BITPLANET

ISSUE ANALYSIS

Assessing Crypto Exchange Soundness: Large-Scale Hack Response and Institutional Operational Risk

Real asset-coverage capacity, market fallout and custodian due-diligence criteria, as seen through the Binance incident

PUBLISHER
Bitplanet Research Lab

DATE
2026 · 11 · 04

DATA AS OF
2026 · 11 · 03

Conflict of Interest Disclosure The publisher of this report is a listed company that holds bitcoin as a treasury asset and pursues businesses in digital assets and AI/data-center infrastructure. It may have interests in the choice of topic and its interpretation. The publisher does not appear as a subject of analysis in this issue and does not recommend the use of any particular exchange or asset-custody arrangement. This report is for information purposes only and is not investment advice. Price changes in past cases do not predict future prices.

EXECUTIVE SUMMARY

LOSS SIZE AND ABILITY TO PAY

Binance has put the hack loss at about $6.3 billion, more than 5 times the value of its Secure Asset Fund for Users (SAFU) just before the incident (about $1.2 billion) (our estimate)[1][2][3]. The company said that, by drawing on part of SAFU, part of its futures insurance fund and company funds, it had covered about 95% of the stolen amount in the same assets by November 2[1]. INTERPRETATION The partial resumption of withdrawals does not mean the loss figure alone can settle whether the exchange is insolvent. The company's real financial capacity to fund further purchases of the remaining tokens and to refill SAFU needs to be examined alongside it.

HOW THE PRICE SHOCK SPREAD

Over the three days from the day of the incident, the maximum drawdown on a closing basis was similar for bitcoin (5.0%) and ether (4.9%) (our estimate)[3]. According to Elliptic's November 2 count, the 18,270 BTC stolen in the initial theft had not moved, yet $627.7 million of derivatives positions were liquidated within 1 hour of the incident becoming known[4][5]. INTERPRETATION The initial price decline should be read as a market reaction to the hack news and the effect of cascading liquidations, rather than as direct market selling of the stolen bitcoin. That said, these data alone cannot fully separate the individual contribution of the two factors. Whether the stolen BTC moves to exchanges or over-the-counter (OTC) desks needs to be monitored on an ongoing basis.

OPERATING STANDARDS FOR INSTITUTIONS

As of 1:43 p.m. KST on November 3, Binance's public deposit and withdrawal status data showed withdrawals enabled for only 27 crypto assets in total. Even for the 10 major assets that had completed proof of reserves (PoR), withdrawals were possible on only 23 of their 72 asset-network pairs (our estimate)[6]. INTERPRETATION The fact that assets exist on an exchange's books and the ability of customers to withdraw them whenever they need to are entirely different matters. Companies and institutions holding bitcoin should look beyond the total reserves of their custodian and review separation of approval authority, withdrawal limits and alternative withdrawal routes in an emergency, taken together.

$6.3B

Binance hack loss

[1]

19%

Pre-hack SAFU value as a share of the loss
(our estimate)

[2][3][1]

27 / 908

Crypto assets open for withdrawal (13:43 KST, November 3)

Count listed in public status data, incl. unsupported tokens

[6]

CONTENTS

01 The hack loss and what actually funds the coverage

02 The gap between 95% coverage and real withdrawal access

03 The bitcoin price decline after the hack and how the shock spread

04 The gap between bitcoin holdings and real withdrawal capacity in an emergency

C Exchange soundness, judged by actual payout after an incident

R References

A Appendix

01 INCIDENT

The hack loss and what actually funds the coverage

At 20:05 UTC on October 29, the first outflow occurred from a Binance wallet on the XRP Ledger. According to TRM Labs, most of the funds left across 10 blockchain networks over about 20 minutes, and a second wave of outflows followed about 3 hours later[7]. Binance formally put the total loss at about $6.3 billion[1]. Chainalysis counted $6.4 billion, and Elliptic counted a total of $6.43 billion across 11 chains including NEAR[8][4]. On October 31, the US Federal Bureau of Investigation (FBI) attributed the attack to TraderTraitor, a North Korea-linked hacking group[9]. North Korea's Kim Yo Jong, for her part, formally denied any involvement on November 3[10].

Table 1. Key timeline from the first outflow to the Phase 2 withdrawal reopening

Time (UTC)	Time (KST)	Event
October 29 20:05	October 30 05:05	First outflow from a Binance wallet on the XRP Ledger, spreading to 10 chains over about 20 minutes[7]
22:15	07:15	Binance suspends withdrawals[11]

Time (UTC)	Time (KST)	Event
October 30 00:13	09:13	Formal pledge to cover customer losses in full[11]
October 30 19:33	October 31 04:33	More than $6.34 billion of company funds set aside; about 80% covered in the same assets as those stolen[1]
November 1 06:00	November 1 15:00	95% coverage announced, then Phase 1 withdrawals reopen, starting with bitcoin [1][12]
November 2 12:45	November 2 21:45	Proof of reserves (PoR) published for 10 major assets as of October 31[1]
November 3 04:00	November 3 13:00	Phase 2 withdrawals begin reopening in sequence for designated assets on 9 networks[1]

※ The detailed timeline of outflows by chain and of freeze and coverage announcements is set out in Appendix ④.

The risk of a structure that combines operating access and transfer approval authority

According to blockchain security firm Blockaid, the attacker registered malicious EIP-7702 delegation code on the Ethereum hot wallet "Binance 14". Just 3 minutes 24 seconds later, a single transaction drained 167,464 ETH along with a number of other tokens[13]. EIP-7702 is an Ethereum standard feature that uses a valid signature from the wallet owner to have the code of a designated smart contract executed directly in that wallet's context[14]. From the bitcoin hot wallet, 18,270 BTC left through ordinary signed transactions. Citing the fact that multiple blockchain wallets produced valid withdrawal signatures within a short window of about 30 minutes, TRM Labs assessed that the core infrastructure the exchange uses to sign hot wallet transactions had likely been compromised[7].

Binance said its initial investigation suggested that the attacker reached the software runtime environment (service containers) via the personal laptop of a development and operations (DevOps) engineer, and that unauthorized withdrawal requests may have been executed through that route[1]. The company later said it had identified additional points of breach but had found no evidence that wallet private keys themselves were leaked. It plans to publish a detailed incident report once its full investigation is complete[1].

INTERPRETATION If the signing and approval system itself could be abused without any private key being leaked, then the firm-wide internal control process running from withdrawal request to approval needs to be re-examined from the ground up, along with the physical custody of keys. If an attacker who breaks into operating systems can bypass and obtain final withdrawal approval authority as well, damage spreads in an instant across every system that shares the approval path, even when assets are physically spread across chains.

Recovery and coverage paths that diverged sharply by asset type

Table 2. Freeze mechanisms and coverage status by type of stolen asset

Asset	Amount taken	Freeze mechanism	Status on November 2	Coverage by Binance
Stablecoins (USDT, USDC, RLUSD)	About 3.4 billion tokens (53.4% of total outflows estimated by TRM)[7]	Issuers have centralized address-freeze functions	Freezes carried out by each issuer (total frozen or seized across all assets: $2.85 billion)[4]	Customer balances in the 10 major assets announced as fully backed[1]
Bitcoin	18,270 BTC[7]	No issuer freeze mechanism	No movement from 19 addresses as of the 07:00 UTC count on November 2[4]	BTC customer balances announced as fully covered[1]
Ether	200,630 ETH[7]	No protocol-level freeze mechanism (though decentralized lending services can restrict new transactions)[15]	Attacker swapped stolen assets mainly into ETH[9]	Customer balances in the 10 major assets announced as fully covered[1]
Low-liquidity tokens still being purchased	About 5% of the loss (company statement)[1]	Varies with how each token is controlled	Process of sourcing the required amounts in the market under way	Further purchases under way on the open market and over the counter (OTC)[1]

On a blockchain, a "freeze" ties up stolen assets so that they can no longer move, while "recovery" means the process by which the exchange actually gets those assets back. "Covering customer assets," by contrast, means the company putting in its own resources to replace them with assets of the same type, and a "customer payout" is complete only when customers actually withdraw their assets through withdrawal requests. Frozen amounts counted by TRM or Elliptic therefore do not translate directly into cash-equivalent amounts returned to the exchange. Tether said it had itself frozen more than $1.5 billion of USDT, and Reuters reported that Circle's USDC freezes exceeded $1.1 billion[16][17].

INTERPRETATION Even when the same amount is stolen, the practical recovery path and its cost differ completely depending on which type of asset was taken. With stablecoins, central control by the issuer can quickly block an attacker from cashing out, but separate legal and administrative steps are needed before those funds can be returned to the exchange. Bitcoin and ether, on the other hand, have no function for forcibly locking an address, so before any recovery an exchange may have to deploy its own liquidity or buy the assets directly in the market to make customer balances whole. The remaining roughly 5% that Binance has yet to fully secure consists of tokens with very low liquidity, and the time needed to source them is also a factor delaying the point at which coverage of all customers is complete[1].

02 RECOVERY

The gap between 95% coverage and real withdrawal access

Binance's recovery should be assessed along three separate dimensions: the share of stolen assets it has re-secured, the range of assets for which withdrawals are actually allowed, and its liquidity capacity to absorb withdrawal demand. The "95% coverage" the company announced publicly refers to the first of these: the share of total stolen assets that it has replenished from its own resources.

Table 3. Three key indicators for assessing an exchange's state of recovery

Indicator	Definition	Value on November 3	Limits of interpretation
Coverage ratio	Share of the total value of stolen assets re-secured in the same assets	About 95%[1]	Relies on the company's own figures; may vary with the total-loss basis used as the denominator
Withdrawal access	Range of crypto assets and networks for which withdrawals are actually allowed	Withdrawals open for only 27 of 908 listed in the public status data (40 of 1,365 asset-network pairs)[6]	Based on a 13:43 KST query. The denominator also includes delisted tokens no longer supported for trading, among others
Liquidity response	Cumulative net outflows since withdrawals reopened, compared with total platform assets	Cumulative net outflows of $4.72 billion, 2.8% of total platform assets ($171 billion)[17][12]	A snapshot observed while withdrawals were only partly open for some major assets

Assets secured, but withdrawal routes not yet open

Binance began withdrawal services at 06:00 UTC on November 1, starting with bitcoin, for the 15 networks designated for Phase 1[1][12]. According to a status page checked by The Block the same day, however, withdrawals were still blocked for 531 of 552 coins in total[18]. As of 9:32 a.m. KST on November 3, Binance's public status data showed withdrawals allowed for only 14 assets and 27 asset-network pairs. After Phase 2 withdrawals reopened at 1 p.m., withdrawable assets had expanded to only 27 assets on 14 networks, 40 pairs in total, at 1:43 p.m. The 10 major assets that had completed proof of reserves (PoR) verification could each be withdrawn on at least one network, but only 23 of their 72 network pairs in total were actually open for withdrawal (our estimate)[6]. The same crypto asset is treated as a separate pair for each blockchain network it uses.

Of the 1,325 pairs on which withdrawals remained blocked, 505 were marked "Wallet Maintenance," 389 "Low Hot Wallet Balance" and 341 "Unsupported Token" (our estimate)[6]. Binance explained the low hot wallet balance by saying that it was temporarily limiting withdrawals while it refilled and moved funds into its hot wallets. Further networks will open in sequence only after each network fully passes its own security and stability checks[1].

INTERPRETATION Even when assets are fully recorded in the proof-of-reserves ledger, they can move only once the technical withdrawal route that lets customers actually send them out is opened. Safely refilling hot wallet balances and running technical checks network by network takes real time. Withdrawal delays should therefore not be read straight away as a fundamental asset shortfall at the exchange. Conversely, the limited suspension reasons the company has disclosed are not enough to accept without question that every withdrawal delay is purely a matter of operating procedure.

What SAFU absorbed and how company resources were brought in

SAFU (Secure Asset Fund for Users) is an emergency reserve that Binance built up by converting the entire fund, about $1 billion, into bitcoin in February[19]. Just before the hack, the SAFU bitcoin wallet was worth about $1.2 billion, around 19% of the total loss in this incident (about $6.3 billion) (our estimate)[2][3][1]. On October 30, Binance set aside more than $6.34 billion of company funds to cover customer assets, of which about $5 billion was already held as reserves in the same types of assets as those stolen. On October 31 it then formally designated part of SAFU, the surplus in its futures insurance fund above risk-management thresholds, and additional company resources as funding for loss coverage[1]. The same day, 7,499 BTC, half of the reserve, was transferred out of the SAFU wallet[2].

As of 9:31 a.m. KST on November 3, about 7,500 BTC remained at SAFU's public blockchain address, worth about $577 million at the bitcoin price at the time. At the same price, about $423 million of additional funds would be needed to reach the SAFU refill target of about $1 billion that Binance has stated (our estimate)[2][3][1]. Before the incident, Binance's total public wallet balances amounted to about $144 billion, but because that figure includes assets deposited by customers worldwide, it must be kept strictly apart from the resources the company can freely use to cover losses[20][21].

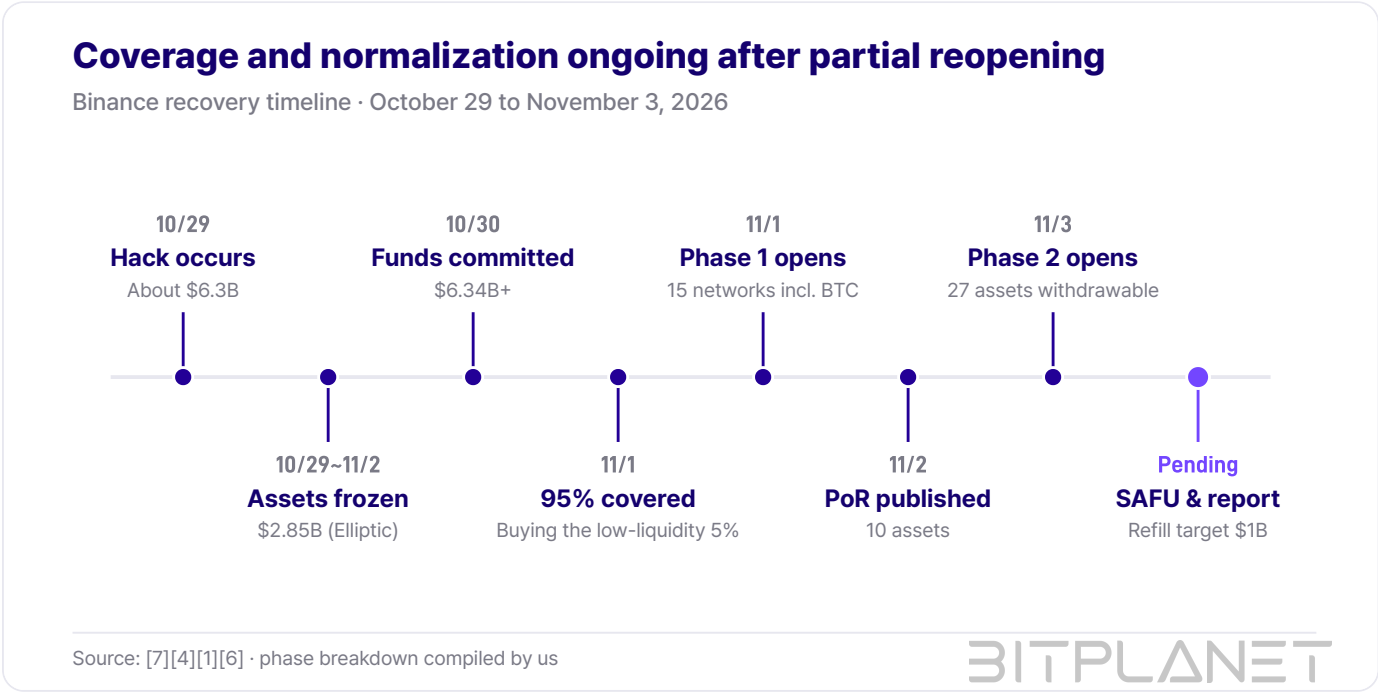
INTERPRETATION Since SAFU alone could not cover even 1/5 of the total loss, a large injection of additional company resources was unavoidable to cover customer assets in full. Binance added its own corporate funds to SAFU and part of its futures insurance fund. With SAFU's bitcoin holdings cut in half as a result, its capacity to absorb any further black swan (an unexpected incident) is substantially weakened until the fund is fully refilled to its target level. If another security incident or asset loss occurs during this vulnerable period, the company will bear an even heavier financial burden.

The limits of what proof of reserves and net outflow data show

At 12:45 UTC on November 2, Binance published proof of reserves for 10 major crypto assets as of 00:00 UTC on October 31. Customers holding BTC, ETH, USDT, BNB, SOL, USDC, XRP, USD1, RLUSD and ZEC can each verify whether their deposit balances were properly included in this attestation[1]. According to crypto.news, reserve ratios for the major assets stood at 100.04% for bitcoin, 101.30% for BNB and 100.00% for Tether (USDT). The USDT reserve ratio in particular came down somewhat from 103.88% as of October 1, and the number of assets covered by the regular report was cut sharply from 55 to 10[22]. Binance plans to widen the range of covered assets again on November 4 and update its balance records[1]. Proof of reserves is a procedure that confirms holdings of the covered assets and the level of backing against customer balances at a particular snapshot. It is not a full audit by an accounting firm certifying the exchange's total contingent liabilities and overall financial soundness[21].

Cumulative net outflows in the first 9 hours 30 minutes after withdrawal services partially reopened reached about $3.64 billion[12]. A Binance spokesperson then told Reuters on November 2 that cumulative net outflows had reached $4.72 billion[17]. According to DefiLlama data cited by The Block, 24-hour net outflows peaked at about $7 billion before easing to about $3.29 billion as of November 2[23].

INTERPRETATION Net outflow data from a controlled state, in which withdrawals are allowed only for a limited set of assets and networks, make it hard to assess objectively whether the exchange could cope if all customers demanded full withdrawals. If the range of permitted withdrawals is opened up fully, pent-up withdrawal demand could surge and net outflows could spike again.



03 MARKET IMPACT

The bitcoin price decline after the hack and how the shock spread

Table 4. Bitcoin and ether returns around the hack

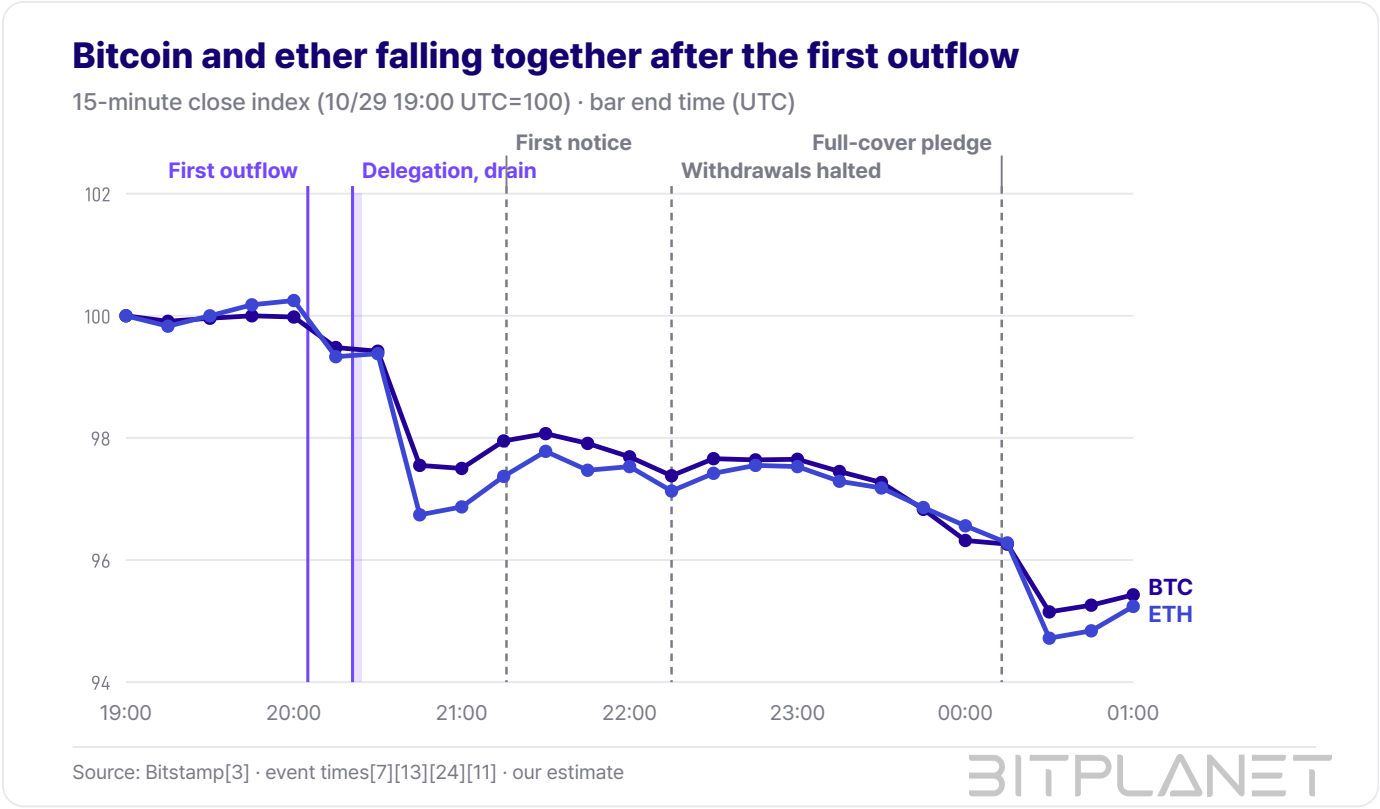
Time (UTC)	Event	BTC 1h return before	BTC 1h return after	BTC 4h return after	ETH 1h return after	ETH 4h return after
October 29 20:05	First outflow occurs	-0.02%	-2.48%	-3.66%	-3.36%	-3.67%
21:16	Exchange issues first official notice	-1.54%	-0.58%	-2.52%	-0.24%	-2.11%

Time (UTC)	Event	BTC 1h return before	BTC 1h return after	BTC 4h return after	ETH 1h return after	ETH 4h return after
22:15	Crypto withdrawals suspended	-0.58%	0.07%	-2.29%	0.16%	-2.70%
October 30 00:13	Pledge to cover customer losses in full	-1.36%	-0.93%	0.32%	-1.36%	-0.71%
November 1 06:00	Phase 1 withdrawal services reopen	0.10%	0.14%	0.30%	0.03%	0.08%

※ Returns calculated from the close of the last 15-minute bar completed by each reference time. For example, the reference price for 20:05 is the close of the bar that ended at 20:00 sharp (our estimate)[3].

In the 1 hour after the first outflow, bitcoin fell 2.48% and ether 3.36%. From the 20:00 bar to the 00:15 bar, just after the pledge to cover losses in full, the cumulative decline came to 3.72% for bitcoin and 3.96% for ether. Over the three days from the day of the incident, the maximum drawdown on a closing basis was 5.0% for bitcoin and 4.9% for ether, and on an intraday-low basis 6.2% and 7.9% respectively. Both assets showed only minimal volatility around the Phase 1 withdrawal reopening (our estimate)[3].

INTERPRETATION Because bitcoin and ether fell together right after the first outflow, it is hard to read the move simply as a shock from bad news specific to bitcoin. Ether, however, was also a direct target of this hack, and the FBI said the attacker was converting other stolen altcoins into ether[9]. A simple comparison of the two assets' returns therefore cannot cleanly separate a bitcoin-specific price shock from market-wide risk-off sentiment.



The price decline and its transmission through supply, liquidations and risk-off

According to Elliptic's count at 07:00 UTC on November 2, the 18,270 BTC taken in the initial theft were split across 19 separate blockchain addresses and have sat there without further movement. However, in the course of converting other stolen funds into bitcoin, funds worth about 28 BTC were found to have passed through CoinJoin, a technique that bundles many transfers into one to obscure tracing[4].

A heavy wave of forced liquidations hit the market early in the incident. According to CoinGlass data cited by BeInCrypto, $627.7 million of derivatives positions were liquidated in just 1 hour after news of the hack reached the market, and about 97% of that volume was long positions betting on price rises[5]. Bitcoin was already in a downtrend, having fallen 3.3% over the week and 2.6% over the month to the day before the incident (our estimate)[3].

Trading volumes also surged in the domestic Korean crypto market right after the incident. Daily trading value in Upbit's BTC/KRW market reached KRW 168 billion on October 30 (UTC daily bar), 2.49 times the average for the prior 7 days (October 22–28). It then returned to the pre-incident 7-day average level on November 2 (our estimate)[25].

INTERPRETATION No large further movement of the stolen bitcoin was observed, yet the sharp market-wide price decline and large derivatives liquidations were real. Direct market selling pressure from the stolen bitcoin alone is therefore not enough to explain the initial price shock. How far cascading liquidations amplified the decline, and how much risk-off sentiment from weaker investor confidence played a part, are hard to quantify from these data alone. Separately, the minimal price movement observed right after withdrawals reopened may also reflect recovery expectations being priced in ahead of time, so it cannot be equated with a full assessment of the exchange's ability to pay.

A multi-angle comparison with 8 past major exchange incidents

The comparison covers 8 past exchange incidents in total. Alongside the Mt. Gox collapse, which saw the largest bitcoin loss on record, we selected the main cases that dealt a major shock to the industry[26]. Each incident falls into one of three types, depending on who (customers or the exchange) absorbed the loss and how. Mt. Gox and FTX halted withdrawals and then entered bankruptcy and rehabilitation proceedings[27][28]. Bitfinex chose a forced haircut, cutting customer account balances across the board by 36.067%[29]. Coincheck, KuCoin, DMM Bitcoin, Bybit and Bitget, on the other hand, covered customer losses using recovered funds together with their own resources, insurance funds and similar sources.

Setting each incident's close on the day before its reference date at 100, we calculated how far bitcoin fell to its lowest close among the UTC daily bars over the three days (3D) and seven days (7D) starting on the reference date. The intraday maximum drawdown was calculated separately from the lowest intraday price over the three days[3]. For Mt. Gox and FTX, the date withdrawals were fully halted was used as the reference date. In FTX's case, the hack itself occurred on November 12, after the withdrawal halt, so separate values based on the hack date are also shown[30].

Table 5. Loss size and maximum bitcoin drawdown in past major exchange incidents, by type

Incident	Type	Price reference date (UTC)	Loss size	Share of BTC market cap	3D close	3D intraday low	7D close	ETH 3D close
Mt. Gox	Halt and bankruptcy	February 7, 2014 (withdrawal halt)	About 650,000 BTC (revised estimate) [26]	5.22%	-10.9%	-19.0%	-20.9%	N/A
FTX	Halt and bankruptcy	November 8, 2022 (withdrawal halt)	Misuse of customer deposits[31]	N/A	-22.9%	-24.1%	-22.9%	-29.9%
FTX (hack date)	Halt and bankruptcy	November 12, 2022	$477 million[30]	0.15%	-4.1%	-7.2%	-4.1%	-5.1%
Bitfinex	Customer haircut	August 2, 2016	119,756 BTC[32]	0.76%	-10.9%	-23.3%	-10.9%	N/A
Coincheck	Exchange-covered	January 26, 2018	About $530 million[33]	0.28%	-0.6%	-8.0%	-19.3%	0.0%
KuCoin	Exchange-covered	September 26, 2020	About $285 million[34]	0.14%	0.0%	-0.9%	-1.0%	0.0%
DMM Bitcoin	Exchange-covered	May 31, 2024	4,502.9 BTC[35]	0.02%	-1.3%	-2.5%	-1.3%	0.0%
Bybit	Exchange-covered	February 21, 2025	About $1.5 billion[36]	0.08%	-2.2%	-3.6%	-14.5%	-2.8%
Bitget	Exchange-covered	September 24, 2026	About $388 million[37]	0.02%	-0.3%	-1.8%	-1.1%	0.0%
Binance	Exchange-covered	October 29, 2026	About $6.3 billion[1]	0.39%	-5.0%	-6.2%	Pending	-4.9%

※ Prices and shares of market cap are based on raw data from Bitstamp and Blockchain.com[3][38]. The Mt. Gox share uses circulating supply at the end of February 24, the day before the site closed; the others use the day before the hack was disclosed[26]. ETH values are not shown for incidents before 2017, for which Bitstamp has no ETH prices. Binance's 7-day value can be calculated after the UTC daily bar closes on November 4. 0.0% covers both cases with no close below the reference price and cases with a small decline that rounds to 0.0% at one decimal place.

Table 6. Treatment of customer assets and time to withdrawal reopening or repayment in past incidents

Incident	Treatment of customer assets	Withdrawal halt	Time to reopening, start of repayment or transfer	Final repayment and resolution
Mt. Gox	Bankruptcy and rehabilitation	BTC withdrawals halted February 7, 2014[27]	No reopening. 3,801 days until BTC/BCH repayments began (July 5, 2024)[39]	Repaid in instalments in yen and BTC/BCH under the rehabilitation plan[39]
FTX	Bankruptcy	November 8, 2022[28]	No reopening. 833 days until first distributions to small creditors began (February 18, 2025)[40]	Cash distributions based on dollar values as of the bankruptcy petition[40]
Bitfinex	Customer haircut	August 2, 2016	8 days (reopening on August 10 as scheduled by the company)[29]	BFX tokens issued. Some converted into equity; remaining tokens redeemed on April 3, 2017[29]
Coincheck	Exchange-covered	January 26, 2018; full halt including yen	Yen 18 days; 5 assets including BTC 45 days[41][42]	Cash compensation of JPY 88.549 per 1 XEM to NEM holders[43]
KuCoin	Exchange-covered	September 26, 2020	BTC, ETH and ERC20-USDT 11 days. Reopening of all tokens announced at 57 days (some limits and exceptions kept)[34]	Losses beyond recovered funds covered by the company and its insurance fund[34]
DMM Bitcoin	Exchange-covered	Crypto-asset withdrawals halted May 31, 2024; yen withdrawals maintained[35]	281 days until accounts were transferred to SBI VC Trade (March 8, 2025)[44]	BTC fully guaranteed with group support, then business closed and transferred[35][44]

Incident	Treatment of customer assets	Withdrawal halt	Time to reopening, start of repayment or transfer	Final repayment and resolution
Bybit	Exchange-covered	No halt[45]	Processing of withdrawal requests announced as complete about 13 hours after the hack[45]	ETH shortfall filled within 72 hours; 1:1 reserves maintained[45]
Bitget	Exchange-covered	September 24, 2026[37]	BTC 4 days, USDT 6 days, other tokens and fiat 8 days[37]	Covered with a protection fund; company said customer balances were unaffected[37]
Binance	Exchange-covered	October 29, 2026[11]	Phase 1 (BTC and others) 3 days, Phase 2 5 days. Full reopening in progress[1]	About 95% replenished with company funds, SAFU and the futures insurance fund[1]

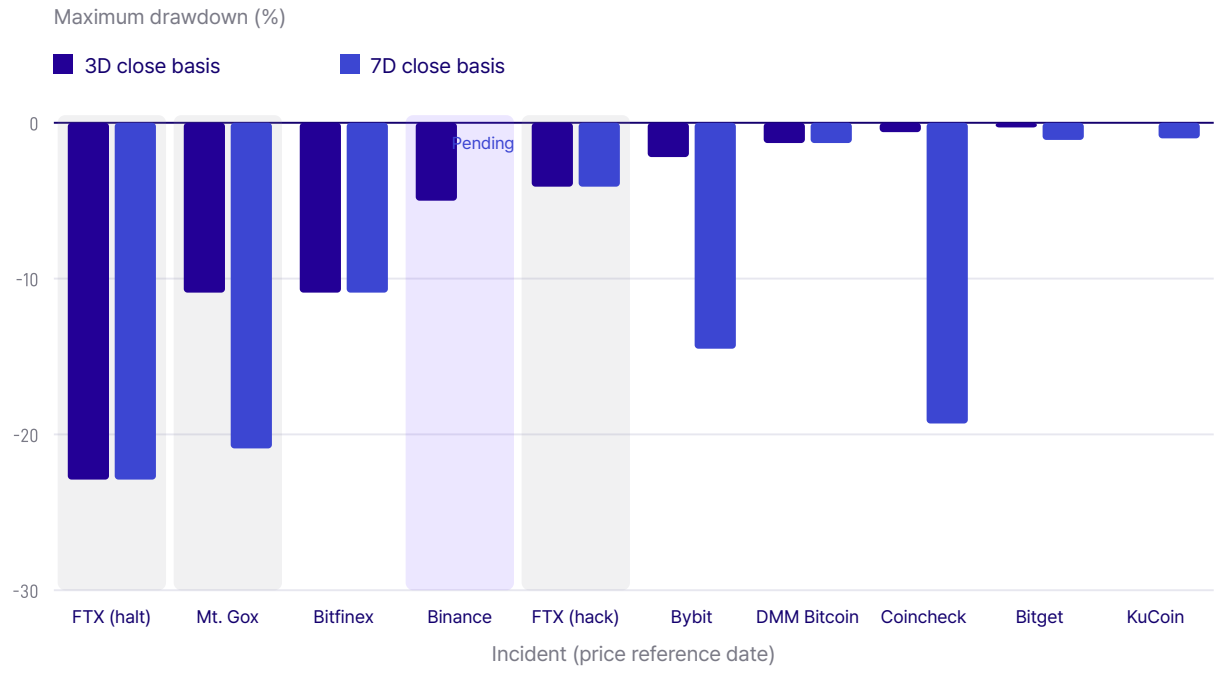
※ Day counts are calendar-day differences between the withdrawal halt and each reopening, distribution or transfer date (our estimate). The time to reopening differs from the time to post-bankruptcy distributions or account transfers. Coincheck dates are as reported in Japan time.

INTERPRETATION The 3 past cases in which the three-day maximum drawdown on a closing basis from the reference date exceeded 10% were all catastrophic cases in which withdrawal services were never reopened or customer accounts were forcibly cut. By contrast, in the other 5 cases, where the exchange stepped in to cover losses in full, the three-day maximum drawdown on a closing basis was at most about 2.2%. Even among these well-handled cases, however, the time needed to normalize varied widely. KuCoin announced the reopening of deposits and withdrawals for all tokens after 57 days but kept some withdrawal limits and exceptions, while DMM Bitcoin gave up on reopening withdrawals itself and moved customer accounts to another firm after 281 days[34][44]. Bybit responded without halting withdrawals, yet its 7-day maximum drawdown on a closing basis widened to 14.5%[46]. That said, Bitfinex's haircut policy was announced after the three-day observation window, and FTX's 22.9% is the drawdown during the withdrawal halt before the hack[29]. Short-term price reactions alone are therefore not enough to assess each exchange's loss-bearing structure and financial soundness on a uniform basis.

Binance's 3-day drawdown in this incident (5.0%) is the largest among the 6 exchange-covered cases compared here. Its loss as a share of bitcoin market cap (0.39%) was meaningfully larger than in the other covered cases (0.02–0.28%), and the hack came at a fragile point, with bitcoin already under 3.3% of downward pressure over the preceding week. In addition, the October 29 daily bar used as the reference date also includes about 20 hours of trading before the first outflow occurred (our estimate)[7].

Larger three-day and seven-day drawdowns in halt and bankruptcy cas es

vs. close on the day before the reference date · grey band: halt and bankruptcy · purple band: Binance



Source: Bitstamp[3] · our estimate · unit % · Binance 7D calculated after the 11/4 close

BITPLANET

Larger three-day and seven-day drawdowns in halt and bankruptcy cases · Data table

Incident (price reference date)	3D close basis (%)	7D close basis (%)
FTX (halt)	-22.9	-22.9
Mt. Gox	-10.9	-20.9
Bitfinex	-10.9	-10.9
Binance	-5	Pending
FTX (hack)	-4.1	-4.1
Bybit	-2.2	-14.5
DMM Bitcoin	-1.3	-1.3
Coincheck	-0.6	-19.3
Bitget	-0.3	-1.1

Incident (price reference date)	3D close basis (%)	7D close basis (%)
KuCoin	0	-1

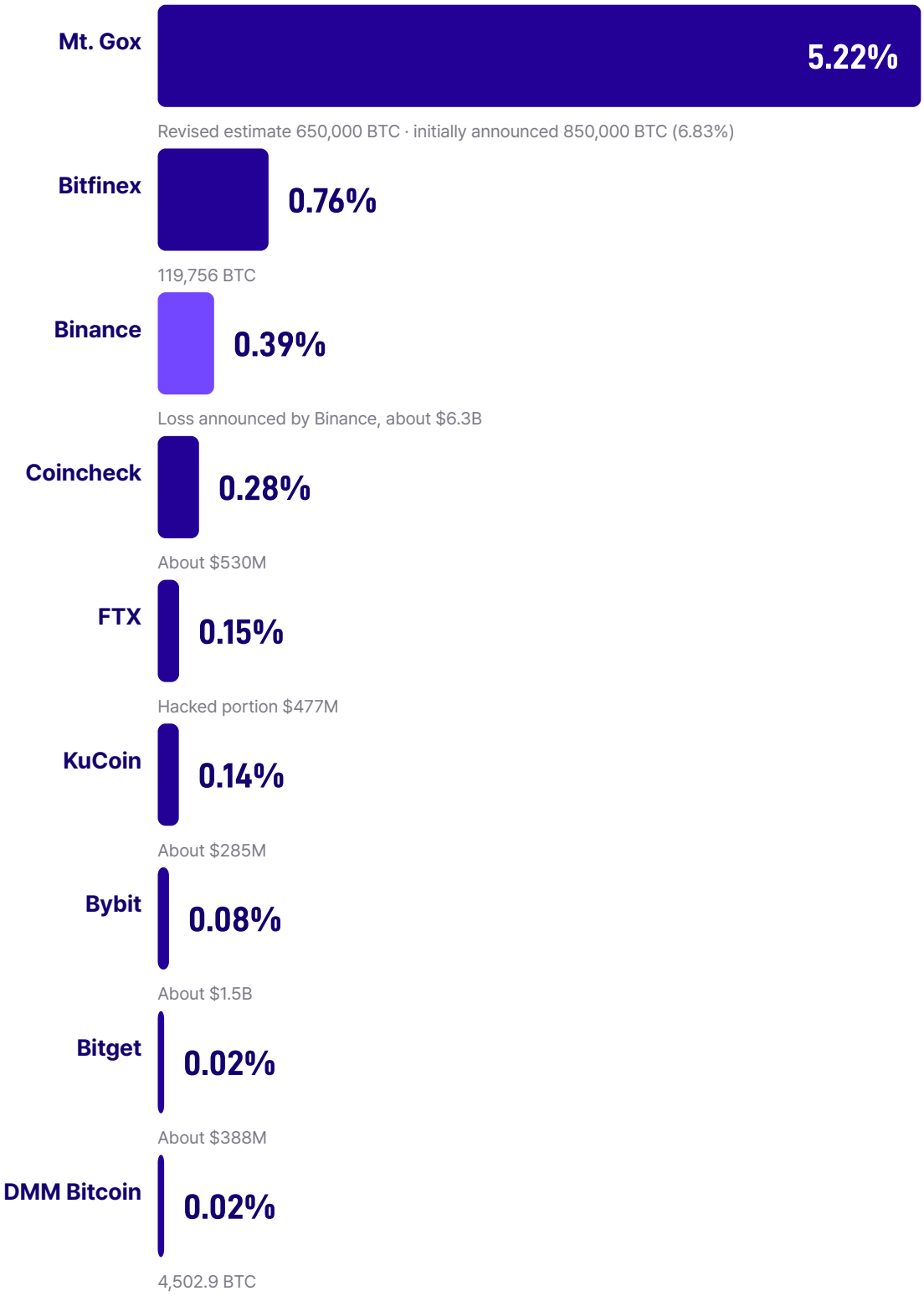
The loss relative to market size and to exchange resources

Binance's hack loss of $6.3 billion equals 0.39% of bitcoin's total market cap the day before the incident (about $1.6335 trillion) (our estimate)[3][38][1]. That is about 1/14 of the share calculated for the Mt. Gox collapse on the revised estimate of 650,000 BTC (5.22%). Against the share based on the originally announced 850,000 BTC (6.83%), it is only about 1/18 (our estimate)[26]. This ratio measures the loss against the size of the bitcoin market at the time; it does not directly indicate the actual price shock or the exchange's ability to pay.

To assess an exchange's real financial risk accurately, however, the comparison should be with the size of the resources the company can mobilize immediately to cover losses in an emergency, not with the total loss alone. In this incident the loss was more than 5 times the value of the Secure Asset Fund for Users (SAFU), and Binance said that, by mobilizing its own corporate funds and other resources, it had re-secured about 95% of the stolen assets within three days of the incident[1].

Binance loss at 1/14 of Mt. Gox relative to market size

Day before hack disclosure (%) · Mt. Gox based on supply the day before site closure (2/24)



Source: [3][38][26][1] and per-incident sources in Table 5 · our estimate

BITPLANET

Binance loss at 1/14 of Mt. Gox relative to market size · Data table

Item	Value	Note

Item	Value	Note
Mt. Gox	5.22%	Revised estimate 650,000 BTC · initially announced 850,000 BTC (6.83%)
Bitfinex	0.76%	119,756 BTC
Binance	0.39%	Loss announced by Binance, about $6.3B
Coincheck	0.28%	About $530M
FTX	0.15%	Hacked portion $477M
KuCoin	0.14%	About $285M
Bybit	0.08%	About $1.5B
Bitget	0.02%	About $388M
DMM Bitcoin	0.02%	4,502.9 BTC

04 INSTITUTIONS

The gap between bitcoin holdings and real withdrawal capacity in an emergency

The outflow of 18,270 BTC in this incident was accompanied by valid signatures from Binance wallets[7]. The company said its official investigation had found no evidence that the wallet private keys themselves were stolen. In the investigation disclosed so far, the targets flagged as possibly compromised are not the bitcoin protocol itself but the exchange's internal operating environment (DevOps) and its signing and approval system[1].

INTERPRETATION Ordinary companies and institutional investors that hold bitcoin as a large treasury asset should manage the internal approval framework and operational controls of the custodian holding it on their behalf as a core compliance risk, in addition to the market price risk of the asset itself. Losses arising from an exchange's operations, as in this Binance incident, must be clearly distinguished from a security failure of the blockchain network itself. Even with bitcoin on the balance sheet, without rigorous custody and withdrawal control procedures the asset cannot be put to use in time when it is needed in an emergency.

Table 7. Operational control criteria to check when using an exchange or custodian

Area	Detailed review items	Lessons from the Binance hack
Separation of approval authority	Full separation of operating-system access rights from actual asset-transfer approval rights, and mutual independence among approvers	Possibility raised that a hacker with access to the operating environment bypassed internal approval steps to request withdrawals[1]
Multi-approval framework	Multiple approvals required for large asset withdrawals and changes to wallet permissions	Abuse of the delegation feature, in which a malicious EIP-7702 delegation signature changes a wallet's executing code[13][14]
Withdrawal limits	Caps on cumulative withdrawals per hour and per transaction, and automatic withdrawal pauses when anomalous transactions are detected	Large sums left simultaneously from as many as 10 chains over about 20 minutes[7]
Wallet and custodian diversification	Physical diversification of assets by custodian, blockchain and individual wallet, and the share held in cold wallets	Hot wallets on multiple chains produced valid withdrawal signatures all at once within about 30 minutes[7]
Emergency withdrawal plan	Alternative withdrawal routes to activate if the main custodian's withdrawal service is suspended, and the reserve liquidity they require	Only 27 of 908 assets listed in public status data at 13:43 KST on November 3 open for withdrawal. Denominator also includes unsupported tokens[6]
Custodian soundness assessment	Beyond deposit size alone, verification of real capacity to guarantee payment, internal operating controls and post-incident service continuity	Weaker transparency, including a sharp cut in assets covered by proof of reserves from 55 to 10[22]

Korean financial regulators' approach to supervising virtual asset service providers points the same way. On November 2, the Financial Services Commission held an emergency inspection meeting with the Financial Supervisory Service, the Financial Security Institute, the Digital Asset eXchange Alliance (DAXA) and the heads of major domestic exchanges. Administrators' system access controls, strict withdrawal approval procedures, cold wallet storage ratios and the status of insurance and emergency reserves were the core items under review. Regulators asked domestic exchanges to raise the share of assets held in cold wallets, build up their own emergency reserves and monitor deposits and withdrawals at all times[47].

INTERPRETATION When assessing a crypto exchange or a specialist custodian, one should not be swayed by total asset holdings or by fragmentary proof-of-reserves figures alone. What needs to be verified, dispassionately, is whether it has in place in advance the substantial resources to return deposited assets to customers in full even after a major security incident, and transparent operating procedures to deploy them quickly. Even Binance could not fill the huge loss with its emergency fund SAFU alone and had to combine it at short notice with part of its futures insurance fund and its own corporate funds.

Domestic and overseas price gaps after adjusting for the USDT price

On October 30, Upbit and Bithumb posted notices urging caution when sending crypto assets to Binance and said they could restrict withdrawals if necessary[48][49]. This was a milder step than in the Upbit hack in November 2025, when major domestic exchanges fully suspended withdrawals to Upbit[50].

As of 9:29 a.m. KST on November 3, Upbit's KRW price for bitcoin was 1.15% higher than the Bitstamp USD price converted into won. The USDT premium on Upbit, calculated at the same exchange rate, was 0.99% (our estimate). At the previous observation points, the gaps were 1.6% and 1.3% respectively at 9:49 a.m. on October 30, and 0.52% and 0.39% respectively at 9:29 a.m. on November 2[3][25][51].

Table 8. Domestic and overseas price gaps for Upbit crypto assets, converted at the USDT price

Observation time (KST)	Upbit USDT price	BTC	ETH	XRP
October 29 09:29 (pre-incident)	KRW 1,339	0.16%	0.12%	0.06%
October 30 09:49	KRW 1,356	0.28%	0.29%	0.20%
November 2 09:29	KRW 1,340	0.13%	0.12%	0.06%
November 3 09:29	KRW 1,346	0.16%	0.19%	0.15%

※ Formula: Upbit KRW price ÷ (Bitstamp USD price × Upbit USDT KRW price) − 1. Based on 1-minute bar closes for the same minute (our estimate)[25][3].

Converted at the KRW price of USDT, the domestic and overseas price gaps for the 3 major assets, bitcoin, ether and XRP, narrowed to within 0.3% at all four observation points. Once the effect of the USDT price gap on Upbit is taken out of the domestic KRW premium, the residual price gap for each coin was minimal. The USDT price, however, reflects a combination of won-dollar exchange rate volatility and USDT supply and demand within the domestic market. Indeed, on October 30 total trading value in Upbit's KRW markets jumped to 2.49 times the daily average of the prior 7 days (October 22–28) for bitcoin, 2.31 times for ether and 1.88 times for XRP, before returning to the pre-incident 7-day average level on November 2 (our estimate)[25].

INTERPRETATION Although Upbit and Bithumb issued caution notices warning that withdrawals to Binance might be restricted, domestic and overseas price gaps after USDT conversion were not large at the 4 observation points analysed. This contrasts clearly with the halt of deposits and withdrawals at Upbit in November 2025, when the price of Jito (JTO) was more than 35% above overseas prices[52]. Still, the limited sample used here does not allow us to generalize that asset movement between domestic and overseas markets was fully smooth, or that the domestic-overseas price gaps came entirely from exchange rate moves.

C CONCLUSION

Exchange soundness, judged by actual payout after an incident

Within three days of the incident, Binance announced a plan for funding the coverage, said it had re-secured about 95% of the stolen amount in the same assets, and reopened withdrawal services for some major assets in phases. In the past, Mt. Gox and FTX failed to overcome their withdrawal paralysis and went straight into court-supervised rehabilitation and bankruptcy proceedings. It took Mt. Gox about 10 years to begin BTC/BCH repayments and FTX about 2 years to make its first cash distributions to small creditors.

Table 9. 5 key conditions for judging whether a crypto exchange crisis is subsiding

Condition	Status on November 3	Potential risk if the condition is delayed
Full coverage of all assets	About 95% secured; OTC purchases of the remaining 5% in low-liquidity tokens under way[1]	Prolonged withdrawal delays and deepening distrust among customers holding the not-yet-covered tokens
Normal withdrawals on major networks	27 assets open for withdrawal in public status data; only 23 of 72 pairs open for the 10 PoR assets[6]	An entrenched bottleneck in which customers cannot move deposited assets to safe outside custody
Handling large net outflows	Cumulative net outflows of $4.72 billion, about 2.8% of total platform assets[17][12]	Possibility that rising net outflows strain hot wallet liquidity when permitted withdrawals are widened fully
SAFU refill	About 7,500 BTC remaining (about $577 million), $423 million short of the $1 billion target[2][1]	A continued reduction in the buffer the exchange holds against the next unexpected security incident
Root cause and approval framework improvements	Official incident white paper to be published after the full investigation is complete[1]	Continued uncertainty over the breach path and whether the approval framework has been improved

INTERPRETATION The first thing to monitor is how fast the number of asset-network pairs with normal withdrawals expands and how smoothly customer withdrawals are actually processed. If the exchange buys the remaining tokens, widens the set of permitted withdrawals and still handles the incoming withdrawal requests without delay, its customer payout system can be judged to have effectively returned to a normal track. Conversely, if processing delays arise or withdrawal suspensions caused by low hot wallet balances recur, the exchange's liquidity management capability needs to be fully reassessed.

INTERPRETATION The follow-up reserve count scheduled for November 4 is the next piece of evidence for confirming the scope of the assets covered. Whether the stolen bitcoin flows to centralized exchanges or OTC prime brokerage desks also needs to be tracked separately, to gauge the risk of potential selling supply reaching

the market. Whether SAFU is fully refilled, together with the official incident investigation report and follow-up measures, should be used to verify whether the exchange has restored the financial buffer to face the next crisis and whether it has improved its underlying security architecture.

Key Conclusion

INTERPRETATION Assessing the soundness of a crypto exchange requires verifying not only its defensive security, which blocks intrusions at the source, but also its practical capacity to cover customer assets quickly and restore normal withdrawal services right after an unexpected major incident. Even in an unprecedented large-scale hack, Binance mobilized its own corporate resources and reserve funds to re-secure the stolen assets quickly and carry out phased withdrawals. For customer payouts to be normalized in the full sense, however, it still has to complete the purchase of the outstanding remaining tokens and prove to the market that it can meet broad withdrawal demand from customers worldwide without bottlenecks.

R REFERENCES

References

#	Title · URL	Publisher	Date
[1]	Binance official security incident and recovery updates Primary 2026-10-30 02:23 UTC · Security Incident Update: initial investigation https://www.binance.com/en/support/announcement/detail/c5a8729a97ac486d963784d96c5642d7 2026-10-30 19:33 UTC · Update #2: company funds allocated https://www.binance.com/en/support/announcement/detail/d3306d9dca5243548c813b605e1d1751 2026-10-31 15:23 UTC (updated) · Update #3: coverage funding and SAFU plan https://www.binance.com/en-AU/support/announcement/detail/1fdf1f61559c401da0435895ffcccb62 2026-11-01 04:08 UTC · Update #4: Phase 1 withdrawals reopen https://www.binance.com/en/support/announcement/detail/73911fb819b240f88b88256bdd318eda 2026-11-02 12:45 UTC · Update #5: proof of reserves https://www.binance.com/en-PH/support/announcement/detail/185bd9a4717f44088b3be70287b8237f 2026-11-03 02:40 UTC · Update #6: Phase 2 withdrawals reopen https://www.binance.com/en/support/announcement/detail/2d83c325ab6e49c6bd6c5de8803b11a6	Binance	2026-10-30~11-03

#	Title · URL	Publisher	Date
[2]	Confirmed transaction history of the SAFU bitcoin address **Primary** https://blockstream.info/address/1BAuq7Vho2CEkVkUxbfU26LhwQjbCmWQkD	Blockstream Explorer	Accessed 2026-11-02/03
[3]	BTC, ETH, XRP/USD OHLC raw data (daily, 15-minute and 1-minute bars) **Primary** BTC/USD daily https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=86400&limit=100&start=1790467200&end=1793577600 BTC/USD 1-minute https://www.bitstamp.net/api/v2/ohlc/btcusd/?step=60&limit=1&start=1793665740&end=1793665799 ETH/USD daily https://www.bitstamp.net/api/v2/ohlc/ethusd/?step=86400&limit=5&start=1793145600&end=1793491200 XRP/USD 1-minute https://www.bitstamp.net/api/v2/ohlc/xrpusd/?step=60&limit=1&start=1793665740&end=1793665740	Bitstamp	Accessed 2026-11-03
[4]	How North Korea is laundering the $6.4 billion stolen from Binance **Primary** https://www.elliptic.co/insights/how-north-korea-is-laundering-the-6-4-billion-stolen-from-binance/	Elliptic	2026-11-02
[5]	Crypto Liquidations Top $628 Million in an Hour as Binance Hack Fears Sink Bitcoin https://beincrypto.com/crypto-liquidations-binance-hack-fears/	BeInCrypto	2026-10-29
[6]	Deposit and withdrawal status by asset and network **Primary** https://www.binance.com/bapi/capital/v1/public/capital/getNetworkCoinAll	Binance	Accessed 2026-11-03 09:32 and 13:43 KST
[7]	North Korea Steals USD 6.36 Billion From Binance in the Largest Hack in History https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history	TRM Labs	2026-10-29 (data as of 10-30 00:30 UTC)
[8]	The $6.4 Billion Binance Hack: Tracing the North Korea Link https://www.chainalysis.com/blog/binance-exploit-latest-findings-and-response/	Chainalysis	2026-10-30
[9]	North Korea Responsible for $6 Billion+ Binance Attack **Primary** https://www.fbi.gov/investigate/cyber/alerts/2026/north-korea-responsible-for-6-billion-binance-attack	FBI	2026-10-31
[10]	N. Korean leader's sister blasts FBI's crypto theft probe as 'political provocation' https://en.yna.co.kr/view/AEN20261103000600315	Yonhap News Agency	2026-11-03
[11]	Binance Hack: Exchange Pledges to Cover All Losses https://financefeeds.com/binance-will-cover-all-losses-hack/	FinanceFeeds	2026-10-30

#	Title · URL	Publisher	Date
[12]	Binance official notices on frozen amounts and withdrawal status **Primary** 2026-10-30 00:52 UTC · Frozen amount updated https://x.com/binance/status/2115970069696217576 2026-11-01 16:12 UTC · Withdrawal and reserve status https://x.com/binance/status/2116926305254133892 2026-11-02 · Withdrawals reopen for 5 fiat currencies https://x.com/binance/status/2117164969582330063	Binance	2026-10-30~11-02
[13]	Binance $6.3B Hack: Using Advanced AI Models, Blockaid Detects the Biggest Theft in Crypto History https://blockaid.io/blog/binance-55b-hack-using-advanced-ai-models-blockaid-detects-the-biggest-theft-in-crypto-history	Blockaid	2026-10-29
[14]	EIP-7702: Set Code for EOAs **Primary** https://eips.ethereum.org/EIPS/eip-7702	Ethereum Improvement Proposals	2024-05
[15]	Binance Hot Wallet Exploit: Aave's Response https://governance.aave.com/t/binance-hot-wallet-exploit-aaves-response/25954	LlamaRisk, Aave Governance	2026-10-30
[16]	Tether Freezes Over $1.5 Billion From Binance Hack, Keeping Funds Out of North Korea's Reach **Primary** https://tether.io/news/tether-freezes-over-1-5-billion-from-binance-hack-keeping-funds-out-of-north-koreas-reach/	Tether	2026-11-02
[17]	Binance clients pull $4.7 billion after hack as crypto world studies fallout https://live.euronext.com/en/financial-news/binance-clients-pull-47-billion-after-hack-crypto-world-studies-fallout	Reuters (via Euronext)	2026-11-02
[18]	Binance sees $3.64 billion in net outflows after reopening withdrawals following record hack https://www.theblock.co/news/business/2026-11-01-binance-sees-3-64-billion-in-net-outflows-after-reopening-withdrawals-following-record-hack-432259	The Block	2026-11-01
[19]	Binance finalizes $1 billion SAFU reserve conversion into bitcoin https://www.theblock.co/post/389567/binance-finalizes-1-billion-safu-reserve-conversion-into-bitcoin	The Block	2026-02-12
[20]	Potential multi-billion Binance hack hitting crypto markets https://www.coindesk.com/business/2026/10/29/potential-multi-billion-binance-hack-hitting-crypto-markets	CoinDesk	2026-10-29
[21]	What Is Proof of Reserves (PoR)? **Primary** https://www.binance.com/en/academy/articles/what-is-proof-of-reserves-and-how-it-works-on-binance	Binance Academy	Updated 2026-05-14
[22]	Binance USDT reserves drop 7.95% as report narrows to 10 assets https://crypto.news/binance-usdt-holdings-fall-proof-of-reserves-october-2026/	crypto.news	2026-11-02

#	Title · URL	Publisher	Date
[23]	Binance completes latest proof of reserves as it works to restore assets, withdrawals after record hack https://www.theblock.co/news/business/2026-11-02-binance-zero-knowledge-proof-of-reserves-snapshot-hack-recovery-432321	The Block	2026-11-02
[24]	Binance Rewrote Its Hack Statement Twice in 13 Minutes https://financefeeds.com/binance-hack-statement-edited-user-funds-safe/	FinanceFeeds	2026-10-30
[25]	KRW-BTC, ETH, XRP, USDT 1-minute and daily bars **Primary** https://api.upbit.com/v1/candles/minutes/1?market=KRW-BTC&to=2026-11-02T00%3A30%3A00Z&count=2 https://api.upbit.com/v1/candles/minutes/1?market=KRW-USDT&to=2026-11-02T00%3A30%3A00Z&count=2 https://api.upbit.com/v1/candles/minutes/1?market=KRW-BTC&to=2026-11-03T00%3A30%3A00Z&count=2 https://api.upbit.com/v1/candles/minutes/1?market=KRW-USDT&to=2026-11-03T00%3A30%3A00Z&count=2 https://api.upbit.com/v1/candles/days?market=KRW-BTC&to=2026-11-03T00:00:00Z&count=20 https://api.upbit.com/v1/candles/minutes/1?market=KRW-ETH&to=2026-11-03T00%3A30%3A00Z&count=1 https://api.upbit.com/v1/candles/minutes/1?market=KRW-XRP&to=2026-11-03T00%3A30%3A00Z&count=1	Upbit	Accessed 2026-11-02/03
[26]	MtGox notices on its rehabilitation filing and the size of its bitcoin loss **Primary** 2014-02-28 · Rehabilitation filing and initial loss figure announced https://www.mtgox.com/img/pdf/20140228-announcement_eng.pdf 2014-03-20 · 200,000 BTC found in an old-format wallet https://www.mtgox.com/img/pdf/20140320-btc-announce.pdf	MtGox	2014-02-28·03-20
[27]	Mt. Gox pauses all Bitcoin withdrawals due to technical issues https://thenextweb.com/news/mt-gox-pauses-all-bitcoin-withdrawals-due-to-technical-issues	The Next Web	2014-02-07
[28]	FTX Exchange Halts All Crypto Withdrawals https://www.coindesk.com/business/2022/11/08/ftx-exchange-halts-all-crypto-withdrawals	CoinDesk	2022-11-08
[29]	Bitfinex notices on customer account treatment, withdrawal reopening and BFX redemption **Primary** 2016-08-06 · Bitfinex Interim Update: customer account haircut and BFX issuance https://blog.bitfinex.com/announcements/bitfinex-interim-update/ 2016-08-10 · Site Update: withdrawals of major assets reopen https://blog.bitfinex.com/announcements/site-update/ 2017-04-03 · 100% Redemption of Outstanding BFX Tokens https://blog.bitfinex.com/announcements/100-redemption-outstanding-bfx-tokens/	Bitfinex	2016-08~2017-04

#	Title · URL	Publisher	Date
[30]	$477 million in "unauthorized transfers" from FTX https://www.elliptic.co/insights/477-million-in-unauthorized-transfers-from-ftx/	Elliptic	2022-11
[31]	Samuel Bankman-Fried Sentenced to 25 Years in Prison https://www.justice.gov/usao-sdny/pr/samuel-bankman-fried-sentenced-25-years-prison	US Attorney's Office for the Southern District of New York, US Department of Justice	2024-03-28
[32]	Bitcoin drops 20% after $70M worth of bitcoin was stolen from Bitfinex exchange https://techcrunch.com/2016/08/02/bitcoin-drops-20-after-70m-worth-of-bitcoin-was-stolen-from-bitfinex-exchange/	TechCrunch	2016-08-02
[33]	The Coincheck Cryptocurrency Hack: Everything You Need to Know https://fortune.com/2018/01/29/coincheck-japan-nem-hack	Fortune(Reuters)	2018-01-29
[34]	KuCoin notices on withdrawal reopening and loss coverage Primary 2020-10-07 · BTC, ETH and ERC20-USDT withdrawals reopen https://www.kucoin.com/announcement/en-btc-eth-usdt-deposits-and-withdrawals-now-open 2020-11-22 · Reopening of all tokens announced, with limits and exceptions https://www.kucoin.com/announcement/en-deposit-and-withdrawal-services-for-all-tokens-now-resumed-on-kucoin 2021-02-04 · A Letter from KuCoin CEO: results of loss coverage https://www.kucoin.com/announcement/a-letter-from-kucoin-ceo-2020-2021-and-beyond	KuCoin	2020-10~2021-02
[35]	DMM Bitcoin、482億円相当のビットコインが不正流出 https://gamebiz.jp/news/387011	gamebiz	2024-05-31
[36]	North Korea Responsible for $1.5 Billion Bybit Hack (Alert I-022625-PSA) Primary https://www.ic3.gov/PSA/2025/PSA250226	FBI IC3	2025-02-26
[37]	Bitget Hack Explained: Timeline, Impact and Security Response Primary https://www.bitget.com/academy/bitget-security-incident-what-happened-timeline-impact-response	Bitget	2026-09-27, updated 10-20
[38]	Total Bitcoins in Circulation raw data https://api.blockchain.info/charts/total-bitcoins?timespan=all&format=json&sampled=false	Blockchain.com	Accessed 2026-10-30
[39]	Mt Gox starts making repayments in bitcoin and bitcoin cash: trustee https://www.theblock.co/post/303614/mt-gox-starts-making-repayment-in-bitcoin-and-bitcoin-cash-trustee	The Block	2024-07-05

#	Title · URL	Publisher	Date
[40]	FTX begins initial fund distributions to customers as its bankruptcy recovery forges on https://www.theblock.co/news/markets/2025-02-18-ftx-begins-initial-fund-distributions-to-customers-as-its-bankruptcy-recovery-forges-on-341633	The Block	2025-02-18
[41]	Coincheck Resumes Yen Withdrawals, Lawsuit on Its Way https://www.financemagnates.com/cryptocurrency/news/coincheck-resumes-yen-withdrawals-lawsuit-way/	Finance Magnates	2018-02-13
[42]	コインチェックが一部通貨の出金と売却を順次再開 https://coinpost.jp/?p=17594	CoinPost	2018-03-12
[43]	不正に送金された仮想通貨NEMの保有者に対する補償について Primary https://corporate.coincheck.com/press/dG-nDV-c	Coincheck	2018-03-12
[44]	DMM Bitcoin 口座移管に関するFAQ Primary https://www.sbivc.co.jp/faqs/content/v_d3sfi_r https://gamebiz.jp/news/396823	SBI VCトレード	Accessed 2026-11-03
[45]	Bybit Security Incident: Timeline of Events and FAQs Primary https://www.bybit.com/en/learn/this-week-in-bybit/bybit-security-incident-timeline	Bybit	2025-03-03
[46]	Bybit Hack Postmortem (The Week On-chain Week 08) https://research.glassnode.com/the-week-onchain-week-08-2025/	Glassnode	2025-02-26
[47]	Emergency inspection meeting held with domestic virtual asset service providers over the Binance hack (바이낸스 해킹 관련 국내 가상자산사업자 긴급 점검회의 개최) Primary https://www.fsc.go.kr/no010101/88054	Financial Services Commission (금융위원회)	2026-11-02
[48]	Withdrawal caution notice for digital assets sent to the Binance exchange (Binance(바이낸스) 거래소 대상 디지털 자산 출금 주의 안내) Primary https://www.upbit.com/service_center/notice?id=838564319&view=share	Upbit	2026-10-30 07:46:40 KST
[49]	Withdrawal caution notice for the Binance exchange (바이낸스(Binance) 거래소 대상 출금 주의 안내) Primary https://feed.bithumb.com/notice/1655461	Bithumb	2026-10-30 08:00:56 KST
[50]	[Upbit hack] Bithumb, Coinone, Korbit and Gopax suspend withdrawals to Upbit ([업비트 해킹] 빗썸·코인원·코빗·고팍스, 업비트로 출금 중단) https://www.blockmedia.co.kr/archives/1012084	Blockmedia (블록미디어)	2025-11-27
[51]	USD exchange rates https://open.er-api.com/v6/latest/USD	ExchangeRate-API	Updated 2026-11-01/02 00:02:31 UTC
[52]	Some coins rose 126% after the Upbit hack: the paradox of a deposit and withdrawal halt (업비트 해킹 후 126% 뛴 코인도...입출금 중단의 역설) https://www.hankyung.com/article/202511282040i	The Korea Economic Daily (한국경제)	2025-11-28

A APPENDIX

Data limitations, calculation basis and detailed timeline

① Limitations

- The comparison set is 8 past exchange incidents plus the Binance hack. In some cases the compensation policy was decided after the price observation window, and the sample is too small to estimate statistically the effect of the loss-bearing structure from differences in drawdowns.
- Price comparisons start from the withdrawal halt date for Mt. Gox and FTX and from the hack disclosure date for the other exchanges. The 3-day and 7-day windows are based on UTC calendar days, so the first day also includes trading before the incident occurred. Point-in-time returns are based on 15-minute bar closes and do not capture moves within 15 minutes.
- BTC, ETH and XRP dollar prices come from a single exchange, Bitstamp. Domestic prices are Upbit minute bars, and exchange rates are the daily published rates available at each observation time. The KRW premium does not deduct conversion costs or fees and so differs from actual arbitrage returns.
- Withdrawal access is the value obtained by querying Binance's public deposit and withdrawal status data at specific times. The denominator also includes pairs that were blocked for reasons unrelated to the incident, such as "Unsupported Token." Asset-level reserve ratios in the proof of reserves are cited from press tallies.
- Binance's estimate of about $6.3 billion and the estimates of the various analytics firms differ in the chains and assets included and in the valuation time. Frozen and seized amounts are kept separate from returned amounts, and the final net loss has not been calculated.

② Formulas for Our Own Estimates

The formulas, reference times and sources applied to our estimates in the main text are set out below.

Indicator	Formula	Reference date and observation window	Source
Loss as a share of BTC market cap	Loss (USD) ÷ (BTC/USD close on the day before the hack was disclosed × circulating supply at the end of that day). For incidents measured in BTC: BTC lost ÷ circulating supply	Mt. Gox 2014-02-24 (day before the site closed), FTX 2022-11-11, Binance 2026-10-28. Others: day before the hack was disclosed	, sources for each incident's loss[3][38]
3D and 7D maximum decline (close)	min(0, lowest close over D to D+2 or D to D+6 ÷ D−1 close − 1)	UTC daily bars, first day included. Same method for ETH	[3]

Indicator	Formula	Reference date and observation window	Source
3D maximum decline (intraday low)	Same method, using intraday lows instead of closes	3 UTC daily bars, first day included	[3]
Point-in-time returns	Prior 1 hour: P(t) ÷ P(t − 1 hour) − 1. After: P(t + 1 hour or 4 hours) ÷ P(t) − 1. P(t) is the close of the last 15-minute bar completed by t	Reference price at the first outflow (20:05): $80,745.42 (BTC), $2,334.38 (ETH)	[3]
Cumulative decline (first outflow to coverage pledge)	00:15 bar close ÷ 20:00 bar close − 1	BTC 77,744.86 ÷ 80,745.42 − 1 = −3.72%, ETH 2,241.96 ÷ 2,334.38 − 1 = −3.96%	[3]
Pre-incident 7-day and 30-day returns	D−1 close ÷ D−8 or D−31 close − 1	81,250.12 ÷ 84,023.24 − 1 = −3.3%, 81,250.12 ÷ 83,461.65 − 1 = −2.6%	[3]
Binance 3D maximum decline	BTC close 77,187.27 ÷ 81,250.12 − 1 = −5.0%, low 76,172.75 ÷ 81,250.12 − 1 = −6.2%. ETH close −4.9%, low −7.9%	D = 2026-10-29, D−1 = 2026-10-28	[3]
SAFU value relative to the loss	15,000.00147092 BTC just before the hack × $80,320.32 ≈ $1.2048 billion. ÷ $6.3 billion = 19.1%	Close of the 1-minute bar starting 20:04 UTC	[2] [3] [1]
SAFU balance and refill shortfall	7,500.00136678 BTC × $76,925.02 ≈ $576.94 million. $1 billion − $576.94 million ≈ $423.06 million	Balance at 09:31 KST on November 3; close of the 1-minute bar starting 09:29 KST	[2] [3] [1]
Withdrawal access	Number of assets marked withdrawable ÷ number of non-fiat assets listed in the public status data (27 ÷ 908). Pairs: 40 ÷ 1,365. The 10 proof-of-reserves assets: 23 ÷ 72	Public status data at 2026-11-03 04:43 UTC	[6]
Main reasons for withdrawal suspension	Suspended pairs by reason ÷ 1,325 suspended pairs	Wallet Maintenance 505, Low Hot Wallet Balance 389, Unsupported Token 341	[6]

Indicator	Formula	Reference date and observation window	Source
Cumulative net outflow ratio	$4.72 billion ÷ $171 billion = 2.8%	Net outflows from the spokesperson's November 2 statement; platform assets from the company's October 28 disclosure	[17] [12]
Loss relative to public wallet balances	$6.3 billion ÷ $144 billion = 4.4%	Public wallet balances as reported before the incident	[20] [1]
Share of the 3 stablecoins	(USDT 1,875 + 612.7 + USDC 823 + RLUSD 88.5) ÷ 6,360 = 53.4%	Quantities in millions of tokens converted at $1 per token. Denominator is TRM's total at the time of theft	[7]
KRW premium	BTC: 103,703,000 ÷ (76,925.02 × 1,332.76172) − 1 = 1.15%. USDT: 1,346 ÷ 1,332.76172 − 1 = 0.99%	1-minute bar close at 09:29 KST on November 3; exchange rate as updated at 09:02:31 KST on November 2	[25] [3] [51]
Domestic and overseas price gap converted at USDT	Upbit KRW price ÷ (Bitstamp USD price × Upbit USDT KRW price) − 1	The four times in Table 8; 1-minute bar closes for the same minute	[25] [3]
Upbit trading value multiple	Trading value on the relevant UTC daily bar ÷ daily average for October 22–28	BTC KRW 167.97 billion ÷ KRW 67.59 billion = 2.49x, ETH KRW 90.27 billion ÷ KRW 39.03 billion = 2.31x, XRP KRW 158.06 billion ÷ KRW 83.93 billion = 1.88x	[25]
Mt. Gox loss share and multiples	650,000 ÷ 12,441,400 ≈ 5.22%, 850,000 ÷ 12,441,400 ≈ 6.83%. About 13.5x and 17.7x Binance's 0.386%, respectively	Circulating supply at the end of 2014-02-24	[3] [38] [26]
Binance loss share	$6.3 billion ÷ (81,250.12 × 20,105,046.875) = 0.386%	End of 2026-10-28	[3] [38] [1]

③ Methodology

- Source priority: official materials from companies and regulators, then raw data and aggregator databases, then specialist media, then syndicated media, then community sources.

- Source classification: a source is classed as primary only when the original was checked directly. Content conveyed through reporting is attributed to the outlet that reported it.
- Reference and access dates: values fixed at a specific point in time carry their reference date; dashboard figures that change in real time carry their access date.
- Conflicting figures: where different figures are found, both are presented. Where a reference value has to be chosen, disclosure of the calculation scope, clarity of the query time and separability of line items take precedence over the outlet's profile, and the basis for the choice is stated in the main text.
- Our estimates: each of our estimates is presented individually in Appendix ② with its formula, reference date and limitations.
- Legal and regulatory interpretation: regulators' materials are cited only to explain the general classification of structures and their possible application, and are not read as an official classification or approval of any specific product. Descriptions of product structures and regulatory interpretation are kept in separate paragraphs.
- Conflict of interest disclosure: the same disclosure wording appears in a fixed position at the top of every report.

④ Detailed timeline from the first outflow to the Phase 2 withdrawal reopening

Time (UTC)	Time (KST)	Event
October 29 20:05	October 30 05:05	First outflow from a Binance wallet on the XRP Ledger, followed by outflows from Solana and Optimism wallets[7]
20:20	05:20	18,270 BTC moved out of the bitcoin hot wallet[7]
20:20:59	05:20:59	Malicious EIP-7702 delegation registered on Ethereum hot wallet "Binance 14"[13]
20:24:23	05:24:23	167,464 ETH, USDT and other assets moved out[13]
20:41~23:56	05:41~08:56	USDC outflow from a separate Ethereum smart account. Assets newly arriving in the compromised wallets also drained[13][7]
21:16	06:16	Binance issues first statement, saying it is investigating a security issue[24]
22:15	07:15	Binance suspends withdrawals[11]
23:05	08:05	Second wave of outflows from Avalanche and Polygon wallets[7]
23:22	08:22	Binance announces $2.54 billion frozen[11]

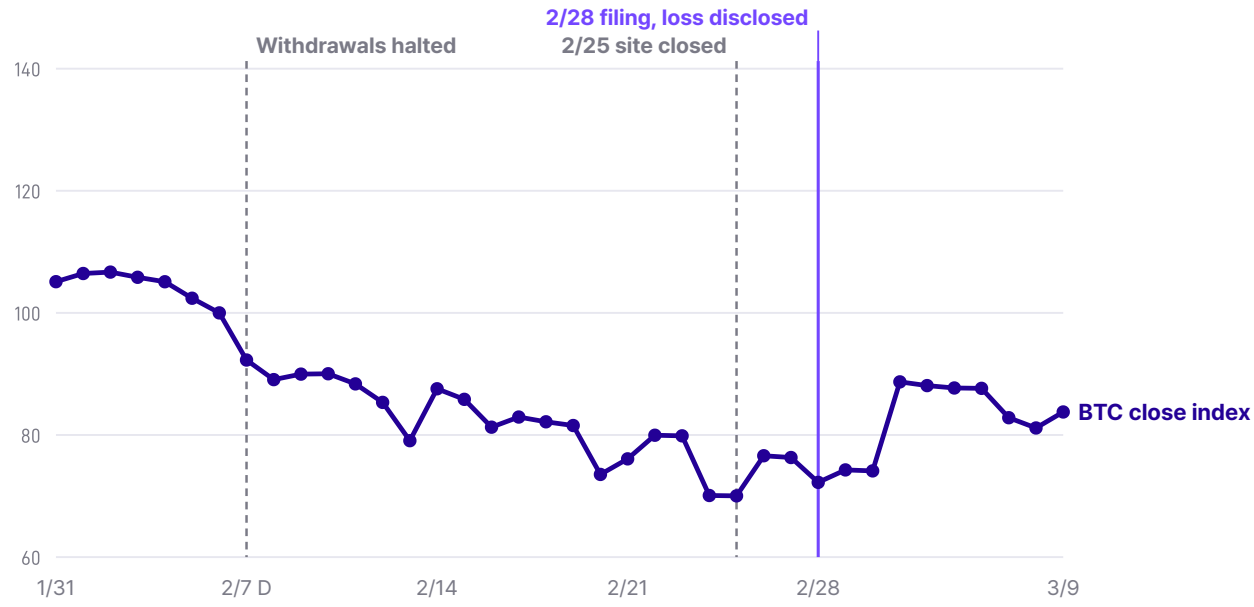
Time (UTC)	Time (KST)	Event
October 30 00:13	09:13	Pledge to cover losses in full; deposit and withdrawal suspension notice[11]
October 30 00:52	October 30 09:52	Binance updates the frozen amount to about $3 billion[12]
October 30 19:33	October 31 04:33	More than $6.34 billion of company funds set aside. About 80% announced as covered in the same types of assets as those stolen[1]
October 31 14:24	October 31 23:24	About 90% announced as covered. Balances as of 00:00 UTC on October 31, used for the proof of reserves, published[1]
October 31 14:51	October 31 23:51	7,499 BTC transferred from SAFU[2]
October 31	October 31	FBI attributes the attack to North Korea's TraderTraitor[9]
November 1 04:08	November 1 13:08	About 95% announced as covered. Binance says customer balances in the 10 major assets, including bitcoin, are fully backed[1]
November 1 06:00–12:36	November 1 15:00–21:36	Withdrawals reopen starting with bitcoin, extending to the eligible assets on the 15 networks designated for Phase 1[1][12]
November 2 08:00	November 2 17:00	Withdrawals of 5 fiat currencies including the US dollar announced as reopened. 28 currencies available for withdrawal[12]
November 2 12:45	November 2 21:45	Proof of reserves published for the 10 major assets as of October 31. Customers can verify their individual balances[1]
November 3 04:00	November 3 13:00	Sequential reopening begins for additional assets on BSC, Ethereum, Solana, XRP, Sui and others, and for some assets on Arbitrum, Optimism, Tron and Base[1]

⑤ Bitcoin price paths by incident

Each chart rebases the bitcoin close on the day before the reference date to 100. Past cases are shown from 7 days before to 30 days after the reference date, and Binance from 7 days before to 4 days after the reference date, November 2. All charts use a vertical axis of 60–140 so that drawdowns can be compared across incidents on the same scale. DMM Bitcoin and Bitget are omitted because their loss shares, about 0.02% each, are the smallest.

Mt. Gox withdrawal halt, max BTC closing drawdown · 3D 10.9%

Reference date (D) 2014-02-07 · prior close=100 · 3D D to D+2

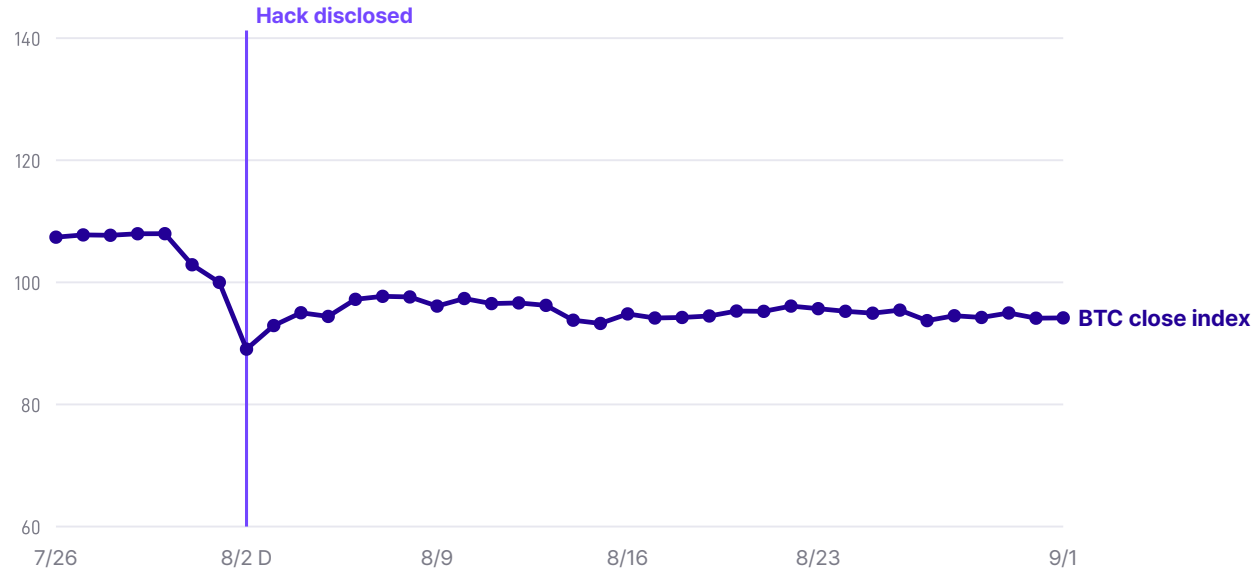


Source: Bitstamp BTC/USD daily[3] · withdrawal halt[27] · site closure, filing, loss disclosure[26] · our estimate

BITPLANET

Bitfinex hack, max BTC closing drawdown · 3D 10.9%

Reference date (D) 2016-08-02 · prior close=100 · 3D D to D+2

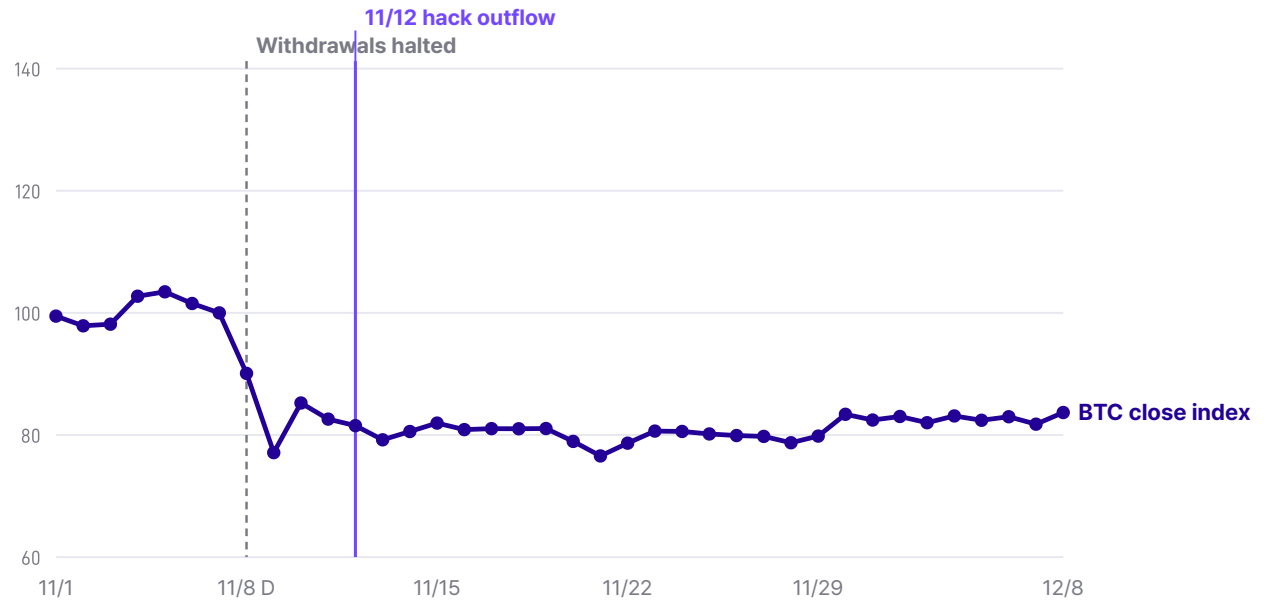


Source: Bitstamp BTC/USD daily[3] · reference date[32] · our estimate

BITPLANET

FTX withdrawal halt, max BTC closing drawdown · 3D 22.9%

Reference date (D) 2022-11-08 · prior close=100 · 3D D to D+2



Source: Bitstamp BTC/USD daily[3] · reference date[28] · hack[30] · our estimate

BITPLANET

Coincheck hack, max BTC closing drawdown · 3D 0.6%, 7D 19.3%

Reference date (D) 2018-01-26 · prior close=100 · 3D D to D+2, 7D D to D+6

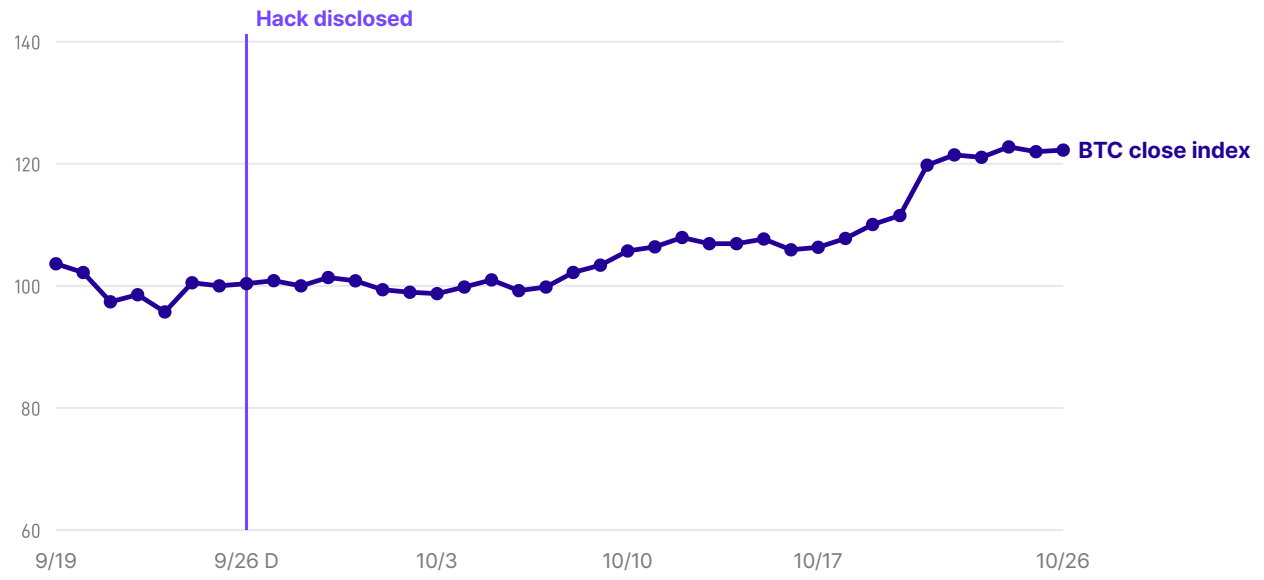


Source: Bitstamp BTC/USD daily[3] · reference date[33] · our estimate

BITPLANET

KuCoin hack, max BTC closing drawdown · 3D 0.0%

Reference date (D) 2020-09-26 · prior close=100 · 3D D to D+2

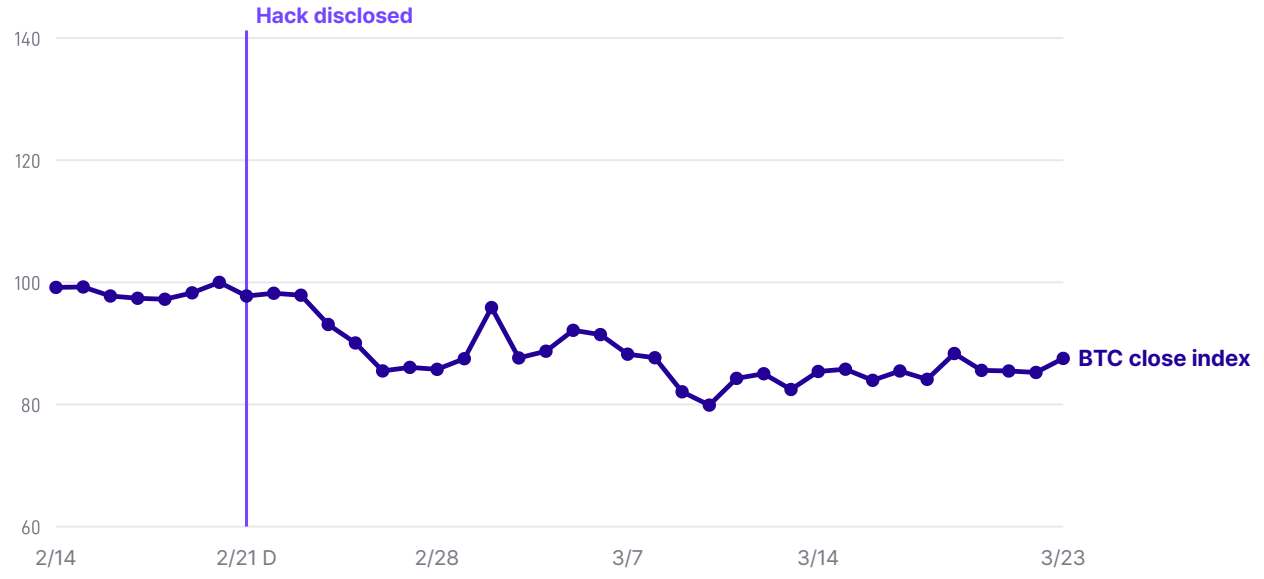


Source: Bitstamp BTC/USD daily[3] · reference date[34] · our estimate

BITPLANET

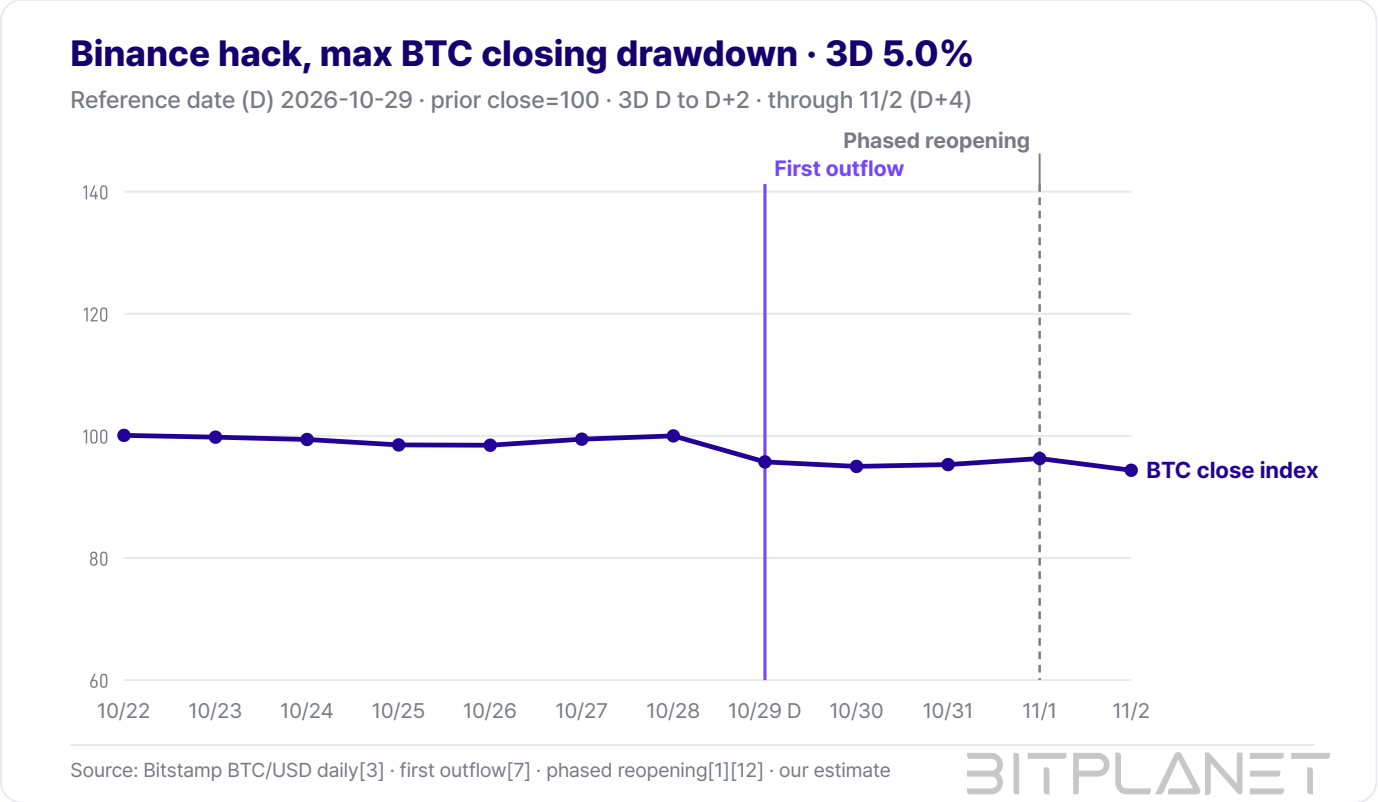
Bybit hack, max BTC closing drawdown · 3D 2.2%, 7D 14.5%

Reference date (D) 2025-02-21 · prior close=100 · 3D D to D+2, 7D D to D+6



Source: Bitstamp BTC/USD daily[3] · reference date[36] · our estimate

BITPLANET



PUBLISHED BY Bitplanet Research Lab WRITTEN BY Taewon Kim REVIEWED BY Sooyoung Kim

Disclaimer This material is an industry analysis provided for information purposes only and is not investment advice. It does not recommend buying or selling any specific security and does not present price forecasts or price targets. The authors are not lawyers or registered investment advisers, and all figures are based on public sources (as of the time of writing and subject to change thereafter).