COIN Rabbit

Protecting Capital Is More Than Security.
Lessons From the Binance Hack

Industry Report

Expert perspectives on risk, business models and counterparties after the largest theft in crypto history.

Supported by

Bitcoin Life, Compass Mining, Coinchange, Vnish & HashCore, and Realiz Group

Key lessons

Keeping crypto assets safe takes more than strong security. It also depends on how a platform operates, handles client funds, and manages risk. Based on insights shared by industry leaders, we've identified six things worth looking at before trusting a platform with your capital:

01 ***Business Model***

Choose platforms that keep client assets separate and never use them for their own business.

02 ***Diversification***

Diversify where you hold assets as well as what you hold.

03 ***Trust***

Don't trust a platform just because of its size or reputation. Understand who controls your assets.

04 ***Infrastructure***

Attackers can get in through any link around your funds. Make sure no single breach can put everything at risk.

05 ***Risk Management***

Before chasing higher yields, understand where the returns come from and what risks you're taking.

06 ***Verification***

Find out in advance what happens to your assets if the platform is hacked or something else goes wrong.

Special experts



Walter Barrett

Chief Strategy & Growth Officer, CoinRabbit



Peter Lane

CEO, Bitcoin Life



Kris Bakker

Head of Account Management,
Compass Mining



Maxim Galash

CEO, Coinchange



Evgeny Kislov

CBDO, Vnish & HashCore



Brice Vandevoorde

CEO, Realiz Group

1. Introduction

On 29 October 2026, attackers stole an estimated $6.36 billion from Binance in what was reported as the largest theft in digital asset history. According to Binance's preliminary investigation, the attackers used social engineering tactics, including fake job interviews, alongside malicious software to compromise employees' devices and gain unauthorized access to the exchange's wallet-signing infrastructure. Binance reported finding no evidence that its private keys had been compromised.

The incident was part of a wider pattern. Between January and October 2026, DefiLlama recorded 325 hacks resulting in combined losses of $8.7 billion, surpassing the total recorded in any previous full year in its dataset. Several major incidents, including Drift and Kelp DAO, exposed weaknesses in access controls, external dependencies and operational processes.

These cases raise a bigger question: what actually keeps client capital safe? Strong technical security matters, but so do the way platforms operate, who controls client assets, how those assets are used and what happens when something goes wrong. For platforms, this means examining their business models, operational standards and reliance on counterparties. For institutions and investors, it means understanding where their capital is held, how it is protected and what they should expect from the platforms they use.

This report looks beyond the technical details of the Binance incident to examine how platforms, institutions and investors can better protect capital. Drawing on market data and insights from industry leaders, it examines the Binance case in the context of other major hacks in 2026, highlights six key lessons and introduces a five-layer framework for evaluating how crypto platforms protect and preserve client capital.

2. The case in context

Almost 78% of the year's losses came from four incidents at centralised exchanges, while 232 DeFi incidents together accounted for $1.19 billion. Without Binance, losses for January–October 2026 ($2.38 billion) would be close to the same period of 2025 ($2.51 billion). A small number of major incidents accounted for a disproportionate share of the damage, highlighting how much capital can be exposed when a large platform suffers a serious security failure.

Losses by attack type, excluding Binance

Attack type	Losses	Incidents
Key compromise	$721 m	36
Bridge and cross-chain	$701 m	34
Access control	$371 m	54
Token and share accounting	$250 m	58
Frontend and infrastructure	$144 m	16
Oracle manipulation	$75 m	42
Protocol logic	$26 m	43

Source: DefiLlama data, compiled by Cryptsy. Main attack types shown.

In most of these cases, attackers did not break the cryptography. Outside Binance, more than half of losses came through key compromise, access control failures and attacks on infrastructure, and the same pattern held beyond exchanges.

Drift lost $295 million after attackers obtained admin approvals, the contracts at Kelp DAO acted on false data from an external source, and a Coldcard firmware flaw and tampered Ledger devices cost self-custody users more than $200 million. Moving assets off an exchange changes the type of risk, but does not remove it.

2. The case in context

The year’s largest incidents

Date	Target	Loss	Attack type
29 Oct	Binance	$6.36 bn	Frontend and infrastructure
24 Sep	Bitget	$387 m	Key compromise
6 Sep	Liquid Network	$320 m	Bridge and cross-chain
1 Apr	Drift	$295 m	Access control
18 Apr	Kelp DAO	$293 m	Bridge and cross-chain

Source: DefiLlama data, compiled by Cryptsy.

The data shows that crypto losses arise from different points of failure. Compromised keys, weak access controls, vulnerable bridges and infrastructure failures each expose capital in different ways. No single security measure can address all of them.

For investors, this makes evaluating a platform more complicated than checking whether it uses cold storage or has passed a security audit. The more important question is how its technical safeguards, operational controls and business practices work together to protect client assets – and limit losses when something fails.

3. Lessons from the Binance case

LESSON 1. BUSINESS MODEL

Choose platforms that keep client assets separate and never use them for their own business.



Walter Barrett, Chief Strategy & Growth Officer
CoinRabbit

Keeping client funds safe takes more than protection from hackers. It also requires a business model designed to preserve capital rather than expose client assets to additional risks. The Binance case illustrates why this distinction matters: according to the exchange, customer balances remained unaffected by the hack, while the company covered the losses using its own resources. Strong security can reduce the risk of an attack, but how a platform holds and uses client assets also influences what happens when something goes wrong.

For years, the safety of client funds has been judged mainly by technical security: encryption, key storage and access controls. By these measures, a platform built for short-term returns and one designed for long-term holding can look the same. The real difference lies in what happens to client assets once they arrive: whether they remain segregated and available or are used to finance the platform's own business.

Protection and Preservation

Capital protection addresses specific threats and limits losses when something goes wrong, through secure custody, insurance arrangements and other safeguards. Capital preservation is broader. It asks whether assets remain available to their owners over time, how they are used and who has access to them. Protection deals with threats; preservation also deals with the conditions under which capital is held.

This distinction is familiar in traditional finance. Custody arrangements can separate client assets from a firm's own balance sheet, while lending and investment activities introduce different obligations and risks. Economist Jesús Huerta de Soto argued that money entrusted for safekeeping should not be lent out. Once the same funds are treated as available to both the depositor and a borrower, the system becomes vulnerable when both need access to them.

3. Lessons from the Binance case

The crypto industry has developed sophisticated protection tools, from cold storage and MPC to Proof of Reserves. Regulatory frameworks such as MiCA have also brought greater attention to custody and the segregation of client assets. But technical safeguards and regulatory requirements do not eliminate the need to understand how a platform uses the assets it holds.

What 2022 showed

In 2022, some of the industry's most damaging failures were not caused by hacks. They resulted from how platforms handled customer funds.

Celsius attracted deposits by offering high yields and deployed those assets in lending and investment activities. When withdrawals were frozen in June, customers could no longer access their funds. The company filed for bankruptcy the following month.

FTX also collapsed without an external hack being the primary cause. Billions in customer assets had been transferred to Alameda Research, leaving the exchange unable to meet withdrawal requests when confidence evaporated.

In both cases, the problem went beyond technical security. Client assets had been exposed to risks arising from the platforms' own business activities.

What 2026 adds

The Binance case presents a different scenario. The exchange suffered a major security breach, but reported that customer balances remained unaffected and that the losses would be covered from its own resources.

The attackers gained unauthorized access to the exchange's wallet-signing infrastructure and stole assets from a Binance-controlled wallet. Binance stated that customer funds were not used to absorb the loss. As co-CEO Richard Teng put it: "We never use any customer funds, so they are not impacted."

Binance reported setting aside more than $6.34 billion to cover the incident, including approximately $5 billion in the stolen tokens. Its Proof of Reserves, verified on 2 November, showed that customer balances across ten major assets were backed at least 1:1.

3. Lessons from the Binance case

The contrast with 2022 is significant. FTX and Celsius had exposed client funds to risks through their business models before their crises began. In the Binance case, the company reported absorbing the consequences of a security breach without passing the losses on to customers.

The key distinction is not whether a platform can be hacked. It is whether a security incident or a failure of its business model puts client capital at risk. Technical safeguards can reduce the likelihood of an attack, but the way a platform holds and uses client assets helps determine who ultimately bears the loss.

How CoinRabbit Applies This

At CoinRabbit, we follow a simple principle: client collateral secures the client's loan and nothing else. We do not lend it out, rehypothecate it or use it to generate additional returns, and the liquidity behind our loans does not depend on reusing client assets. This separation is central to our approach to capital preservation. It limits clients' exposure to risks from the platform's own lending and investment activities, and avoids the additional risks that come with reusing their collateral.

LESSON 2. DIVERSIFICATION

Diversify where you hold assets as well as what you hold.



Peter Lane, CEO
Bitcoin Life

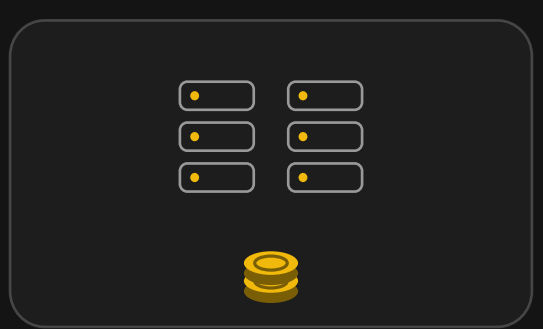
Coming from traditional wealth management and now building Bitcoin Life, I see the Binance case as a reminder that accepting Bitcoin's volatility doesn't mean accepting avoidable risks around custody, counterparties or access to your assets. Price swings come with owning the asset, but the risks of a particular provider can be managed.

The first step is to ask the same questions as in traditional finance: who holds the assets, whether they are kept separate from the provider's own funds, who can move them and what happens if the provider fails. Investors tend to focus on returns, but if a provider fails, those returns can be lost along with the assets.

3. Lessons from the Binance case

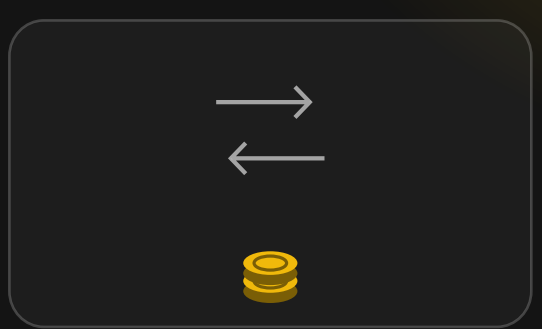
KEY TAKEAWAY

Three ways to reduce concentration risk



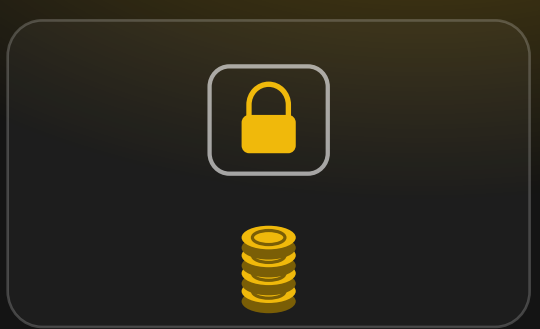
Separate providers

Avoid shared custodians and infrastructure



Limit exchange balances

Keep only what you need for trading



Separate savings

Keep long-term holdings apart

Based on Peter Lane's commentary, CEO of Bitcoin Life

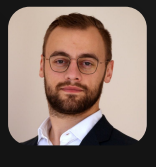
Even if you are confident in Bitcoin itself, no single platform should hold all of it. At Bitcoin Life, we review our counterparties regularly, keep balances on trading venues to what we need for trading and track how our partners depend on each other. Splitting assets between two providers helps only if they don't use the same custodian or infrastructure, because otherwise one failure can affect both. Personally, I keep long-term holdings separate from money I may need in the near term, so a problem at one provider never forces me to touch my savings.

Spreading assets limits the damage, but it's still worth planning for the case where something fails. Security can break down through people, processes or third parties, so you should know in advance how much you could lose and how quickly you could move assets. A provider's capital matters, but its ability to cover losses should be the last line of defence, behind strong governance, independent oversight and recovery plans. In wealth management we always ask what happens to the client if something goes wrong, and that question should shape a business from the start.

3. Lessons from the Binance case

LESSON 3. TRUST

Don't trust a platform just because of its size or reputation. Understand who controls your assets.



Kris Bakker, Head of Account Management
Compass Mining

The situation at Binance has shown us that even the most well-known exchanges are not invulnerable to hacks. We should not blindly trust a company based on its size or reputation, but instead understand what safety measures it has put in place to protect our assets. At Compass Mining, we always encourage self-custody, and everyone should take risk management very seriously.

The case reinforces the way we already work at Compass Mining. Our clients don't have to worry about their funds being held by a different entity: the Bitcoin our customers mine goes directly from the mining pool to the customer's wallet. This way, customers receive their earnings in whichever wallet they prefer, whether that is on an exchange or in self-custody.

KEY TAKEAWAY

Trust needs evidence

1. Who holds your assets?
2. What safeguards are in place?
3. How the platform manages risk?

Based on Kris Bakker's commentary, Board Advisor at Compass Mining

3. Lessons from the Binance case

The main lesson for me is that the old motto still holds true: "Not your keys, not your coins." Making use of an exchange or platform doesn't have to be a bad thing, but you should be aware of the trade-offs.

Technological advancement is a cat-and-mouse game between those trying to protect people and those trying to harm them. Even with years of investment in security, vulnerabilities will always exist. Whether you are a service provider or a consumer, it is important to always be vigilant and on the lookout for scams, security threats and other risks. Everyone should be using a strong form of multi-factor authentication.

LESSON 4. INFRASTRUCTURE

Attackers can get in through any link around your funds. Make sure no single breach can put everything at risk.



Evgeny Kislov, CBDO
Vnish/HashCore

The Binance case shows that security has to cover every link in the chain, not only private keys. Attackers increasingly avoid the front door and go after weaker points around it: devices, third-party libraries, updates and low-level code dependencies. With AI helping them find these blind spots faster, static defence models can’t keep up, and no company is fully immune, however big or well-funded it is.

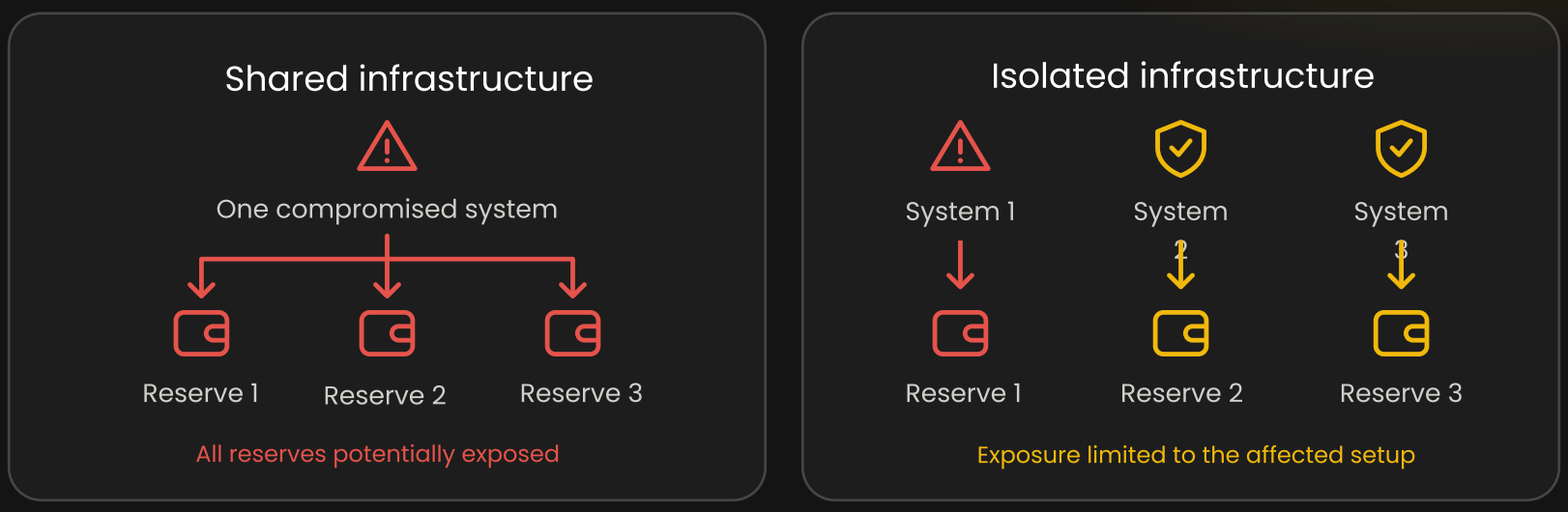
For the market, this means two things. Clients and enterprise teams will push harder for non-custodial infrastructure, because every third party that holds or touches assets is one more link that can fail. And reserves need to be split across fully isolated setups, since a multi-sig wallet alone doesn’t help if one breach can still reach everything.

3. Lessons from the Binance case

KEY TAKEAWAY

One breach shouldn’t expose everything

Isolate reserves and access systems so that compromising one does not automatically expose the rest.



Based on Evgeny Kislov’s commentary, CBDO of Vnish & HashCore

We apply the same logic to our own treasury. Vnish works at a lower level of the stack, focusing on hardware efficiency, Stratum protocols and hashrate routing rather than holding client funds, so our core software isn’t directly exposed to exchange hacks. Still, after the Binance news our finance and security teams reviewed counterparty exposure, access permissions and reserve management. We also see the need to monitor financial flows the way our clients use HashCore Pulse to monitor ASIC health, with automatic circuit-breakers that freeze activity as soon as an unusual withdrawal or suspicious session appears.

On the product side, we are one of those links ourselves. Our firmware and management software run on large industrial mining fleets, so our top priority is making sure they never become a back door into our clients’ networks or assets. That is why we build on zero-trust architecture, with secure boot, signed updates and verification at every step, so that nothing running on physical hardware can be tampered with remotely.

3. Lessons from the Binance case

LESSON 5. RISK MANAGEMENT

Before chasing higher yields, understand where the returns come from and what risks you're taking.



Maxim Galash, CEO
Coinchange

The Binance incident is a reminder that part of any return above the risk-free rate is payment for the risk that the platform fails. Investors usually compare platforms by the rates they offer, but the rate says nothing about how large that risk is, and for years the market had no clear way to measure it.

The cost of ignoring it is easy to underestimate. A $100 million portfolio earning 6% makes $6 million a year, so if the assets are lost in a single platform failure, it would take more than ten years of returns to make up for it. Against that, an extra fraction of a percent in yield says very little on its own, and it’s worth weighing against the risk you take to get it.

KEY TAKEAWAY

Part of any yield is payment for the risk that the platform fails

Example: you keep $100M on a platform that pays 6% a year.

1	You earn	$6M a year
2	If the platform fails, you can lose	$100M
3	To earn that back, you need	more than 10 years

Based on Maxim Galash’s commentary, CEO of Coinchange

3. Lessons from the Binance case

At Coinchange, we see this every day in conversations with clients' risk committees, who increasingly want to understand the risk behind a strategy before they look at its return. No client assets were affected by the Binance breach, but the incident made us speed up how quickly and in how much detail we can show clients where their exposure lies.

"We take security and counterparty risk management seriously, structuring strategy execution and custody around the core principles of capital preservation."

For the market as a whole, the problem is that this risk is still hard to measure from the outside. Crypto already has tools that can limit the damage, from freezing stolen tokens to on-chain tracing, but they are used unevenly and rarely written into contracts. Making them standard, and adding disclosed security standards, priced insurance and risk ratings, would give investors a way to compare platforms by risk as easily as by yield.

LESSON 6. VERIFICATION

Find out in advance what happens to your assets if the platform is hacked or something else goes wrong.



Brice Vandevoorde, CEO
Realiz Group

Clients will stop accepting "trust us" and start asking "show us." Binance deserves credit for covering the loss from its reserves, but that protection came from one company's balance sheet, not from the structure. Banks, family offices and institutional investors will now ask the same questions they ask in TradFi, and they will expect to see the answers on paper.

For us, the case confirms our choices more than it changes them. Realiz has built on regulated Luxembourg infrastructure with licensed partners for custody, trading and compliance. We never hold client assets ourselves, so no single point of failure, including us, can put investor capital at risk.

With counterparties, we'll push even harder on the questions we already ask, especially who supervises them and how they vet their own people, because a regulator's oversight and a partner's hiring checks are things we can verify rather than take on trust.

3. Lessons from the Binance case

KEY TAKEAWAY

Find out what can happens to your assets if something else goes wrong

1. Where are the assets legally held?
2. Who is the regulated custodian?
3. What happens if the platform is compromised?

Based on Brice Vandevoorde's commentary, CEO of Realiz Group

Digital assets are now valuable enough to attract state-level attackers. Large pools of value concentrated on a few platforms make easy targets, and the weak point is often a person. With AI, technology moves so fast that security becomes outdated faster than ever. And not everyone is honest, which won't change anytime soon. Part of our role is also to raise our children with better values.

The answer isn't to step back. It's to apply what made traditional markets resilient: separation of issuer, custodian and venue, supervision, legal certainty and accountability. These are things clients can verify rather than take on trust. MiCA, the DLT Pilot Regime and Luxembourg's blockchain laws were built for exactly this.

The main lesson is that security depends on structure as much as on technology. The attackers didn't break the cryptography but tricked one person. No system is hack-proof, but you can design one so that a breach doesn't become a client loss.

4. Five layers of capital preservation

Capital preservation is a business decision as much as a security feature. The Binance case shows that even the strongest security systems can fail. The consequences of an attack depend on how client assets are held, how risks are distributed and whether the platform can absorb the loss.

For investors, this means looking beyond security at the whole platform: its business model, custody arrangements, infrastructure and risk controls, and how well they work together to preserve capital.

The five-layer framework below brings these factors together and offers a practical way to assess how crypto platforms protect client assets and manage risk.

Layer 1

Business model, horizon and risk governance

ASK

How does the business earn, where does its liquidity come from and over what horizon does it plan?

LOOK AT

The source of income (fees for services versus returns from reinvesting client assets), the funding of loans and withdrawals (independent funding sources versus client deposits), the alignment of product terms with clients' investment horizons.

WHY IT MATTERS

Binance could cover the loss because it had more than $6.34 billion in company funds to draw on. Celsius, which paid clients up to 18% on their deposits, had no such cushion in 2022.

Layer 2

Holding, segregation and reuse of client assets

ASK

Whose assets are they, and what are they allowed to be used for?

LOOK AT

The legal ownership of client assets, their segregation from the platform's own funds, the conditions under which they can be pledged or reused, the independence of custody from trading activities.

WHY IT MATTERS

After the hack, Binance's Proof of Reserves showed client holdings in ten major assets backed at least 1:1. At FTX, client deposits had been diverted to Alameda Research, and the gap surfaced as soon as clients tried to withdraw.

4. Five layers of capital preservation

Layer 3

Counterparties and concentration

ASK

How many parties can reach the assets, and how much capital sits with one venue?

LOOK AT

Custodians, venues, lenders, service providers and their roles; shared infrastructure.

WHY IT MATTERS

Binance froze withdrawals for nearly three days, locking in everyone who held liquidity there. After the Kelp DAO exploit, Aave deposits fell by $15 billion, although Aave itself had not been hacked.

Layer 4

Signing and operational security

ASK

Who can request, approve and execute a transfer?

LOOK AT

Approval and execution roles; hot wallet exposure and device security.

WHY IT MATTERS

At Binance, a compromised engineer's laptop led to a service that could submit withdrawals; at Bitget, spoofed transaction data triggered the exchange's own approvals. In neither case were private keys stolen.

Layer 5

Record under stress

ASK

Has the platform ever been hacked, and how did it respond — to its own incidents and to major hacks at other platforms?

LOOK AT

Any past incidents and how they were handled, and what the platform said publicly after major hacks elsewhere.

WHY IT MATTERS

A platform's past behaviour is the best guide to how it will act under pressure. How it handled earlier incidents, and how openly it responded to others, shows what clients can expect if something goes wrong.

Sources

1. Binance. (2026, October 30). Security incident update. Binance Square. https://www.binance.com/square/post/382974122328634
2. Binance. (2026, November 3). Preliminary investigation report on the 29 October security incident. Binance Square. https://www.binance.com/square/post/384314395829022
3. Bit.com. (2026, September 28). Bitget hack: How spoofing took $387.5 million without a stolen key. BIT Knowledge Hub. https://www.bit.com/knowledge-hub/bitget-hack
4. Bit.com. (2026, August 7). Coldcard: The security-first wallet that got hacked. BIT Knowledge Hub. https://www.bit.com/knowledge-hub/coldcard-the-security-first-wallet-that-got-hacked
5. BleepingComputer. (2026, October 30). Binance links $6.3 billion crypto theft to compromised DevOps laptop. https://www.bleepingcomputer.com/news/security/binance-links-63-billion-crypto-theft-to-compromised-devops-laptop/
6. Coinpaprika. (2026, November). DeFi risks explained: Smart contract, oracle & curator risk. https://coinpaprika.com/education/defi-risks
7. Cointelegraph. (2026, April 22). Aave deposits fall by $15B as Kelp exploit sparks flight from DeFi lender. https://cointelegraph.com/news/aave-deposits-drop-15b-kelp-dao-exploit
8. Cryptopolitan. (2026). Binance completes Proof of Reserves after $6.3B hack as withdrawals resume. https://www.cryptopolitan.com/binance-completes-proof-of-reserves-after-6-3b-hack-as-withdrawals-resume/
9. Cryptsy. (2026). Crypto hacks 2026: Losses by month, attack and target. https://cryptsy.com/crypto-hacks/
10. Decrypt. (2026, October 30). Binance sets aside $6.34B to cover hack losses, CEO says "your assets are safe". https://decrypt.co/382237/binance-sets-aside-6-34b-to-cover-hack-losses-ceo-says-your-assets-are-safe
11. DefiLlama. (2026). Crypto & DeFi hacks database [Data set; data for January–October 2026, accessed November 2026]. https://defillama.com/hacks
12. eSecurity Planet. (2026, October 14). Ledger confirms hardware wallet tampering amid $86M crypto theft reports. https://www.esecurityplanet.com/threats/news-ledger-hardware-wallet-tampering-crypto-thefts/
13. European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets (MiCA). Official Journal of the European Union, L 150, 40–205. https://eur-lex.europa.eu/eli/reg/2023/1114/oj
14. Fortune. (2022, June 13). Celsius blocks withdrawals after offering 18% interest on crypto deposits. https://fortune.com/2022/06/13/celsius-blocks-withdrawals-18-percent-interest-crypto-alex-mashinsky/
15. Halborn. (2026, April). Explained: The Kelp DAO hack (April 2026). https://halborn.com/blog/post/explained-the-kelp-dao-hack-april-2026
16. HashCore. (n.d.). HashCore Pulse. https://hashcore.com/pulse
17. Huerta de Soto, J. (2020). Money, bank credit, and economic cycles (4th ed.). Ludwig von Mises Institute. https://mises.org/library/book/money-bank-credit-and-economic-cycles
18. Silicon Report. (2026, November 1). Binance begins restoring customer withdrawals after about $6.3B theft. https://www.siliconreport.com/binance-begins-restoring-customer-withdrawals-after-about-6-3b-theft
19. Teng, R. [@_RichardTeng]. (2026, October 30). We never use any customer funds, so they are not impacted [Post]. X. https://x.com/_RichardTeng/status/2116176335722913865
20. The Block. (2022, June 13). Crypto lending firm Celsius pauses withdrawals and transfers, citing market conditions. https://www.theblock.co/post/151522/crypto-lending-firm-celsius-pauses-withdrawals-and-transfers-citing-market-conditions
21. The Block. (2022, July 13). Crypto lender Celsius declares Chapter 11 bankruptcy in New York. https://www.theblock.co/news/regulation/2022-07-13-crypto-lender-celsius-declares-chapter-11-bankruptcy-in-new-york-157491
22. The Block. (2026, November 2). Binance completes latest proof of reserves as it works to restore assets, withdrawals after record hack. https://theblock.co/news/business/2026-11-02-binance-zero-knowledge-proof-of-reserves-snapshot-hack-recovery-432321
23. U.S. Securities and Exchange Commission. (2022, December 13). SEC charges Samuel Bankman-Fried with defrauding investors in crypto asset trading platform FTX (Press Release 2022-219). https://www.sec.gov/news/press-release/2022-219