The Evolution of Crypto Exchange Breaches (2011–2025)

Cryptocurrency exchanges have been prime targets for hackers since the early days of Bitcoin. Over the past decade and a half, the scale and sophistication of attacks have grown dramatically – from small breaches on fledgling platforms to **mega-hacks** orchestrated by state-sponsored groups. In this post, we examine major exchange breaches from 2011 through 2025, analyze the technical causes behind them, and identify recurring failure modes. By understanding how these intrusions occurred, security researchers and exchange operators can derive practical lessons to better secure crypto infrastructure.

Timeline of Major Crypto Exchange Hacks (2011–2025)

Below is a chronological timeline of significant crypto exchange breaches and hacks, including the date, exchange, estimated losses, and a brief description of each incident:

Date	Exchange	Amount Stolen	Description and Outcome (with source)
June 19, 2011	**Mt.Gox**	$8,750,000	A hacker used an auditor's compromised credentials to fraudulently sell large volumes of BTC on Mt.Gox, crashing the price to 1 cent and affecting accounts valued at over $8.7 million.
Oct 5, 2011	**Bitcoin7**	n/a	Bitcoin7 suffered a hacking intrusion that **compromised customer wallets and its user database**, exposing sensitive KYC information (IDs, bank details, etc.). The exchange shut down shortly after.
Mar 2012	**Bitcoinica**	$228,000	In a **cloud server breach**, attackers stole 43,554 BTC from Bitcoinica's unencrypted hot wallet on Linode's servers. This was part of a broader Linode hack affecting multiple Bitcoin services.
May 2012	**Bitcoinica**	$87,000	Just weeks later, Bitcoinica was **hacked again** – this time attackers accessed the exchange's user database and stole 38,000 BTC. (The funds were later reportedly recovered or refunded.)
July 2012	**Bitcoinica**	$300,000	A **third compromise** at Bitcoinica resulted in 40,000 BTC stolen (worth ~$300k at the time), though the coins were being held at Mt.Gox and were eventually refunded. Bitcoinica shut down amid these repeated hacks.

Date	Exchange	Amount Stolen	Description and Outcome (with source)
Sept 3, 2012	**Bitfloor**	$250,000	Bitfloor (a U.S. exchange) was **hacked and lost 24,000 BTC** (roughly $250k). The founder later revealed the breach was enabled by an **unencrypted wallet backup** being stored on the server, which allowed the thief to obtain the hot wallet keys.
May 10, 2013	**Vircurex**	$352,000	Attackers acquired login credentials to Vircurex's VPS hosting account and reset all server passwords, **raiding hot wallets** of ~1,454 BTC, 225k TRC, and 23k LTC (worth ~$352k total).
Oct 23, 2013	**Inputs.io**	$1,200,000	**Two hacks** on Inputs.io (a Bitcoin web wallet service) led to ~4,100 BTC stolen. The attacker compromised the hosting provider via old email accounts and **bypassed 2FA due to a server-side flaw**, ultimately draining about $1.2M. Inputs.io shut down, unable to repay users.
Feb 7, 2014	**Mt.Gox**	$661,348,000	A leaked document revealed that over the course of 2011–2014, **hackers siphoned approximately 744,408 BTC from Mt.Gox's hot wallets** (plus 100k BTC of company funds). The theft (worth $661M at the time) left the exchange insolvent, leading to its collapse and the *largest Bitcoin heist in history*.
Feb 17, 2014	**Picostocks**	$4,434,000	Picostocks exchange announced ~5,896 BTC missing from both its "hot" *and* "cold" wallets. Because offline cold wallets were somehow accessed, the incident was suspected to be an **inside job** (potentially by someone with internal access to cold storage).
Mar 2, 2014	**Flexcoin**	$600,000	Bitcoin storage service Flexcoin was **hacked and robbed of 896 BTC** (~$600k) from its hot wallets. Flexcoin shut down immediately, as it had kept no cold reserve – illustrating the dangers of relying solely on hot storage.
Mar 4, 2014	**Poloniex**	$67,500	A **software bug** in Poloniex's withdrawal code allowed an attacker to withdraw 97 BTC (12.3% of Poloniex's BTC) in an attack. The

Date	Exchange	Amount Stolen	Description and Outcome (with source)
			exchange's owner acknowledged a critical vulnerability and fully reimbursed the ~$67k loss, enabling Poloniex to continue operating.
Mar 11, 2014	**CryptoRush**	$630,000	Small altcoin exchange CryptoRush was hacked, losing ~950 BTC and 2,500 LTC (worth ~$630k). The incident's severity (virtually all user funds lost) forced the exchange to close, amid speculation of possible internal malfeasance.
July 14, 2014	**MintPal**	$1,933,000	MintPal suffered a **hot wallet breach** that stole ~8 million Vericoin (VRC), about 30% of that coin's supply (~$1.9M). MintPal later relaunched, but the hack significantly damaged its reputation.
July 29, 2014	**Cryptsy**	$9,580,000	In a belated revelation, Cryptsy claimed it was hacked in July 2014, losing ~13,000 BTC and 300,000 LTC (~$9.58M). (Years later, many accused Cryptsy's CEO of fabricating the hack to cover an internal fraud, though the true story remains contested.)
Jan 4, 2015	**Bitstamp**	$5,100,000	Bitstamp's hot wallets were **compromised on Jan 4** and 18,866 BTC were stolen (~$5.1M). The breach was later traced to a **spear-phishing attack**: attackers sent malware-laced emails to Bitstamp employees, one of whom unwittingly ran the malware, allowing thieves to obtain the wallet keys. Bitstamp quickly suspended service, then improved security (including multisig for withdrawals) and resumed operations.
Jan 27, 2015	**796.com**	$270,000	Chinese exchange 796 was hacked, losing 1,000 BTC (~$270k). Hackers had compromised parts of the exchange days prior; during recovery, a **mistake in a customer service process** led to the coins being irretrievable. (The incident was attributed to security gaps and operational errors.)
Feb 14, 2015	**BTER**	$1,750,000	BTER announced that **7,170 BTC were stolen from its cold wallet** (≈$1.75M) – an unusual case of a purported *cold storage* hack. The

Date	Exchange	Amount Stolen	Description and Outcome (with source)
			breach raised suspicions of an insider, since properly secured cold wallets are typically inaccessible to remote attackers.
Feb 18, 2015	**KipCoin**	$728,000	KipCoin (China) had its wallet servers hacked on Lunar New Year's Eve; ~3,000 BTC were lost (~$728k). The exchange went offline after announcing the breach, suggesting an inability to cover the losses.
May 22, 2015	**Bitfinex**	$329,000	Bitfinex (Hong Kong) reported that its hot wallets were **compromised** and ~1,460 BTC stolen (~$329k). This small 2015 incident foreshadowed a much larger attack on Bitfinex the next year.
May 9, 2016	**Gatecoin**	$2,140,000	Hong Kong exchange Gatecoin lost ~185,000 ETH and 250 BTC (~$2.14M) in a **hot wallet breach** that began on May 9 and went undetected for three days. The attackers exploited vulnerabilities in Gatecoin's systems to siphon funds; the exchange later reimbursed users partially and improved its security.
June 30, 2016	**ShapeShift**	$200,000	ShapeShift, a crypto swap service, suffered a series of thefts totaling ~$200k. Uniquely, these were **inside jobs** – a disgruntled employee stole keys and emptied multiple hot wallets over two weeks. ShapeShift rebuilt its infrastructure and resumed service, having learned a harsh lesson about insider threats.
Aug 2, 2016	**Bitfinex**	$72,000,000	In one of the biggest Bitcoin exchange hacks at the time, **119,756 BTC (~$72M) were stolen** from Bitfinex's segregated customer wallets. Bitfinex's multi-signature arrangement (with BitGo) was **exploited due to a vulnerability** in the system's design or key management. The exchange spread losses across users and later issued tokens to compensate victims, emphasizing the need for careful multisig implementation.
Oct 13, 2016	**Bitcurex**	$1,500,000	Polish exchange Bitcurex closed after a hack that resulted in ~2,300 BTC missing (≈$1.5M). As one of Europe's oldest Bitcoin exchanges,

Date	Exchange	Amount Stolen	Description and Outcome (with source)
			its abrupt shutdown underscored that even established platforms remained at risk without continual security upgrades.
Apr 26, 2017	**Yapizon**	$4,850,000	South Korean exchange Yapizon (later rebranded to YouBit) lost 3,831 BTC (~$4.85M), roughly **37% of its total assets**, in a hacking incident. The exchange immediately absorbed the losses by haircutting customer balances, and continued operating under the new name "YouBit."
Jun 27, 2017	**Bithumb**	n/a (data breach)	Bithumb (South Korea) announced a **database breach** – personal data of 31,800 customers (3% of users) was stolen. While no direct crypto theft from the exchange's wallets occurred, several users later reported phishing and fraud attempts. Bithumb compensated some users for ensuing losses, and regulators pushed Korean exchanges to tighten data security.
Dec 19, 2017	**YouBit**	n/a (17% of funds)	YouBit (formerly Yapizon) was hacked a second time, losing an estimated **17% of its remaining assets**. The hit was fatal – the small exchange filed for bankruptcy the same day. (South Korean officials later linked the YouBit attacks to North Korean hacking groups, presaging the rise of state-sponsored crypto theft.)
Jan 26, 2018	**Coincheck**	$500,000,000	In one of the largest heists ever, hackers infiltrated Coincheck (Japan) and stole ~523 million NEM (XEM) tokens – worth approximately **$500M**. The coins had been kept in a single-signature *hot wallet*. Coincheck admitted to operational failures (e.g. lack of multisig and keeping too much in hot storage) and later reimbursed users, while regulators penalized and forced improvements.
Feb 8, 2018	**BitGrail**	$170,000,000	Italian exchange BitGrail lost 17 million Nano (XRB) coins (~$170M) in a hack. Controversy surrounds this case: BitGrail's owner claimed the Nano protocol had a flaw, while others

Date	Exchange	Amount Stolen	Description and Outcome (with source)
			blamed BitGrail's own wallet security. The incident (and ensuing legal battles) highlighted the **fragility of small exchanges** handling large crypto values without robust safeguards.
June 10, 2018	**Coinrail**	$40,000,000	Coinrail (South Korea) reported a cyber intrusion in which hackers stole a mix of ERC-20 tokens, initially estimated at **$40M**. The attack on this smaller exchange rattled crypto markets at the time, illustrating that even lesser-known platforms were not off limits.
June 19, 2018	**Bithumb**	$31,000,000	Bithumb was hacked and approximately **35 billion KRW (~$31M) in various cryptocurrencies were stolen**. The breach – Bithumb's second in a year – was reportedly due to an attack on a hot wallet. The exchange froze withdrawals and moved assets to cold storage; fortunately, it had sufficient reserves to cover user losses.
July 9, 2018	**Bancor**	$23,500,000	Bancor, a decentralized exchange service, lost ~$23.5M in user funds when a hacker **compromised a wallet used to upgrade smart contracts**. This incident, though involving a DEX, showed that centrally stored keys (even for contract management) can be a point of failure. Bancor was able to freeze some stolen tokens due to built-in controls, sparking debate about decentralization and security trade-offs.
Sept 14, 2018	**Zaif**	$60,000,000	Japan's Zaif exchange was hacked, with **~6.7 billion JPY (~$60M) in crypto stolen**, including ~6,000 BTC. The attack went undetected for two days. Zaif's parent company ultimately sold a majority stake to cover the losses, a reminder of how a single breach can bankrupt an exchange without sufficient buffers.
Oct 28, 2018	**MapleChange**	$5,000,000	Canadian exchange MapleChange announced that virtually **all its funds (~$5M) were "lost" in a hack**, and that it couldn't refund users. Many in the community

Date	Exchange	Amount Stolen	Description and Outcome (with source)
			suspected an **exit scam or insider theft**, given the sketchy circumstances. Regardless, customers of MapleChange suffered total losses.
Jan 2019	**Cryptopia**	$3,620,000	New Zealand-based Cryptopia was **hacked on January 14, 2019**, leading to "significant losses" of ETH and tokens (~$3.6M). The exchange paused and eventually went into liquidation. (Later, in 2020, a **former Cryptopia employee** pled guilty to stealing another ~$170k in crypto by illicitly copying wallet keys, underscoring internal risks even after a platform's collapse.)
Feb 15, 2019	**Coinmama**	n/a (user data)	Coinmama (a brokerage service) was one of 24 sites hit in a massive data breach. Around **450,000 Coinmama user emails and hashed passwords** were leaked. No crypto was stolen directly from Coinmama, but the incident prompted industry-wide reviews of password security and data storage practices.
Mar 24, 2019	**DragonEx**	n/a	DragonEx (Singapore) disclosed it **suffered a cyberattack** on March 24, with users' and the exchange's crypto funds "transferred and stolen". The total amount was not revealed, but DragonEx immediately took its platform offline. (It later resumed with a restructuring plan; the hack was suspected to originate from malware delivered via a messaging app.)
Mar 25, 2019	**CoinBene**	$100,000,000	CoinBene, once a top-10 exchange by volume, suddenly went into "maintenance" in late March while **over $100M in tokens vanished from its wallets**. The exchange denied being hacked, but blockchain analysis strongly indicated a theft. This evasiveness demonstrated the lack of transparency that still plagues some exchanges during security incidents.
Apr 1, 2019	**Bithumb**	$13,000,000	Bithumb's hot wallets were hacked for **~$13M in EOS tokens** in what the exchange suspected was an **"insider job"**. The breach

Date	Exchange	Amount Stolen	Description and Outcome (with source)
			was detected by abnormal withdrawal alerts. Bithumb immediately froze its system and later managed to recover some stolen EOS.
May 7, 2019	**Binance**	$40,000,000	Binance, the world's largest exchange, **lost 7,000 BTC** (~$40M) from its hot wallet in a "large scale security breach." Hackers obtained a large number of user API keys, SMS 2FA codes, and other credentials, then executed a coordinated withdrawal via Binance's API. Binance halted withdrawals and covered all losses via its SAFU insurance fund. The attack highlighted **phishing and malware** as effective tools even against top-tier exchanges.
June 27, 2019	**Bitrue**	$4,200,000	Bitrue (Singapore) was hacked and **~$4.2M in XRP and ADA coins stolen** from users' accounts. The attacker exploited a vulnerability in Bitrue's internal process (related to access control for a privileged account). Bitrue reimbursed affected users and improved its access control policies.
July 12, 2019	**BITPoint**	$32,000,000	Japan's BITPoint exchange had **3.5 billion JPY (~$32M) stolen from its hot wallets** (including Bitcoin, Ethereum, XRP, etc.). Notably, ~$23M of the losses were client assets. BITPoint's parent firm offered to compensate customers, and investigators later tracked much of the stolen funds to exchanges overseas.
Nov 27, 2019	**Upbit**	$49,000,000	Upbit (South Korea) saw a sudden transfer of **342,000 ETH (~$49M) from its Ethereum hot wallet to an unknown address**. The exchange acknowledged a hack and froze all wallets. Given similarities to other attacks, intelligence sources attributed this to North Korea's Lazarus Group (though not officially confirmed). Upbit covered the loss from corporate funds and enhanced its wallet security, including adding multi-sig.

Date	Exchange	Amount Stolen	Description and Outcome (with source)
Feb 6, 2020	**Altsbit**	$73,000	A small Italian exchange, Altsbit, was **hacked overnight**, losing most of its crypto holdings (~$73k worth of BTC, ETH, and tokens). The incident wiped out Altsbit's reserves – a stark reminder that minor exchanges are often under-protected and may not survive a security failure. (Altsbit announced it would shut down after partially refunding users.)
May 14, 2020	**BlockFi**	n/a (data breach)	BlockFi, a crypto lending platform, **suffered a data breach** – an attacker compromised an employee's phone via SIM swap and gained access to internal systems, exposing some client data. No funds were stolen, but customer info (like names, emails) was leaked. The breach led BlockFi to harden its account access controls (e.g. requiring hardware 2FA for employees).
Mid 2020	**BuyUcoin**	n/a (data breach)	BuyUcoin (India) reportedly **had data for ~325,000 users leaked** on the dark web. The dumped information included names, email addresses, hashed passwords, and wallet activity. While no direct theft occurred on the platform, the leaked data could enable **targeted phishing** against users – a persistent indirect risk from exchange breaches.
Sep 8, 2020	**Eterbase**	$5,400,000	Slovakian exchange Eterbase was **hacked on Sept 8, 2020**, with roughly **$5.4M in cryptocurrencies stolen**. The thieves infiltrated Eterbase's hot wallets and then laundered the funds through decentralized exchanges. Eterbase cooperated with law enforcement and eventually shuttered its exchange business, pivoting to become a crypto payment platform.
Sep 26, 2020	**KuCoin**	$280,000,000	In a major 2020 incident, **KuCoin's hot wallet private keys were stolen**, and the attackers drained about $280M in Bitcoin, ETH, and tokens. KuCoin reacted swiftly: it froze its platform, re-issued wallets, and worked with other projects to freeze or recover many

Date	Exchange	Amount Stolen	Description and Outcome (with source)
			stolen tokens. About 84% of the funds were eventually recovered, illustrating an industry-wide effort to mitigate damage.
Dec 23, 2020	**Livecoin**	n/a	Livecoin (Russia) abruptly announced it was **"hacked" and lost control of its servers**. Hackers apparently manipulated Livecoin's exchange rates to drastically inflate prices and then stole funds amid the chaos. Livecoin urged users to stop using its site and later shut down, leaving many questions about the true nature of the incident.
Feb 1, 2021	**Cryptopia**	$45,000	More than a year after Cryptopia's liquidation, the **defunct exchange was hacked again**. Around $45k in dormant Bitcoin were taken from wallets in February 2021. This was eventually revealed to be an **insider theft** – a former Cryptopia employee had illicitly copied wallet keys and later used them to steal leftover funds. The employee was caught and pleaded guilty, highlighting the need to secure old keys even after an exchange closes.
Apr 29, 2021	**Hotbit**	n/a (attempted)	Hotbit (a global exchange) **suffered a serious cyber attack** that crippled services and forced it offline for days. The attackers tried to access Hotbit's wallets but were reportedly thwarted by risk controls. Although no funds were stolen, Hotbit had to rebuild servers—demonstrating how even unsuccessful hacks can cause extended downtime for recovery.
Aug 19, 2021	**Liquid**	$80,000,000	Liquid (Japan) was **hacked via its warm wallets**, with about $80M in cryptocurrencies moved out. The attacker gained control of Liquid's DNS records (through social engineering a domain registrar), then obtained access to hot wallets. Liquid announced that only its warm (hot) wallets were affected and immediately transferred all other assets to cold storage. The hack was later linked to North Korean actors. Liquid secured new investment to cover user losses.

Date	Exchange	Amount Stolen	Description and Outcome (with source)
Dec 5, 2021	**BitMart**	$150,000,000	BitMart (Cayman Islands) was **hacked** and approximately **$150M in various tokens were stolen** from two of its hot wallets. The root cause was *the theft of BitMart's private keys* for those wallets (possibly through a compromised AWS server). BitMart suspended withdrawals and used its own funds to reimburse affected users, while tracing efforts indicated the attackers used decentralized exchanges to swap and obfuscate the loot.
Dec 11, 2021	**AscendEX**	$78,000,000	AscendEX (formerly BitMax) reported an unauthorized transfer of assets from one of its hot wallets, resulting in a **$77.7M loss** across Ethereum, BSC, and Polygon tokens. The **hot wallet was breached** by exploiting a vulnerability in the exchange's infrastructure. AscendEX reimbursed all affected users and published a post-mortem promising to strengthen wallet security (including more robust multi-signature procedures).
Jan 9, 2022	**LCX**	$6,800,000	Liechtenstein-based LCX confirmed one of its hot wallets was **compromised**, with ~$6.8M in ETH and tokens stolen. Blockchain investigators (PeckShield) flagged the hacker's address quickly. LCX paused deposits/withdrawals and worked with law enforcement; by April 2022, they recovered a portion of the funds. (The stolen tokens were largely illiquid, which limited the hacker's ability to cash out.)
Jan 17, 2022	**Crypto.com**	$34,000,000	Crypto.com disclosed that **483 user accounts were drained** of a total of $34M in crypto after attackers **bypassed its 2FA system**. A flaw allowed malicious withdrawals without requiring the users' 2FA approval. The exchange revoked all customer 2FA tokens platform-wide, added additional safeguards, and later moved to a completely new multi-factor auth architecture. All affected customers were fully reimbursed.

Date	Exchange	Amount Stolen	Description and Outcome (with source)
Nov 1, 2022	**Deribit**	$28,000,000	Leading crypto derivatives exchange Deribit **suffered a hot wallet hack** around Nov 1, losing $28M in customer assets. Deribit immediately halted withdrawals and used reserve funds to cover losses, stating that its cold storage remained secure. (The breach was later attributed to a compromised server API key). Normal operations resumed after a few days once Deribit rotated wallet addresses and enhanced its security around key management.
Nov 11, 2022	**FTX**	$477,000,000	Mere hours after FTX filed for bankruptcy on Nov 11, an **unknown actor accessed FTX's wallets and stole roughly $477M** in crypto. The thief (possibly an insider or hacker who had maintained backdoor access) siphoned assets from FTX and FTX US wallets amid the chaos. This *post-collapse heist* further complicated the FTX case – the stolen funds began moving through mixers and bridges. The FTX estate and law enforcement continue to investigate the incident, but the attacker remains unidentified.
Apr 10, 2023	**GDAC**	$13,000,000	South Korean exchange GDAC was hacked on April 9, with **$13M (23% of its custodial assets) drained from its hot wallet**. GDAC promptly announced the hack, froze its platform, and notified law enforcement. The stolen coins (mostly major tokens) were tracked to an unknown wallet. The incident underscored that even medium-sized exchanges must continually guard their online wallets.
Sept 12, 2023	**CoinEx**	$54,000,000	CoinEx (Hong Kong) experienced a **breach of multiple hot wallets** on Sept 12, resulting in ~$54M in crypto being siphoned out. Security analysts tied the hack to the **North Korea–linked Lazarus Group**, noting overlaps with addresses used in other attacks. CoinEx admitted "lax security" for its hot wallets facilitated the attack. The exchange froze withdrawals, promised to fully compensate

Date	Exchange	Amount Stolen	Description and Outcome (with source)
			users, and began migrating to a new wallet architecture with enhanced security (including multisig).
Feb 21, 2025	**Bybit**	$1,500,000,000	**Bybit suffered the largest crypto exchange hack in history**, losing nearly 401,000 ETH (≈$1.5 **billion**) from what was supposed to be a secure cold wallet. In this sophisticated attack, hackers *infiltrated Bybit's deployment process*: they compromised a developer's machine and injected malicious code into Bybit's transaction signing system, tricking the exchange into authorizing the huge transfer out of cold storage (via a complicated phishing attack). Bybit immediately formed an alliance with blockchain analysis firms and law enforcement to track the funds and offered a 10% bounty for recovery. The breach, attributed to the Lazarus Group, revealed new vulnerabilities in multisig wallet workflows and has sent shockwaves through the industry.

Technical Analysis: How and Why These Hacks Happened

While the above timeline spans a wide range of exchanges and circumstances, most of these breaches fall into a few **thematic categories of attack vectors**. Here, we break down the hacks by their root causes and examine the common security failures that enabled them:

1. Hot Wallet Compromises – Stolen Private Keys in Online Wallets

The **most frequent pattern** among exchange hacks is the compromise of hot wallets – the online wallets that exchanges use for day-to-day liquidity. In a hot wallet attack, the adversary is able to *obtain the private keys* controlling the exchange's crypto funds, and thus freely transfer out the assets. The initial entry vector varies (it could be malware on an employee PC, an exposed server API, stolen credentials, etc.), but ultimately the attacker gains access to what is effectively the **keys to the kingdom**.

Once an attacker steals an exchange's hot wallet keys, they can swiftly withdraw large sums before being noticed. Examples abound: in **2019, Binance's hackers obtained a cache of API keys and 2FA codes**, which allowed them to access accounts and trigger a withdrawal of 7,000 BTC from a hot wallet. In **2020, KuCoin's intruders directly stole the private keys to the exchange's hot wallets** (for multiple tokens), facilitating a $280M heist. Just recently in **2023, the CoinEx hack was enabled by lax security on hot wallets**

– attackers accessed several hot wallet keys and drained ~$54M before the breach was detected.

Hot wallet thefts typically exploit one or more security lapses such as:

- **Social engineering or malware** to penetrate the exchange's network: For instance, the Bitstamp 2015 breach was caused by employees falling for phishing emails that delivered malware, ultimately exposing the wallet server's keys. Similarly, **Liquid 2021's $80M hack was traced to a targeted social engineering attack** on domain registrar and hosting accounts, allowing hackers to **take control of Liquid's warm wallet infrastructure**. Once inside the network, attackers scour for private key files, unlocked key management systems, or sensitive credentials.

- **Vulnerabilities in servers or devops pipelines**: Several incidents occurred because underlying systems were not adequately secured. The **2016 Bitfinex hack** (119k BTC) is believed to have stemmed from a flaw in Bitfinex's multisig setup with BitGo – the attackers found a way to initiate withdrawals from Bitfinex wallets despite the 2-of-3 multisig, possibly by compromising the API or key usage policies. In the **2025 Bybit hack**, attackers went a step further by infiltrating Bybit's software supply chain: they hacked a developer's environment and inserted malicious code into Bybit's signing process, tricking the system into signing a massive fraudulent withdrawal from cold storage. This sophisticated **supply-chain attack** exploited trust in the deployment process rather than a direct server vulnerability, but the end result was the same – unauthorized control of keys.

- **Third-party platform breaches**: Exchanges that rely on cloud providers, DNS registrars, or wallet management services can be compromised through those dependencies. The **2012 Bitcoinica Linode hack** and **2013 Vircurex VPS hack** are early examples where attackers didn't attack the exchange app itself but the hosting provider, then pivoted to wallet theft. In 2020, hackers changed DNS settings for **KuCoin's web domain** (via registrar compromise) – while that attempt aimed to phish users, it shows another path to internal network access. More recently, **Liquid's 2020 and 2021 incidents** involved both DNS and cloud storage breaches. Any weakness in the extended tech stack (IT infrastructure, CI/CD pipeline, etc.) can ultimately lead to the hot wallets if not isolated properly.

Once thieves control a hot wallet key, **time-to-exfiltration is often just minutes**. Because of this, many exchanges now limit the amount kept in hot wallets (e.g. only enough for 1–2 days of withdrawals) and use *multisignature* or *multi-party computation (MPC)* to require multiple approvals for large transfers. However, as seen in the Bitfinex case, multisig itself must be implemented correctly – a poorly designed multisig can be as vulnerable as a single-sig wallet if one signer's system is compromised. According to blockchain analytics, a significant portion of exchange hacks over the years have been hot wallet exploits, which is why **cold storage** is universally recommended for the bulk of funds.

Even in 2022–2023, we saw that hot wallet attacks remain prevalent. The **Deribit hack (Nov 2022)** was a straightforward hot wallet compromise of $28M. The **GDAC hack (Apr 2023)** saw 23% of the exchange's assets drained from a hot wallet. These underscore that **hot wallets are inherently high-risk**. Exchanges must minimize the amount in hot wallets, secure the machines running wallet processes, enforce strict network segmentation, and use hardware security modules or multisig to make key theft harder. As one security analysis noted, a single private-key hot wallet is "more vulnerable to phishing attacks" and malware, whereas multisig or sharded-key setups can provide resilience. In short: **the fewer assets exposed to the internet, the better**.

2. Software Bugs and Logic Flaws – Exploiting the Exchange Code

Not all attacks require stealing keys or credentials; some hackers have directly exploited weaknesses in the exchange software itself. Logic errors, coding mistakes, or improper validation in the platforms' trading or withdrawal systems have led to major breaches:

- **Withdrawal algorithm flaws:** The classic example is **Poloniex in 2014**, where the exchange's code failed to correctly handle concurrent withdrawals. The attacker discovered they could rapidly submit multiple withdrawal requests and trick the system into debiting the same funds multiple times, pulling out **97 BTC (12% of Poloniex's BTC) without having that balance**, in essence a race-condition bug – a concurrency issue in Poloniex's software that a savvy hacker identified. Poloniex immediately patched the bug and covered the 97 BTC shortfall from its own pocket, but the incident proved that a *single coding error can cost an exchange its solvency*. Similarly, in early 2021, an attacker exploited a bug in **Roll (a crypto social token platform)** to mint and sell tokens, though not an exchange, it exemplifies software logic issues.

- **Improper authentication/authorization checks:** In some cases, exchanges had endpoints that didn't enforce the proper security checks. A vulnerability might allow an API call to withdraw funds without verifying ownership or 2FA, etc. The **Crypto.com 2FA bypass in Jan 2022** is one instance – a flaw in the 2FA system logic allowed attackers to confirm withdrawals **without the second factor**, so long as they had the username/password. This bug cost $34M before detection. Another example was **Coinbase's 2021 SMS 2FA flaw**: a bug in the SMS account recovery flow allowed attackers who knew a user's password to **reset 2FA and access accounts**. More than 6,000 Coinbase users had funds drained as a result. These incidents show that not only user-facing code but also authentication flows must be airtight.

- **Blockchain protocol quirks:** Occasionally, the issue lies in how an exchange integrates a cryptocurrency. For instance, the **BitGrail 2018 hack** was theorized to stem from BitGrail's **inadequate handling of Nano transactions**, potentially allowing double-spends or replaying of withdrawal requests due to a protocol integration bug. While not definitively proven, it highlighted the danger of rolling out

support for new assets without rigorous testing. Another case is **Coincheck's NEM wallet** – it wasn't a software bug per se, but the decision to use a simple single-signature hot wallet (due to lack of library support for multisig at the time) was a *design weakness* that hackers exploited by simply attacking that one point of failure.

- **Smart contract and DeFi-related exploits:** As exchanges expanded services (staking, decentralized exchange integration, etc.), new attack surfaces emerged. Bancor's 2018 hack showed that even a "decentralized" exchange with a smart contract can be hacked if an admin key or update mechanism is compromised. In recent years, some centralized exchanges also suffered from vulnerabilities in cross-chain bridge smart contracts (e.g., if an exchange runs a bridge for its own token). While our list largely excludes pure DeFi exploits, it's worth noting the **KuCoin 2020 hack's aftermath**: much of the stolen ERC-20 tokens were frozen because projects like Tether and others could **pause or reissue tokens**, which is a double-edged sword from a decentralization standpoint but helped limit damage. This interplay between CEX security and smart contract security is increasingly important.

The key lesson with software vulnerabilities is that exchanges must adhere to **secure development practices**. Code should be audited (internally and by third parties), especially critical wallet handling logic. Unit and integration tests should cover edge cases for trading and withdrawal (e.g., ensure no negative balances, no double-withdrawal possible, all authentication steps enforced). **Bug bounty programs** can incentivize white-hat hackers to report flaws responsibly. Many exchanges, after suffering a bug-induced hack, dramatically increased their code review and testing standards – for example, Poloniex's quick recovery was credited to the owner's transparent handling and immediate fix, and Crypto.com's overhaul of its 2FA system was aimed at preventing such an exploit from recurring.

Despite best efforts, logic bugs can still slip through, so **defense in depth** helps: limits on withdrawal rates, anomaly detection (e.g., Poloniex noticed funds mismatch thanks to user reports), and manual review for suspicious large transactions can act as circuit-breakers. In summary, robust software engineering and proactive security testing are as vital as guarding against external hackers.

3. Insider Attacks and Insider-Facilitated Theft

Some of the most damaging "hacks" weren't purely external – they involved insiders abusing their access or colluding with attackers. Exchanges aggregate enormous wealth, and unfortunately, employees or founders with ill intent (or those coerced by criminals) can turn into the ultimate vulnerability.

Confirmed cases of insider attacks include **ShapeShift 2016**, where a staff member stole keys and emptied hot wallets multiple times. The insider knew ShapeShift's security structure intimately, allowing them to strike repeatedly until caught. Similarly, an

unnamed Cryptopia developer in 2019 had secretly kept private keys when the exchange shut down, and later he embezzled funds from the leftover wallets (until an audit traced the theft). These examples show an insider can sometimes do what external hackers struggle with – directly access critical systems or keys – unless strong internal controls are in place.

Other incidents are *suspected* to be insider jobs or inside-assisted:

- **Suspicious exits:** When an exchange claims a hack and disappears, insiders are often suspected. The MapleChange hack of 2018 ($5M) immediately drew suspicions of an exit scam because the exchange operators went silent and no technical details were provided. While not proven, the lack of transparency suggested that the "hack" might have been an inside theft or even a fabricated cover story. Similarly, **Cryptsy's 2014 hack** (revealed in 2016) was accused of being an inside job by its CEO by many users, though a class-action lawsuit later aimed to recover missing funds regardless of cause.

- **Collusion with external hackers:** In some large hacks, there's speculation that an employee might have helped the attackers by providing information or unwittingly opening a backdoor. The **2016 Bitfinex hack** raised questions since it required navigating Bitfinex's multisig scheme – possibly with knowledge of its inner workings. More concretely, **in 2020 an employee of BlockFi was bribed by criminals** (through LinkedIn recruiting ruses) to obtain user data, and **an attempted insider plot at Kraken in 2019** was foiled when an employee reported the bribe offer. These cases, while not leading to major hacks, highlight that well-funded hackers do try to recruit exchange insiders.

- **Negligence or misconduct by founders:** Apart from outright malicious intent, some breaches result from **founders' poor operational practices**, which blur into the insider realm. Mt.Gox's long-term theft (2011–2014) might not have been an inside job in the sense of a single rogue actor – but the fact that *hundreds of thousands of BTC were stolen over years* suggests **internal negligence** at best, or possible complicit activity at worst. Similarly, the collapse of QuadrigaCX in 2019 (while not a hack) involved the founder mismanaging and possibly stealing crypto – a stark reminder that trusted insiders can undermine security without any "hack" at all.

Preventing insider attacks requires a different approach than external hacking defense. Exchanges need **strict internal controls and oversight**: for example, no single individual should ever be able to unilaterally move large sums from cold storage. Multi-signature schemes should involve multiple employees (and ideally automated co-signers with policies) so that one rogue actor can't execute a transfer alone. Background checks and monitoring of staff with access to sensitive systems are important. Many exchanges now employ **separation of duties** – e.g., engineers may deploy code but not have key access,

finance personnel can initiate withdrawals but need tech admins to approve, etc., so that collusion would be required to bypass all controls.

Another mitigation is *transparency*: If an exchange is open about security processes, it's harder for an insider to act without raising alarms. ShapeShift, after its insider incident, famously eliminated custodial hot wallets for a time (switching to a purely non-custodial model) specifically to remove the risk of insider theft of customer funds. While not all can follow that model, it underscores how seriously they took the threat.

In essence, exchanges must remember that **human trust is a security vulnerability**. The threat can come from within, so checks and balances are needed – much like in traditional finance where no single trader or treasurer can move millions without sign-off. Crypto exchanges are implementing similar controls as they mature.

4. Account Takeovers and 2FA Bypasses – Targeting Users to Get to Exchanges

Not all crypto exchange breaches involve attacking the exchange's infrastructure directly. Often, attackers go after the *users' accounts* on the exchange by stealing login credentials and bypassing account security measures. While these account takeover incidents might not always make headlines as "exchange hacks," they can lead to substantial losses for customers and thus are a crucial part of the security landscape.

SIM swapping and phishing are the primary tools in these attacks. Crypto exchange users have been repeatedly victimized by SIM swap gangs that hijack a victim's mobile number to intercept SMS 2FA codes, then drain the victim's exchange account. For example, in 2019–2020 a group dubbed "The Community" **stole millions in crypto via SIM swaps**, targeting high-net-worth exchange users. In one case, a SIM swapper stole $24 million worth of cryptocurrency from a single individual by rerouting the SMS codes needed to log in to their exchange accounts. Mobile carriers have been notoriously vulnerable to social engineering, making SMS-based 2FA a weak link for exchange accounts.

Exchanges themselves have started acknowledging this threat. In late 2021, **Coinbase disclosed that at least 6,000 users had funds stolen from their Coinbase accounts via an SMS 2FA exploit** – the attackers phished users' logins *and* leveraged a flaw in Coinbase's SMS authentication flow to take over accounts. Coinbase quickly fixed the vulnerability and reimbursed users, but notably **95% of Coinbase users were (at the time) using SMS 2FA**, which made this attack very effective. This led Coinbase and other exchanges to heavily promote stronger 2FA methods (like authenticator apps or hardware keys) for users. Similarly, **Crypto.com's 2FA bypass hack** can be seen as an account takeover en masse – the attacker found a general weakness in how 2FA was implemented and exploited it to approve withdrawals from hundreds of user accounts without their consent.

Beyond 2FA, **credential stuffing and database leaks** also facilitate account takeovers. If users reuse passwords across sites, a breach of another service (like the Coinmama

password leak in 2019) can lead to attackers trying those credentials on exchange logins. Several exchanges have reported waves of attempted logins using credentials from unrelated breaches. This is why most exchanges now have anti-stuffing measures like rate-limiting and anomaly detection for login attempts, as well as mandatory 2FA on sensitive actions.

From the exchange's perspective, user account takeovers are tricky – they could happen due to user mistakes (falling for phishing, using weak passwords) which are outside the exchange's direct control. However, exchanges are expected to **provide robust account security features by default** to mitigate these risks:

- **Strong multi-factor authentication:** Encourage or require the use of TOTP apps or hardware security keys (U2F/WebAuthn) instead of SMS. Hardware keys, in particular, are immune to phishing and SIM swaps. Some exchanges (like Binance and Coinbase) now support and recommend security keys for logins and withdrawals.

- **Withdrawal whitelisting and delays:** Features like address whitelists (where a new withdrawal address cannot be used until a waiting period passes) can prevent immediate large withdrawals to an attacker's address, giving time to react. Crypto.com introduced a 24-hour withdrawal address delay after their hack, so that even if an account is taken over, the user might get notified and lock their account before funds actually leave.

- **Behavioral analytics:** Exchanges employ risk engines that flag unusual account activity – e.g., if a login occurs from a new location and then attempts a large withdrawal, it may be held for manual review. These systems helped in some cases (for instance, Coinbase noted they have systems to detect anomalous behavior, which were upgraded post-2021 incident).

- **Insurance or compensation funds:** Though not a prevention, many top exchanges have set aside insurance funds (like Binance's SAFU) so that if user accounts are compromised on a large scale, the exchange can make customers whole. This creates a financial incentive for the exchange to *proactively harden account security*, since they bear the loss if many accounts get hacked due to a systemic issue.

Even as exchanges fortify their own walls, attackers will undoubtedly continue targeting the human element – whether it's the exchange staff (insiders) or its customers (phishing targets). Security is only as strong as the weakest link, and often that weakest link is a person tricked into revealing a password or 2FA code. Therefore, ongoing user education is also key: exchanges regularly send warnings about **common scams, phishing emails, and the dangers of SIM swapping**. In the long run, wider adoption of phishing-resistant authentication (e.g. physical keys) and perhaps passwordless login tech could greatly reduce account takeovers.

5. Other Notable Failure Modes

While the four categories above cover the vast majority of cases, a few additional points are worth noting:

- **Cold Storage Mismanagement:** It's exceedingly rare for true cold (air-gapped) storage to be hacked by external parties, but a couple of incidents (BTER 2015's cold wallet hack, Picostocks 2014's cold+hot theft) suggest either insiders or that those "cold" wallets weren't as cold as claimed. Exchanges must ensure cold keys are generated and stored entirely offline, and consider **multi-person controls** (e.g., requiring multiple people to access a safe or hardware module) to use them. The Bybit 2025 case demonstrates that even "cold" wallets can be compromised if the process to use them is subverted. Bybit believed its huge Ether treasury was secure in cold multisig, yet attackers **tricked the signing process during what appeared to be a routine transfer**, effectively turning the cold wallet hot for one fatal moment. This emphasizes that cold storage procedures need as much scrutiny as online systems – including secure, out-of-band verification for large transfers.

- **Partial Audits and Ghost Funds:** Some exchanges have discovered hacks only after the fact when trying to reconcile accounts. For example, Mt.Gox famously didn't realize the extent of its losses until it was too late, partly due to poor accounting. Regular internal audits and real-time monitoring of wallet balances vs. user balances are crucial to catch suspicious discrepancies early (as Poloniex did in 2014 thanks to user reports, and as Yapizon/Youbit did in seeing 17% funds missing). **Proof-of-reserves** mechanisms that are now emerging industry-wide may also help users detect if an exchange's crypto holdings are inexplicably low.

- **DDoS as diversion:** A common tactic (especially in earlier years) was to flood an exchange with a denial-of-service attack to distract the ops team while attempting a hack or exploiting chaos in the markets. Mt.Gox in 2013 experienced simultaneous DDoS attacks during high volatility, and some minor exchanges reported DDoS attacks coinciding with attempted breaches. While DDoS itself doesn't steal funds, exchanges need DDoS protection so that monitoring and security processes aren't overwhelmed or blinded at critical moments.

- **User Data Leaks:** As seen with Coinmama, BuyUcoin, and even Bithumb's 2017 leak, breaches that expose user data (even if no crypto is stolen directly) can lead to secondary attacks. Exposed email/password combos lead to account takeover tries; leaked KYC documents can facilitate identity theft. Thus, exchanges must secure not only crypto wallets but also databases of user information (encrypting sensitive data at rest, strict access controls, etc.). Regulatory compliance (like GDPR) increasingly mandates this, but security benefits too.

Overall, the technical causes of exchange breaches boil down to **security oversights** – whether in technology, processes, or human factors. Attackers, ranging from lone hackers

to organized crime syndicates and nation-state APTs, will seize on any weakness. Lazarus Group (North Korea) in particular has been implicated in numerous recent hacks (KuCoin, Liquid, CoinEx, and Bybit among others), often using a blend of social engineering and malware to get inside networks. Their involvement has raised the stakes for exchanges, who now face not just casual cybercriminals but well-resourced adversaries with patience and sophisticated toolsets.

Conclusion: Lessons Learned and Mitigation Strategies

From 2011's Mt.Gox fiasco to the record-smashing Bybit hack of 2025, the history of crypto exchange breaches has taught the security community some hard lessons. Exchanges that failed to learn from others often *became* lessons themselves. Here are the most important takeaways and defenses that have emerged:

- **"Hot Wallets = Hot Targets."** Minimize hot wallet exposure. The vast majority of exchange losses came from hot wallets, so only keep what's needed for liquidity in them. Use **multisignature or MPC** for hot wallets so that a single server breach or key theft isn't catastrophic. If possible, **geographically distribute keys** or use HSMs (Hardware Security Modules) to make illicit key exfiltration extremely difficult. Cold storage should hold the bulk (>95%) of funds, and transferring from cold to hot should require manual human authorization in multiple steps. In practice, many top exchanges now have dedicated cold-wallet teams, out-of-band transfer approval, daily withdrawal limits, and other mechanisms to protect against hot-wallet draining.

- **Secure the Development Pipeline.** Advanced attackers might target the software supply chain. Implement **code-signing, integrity checks, and least-privilege principles** for deployment systems. Developers should not have direct access to production keys, and any code affecting wallet transactions should be reviewed by multiple engineers. Infrastructure-as-code and reproducible builds can help detect unauthorized changes. Exchanges should also monitor their DNS records, cloud console access, and third-party integrations (like analytics scripts) to prevent breaches via those vectors.

- **Comprehensive Auditing and Monitoring.** Exchanges must relentlessly audit their systems – both the code (to catch bugs) and the operations (to catch irregularities). Employ dedicated security teams to perform **penetration testing** and **threat hunting** internally. Monitor wallet addresses on the blockchain: large or unusual movements should set off alarms immediately (some exchanges even integrate with blockchain analytics to watch for their own addresses showing up in mempools unexpectedly). Maintain proper **logs of all access and actions** in systems touching funds, and store backups of those logs securely so that even if hackers try to cover tracks, there's an evidence trail. The faster a breach is detected, the more chance there is to mitigate damage (e.g., by broadcasting transactions to move remaining funds to safe wallets, as KuCoin did).

- **Principle of Least Privilege (PLP).** Restrict access rights for both systems and people. Employees should only have the minimum access necessary for their role. Critical key material or withdrawal authorization should require multiple people (e.g., a "four-eyes" rule). Admin interfaces should be protected by multiple layers of authentication and network restrictions (VPN, IP allowlisting). Implement **secure enclave or blind signing** systems where possible so that even an insider cannot directly see or extract private keys. Many exchanges now use **withdrawal quorums** – a transaction from cold storage might require approval from, say, 3 of 5 senior executives – to reduce single points of failure.

- **Strong User Account Security Features.** Given that end-users can be the weakest link, exchanges need to *help* users protect themselves. This means offering Two-Factor Authentication beyond SMS (and educating users to use it), **email confirmations or push alerts for withdrawals**, optional **whitelisted addresses**, device management (ability to view and revoke devices logged into the account), and **transaction monitoring with AI** to flag if a user's behavior suddenly deviates (which could indicate an account takeover). In Coinbase's case, after the 6,000-user incident, they moved to **hardware security keys** and WebAuthn support for users, which is a trend many others follow. Ultimately, exchanges may move toward requiring phishing-resistant MFA for large transactions.

- **Backups, Insurance, and Incident Response.** Despite best efforts, breaches may still occur. Exchanges should prepare playbooks for incident response: how to quickly **freeze operations** to contain a hack (as many did to stop further losses), whom to contact (law enforcement, blockchain tracing firms) to attempt recovery, and how to communicate transparently to users to maintain trust. Setting up an **insurance fund or obtaining an insurance policy** is now considered best practice – this ensures users can be made whole without bankrupting the exchange. Binance's SAFU fund and other exchanges' contingency reserves have proven crucial in turning a potentially fatal hack into a solvable problem. Additionally, participating in industry cooperation – for example, many exchanges now promptly **blacklist addresses** associated with a hack as soon as intel is shared – can deter would-be thieves by reducing their options to cash out.

- **Regulatory and Compliance Measures.** Regulators have taken note of high-profile hacks and in some jurisdictions require exchanges to adhere to specific security standards (e.g., **Japan's FSA tightened custody rules after Coincheck**, and **US regulators expect SOC2 type audits for larger custodians**). While regulation alone can't prevent hacks, **compliance reviews often force exchanges to shore up weak points**. For instance, requiring a percentage of funds in cold storage or mandating insurance and annual penetration tests are becoming conditions for licensing. These measures push the industry toward a more security-conscious baseline.

Perhaps the silver lining is that each disaster has prompted improvements across the board. The exchange ecosystem in 2025 is far more security-hardened than in 2011. Concepts like **"Don't trust, verify"** are now ingrained – whether it's verifying that code is secure or that insiders can be trusted. Many exchanges collaborate with white-hat hackers and academic researchers to stay ahead of threats. There is also a shift towards *non-custodial trading models* (DEXs, hybrid exchanges) which, if they mature, could eliminate certain risks entirely by not holding user funds. Until then, centralized exchanges remain juicy targets, and thus must remain ever-vigilant.

In conclusion, securing a crypto exchange is a multidimensional challenge: it requires robust software engineering, strict operational security, vigilant human governance, and savvy user-side protections. The breaches from 2011 to 2025 highlight what can go wrong when any of those aspects falter. By learning from these failures – **ensuring keys are safely kept, code is clean, insiders are watched, and users are supported** – the industry can prevent history from repeating itself. Crypto exchanges carry a profound responsibility as gatekeepers of digital assets, and the continued evolution of attack techniques means that security is not a one-time goal but an ongoing process. The war between attackers and defenders will no doubt continue, but the lessons from past battles arm us to better protect the cryptocurrency ecosystem going forward.