buy orders. Especially since a large part of that would have been mine. Since it was an attack by 51% attack I don't see AllCrypt reimbursing anybody.

Total trade volume is only 250K OMC, not 2.5 million OMC. They sold under 250K.

And the last trade price is 0.00000521 BTC which means they sold for that price or above. $2.5M \text{ OMC} * 0.00000521 = 13.025$ or more.

They didn't sell much.

Omniscient - February 10, 2015, 3:55 pm

(Feb 10, 2015 04:49 PM)Abraham Lincoln Wrote: [\[CITE\]](#) Total trade volume is only 250K OMC, not 2.5 million OMC. They sold under 250K.

And the last trade price is 0.00000521 BTC which means they sold for that price or above. $2.5M \text{ OMC} * 0.00000521 = 13.025$ or more.

They didn't sell much.

Not sure we can trust any data that's posted currently on the AllCrypt page. But as I've spoken to

you via PM I don't think the entire standing orders for OMC buy were more than 2 BTC in total. The orders sitting there was like 100000 OMC for .001 BTC. People just having insane orders.

So let's say 51% attack allowed person to deposit millions of OMC then they just hit all the BUY orders and sold off all OMC. Then they withdrew whatever BTC they gained. So far AllCrypt says it's under 2 BTC. That's very probably and likely.

So now the question is how do we fix the OMC problem and correct the BTC loss.

FYI....behind the scenes this is all being worked out and I have faith that it will be quickly resolved effectively. No one should panic. Just chill and wait out the drama.

FrenchcoreRadio - February 10, 2015, 3:56 pm

It really sucks. i hope this does not affect the market too much of OMC

Grim - February 10, 2015, 4:04 pm

such a shitty time for this too happen right when your trying too sell a group for that currency. Hope you and your team can get this resolved as soon as possible. which i have no doubt you will ?

Fudster - February 10, 2015, 4:44 pm

Dam....is this also related to the issue I noticed earlier? "Last block found 2 hours and 28 minutes ago"

Raoul Duke - February 10, 2015, 4:53 pm

(Feb 10, 2015 05:44 PM)Fudster™ Wrote: [\[CITE\]](#) Dam....is this also related to the issue I noticed earlier? "Last block found 2 hours and 28 minutes ago"

This is because everybody has stopped mining until the problem is resolved

Fudster - February 10, 2015, 4:56 pm

(Feb 10, 2015 05:53 PM)Raoul Duke Wrote: [\[CITE\]](#) This is because everybody has stopped mining until the problem is resolved

No. This was before this was even posted. Like this morning.

Abraham Lincoln - February 10, 2015, 5:10 pm

(Feb 10, 2015 05:56 PM)Fudster™ Wrote: [\[CITE\]](#) No. This was before this was even posted. Like this morning.

It's not uncommon for the network to go a few hours without any new blocks.

Silver Fang - February 10, 2015, 5:15 pm

Well if they cashed out the btc then they probably gets away with it. Either way hope it all goes well with the omc.

Fudster - February 10, 2015, 6:06 pm

(Feb 10, 2015 06:10 PM)Abraham Lincoln Wrote: [\[CITE\]](#) It's not uncommon for the network to go a few hours without any new blocks.

Ah, got you. Well if you haven't noticed I started mining:p I'm glad I switched pools before I left. Miner running wwith no work heh. (Power on fans running)

Eagerkid - February 10, 2015, 6:37 pm

I hope this can be resolved, such bad timing

OpenSourcerer - February 10, 2015, 7:05 pm

I still have my 272.49715927 OMC ??????

I hope OMC is able to recover... Sucks for those of you whos wallets where affected.
Also hope that ONE will get more integration with hf, seeing as the only reason to have omc is to get the epic upgrade and the omc award...

ItsATumor - February 10, 2015, 7:37 pm

So all of allcrypts funds were taken? If I misunderstand, who's wallets were affected.

Abraham Lincoln - February 10, 2015, 7:45 pm

(Feb 10, 2015 08:37 PM)ItsATumor Wrote: [\[CITE\]](#) So all of allcrypts funds were taken? If I misunderstand, who's wallets were affected.

Yes. Essentially all of the OMC in AllCrypt's wallets where taken.

Anyone that had OMC on AllCrypt is effected.

ItsATumor - February 10, 2015, 7:56 pm

(Feb 10, 2015 08:45 PM)Abraham Lincoln Wrote: [\[CITE\]](#) Yes. Essentially all of the OMC in AllCrypt's wallets where taken.

Anyone that had OMC on AllCrypt is effected.

Along with a shitty theme they have shitty security, great...

Carl Elias - February 10, 2015, 8:15 pm

Guess it is good I didn't have any on there. I am posting to keep an eye on this but hope it gets resolved soon!

-Ty

allcrypt - February 10, 2015, 8:34 pm

(Feb 10, 2015 08:56 PM)ItsATumor Wrote: [\[CITE\]](#) Along with a shitty theme they have shitty security, great...

Quick reply here - I posted a much longer one in the "AllCrypt is down" thread.

A) Has nothing to do with our security. We have absolutely zero control over the OMC blockchain. If someone makes a legitimate OMC deposit, and after it receives a bunch of confirmations, and is, for every possible way to ensure it's true, confirmed and "solid", they somehow break the OMC blockchain and invalidate the block, there is literally NOTHING we can do about it. About the only thing we COULD do is increase the required number of confirmations to a number so large that it makes the attacker bored and not worth his time to do.

Which makes YOU unable to use your OMC deposits or make any withdrawals from the site for an equal period of time.

Anyone here want to disable all withdrawals from AllCrypt for 3 days every time you deposit OMC? No? Ok then. I'll stick with "there was nothing we could do about it."

And like I said in the other thread, yes, I'm bristly over this. My site was personally attacked, I come here to openly and honestly tell everyone what happened, something I'd venture NO OTHER EXCHANGE would bother to do, and wind up spending more time defending the site than I do providing helpful information.

So on that note, please forgive me for getting a bit shitty here for one moment:

My site gets attacked. I get blamed. I have to investigate. I have to post these defenses in the

forums...

And the best part? Once it's rolled back? MY dev team gets to spend, what I am guessing is around 20 manhours going over every OMC transaction, and every account that was affected by this, MANUALLY, to restore balances and audit everything.

For a coin that we have been the ONLY ones to host your coin, from DAY 1, that has, and here's where I get really shitty, made our site literally .24 BTC since we listed it. Yep. Roughly 62 BTC volume in the history of the coin, about .39% total per trade. \$54. Cloudflare ALONE costs \$200 a month, as security to protect your coin.

Wanna guess the labor costs to pay the dev team for ~20 hours of work to restore the coin? Financially it seems to be in our best interest to dump the coin, since the support base is so small someone managed to pull off a 51% attack. Could happen again. Who knows.

We aren't, because we're not assholes, and we're here to work FOR crypto, and to support the small coins no one else will.

You're welcome. We appreciate your support.

One final note: I, personally, find it fucking HILARIOUS that members of HACKFORUMS are getting pissed off and upset that the HACKFORUMS coin was hacked. Isn't this what you guys do? Just reading the other thread where I replied earlier, I saw no less than three ads in sigs where I learned I could HIRE THEM to hack someone/something.

Here is where I am NOT trying to be an asshole: If the hackforums coin gets hacked, your pulpit you stand behind to shout your righteous indignation is a really, really tiny one.

And if my reaction seems to be way overblown, it comes from being the only site to host a good many coins, that later find "success" on "better" exchanges, and we get crapped on in the process, over and over again. If it wasn't for my personal love of crypto and wanting to help it succeed and grow, I'd have shut the site down months ago. It's absurd amounts of time and money to run the site. Being shit on by the coins that I, personally, fund an exchange for them to grow on... it got old 7 months ago.

I don't post that looking for pity or a pat on the back, it's a business, ultimately I hope to see it become profitable. But my god... you could try and not kick the ONLY EXCHANGE that supports you, maybe?

VRUMM - February 10, 2015, 8:43 pm

(Feb 10, 2015 09:34 PM)allcrypt Wrote: [\[CITE\]](#) Quick reply here - I posted a much longer one in the "AllCrypt is down" thread.

A) Has nothing to do with our security. We have absolutely zero control over the OMC blockchain. If someone makes a legitimate OMC deposit, and after it receives a bunch of confirmations, and is, for every possible way to ensure it's true, confirmed and "solid", they somehow break the OMC blockchain and invalidate the block, there is literally NOTHING we can do about it. About the only thing we COULD do is increase the required number of confirmations to a number so large that it makes the attacker bored and not worth his time to do.

Which makes YOU unable to use your OMC deposits or make any withdrawals from the site for an equal period of time.

Anyone here want to disable all withdrawals from AllCrypt for 3 days every time you deposit OMC? No? Ok then. I'll stick with "there was nothing we could do about it."

And like I said in the other thread, yes, I'm bristly over this. My site was personally attacked, I come here to openly and honestly tell everyone what happened, something I'd venture NO OTHER EXCHANGE would bother to do, and wind up spending more time defending the site than I do providing helpful information.

So on that note, please forgive me for getting a bit shitty here for one moment:

My site gets attacked. I get blamed. I have to investigate. I have to post these defenses in the forums...

And the best part? Once it's rolled back? MY dev team gets to spend, what I am guessing is around 20 manhours going over every OMC transaction, and every account that was affected by this, MANUALLY, to restore balances and audit everything.

For a coin that we have been the ONLY ones to host your coin, from DAY 1, that has, and here's where I get really shitty, made our site literally .24 BTC since we listed it. Yep. Roughly 62 BTC volume in the history of the coin, about .39% total per trade. \$54. Cloudflare ALONE costs \$200 a month, as security to protect your coin.

Wanna guess the labor costs to pay the dev team for ~20 hours of work to restore the coin? Financially it seems to be in our best interest to dump the coin, since the support base is so small someone managed to pull off a 51% attack. Could happen again. Who knows.

We aren't, because we're not assholes, and we're here to work FOR crypto, and to support the small coins no one else will.

You're welcome. We appreciate your support.

One final note: I, personally, find it fucking HILARIOUS that members of HACKFORUMS are getting pissed off and upset that the HACKFORUMS coin was hacked. Isn't this what you guys do? Just reading the other thread where I replied earlier, I saw no less than three ads in sigs where I learned I could HIRE THEM to hack someone/something.

Here is where I am NOT trying to be an asshole: If the hackforums coin gets hacked, your pulpit you stand behind to shout your righteous indignation is a really, really tiny one.

And if my reaction seems to be way overblown, it comes from being the only site to host a good many coins, that later find "success" on "better" exchanges, and we get crapped on in the process, over and over again. If it wasn't for my personal love of crypto and wanting to help it succeed and grow, I'd have shut the site down months ago. It's absurd amounts of time and money to run the site. Being shit on by the coins that I, personally, fund an exchange for them to grow on... it got old 7 months ago.

I don't post that looking for pity or a pat on the back, it's a business, ultimately I hope to see it become profitable. But my god... you could try and not kick the ONLY EXCHANGE that supports you, maybe? If it's so hard, shut down your business. You won't because you know there's potential for success. Don't try to pull that bullshit of an excuse and pretend you are the only option. It only costs no more than \$200 to get listed in an exchange like cryptsy, and for our sake try to act professional at least once. Even if the users are in the wrong, you can't act like a dick about it.

No one here is looking for your pity. The only reason omnicoin only uses allcrypt is because there is fear of pumps and dumps on larger exchanges. I've seen coins with absolutely no purposes buy their way into large exchanges for small amounts of money. Don't try to pick a fight with a whole community. You won't win. Stop acting so petty.

FYI I used allcrypt way before omnicoin was added.

Proficiency - February 10, 2015, 8:52 pm

(Feb 10, 2015 09:34 PM)allcrypt Wrote: [\[CITE\]](#) Quick reply here - I posted a much longer one in the "AllCrypt is down" thread.

A) Has nothing to do with our security. We have absolutely zero control over the OMC blockchain. If someone makes a legitimate OMC deposit, and after it receives a bunch of confirmations, and is, for every possible way to ensure it's true, confirmed and "solid", they somehow break the OMC blockchain and invalidate the block, there is literally NOTHING we can do about it. About the only thing we COULD do is increase the required number of confirmations to a number so large that it makes the attacker bored and not worth his time to do.

Which makes YOU unable to use your OMC deposits or make any withdrawals from the site for an equal period of time.

Anyone here want to disable all withdrawals from AllCrypt for 3 days every time you deposit OMC? No? Ok then. I'll stick with "there was nothing we could do about it."

And like I said in the other thread, yes, I'm bristly over this. My site was personally attacked, I come here to openly and honestly tell everyone what happened, something I'd venture NO OTHER EXCHANGE would bother to do, and wind up spending more time defending the site than I do providing helpful information.

So on that note, please forgive me for getting a bit shitty here for one moment:

My site gets attacked. I get blamed. I have to investigate. I have to post these defenses in the forums...

And the best part? Once it's rolled back? MY dev team gets to spend, what I am guessing is around 20 manhours going over every OMC transaction, and every account that was affected by this, MANUALLY, to restore balances and audit everything.

For a coin that we have been the ONLY ones to host your coin, from DAY 1, that has, and here's where I get really shitty, made our site literally .24 BTC since we listed it. Yep. Roughly 62 BTC volume in the history of the coin, about .39% total per trade. \$54. Cloudflare ALONE costs \$200 a month, as security to protect your coin.

Wanna guess the labor costs to pay the dev team for ~20 hours of work to restore the coin? Financially it seems to be in our best interest to dump the coin, since the support base is so small someone managed to pull off a 51% attack. Could happen again. Who knows.

We aren't, because we're not assholes, and we're here to work FOR crypto, and to support the small coins no one else will.

You're welcome. We appreciate your support.

One final note: I, personally, find it fucking HILARIOUS that members of HACKFORUMS are getting

pissed off and upset that the HACKFORUMS coin was hacked. Isn't this what you guys do? Just reading the other thread where I replied earlier, I saw no less than three ads in sigs where I learned I could HIRE THEM to hack someone/something.

Here is where I am NOT trying to be an asshole: If the hackforums coin gets hacked, your pulpit you stand behind to shout your righteous indignation is a really, really tiny one.

And if my reaction seems to be way overblown, it comes from being the only site to host a good many coins, that later find "success" on "better" exchanges, and we get crapped on in the process, over and over again. If it wasn't for my personal love of crypto and wanting to help it succeed and grow, I'd have shut the site down months ago. It's absurd amounts of time and money to run the site. Being shit on by the coins that I, personally, fund an exchange for them to grow on... it got old 7 months ago.

I don't post that looking for pity or a pat on the back, it's a business, ultimately I hope to see it become profitable. But my god... you could try and not kick the ONLY EXCHANGE that supports you, maybe?

Sheesh. All that money spent, and you can't get a good website theme? None of my business though ? ?

Omniscient - February 10, 2015, 10:45 pm

Responses to the member allcrypt are not helpful. As such I'm closing this thread.

@allcrypt ...be aware that generally speaking members here are making statements on their own behalf and don't reflect the view of the actual Omnicoin dev team.

We'll get this sorted out and we appreciate your efforts.

Thanks.