



Free Article

**FOR YOUR EYES ONLY // DO NOT DISTRIBUTE // DO NOT FORWARD**

**Nothing in this newsletter is legal, financial, tax advice, etc.**

## TO THE READER

WELCOME TO THE WATCHMAN'S TORCH NEWSLETTER

*Location: Karachi, Pakistan (apartment paid for in cash)*

Dear Privacy Seekers,

If you're not familiar with me, I'm Gabriel Custodiet. For those who do know me: nice to see you here. You're looking at the very first edition of the Watchman's Torch newsletter. I've been meaning to start up a premium newsletter for years. After five years of producing the Watchman Privacy Podcast, writing an intermittent free newsletter, and producing numerous privacy courses on Escape the Technocracy, I've finally found the perfect medium to share my knowledge on an ongoing basis.

I'm not going to bog you down with a lengthy introduction. You know why you're here. We're going to keep these issues as succinct as possible: within 10 pages in general. The signal-to-noise ratio of online information has never been worse. I get it.

So buckle up. Let's go.

- Gabriel Delanoe Custodiet



## IS THE TERMINATOR BEHIND A MONERO PRICE SPIKE?

For those familiar with Watchman Privacy, you already know that we're not in the habit of tracking the price of Bitcoin or any other cryptocurrency. Our focus has always been on privacy, not profits. That said, there are rare occasions when cryptocurrency price movements intersect with cybersecurity topics in a meaningful way. Today is one of those moments, and it seems fitting to this discussion.

Those of you who follow cryptocurrency markets may have noticed a remarkable 50% surge in the price of Monero (XMR) in late April. The event coincided with a Bitcoin hack involving the transfer of 3,520 BTC (valued at around \$340 million at the time of this article). For the inquisitive among us, the funds can currently be tracked at this bitcoin address: `bc1qcrpchnrdx87jnal5e5m849fw460t4gk7vz55g`.


What followed was a rapid and calculated maneuver, as the stolen bitcoin was laundered through multiple exchanges and ultimately swapped for monero: the well-known privacy-focused cryptocurrency.

Here's where things get interesting. Due to its focus on privacy, Monero has faced widespread de-listing from mainstream exchanges, creating a highly unusual scenario. The cryptocurrency's limited availability on centralized exchanges means that these platforms typically maintain very low reserves of it. Reportedly, one of the few exchanges that still lists Monero saw its reserves completely drained in under two hours. On top of that, many of the exchanges where Monero remains available are instant-swap services, which inherently require users to take custody of their coins. This "limitation" makes it exceedingly difficult to create "paper monero" (fake or non-existent monero on exchanges). As a result, exchanges were left scrambling to purchase real monero to meet demand, further driving prices upward. This sudden market imbalance was only exacerbated by users frantically searching for ways to access Monero as an on-ramp or off-ramp amidst the chaos.


The situation is reminiscent of Bitcoin's early days, when price action would catch the attention of mainstream media, sending new waves of investors searching for ways to enter this uncharted market.

But the story doesn't stop there. Let's peel back another layer to see what lies beneath. Anyone looking into Monero's recent price surge would have encountered a flood of eye-catching headlines. However, upon closer inspection, many of these articles were low-effort pieces, likely churned out by artificial intelligence. Nestled within the clutter was a perplexing claim about an apparent Monero upgrade called "EP-159." According to these sources, this mysterious update supposedly introducing "compliance" features to the privacy-focused cryptocurrency and was touted as a key driver behind the surge in price.


### 3 Cryptocurrencies to Buy in a Bear Market

 AOL | 2 hours ago


A bear market is one of the best opportunities to invest in crypto, with one key caveat: You need to choose your investments very carefully. Bear markets tend to separate the crypto contenders from the pretenders.




### Monero Surges 50% Amid \$330M Bitcoin Hack

 The Currency Analytics | 1 day ago


Monero (XMR) jumps 50% after \$330 million in stolen Bitcoin is converted into XMR, fueling speculation and bullish momentum across the market.



### Monero Price Surge Likely Attributable to Large Hack: ZachXBT

 CoinDesk | 1 day ago

A suspicious transfer of 3,520 BTC, valued at \$330.7 million, was swapped for monero (XMR), on-chain researcher ZachXBT said. The resulting monero price surge was linked to laundering activities through multiple instant exchanges.



Yet, something doesn't quite add up. For those familiar with Monero's development process, this claim immediately rings alarm bells. **The so-called "EP-159," along with its supposed sibling "EP-160," is nonexistent within Monero's ecosystem.** The buzz surrounding these upgrades appears to be nothing more than junk content, likely generated by AI, to misdirect or manipulate the narrative.

#### Monero can return as a regulation-compatible asset

The alternative explanation for the recent rally is the possibility of [XMR](#) to return as a regulated asset, compatible with major exchanges.

One of the expectations is that the Monero network can implement a long-awaited upgrade, the [EP-159](#). This would allow XMR to perform as a trackable asset, exposing selected wallets.

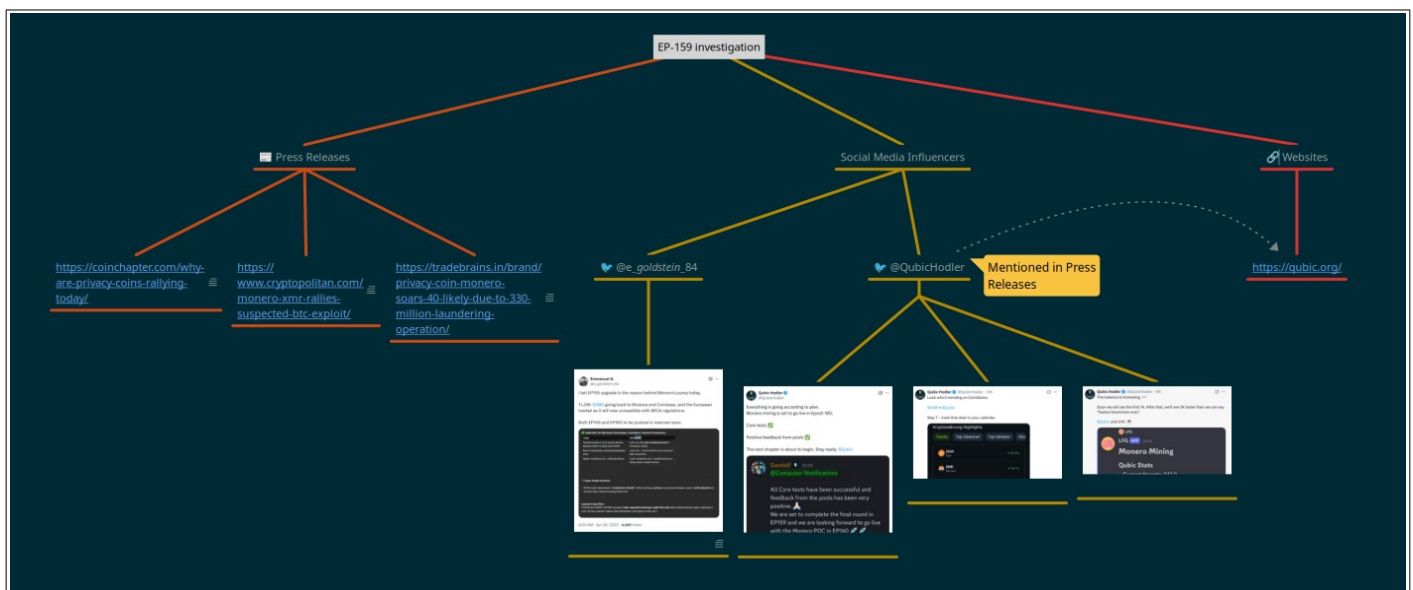
To some, this discrepancy might seem like a dead end, easy to dismiss as noise. But for me, it was only the beginning of my investigation. Armed with basic OSINT (Open Source Intelligence) tools, I began piecing together the puzzle mapping out the network of articles, tracking references, and documenting the chain of links tied to these claims.

Soon, a distinctive pattern emerged. The “press” surrounding Monero’s price surge fell into two categories. On one hand were core articles that subtly linked to a particular social media account (more on that later), and on the other were secondary articles almost certainly AI-driven that recycled content in increasingly garbled forms. These secondary pieces frequently included fabricated claims or outright hallucinations, yet they adhered to the same general structure:

Price Action Report → Hack → Technical Analysis Nonsense → EP-159

It doesn’t take much detective work to see who stands to benefit. The spotlight inevitably shines on the mysterious social media account tied to this operation. This account exhibits a suspiciously predictable pattern tweeting about recent Monero developments, exploiting trending topics, and redirecting attention to their own “token.”

Digging deeper, their posts reveal another red flag: inflated engagement metrics, marked by high like and re-share activity but conspicuously low comment interaction. This imbalance strongly suggests the account is buying likes or using other shady tactics to boost visibility. Despite these artificial boosts, its follower count remains conspicuously low: an odd anomaly for accounts engaged in such promotional strategies.



And so the investigation comes to an end. While these findings may seem like just another cautionary tale, they illustrate a deeper issue at play in the world of digital information: the dangerous consequences of relying on free, unverified content in an age increasingly dominated by AI-generation and manipulative narratives.

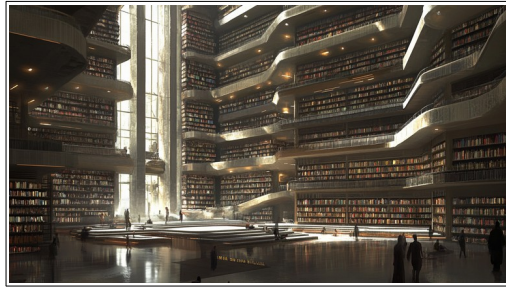
This flood of AI-crafted articles might seem harmless at first glance: an abundance of accessible information for the average reader. Yet it's anything but. These low-effort pieces not only oversimplify and distort complex topics but actively manipulate perceptions, sow confusion, and lend ill-deserved credibility to fabricated claims. As seen in this case, the false narrative around "EP-159" didn't just waste everyone's time; it had the potential to mislead investors, spur ill-informed debates, and inflate price speculation. Worse, it could enable deliberate pump-and-dump schemes that exploit the naïve or unprepared.

People often imagine that if AI ever becomes a threat, it'll look like something out of Terminator: metallic skeletons, glowing red eyes, and the end of civilization as we know it. But that's not where the real fight is happening. Not yet anyway.

The reality is quieter, subtler, and already unfolding all around us. It's not machine guns— it's machine-written articles. It's not killer robots—it's viral misinformation, fake press releases, and algorithm-driven narratives designed to manipulate markets, shape sentiment, and waste your time. And while these systems might not look menacing, they're eroding our ability to tell truth from fiction, signal from noise.

This is the real battlefield. It's not some future sci-fi dystopia—it's right here, right now.

This is man versus machine



## QUOTATION OF THE MONTH

*Metamorphosis is difficult. I imagine the exquisite agony of the caterpillar turning itself into a butterfly, pushing out eye-stalks, pounding its fat-cells into iridescent wing-dust, at last cracking the mother-of-pearl sheath and staggering upright on sticky, hair's-breadth legs, drunken, gasping, dazed by the light.*

John Banville, *The Untouchable*

## BOOK RECOMMENDATION

[\*How to Be Invisible\*](#) by JJ Luna

The late JJ Luna was a juggernaut in the privacy advice world. I recall Michael Bazzell even recognized him as the godfather. Luna cut his teeth on privacy in Franco's totalitarian Spain, so privacy was always a matter of life and death for him. I always appreciated this seriousness. There was no room for error, and his guide is hardcore, full of thousands of details that are worth picking up. None of it is digital. God bless him for that. And requiescat in pace, JJ Luna.

Here's a favorite line from the book:

*I also confess to withholding information in other ways. If I run a small business out of my home, I neglect to get a business license. If I move, I neglect to inform the postal authorities. If asked for information when obtaining an e-mail address, I fail to list my true name and home address.*