HexTrust

Lessons from the ByBit Hack:

Why Institutional-Grade Custody Is Essential for Digital Asset Security

March 2025

Contents

Executive Summary 3

How the ByBit Hack Unfolded 4

The Risks of Traditional Multi-Sig and Self-Custody Models 5

How Hex Trust Custody Prevents These Attacks 6

Why Institutions Need Licensed Custodians 8

Custodial vs. Self-Custodial: Security, Control and Legal Considerations 9

How Institutions Can Protect Themselves 10

Strengthening Institutional-Grade Digital Asset Security 10

Executive Summary

The recent ByBit hack, resulting in a staggering loss of approximately $1.4 billion in ETH, underscores the growing sophistication of cyber threats. The attack exploited vulnerabilities in operational security rather than traditional private key theft, highlighting a fundamental shift in how threat actors target digital asset platforms.

In our pre-webinar analysis, we explored how the attack unfolded, detailing the security gaps that allowed it to happen. In our live AMA webinar, we took the discussion further—breaking down key security flaws, the evolving nature of cyber threats, and most importantly, how **institutional-grade, fully-licensed custodians like Hex Trust provide the necessary infrastructure to prevent similar incidents**.

This article serves as an educational resource for institutions, explaining how Hex Trust Custody, our bank-grade platform for managing Digital Assets, differs from traditional multi-sig solutions, self-custody models, and smart contract wallets, and why regulated custodial infrastructure is essential for securing digital assets.

How the ByBit Hack Unfolded

The ByBit hack was a multi-layered, highly coordinated attack that targeted the operational flow of transactions rather than directly stealing private keys:

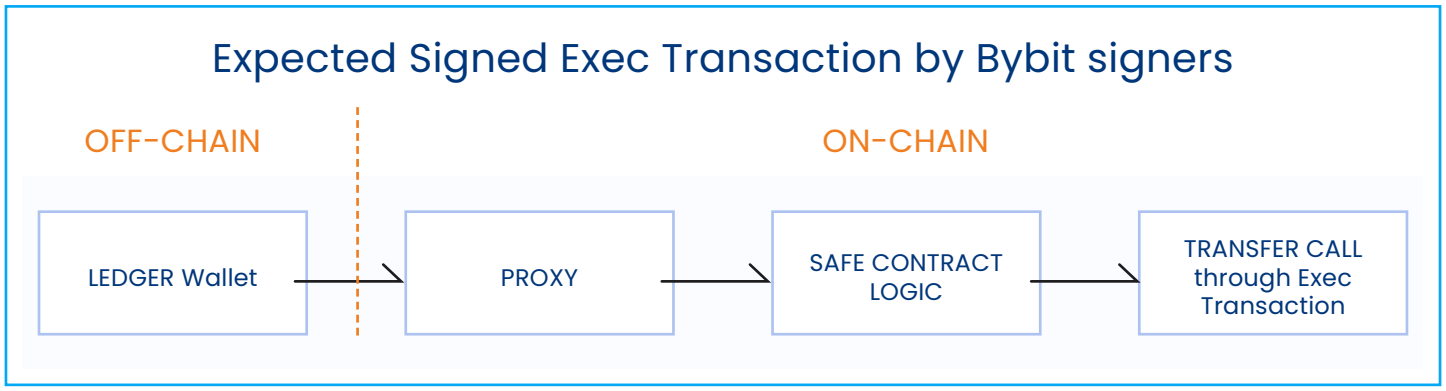
1. **Compromised Safe UI** – Hackers breached the Safe front-end, targeting ByBit's usage of the smart contract wallet.
2. **Blind Signing Risk** – ByBit employees unknowingly approved a fraudulent transaction, assuming it was legitimate due to UI manipulation.
3. **Full Wallet Control Granted to Hackers** – The fraudulent transaction reassigned control of ByBit's Safe Wallet, leading to the massive fund loss.
4. **Use of Delegate Calls** – The transaction changed the Safe Wallet's implementation contract, a common method for smart contract upgrades but also a major security risk when exploited.

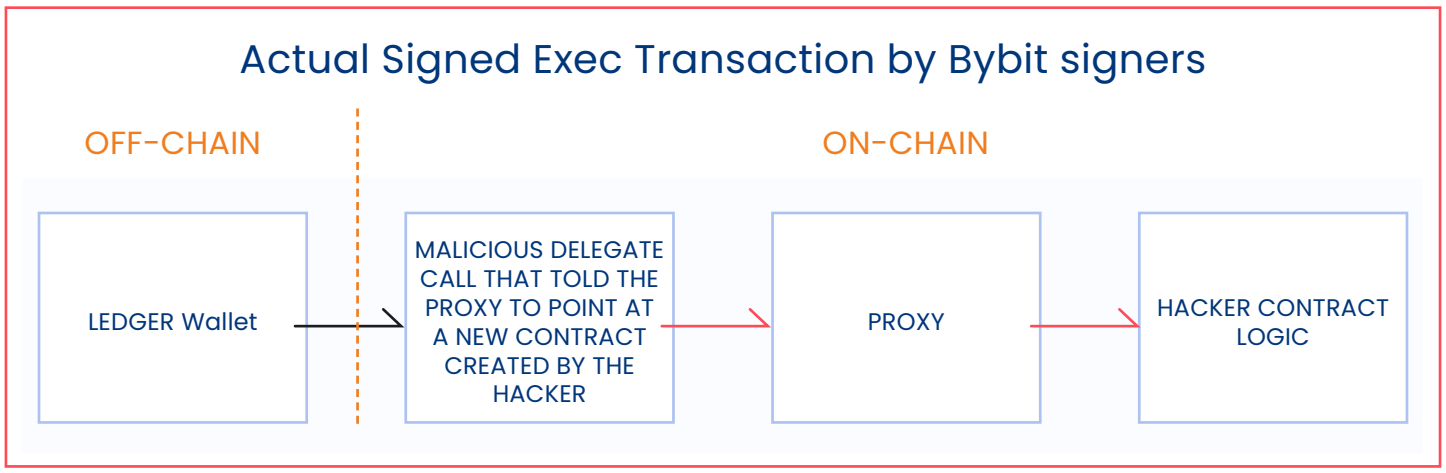
The breach echoes similar attacks on **WazirX ($230M) and Radiant Capital ($50M)**—showing a clear trend where attackers manipulate transaction signing processes rather than directly stealing private keys.

For a detailed breakdown of how the exploit occurred, read our full Bybit Hack Analysis here.

Key Takeaway:

Traditional security models focusing only on private key protection are no longer sufficient.





What Bybit signers expected vs. what actually occurred: The Safe UI could have been manipulated to display misleading transaction details, causing signers to inadvertently approve a different transaction.

The Risks of Traditional Multi-Sig and Self-Custody Models

Many institutions rely on multi-signature (multi-sig) smart contract wallets or self-custody models to secure digital assets. However, these models come with inherent security risks:

- **Multi-Sig Smart Contracts** – While they enforce multiple approvals, they remain vulnerable to smart contract upgrades, UI manipulation, and operational exploits.

- **Self-Custody Risks** – Institutions managing their own security face challenges with blind signing, UI attacks, and inadequate operational security measures.
- **Blind Signing Dangers** – The attack highlighted how difficult it is to verify transactions which display raw hexadecimal data that is unreadable for most users.

The ByBit attack demonstrates that relying solely on multi-sig or self-custody is not enough. Without proper transaction verification and operational security, institutions remain exposed to evolving cyber threats.

Key Takeaway:

Multi-sig is not a silver bullet—institutions need stronger security measures beyond just smart contracts.

How Hex Trust Custody Prevents These Attacks

To mitigate risks like the ByBit hack, **Hex Trust Custody** incorporates a comprehensive, defence-in-depth approach:

- **No Reliance on Smart Contracts**: Hex Trust Custody does not utilize multi-signature smart contract wallets. This design choice eliminates risks associated with proxy contract upgrades, which can be manipulated in a single transaction.
- **Strict Transaction Controls**: Hex Trust's system prevents clients from transferring ownership of funds or accessing private keys directly. Withdrawals are executed directly by Hex Trust Custody

using a standard transfer method, eliminating reliance on proxy mechanisms like ExecTransaction.

- **Enhanced Transaction Decoding and Policy Enforcement**: Hex Trust Custody decodes all smart contract calls received by external sources and sends the decoded content of the transaction to UI, policy verification and approval. Transactions that cannot be decoded, (e.g. due to an unknown smart contract ABI) are clearly flagged as risky and treated as "blind signing." In addition, users can request to activate transaction policies to automatically reject transactions that cannot be decoded.

- **Wallet Segregation and Independent Controls**: Hex Trust's wallets are segregated with independent keys and controls per wallet (e.g., Vault/Blockchain Asset), ensuring that even if one wallet is compromised, other assets remain secure.

- **Cryptographic Integrity**: Once policies are verified, the transaction request is protected cryptographically to prevent tampering

- **Rigorous Approval Verification**: Hex Trust Custody's streamlined mobile app interfaces require comprehensive verification of transaction details. This minimizes the risk of deceptive approvals by enabling both initiators and approvers to review the full transaction context.

Key Takeaway:

These design decisions combine to create a robust, multi-layered defence that protects digital assets and provides clear, transparent, and secure transaction processes—ensuring that such exploits are effectively prevented.

Why Institutions Need Licensed Custodians

Unlike self-custody or multi-sig wallets, fully-licensed custodians operate within regulated frameworks that enforce strict compliance, risk management, security and asset protection measures, including:

- **Segregated assets and independent controls** – Licensed custodians are required to hold client assets in trust, ensuring they remain fully segregated from the custodian's own operations and associated risks. This structure provides an additional layer of protection in the event of insolvency, safeguarding client holdings.
- **Insurance** - Custodians maintain insurance coverage to protect against theft, fraud, or operational failures—offering a safety net that self-custody solutions lack.
- **Risk-managed transaction approvals** – Multi-layered security ensures robust transaction verification.
- **Secure infrastructure** – Prevents UI manipulation, prevents blind signing risks where possible through decoding and highlights blind transactions as risky, and unauthorized contract modifications.
- **Operational Safeguards** – Custodians implement advanced security controls such as segregation of duties, device lockdowns, and proactive malware detection.

Key takeaway:

The role of custodians is **not just about holding assets**—it's about **ensuring transaction integrity, operational security, and risk management** at every step.

Custodial vs. Self-Custodial: Security, Control and Legal Considerations

Beyond security, **legal liability is another crucial differentiator** between custodial and self-custodial solutions:

The Custodial Advantage:

Licensed custodians operate within regulated frameworks, assuming legal responsibility for safeguarding client assets. Their agreements typically outline:

- **Liability in case of loss.**
- **Recourse options for clients.**
- **Compliance and regulatory oversight.**

The Self-Custody Trade-Off:

The principle of "not your keys, not your coins" means sole responsibility for assets. Self-custody providers typically specify:

- **No provisions for private key recovery.**

- **Limited protection against unauthorized transactions.**
- **No legal liability on the platform's part.**

How Institutions Can Protect Themselves

- **Train Employees on Social Engineering Attacks** – Conduct phishing simulations and cybersecurity training.
- **Enforce Strong Device Security** – Implement endpoint detection & response (EDR) software, device lockdown.
- **Strict access control policies** Follow principle of least privilege, where minimal access is granted with strict segregation of duty.
- **Ensure Robust Network Security** – Use network segmentation, VPNs, and firewalls to block suspicious traffic.
- **Implement Secure Workflows** – Use dedicated, hardened devices for transaction verification and enforce multi-person approval workflows.
- **Evaluate Custodians Carefully** – Ensure your custody provider protects transaction integrity with cryptographic verification and policy enforcement.

Strengthening Institutional-Grade Digital Asset Security

The ByBit hack serves as a wake-up call for the industry. It is no longer enough to protect private keys—security measures must extend across transaction verification, operational integrity, signing request authentication and infrastructure hardening.

To scale digital finance securely, institutions must adopt an end-to-end security strategy where all security controls work together in coordination.

At Hex Trust, we remain committed to setting the standard for institutional-grade custody—prioritizing compliance, risk management, governance, and security to empower institutions in navigating the evolving digital asset landscape with confidence.

Ready to upgrade your custody solution? Get in touch with Hex Trust and discover how our institutional-grade security infrastructure can safeguard your digital assets.

Contact partnerships@hextrust.com to learn more.

Disclaimer

This post is for informational purposes only and is not financial, investment or other advice, nor a recommendation, endorsement, offer, solicitation or sale of any kind in any jurisdiction. As always, users should do their own research are urged to seek independent financial, investment and other advice before taking any initiative in connection with the information contained herein. The information contained in this article is intended to be current at the time of publication, but may not remain so indefinitely. Products or services mentioned in this material are subject to legal and regulatory requirements in applicable jurisdictions and may not be available in all jurisdictions nor to all persons.

Attributed to:



Rafal Czerniawski

Co-founder & CTO



Tommaso Natale

Chief Engineering Officer



Giorgia Pellizzari

Head of Custody



The Leader in Digital Asset Solutions

