Morgan Stanley | RESEARCH

GLOBAL IDEA

October 31, 2026 01:59 PM GMT

Digital Assets

The Binance Hack: Risks Beyond the Breach

The world's largest crypto exchange suffered a record $6.3bn hack. We expect further market disruption and see broader implications for crypto security, custody, and regulation. This raises downside risk to COIN/GEMI earnings & multiples; HOOD less exposed, though NT sentiment risk remains.

Felix Stratmann
Equity Strategist
Felix.Stratmann@morganstanley.com +44 20 7677-0365

Michael J. Cyprys, CFA, CPA
Equity Analyst
Michael.Cyprys@morganstanley.com +1 212 761-7619

Kade O'Reilly
Research Associate
Kade.O'Reilly@morganstanley.com +1 212 761-2913

Key Takeaways

- Muted initial reaction, but risks remain. Withdrawal restrictions, reduced liquidity, and deleveraging could drive further weakness.
- Crypto hacks often reflect control failures, not blockchain flaws. Major breaches have exploited custody and operational infrastructure.
- Regulation could strengthen investor protection through operational standards, asset segregation, and accountability.
- Spot DEX migration looks limited. Perpetual DEXs have a stronger case, but independent custody offers an alternative.
- Limited read-through to tokenization. We see little impact on the longer-term thesis for blockchain-based issuance and settlement.

We expect further pressure on crypto markets despite the relatively benign initial reaction. Binance's reimbursement commitment and the freezing of ~$3bn of stolen assets have helped contain the sell-off, but we see risks from withdrawal restrictions, reduced liquidity, and deleveraging. Historically, major hacks have been followed by delayed market weakness, although causality is difficult to establish.

The incident highlights vulnerabilities in custody and operational controls, rather than underlying blockchain technology. The integration of trading, custody, and settlement within centralized exchanges (CEXs) can amplify these risks. Regulation could strengthen investor protection through operational safeguards and accountability, potentially benefiting regulated custodians, including banks.

We see greater potential for separation of custody from execution than wholesale migration toward decentralized exchanges (DEXs). Importantly, we see limited implications for the longer-term tokenization thesis, as tokenized assets can operate within regulated issuance, custody, and settlement frameworks without relying on crypto exchanges.

Stock implications: Negative read-across for COIN/GEMI post the reported $6.3bn Binance hack, adding downside risk to our 2027 earnings forecasts and valuation multiples as the crypto trading recovery faces renewed headwinds. While potential share gains could provide some offsets for COIN/GEMI, we see less direct earnings risk at HOOD, though NT sentiment and valuation could come under pressure.

investors should be aware that the firm may have a conflict of

Research as only a single factor in making their investment decision.

For analyst certification and other important disclosures, refer to the Disclosure Section, located at the end of this report.

+= Analysts employed by non-U.S. affiliates are not registered with FINRA, may not be associated persons of the member and may not be subject to FINRA restrictions on communications with a subject company, public appearances and trading securities held by a research analyst account.

What Happened

On 29 October 2026, Binance, the world's largest centralized cryptocurrency exchange (CEX) by trading volume (~30% spot share, ~40% futures share MTD), suffered a security breach affecting an estimated$6.3bn in cryptoassets, potentially the biggest hack in crypto history. While the precise cause remains under investigation, early reports suggest attackers gained access to Binance's withdrawal systems, potentially through a compromised employee laptop. According to blockchain intelligence firms, most of the stolen assets were moved across 10 blockchains within approximately 20 minutes, pointing to a compromise of transaction approval processes rather than the underlying blockchain technology. Notably, **the attackers also leveraged DeFi and other crypto market infrastructure to rapidly convert stolen assets into harder-to-freeze cryptocurrencies.** Blockchain intelligence firms identified the use of decentralized trading platforms, market makers, and lending protocols to move or borrow against stolen assets before freezes could take effect, complicating efforts to recover the funds.

Binance has moved to contain the losses, working with stablecoin issuers (including Circle and Tether), blockchain networks, and law enforcement to freeze approximately $3bn of affected assets (~48%). Most restrictions involved issuer-level token freezes, while Arbitrum's Security Council conducted a direct network-level intervention. However, TRM Labs estimates that attackers still control around $2.4bn in BTC and ETH beyond the reach of issuer-level freezes, illustrating the limitations of existing recovery mechanisms. Binance temporarily suspended withdrawals, while deposits remain operational. Binance has committed to reimbursing all losses through its SAFU emergency fund and corporate resources, although full restitution has yet to be independently verified.

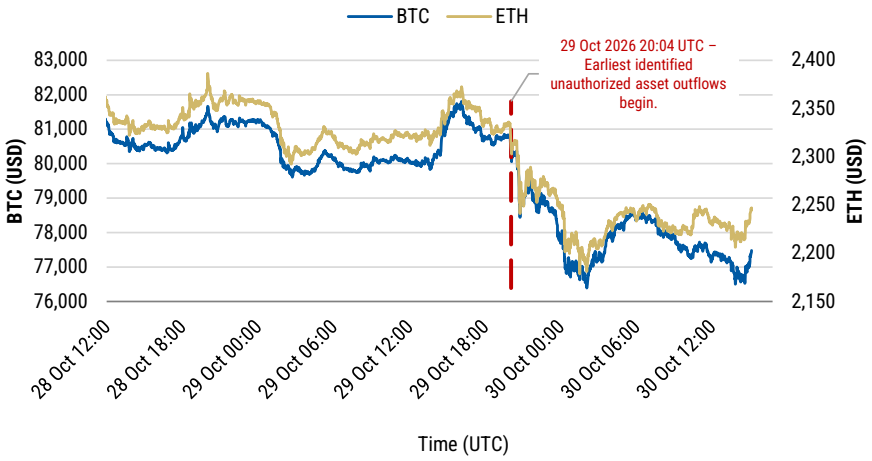
Binance has pledged to cover all losses and has announced that it has allocated more than $6.34bn of company funds, including $5bn already held in the affected tokens. It says it is purchasing the remaining approximately $1.34bn through spot and OTC markets. This reduces the apparent near-term solvency risk, although independent verification remains outstanding.

Market Impact and Historical Context

Market Impact

Despite the severity of the hack, crypto markets have held in relatively well, but we expect the event to weigh on market sentiment and increase volatility. BTC and ETH initially fell 4.9% and 5.7%, respectively, but have recovered somewhat to sit at down 3.6% and 2.7%, respectively, since the hack. Some assets have fared better, with HYPE only down 0.1%. Given the severity of the incident, this market reaction feels relatively benign to date, but likely reflects Binance's commitment to reimburse affected customers and its ability to freeze approximately $3bn of stolen assets.

Exhibit 1: Crypto prices have held up relatively well despite the record Binance hack



We see disruption to market liquidity and leveraged trading as the key near-term risks. Binance's suspension of withdrawals restricts collateral transfers between exchanges, potentially limiting market makers' ability to replenish margin, reducing arbitrage activity, and forcing position unwinds. We believe this could amplify downside pressure as liquidity deteriorates. Early signs of disruption include sharply wider Binance bid-ask spreads, bearish options positioning, and ~$1.6bn of market-wide futures liquidations.

We see the resumption of Binance withdrawals (expected by Sunday, 1 November) as the next critical test for market confidence. Prolonged restrictions, significant customer outflows following reopening, additional security disclosures, and continued deleveraging could drive further weakness. Conversely, an orderly reopening and independent verification of customer-asset backing would help mitigate these risks.

We see the attackers' use of DeFi and market-making infrastructure as an additional source of potential contagion, with stolen assets flowing through otherwise unaffected platforms and creating liquidity, counterparty, and compliance risks beyond Binance itself.

Historical Context

The Binance incident is the latest in a series of major cryptocurrency hacks, with billions of dollars stolen from centralized exchanges, cross-chain bridges, and decentralized finance (DeFi) protocols over the past five years. **While these incidents have raised concerns around the security of digital assets, many of the largest losses have resulted from failures in operational controls, access management, and transaction authorization, rather than vulnerabilities in the underlying blockchains themselves.** Chainalysis estimates that compromised private keys accounted for 44% of stolen cryptoassets in 2024, highlighting the importance of how digital assets are safeguarded and controlled.

Several high-profile incidents illustrate these vulnerabilities.

- The $1.5bn Bybit hack in February 2025 involved attackers compromising a third-party wallet provider and manipulating its transaction-signing interface, allowing malicious transfers to be approved by authorized personnel.
- Similarly, the $308m DMM Bitcoin hack in May 2024 originated from a social-engineering attack against an employee of a third-party wallet software provider.
- The $625m Ronin bridge exploit in March 2022 involved compromised validator credentials and inadequate separation of signing authority.

In each case, attackers exploited weaknesses in the systems and processes governing access to digital assets, rather than breaking the underlying blockchain's cryptography.

However, not all hacks can be attributed to operational failures. **DeFi protocols and cross-chain bridges have also suffered losses from vulnerabilities in smart-contract code, verification mechanisms, and protocol design, including the Wormhole and Euler exploits.** Still, the historical record suggests that security risks frequently arise at the application, custody, and governance layers, rather than from blockchain technology itself.

The implications extend beyond cybersecurity. **For centralized exchanges in particular, the concentration of trading, custody, and asset-transfer functions can amplify the consequences of operational failures.** This raises broader questions around the resilience of crypto market infrastructure, the impact of security breaches on customer confidence and trading activity, and whether greater separation of custody functions, stronger institutional safeguards, and regulatory oversight could mitigate these risks.

Exhibit 2: Binance hack could be the largest of the last 5 years

#	Date	Venue	Type	Stolen $m	Recovery / compensation (status | facts)	Attack vector (class | mechanism)
1	Oct-26	Binance	CEX	6,300	Pledged | ~$3.0bn frozen; SAFU + own funds cover	Infra compromise | DevOps laptop → withdrawal service
2	Feb-25	Bybit	CEX	1,460	Made whole | $48m recovered, $31m frozen (~5%)	Infra compromise | Tampered signing UI misled signers
3	Mar-22	Ronin (Axie)	Other DeFi	625	Made whole | ~$30m seized; Sky Mavis refunded users	Social engineering | 5-of-9 validator keys taken over
4	Oct-22	BNB Chain bridge	Other DeFi	586	No user loss | ~$430m halted by validator pause	Bridge flaw | Forged Merkle proof minted 2m BNB
5	Nov-22	FTX (post-bankr.)	CEX	477	None reported | Some tokens blocked; no restitution	Social engineering | SIM-swap of FTX account (alleged)
6	Sep-26	Bitget	CEX	388	Venue absorbed | Protection Fund used; ~$1m frozen	Infra compromise | Vendor tool flaw; forged withdrawals
7	Feb-22	Wormhole	Other DeFi	326	Made whole | Jump refilled 120k ETH; none recovered	Bridge flaw | Forged guardian signature minted wETH
8	Sep-26	Liquid Network	Other DeFi	319	Partial | 3,400 BTC (85%) returned; ~598 BTC missing	Protocol flaw | Proof-cache bug minted unbacked L-BTC
9	May-24	DMM Bitcoin	CEX	308	Made whole | Accounts moved to SBI VC Trade (1:1)	Social engineering | Vendor manipulated; tx intercepted
10	Apr-26	KelpDAO (rsETH)	Other DeFi	292	Made whole | rsETH re-backed; $71m frozen	Infra compromise | RPC nodes hijacked; 1-of-1 verifier
11	Apr-26	Drift Protocol	DEX	285	Partial | ~1% paid; recovery tokens; ~$3m frozen	Social engineering | Admins pre-signed txs; fake collateral
12	Jul-24	WazirX	CEX	235	Partial | ~85% paid; 15% as recovery tokens	Infra compromise | Multisig signers shown false tx data
13	May-25	Cetus	DEX	223	Partial | $162m returned; pools ~85%+ restored	Protocol flaw | Integer overflow in liquidity maths
14	Sep-23	Mixin Network	Other centralized	200	Partial | Compensation proposed; recovery not verified	Infra compromise | Third-party cloud database breached
15	Mar-23	Euler Finance	Other DeFi	197	Made whole | 100% returned by exploiter (negotiated)	Protocol flaw | Flash loan + flawed donate/health check
16	Dec-21	BitMart	CEX	196	Pledged | Operator promised cover; unverified	Key compromise | ETH/BSC hot-wallet keys stolen
17	Aug-22	Nomad	Other DeFi	190	Partial | ~$37m returned by white hats	Bridge flaw | Faulty trusted root; withdrawals replayable
18	Sep-22	Wintermute	Other centralized	160	Venue absorbed | Firm funds only; no customer loss	Key compromise | Vanity-address key brute-forced
19	Dec-21	Vulcan Forged	Other centralized	140	Made whole | Treasury-funded replacement reported	Key compromise | Custodial player-wallet keys stolen
20	Nov-25	Balancer V2	DEX	128	Partial | ~$28m recovered (incl. $19.7m StakeWise)	Protocol flaw | Rounding error in stable-pool maths

Vector classes: Social engineering (people/vendor/SIM) · Infra compromise (backend, vendor tooling, signing UI, cloud) · Key compromise · Protocol flaw (code/maths) · Bridge flaw (on-chain verification)
Status: Made whole = users restored 1:1 (not necessarily via recovery) · Venue absorbed = operator bore loss · Pledged = commitment only · Frozen ≠ returned

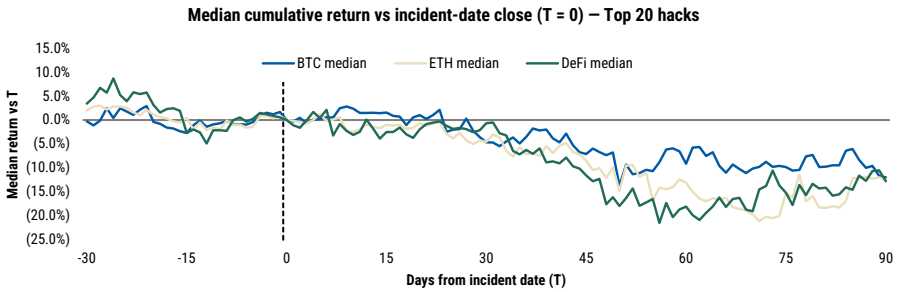
Note: Last 5 years of hacks only

How have markets reacted to hacks in the past?

Across the 20 largest crypto hacks since late 2021, the market reaction has been a slow grind lower rather than an immediate shock. The median BTC and ETH moves on the day of the incident were modest (-1.6% and -0.9%), and both were roughly flat a week later (+0.5% and +0.1%). The weakness came later: the median return is about -4.7% for BTC and -4.6% for ETH after 30 days, and about -12% for both after 90 days. DeFi-related names showed a similar drift lower.

These results describe association, not causation, and should be interpreted with caution. The sample is small (20 events, with only 17 having a full 90-day window), so the median path becomes noisier over time. Several large hacks fell in 2022, when crypto was already in a broad drawdown, and several recent ones are too new to have complete windows.

Exhibit 3: Crypto hacks have often been met with muted price action initially and a longer-term drift lower, although events in question frequently occurred within the context of an existing crypto downtrend

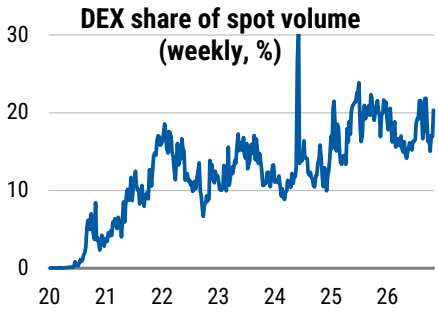


Source: Talos CM Market Data

The Bybit hack in February 2025 provides a useful precedent for how security breaches can redistribute CEX market share. Bybit's share of spot trading volumes fell from 9.9% in January to 5.4% in March (-4.5pp), with Binance (+4.7pp), Huobi (+2.1pp), and Bullish (+1.8pp) among the largest beneficiaries. The impact on perpetual futures was more muted, with Bybit's share declining from 16.0% to 14.5% (-1.4pp), while MEXC (+2.1pp), Gate.io (+1.0pp), and OKX (+0.6pp) gained share. Bybit subsequently recovered some spot share, reaching 7.0% by May. This suggests that hacks can drive meaningful competitive displacement, particularly in spot trading, without necessarily causing a permanent loss of market share.

Will CEX Hacks Drive a Migration to DEXs?

Exhibit 4: Spot DEX share gains appear driven by factors beyond CEX security concerns



Source: DeFiLlama

While major CEX hacks could strengthen the appeal of decentralized trading, we see limited evidence of a structural shift in spot volumes. Centralized exchanges generally retain advantages in execution costs, liquidity, and market depth, while investors can move assets into independent custody following execution. Increasingly, off-exchange settlement arrangements also allow institutions to access CEX liquidity without pre-funding exchange wallets. We believe the recent growth in spot DEX market share has been driven more by memecoin speculation and trading in long-tail tokens than by security concerns.

The argument is stronger for perpetual futures, where traders traditionally maintain collateral on centralized exchanges to support open positions, creating more persistent counterparty exposure. Decentralized platforms such as Hyperliquid offer an alternative, with collateral and positions managed through on-chain infrastructure rather than exchange-controlled wallets. However, institutional off-exchange custody and collateral solutions, including Copper ClearLoop, Fireblocks Off Exchange, and bank triparty arrangements, increasingly allow traders to retain centralized execution while reducing their direct exposure to exchange custody.

The more consequential structural shift may therefore be the separation of custody from execution, rather than wholesale migration toward DEXs. Crypto exchanges have historically combined trading, custody, and settlement within vertically integrated platforms, concentrating operational risk. Repeated security breaches could encourage investors to move assets toward independent custody while continuing to trade on CEXs. **This would preserve the role of centralized exchanges as liquidity and execution venues, while potentially benefiting regulated custodians, including banks, as institutional investors place greater emphasis on asset segregation, operational resilience, and investor protection.**

We see limited read-through from the Binance hack to the longer-term growth of tokenized assets. The incident primarily highlights weaknesses in intermediary controls and custody infrastructure, rather than underlying blockchain technology. Tokenized securities, funds, and other real-world assets can operate within regulated issuance, custody, and settlement frameworks without relying on crypto exchanges. While operational and cybersecurity risks remain relevant, we do not see this incident as fundamentally undermining the investment case for tokenization, which is driven by potential improvements in settlement efficiency, collateral mobility, and market accessibility.

Where Could Regulation Help

The frequency and scale of cryptocurrency hacks raise questions around whether stronger regulation could mitigate security risks and improve customer protection. While regulation cannot eliminate cyberattacks or vulnerabilities in blockchain applications, traditional financial markets provide an established framework for managing operational risks, safeguarding client assets, and allocating liability when failures occur.

Crypto exchanges have historically combined trading, custody, and settlement within integrated platforms, concentrating operational and counterparty risk. Traditional securities markets generally operate through distinct intermediaries and regulatory safeguards governing these functions, including client-asset segregation, operational controls, capital requirements, and independent oversight. Although vertical integration is not universally prohibited, these safeguards can limit the concentration of risk and protect customer assets from misuse or intermediary failure.

Regulatory frameworks are increasingly extending similar principles to crypto. The EU's MiCA establishes client-asset protections and custodian liability for attributable losses, while DORA requires technology-risk management, resilience testing, and third-party oversight. Proposed US legislation, including the CLARITY Act, has sought to introduce clearer oversight and custody safeguards, although its failure to progress leaves uncertainty around the future regulatory framework for spot crypto trading.

We see regulation's value in making operational safeguards and client protections enforceable, rather than eliminating hacks altogether. Importantly, Binance already operates through separately regulated exchange, custody, and brokerage entities under Abu Dhabi's ADGM framework. The question is therefore whether legal separation is matched by effective operational controls, clear liability, and sufficient financial resources to absorb losses. **We believe this could support demand for regulated custodians, including banks, whose competitive advantage may increasingly extend beyond technology to financial capacity, institutional servicing, and enforceable client protections.**

Exhibit 5: Regulation could help prevent, contain, and absorb crypto losses

	01 PREVENTION	02 INTERVENTION	03 LOSS ABSORPTION	04 ACCOUNTABILITY
OBJECTIVE	Reduce breach likelihood	Contain theft and movement	Increase recovery capacity	Clarify who bears losses
CORE CONTROL	• Access controls • Third-party oversight • Transaction authorization	• Incident response • Issuer freezes • Lawful coordination	• Prudential safeguards • Insurance • Indemnities	• Client segregation • Custody duties • Supervision
KEY LIMITATION	Cannot guarantee systems or people are never compromised	No general right to reverse BTC or ETH transfers	Minimum capital and insurance are not full loss guarantees	Claims depend on cause, contract, jurisdiction and solvency
OUTCOME	LOWER PROBABILITY ›	LIMIT SPILLOVERS ›	FINANCE RESTITUTION ›	ENFORCE OBLIGATIONS

Implications for Stocks

Michael Cyprys - US Brokers, Asset Managers & Exchanges

Negative read-across for COIN and GEMI, with growing downside risk to our earnings estimates and valuation multiples. We view the reported $6.3bn Binance hack as another headwind to an already challenging crypto trading backdrop, with potential to weigh on customer confidence, retail engagement and institutional activity. Recall that trading volumes were already tracking below expectations in October following a stronger September, increasing risk to our forecasts for a recovery in crypto activity. In our recent COIN initiation, we outlined a sharp rebound in 2027 transaction revenue, underpinned by recovering crypto volumes and retail participation. We now see a more challenging path to that recovery, with **scope for meaningful downward revisions to our volume and earnings forecasts for both COIN and GEMI should weakness persist**. GEMI appears particularly exposed given its smaller scale and greater reliance on crypto trading, while COIN's broader revenue base, derivatives and market-share gains provide some offsets. Importantly, we **see risk extending beyond earnings, as weaker confidence in the recovery could also pressure valuation multiples**.

We see less direct earnings risk at HOOD, where crypto accounted for just 8% of 3Q26 revenue vs. 21% a year ago, though the shares have historically traded alongside crypto-exposed names and could face sentiment-driven pressure.

The Binance hack renews focus on security and confidence across crypto market infrastructure. As our Digital Assets team discusses, Binance suffered an estimated $6.3bn security breach on Oct. 29, potentially the largest crypto hack on record. Approximately $3bn of affected assets have been frozen, while Binance has pledged to reimburse customer losses. While crypto prices have held up well given the magnitude of the incident, we see uncertainty around longer-term implications for customer confidence and trading activity. Disruptions to withdrawals and collateral movements could weigh on market liquidity and contribute to further deleveraging. Historical analysis of major crypto hacks shows that price weakness has often materialized over subsequent months rather than immediately, though many of these incidents coincided with broader crypto-market downturns. Importantly, while heightened volatility and liquidations can temporarily support trading volumes, we see greater risk that a prolonged period of weaker confidence dampens customer engagement and trading activity.

Potential market-share offsets, though weaker industry volumes remain the bigger near-term risk. Neither COIN nor GEMI was directly impacted in the incident, and we see potential for customers to shift assets toward platforms perceived as having stronger custody, security and regulatory safeguards. COIN's scale, institutional infrastructure and growing share of crypto trading volumes could position it to benefit from such migration. That said, market-share gains may not fully offset a weaker industry backdrop, particularly given Coinbase's reliance on higher-monetizing retail activity. Longer term, the incident could reinforce demand for regulated custody and stronger operational controls, potentially benefiting scaled financial platforms. Near term, we'd focus on trading-volume trends into November, retail engagement, exchange market shares, customer asset flows and signs of further deleveraging. Continued weakness would increase the likelihood of downward estimate revisions and multiple compression across crypto-exposed exchanges.

Digital assets, sometimes known as cryptocurrency, are a digital representation of a value that function as a medium of exchange, a unit of account, or a store of value, but generally do not have legal tender status. Digital assets have no intrinsic value and there is no investment underlying digital assets. The value of digital assets is derived by market forces of supply and demand, and is therefore more volatile than traditional currencies' value. Investing in digital assets is risky, and transacting in digital assets carries various risks, including but not limited to fraud, theft, market volatility, market manipulation, and cybersecurity failures—such as the risk of hacking, theft, programming bugs, and accidental loss. Additionally, there is no guarantee that any entity that currently accepts digital assets as payment will do so in the future. The volatility and unpredictability of the price of digital assets may lead to significant and immediate losses. It may not be possible to liquidate a digital assets position in a timely manner at a reasonable price.

Regulation of digital assets continues to develop globally and, as such, federal, state, or foreign governments may restrict the use and exchange of any or all digital assets, further contributing to their volatility. Digital assets stored online are not insured and do not have the same protections or safeguards of bank deposits in the US or other jurisdictions. Digital assets can be exchanged for US dollars or other currencies, but are not generally backed nor supported by any government or central bank.

Before purchasing, investors should note that risks applicable to one digital asset may not be the same risks applicable to other forms of digital assets. Markets and exchanges for digital assets are not currently regulated in the same manner and do not provide the customer protections available in equities, fixed income, options, futures, commodities or foreign exchange markets.

market making, providing liquidity, fund management, commercial banking, extension of credit, investment services and investment banking.

Valuation Methodology and Risks

Coinbase Global Inc (COIN.O)

Derived from 20.0x target EV/EBITDA on 2028E adj. EBITDA. We anchor on 2028 rather than the sharper 2027 recovery as a better measure of normalized mid-cycle earnings. The multiple is broadly consistent with COIN's historical valuation and digital-asset peers, while recognizing its scale, liquidity, institutional position and broader revenue mix.

Risks to Upside

- Stronger crypto volumes and adoption
- More resilient retail take rates
- Faster regulatory clarity and product expansion
- Stronger derivatives, Everything Exchange, stablecoin, and Base monetization

Risks to Downside

- Weaker volumes and retail engagement
- Faster take rate compression
- Regulatory delays or reversal
- Slower to monetize new products

Gemini Space Station, Inc (GEMI.O)

Derived from 4.7x target EV/Sales multiple on 2028 Revenue. Our target multiple reflects a warranted discount to where peers (HOOD, COIN) are trading on '28 due to lack of scale and unprofitability, but we see scope for multiple expansion if the company grows prediction mkts and develops a track record in growing the card business and translating those users into active exchange members, while a supportive regulatory backdrop supports growth.

Risks to Upside

- Stronger crypto activity and share retention
- Card customer acquisition and exchange conversion reaccelerate
- New products scale faster than expected
- Profitability inflects sooner than expected

Risks to Downside

- Continued share loss despite stronger crypto mkts
- Card acquisition and engagement remain weak
- Newer products fail to achieve meaningful scale
- Investment needs extend losses and require dilutive capital raise

Robinhood Markets, Inc. (HOOD.O)

Valuation based on discounting 2031e EPS from existing business an
new business lines, to which we ascribe a 25x P/E multiple reflecting a
profile in 2031 and discount back to arrive at our PT. The largest contri
EPS include crypto, European brokerage, credit card, and banking / a

Risks to Upside



- Animal spirits sustain higher retail trading
- Favorable regulatory backdrop, including for crypto and prediction mkts., enhance rev opportunity
- Faster adoption of new initiatives
- Higher-for-longer rates

Risks to Downside

- Intense competition for Gen Y/Z customers
- Regulatory change that curtails order flow or interchange revenues
- Rapid rate cuts
- Tech glitch that dents customer confidence and invites regulatory scrutiny