Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

Alleged Coinomi exploit shows how easy it is to have Bitcoin stolen (decryptmedia.com)

131 points by timcc50 on Feb 27, 2019 | hide | past | favorite | 171 comments

rory096 on Feb 27, 2019 | next [–]

To *Google Chrome's* spellchecker. It's a bad vulnerability, but it's unlikely that it's really the attack vector here.

GuB-42 on Feb 27, 2019 | parent | next [–]

Official response by Coinomi

https://medium.com/coinomi/off…

Summary: Yes, there was a bug, we fixed it, but it was not exploitable in practice for a variety of reasons. Most importantly, the seed phrase wasn't being transmitted in plain text.

Veen on Feb 27, 2019 | parent | prev | next [–]

Right. The "thief" would have to be extremely lucky to have been intercepting the right data, recognized what the key was, and used it. As mentioned in the story, I suspect this chap found the vulnerability and is hoping to parlay it into a payout.

cjbprime on Feb 27, 2019 | root | parent | next [–]

No, more than that: assuming the connection to the spell checker uses TLS, the thief would have to *be Google*.

I'd be surprised if it doesn't use TLS?

hackinthebochs on Feb 27, 2019 | root | parent | next [–]

There was another instance of a massive coin theft a year or so ago and the weak link again was the recovery seed being sent to a Google server. The guy described his operational security and it seemed like he did everything right. The only slip up he could point to was that he had mistakenly pasted his seed into his Chrome address bar (which then performs an automatic lookup). It was shortly after that when his funds were drained.

I'm certainly not saying it was someone at Google, but it would be a mistake to not consider them an adversary in the battle to secure your funds.

781 on Feb 27, 2019 | root | parent | next [–]

A ton of people use GMail for their crypto accounts.

Claiming that someone at Google stole the funds is quite an extraordinary claim. You should have more proof than just the seed being sent to their spellchecker.

hackinthebochs on Feb 27, 2019 | root | parent | next [–]

I'm not sure what the volume of gmail accounts is supposed to demonstrate. But gmail is known to be high value, and so it stands to reason that internal safeguards around access to gmail accounts would be much greater than data from a spellcheck API or search autocomplete.

It certainly is an extraordinary claim, but there does come a point where the totality of evidence points to the likelihood of it. I'm not saying we're at that point, but in my mind we've reached the point of reasonably possible.

lilyball on Feb 28, 2019 | root | parent | next [–]

Spellcheck API or autocomplete is also expected to end up with a *ton* of sensitive information sent to it. I would expect them to either not keep logs of the actual query strings to begin with, or heavily restrict access to them.

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

dontbenebby on Feb 27, 2019 | root | parent | prev | next [–]

So, I'm not super familiar with crypto/blockchain beyond reading a couple academic papers but... how can you use it "offline"?

I saw someone in the parent comments mention that using your phrase on a machine connected to the internet can be risky... how can you make use of those coins then? Do you download some onto a usb to manually transfer over?

hackinthebochs on Feb 27, 2019 | root | parent | next [–]

You identify yourself to the network as the legitimate owner of an address by signing a transaction with a private key for that address. So using your coins offline involves signing your transaction using a computer that is air-gapped and then manually transferring the signed transaction to the online computer to be pushed to the network. There are user friendly ways of doing this using QR codes and similar things.

dontbenebby on Feb 28, 2019 | root | parent | next [–]

Thanks for the explanation.

cjbprime on Feb 27, 2019 | root | parent | prev | next [–]

That's the weak link they knew about. It is very unlikely to be the actual weak link.

gcbw2 on Feb 27, 2019 | root | parent | prev | next [–]

or wait for google to "anonymize" the data and release it internally for their researchers.

jakevoytko on Feb 27, 2019 | root | parent | prev | next [–]

The thief in that case would likely be a browser extension

cjbprime on Feb 27, 2019 | root | parent | next [–]

It's a desktop app.

ceejayoz on Feb 27, 2019 | parent | prev | next [–]

Yeah. This is pretty far-fetched.

> He argues that Coinomi's built-in spell checker automatically checked his seed phrase which involved sending it as plain text to a Google-owned website. This meant it could have been intercepted, leading to the loss of funds.

"As plain text" here almost certainly means "fully encrypted with TLS"...

cabaalis on Feb 27, 2019 | root | parent | next [–]

I felt like you did, and watched the video and he is certainly looking at an HTTPS data stream.

I think the argument though is that the request is being logged and that some employee is reviewing logs and grabbing data.

If that is the case, then it seems there is a known pool of suspects to charge with theft...

ceejayoz on Feb 27, 2019 | root | parent | next [–]

Yeah, and the amount of data to sift through there would be truly enormous.

I'd wager there was just some malware on the machine.

SketchySeaBeast on Feb 27, 2019 | root | parent | next [–]

Apparently it's a list of 12 words from 2048. I guess you could potentially try and pattern match that, but that'd be a ton of a sifting.

Phlarp on Feb 27, 2019 | root | parent | prev | next [–]

The amount of data to sift through? What website am I on right now? Just grep for 64 character strings.

The regex is so simple I think it a little naive not to assume _someone_ has a script running to sniff out keys. It would be trivial for an ISP employee to watch for such strings in unencrypted traffic streams. Think what cloudflare could find if they went looking.

ceejayoz on Feb 27, 2019 | root | parent | next [–]

The stream *isn't* unencrypted, though. Chrome's cloud spellchecker sends over HTTPS, for obvious reasons. (It's also an opt-in feature.)

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

I strongly suspect grepping against inbound production traffic to Google's spellcheck service is fairly difficult to do unnoticed.

Malware, on the other hand, is quite prevalent. Plenty of folks lose their crypto on a daily basis in that manner.

▲ Phlarp on Feb 27, 2019 | root | parent | next [–]

Sure, but think of how porous this could be even with HTTPS-- it doesn't have to be a google admin grepping inbound traffic. It could be happening with a custom installed certificate for a workplace or university network or it could be happening with a third party service or API behind HTTPS termination. Even something trivial like analytics could potentially leak this info. Malware is certainly a possibility, but it could just as easily have been phished or grabbed with an XSS.

▲ tbodt on Feb 28, 2019 | root | parent | prev | next [–]

Access to this data is very tightly controlled, it's likely a single digit number of people.

▲ sofaofthedamned on Feb 27, 2019 | parent | prev | next [–]

Exactly. There's billions of entries there each day, it's just symptomatic of bad secops where the spellchecker upload is the canary for other rank stupidity.

▲ tzumby on Feb 27, 2019 | parent | prev | next [–]

Why in the world would they need a spell checker when the whole mnemonic phrase standard has a checksum (last word in every phrase is the checksum)

▲ wcoenen on Feb 27, 2019 | root | parent | next [–]

The Android EditText control has this enabled by default, and the documentation of the control doesn't mention it:

https://developer.android.com/r…

To disable it, the developer needs to add the "textNoSuggestions" flag to the input type.

▲ ccnafr on Feb 27, 2019 | prev | next [–]

It's not an exploit. It's a vulnerability baked in the wallet app source code. There's a difference.

The article seems to have been written by someone who has a poor grasp on security terms.

I'd recommend reading the researcher's write-up and avoid getting the wrong idea of what's happening there: https://www.avoid-coinomi.com/

▲ Dirlewanger on Feb 27, 2019 | parent | next [–]

Yup, not saying that if Coinomi was open source this wouldn't have happened...but, chances are someone would have caught this if it was.

▲ AgentME on Feb 27, 2019 | root | parent | next [–]

All I can think is who the hell even uses a closed source cryptocurrency wallet? I'm not completely an open source purist in all places, but if there's ever a place to be one, it's in cryptocurrency. You'd think people that wanted to hold money that they didn't trust to banks wouldn't then trust that money to a random unreviewed app.

It frustrates me that unfamiliar people are going to see this article (or ones about random fly-by-night exchanges running away with deposits) and just come away thinking this type of problem is an unavoidable part of cryptocurrency, which it's not. Maybe it is for people who don't do their research, but I'm not telling them to use cryptocurrency. I hate that whenever there's talk about cryptocurrency, these amateur cases dominate the conversation. It'd be like if every time the act of camping was brought up, people were aghast and talked about how unsafe camping is and how it's a horrible thing because of how some family died camping recently (after they went camping in the middle of the desert without supplies).

▲ ryanlol on Feb 27, 2019 | root | parent | prev | next [–]

Why would access to the source have helped here? Presumably the code responsible for this is buried deep within some library they're using for the text field.

It seems rather likely to me that something like this would never be spotted by looking at the source, you'd have to analyze the application at runtime.

▲ wcoenen on Feb 27, 2019 | prev | next [–]

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

If I were a security consultant, I would be a bit more hesitant about telling the world that I casually entered a seed phrase worth $60K into an online device, never mind which software it was. The report mentions that the seed phrase originally came from his exodus wallet (desktop software), which is also a wallet that is not suitable for storing such large amounts.

For those amounts, use a hardware wallet, or software that supports generating the transactions offline so that the device with the key never has to go online.

▲ hombre_fatal on Feb 27, 2019 | parent | next [–]

I've been the victim of social-engineering attacks for less.

If you know someone holds cryptocurrency, doesn't hurt to attack their AWS account in case they are running bitcoind on EC2.

▲ updateYourMind on Feb 27, 2019 | parent | prev | next [–]

Can someone who finds your hardware wallet use it to sign tx? I'm guessing there is a PIN.

▲ hanniabu on Feb 27, 2019 | root | parent | next [–]

Yes, there is a pin and usually a limit to attempts. Ledger has a 3 attempt limit and then it'll reset the device. You can retrieve your funds by entering a 23 word mnemonic phrase that was generated when first setting up the ledger (and keys).

▲ Zenbit_UX on Feb 27, 2019 | root | parent | next [–]

24 word

▲ paraxisi on Feb 27, 2019 | prev | next [–]

The video in the article essentially shows nothing; the claim is "Google stole my coins."

Possible? Sure. Likely? No.

The corroboration with the two users from Reddit is useless because they didn't use a seed phrase.

edit/ To clarify: Yes, this is a stupid practice. You should be doing this locally or ideally not at all. But thinking Google is stealing your coins is a pretty big stretch.

▲ 40acres on Feb 27, 2019 | prev | next [–]

Decentralized currency is simply not viable for the mainstream, an economy needs institutions that can be relied upon and a certain level of centralized control to take the wheel when things go sour. There are still gains to be made via speculation but the dreams of folks like Nick Szabo will not be realized with crypto in its current state.

▲ hanniabu on Feb 27, 2019 | parent | next [–]

Everyone on here seems to be very bitter and salty about this stuff and I'm not sure why they're not seeing the bigger picture. This is probably the same group that would have laughed at predictions that there would be personal computers.

As the technology improves, all this stuff will be abstracted from the user. There are ongoing experiments to solve this issue such as a way to store your keys in a decentralized manner in case it is lost. This can be combined with the ability to automatically move funds to different accounts periodically and also to keep funds spread across different accounts. The UX will come and the are many efforts working on this. It just takes time.

▲ ChicagoBoy11 on Feb 27, 2019 | root | parent | next [–]

I think the claim is the more this infrastructure gets built out, the more players need to enter to make it workout, the bigger the footprint and calls to regulate it get, etc. will certainly make it a more functional system for the end user but also will bring about the same thing we dislike about current financial systems that involve lots of intermediaries, regulations, etc.

You have to argue that this maturation process will not be plagued by the sorts of issues that our very mature regular banking system is. And that's not a certainty.

▲ anyfoo on Feb 27, 2019 | root | parent | prev | next [–]

> Everyone on here seems to be very bitter and salty about this stuff and I'm not sure why they're not seeing the bigger picture. This is probably the same group that would have laughed at predictions that there would be personal computers.

That first sentence is a great way to start an argument. And having been there for the rise of the PC, I do not agree with your analogy. Just like with the Internet analogy that usually comes up, the problem with PCs was more getting one. PCs were very expensive, cryptocurrencies are plenty available to anyone

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

who wants them. There were skeptics with PCs, but still people jumped readily at every use case opportunity that presented itself and constantly came up with new ones. The blockchain is trying to find them for years and years now.

As for the abstraction: Well, yeah, you abstract the whole "cryptocurrency" aspect away to make it work, until you may as well just use the proven, regular banking system. And then to allow for such regular processes as litigation or the simple undoing of human mistakes, you abolish the "immutable ledger" concept entirely.

Am I bitter and salty about it? Given that cryptocurrencies are now consuming more energy than all solar panels combined, singlehandedly erasing the progresses we made there: Yes, definitely.

▲ dreamcompiler on Feb 28, 2019 | root | parent | prev | next [–]

> As the technology improves, all this stuff will be abstracted from the user.

I'm not optimistic. We still have an Internet on which it's basically impossible for a non-expert user to reliably send or read encrypted email.

▲ hanniabu on March 1, 2019 | root | parent | next [–]

I believe this is done on purpose because it's not in the company's interests to have your data encrypted. There's no incentive for them to make it easier. It's certainly possible though.

▲ anjc on Feb 27, 2019 | prev | next [–]

Between people losing their keyphrase, to software wallets being hacked, to hardware wallets being compromised...at what point is it more safe to just keep your coins on a reputable, insured, exchange? I think the odds of Coinbase doing a Mt. Gox are a lot more slim than the odds of a random person screwing up their own storage solution.

▲ AgentME on Feb 27, 2019 | parent | next [–]

>to hardware wallets being compromised

The only hardware wallet compromises I've heard of still required someone to have physical access to the device. If you can keep the device in your possession, it's still much safer than any of the alternatives.

▲ dontbenebby on Feb 27, 2019 | prev | next [–]

Why would you spell check a password? Passphrases are in vogue, but a field whose very mature is to be high entropy probably doesn't conform to traditional spelling/grammar...

▲ api on Feb 27, 2019 | prev | next [–]

Why does a *spell checker* need to live in the cloud?

To harvest user text for marketing analytics of course. Never mind.

▲ tzumby on Feb 27, 2019 | parent | next [–]

In the context of wallet word seeds you are correct. The dictionary is a 2048 word list that is standardized. If you want to spell check that you can roll something offline. Furthermore, the whole phrase has a checksum step so you'll know if you got one of the words wrong after you're done inputting the words.

▲ SketchySeaBeast on Feb 27, 2019 | parent | prev | next [–]

You NEED live updates for spellcheck, or you'll end up with a bunch of red squigglies every time you try and write "bingeable" or "rando".

▲ api on Feb 27, 2019 | root | parent | next [–]

So you click "learn." Done. This has been a solved problem since the 1980s.

Dictionary updates are also tiny and local storage is gigantic compared to the size of even a massive multi-language dictionary. This is just total nonsense.

▲ SketchySeaBeast on Feb 27, 2019 | root | parent | next [–]

Yeah, sorry, that didn't come through in my text, it IS a ridiculous scenario.

▲ api on Feb 27, 2019 | root | parent | next [–]

Ahh! Yeah, your sarcasm went *whoosh*. :)

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

netsharc on Feb 27, 2019 | parent | prev | next [–]

Probably because it remains very up-to-date without the difficulty of distributing giant dictionaries as updates (well, obviously new words can be delivered as diffs to existing offline dictionaries).

But yeah, if you have access to the world's repository of [something], it's very interesting to see who wants to find out about that thing. Like people editing Sarah Palin's Wikipedia page days before she was announced in 2008. Or Apple forbidding use of Google in their office, because hey, imagine if there's a spike of Google searches for a specific chip or technology from a particular Cupertino IP, and someone is watching.

Or if you control people's communication media and can see who's messaging who, with what frequency, and what content (Hello Mark!).

Filligree on Feb 27, 2019 | parent | prev | next [–]

To harvest spelling for the use of the spellchecker. Why would you manually build a database of correct spellings when the spellchecker already sees all of them?

Arnt on Feb 27, 2019 | parent | prev | next [–]

"Never attribute to anything else that which you can attribute to malice", right?

In this case my first guess would be the database and deployment. That spell checker supports three hundred and umpty-seven languages, right? And I've heard it's based on the words from Google's web index, which I imagine some people might be happy mirroring on their phone but others not.

Just guessing.

api on Feb 27, 2019 | root | parent | next [–]

Normally I agree with that principle, but in the case of surveillance capitalism I've learned it's often the opposite. Any excuse whatsoever to hoover customer data to feed into marketing analytics is taken, with few exceptions. It's become the primary business model of the Internet and of consumer-oriented computing. Consumer oriented Internet services that do not productize the user are the exception.

Things like mobile apps and cloud-based assistance services are guilty unless proven innocent and I only use them if the value proposition is so high that the cost/risk is acceptable. I also try to limit their permissions as much as I can.

I tried Grammarly for five minutes. It was cool, but I dropped it when I realized that its business model was obvious. It was uploading every single thing I typed into anything to the mothership. Not only is this invasive as hell but it's also a *massive* security vulnerability. I don't feel like having my company's bank accounts emptied because someone hacks Grammarly or a disgruntled employee dumps the database and sells anything that looks like an account number on the dark web.

RodgerTheGreat on Feb 27, 2019 | root | parent | next [–]

I was aghast the first time I encountered Grammarly; it's an immense security risk, and services like it prey upon the ignorance of end users.

I've had conversations with a number of my coworkers who deal with sensitive (PII) data about the plugin. None had realized it was phoning home to do its work, and in every instance so far they've uninstalled it immediately afterward.

VikingCoder on Feb 27, 2019 | parent | prev | next [–]

"Jake Gyllenhaal". The words people are spelling changes all of the time.

yingw787 on Feb 27, 2019 | prev | next [–]

I still don't get cryptocurrencies. Yes, a blockchain works when zero trust is needed/desired for transactions, but that's still an implementation-level concern, and implementations aren't perfect. Without legal means of redress, somebody is always going to get burned. If there are legal means of redress, then by definition you trust somebody, right?

I think a blockchain fits well when you need to verify a legal authority, like a felonies database (can you trust the cop that filed the report?), but otherwise it kind of just goes around the legal system; by doing so, you're just re-inventing the wheel.

andrewla on Feb 27, 2019 | parent | next [–]

Why would you say that there's no legal means of redress? If someone steals my cryptocurrency, then I can still have law enforcement track them down and attempt to recover the funds.

This is not dissimilar to how cash works -- if someone takes my cash, by fraud, by theft, or in legitimate exchange for goods or services, that's it. They can now spend it however they want. Cash itself is a

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

trustless system in the same sense. Where there is trust it's largely a matter of preventing forgery; which is not dissimilar to the idea of preventing double-spends.

But until Bitcoin there was no real way to do cash-like transactions electronically.

In other words, the utility of Bitcoin is well-established; humans have been using cash for a very long time. The implementation is novel. I don't speak here to the general "blockchain" concept, which has become so nebulous that I don't feel it's worth making general statements about.

jayd16 on Feb 27, 2019 | root | parent | next [–]

If you have to rely on and/or beholden to legal action, then BTC doesn't really provide trust at all.

>But until Bitcoin there was no real way to do cash-like transactions electronically.

There was Venmo and all the other small cash transfer apps. BTC is decentralized but that's of questionable worth to an end user.

ALittleLight on Feb 27, 2019 | root | parent | next [–]

Venmo isn't exactly like cash. For example, my brother showed me that my transaction history was public by default (it hadn't even occurred to me that this was a conceivable design choice) and my brother was able to see who I had recently shared money with and in what amounts. Even if you know to disable that setting, that only prevents random people from seeing your transaction history, while Venmo and legal authorities still have easy access to it. Cash is nice because there is no history to it. It's private and anonymous.

jayd16 on Feb 27, 2019 | root | parent | next [–]

Venmo is just a popular example and there are a lot of others. However, if privacy is your concern, global public ledger tech isn't a good option either.

phil21 on Feb 27, 2019 | root | parent | next [–]

All other options like this share the property of a centralized trusted source mediating your transactions.

The entire point is Bitcoin is like "cash for the Internet" in that once I hand someone $20 in BTC it's just like handing them $20 in physical cash. I have no third party either telling me I can't make that transaction, or with the ability to reverse the transaction after the fact. This is a feature, not a bug.

Anything to disintermediate financial institutions that like to apply political and corporate policy on who I can conduct business with is a good thing in my opinion. This means my options when the third party frauds me are the traditional options employed by folks dealing with cash transactions since money was invented. I can sue them in court, forget about it, or round up some friends with lead pipes.

I think many folks completely miss the point. Cash is useful. Cashless society is about the worst dystopia I can imagine - with unaccountable third parties and government able to track your every spending move, while simultaneously applying their political or legal policy to every transaction. Bitcoin's first step into introducing cash-like digital currency is the innovation, and it clearly is needed. Certainly not perfect (privacy could be far better, security is a real problem, etc.) - but it's far better than anything that had previously come along.

Comparing venmo to bitcoin is simply not a comparison - they solve entirely different problems. Venmo lets you send money from your bank account to another bank account with all those political and legal restrictions applied to your transaction. Bitcoin effectively lets you send cash to anyone you want, in any amount, and no one can stop that transaction from happening because they didn't like the person you are sending it to or what you were buying.

jayd16 on Feb 27, 2019 | root | parent | next [–]

The issue is that it is comparable for many of the use cases that people refer to when talking about Bitcoin. You are personally concerned with a central authority but the majority of users are not. Its not so much that people miss the point of, its just not relevant to most people. Its not made better by the BTC evangelists cramming bitcoin into every conceivable problem, either.

phil21 on Feb 28, 2019 | root | parent | next [–]

Fair enough, I was being uncharitable there.

I do agree most users do not have the same concerns so the use case is far more limited than the hype. I do also still see a lot of value in "digital cash" as a whole, but I never really bought the whole store of value argument and the raft of grifters it attracted.

repomies68 on Feb 27, 2019 | root | parent | prev | next [–]

Grin is quite amazing concept when it comes to privacy.

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

bilbo0s on Feb 27, 2019 | root | parent | prev | next [–]

>If you have to rely on and/or beholden to legal action, then BTC doesn't really provide trust at all...

Yep. Gotta agree with Jayd16 here, if you still need law enforcement, (ie - government), then bitcoin is not useful for operating without trust. The breathless hype about bitcoin was not just the technology level "distributed ledger" thing, but also the idea that you could do things independent of the system. If you still need the system to make it all work, then it definitely fails on the latter hype point.

shawnz on Feb 27, 2019 | root | parent | next [–]

> the idea that you could do things independent of the system. If you still need the system to make it all work, then it definitely fails on the latter hype point.

Bitcoin is independent of the "system" but that doesn't mean you don't still need some system. You're just not locked in to any particular system. Using bitcoin doesn't automatically make you an anarchist.

50656E6973 on Feb 27, 2019 | root | parent | prev | next [–]

>If someone steals my cryptocurrency, then I can still have law enforcement track them down and attempt to recover the funds.

Is this something that actually happens? Police hardly help with with recovering stolen physical goods; I highly doubt they'd even consider helping if your crypto gets hacked

repomies68 on Feb 27, 2019 | root | parent | next [–]

They might claim that they tried to help.

justsayin_3000 on Feb 27, 2019 | root | parent | prev | next [–]

>> Why would you say that there's no legal means of redress? If someone steals my cryptocurrency, then I can still have law enforcement track them down and attempt to recover the funds.

Then you are effectively trusting a third party to make it right when you have been wronged. Isn't this contradictory to the promise of blockchains: That trusting a third party is not required??

Taking this further, you are saying that the data on a blockchain cannot be trusted because the transactions might be reversed due to outside action. Honest question: How does this fit into the concept of a blockchain?

wil421 on Feb 27, 2019 | root | parent | prev | next [–]

If someone steals money from my Bank account my bank will retun the money next business day. No police reports required and little intervention on my part. I've had it happen twice when my card was skimmed in Europe. Both times they called me to report suspicious activity.

Your comparing cash to something electronic. No matter how you spin it Bitcoin is not physical. It's more akin to cash in a bank account. Cash is in my hand, Bitcoin is virtual.

>The $0 Liability Guarantee covers fraudulent transactions made by others using your Bank of America consumer credit cards and consumer and small business debit and ATM cards. To be covered, report transactions made by others promptly, and don't share personal or account information with anyone. Access to funds next business day in most cases, pending resolution of claim. Consult client and account agreements for full details.[1]

[1]https://www.bankofamerica.co…

mikeash on Feb 27, 2019 | root | parent | next [–]

Bitcoin is an attempt to make digital stuff that behaves as much as possible like physical cash. In terms of the way it works, a bank account is very much not the correct analogy. Cash is.

Losing $60,000 in Bitcoin is like losing $60,000 in cash. It's not exactly a surprise that it can happen, and it's expected that there will be no real recourse.

I think the trouble is that people still aren't really thinking of it properly. If this story happened with cash, the first question everybody would be asking would probably be, "Why did you have $60,000 in cash sitting around? What did you think was going to happen?"

Like cash, most people shouldn't be holding large amounts of Bitcoin themselves. If they want large Bitcoin holdings for whatever reason, they should be held with a trustworthy entity that can properly secure them, like a bank. If they do insist on holding large amounts of Bitcoin directly, they need to understand that it's like keeping a vault full of cash, and they need to work hard to keep it secure.

fixermark on Feb 27, 2019 | root | parent | next [–]

Correction: BTC is an attempt to make digital stuff that behaves as much as possible like physical *gold*.

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

Cash is a fiat currency and reproducible infinitely by the controlling government. The point of gold (as a money medium) is that it self-regulates the amount in circulation by being a tangible material in finite supply with cost associated in seeking more. This model has significant benefits and drawbacks (and, it's probably worth noting, its drawbacks are what led to the fiat model most countries use today).

▲ mikeash on Feb 27, 2019 | root | parent | next [–]

I don’t think “cash” necessarily implies fiat. Bitcoin’s model of creating new currency is different from both fiat and gold, although it’s certainly a lot closer to gold.

▲ 908087 on Feb 28, 2019 | root | parent | prev | next [–]

Remember the last time 20 different entities forked gold, and battles erupted over which one was "the one true gold"?

Neither do I.

▲ jancsika on Feb 27, 2019 | root | parent | prev | next [–]

Then you're fighting two fronts.

Practical digital cash of the type you describe needs to have two properties in addition to preventing double spending-- a) quick transaction time (close to immediate) and b) extremely small fees. Otherwise having small amounts of the digital cash doesn't make any sense.

Worse, you've got prior art in Ecash that not only had those properties but also unlinkability. So it can be done, Bitcoin doesn't do it, and as a result the market for it is extremely small and out of touch with the hype around it.

▲ driverdan on Feb 27, 2019 | root | parent | prev | next [–]

> they should be held with a trustworthy entity that can properly secure them, like a bank

No such entity exists.

▲ mikeash on Feb 27, 2019 | root | parent | next [–]

Perhaps, in which case the logical conclusion is that you should never hold a significant amount of Bitcoin in any way.

▲ friendzis on Feb 27, 2019 | root | parent | prev | next [–]

In terms of the way it works, cash is very much not the correct analogy, too.

Transaction wise, cash transactions happen both live and physically, meaning you have *some* means to make sure the counterparty honors their part of transaction. Electronic cash systems involve third party to coerce the counterparty or refund you. In Bitcoin world, apart from hopes and dreams and magical reputation, there is literally no way to stop the counterparty shoving you their Prodeum. Bitcoin removes the trusted third party of electronic cash, but fails to introduce physical measures of physical cash.

Bitcoin transactions are hardly even transactions, more like throwing money into numbered bin and hoping for the best. To be fair, the system has not gone down the drain once some form of market formed, so the hopes mostly did not backfire. The absence of full transactions in my opinion (I may be wrong, though) means Bitcoin IOUs cannot exist and with that whole financial products market, for better or worse.

Loss wise, cash is either in your posession or not and a lot of times can be recovered when lost. Stolen private keys can remain dormant for indefinite amount of time until they are actually used to move coins to a different address. With cash that one has in their immediate possession it would be immediately obvious if someone tries to take them away. If physical cash bills got sticky, you have taken an extra bill, dropped it on a counter and noticed your mistake, then you can still take back the extra bill. If you have transferred too much/many coins, then it's SFYL. Forgetting a wallet with physical cash somewhere can be SFYL, can still be recoverable if no one took possession of it. Losing access to private keys is permanent SFYL.

▲ gruez on Feb 28, 2019 | root | parent | next [–]

>cash transactions happen both live and physically, meaning you have some means to make sure the counterparty honors their part of transaction

I'm assuming you're referring to threat and/or use of violence, but that's not a viable option if the counterparty is prepared. Are you really willing to get into a fist/knife/gun fight if you're trying to sell a Xbox and the other side doesn't want to pay up?

▲ friendzis on Feb 28, 2019 | root | parent | next [–]

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

Not necessarily violence, transaction happening in a public place with oversight poses risk of being exposed/caught, which could be enough to deter the counterparty from running away with goods or money, scammers tend to go for easier targets, but yes, physical measures including violence are an option with cash, while electronic one-sided irreversible pseudonymous transactions mostly eliminate those options.

The point is that the threat model of Bitcoin is quite different from that of cash.

▲ mikeash on Feb 28, 2019 | root | parent | next [–]

That's a property of how you use it. You can use cash in private, or even without being anywhere near the recipient (for example, by mailing it). You can carry out a Bitcoin transaction while next to the recipient in public if you want.

This is another example of how people don't think of it properly. Sending Bitcoin to some stranger online is basically equivalent to mailing them cash (minus the chance of having the letter stolen). Most of us would understand that mailing cash to a stranger is probably a bad idea, but Bitcoin is used differently.

▲ ravingraven on Feb 27, 2019 | root | parent | prev | next [–]

>Your comparing cash to something electronic. No matter how you spin it Bitcoin is not physical.

You say that like it's a bad thing. Bitcoin is something that has the advantage of physical cash (trust-less) and the advantage of electronic communications (you can't practically send cash to the other side of the world).

It also, of course, has the disadvantage of physical cash which is, once it's gone, it's gone. There is no way to reverse trust-less transactions now and there was none in the (pre-Bitcoin) past. Nothing has changed there and this is not what crypto solves. What crypto solves is trust-less transactions over the internet.

▲ rootusrootus on Feb 27, 2019 | root | parent | next [–]

Doesn't it also have the disadvantage that, unlike physical cash, it can be stolen electronically? At least with cash someone has to mug me in person to take it, which reduces the attack surface quite a lot.

▲ lunaynx on Feb 27, 2019 | root | parent | next [–]

You could write down your seed on paper instead of storing it or the private key electronically.

▲ updateYourMind on Feb 27, 2019 | root | parent | prev | next [–]

You can have a bank working on top of a cryptocurrency network. It's the same except that everything is transparent + you don't need a bank if you don't want one.

▲ repomies68 on Feb 27, 2019 | root | parent | next [–]

Essentially all these services and exchange that offer bitcoin wallets are like banks. I think they have been the main way to get and hold bitcoin since the early days, I would guess normal standalone wallets are in the minority when it comes to the amount of users. For quantity stored maybe not so much.

▲ Scene_Cast2 on Feb 27, 2019 | root | parent | prev | next [–]

You're conflating reduction of risk (system-wide) and offloading of risk.

In your bank example, the bank likely took the financial hit. With bitcoin as an underlying tech, there's some reduction of risk (with a whole bunch of asterisks).

▲ wil421 on Feb 27, 2019 | root | parent | next [–]

Why would I care if the banks took a hit? If fraud was hurting their margins significantly we would see the government step in. The banks would also do more to prevent it. The US just switched over to chip cards.

▲ JangoSteve on Feb 27, 2019 | root | parent | next [–]

Because you're paying for it with your money. They can afford to take a hit (and can afford the insurance for such losses) because of the fees they charge you directly, and the money they make utilizing your principle for other purposes while it's there.

▲ dylkil on Feb 27, 2019 | root | parent | prev | next [–]

Your bank takes the loss on those stolen funds.

Bitcoin is more akin to cash in hand than cash in a bank account, the title of the white paper is a 'A Peer-to-Peer Electronic Cash System'.

It behaves like cash.

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

snissn on Feb 27, 2019 | root | parent | prev | next [–]

There could be a crypto based bank account just like there are usd based bank accounts

fixermark on Feb 27, 2019 | root | parent | prev | next [–]

There's a significant difference between Bitcoin and cash, which is that the worst-case scenario for loss of your cash is the government in control of it just prints more and gives it to you (in effect, distributing the cost of your loss among everyone who holds that currency). This is not technically possible with Bitcoin, and AFAIK no system has grown up organically yet to provide some kind of "loss insurance" in the form of keeping some BTC in reserve for making victims whole.

awrence on Feb 27, 2019 | root | parent | next [–]

What you're describing is basically an insurance mechanism. There is no reason you couldn't implement the same for cryptos. But at least under that explicit framework, those who had not participated in that scheme would not have to pay the risk premium associated with it which is currently incurred by fiat holders whether they like it or not (under your scenario).

ravingraven on Feb 27, 2019 | root | parent | prev | next [–]

>This is not technically possible with Bitcoin [...]

Of course, it is. The government could force everyone to send Bitcoins to a special account which is then distributed to victims (i.e. a tax). That would actually be *better* than what we have now. By printing more cash, people with cash are punished while actually rich people (who own stock, real estate, factories, jets etc.) are not.

fixermark on Feb 27, 2019 | root | parent | next [–]

By "not technically possible," I meant specifically that no government can cause new BTC to manifest into existence. The scenario you're describing is (government mandated and legally enforced) loss insurance, which is the system I observed hasn't (to my knowledge) organically manifested yet.

yingw787 on Feb 27, 2019 | root | parent | prev | next [–]

I think the difference is the police officially recognize one currency and do not officially recognize the other. The U.S. dollar is backed by the full faith and trust of the U.S. government. A cryptocurrency's value is backed by the amount of other fiat currencies pumped into it. If in the future, an authority figure (say, the President of the United States) created a cryptocurrency and ordered the FBI to prioritize cybercrimes relevant to that currency and drop investigations for others, you'd be in a bad place if somebody in a different state stole your money. He/she could never do that with the U.S. dollar, since manipulating that infringes on his/her literal ability to order people around.

andrewla on Feb 27, 2019 | root | parent | next [–]

There is not a separate crime of "theft of money" and "theft of property". Electronic crimes, like the theft of key material, is usually covered by different laws.

In places where there have been cryptocurrency thefts that have been prosecuted, they have been primarily pursued as cases of theft -- the US statutory definitions of theft usually only use the monetary value (the USD equivalent) as the determiner of the severity.

While such a policy of "do not pursue bitcoin theft" would theoretically be possible either as an explicit policy or an informal, I thing it would be unlikely to survive judicial scrutiny; it would be like insisting that car thefts only be investigated and prosecuted for American-made cars.

duado on Feb 27, 2019 | parent | prev | next [–]

It’s great for people who are sheltered enough to think that their governments are the least trustworthy organizations in existence, or who live in countries where they are.

treis on Feb 27, 2019 | root | parent | next [–]

When you're buying drugs or transferring money for other illegal purposes the government is definitely the organization you have the least trust in.

curiousgal on Feb 27, 2019 | root | parent | next [–]

I always find such opinions quite pigeonholed. Many third world countries do not have access to online banking or credit cards. Cryptocurencies were the only way I could pay for goods and services online and the only thing that made me feel like an actual citizen of the world and not just some content pirate.

treis on Feb 27, 2019 | root | parent | next [–]

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

Those barriers are likely due to money laundering laws and whoever is accepting the bitcoin is (probably) breaking the law when they convert to USD or other currencies. So you're right that it's not necessarily illegal purchases so much as illegal transactions.

You can break the cryptocurrency usage into 4 main groups: Speculators, Lawbreakers, Libertarian types, and Techies. Otherwise, the financial system provides cheaper or more convenient options for payment.

curiousgal on Feb 27, 2019 | root | parent | next [–]

> Those barriers are likely due to money laundering laws

Again, the world is much bigger and more nuanced than you think, non-covertible currencies are a thing and they are due to a country's central bank policy not money laundering laws.

> the financial system provides cheaper or more convenient options for payment.

No it does not, if I had had ways to pay for a server using my country's currency, I would have used it.

treis on Feb 27, 2019 | root | parent | next [–]

>Again, the world is much bigger and more nuanced than you think, non-covertible currencies are a thing and they are due to a country's central bank policy not money laundering laws.

What difference does it make which law or "policy" the users are circumventing?

>No it does not, if I had had ways to pay for a server using my country's currency, I would have used it.

And if it were legal to do so there would be a way.

Erlich_Bachman on Feb 27, 2019 | root | parent | prev | next [–]

You do realize the world is bigger than US and EU, right? That there are many other countries in the world where the situation is not the same as in the first world?

treis on Feb 27, 2019 | root | parent | next [–]

No, this is the first I'm hearing of it. Please go on about these "other countries".

duado on Feb 28, 2019 | root | parent | next [–]

Venezuela is a place where the government is the equivalent of a guy bursting into a shopping mall and shooting it up. In their case Bitcoin does have a genuine purpose.

treis on Feb 28, 2019 | root | parent | next [–]

And that purpose is breaking Venezuelan law. If the Venezuela government weren't a bunch of gangsters and made hard currency transactions legal then they wouldn't use Bitcoin.

reidjs on Feb 27, 2019 | parent | prev | next [–]

You're right that crypto is pretty useless for people like you and I who have access to high quality bank services. But to people who don't really have access to legitimate bank services they're a godsend.

swarnie_ on Feb 27, 2019 | root | parent | next [–]

Because i really don't know.... How common is it to have access to electricity, an internet capable device, internet connection and a knowledge of cryptocurrencies but not a bank?

latchkey on Feb 27, 2019 | root | parent | next [–]

Originally from California, but now living in Vietnam for the last 3 years. My experience here is that what you're asking about is actually something very common.

People in small villages have modern cell phones and thanks to the govt military owning the primary telco, fast internet. They might not have access to a bank due to being so remote. They also don't trust their banks, for good reason [1].

[1] https://e.vnexpress.net/news/n…

reidjs on Feb 27, 2019 | root | parent | prev | next [–]

banking services aren’t exactly a right, they have the right to refuse service to anyone they want. So under certain circumstances, eg, you have a bad credit history, are not a citizen, or don’t have enough money, it can be difficult to open a bank account in certain countries.

mindcandy on Feb 27, 2019 | root | parent | prev | next [–]

Try to think outside of the US/Eurozone. At least a billion unbanked individuals still have cellphones.

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

Meanwhile in SF, the homeless all have cell phones. They are also frequent customers of Bitcoin ATMs according to an convenience store clerk that I asked because he watches over one.

▲ knorker on Feb 28, 2019 | root | parent | next [–]

1) Why can't the cellphone connect to a bank? Or ANY central database?

2) How exactly is it a good idea to have your wallet on a cellphone?

As for homeless & Bitcoin ATMs. Yes: 3) That's how I'd launder money too. Pay off a homeless person to go to a bitcoin ATM. 4) That's how I'd conduct drug deals too if I were homeless and in the drug trade as buyer or seller.

You can't just say "homeless people use bitcoin ATMs therefore bitcoin is good for homeless people".

(no, I'm not saying homeless = drug related, and you know I'm not)

▲ DanBC on Feb 27, 2019 | root | parent | prev | next [–]

In the UK a "fraud marker" will make it very difficult for a person to open a bank account.

▲ knorker on Feb 28, 2019 | root | parent | next [–]

"I only accept bitcoin" is the biggest fraud marker there is, though. :-P

What I mean is that this is a non-solution to that problem.

▲ knorker on Feb 27, 2019 | root | parent | prev | next [–]

It's not.

It's the same logic where cryptocurrency advocates say that if a country's currency goes down the crapper then the people can use bitcoin, and the country can't break that! But why can't they just use dollars, or euros, instead? Because the local government would make that illegal! Why wouldn't they make bitcoin use illegal? Because... because... shut up!

▲ golergka on Feb 27, 2019 | root | parent | prev | next [–]

How many banks allow you to buy drugs with your account?

▲ swarnie_ on Feb 27, 2019 | root | parent | next [–]

This thread is about access to banking, What does drugs have to do with this?

▲ knorker on Feb 28, 2019 | root | parent | next [–]

Because bitcoin.

The killer feature for bitcoin is buying drugs. It's essentially all it is for. That and tax evasion and speculation.

▲ syn0byte on Feb 27, 2019 | parent | prev | next [–]

What redress do you think you have even if you "trust" someone? That 100 dollar widget you bought in cash didn't work? Well fuck you, see you in court. Now what? Are you going to take the store to court over 100 bucks? Pay with a card and your card company doesn't want to reverse charges? Same problem... I'd bet that per 5000 transactions, debit and credit cards have more fraud that the 'end user' has no remediation for than bitcoin does.

Sometimes, reinventing the wheel is exactly the point when the wheel has been engineered to favor the engineers.

▲ knorker on Feb 27, 2019 | root | parent | next [–]

If your card company doesn't reverse charges you can take them to small claims court, and also change card company.

You can't point to *one* case and say that it doesn't work. My experience is that you as a consumer *will* win a chargeback. It's so reliable that there mere mention of it to a merchant will make them refund you, because their fees go up if their chargeback rate goes up.

Also cryptocurrencies make this infinitely worse, not better.

If you want to make a case for cryptocurrencies you should actually go with the safety for *the merchant*, not the consumer. The consumer holds the power with credit cards. But then again today the merchant can always choose to only take debit cards, thus fixing the whole problem.

And it's not like you don't have to trust anyone to use cryptocurrencies. The government will still kick down your door if you break the law because *that's what people want from society*.

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

swish_bob on Feb 27, 2019 | root | parent | next [–]

Also the losing side pays the chargeback fees in a chargeback case, which is why for small sums, unless the issuing bank is damned sure they'll win the chargeback, they'll just write it off and give the money to the customer.

yingw787 on Feb 27, 2019 | root | parent | prev | next [–]

Of course you can stiff the legal system. But you can only stiff it so far. I Googled "Ethereum steal" and the top three results have figures in the millions, through something as straightforward as a 51% attack. No court system can simultaneously claim to be fair and just and legitimate, and let slide a $1.1M USD theft. And in such situations, other people usually have a bone to pick with said thief too, bolstering resources on your side.

If a cryptocurrency scales and somebody pulls off a Madoff-level theft (>$64B USD), could you guarantee some amount of clawbacks by technology alone? I wouldn't bet on it.

AgentME on Feb 27, 2019 | root | parent | next [–]

>through something as straightforward as a 51% attack

... which has never been done before on Ethereum (or Bitcoin). Are you talking about Ethereum Classic? It's something entirely different and amateur. Using it as a criticism of Ethereum is like complaining banks are untrustworthy because a kid at school called himself a bank and didn't give the money back you lent him.

jayd16 on Feb 27, 2019 | root | parent | prev | next [–]

A block chain doesn't solve this in any way. By the time you determine your widget doesn't work, the transaction is complete.

manigandham on Feb 27, 2019 | parent | prev | next [–]

A blockchain is just an immutable database that can be appended to or overwritten by majority.

It doesn't have anything to do with *trust* and definitely doesn't provide any form of it, but trust is at the core of several human concerns like currency. Thus, blockchains are fundamentally unable to serve those uses regardless of how much hype is thrown at it.

basch on Feb 27, 2019 | root | parent | next [–]

part of trust is eliminating double spend. you can "trust" that when you received ownership of the digital asset, that somebody else didnt also get a copy or equal ownership. the decentralized trust replaces an authority saying "so and so owns this" or "you already spent that dollar." this happens in an environment where participants DONT trust each other to not cheat.

dmitriid on Feb 27, 2019 | root | parent | next [–]

when participants don’t trust each other, they delegate to a third party they both trust: a bank, a notary, an external accountant, etc.

Blockchain provides nothing, and people end up building replicas if real-world trust systems around it (even silk road had a reputation system not built on blockchains)

manigandham on Feb 27, 2019 | root | parent | prev | next [–]

None of that has to do with blockchain. You as a human have the same *trust* in something.

In this case, instead of a verified, regulated, audited central bank, you've decided to instead trust anonymous, unaudited, unregulated actors who vote in majority.

AgentME on Feb 27, 2019 | root | parent | next [–]

There's a difference between trusting a human with your money, and trusting that you correctly understand an open system which fully incentivizes everyone to operate predictably.

It's the difference between trusting Facebook to keep your messages private and trusting PGP to keep your messages private.

manigandham on Feb 27, 2019 | root | parent | next [–]

Yea, that difference isn't relevant here, and your second sentence is not an example of the first. We know the encryption works but nothing about blockchain/bitcoin incentivizes anyone to operate predictably.

Humans are soft, irrational and messy in interactions. This isn't compatible with the perfectly technical math-based operations of bitcoin as a currency, and that's after they choose to trust it in the first place.

AgentME on Feb 27, 2019 | root | parent | next [–]

I mean sure, there's always the always the possibility that a majority of miners ally together, forfeit millions of dollars of mining rewards, and likely cause all of their cryptocurrency holdings to plummet in value, all in order to double-spend a few of their own transactions. But if we're going to worry about the possibility of everyone involved becoming irrational, then I'm going to worry about the more realistic scenario of my bank doing something surprising with my money and causing me to go through legal hell, especially if my lawyer and the judge decide to be irrational too since we're comparing against a case of whole groups of people acting irrationally.

It's also worth mentioning that Bitcoin and Ethereum have never had a 51% double-spend attack. People do occasionally go through legal hell related to their bank/paypal/whatever accounts, or have problems sending money through their bank to who they want to send it to.

manigandham on Feb 27, 2019 | root | parent | next [–]

It's not about all people being irrational, it's about humans having negotiations and softly defined deals when it comes to money. Bitcoin doesn't fit this scenario like human-powered trusted authorities do.

There's a reason why the legal system exists to offer you the case-by-case evaluation when needed. Many people have lost money through bitcoin, through hacks or poorly coded contracts, or to scams, or directly funded criminals and terrorists. Those people would have much preferred a little "legal hell" as you call it rather than no recourse at all.

AboutTheWhisles on Feb 27, 2019 | root | parent | prev | next [–]

Requiring trust is not a positive aspect of currencies. Gold and silver succeeded in large part because they can be verified.

manigandham on Feb 27, 2019 | root | parent | next [–]

Gold and silver have nothing to do with currency, and they can only be used as such through trust in a currency system by participating people.

There is no such thing as a trustless currency.

AboutTheWhisles on March 11, 2019 | root | parent | next [–]

This is completely untrue to the point of being the polar opposite of reality. Look up the attributes of ideal money.

Gold and silver are the original currencies. They are trustless because they can be verified easily and transferred physically.

The more trust a currency requires, the less valuable it becomes due to decreased fungibility and liquidity.

coliveira on Feb 27, 2019 | parent | prev | next [–]

The worst problem in my opinion is not even this. With crypto currencies you can NEVER be sure that you are the owner of what you think you own. The only thing that guarantees your property of crypto currency is the EXCLUSIVE ownership of a private key. But what guarantees that other people don't already have access to the key you think is private, through any of the millions of forms of hacking that are available? Even if you have your private key secured nowadays, there is always the possibility that someone else in the past hacked and had access to that same private key and can use it at any time. So, even the notion private property cannot be guaranteed with crypto currencies.

theli0nheart on Feb 27, 2019 | root | parent | next [–]

The same could be said for any number of things we consider to be private property. Unless you physically can see with your own eyes everything that you "own", how do you know some bad actor hasn't run off with it? Well, our society gives us a whole bunch of protections in place which give us some peace of mind (security systems, laws, etc.), but you can't know for *sure* without some verification.

So if you have the private key in your hand, and the address with your Bitcoin still has Bitcoin, while someone else *could* have your private key, why wouldn't they just transfer the money out?

jjnoakes on Feb 27, 2019 | root | parent | next [–]

> The same could be said for any number of things we consider to be private property.

Except if we are wrong in those other cases, we can usually use the legal system to help us recover our stolen property.

> So if you have the private key in your hand, and the address with your Bitcoin still has Bitcoin, while someone else could have your private key, why wouldn't they just transfer the money out?

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

Maybe they are waiting for you to deposit more bitcoin into that address, or maybe they are waiting to collect more private keys before exploiting them all at the same time, or maybe they... why speculate?

The idea that money can disappear without recourse because of one mistake in security or one highly motivated targeted attack is not, in my opinion, a desirable property of a currency.

▲ theli0nheart on Feb 27, 2019 | root | parent | next [–]

> Maybe they are waiting for you to deposit more bitcoin into that address, or maybe they are waiting to collect more private keys before exploiting them all at the same time, or maybe they... why speculate?

Well, from a criminal's point of view, I don't see the upside in waiting. The owner of the coins could move them at any time, and then your loot is gone for good. I think it's safe to assume that if someone else has possession of your private keys, your addresses will be drained immediately.

▲ jjnoakes on Feb 27, 2019 | root | parent | next [–]

Sure, maybe for a random target. Maybe for a targeted attack the criminal knows more money is coming in and doesn't want to tip his hand yet. Who knows... that's the point of not speculating.

▲ hombre_fatal on Feb 27, 2019 | root | parent | prev | next [–]

On the other hand, after being the victim of social engineering attacks on AWS and Gandi, I often feel like I don't really own anything when anyone with mere persistence can attack a customer support vector.

Or the fact that in pull based financial systems like the US, someone who got your debit card number when buying a coffee can charge you again in the future, so you need to be eternally vigilant with your statements.

To me, cryptocurrency is a breath of fresh air in these regards. It's a predictable system to plan around.

▲ vkou on Feb 27, 2019 | root | parent | next [–]

> Or the fact that in pull based financial systems like the US, someone who got your debit card number when buying a coffee can charge you again in the future, so you need to be eternally vigilant with your statements.

Which is why banks analyze your transaction history, and call you when they observe suspicious patterns of use of your credit card.

▲ hombre_fatal on Feb 27, 2019 | root | parent | next [–]

And it's full of false positives, false negatives, only works in some conditions, and it's not a service I want to pay for on every single transaction. That's basically a bandage on top of a shitty system.

I'm not so naive to say that one thing is the best, but I'm willing to speak up for trade-offs in these absolutist arguments.

▲ vkou on Feb 27, 2019 | root | parent | next [–]

> And it's full of false positives, false negatives, only works in some conditions, and it's not a service I want to pay for on every single transaction. That's basically a bandage on top of a shitty system.

The per-transaction costs of this fraud-prevention are miniscule, the false positives don't affect me (I get a phone call, and I tell them everything's fine), and I have recourse, both procedural, and legal against false negatives.

Just because you sprinkle a bunch of crypto powder on a transaction doesn't mean that all possibility for fraud goes away. The median per-transaction cost in crypto for this sort of thing is zero, while the worst-case cost is 'you lose the entire transaction/all your money'. And that latter one happens far too frequently for me to bank my life on it.

▲ hombre_fatal on Feb 27, 2019 | root | parent | next [–]

I like the piece of mind that when I send or receive 0.001 BTC, it's final.

You've been steering this towards your crypto=bad hobby horse. But if your point is that you wouldn't "bank your life" on something, we can agree. I wouldn't "bank my life" on anything, like hoping I catch a recurring payment on my debit statement that I 100% canceled.

▲ hanniabu on Feb 27, 2019 | root | parent | prev | next [–]

This will all be abstracted in time. One way I can think of is to have the funds periodically moved to different addresses, and obviously don't keep all your funds in a single address. This can all be automated and abstracted.

▲ emiliobumachar on Feb 27, 2019 | root | parent | prev | next [–]

theli0nheart has addressed that we're not dealing in absolutes. To complement, I can be pretty sure that if someone unscrupulous had hacked my private key away, they would have been very incentivised to empty the account immediately, before I *or another thief* did it. If it was just me, sure, they could take a risk and wait for bigger deposits. But tragedy of the commons also happens to criminals.

▲ tim333 on Feb 27, 2019 | root | parent | prev | next [–]

>... there is always the possibility that someone else in the past hacked and had access to that same private key

That one's not too hard - if in any doubt transfer to a new wallet with a new private key.

Nothing is 100% secure - you can but do a reasonable job. My biggest worry when I have my own keys is losing the keys rather than being hacked.

▲ sametmax on Feb 27, 2019 | root | parent | prev | next [–]

That's why we have the ledger.

▲ mrguyorama on Feb 27, 2019 | root | parent | next [–]

How does that stop others from gaining access to your private keys?

▲ sametmax on Feb 27, 2019 | root | parent | next [–]

It's a hardware wallet, pretty hard to hack: https://www.ledger.com/

▲ duxup on Feb 27, 2019 | parent | prev | next [–]

The number of legitimate uses seems to drop pretty dramatically when you talk about a system that is used in a zero trust situation and irreversible.

I think the block chain philosophy as far as crypto currency and use for legitimate business just doesn't go hand in hand like some folks thought it might. People really don't want to do business if there is zero trust, and centralized databases, and strong courts, are fine. Even when there aren't strong courts blockchain doesn't so much fill the gap as provide a risky solution... that involves a lot of illegal and undesirable behavior.

▲ awrence on Feb 27, 2019 | parent | prev | next [–]

True cryptocurrencies, read properly decentralized (which currently means through an expensive and well distributed PoW process) allow the creation of digital assets whose issuance and transfer mechanisms can't be tempered with by a central agent. This is a true pretty massive innovation. This is not reinventing the wheel, that wheel did not exist until bitcoin showed up.

It comes with unique upsides, eg: a central bank can’t inflate them, which for monetary assets, is a massive part of the valuation equation, eg: I can transact in them in a collapsed economy with no functioning money (ie venezuela). It comes with downsides, eg: if i get my bitcoin stolen I have less governmental power to find redress. But there’s a bit of a fallacy in the thinking that fiats are better from that perspective.

I would argue fiats are generally the same but the government has an additional option in that they can print more money to make specific people whole. Example a bank goes under because there was fraud, someone managed to pull out fiat through some means (pulling out cash for example). Because the government owns the press they can print more fiat to make depositors whole. This isn’t a magic bullet though, because you’re in effect imposing a monetary tax on the rest of the fiat saving community by doing so.

Outside of that solution, which isn’t a 0 cost one, the situation is identical to cryptos, you have to go through the courts to get your stolen holdings back. And if you lost them, it's no different than if your bundle of cash had gone up in flames or your stash of gold had gone down with a ship, you'd be out of luck. The massive thing cryptos provide is a digital savings mechanism that can’t be inflated by a central agent. If you’re a digital monetary saver, that’s a hugely compelling alternative which has a massive potential market base.

▲ nradov on Feb 27, 2019 | root | parent | next [–]

When a bank fails the US government doesn't print more currency. The depositors are made whole from an existing insurance fund, which the failed bank had been paying into the whole time (along with all other banks). It's risk pooling, not inflation.

▲ tim333 on Feb 27, 2019 | parent | prev | next [–]

>just goes around the legal system; by doing so, you're just re-inventing the wheel.

Going around the legal system is actually a big deal both for straight criminal stuff like extortion and also things that morally not too bad but where the law is a pain like raising money for ventures with less

paperwork and fees or sending funds to Venezuela without the approval of its present government.

▲ kryogen1c on Feb 27, 2019 | parent | prev | next [–]

> Yes, a blockchain works when zero trust is needed/desired for transactions, but that's still an implementation-level concern

This premise is not true and is one of the (many) reasons why blockchain is just a buzzword.

Maintaining the ledger still requires trust, even if that trust is less centralized than a single company (and thats often not the case either)

▲ repomies68 on Feb 27, 2019 | parent | prev | next [–]

What's wrong with reinventing the wheel? I think having alternatives for financial transactions is just a good thing in itself. Of course you don't have to use them if you don't like.

▲ thefounder on Feb 27, 2019 | parent | prev | next [–]

Some people want just virtual cash. No banks, chargebacks, 3rd parties(visa, paypal etc) additional "verification" etc. Just old good "hard" cash for the XXI century.

▲ mikeash on Feb 27, 2019 | root | parent | next [–]

I'm not entirely convinced that they do. Many say that they do, but then don't treat it the way they would treat a similar quantity of cash, lose it, and are befuddled as to how it happened.

▲ thefounder on Feb 28, 2019 | root | parent | next [–]

That's because the technology is new and people seem to trust wallets and exchangers usually developed unknown amateurs. This leads us to issue number two:

Many holding crypto currencies are using the funds as investment so I assume they were aware of the high risk to loose all the funds for various reasons. Once the crypto investments/ponzi scheme is gone we can work on crypto payments.

▲ panarky on Feb 27, 2019 | parent | prev | next [–]

Your comment is irrelevant to this article.

This article is about an unproven accusation that Coinomi wallets can be exploited because the seed phrase is spell-checked over a TLS connection.

▲ arisAlexis on Feb 27, 2019 | prev | next [–]

so if an unknown mail provider in Zimbabwe gets hacked email is insecure. Logical

▲ YeahSureWhyNot on Feb 27, 2019 | prev | next [–]

the crypto tech was marketed as the most secure financial instrument but so far it has been repeatedly proving itself to be quite the opposite:)

▲ MusaTheRedGuard on Feb 27, 2019 | prev | next [–]

This entire thread: "Why don't you just use the post office why do you need email?"

▲ chdaniel on Feb 27, 2019 | prev [–]

You know what's the most painful thing? If (I'd say when) years go by and Bitcoin value is a significant multiple of what it is today... Much like those who lost their wallets in 2011-2012-2013, most probably it will be haunting

▲ SmellyGeekBoy on Feb 27, 2019 | parent | next [–]

Pull the other one... That ship has well and truly sailed.

▲ isostatic on Feb 27, 2019 | parent | prev [–]

Wasn't there a Big Bang Theory episode where this happened?

▲ glaurung_ on Feb 27, 2019 | root | parent [–]

Not sure about big bang, but there's a scene in the most recent season on Silicon Valley about this scenario.

Captured 2026-10-30T07:51:17.637Z from https://news.ycombinator.com/item?id=19263332

Consider applying for YC's Winter 2027 batch! Applications are open till November 2.

Guidelines | FAQ | Lists | API | Security | Legal | Apply to YC | Contact

Search: