

Forum:[Hack Forums](#)

Thread: [Privacy Coins](#)

Omniscient - November 26, 2025, 10:28 am

Who had Privacy Coins as their 2025 Bingo Card crypto that was gonna moon?

NFT's...NOPE

Smart Contracts...NOPE

High TPS...NOPE

It's Privacy Coins.

ZEC up 500% YTD (actually just 60 days)

XMR up 300% YTD

DASH up 200% YTD

I'm actually fairly pleased with the market. Although I think it's all manipulation that started with Zcash but ultimately brought attention to Monero.

SUI-3183372 - November 26, 2025, 11:33 am

Perps and Privacy have emerged as H2's winning narratives.

Perps made sense to me, and while a few specific platforms haven't done well, generally if you were invested in the perps space, you made off very well.

What made less sense was privacy coins. ZEC, XMR, RAIL all had really solid years, especially H2 of this year, and there was seemingly no catalyst for this. There was no global movement towards privacy, there wasn't any major event that created a demand for heightened privacy awareness, these coins pumped out of no where.

I fully support privacy coins, they serve a great purpose and I will advocate for them always. That being said, my stance on them as investments has not changed. Governments and centralized entities will always view privacy coins as a threat, there will always be a war waged against privacy coins, and all privacy coins risk being deplatformed at a moment's notice, which creates a perpetual risk for these coin's price action. For this reason alone I do not consider them to be safe investments, and I don't hold any for investment purposes. I wholeheartedly support those who utilize these coins, and those who disagree with my investment stance and made a nice profit off H2's pump, congrats on your wins, couldn't have happened to better coins.

Omniscient - November 26, 2025, 11:38 am

(Nov 26, 2025 12:33 PM)SUI-3183372 Wrote: [\[CITE\]](#) Perps and Privacy have emerged as H2's winning narratives.

Perps made sense to me, and while a few specific platforms haven't done well, generally if you were invested in the perps space, you made off very well.

What made less sense was privacy coins. ZEC, XMR, RAIL all had really solid years, especially H2 of this year, and there was seemingly no catalyst for this. There was no global movement towards privacy, there wasn't any major event that created a demand for heightened privacy awareness,

these coins pumped out of no where.

I fully support privacy coins, they serve a great purpose and I will advocate for them always. That being said, my stance on them as investments has not changed. Governments and centralized entities will always view privacy coins as a threat, there will always be a war waged against privacy coins, and all privacy coins risk being deplatformed at a moment's notice, which creates a perpetual risk for these coin's price action. For this reason alone I do not consider them to be safe investments, and I don't hold any for investment purposes. I wholeheartedly support those who utilize these coins, and those who disagree with my investment stance and made a nice profit off H2's pump, congrats on your wins, couldn't have happened to better coins.

There are many countries pushing for tracking. Especially Europe where I can't get a Coinbase payment without the member knowing my business name and what the payment is for. In my view, there is a reason for Privacy Coins being attractive to crypto bros who are having their privacy invaded and maybe it's making enough of them uncomfortable that measures are being taken. As the world pushes for transparency, I think a countering towards privacy is going to happen.

Aadgjmptw72 - November 26, 2025, 11:43 am

Privacy coins imo have been undervalued for a long time. Glad to see them going up.

SUI-3183372 - November 26, 2025, 11:46 am

(Nov 26, 2025 12:38 PM)Omniscient Wrote: [\[CITE\]](#) There are many countries pushing for tracking. Especially Europe where I can't get a Coinbase payment without the member knowing my business name and what the payment is for. In my view, there is a reason for Privacy Coins being attractive to crypto bros who are having their privacy invaded and maybe it's making enough of them uncomfortable that measures are being taken. As the world pushes for transparency, I think a countering towards privacy is going to happen.

Law enforcement, governments, web2 tech giants, many financial institutions, and other centralized entities will be motivated to never allow that to become a reality, and that's what scares me away from this vertical as an investor. Bitcoin can't be stopped, banks and govs tried for a while and failed. Privacy preserving coins though, the war is far from over, there will be many more attacks against specific coins and the privacy vertical in general before it either emerges as unstoppable or it gets beaten into the ground. XMR, ZEC, TORN, etc aren't going anywhere, they're here to stay, but I do fear for their token values as they take on attacks from different angles.

I'm aligned in your desire to see this happen though, privacy has always been a very appealing topic for me and I have attempted to employ privacy preserving tactics in just about everything that I do in life.

Btc to 0 - November 26, 2025, 11:57 am

What do you guys think about COTI gem ?

Respect - November 26, 2025, 11:59 am

I've been heavily invested in privacy coins since about 2019, glad they are finally getting the attention they deserve, whether it's manipulation or not!

Smart Contracts are fantastic as well, but it's always been a longer time horizon for those, as theres alot of other pieces that need to fall into place first with regards to bringing banking & traditional finance into the 21st century.

Things like Chainlink will have their day, but that day is not now nor is it soon. Likely 2030+

Popular - November 26, 2025, 2:33 pm

(Nov 26, 2025 12:43 PM)Aadgjmptw72 Wrote: [\[CITE\]](#) Privacy coins imo have been undervalued for a long time. Glad to see them going up.

Yea, and tbh it sucks to admit but I remember laughing with some friends and telling myself privacy coins wont do shiiiiiiiit, and now I'm like :(<.< >.>

Omniscient - November 26, 2025, 3:38 pm

I actually think a full delisting of XMR on all KYC CEX's would help Monero value immensely.

MOE - November 26, 2025, 5:47 pm

(Nov 26, 2025 11:28 AM)Omniscient Wrote: [\[CITE\]](#) Who had Privacy Coins as their 2025 Bingo Card crypto that was gonna moon?

NFT's...NOPE
Smart Contracts...NOPE
High TPS...NOPE

It's Privacy Coins.

ZEC up 500% YTD (actually just 60 days)
XMR up 300% YTD
DASH up 200% YTD

I'm actually fairly pleased with the market. Although I think it's all manipulation that started with Zcash but ultimately brought attention to Monero.

I was not surprised, there was a lot of fake news circulating about ZEC being the bitcoin 2.0 for the past weeks on all social media platforms basing it on whitepapers/screenshots taken from the past, there was also people trying to link Satoshi to being also behind ZEC/this was the future for "bitcoin". Also to be honest, privacy coins are still a force to be reckoned with...especially ZEC/XMR.

Could also be just a signal for another bull run, or just some tactic to get people to sell their bags with FOMO. Time will tell all, but at least those coins have use. Happy for anyone that profited on those coins.

Truth - November 26, 2025, 9:59 pm

The best privacy coin is actually already in the top 10(minus stables) its Bitcoin Cash(BCH) with cash fusion.

people are really sleeping but BCH has been stable in the top ~10ish since it pretty much started, was the last coin to flip ETH and will do it again.

These other coins are hot for a minute, come quote me in a year or 2 when they are out of the top 20 forgotten onto the new thing

stdio - November 26, 2025, 10:14 pm

I remember buying ZEC below 100\$ and riding all the way to 500\$ and this was many many years ago (2016-2017), since then it's been tanking.. This appears to be whales manipulating the price to rid of their bags.

XMR is solid tech though, would always be holding this dearly in case the government turn on us.

Mewtwo - November 27, 2025, 7:52 am

I got my Monero hat, both from 2018 and a new one in 2025. I've always been a supporter for Monero. Even places I've been to, like Seattle, it's nice to see a sticker on a pole that says "use

#monero, it's the people's money".

We don't need institutions to invest into XMR. Neither do we need anyone to know how much assets we hold, or where it's been sent. Why should a bank or crypto website care about someone who's gambling? Or uses it on the dark web?

Omniscient - November 27, 2025, 10:15 am

(Nov 26, 2025 10:59 PM)Truth Wrote: [\[CITE\]](#) The best privacy coin is actually already in the top 10(minus stables) its Bitcoin Cash(BCH) with cash fusion.

people are really sleeping but BCH has been stable in the top ~10ish since it pretty much started, was the last coin to flip ETH and will do it again.

These other coins are hot for a minute, come quote me in a year or 2 when they are out of the top 20 forgotten onto the new thing

I disagree that using Cash Fusion with BCH is the way to go. It's like walking into a bank with a mask on. They know you're up to no good. Using Mixers, immediately puts your Risk Level to severe. Your KYC exchange account will be closed. That's not privacy, it's just obfuscation. Monero is privacy, they can't even do risk level assessments, which is why KYC exchanges can't accept it.

Mixers aren't the solution because it only proves someone is going out of their way to hide origins. Raises masses suspicions. Now if a chain had Coinjoin as part of the protocol that would be different. If it was required and part of every transaction. But then again, we already have Monero so what's the point of all those extra UTXO's to hide origin?

Monero is the only one I have found that is a real privacy coin by default, no other option, no tricky settings or particular wallets.

SUI-3183372 - November 27, 2025, 10:53 am

(Nov 26, 2025 10:59 PM)Truth Wrote: [\[CITE\]](#) The best privacy coin is actually already in the top 10(minus stables) its Bitcoin Cash(BCH) with cash fusion.

people are really sleeping but BCH has been stable in the top ~10ish since it pretty much started, was the last coin to flip ETH and will do it again.

These other coins are hot for a minute, come quote me in a year or 2 when they are out of the top 20 forgotten onto the new thing

Ah, the "I hedge my btc 1:1 with BCH and BSV" man. How's that been working out for you? Craig make you rich yet?

First time I've seen you not shill BSV to us like we're idiots though, props for that.

oh dear

Omniscient - November 27, 2025, 11:06 am

(Nov 27, 2025 11:53 AM)SUI-3183372 Wrote: [\[CITE\]](#) Ah, the "I hedge my btc 1:1 with BCH and BSV" man. How's that been working out for you? Craig make you rich yet?

First time I've seen you not shill BSV to us like we're idiots though, props for that.

oh dear
You forgot about Bitcoin Gold.

i am - November 27, 2025, 6:13 pm

Hate to be that guy, but yes I saw it coming and have been shilling these as investments for years. As the broader economy deteriorates and the world becomes less stable the black market tends to grow. As government overstepping against privacy grows, more and more black market capital will move onto these coins and drive them up.
I will be continuing to quietly dollar cost average these for the next several years.

Truth - November 27, 2025, 8:27 pm

(Nov 27, 2025 11:15 AM)Omniscient Wrote: [\[CITE\]](#) I disagree that using Cash Fusion with BCH is the way to go. It's like walking into a bank with a mask on. They know you're up to no good. Using Mixers, immediately puts your Risk Level to severe. Your KYC exchange account will be closed. That's not privacy, it's just obfuscation. Monero is privacy, they can't even do risk level assessments, which is why KYC exchanges can't accept it.

Mixers aren't the solution because it only proves someone is going out of their way to hide origins. Raises masses suspicions. Now if a chain had Coinjoin as part of the protocol that would be different. If it was required and part of every transaction. But then again, we already have Monero so what's the point of all those extra UTXO's to hide origin?

Monero is the only one I have found that is a real privacy coin by default, no other option, no tricky settings or particular wallets.

its a snap of a finger to get BTC/BCH/BSV to have privacy by default, anything of value will be added to the main chain. Its all open source software and can be forked in a second.

shitcoins are like someone making a man-made metal and telling you hey buy their man-made metal instead of gold. Bitcoin was the discovery like gold, everything else is pretty much a hustle or sham.

Monero, zcash, sol, eth, etc are pretty cool tech, just like stainless steel can be a cool metal, will I look at it like I want to invest into it the same way as gold? not a chance.

Gold is ~\$30T marketcap and only one chain actually can compete at that level. Its always been Bitcoin or bust.

I will still ride a few pump and dumps along the way. Looks like the zcash one is on its dump stage, but the idea I would hold any of these long term, nah, Bitcoin only. All my other holdings I am looking for an exit, not trying to be a bag holder. Only Bitcoin consistently makes new ATH. People rave about the privacy pump but they haven't even made new all time highs lol what kind of pump is that. Tell me when they are 4-5x previous cycle ATH like Bitcoin then I will give credit to the pump.

Anyways, as always, we'll see in a few years.

(Nov 27, 2025 11:53 AM)SUI-3183372 Wrote: [\[CITE\]](#) Ah, the "I hedge my btc 1:1 with BCH and BSV" man. How's that been working out for you? Craig make you rich yet?

First time I've seen you not shill BSV to us like we're idiots though, props for that.

oh dear

The funny thing is Satoshi himself also didn't sell any of his forks, still holding them 1:1 for whatever reason

BCH doing decent but BSV is obviously delisted on pretty much all US & major exchanges so its always been less likely to pump.

I actually dont mind BSV under \$20, I will be buying some and if it gets under \$10 that would be pretty decent buy too. Its just lunch/dinner money at that point lol

with my BTC/BCH holdings too, I dont care as much how BSV does, but, I always support what the Bitcoin whitepaper calls "Competing chains"

Unless they change the parameters like bitcoin gold or eCash, then no its no longer Bitcoin imo. It should always be a 1:1 fork/airdrop to all Bitcoin holders.

Anyways, I call it the Satoshi portfolio, we'll see how it does in a year or 2, feel free to post your portfolio.

pro0 - November 28, 2025, 11:28 am

Monero really looks like the future. More people are switching to privacy-focused OS on their laptops and phones, and with all the new government censorship and laws, privacy coins are going to become even more important. On the other hand, the people behind Zcash and all the marketing around it just feel a bit suspicious compared to Monero's grassroots approach.

Mewtwo - December 4, 2025, 4:33 am

Saw this video today

Just proves XMR will always be the KING. They can't trace anything with XMR.

SIM-3107656 - December 4, 2025, 10:42 pm

(Dec 4, 2025 05:33 AM)Mewtwo Wrote: [\[CITE\]](#)

Saw this video today

Just proves XMR will always be the KING. They can't trace anything with XMR.

They can't "seize" BTC. Only if they have keys or access. XMR has no advantage over BTC in this matter. Only in publicity of txs happening. BTC is superior.

Omniscient - December 5, 2025, 3:22 pm

(Dec 4, 2025 11:42 PM)SIM-3107656 Wrote: [\[CITE\]](#) They can't "seize" BTC. Only if they have keys or access. XMR has no advantage over BTC in this matter. Only in publicity of txs happening. BTC is superior.

Wrong.

They can forensically link your wallet to KYC exchanges. They know your BTC address. They

know that addresses activity and balance.

With XMR, even if I deposit XMR into a KYC exchange, guess what, they don't even know my XMR address it was sent from. That's PRIVACY.

Massive difference.

AI Quote: Short answer: No. The receiving wallet does not know your sending address when you send XMR.

Here's why:

? Monero's design hides the sender

Monero uses one-time stealth addresses, ring signatures, and confidential transactions, which together make it impossible for the receiver to know your actual sending address.

What the receiving wallet does see*:

That it received XMR. The amount (only the receiver knows this, not the public).
The one-time stealth address created for the transaction.

What the receiving wallet does NOT see*:

Your sender address. Any link to your wallet.
Your balance or transaction history. The ring members' identities.

? How Monero hides the sender

When you send XMR:

- 1. Your wallet creates a ring signature that mixes your output with several decoy outputs.
- 2. It generates a unique, one-time stealth address for the receiver.
- 3. The blockchain only shows:

A group of possible signers (the ring)
A stealth output

None of this links back to your wallet address.

? Can the receiver *ever know who sent the XMR?

Only if you tell them outside the blockchain.
There is no on-chain proof of the sender unless you voluntarily share your tx private key, which is optional and normally used only for support or verification.

? Summary

Question	Answer
Does the receiver know my Monero address?	No
Can they see my wallet balance or history?	No

| Can they identify the sender from the transaction? | No |
| Can I reveal I sent it? | Only by sharing the tx private key manually |

If you want, I can also explain:

How view keys work

How exchanges detect incoming XMR How to prove payment to someone without revealing your wallet

Whether outgoing transactions leak anything to the receiver

Just let me know!

Snowyy - December 5, 2025, 3:52 pm

(Dec 5, 2025 04:22 PM)Omniscient Wrote: [\[CITE\]](#) Wrong.

They can forensically link your wallet to KYC exchanges. They know your BTC address. They know that addresses activity and balance.

With XMR, even if I deposit XMR into a KYC exchange, guess what, they don't even know my XMR address it was sent from. That's PRIVACY.

Massive difference.

AI Quote: Short answer: No. The receiving wallet does not know your sending address when you send XMR.

Here's why:

? Monero's design hides the sender

Monero uses one-time stealth addresses, ring signatures, and confidential transactions, which together make it impossible for the receiver to know your actual sending address.

What the receiving wallet does see*:

That it received XMR. The amount (only the receiver knows this, not the public).
The one-time stealth address created for the transaction.

What the receiving wallet does NOT see*:

Your sender address. Any link to your wallet.
Your balance or transaction history. The ring members' identities.

? How Monero hides the sender

When you send XMR:

1. Your wallet creates a ring signature that mixes your output with several decoy outputs.

- 2. It generates a unique, one-time stealth address for the receiver.
- 3. The blockchain only shows:

A group of possible signers (the ring)
A stealth output

None of this links back to your wallet address.

? Can the receiver *ever know who sent the XMR?

Only if you tell them outside the blockchain.

There is no on-chain proof of the sender unless you voluntarily share your tx private key, which is optional and normally used only for support or verification.

? Summary

Question	Answer
Does the receiver know my Monero address?	No
Can they see my wallet balance or history?	No
Can they identify the sender from the transaction?	No
Can I reveal I sent it?	Only by sharing the tx private key manually

If you want, I can also explain:

How view keys work

How exchanges detect incoming XMR How to prove payment to someone without revealing your wallet

Whether outgoing transactions leak anything to the receiver

Just let me know!

Its awesome how Monero works, sad to see that more exchanges aren't accepting deposits via blockchain anymore though.

Omniscient - December 5, 2025, 4:07 pm

(Dec 5, 2025 04:52 PM)Snowyy Wrote: [\[CITE\]](#) Its awesome how Monero works, sad to see that more exchanges aren't accepting deposits via blockchain anymore though.

I disagree. Monero doesn't need CEX's. It's the People's Crypto IMHO. Exchanges have often done nothing but cause problems.

Snowyy - December 5, 2025, 8:11 pm

(Dec 5, 2025 05:07 PM)Omniscient Wrote: [\[CITE\]](#) I disagree. Monero doesn't need CEX's. It's the People's Crypto IMHO. Exchanges have often done nothing but cause problems.

That's fair, I'm talking about people who are newer into crypto who want ease of access to put funds in their external wallet. If you can't deposit that crypto, likely you can't withdraw it either.

SIM-3107656 - December 7, 2025, 8:28 am

(Dec 5, 2025 04:22 PM)Omniscient Wrote: [\[CITE\]](#) Wrong.

They can forensically link your wallet to KYC exchanges. They know your BTC address. They know that addresses activity and balance.

With XMR, even if I deposit XMR into a KYC exchange, guess what, they don't even know my XMR address it was sent from. That's PRIVACY.

Massive difference.

AI Quote: Short answer: No. The receiving wallet does not know your sending address when you send XMR.

Here's why:

? Monero's design hides the sender

Monero uses one-time stealth addresses, ring signatures, and confidential transactions, which together make it impossible for the receiver to know your actual sending address.

What the receiving wallet does see*:

That it received XMR. The amount (only the receiver knows this, not the public).
The one-time stealth address created for the transaction.

What the receiving wallet does NOT see*:

Your sender address. Any link to your wallet.
Your balance or transaction history. The ring members' identities.

? How Monero hides the sender

When you send XMR:

1. Your wallet creates a ring signature that mixes your output with several decoy outputs.
2. It generates a unique, one-time stealth address for the receiver.
3. The blockchain only shows:

A group of possible signers (the ring)
A stealth output

None of this links back to your wallet address.

? Can the receiver *ever know who sent the XMR?

Only if you tell them outside the blockchain.
There is no on-chain proof of the sender unless you voluntarily share your tx private key, which is optional and normally used only for support or verification.

? Summary

Question	Answer
Does the receiver know my Monero address?	No

Can they see my wallet balance or history?	No
Can they identify the sender from the transaction?	No
Can I reveal I sent it?	Only by sharing the tx private key manually

If you want, I can also explain:

How view keys work

How exchanges detect incoming XMR How to prove payment to someone without revealing your wallet

Whether outgoing transactions leak anything to the receiver

Just let me know!

IDK what does CEX have to do with private keys. Even tho if they leave KYC CEX to addy, even if they know addy, they only know public key. Cannot seize it without private key... ? They cannot lock it as USDT / USDC and many other coins. It is superior blockchain in this matter. Monero is same but extra, anonymity in blockchain itself has nothing with "seize"-ability. So no clue what are you trying to achieve by mixing CEXes into this conversation. BTC itself has no kyc or XMR. That's on you.

Omniscient - December 8, 2025, 12:31 pm

[SIM-3107656](#)

You stated BTC is superior (over Monero).

My argument is that because of the privacy of addresses this is not true. Because I can interact with a CEX under Monero and I would get way more privacy than I would if I used Bitcoin.

You can use a CEX with Monero all day long and it does nothing to your ability to remain private.

TehHaxx - December 12, 2025, 4:00 pm

Does anyone mind making me a TL'DR guide on how to purchase HODL and sell XMR as anonymously as possible, purchasing it both via Fiat and crypto

Omniscient - December 12, 2025, 4:05 pm

(Dec 12, 2025 05:00 PM)TehHaxx Wrote: [\[CITE\]](#) Does anyone mind making me a TL'DR guide on how to purchase HODL and sell XMR as anonymously as possible, purchasing it both via Fiat and crypto

Once you have XMR, it's anonymous. So how you get it, is mostly irrelevant.