

Forum:[Hack Forums](#)

Thread: [My Zcash Experience](#)

Omniscient - January 8, 2026, 3:18 pm

My Zcash Experience (Why I'm Done With It)

In April, I noticed Zcash starting to gain serious momentum, both in price action and social media hype.

At the time, it was trading around \$30. It eventually ran past \$700, and as of today sits around \$425.

Given the hype, I figured it was worth actually using Zcash instead of just watching the chart.

For context, I've used Monero for years and consider it a real privacy coin. It works, it's reliable, and privacy is not optional. I assumed Zcash would offer something comparable. I was very wrong.

Zcash "privacy" is optional (and that's the problem)

For anyone unfamiliar, Zcash privacy is not default. It's optional.

Privacy only exists when using shielded addresses. While funds are in shielded addresses, transactions and balances are private. Sounds good in theory.

Here's the catch:

I could not find a single KYC exchange that supports shielded deposits. If you want to interact with exchanges, your ZEC must be moved to a transparent address, completely breaking privacy.

Some exchanges support shielded withdrawals, which is a small plus, but the moment you want liquidity, privacy is gone.

Wallet hell begins

I started looking for a Windows desktop wallet that supports shielded addresses.

I was recommended zecwallet.co, except the site has been offline for weeks. There is a zecwallet.com, but I strongly recommend not installing it. It was buggy, failed to run properly in a Linux VM, and my antivirus flagged it. I also have no idea who operates it.

At that point, someone in Convo pointed me to the Brave Wallet. I already used Brave, but didn't realize it supported shielded ZEC. It does, but only after enabling it in settings.

Unfortunately, the experience was still bad:

Shielded balance took a long time to appear

You cannot send from shielded to transparent

Syncing and balance updates were slow and inconsistent

So now I needed another wallet just to move my own funds.

Android wallets: even worse

Since desktop options were failing, I moved to Android wallets.

Nighthawk was the first one I tried:
Could receive shielded ZEC

Balance took forever to sync

Wallet constantly glitched

Send transactions failed

One failed transaction took 12 hours to clear and return the balance

At this point, I had \$50 stuck in a wallet I couldn't spend from.

Next, I tried YWallet:
Looked better initially

Still wouldn't send from shielded to transparent

Imported my Nighthawk seed

Waited 24 hours for balance to sync

Balance never appeared

Finally, I tried Zashi:
Imported the same seed

Correct balance appeared within 30 minutes

Shielded -> transparent transaction worked

I was able to recover my stuck funds back into Brave

Final outcome

Today, I moved all my ZEC to an exchange and traded it for BTC.

My conclusion: Zcash is terrible to actually use.

Optional privacy is a joke

Wallet ecosystem is unreliable

Sync times are absurd

Balance delays are constant

You often need multiple wallets just to move your own money

Can Zcash be used privately? Sure, technically.

Is it practical? Not at all.

It is nowhere near the reliability or usability of Monero.

I'm done with it.

Thanks for reading.

Mewtwo - January 8, 2026, 4:07 pm

It's interesting to note whether traceability is even possible with ZEC. One way for sure is timing and amount once it becomes transparent again. Also, Zcash privacy pool seems to be small, so it makes it a lot more easier for forensics to trace.

Mandatory privacy for all transactions is what will make a blockchain fully anonymous.

Omniscient - January 8, 2026, 4:12 pm

(Jan 8, 2026 05:07 PM)Mewtwo Wrote: [\[CITE\]](#) It's interesting to note whether traceability is even possible with ZEC. One way for sure is timing and amount once it becomes transparent again. Also, Zcash privacy pool seems to be small, so it makes it a lot more easier for forensics to trace.

Mandatory privacy for all transactions is what will make a blockchain fully anonymous.

Zcash has Elliptic Risk Assessment Levels. The good news is that's why it's on exchanges. The bad news is that privacy is lost.

Monero has not a single crypto blockchain analysis company that can do AML risk scores. That's all I really need to know.

SUI-3183372 - January 8, 2026, 10:20 pm

Just missed ya

StuffSneak - January 8, 2026, 11:26 pm

Thank you for sharing the experience. Optional Privacy while sounds great to be honest, so many restrictions on real world use make it undesirable.

Mewtwo - January 9, 2026, 5:19 am

(Jan 8, 2026 05:12 PM)Omniscient Wrote: [\[CITE\]](#) Zcash has Elliptic Risk Assessment Levels. The good news is that's why it's on exchanges. The bad news is that privacy is lost.

Monero has not a single crypto blockchain analysis company that can do AML risk scores. That's all I really need to know.

DAC8 just started rolling out in the EU. Basically it's mandatory reporting on exchanges, offline wallets, freezing assets on exchanges if audits don't match. I think this is going to pressure a lot of folks to start using XMR and DEX to avoid the stress of DAC8 entirely.

? sentient ? - January 9, 2026, 5:46 am

(Jan 9, 2026 06:19 AM)Mewtwo Wrote: [\[CITE\]](#) DAC8 just started rolling out in the EU. Basically it's mandatory reporting on exchanges, offline wallets, freezing assets on exchanges if audits don't match. I think this is going to pressure a lot of folks to start using XMR and DEX to avoid the stress of DAC8 entirely.

The crypto part isn't just EU. DAC8's crypto tax transparency framework is basically equivalent to CARF which is the worldwide equivalent pushed by OECD.

IMO it's extremely bad bad and I'll describe exactly why in an hypothetical scenario.

If say, you're hypothetically buying drugs from a friend, and send them a bank transaction then it's relatively private.

If you send him 50\$ from a custodial wallet or exchange, they have your KYC and will report it to your tax domicile, which will learn that you sent 50\$ from your account.

If he received it in a custodial wallet or exchange, they'll know he received 50\$ as well.

They'll basically know everything. Deposits, withdrawals, transactions, crypto-to-crypto conversions, etc. It's way worse than a regular banking account where only the balance would be reported under CRS.

This applies to everything.

So CARF/DAC8 effectively completely ends privacy. It's actually interesting that Omni hasn't touched this subject, though [he's the first](#) (and you the second) person to mention it AFAIK.

It's even more dystopian for EU's DAC8 since it extends to e-Money as well (think Paypal, Wise and others), as long as you have over 10,000\$ on average there, these e-Money accounts are basically equivalent to bank accounts under DAC8 and subject to regular bank CRS as well.

And while this has no immediate consequences, since data recording only started January 1, 2026 and submission only starts in 2027, obviously whatever you do in custodial platforms in 2026 will be reported in 2027, which is 1 year from now.

Mewtwo - January 14, 2026, 12:53 pm

<https://www.theblock.co/post/385629/zcash-foundation-says-sec-has-closed-book-on-years-long-pro>

[be](#)

I wonder if this is the true reason why the team left. Maybe they were pressured to do this by the USA

Omniscient - January 15, 2026, 9:29 am

(Jan 14, 2026 01:53 PM)Mewtwo Wrote: [\[CITE\]](#)

<https://www.theblock.co/post/385629/zcash-foundation-says-sec-has-closed-book-on-years-long-probe>

I wonder if this is the true reason why the team left. Maybe they were pressured to do this by the USA

I kind of think not but maybe it has something to do with the timing. Maybe the team needed the money people for lawyers and once this was settled they felt comfortable leaving. Who knows. I just think Zcash doesn't have a future against Monero with the experience I've had using ZEC.

Siipi - January 28, 2026, 1:58 am

Why don't you just stick with Zashi and use shielded pool with Njalla, for example, and trade via ShapeShift? Transparent transactions don't matter if you use shielded pool and Tor to hide transaction history.

The Electric Coin Co left due to the removal of grants to Electric Coin Co and Zcash Foundation. They started a new company and apply for community grants from the lockbox of all users and Zcash Community Grants. Now the reserch and development isn't linked to a central company but to the community. Anyone can participate and apply for grants. Also, mining pools don't bring centralization as the nodes decide which miners to trust and the zk-proofs show if there's something wrong with transactions.

Omniscient - January 28, 2026, 9:29 am

(Jan 28, 2026 02:58 AM)Siipi Wrote: [\[CITE\]](#) Why don't you just stick with Zashi and use shielded pool with Njalla, for example, and trade via ShapeShift? Transparent transactions don't matter if you use shielded pool and Tor to hide transaction history.

The Electric Coin Co left due to the removal of grants to Electric Coin Co and Zcash Foundation. They started a new company and apply for community grants from the lockbox of all users and Zcash Community Grants. Now the reserch and development isn't linked to a central company but to the community. Anyone can participate and apply for grants. Also, mining pools don't bring centralization as the nodes decide which miners to trust and the zk-proofs show if there's something wrong with transactions.

Doesn't that also seem like a lot more work than just using Monero? The fact that there are so few good wallets that support Zcash is alarming to me. Even worse is they are mobile apps. Sorry but zero trust for anything on a phone coming from app stores.

I can run Monero CLI from a VMware Linux install with Tor super easily. Zero need for third parties and very secure.

DragonModded - January 28, 2026, 7:51 pm

(Jan 8, 2026 04:18 PM)Omniscient Wrote: [\[CITE\]](#) My Zcash Experience (Why I'm Done With It)

In April, I noticed Zcash starting to gain serious momentum, both in price action and social media

hype.

At the time, it was trading around \$30. It eventually ran past \$700, and as of today sits around \$425

Given the hype, I figured it was worth actually using Zcash instead of just watching the chart.

For context, I've used Monero for years and consider it a real privacy coin. It works, it's reliable, and privacy is not optional. I assumed Zcash would offer something comparable. I was very wrong.

Zcash "privacy" is optional (and that's the problem)

For anyone unfamiliar, Zcash privacy is not default. It's optional.

Privacy only exists when using shielded addresses. While funds are in shielded addresses, transactions and balances are private. Sounds good in theory.

Here's the catch:

I could not find a single KYC exchange that supports shielded deposits. If you want to interact with exchanges, your ZEC must be moved to a transparent address, completely breaking privacy.

Some exchanges support shielded withdrawals, which is a small plus, but the moment you want liquidity, privacy is gone.

Wallet hell begins

I started looking for a Windows desktop wallet that supports shielded addresses.

I was recommended zecwallet.co, except the site has been offline for weeks. There is a zecwallet.com, but I strongly recommend not installing it. It was buggy, failed to run properly in a Linux VM, and my antivirus flagged it. I also have no idea who operates it.

At that point, someone in Convo pointed me to the Brave Wallet. I already used Brave, but didn't realize it supported shielded ZEC. It does, but only after enabling it in settings.

Unfortunately, the experience was still bad:
Shielded balance took a long time to appear

You cannot send from shielded to transparent

Syncing and balance updates were slow and inconsistent

So now I needed another wallet just to move my own funds.

Android wallets: even worse

Since desktop options were failing, I moved to Android wallets.

Nighthawk was the first one I tried:
Could receive shielded ZEC

Balance took forever to sync

Wallet constantly glitched

Send transactions failed

One failed transaction took 12 hours to clear and return the balance

At this point, I had \$50 stuck in a wallet I couldn't spend from.

Next, I tried YWallet:
Looked better initially

Still wouldn't send from shielded to transparent

Imported my Nighthawk seed

Waited 24 hours for balance to sync

Balance never appeared

Finally, I tried Zashi:
Imported the same seed

Correct balance appeared within 30 minutes

Shielded -> transparent transaction worked

I was able to recover my stuck funds back into Brave

Final outcome

Today, I moved all my ZEC to an exchange and traded it for BTC.

My conclusion: Zcash is terrible to actually use.
Optional privacy is a joke

Wallet ecosystem is unreliable

Sync times are absurd

Balance delays are constant

You often need multiple wallets just to move your own money

Can Zcash be used privately? Sure, technically.

Is it practical? Not at all.

It is nowhere near the reliability or usability of Monero.

I'm done with it.

Thanks for reading.

lol, you actually wasted that much time to figure out something that 99 percent of people could have figured out on their own, so was it manipulated up? or are people just mentally ill for saying and thinking that? btw i knew about the uselessness of shielded addresses without even touching it

Mewtwo - September 4, 2026, 3:33 pm

Zcash is now above \$1000. Is it going to surpass 5K ATH?