What Can We Learn from the Bybit Incident and the Failures of Crypto's So-Called 'Gods'?

Santosh Pandit, London, 26 February 2025

On 21 February 2025—coinciding with my birthday—Bybit, a Dubai-based cryptocurrency exchange, suffered a staggering loss of approximately USD $1.4 billion. Hackers, believed to be North Korea's Lazarus Group[1], exploited a cold wallet, making off with 401,000 Ethereum in what is now the largest cryptocurrency heist on record.

The breach rattled investors, traders, and the self-proclaimed "crypto faithful," triggering declines in Ethereum and Bitcoin prices. More significantly, it exposed glaring vulnerabilities beneath the industry's leading players and their figureheads, such as Bybit's CEO, Ben Zhou—once hailed as a visionary.

This debacle prompts critical questions: **what does it reveal about cryptocurrency security, and why do we persist in idolising these so-called 'Crypto Gods'?**

Here is my personal take, based on what is publicly known about the incident.

Lesson 1: Billion-Dollar Stakes Require Robust Defences, Not Justifications

Cryptocurrency is no longer a niche experiment for a handful of enthusiasts; it is a multibillion-dollar industry. Bybit alone handles billions in monthly transactions. Mainstream platforms like Revolut offer crypto trading, and established exchanges like Coinbase demonstrate its broad appeal. Losing 1.4 billion in a single incident is not a minor setback—it's a disaster.

[1] Is it really Lazarus Group? I am not so sure.

The hackers didn't employ groundbreaking techniques; they deceived wallet signers with a falsified interface and manipulated a smart contract to redirect funds[2]. These are well-documented tactics, seen in breaches at WazirX and Radiant Capital in 2024, yet Bybit failed to adapt.

Claims that "the industry is chaotic" or "Lazarus is too sophisticated" hold no weight. When managing sums of this magnitude, excuses are unacceptable. Bybit should have implemented out-of-band verification, rigorous contract audits, and stringent monitoring. Instead, they left vulnerabilities unaddressed and are now lamenting the consequences. The industry's disorder is a call to action, not a shield.

Lesson 2: Advanced Persistent Threats Test You—They Don't Excuse You

Attributing the attack to Lazarus—North Korea's notorious cyber operatives—casts it as a cinematic showdown. The execution was undeniably polished: spoofed interfaces, rapid laundering through decentralised exchanges, and a scale consistent with Lazarus's track record, as noted by analysts like ZachXBT. Yet, even if a state-sponsored group was responsible, this does not absolve Bybit. The breach succeeded due to human error and unexamined code—flaws the attackers exploited, not created.

Dismissing it as "they're too advanced" sidesteps accountability. These methods are not new; they echo the 2022 Ronin breach and others. Bybit's responsibility was not to outmanoeuvre a nation-state after the fact, but to prevent the attack outright. Measures like air-gapped keys, multi-step verification, or a 24-hour delay on large transactions could have thwarted it. The lesson? **Design systems to withstand the worst scenarios—or don't participate**.

Lesson 3: There Are No Crypto Gods

In my personal life, I hold a strong faith in God, but in the financial realm, I am firmly sceptical. Ben Zhou, Bybit's CEO, was once a celebrated figure—building the exchange from scratch into a global powerhouse, earning praise across platforms like X. The hack has tarnished that image. While his swift admission, promise of a 10% bounty on the stolen funds, and efforts to stabilise Bybit post-breach deserve recognition, the failure occurred on his watch. No amount of polished communication can erase that.

This pattern extends beyond Zhou to the broader cult of personality in cryptocurrency. Leaders are lauded as infallible until they falter, at which point the refrain becomes, "Nobody's perfect." But when billions are at stake, near-perfection is the expectation. Zhou's supporters were justified in admiring his achievements, but equating effort with invulnerability was misguided. The lesson is clear: stop deifying these individuals. They are executives, not deities, and their errors are failures, not plot twists. Bernard Madoff, once revered in wealth management, offers a stark historical parallel.

[2] There are a couple of YouTube videos that speculate how the hackers may have exploited the multi-signature feature. It remains to be seen whether the hack was due to human error; or fundamental weakness of the multi-sig feature.

Lesson 4: Resilience Does Not Replace Prevention

Credit is due to Bybit for weathering the storm: despite 4 billion in withdrawals, they maintained solvency, kept funds fully backed, and avoided collapse. Zhou's prompt apology and commitment to cover losses showed resolve. However, resilience is not a substitute for preparedness. The 1.4 billion was lost not because Bybit recovered well, but because they were unprepared. In this domain, preventing the loss outweighs any recovery effort. The lesson? Don't rely on a strong recovery—build a system that avoids the need for one.

The Takeaway

The Bybit breach is not an anomaly; it's a recurring alarm we've too often ignored. With stakes this high, everyone—exchanges, executives, and investors—must sharpen their approach. Security must outpace the money, not lag behind it. Citing industry challenges or sophisticated adversaries is no defence at this stage. As for the 'Crypto Gods'? They are human, fallible, and unworthy of blind faith. Bybit survives, but at a 1.4 billion cost—a stark reminder: secure it, or lose it. No justifications, no idols—just results.

My Perspective

I've never placed trust in cryptocurrency exchanges or their leaders. Time will reveal how many opportunists masquerade as visionaries. Their assurances—open-source code, customer insurance, cold wallets, audits, penetration testing, and certifications like ISO 27001 or SOC II—sound reassuring but fall short. These are valuable measures, yet insufficient without accountability at every level and a global resolve to deter malicious actors. Until then, cryptocurrency remains a target-rich environment for criminals.

Would I invest £100 in Bybit? I evaluate the cybersecurity posture of all my service providers rigorously, relying on passive Cyber Threat Intelligence (CTI). For Bybit, I lack the visibility to assess this effectively. I could be wrong, but they seems to be using cheap tricks to hide. But unless I have their written permission, I will not be able to gather sufficient CTI. Conduct your own due diligence.

What are your thoughts? Am I too critical? My inbox is open for discussion.

Santosh
26 February 2025

Technical Annex: Tactics, Techniques, and Procedures (TTPs) Used in the Bybit Hack and Potential Defences

Tactics, Techniques, and Procedures (TTPs)

1. **Initial Access: Social Engineering via UI Spoofing**
    - *How*: Hackers falsified the transaction approval interface, deceiving signers into authorising transfer.
    - *Why It Worked*: Reliance on the interface without secondary verification.
2. **Execution: Smart Contract Manipulation**
    - *How*: Modified the contract during the transfer to divert 401,000 ETH to their wallet.
    - *Why It Worked*: Lack of pre-execution code scrutiny.
3. **Persistence: Evading Detection**
    - *How*: Masked the activity as legitimate until the funds were extracted; no alerts triggered.
    - *Why It Worked*: Inadequate real-time monitoring.
4. **Exfiltration: Rapid Fund Distribution**
    - *How*: Split the proceeds across multiple addresses, moving them via decentralised exchanges and bridges.
    - *Why It Worked*: No restrictions on large outflows.
5. **Defence Evasion: Laundering Techniques**
    - *How*: Converted ETH into Bitcoin and stablecoins, routing through high-volume pools.
    - *Why It Worked*: Limited ability to halt funds quickly.
6. **Command and Control: Covert Operations**
    - *How*: Pre-installed the exploit, avoiding detectable communication.
    - *Why It Worked*: Basic scans missed dormant threats.

Potential Defences

1. **Against UI Spoofing**
    - *Hardware Tokens*: Require physical devices (e.g., YubiKey) for approvals, immune to interface fakery.
    - *Out-of-Band Confirmation*: Mandate phone or app verification for significant transactions.
    - *Tamper-Resistant Verification*: Display transfer details via QR code on a separate device.
2. **Against Contract Manipulation**
    - *Formal Audits*: Use mathematical verification tools (e.g., Certora) to detect flawed logic.
    - *Time Delays*: Enforce a 24-hour hold on large transfers for review.
    - *Simulations*: Test transactions in a controlled environment to identify anomalies.
3. **Against Detection Evasion**
    - *Real-Time Monitoring*: Deploy blockchain analytics (e.g., Chainalysis?) to track funds continuously.
    - *Anomaly Detection*: Use AI to flag unusual patterns, even if disguised.
    - *Segregated Roles*: Separate teams for initiating, approving, and auditing transfers.
4. **Against Fund Distribution**
    - *Transfer Limits*: Automatically pause transactions exceeding 1,000 ETH for manual review.
    - *Fund Tracing*: Pre-tag wallets with analytics providers for swift tracking.
    - *Rate Controls*: Restrict the speed and volume of cold wallet outflows.
5. **Against Laundering**
    - *Rapid Response*: Collaborate with stablecoin issuers or bridges to freeze funds immediately.
    - *Identity Enforcement*: Pressure exchanges to verify recipient identities.
    - *Incentives*: Offer substantial rewards to ethical hackers to outpace criminals.
6. **Against Covert Exploits**
    - *Endpoint Security*: Use a combination of tools to detect hidden threats.
    - *Zero-Trust Model*: Verify every action, assuming compromise.
    - *Code Integrity*: Require signed updates to block unauthorised changes.