276

reckless How I lost ~4 BTC on Lightning Network (self.Bitcoin)

submitted 4 days ago * by ZipoTm

INWHY Today at 7:53 AMam I able to loose money after force-closing channels? Screenshot 2019-10-23 at 7.51.16.pngScreenshot 2019-10-23 at 7.51.16.png

50 replies

Will O'Beirne 2 hours agoYes, if you force close using an older invalid state, they can take the money while it's timelocked if their node is online.

INWHY 2 hours agowow... looks like I lost 4BTC

INWHY 2 hours agobecause my LND wasn't syncronised, that's weird (edited)

moli 2 hours ago#reckless :rekt:

INWHY 2 hours agoit was buggy and stuck...

moli 2 hours agoto be frank this isn't the first time i've seen you with the same issue of carelessly locking so much money on useless nodes and then decided to just mass

close them all

INWHY 2 hours agoI've used the default closeallchannels --force function, nothing else, to be frank. (edited)

INWHY 2 hours agoalso, my node wasn't useless, but one of the biggest in the network, called LIGHTNING-CASINO.COM

moli 2 hours agoah this time it's worse because you force closed from an older state

moli 2 hours agoyou know it's a "no-no", right? because it's a breach

INWHY 2 hours agoI've force-closed from a backup, because there was a power outage, then why the "no-no" function is ever available?! (edited)

moli 2 hours agohow old was the backup?

INWHY 2 hours agofew days prior, but after force-closing them the LND got stuck without synchronising the graph

INWHY 1 hour agoI'm working as a system administrator, have some server knowledge and I bet that everybody who have bigger node will face the same issues, it happens only when you close* you channels, openings are fine

moli 1 hour agoso the backup is a few days old? even a few minutes or hours old , they can cause a breach, that's how it is

INWHY 1 hour agothen how to proceed if the channel graph file is broken? that happened after updating from vulnerable LND 6.1 to 7.1 beta

INWHY 1 hour ago@moli if "few minutes" old backup can cause a breach, that means that LND doesn't support backups at all, am I right? make backups and after 10 minutes they are old and unusable... (edited)

moli 1 hour ago@INWHY since the beginning of lnd and lightning network, we've been told not to do backups

moli 1 hour agochannel state is very dynamic you can't back it up like any static files

INWHY 1 hour agowhat's the purpose of the backup functions then?

moli 1 hour agowhat backup functions?

INWHY 1 hour agoexportchanbackup and restorechanbackup

moli 1 hour agothat is different

INWHY 1 hour agoI have those files

moli 1 hour agothose files are for recovery, but you said you did a backup of the data directory .lnd and you ran it after a power outage?

INWHY 1 hour agoyes, am I able to use those recovery SCB files?

INWHY 1 hour agoalso, they are 3 different types, JSON one, binary one, and 2nd type of binary one

moli 1 hour agoyes, which lnd version are you running?

INWHY 1 hour ago7.1

- News articles that do not contain the word "Bitcoin" are usually off-topic. This subreddit is not about general financial news.
- Submissions that are mostly about some other cryptocurrency belong elsewhere. For example, /r/CryptoCurrency is a good place to discuss all cryptocurrencies.
- Promotion of client software which attempts to alter the Bitcoin protocol without overwhelming consensus is not permitted.
- No referral links in submissions.
- No compilations of free Bitcoin sites.
- Trades should usually not be advertised here. For example, submissions like "Buying 100 BTC" or "Selling my computer for bitcoins" do not belong here. /r/Bitcoin is primarily for news and discussion.
- Please avoid repetition — /r/bitcoin is a subreddit devoted to new information and discussion about Bitcoin and its ecosystem. New merchants are welcome to announce their services for Bitcoin, but after those have been announced they are no longer news and should not be re-posted. Aside from *new* merchant announcements, those interested in advertising to our audience should consider Reddit's self-serve advertising system.
- Do not post your Bitcoin address unless someone explicitly asks you to.
- Be aware that Twitter, etc. is full of impersonation.

Related communities

Sorted roughly by decreasing popularity.

- **Bitcoin Beginners**
- Local Bitcoin communities
- BitcoinMarkets
- BitcoinAirdrops

INWHY 1 hour agoScreenshot 2019-10-23 at 9.16.30.pngScreenshot 2019-10-23 at 9.16.30.png

INWHY 1 hour agoScreenshot 2019-10-23 at 9.17.01.pngScreenshot 2019-10-23 at 9.17.01.png

moli 1 hour agoso did you run the SCB ? how did you run the "backup" ?

INWHY 1 hour agovia exportchanbackup --all > backup

INWHY 1 hour agoand exportchanbackup --output_file channel-backup-file

moli 1 hour agobut you said you ran a .lnd backup and force closed all your channels? (edited)

moli 1 hour agothis is very confusing

INWHY 1 hour agoyes, using previous files state. I wonder, am I able to use those static channel backups at the moment? (edited)

moli 1 hour agono

moli 1 hour agoyou have already closed all your channels with an older state? that's it, the money is gone

INWHY 1 hour agohow can I know if the state is older or not?

moli 1 hour agothe backup was a few days old

INWHY 1 hour agoas you said even few minutes old backup is enough to cause a breach, which makes them totally unusable

INWHY 1 hour agoin my case, I have veeam backups for the last ~320 days + SCBs, + paper backup, and after force-closing all channels which LND approved and initiated, my funds are lost and unavailable

moli 1 hour agoif you run an older backup, lnd still can run but when you force close channels, that's when the breach happens

INWHY 1 hour agounderstood, my final conclusion is that just need to forgot about backups there... or need to make totally live SCBs every single second... (edited)

moli 1 hour agoafter the power outage if your current .lnd data could not start, you could use the SCB recovery and it would ask your peers to close channels and you would get your money back

INWHY 1 hour agoI was unable to recover the channels from the SCB, because there was an error that those channels are already existing, about the peers there are more than 400 channels, just cannot contact them. (edited)

INWHY 45 minutes agoI bet that exchanges will start using that technology only* if they have a good and stable backup structure... without it only enthusiast like me will rush on it (edited)

INWHY 40 minutes ago@moli thank you for all that info. appreciated

moli 38 minutes agonp, sorry for your loss.. but please this is so fundamental i hope you would do some reading or asking for help before doing something drastic next time :+1::skin-tone-3:

Update: https://github.com/lightningnetwork/lnd/issues/2468

417 comments **share** **save** **hide** **report**

can also use Bitcoin Core as a very secure Bitcoin wallet.

> - Latest stable version: ***0.18.1 (August 2019)*** [BitTorrent]
> - Release Announcement
> - You *MUST* verify the integrity of this software before running it.

Style sheet credits

The CSS used by this subreddit is the Erdune Theme modified by /u/Annihilia and /u/konkedas. Logo design by /u/Annihilia. Check out his other work here.

Ad campaign:

We previously collected donations to fund Bitcoin advertising efforts, but we no longer accept donations. The funds already donated will be spent on some sort of advertising, as intended. As of now, 10.35799117 BTC was spent out of 22.51357574. If you have ideas for the remaining BTC, see here for more info.

MODERATORS message the moderators

theymos
BashCo
frankenmint
rbitcoin-bot
Aussiehash
ThePiachu
Avatar-X
DigitalGoose
thieflar
rBitcoinMod

...and 12 more »

< > discussions in r/Bitcoin X

3186 · 115 comments

These past few weeks in a nutshell

0:31

top 200 comments - show all 417
sorted by: **best**

[–] **BeTeeC** redditor for 3 months 55 points 4 days ago

How did you stay so calm? Tell me that's not your whole stack? I'd be nowhere near this calm.

permalink embed save report give award reply

[–] **ZipoTm** [S] 61 points 4 days ago

I still have some hope... @guggero from http://lightningcommunity.slack.com may help me... I'm just stuck in some kind of hypnotic state...

permalink embed save parent report give award reply

[–] **etmetm** [ ] 38 points 4 days ago

I local force closed my channels with you around the 2nd of October, as your node was not available for quite some weeks, so those should be fine.

I'll send you the details in a private message.

permalink embed save parent report give award reply

[–] **BeTeeC** redditor for 3 months 34 points 4 days ago

Yeah I have a lot of sympathy for you, dude. I'm not really familiar with LN to the extent that you're dealing here, so can't help. Just generally feel pretty bad for you.

permalink embed save parent report give award reply

[–] **vakeraj** 6 points 4 days ago

If all or even most of your BTC is locked up in LN channels, you're an idiot. This is an early stage, highly experimental technology with lots of bugs to iron out.

permalink embed save parent report give award reply

[–] **Smoy** 30 points 4 days ago

So no one should be using lightning is what im gathering from this statement? Because who would think a loss of any btc would be acceptable

permalink embed save parent report give award reply

[–] **bitusher** 27 points 4 days ago

Just use lightning for a few hundred dollars of spending cash and have live backups. Normal users having 4BTC in lightning channels at this stage is reckless.

Most of these complaints are often just altcoiners concern trolling however so be skeptical when you hear about someone losing so much money or having huge problems as well.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **vakeraj** 16 points 4 days ago

> Most of these complaints are often just altcoiners concern trolling.

Bingo!

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **Smoy** 7 points 4 days ago

I really couldnt stand losing a few hundred dollars tho so that seems like too much money

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **bitusher** 2 points 4 days ago

If a few hundred dollars is a lot of money for you than you should likely not be investing in any cryptocurrency at all as the first rule is to have a fiat savings account for emergencies.

You can use Bitcoin and lightning with small amounts, but do not invest or speculate with cryptocurrencies until your finances are sorted

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **Smoy** 13 points 4 days ago

I have plenty of savings, but losing btc for no reason, even 1 sat is unacceptable to me. Its also sad to see this statement, considering this whole venture and block size debate was so that people in developing nations could stay on. Yet the sentiment now seems to be theyre too poor to use btc.

Theres a big difference between having a few hundred dollars worth of btc changing value and that amount of btc just disappearing

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **bitusher** 11 points 4 days ago

> but losing btc for no reason, even 1 sat is unacceptable to me.

1 sat is a fraction of a penny , you are being a bit unreasonable here.

> this whole venture and block size debate was so that people in developing nations could stay on.

I'm a tico in a developing country and am opposed to raising the blocksize beyond 4m weight for now.

> Yet the sentiment now seems to be theyre too poor to use btc.

Im saying you can use BTC, but unless you have a fiat savings don't speculate or invest in it . Use it if you need to as p2p currency.

> Theres a big difference between having a few hundred dollars worth of btc changing value and that amount of btc just disappearing

People make stupid mistakes all the time by investing in scam ICOs/altcoins or getting scammed by con artists. We don't know if he was just ignorant or was deliberately trying to steal his customers BTC but lightning worked as intended when he manually used an old channel state. This user ignored all the warnings that we repeatedly made so many of his customers got some free BTC , would have been smart of him to simply flip this around and tell his clients he was awarding them a gift for their business and welcome them to use his service more.

permalink **embed** **save** **parent** **report** **give award** **reply**

continue this thread

[–] **the_evil_priest** 1 point 3 days ago

really if you use segwit... you pay like maximum 50 cents to be in the first block, usually.
that is concidered a big fee for skilled bitcoiners! Those who are skilled set their own fees way lower than 50cents and get their transactions confirmed quickly, usually

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **vakeraj** 11 points 4 days ago

No, no one should put a **life changing amount of money** into Lightning, for now.

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (11 replies)

[–] **ssvb1** 7 points 4 days ago

> So no one should be using lightning is what im gathering from this statement? Because who would think a loss of any btc would be acceptable

People are always risking to lose their coins in hot wallets, with or without lightning. Just like they are risking to lose cash that they carry around in their pockets. So it is recommended to have some pocket money for everyday spending in your mobile hot wallet, but keep savings/investments in a cold wallet disconnected from the Internet. That's what normal users are expected to do.

Big LN routing node operators, such as the OP, are a special case. They are doing business and wilfully taking risks because they are expecting to earn more. In the same way as various crypto exchanges are getting hacked regularly, but there is no shortage of them because they are also making big profits.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **ssvb1** 4 points 4 days ago

> But im not at risk at losing my on chain transactions.

If you are keeping all your crypto savings in a hot wallet, then you may lose everything on some unlucky day and won't be saved by the on-chain magic.

For example, there was a recent vulnerability in Electrum wallet application, which allowed malicious websites to steal your coins: https://electrum.readthedocs.io/en/latest/cve.html

There were also a lot of vulnerabilities in other software and system components, which could allow hackers to get access to the data on your phone or computer. Thus giving them an opportunity to steal your private key.

TL;DR; If anything is connected to the Internet, then it may be hacked some day.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **archer_III** 2 points 4 days ago

"Just like they are risking to lose cash that they carry around in their pockets. "

What about people that carry debit/credit cards in their pockets?

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **neonzzzzz** 1 point 3 days ago

They aren't risk free either.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **archer_III** 1 point 3 days ago

Yes it is always a pain to have to call the bank to block the card and reverse fraudulent charges

permalink embed save parent report give award reply

[–] **Smoy** 2 points 4 days ago

But im not at risk at losing my on chain transactions. So why would i use something that would risk me losing anything. Cash isnt a good example here because cash cant get deleted.

permalink embed save parent report give award reply

[–] **Karma9000** 7 points 4 days ago

Cash can’t be backed up, either, and is at risk of physical loss/theft/seizure. It’s lower risk if you’re not carrying around a ton of it wherever you go.

permalink embed save parent report give award reply

[–] **sebthauvette** 4 points 4 days ago

At the moment, lightning is still in development and not supposed to be used unless you want to test it and take the risk of encountering problems.

I think that lightning will be useful to make multiple small transactions (day to day expenses) without paying huge transaction fees. However, for long term storage and big transactions, on chain transactions work perfectly fine.

permalink embed save parent report give award reply

[–] **Smoy** 1 point 4 days ago

Gotchya, thanks

permalink embed save parent report give award reply

[–] **JcsPocket** 9 points 4 days ago

To be clear this guy handled things in the worst way possible. I use static channel backups which to users nodes looks like just a normal channel close which would be approved 99% of the time. Unless a user makes a custom malicious client he would have been fine with simple static backup.

For more protection and less trust there are scripts that keep channel state backed up in real time as it changes. For someone with 40k this should have been done.

What you DONT DO is carelessly force close every channel when you're not even sure your state is correct. Throwing caution in the wind its literally the worst thing you could do.

For the record I stalked you a bit before replying to make sure you're not an altcoiner kicking up dust. Youre actually a really good person.

yanggang2020

permalink embed save parent report give award reply

[–] Smoy 2 points 3 days ago

Lol thanks for the rundown. Very informative. And fuck yes Yang 2020, the only candidate who is likely to embrace crypto

permalink embed save parent report give award reply

load more comments (11 replies)

[–] whalecheetah 2 points 4 days ago

In all fairness this is why a lot of people don't use lightning just yet

It is still experimental

permalink embed save parent report give award reply

[–] perogies 2 points 3 days ago*

Let the devs play with and lose their own Bitcoin. No one has any reason to use this alpha product right now.. Fees on chain are cheap and 99% of us don't want to spend our Bitcoin anyway.

permalink embed save parent report give award reply

[–] lemineftali 1 point 3 days ago

I’m trying to set up a sat node and would like to tinker around. I’m happy to throw $20 into teaching myself how LN works. The trick is to just use a ridiculously small amount and learn though.

permalink embed save parent report give award reply

[–] perogies 3 points 3 days ago

If it ever becomes popular it will be because everything that makes it complicated and risky has been fixed and abstracted away. But yeah, if you want to experiment go for it.

permalink embed save parent report give award reply

[–] neonzzzzz 1 point 3 days ago

For educational purposes it's wise to start with testnet with worthless coins.

permalink embed save parent report give award reply

load more comments (6 replies)

[–] **ilpirata79** 18 points 4 days ago*

You should ask your peers to give your bitcoins back. They should have the last valid state so if they're honest they could do that.

p.s. I would do it (refund your btcs).

permalink embed save parent report give award reply

[–] **XavierFartboner** 18 points 4 days ago

lmao. He'd be lucky if he got back even .01% by simply asking nicely. It's laughable that btc/lightning network got shoved into every conversation having anything to do with crypto payments when it is clearly 100% not ready. I mean if not even a sys admin is capable yet, what hope does Carol from accounting have?

permalink embed save parent report give award reply

[–] **etmetm** [ ] 18 points 4 days ago

To be fair, LN is still at #reckless "for enthusiasts" state and I believe chances are higher at this time to get node operators to cooperate to refund breach funds...

permalink embed save parent report give award reply

[–] **klondikecookie** 2 points 1 day ago

> I haven't seen any breaches, and neither has anyone I know. I find it really hard to believe someone had hundreds of breaches without anyone seeing any

https://twitter.com/JackMallers/status/1187848195101073408

permalink embed save parent report give award reply

[–] **MakeMeAnICO** 0 points 4 days ago

LN will always be reckless and just 18 months away

permalink embed save parent report give award reply

[–] **norfbayboy** 5 points 4 days ago

Bitcoin itself is still BETA.

permalink embed save parent report give award reply

load more comments (1 reply)

[–] **fresheneesz** 6 points 4 days ago

Why? Because technology never gets better right?

permalink embed save parent report give award reply

load more comments (2 replies)

load more comments (1 reply)

[–] **ilpirata79** 6 points 4 days ago

Throwing some emails if he knows the peers should not hurt :)

I agree that this thing is not ready, indeed I wanted to run a node but then I discovered that backups are not possible, so I won't.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **JcsPocket** 8 points 4 days ago

Backup is very possible. There are scripts you can run its not accurate to say the backup is old "every second" It just needs to backup every time it changes.

So you have a script monitoring for file change and making a copy.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **ilpirata79** 8 points 4 days ago

Not enough. Backup and network updates must be made atomically or at least backups should be made *before* network updates. If you operate as you said, backups would come after a new channel state has been established in the network.

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (6 replies)

[–] **whitslack** 3 points 4 days ago

You can't just copy files in the file system. You could happen to catch the file as it was being updated, in which case your copy will be in an inconsistent state.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **koenklaver** 2 points 4 days ago

Would it be possible to run the same node/channels from two (or arbitrarily many) geographically different locations? Would this not mitigate the effect of local power/network outs, especially combined with good backup scripting.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **fresheneesz** 1 point 4 days ago

No. It's much harder to operate the same channel from many machines, because of the issue of state. It's important your node know the latest state. If all your machines have a very reliable way to ensure they're all on the same state, then sure. But it's likely easier in that case to run the channel on a single machine that you just connect to remotely from your arbitrarily many machines.

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (4 replies)

[–] **treebagz** 4 points 4 days ago

Carol from accounting is probably not writing her own client.....

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (1 reply)

load more comments (2 replies)

load more comments (10 replies)

[–] **-JamesBond** 3 points 4 days ago

Don’t worry the hypnotic state will give way to pure dread soon enough. Ask me how I know: lost 10 BTC

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **Rand_alThor_** 1 point 3 days ago

Story time?

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **Miljonars** 1 point 4 days ago

Good luck. Omg.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **gonzobon** 1 point 3 days ago

Can you post an update when/if this gets resolved?

Sorry for your loss. Hope something can be done.

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (7 replies)

[–] **gottagetminenow** 21 points 4 days ago

Do not attempt to do backups of your lnd directory, you are you most likely to have an old state and lose money just like this guy.

If your node fails then follow the guide from the lnd github and don't be afraid to ask for help. There is an LND slack.

https://github.com/lightningnetwork/lnd/blob/master/docs/recovery.md#recovering-using-scbs

permalink **embed** **save** **report** **give award** **reply**

load more comments (2 replies)

[–] **luke-jr** 7 points 3 days ago

This is like posting your wallet private keys on a pastebin service... PEBKAC

permalink **embed** **save** **report** **give award** **reply**

[–] **steuer2teuer** 24 points 4 days ago

So i guess the lesson here is: don't force close your channel from an unsynced backup. If you have sync problems or encounter errors seek help for it but do not force close.

I guess it works this way for a reason. If OP was nefarious he could've used this way to cheat/steal.

permalink embed save report give award reply

load more comments (5 replies)

[–] **InteractiveLedger** 12 points 4 days ago

what? how?

permalink embed save report give award reply

[–] **Rannasha** 50 points 4 days ago

From what I gather from the posted conversation: He closed a channel (or set of channels) using an outdated channel-state.

LN allows parties on either side of the channel to unilaterally close the channel by broadcasting a closing transaction to the network. Each party then gets their balance from that channel refunded. But with each lightning transaction you make, this closing transaction has to be updated to reflect the latest balance of the channel.

That means that a different version of the closing transaction exists (but isn't broadcast necessarily) for each lightning payment made on a channel. Now, this would allow someone to submit an outdated closing transaction. For example: I buy an item using LN to pay, but then submit the closing transaction from before the purchase, meaning I get the funds rather than the merchant. To discourage this, the system is designed so that when an outdated closing transaction is broadcast to the network, the other party can prove that they have a more recent closing transaction and claim all the funds in the channel. It's essentially a "don't cheat or you lose all your money" safeguard.

What apparently happened in this case is that the OP had to restore a backup for his system and this backup didn't contain the most recent closing transactions. So when closing the channel, the other parties were able to claim their full contents (this process can be automated, so it may not have been an active action of the counterparties to do this).

permalink embed save parent report give award reply

[–] **InteractiveLedger** 34 points 4 days ago

The "don't cheat or you lose all your money" feature is good as a safeguard, but it also acts as a double edged sword as the network doesn't recognize this as a human error. I think this is a common occurrence and maybe the LN devs can put a safeguard towards this 'feature'. It's bound to repeat itself, eventually.

permalink embed save parent report give award reply

[–] **vegarde** 18 points 4 days ago

He also had static channel backup, but did not properly do his research on how to use it, and/or the required patience.

Anyone that uses systems that developers says are only ready for early adoption should do their own research into how to properly use it.

My sympathy is somewhat limited, here.

permalink embed save parent report give award reply

[–] **dubblies** 5 points 4 days ago

Exactly. He was playing with experimental toys that he had too much money into. Its not like they said this is production ready and actually say the opposite.

permalink embed save parent report give award reply

[–] **ilpirata79** 10 points 4 days ago*

They should implement a real 100% safe backup solution. As of now, even if you backup every second you risk losing *all* your channel funds. The static channel backup could work, but it's not very detailed so I am not sure it is reliable 100% of time.

permalink embed save parent report give award reply

[–] **rabbitlion** 7 points 4 days ago

You only risk losing the funds if you force close channels though. Basically, you can do backups and you can restore backups, but you should be very careful about force closing channels after a restore and only do it if you are absolutely sure that you have the latest version (which is maybe impossible to determine).

permalink embed save parent report give award reply

[–] **next89** 6 points 4 days ago

WARNING: You restored the wallet within the last 24 hours. If you FORCE CLOSE the channel you may risk losing all your bitcoin. ARE YOU SURE YOU WANT TO PROCEED?

-Yes, I'm aware I can lose all my bitcoins.

-No

permalink embed save parent report give award reply

[–] **rabbitlion** 5 points 4 days ago

The problem is there's no time limit on this risk, so 24 hours isn't enough.

permalink embed save parent report give award reply

[–] **InteractiveLedger** 1 point 3 days ago

This is probably a good warning if you are somewhat technical or well versed in this sort of thing. But for the average person, this will be a disaster. But it's okay, problems like this will arise and we will at least know where we stand. Devs will (hopefully) see this as an issue and try to solve it.

permalink embed save parent report give award reply

[–] **bitusher** 3 points 4 days ago

Many wallets have this like eclair which autobackups to your google drive

permalink embed save parent report give award reply

load more comments (5 replies)

[–] **cqv** 1 point 4 days ago

This reminds me of the wallets that would generate random non-deterministic addresses. You had to update your backup so that the newly generated addresses were included.

permalink embed save parent report give award reply

[–] **Elum224** 8 points 4 days ago

Yes there is Eltoo, which requires an update on Bitcoin, it will make broadcasting of stale states harder to do by accident.

permalink embed save parent report give award reply

[–] **whitslack** 4 points 4 days ago

`SIGHASH_NOINPUT` for the win!

permalink embed save parent report give award reply

[–] **Quantris** 5 points 4 days ago

I think the safeguard is that "force" close is not the default. You have to explicitly ask for that, and before doing so it's your responsibility to figure out if that force close will look like "cheating" or not.

permalink embed save parent report give award reply

[–] **koenklaver** 3 points 4 days ago

But if you don't force close the channel is essentially locked from your perspective right? You cannot close it and are reliable on others to settle the channel. Is there a way to ask the network about a state of the channel?

permalink embed save parent report give award reply

[–] **whitslack** 5 points 4 days ago

> Is there a way to ask the network about a state of the channel?

Channel states are explicitly **not** public information, as that would completely destroy privacy.

permalink embed save parent report give award reply

[–] **--algo** 1 point 4 days ago

Also, a rogue actor could reply with an old state and then steal your funds by using their actual, newer state

permalink embed save parent report give award reply

[–] **Rand_alThor_** 1 point 4 days ago

So there is no way to know the state of the channel if you have to go from a backup?

permalink embed save parent report give award reply

load more comments (1 reply)

[–] **Quantris** 3 points 3 days ago

I'm not super familiar with latest implementations. I don't think there's an infallible way to ask the network (I think it's unavoidable that if you admit lacking knowledge, there's an incentive to lie to you).

Trying a cooperative close first would make sense though. Best case it goes through.

One point is that any channel update must have been signed by you. So in principle you could ensure this is logged / backed up before sending it out, s.t. you should be able to know if you have the most recent state or not. It's definitely a fair complaint if this isn't done for you by the software, though it's still beta software.

permalink embed save parent report give award reply

[–] **jonny1000** 3 points 4 days ago

I thought new versions of LND check the counterparty before closing a channel, to check if the other party has a later state. If both nodes are honest and the counterparty is online, the node won't broadcast an earlier state even if it lost the later state.

Is that not the case?

permalink embed save parent report give award reply

[–] **--algo** 5 points 4 days ago

> If both nodes are honest

???? what happened to trustless?

permalink embed save parent report give award reply

[–] **Rand_alThor_** 3 points 4 days ago

LN is not trustless

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (1 reply)

[–] **CatatonicAdenosine** 1 point 3 days ago

It's trustless if you have the latest state. If you lose it then you need to trust the counterparty not to broadcast an earlier state.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **jonny1000** 1 point 3 days ago

This is about when you lose a state you signed

Although even in that scenario, would the other party really risk broadcasting an older state? How do they know if you lost the latest state?

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (3 replies)

[–] **arahaya** 2 points 4 days ago

would this flow solve the problem?

> 1. when you run a close command your node asks your peer what his last state is.
> 2. if the state is different than your local state, you could then A) request your peer to close the channel.
> B) force close with your local state.

in the above case can your peer prove to you that his state is the valid one? or at least it is newer?

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **Rannasha** 8 points 4 days ago

This would work, but it relies on the peer being honest, which is an assumption that you don't want to make in a decentralized system like Bitcoin. Consider the following scenario:

> - I have a closing transaction version 4 from a backup.
> - Before closing the channel, I request my peer for the latest version and the peer replies 4 (or lower).

- Under the impression that I have the latest version, I broadcast the closing tx.
- But there is a version 5 of the closing transaction that the peer did not disclose. Upon seeing the channel being closed with an outdated closing tx, the peer proceeds to claim the entire channel contents.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **arahaya** 7 points 4 days ago

hmm, what could have OP done to prevent this?

could he have sent a milisatoshi transaction to create a new state (without knowing state 5)?
or did he need to just wait until his peers close their channels?

how about sending a "please close the channel from your end elsewise I will reject all transaction from you" request?

this seems like a new version of the Byzantine generals problem...

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **rabbitlion** 1 point 4 days ago*

- He could ask the peer for their latest state, but there's no guarantee that the peer will respond truthfully.
- He could ask the peer to close the channel from their end, but there's no guarantee that they'll comply.
- He could try to change the state of the channel. If he has the latest version, the peer will probably accept it, and then he'll know he has the latest version. If he doesn't, the peer will reject it, and then it's possible but not certain that he has an old state.
- ~~He could have waited until the channel timed out.~~

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **ilpirata79** 6 points 4 days ago

Channels never time out...

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **rabbitlion** 2 points 4 days ago

Hmm I was under the impression that you put some sort of an end date on the channel when opening it but I can't find anything about it now so it seems you are right.

So then there's no certain way to prevent things like this?

permalink embed save parent report give award reply

[–] **ilpirata79** 1 point 3 days ago

This has been somewhat discussed.

My opinion is that currently there is no 100% safe solution for nodes that want to route payments. Lnd is the least incomplete but it could still make you lose funds if on-flight HTLCs are lost.

Some wallets for end users should work well because they backup on Gdrive or Dropbox.

permalink embed save parent report give award reply

[–] **Rand_alThor_** 2 points 4 days ago

Wait so it wasn't even user error then? There's nothing he can do if the peer orchestrated or knew about the backup and wanted to take advantage of it?

permalink embed save parent report give award reply

[–] **rabbitlion** 1 point 3 days ago

It was user error, he shouldn't have tried to force close the channel like that. If the peer was uncooperative the money could have been locked forever, but not stolen. There's not much point in doing that for the peer though.

permalink embed save parent report give award reply

load more comments (1 reply)

load more comments (1 reply)

[–] **whitslack** 7 points 4 days ago

That's how `option_data_loss_protect` works. It relies on your peer being honest. If your peer is dishonest, then they can just tell you that your state is the most recent (a lie), then get you to unilaterally close the channel (easy to do), then broadcast their justice transaction to take all your money.

permalink embed save parent report give award reply

[–] **Rand_alThor_** 1 point 4 days ago

Should there be a way to close that can request a state from the peer and if both sides agree to that state, it can be closed, even if it wasn't the final state.

I guess there would be other things to work out but it stops one from being trapped and tricked. If the peer refused to send a state you at least know they are trying to fuck you.

permalink embed save parent report give award reply

load more comments (2 replies)

[–] whitslack 1 point 4 days ago

!bottle 500 sat

permalink embed save parent report give award reply

[–] bottlepay redditor for 3 months 1 point 4 days ago

Sweet tendies Batman! u/Rannasha you just received 500 sats from u/whitslack, claim them by activating your Reddit wallet 🚀

Bot Info | *Bottle Login* | *About* | *Feedback*

permalink embed save parent report give award reply

[–] Elum224 13 points 4 days ago

Thanks for posting the whole log. +Respect for bearing your mistakes for us to learn from.
It's a good lesson in making sure to read the manual and practicing with small amounts of money before committing huge funds into bitcoin.

permalink embed save report give award reply

[–] captkos 37 points 4 days ago

So you decided to start testing the LN with 4 BTC ?

permalink embed save report give award reply

[–] evilgrinz 6 points 4 days ago

First, no one is hiding this stuff, second there are tons of people you can talk to about this. If that is a big portion of your Bitcoin stack, that was really irresponsible. Don't burn bridges with people that you need help from. The state of LN is honest when your talking to devs, if your reckless with beta software that includes storing value, don't do it again.

permalink embed save report give award reply

[–] Hanspanzer 1 point 3 days ago

exactly

permalink embed save parent report give award reply

[–] BlankEris 6 points 4 days ago

Sorry for your loss but why would you put 4 BTC in the lightning network?

They explicitly state it's in beta and not to add any funds you're not willing to lose.

permalink embed save report give award reply

[–] zenethics 10 points 4 days ago

So, you tried to close channels using an old state? Ya, you can't do that dude. What you did is indistinguishable from someone trying to doublespend.

permalink embed save report give award reply

[–] blockocean 1 point 3 days ago

How can OP verify the channel state is old if he can only trust his peers not to lie about the state?

permalink embed save parent report give award reply

[–] zenethics 1 point 3 days ago

I'd need to go see what he was doing exactly. In my understanding of LN, he would need to sign every new transaction to invalidate old ones; so he'd know the most recent transaction because if he didn't, then the transaction didn't happen. Now if you lose your most recent transaction... then, ya, its kind of like losing your private keys. From skimming his transacript it sounds like he tried to use some kind of backup feature? Which, I don't know how that would work (and this is not me saying that it wouldn't).

permalink embed save parent report give award reply

[–] Mr--Robot 4 points 4 days ago

when watchtowers on every wallet/node?

permalink embed save report give award reply

[–] etmetm [ ] 3 points 4 days ago

Watchtowers did their job. When Eltoo, really

permalink embed save parent report give award reply

[–] arruah 4 points 4 days ago

18 months.

permalink embed save parent report give award reply

[–] etmetm [ ] 2 points 4 days ago

While 18 months seems to be a meme of the people unsupportive of LN trying to argue LN will never surface, 18 months may just be close to the actual timeline for Eltoo...

permalink embed save parent report give award reply

[–] dubblies 2 points 4 days ago

Eltoo would not have fixed this either. He broke into his own house and got arrested by the system he trusted to use. He literally cause his own breach of channel and lost the funds. He loaded up a backup FOLDER SET OF FILES and ran it. Dumb dumb dumb.

permalink embed save parent report give award reply

[–] **aenarion23** 5 points 4 days ago

Eltoo would have fixed this because you cannot lose money in the way he did.

permalink embed save parent report give award reply

[–] **dubblies** 3 points 4 days ago

I best read up eltoo then because I am clearly not informed. My mistake, thank you stranger. :)

permalink embed save parent report give award reply

[–] **etmetm** [ ] 1 point 4 days ago

!Intip 1000

permalink embed save parent report give award reply

[–] **aenarion23** 2 points 4 days ago

Thx

permalink embed save parent report give award reply

[–] **Intipbot** 1 point 4 days ago

Hi u/etmetm, thanks for tipping u/aenarion23 **1000** satoshis!

More info | *Balance* | *Deposit* | *Withdraw* | *Something wrong? Have a question? Send me a message*

permalink embed save parent report give award reply

load more comments (2 replies)

[–] **RustyReddit** 4 points 1 day ago

There are no penalty transactions anywhere near that time (checked blocks 600,000 to 601,000). So either you're still very confused about what's going on...

permalink embed save report give award reply

load more comments (1 reply)

[–] **LoneroLNR** 11 points 4 days ago

Welcome to the club of people who lost large amounts of crypto over ridiculous reasons!

permalink embed save report give award reply

[–] **erkzewbc** 4 points 3 days ago

It seems my lnd detected you had lost your channel states when you tried to reconnect on 2019-10-02, so it force-closed the channels, sending the balance back to your wallet.

So at least *that* wasn't so bad.

permalink **embed** **save** **report** **give award** **reply**

[–] **danbadjar** redditor for 3 weeks 5 points 3 days ago

Hello from BlackPearl public node here. You should backup your channels when the channels.backup is changed.

You can track that with: md5sum channels.backup

If the MD5 is changed then do backup.

In case of power fault don't use your old .lnd directory but I strongly suggest you to create a new one restoring from seed.

Only after that you can safely import your exported channels.

Tested some lnd versions ago. It has worked.

Sorry for your loss, man.

permalink **embed** **save** **report** **give award** **reply**

load more comments (2 replies)

[–] **BTCRedux** 7 points 4 days ago

Sorry to hear of your loss.

permalink **embed** **save** **report** **give award** **reply**

[–] **Spartan3123** 14 points 4 days ago

And this is why i use custodian LN wallet, with only 100 dollars on it. People claiming that everyone will have all your btc only on the LN are morons.

BTC in a BTC wallet will always be safer than an online LN wallet.

There were seriously and posts clamming everyone will use LN and whales and node operators make onchain txns every now and then. I want to slap these people across the face sometimes

permalink **embed** **save** **report** **give award** **reply**

[–] **Touchmyhandle** 2 points 4 days ago

Who knows what UX improvements will be made in the future, but for now it looks really bleak. LN seems like it's getting more and more complicated due to coders who are too smart to realise it's not what the market wants. Bitcoin is basically a failed tech if the only way to scale is on chain though.

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (5 replies)

load more comments (1 reply)

[–] **Aussiehash** 17 points 4 days ago

As far as I am aware

> The Lightning Network is still in development and currently limits individual channel capacity to 0.16 BTC

So sending 4 btc to lightning-casino.com, is gambling in more ways than one

permalink embed save report give award reply

[–] **igadjeed** 17 points 4 days ago

I read it as the OP runs this casino site and closed many channels all at the same time, total value 4BTC. The software has a close-all function
A lucky bonus for all the people on the other side of those channels

permalink embed save parent report give award reply

[–] **thesmokecameout** 2 points 4 days ago

It's an advertising expense, really. BRB, opening an account with lightning-casino.com!!!

Update: not even a real casino. :-(

permalink embed save parent report give award reply

[–] **castorfromtheva** 8 points 4 days ago

This. So whoever does something like that has: either not done *any* research before playin' around with *such* amounts... or 4 BTC means nothing to him as he owns dozen times this amount remaining.

permalink embed save parent report give award reply

[–] **spirit-receiver** 12 points 4 days ago

Also, the documentation is very clear that you'll lose your money if you publish old channel states. This probably falls in the 'not done any research' category.

permalink embed save parent report give award reply

[–] **ZipoTm** [S] 4 points 4 days ago

Sold my apartment and should work few years more to bring those money back... because some of them are not mine.

permalink embed save parent report give award reply

[–] **castorfromtheva** 3 points 4 days ago

Omg.

permalink embed save parent report give award reply

[–] **ilpirata79** 6 points 4 days ago

Sold an apartment for 4 bitcoins and you still need money? Cmon...

permalink embed save parent report give award reply

[–] **XavierFartboner** 4 points 4 days ago

crazy to think solving 30 captchas on some random faucet back in 2009 would eventually lead to buying an apartment outright in whatever country OP is from.

permalink embed save parent report give award reply

load more comments (2 replies)

[–] **Quintall1** 1 point 4 days ago

a 30.000 dollar apartement? can i maybe know your general area, i have some buildings to invest in

permalink embed save parent report give award reply

[–] **ZipoTm** [S] 10 points 4 days ago

It was based in Stara Zagora, Bulgaria

permalink embed save parent report give award reply

[–] **BullRun03** redditor for 5 weeks 1 point 3 days ago

Seriously? You just force closed on a whim with funds which weren't just gravy you had laying around but belonged to other people? WTF.

permalink embed save parent report give award reply

load more comments (1 reply)

[–] **_Filip_** 1 point 4 days ago

He says that he owns that node and for whatever reason he had to close all channels he had open (presumably with punters).

permalink embed save parent report give award reply

[–] **chairoverflow** 3 points 4 days ago

bud does the money still exist? like in the other channel party was credited or it went into fees etc.

permalink embed save report give award reply

[–] **Elum224** 10 points 4 days ago

The other person receives the funds.

permalink embed save parent report give award reply

[–] **chairoverflow** 3 points 4 days ago

TYVM

permalink embed save parent report give award reply

load more comments (2 replies)

[–] **etmetm** [ ] 9 points 4 days ago

This is one reason why we need Eltoo...

From what I understand with Eltoo watchtowers will be more important then, as there's more incentive to try and cheat but there will be no penalty just correction of balances.

permalink embed save report give award reply

[–] whitslack 4 points 4 days ago

The importance of watchtowers is frankly way overstated. Turn on your node once every two weeks for a few minutes. Done. No need for watchtowers.

permalink embed save parent report give award reply

[–] fresheneesz 1 point 4 days ago

Watchtowers are for more than just watching for old state - they're state backups as well.

permalink embed save parent report give award reply

[–] pardus79 2 points 4 days ago

No they are not. Watchtowers are not given any channel info. They are not given any channel state information.

"The watchtower stores fixed-size, encrypted blobs and is only able to decrypt and publish the justice transaction after the offending party has broadcast a revoked commitment state."

permalink embed save parent report give award reply

[–] fresheneesz 1 point 4 days ago

> Watchtowers are not given any channel info.

Well, I'll ignore that the "justice transaction" is channel info. Regardless of that, the justice transaction is the state backup I'm talking about. I don't believe there is any important data for restoring your node other than your justice transaction (representing the current channel balance) and your private key (which can be backed up once on creation, and so doesn't have backup issues).

permalink embed save parent report give award reply

[–] pardus79 2 points 4 days ago

A justice transaction only sends all the funds in the channel to your side, not closing the channel based on the most recent channel state. When you use a watchtower, you're telling them to look for a transaction on the blockchain with a particular hash (you don't give them the transaction details, only a hash, for privacy reasons) and if they see it, they can decrypt the blob and publish the justice transaction. A justice transaction does not have channel state info at all. It only says "send ALL the funds to me". So a watchtower is not a channel backup source.

Also, even if watchtowers stored the channel states, it would be just as dumb to rely on them to have the most up to date channel balance as it would be to trust your .lnd folder backup to (like this dude did). If the watchtower gave you an out of date channel state, you would lose your funds trying to force close from it.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **fresheneesz** 1 point 3 days ago

> A justice transaction only sends all the funds in the channel to your side, not closing the channel based on the most recent channel state.

Fair point.

> it would be just as dumb to rely on them to have the most up to date channel balance as it would be to trust your .lnd folder backup to

Its dumb to rely on *any* single location. Redundant backups are what's needed. If you have one on your machine and your drive dies or gets corrupted, then you can go to your watchtower (or wherever else).

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (8 replies)

load more comments (2 replies)

[–] **fresheneesz** 3 points 4 days ago

I'm really hoping we get to a solution where the incentive not to cheat is at least the transaction fee the cheater forced their channel partner to pay. No punishment at all is insecure because it incentivizes attempted theft as a numbers game (force close 1000 channels with old state expecting 1 will fail to correct).

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **etmetm** [ ] 3 points 4 days ago

Thanks, I had not considered this yet! I'd too hope fees are sufficient to deter cheating attempts with Eltoo.

From my understanding you can still employ breach based channel security for the channels you open like today if you feel it's better in terms of the risks involved. I'd hope the same would be true for channels opened to your node, that you have a choice which type of remedy actions to support.

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **klondikecookie** 2 points 16 hours ago

Currently LND doesn't do penalty. If you run an old invalid state, your channels would just be closed and you don't lose your coins. Try it on Testnet to see. Unless you do some hackery stuff then maybe

> the penalty would kick in. But someone who "accidentally" or "cluelessly" runs an old invalid state is probably not someone who knows how to cheat.

permalink **embed** **save** **parent** **report** **give award** **reply**

load more comments (4 replies)

[–] **e3ee3** 6 points 4 days ago

You tried to take money out enforcing an outdated contract. By the rules you lose the money. Lightning Network cannot tell whether it was intentional or not.

permalink **embed** **save** **report** **give award** **reply**

[–] **HodlOnToYourButts** 6 points 4 days ago*

In the future follow a **STRICT** hierarchy:

> - Development - run BTC / LND in "simnet" mode. Generate your own blockchain. Limit access to developer(s) only. Test your code, backups, new features, patches, etc here first. Breaking something here loses you nothing and is easy to flush data directories and start over.
> - Testing - run BTC / LND in "testnet" mode and "beta" test your software with a small group of vetted users. Test your code, backups, new features, patches, etc here **AFTER** they work on "simnet". Breaking something here loses you time, but not money, and your testers will help you discover bugs before they become problems.
> - Production - run BTC / LND in "mainnet" - **AFTER** testing your code, backups, new features, patches, etc on **BOTH** "simnet' and "testnet" you may run your code on "mainnet" with real money.

Lightning is still in **beta** and some improvements are still in **alpha**. To limit exposure treat a lightning wallet like you would any "hot" wallet. Keep the wallet balance to a minimum to limit exposure. Investigate using Lightning Loop to move your BTC from off-chain lightning channels to on-chain cold wallet and back again when a withdrawal is requested.

Complaining about getting wet when your ignored the warnings and sat in the "splash" zone is childish.

"Evolution forged the entirety of sentient life on this planet using only one tool… The mistake." -Dr. Robert Ford (Westworld - HBO)

P.S. This is coming from someone who lost over 4.5 BTC betting on pig races in BitVegas about 6 years ago. So yea...

permalink **embed** **save** **report** **give award** **reply**

[–] **wsheep** 10 points 4 days ago

#reckless

permalink embed save report give award reply

[–] **BeTeeC** redditor for 3 months 13 points 4 days ago

Maybe, but is that how we respond to people who've lost a lot of money? I was enraptured by bitcoin for its ability to protect people's value. Of course this is not Bitcoin's fault, but I still don't think it's very appropriate to rub salt into a fresh wound.

You do you.

permalink embed save parent report give award reply

[–] **Mccawsleftfoot** 16 points 4 days ago

#reckless is a meme. Elizabeth Stark coined the phrase to discourage people from putting their bitcoin on mainnet lightning.

We've all heard the warnings. If you have 4 BTC on LN, you're either very wealthy and very reckless, or very stupid and very reckless.

With bitcoin fees this low there's really no reason to use lightning. It's still got a way to go to prevent things like this in the future.

permalink embed save parent report give award reply

[–] **etmetm** [ ] 2 points 4 days ago

While you're right that LN still has way to go - there ARE reasons to use LN.

!Intip 1000 - onchain fees are larger than that.

permalink embed save parent report give award reply

[–] **Intipbot** 1 point 4 days ago

Hi u/etmetm, thanks for tipping u/Mccawsleftfoot **1000** satoshis!

More info | *Balance* | *Deposit* | *Withdraw* | *Something wrong? Have a question? Send me a message*

permalink embed save parent report give award reply

[–] **pinkwar** 4 points 4 days ago

ITT closing channels with an old state makes you lose your money.

That's the mechanism they use to avoid malicious closing of channels. It has been known for years.

I'm sorry you lost so much.

permalink embed save report give award reply

[–] **E-renter** 30 points 4 days ago*

I'm sorry but I have to say f*** the Lightning Network. I will never lock more than a couple Satoshi's in there just for experimentation purposes until this s*** gets sorted. shit like that should just not be possible with a couple of built in commands and hit the enter key bye-bye 4 BTC. Oh and somehow it is OP's fault because there was a power outage. Ridiculous.

"moli 1 hour ago so the backup is a few days old? even a few *minutes* or hours old , they can cause a breach, that's how it is"

P.s. What a worthless "backup" system.

permalink embed save report give award reply

[–] **calaber24p** 14 points 4 days ago

If he had asked anyone working on the lightning they all would have told him to not test with that amount. Each of the developers have been very upfront in saying we're still in pre alpha and there is a ton of work to do. He acted recklessly without knowing how the software even worked.

This is the equivalent of someone posting their private key instead of public key and claiming its bitcoins fault and that bitcoin is stupid.

permalink embed save parent report give award reply

[–] **gottagetminenow** 26 points 4 days ago

You do not backup the lnd directory, EVER. If the node fails you use the channel.backup file to recover your funds.

This guy was using his own backup scheme and he got burned.

permalink embed save parent report give award reply

[–] **eightyWon** 5 points 3 days ago

This. That whole conversation was frustrating as shit to read because the were both talking past each other. If someone would have just said what you just said, the issue would have been so much more clear.

permalink embed save parent report give award reply

load more comments (2 replies)

[–] **only_merit** 25 points 4 days ago

guy used tech he did not understand, with all warnings everywhere that it's still experimental and yet he put 4 BTC in it. and you say it's the tech's fault? you kidding? use Electrum and create anyone can spend tx and propagate it and then claim you lost money because of stupid Electrum? ffs grow up

permalink embed save parent report give award reply

[–] **vakeraj** 17 points 4 days ago

Reddit is full of people that complain more about Lightning than actually learning and gaining experience with it.

permalink embed save parent report give award reply

load more comments (5 replies)

[–] BullRun03 redditor for 5 weeks 3 points 3 days ago

`--force` = *"I really really want to do this thing you just warned me against, I fully accept the risks as I know what I'm doing and have decided that I wish to force this"*

permalink embed save parent report give award reply

load more comments (1 reply)

[–] Trrwwa 11 points 4 days ago

You could have easily said the same thing about btc 5 years ago. People still will cmd line swap the fee and the amount, and the funds are gone.

It's not ready for users to make quick moves without thinking. That's what happened here

permalink embed save parent report give award reply

load more comments (18 replies)

[–] BashCo 3 points 3 days ago

That's a pretty dumb takeaway to be honest. It shows a real lack of understanding and foresight. Even worse, some people upvoted such a dumb statement. We have a long ways to go.

permalink embed save parent report give award reply

load more comments (1 reply)

load more comments (5 replies)

[–] Hanspanzer 2 points 3 days ago

"how I lost 4 BTC on the Bitcoin network"

1) typed wrong address
2) lost keys
3) lost phone, no seed backup
4) PC hacked
5) you name it

honestly the warnings are out there to not use LN with high amounts as it is still experimental. backups are still an issue. also you must use customized software to have capacity of 4 BTC, so you should know what your are doing. #reckless meme ftw

permalink embed save report give award reply

[–] ilpirata79 2 points 3 days ago

Posted yesterday, what a coincidence:

https://www.reddit.com/r/btc/comments/dllqlf/incredible_no_safe_way_to_backup_ln_funds/

permalink **embed** **save** **report** **give award** **reply**

[–] **DarthCoinMaster** 3 points 3 days ago

oh, what a coincidence... your are posting about LN on bcash sub... trying to troll here bcasher?

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **ilpirata79** 1 point 3 days ago

no

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **CONTROLurKEYS** 2 points 3 days ago

Yeah who doesn't keep 4btc in a hot wallet /s

permalink **embed** **save** **report** **give award** **reply**

[–] **BullRun03** redditor for 5 weeks 2 points 3 days ago

`--force`

nuff said.

I `rm -rf /` all the time!

permalink **embed** **save** **report** **give award** **reply**

[–] **-johoe** 2 points 2 days ago

It looks like my node forced-closed the channel from my end when you connected with the old channel state. Your part of the channel (~0.00037 BTC) is still unclaimed in an address only you control. Maybe the same is true for most of the other missing funds.

You may need some additional key information from my node to claim it. I'm not sure how to extract this, though (or if I still have it; is it part of the static channel backup?).

permalink **embed** **save** **report** **give award** **reply**

load more comments (1 reply)

[–] **treebagz** 8 points 4 days ago

It's almost as if the Lightning Network is still in development and the OP should have limited the amount of Bitcoin they put on it.

permalink **embed** **save** **report** **give award** **reply**

[–] **niamhyd** 6 points 4 days ago

this is why BTC is, at this moment in time, a purely speculative asset and I don't believe you can be a SOV without utility. Whilst these factors are in place the long term outlook is not good for BTC. A crisis in

the fiat financial system is needed to get the price back to 20k. Otherwise it's only a matter of time before enough people realise that the emperor has no clothes.

permalink **embed** **save** **report** **give award** **reply**

[–] **Alqpzmyv** redditor for 3 months 1 point 3 days ago

This is an issue with OP's misuse of the lightning network. The main bitcoin network is entirely safe. Use large sums of money over a beta feature at your own risk

permalink **embed** **save** **parent** **report** **give award** **reply**

[–] **TotesMessenger** 3 points 4 days ago*

I'm a bot, *bleep*, *bloop*. Someone has linked to this thread from another place on reddit:

- [/r/bitcoincashsv] More examples of users losing money on LN: "How I lost ~4 BTC on Lightning Network"
- [/r/btc] 4 BTC lost on the lightning network
- [/r/buttcoin] Butter loses 4 BTC supporting Lightning Network
- [/r/cryptoandme] #crypto #cryptonews #bitcoin @nocroom #4 BTC lost on the lightning network
- [/r/cryptocurrency] 4 BTC lost on the lightning network
- [/r/cryptocurrency] How I lost ~4 BTC on Lightning Network
- [/r/cryptocurrency] One of the biggest Lightning Network node operators (LIGHTNING-CASINO.COM) looses 4 BTC after a short power outage.
- [/r/dashpay] Holy! Claim of 4 BTC lost thus far on Lightning Network. Glad Dash has not taken the LN path.
- [/r/ggcrypto] 4 BTC lost on the lightning network
- [/r/nanotrade] LN is the future /s

If you follow any of the above links, please respect the rules of reddit and don't vote in the other threads. (Info / Contact)

permalink embed save report give award reply

[–] David4Neblio 3 points 4 days ago

Where do the lost Bitcoin go?

permalink embed save report give award reply

[–] luke-jr 2 points 3 days ago

Either random peers or mining fees.

permalink embed save parent report give award reply

load more comments (1 reply)

[–] throwawayagin 4 points 4 days ago

Don't put 4btc on lightning yet.

permalink embed save report give award reply

[–] luke-jr 4 points 3 days ago

Or at least don't ask your Lightning wallet to burn it all...

permalink embed save parent report give award reply

[–] throwawayagin 1 point 3 days ago

Hey Luke. I wanted to ask you about stg mind if I pm?

permalink embed save parent report give award reply

[–] luke-jr 1 point 3 days ago

go for it

permalink embed save parent report give award reply

[–] ilpirata79 2 points 4 days ago*

It is crazy that no proper backup solution exists, if not *probably* for LND. That should be the most important thing.

I advise not to run any LN node at the moment if this thing is not sorted out.

permalink embed save report give award reply

[–] etmetm [ ] 10 points 4 days ago

There is: https://github.com/lightningnetwork/lnd/blob/master/docs/recovery.md

There are some DO and DON'Ts when it comes to recovery though. It's an involved procedure.

You must not recover using a copied backup file of the database otherwise what happened to OP may happen.

You can however recover using so called SCBs which you can also backup as a file.

permalink embed save parent report give award reply

[–] ilpirata79 2 points 4 days ago*

I suppose that if you do use SCBs and you also use an external watchtower (that would activate if your peers, having seen that you crashed, try to force close on an old state), things should work.

p.s. The only doubt I still have is related to in-flight HTLCs that could still in theory make you lose all channel funds.

permalink embed save parent report give award reply

[–] Placebo17 1 point 4 days ago

Why do people use LN again?

permalink embed save report give award reply

[–] Raster_Eyes 18 points 4 days ago

For instant transactions that don't require confirmations and near zero fees

permalink embed save parent report give award reply

load more comments (6 replies)

[–] [deleted] 4 days ago*

[deleted]

[–] luke-jr 5 points 3 days ago

Sounds like he tried to claim an old state, which means he'd end up with more bitcoins than he had a right to. So the other side of all the channels would then automatically block it by claiming everything for themselves (as is intended to occur when someone breaches).

permalink embed save report give award reply

[–] blockocean 2 points 3 days ago*

So theoretically you could just ddos one of your peers continuously to prevent them from learning about the current state and hope they try and force close out of frustration.

permalink embed save parent report give award reply

[–] luke-jr 2 points 3 days ago

Your state can't be changed without your node's cooperation and consent...

permalink embed save parent report give award reply

[–] johnturtle 1 point 4 days ago

I am very sorry that this happened to you, I hope you manage to recover your funds. Are going to continue with your lightning casino? It was one of the most upvoted stores at

https://lightningnetworkstores.com/

permalink embed save report give award reply

[–] SecureUpgradesOnly redditor for 1 week 1 point 4 days ago

Why don't you have a backup if above a certain amount the user selects if there is a change of state, or auto backup if change of state?

Or something like that, would that make sense?

permalink embed save report give award reply

[–] ilpirata79 1 point 4 days ago

That work for a lot of cases, but what happens if:

1) New state is saved on the disk

2) New state is sent to the peer

3) Computer crash orribly corrupting the disk

4) no backup has been made of the new saved state on the disk

permalink embed save parent report give award reply

[–] SecureUpgradesOnly redditor for 1 week 1 point 4 days ago

I don't know about LN. If it ever took off, I am aware then a solution would have to be figured out to prevent mass settlement around the same time, affecting the chain.

permalink embed save parent report give award reply

[–] luke-jr 1 point 3 days ago

Encrypt the backup (with a key you CAN make a normal backup of) and ensure it's saved to a remote host before committing to the new state.

permalink embed save parent report give award reply

[–] ilpirata79 2 points 3 days ago

Sure but currently no implementation does this.

permalink embed save parent report give award reply

[–] [deleted] 3 days ago

[removed]

load more comments (1 reply)

[–] MartyDevs 1 point 3 days ago

why and how are bitcoins are lost lightning and where do they go lel?

permalink embed save report give award reply