

Item 2. Management’s Discussion and Analysis of Financial Condition and Results of Operations

Management’s discussion and analysis of our financial condition and results of operations should be read in conjunction with the condensed consolidated interim financial statements and notes thereto included elsewhere in this Quarterly Report on Form 10-Q. Some of the information contained in this Quarterly Report on Form 10-Q includes forward-looking statements that involve risks and uncertainties. You should read the sections titled “Special Note Regarding Forward-Looking Statements” and “Risk Factors” for a discussion of important factors that could cause actual results to differ materially from the results described in or implied by the forward-looking statements contained in the following discussion and analysis.

Overview

Galaxy is a global leader in digital assets and data center infrastructure, delivering solutions that accelerate progress in finance and artificial intelligence (“AI”). We are strategically positioned to bridge traditional finance and the emerging digital economy, facilitating efficient access and adoption of digital assets by institutional clients through our Global Markets and Asset Management & Infrastructure Solutions businesses within our Digital Assets segment. We also develop, and will in the future operate, high performance computing (“HPC”) data center infrastructure to meet the rising global demand for reliable power and scalable compute capacity driven by accelerated AI growth.

Digital Assets

Galaxy’s Digital Assets operating business segment provides a comprehensive and evolving suite of financial products and services tailored for institutions seeking exposure to the digital asset ecosystem. This segment includes our Global Markets and Asset Management & Infrastructure Solutions businesses.

Our Global Markets business provides over-the-counter (“OTC”) spot and derivatives trading, lending, and structured products, as well as transaction advisory and equity and debt capital markets services. Our client base includes more than 1,500 trading counterparties globally as of September 30, 2025, including asset managers, hedge funds, family offices, Qualified Individuals¹ and corporations.

- Galaxy’s trading business includes electronic OTC, high-touch OTC, derivatives trading, and lending. The electronic and high-touch OTC businesses operate on a principal basis, providing liquidity in digital assets to institutional clients and Qualified Individuals. In our electronic OTC business, trading is facilitated through API connectivity. Our high-touch OTC offering mirrors the electronic desk in strategy and risk management, but operates primarily through chat-based channels. The desk utilizes a blend of internal and third-party platforms to access liquidity and manage risk, with 24/7 coverage to support client engagement and execution. The derivatives trading business offers liquidity in options and forwards to institutional counterparties, with trading activity spanning both OTC and exchange-listed and cleared products.
- Our investment banking business provides strategic and transaction advisory services focused on the digital assets sector. The team assists clients with growth strategy, mergers and acquisitions, capital formation, and other financial transactions. Leveraging deep industry knowledge and a strong global network, Galaxy connects innovative companies with institutional investors and delivers customized solutions to support growth, liquidity, and long-term value creation in the digital economy.

Our Asset Management & Infrastructure Solutions business encompasses our investment management division and blockchain infrastructure products and services, with approximately \$17.0 billion in assets across the platform as of September 30, 2025.

- Our asset management business manages a diverse suite of exchange-traded funds (“ETFs”) and alternatives strategies, taking the investing DNA that has been core to Galaxy since our founding and externalizing it for institutional allocators and Qualified Individuals.
- Galaxy’s Asset Management ETFs include a suite of passive and active products developed in partnership with leading asset managers in the U.S., Brazil, Canada, and Europe. Galaxy’s Asset Management passive ETFs feature regulated, spot digital asset ETFs, while its active ETFs provide exposure to digital assets and other

¹ “Qualified Individuals” are Eligible Contract Participants, as defined by the Commodities Exchange Act, knowledgeable employees of Galaxy and accredited investors, who are usually high net worth individuals.

disruptive technologies. Galaxy's Asset Management alternative investment strategies encompass actively managed long-biased and long-short funds, and a venture franchise. Galaxy Asset Management offers a Liquid Crypto Fund designed to provide access to both core and next generation digital assets and an Absolute Return Fund, launched in 2025, which employs a multi-asset strategy with long and short positions across the digital asset ecosystem and adjacent disruptive technologies. Galaxy Asset Management's venture franchise includes Galaxy Interactive, which invests at the intersection of content, technology and social commerce, with a focus on video games and the infrastructure powering immersive virtual worlds. Additionally, our inaugural crypto venture fund targets early-stage investments in protocols, software infrastructure, and financialized applications. The venture franchise also features two global, multi-manager venture funds and manages a subset of Galaxy's balance sheet venture investments.

- Galaxy managed \$10.5 billion in assets across strategies, including ETFs and alternatives, across public and private markets as of September 30, 2025, a 126% increase year-over-year and 81% increase quarter-over-quarter. \$2.4 billion of the \$10.5 billion of assets under management ("AUM") represented engagements managed by Galaxy's asset management team to unwind portfolios on behalf of the estate of FTX as well as assets held within Commodity Pool Operator ("CPO") vehicles. Excluding these opportunistic assets, Galaxy Asset Management's AUM increased by 92% year-over-year to \$8.1 billion as of September 30, 2025, driven by \$3.7 billion of gross inflows and \$2.0 billion of net market appreciation partially offset by \$1.8 billion of gross outflows and increased 53% quarter-over-quarter as of September 30, 2025, driven by \$2.7 billion of gross inflows and \$0.7 billion of net market appreciation partially offset by \$0.7 billion of gross outflows.
- Our Infrastructure Solutions business includes blockchain-centric technology and infrastructure including staking, tokenization and custodial technology.
- Our staking business operates validator nodes to secure blockchains and enable our institutional clients to earn staking rewards, use staked assets as collateral for loans and participate in an increasingly on-chain and decentralized future. Galaxy provides validator services to eleven different blockchain networks, including Ethereum and Solana. As part of our broader suite of infrastructure solutions, we offer secure, institutional-grade cold and hot wallet technology for institutions seeking to self-custody their assets, along with integrated tokenization capabilities.
- Galaxy reported assets under stake ("AUS") of approximately \$6.6 billion as of September 30, 2025, as compared to AUS of approximately \$4.2 billion as of December 31, 2024.

Data Centers

Our Data Centers operating business segment develops, and will in the future operate, HPC infrastructure to meet the growing demand for large-scale, power-ready facilities. Galaxy's Helios data center campus, located in the panhandle region of West Texas, is developing 133 megawatts ("MW") of critical IT load, utilizing approximately 200 MW of gross power capacity, for CoreWeave. In April 2025, CoreWeave exercised its first option under its 15-year lease agreement with Galaxy (the "Lease Agreement"), and in August 2025, we entered into the phase II lease agreement (the "Phase II Lease Agreement") with CoreWeave for the uptake of an additional 260 MW of incremental critical IT load. Also in August 2025, CoreWeave exercised and entered into its second option under the Lease Agreement pursuant to a Phase III option agreement (the "Phase III Option Agreement"), under which it committed to enter into a lease agreement for the uptake of an additional 133 MW of incremental critical IT load. Together, the Phase II Lease Agreement and the Phase III Option Agreement are expected to increase CoreWeave's contracted capacity at the Helios data center campus to 526 MW of critical IT load by 2028. The retrofit of Helios will be completed in phases, with the full 133 MW of initial critical IT load expected to be delivered by the end of the first half of 2026.

Treasury and Corporate

In addition to our two operating business segments, Galaxy holds a diversified portfolio of digital assets, venture, private equity, and fund investments on its balance sheet, and also conducts bitcoin mining operations, all of which are reported within the Treasury and Corporate segment. Treasury engages in proprietary quantitative, arbitrage and macro trading strategies.

Financial and Operational Highlights

- Galaxy generated Net income of \$505.1 million and Net income of \$240.3 million for the three and nine months ended September 30, 2025, respectively, compared to Net loss of \$33.3 million and Net income of \$229.2 million for the three and nine months ended September 30, 2024, respectively.

- Galaxy generated Adjusted EBITDA of \$629.4 million and \$551.1 million for the three and nine months ended September 30, 2025, respectively, compared to Adjusted EBITDA of \$1.9 million and \$353.2 million for the three and nine months ended September 30, 2024, respectively.²
- Total equity as of September 30, 2025 was \$3.2 billion, an increase of 45% from \$2.2 billion as of December 31, 2024.
- In August 2025, Galaxy and CoreWeave entered into the Phase II Lease Agreement and the Phase III Option Agreement, which together are expected to increase CoreWeave’s contracted capacity at the Helios data center campus to 526 MW of critical IT load by 2028.
- On August 15, 2025, Galaxy Helios I LLC (“Galaxy Helios I”) entered into a credit agreement (the “Credit Agreement” and, together with the related transaction documents, the “Project Financing Documents”) with Deutsche Bank AG providing for a senior secured term loan facility in an aggregate principal amount of up to \$1.4 billion (the “Loan Amount”), to finance the first phase of the buildout of our Helios data center campus (the “Project Financing”).

Recent Developments

Tokenized Galaxy

Since September 2025, we enable a natively tokenized version of our Class A common stock, which we refer to as “Tokenized GLXY.” As part of this project, holders of our traditional Class A common stock, which we refer to as “Traditional GLXY,” can obtain Tokenized GLXY. Tokenized GLXY can be held by investors in their self-custodial wallets and transferred bilaterally between “allowedlisted” wallets, and we may in the future permit Tokenized GLXY to be traded over decentralized exchanges or other trading platforms, subject to certain regulatory considerations. Holders of Tokenized GLXY retain the same rights and privileges as holders of Traditional GLXY and on-chain trading of Tokenized GLXY would provide another potential trading market for our Class A common stock, alongside existing trading markets for Traditional GLXY including Nasdaq and the TSX. On May 20, 2025, we entered into a Digital Transfer Agency Agreement with Superstate Services LLC (the “Digital Transfer Agent”) pursuant to which the Digital Transfer Agent has agreed to create and maintain an “Allowlist” of wallet addresses of individuals and entities who have completed the Digital Transfer Agent’s onboarding requirements and are permitted to hold, transfer and facilitate transfers of Tokenized GLXY. Tokenized GLXY provides an additional mechanism for investors to hold and transact in shares in the Company, which may improve settlement efficiency and increase accessibility. Tokenized GLXY may also introduce new risks and uncertainties (including, among others, regulatory and liquidity risks) that could adversely affect the market for, and the trading price of, both Tokenized GLXY and Traditional GLXY.

GalaxyOne

On October 6, 2025, we announced the launch of GalaxyOne. GalaxyOne is a retail financial technology platform designed for individual investors seeking the best of both traditional and digital markets. Its core offerings include (i) access to a Federal Deposit Insurance Corporation (“FDIC”) -insured high-yield demand deposit account offered by our bank partner Cross River Bank for U.S.-based depositors, (ii) a debt security issued by Galaxy Digital LP and guaranteed by GDH LP through the Galaxy Premium Yield Investment Note, initially offering 8.00% yield at the inception of the product, for U.S. accredited investors, and (iii) access to equities and crypto trading via our regulated partners DriveWealth LLC and Paxos, respectively. We are not a bank and are not a member of the FDIC. FDIC-insured high-yield demand deposit accounts and related banking services are provided by our bank partner, Cross River Bank. The Galaxy Premium Yield Investment Note is only available to accredited investors and is offered and sold in unregistered transactions in reliance on Rule 506(c) of Regulation D under the Securities Act. In conjunction with this launch, our legacy GalaxyOne platform for institutional clients was renamed to “GalaxyOne Institutional.”

Private Placement

On October 10, 2025, we entered into investment agreements with certain institutional investors for a \$460 million private strategic investment in our Class A common stock (the “October Private Placement”), consisting of a purchase of 9,027,778 shares of Class A common stock from us and 3,750,000 shares of Class A common stock from certain of our executive officers, including our Founder, at \$36.00 per share. The October Private Placement closed on October 17, 2025.

² See the section titled “Non-GAAP Financial Measures” below for a reconciliation of Net Income / (loss) to Adjusted EBITDA and an explanation for why we consider Adjusted EBITDA to be a helpful metric for investors.

We intend to use the net proceeds to us from the October Private Placement for general corporate purposes and to power the buildout of our Helios data center campus.

2031 Exchangeable Notes

On October 30, 2025, GDH LP issued \$1.3 billion aggregate principal amount of 0.50% exchangeable senior notes due 2031 (the “2031 Exchangeable Notes”). From time to time and subject to the terms of the indenture governing the 2031 Exchangeable Notes, the 2031 Exchangeable Notes are exchangeable for shares of our Class A common stock at the option of the holders thereof. We intend to use the net proceeds from the offering to support growth across our core operating businesses and for general corporate purposes, which may include the repayment of the 2026 Exchangeable Notes (as defined herein).

Our Business Model

Galaxy’s business generates revenue through a variety of channels, creating a diversified and resilient cash flow base that is not directly correlated to any single asset, token, or business line. Within the Digital Assets operating business segment, the Global Markets business earns revenue from spreads on client trades, net interest income from lending activities, and fees from M&A and capital raising transactions. Galaxy’s Asset Management & Infrastructure Solutions business generates management and performance fees on assets under management, fees on assets staked to our validator nodes and licensing fees from institutions who leverage GK8’s proprietary self-custody technology.

Within our Data Centers operating business segment, we expect the majority of revenue to come from long-term lease agreements with cloud service provider clients that Galaxy may obtain from time to time for HPC. Galaxy does not currently earn any revenue from its Data Centers business, but expects this segment to become a significant and diversified source of long-term, predictable revenue for Galaxy, uncorrelated to the prices of digital assets, particularly once we begin to deliver critical IT load for CoreWeave (and potentially other future tenants) starting in 2026.

We also earn revenue by managing a diversified portfolio of digital assets, venture, private equity, and fund investments on our balance sheet, as well as through our bitcoin mining operations, all of which are reported within the Treasury and Corporate segment.

Non-GAAP Financial Measures

To supplement our condensed consolidated financial statements, which are prepared and presented in accordance with GAAP, we use certain non-GAAP financial measures, as described below, to understand and evaluate our business. These non-GAAP financial measures, which may be different than similarly-titled measures used by other companies, are presented to enhance investors’ overall understanding of our financial performance and should not be considered a substitute for, or superior to, the financial information prepared and presented in accordance with GAAP. Adjusted gross profit and Adjusted EBITDA are non-GAAP financial measures that are used by management, in addition to GAAP financial measures, to understand and compare our operating results across accounting periods, for risk management and operational decision-making.

We believe Adjusted gross profit is a helpful non-GAAP financial measure to our management and investors because it eliminates the impact of the directly attributable transaction expenses. As such, it provides useful information about our financial performance, enhances the overall understanding of our past performance and future prospects, allows for greater transparency with respect to important metrics used by our management for financial, risk management and operational decision-making and provides an additional tool for investors to use to understand and compare our operating results across accounting periods.

We believe Adjusted EBITDA provides investors with additional useful information in evaluating Galaxy’s operating performance, as well as a useful measure for period-to-period comparisons of our business performance.

Adjusted gross profit is defined as revenues and gains / (losses) from operations, excluding (i) transaction expenses and (ii) impairment of digital assets.

Adjusted EBITDA is defined as Net income / (loss), excluding (i) equity based compensation, (ii) interest expense on structural debt, (iii) taxes, (iv) depreciation and amortization expense, (v) gains and losses on the embedded derivative on our Exchangeable Notes which ceased to exist upon consolidation as a result of the Reorganization Transactions, (vi) mining-related impairment loss / loss on disposal of mining equipment, (vii) settlement expense, (viii) other (income) / expense, net and (ix) reorganization and reorganization merger costs that we believe are not indicative of our ongoing results. The above items are excluded from our Adjusted EBITDA because these items are non-cash in nature, or because

the amount and timing of these items are unpredictable, are not driven by core results of operations, and render comparisons with prior periods and competitors less meaningful.

These non-GAAP financial measures do not have any standardized meanings prescribed by GAAP and may not be comparable to similar measures presented by other companies in our industry. These non-GAAP financial measures have been prepared by, and are the responsibility of, Galaxy's management, and have not been audited or reviewed by our independent registered public accounting firm. You should not place undue reliance on these non-GAAP financial measures.

The following table presents a reconciliation of Adjusted gross profit to the most directly comparable GAAP measure, revenues and gains / (losses) from operations:

Three Months Ended September 30, 2025				
(in thousands)	Digital Assets	Data Centers	Treasury and Corporate	Total
Revenues and gains / (losses) from operations	\$ 28,805,865	\$ 2,662	\$ 410,326	\$ 29,218,853
Less: Transaction expenses	28,290,508	—	2,269	28,292,777
Less: Impairment of digital assets	197,702	—	—	197,702
Adjusted gross profit	\$ 317,655	\$ 2,662	\$ 408,057	\$ 728,374

Three Months Ended September 30, 2024				
(in thousands)	Digital Assets	Data Centers	Treasury and Corporate	Total
Revenues and gains / (losses) from operations	\$ 8,626,967	\$ —	\$ 85,323	\$ 8,712,290
Less: Transaction expenses	8,509,752	—	26,383	8,536,135
Less: Impairment of digital assets	47,931	—	60,535	108,466
Adjusted gross profit	\$ 69,284	\$ —	\$ (1,595)	\$ 67,689

Nine Months Ended September 30, 2025				
(in thousands)	Digital Assets	Data Centers	Treasury and Corporate	Total
Revenues and gains / (losses) from operations	\$ 50,580,979	\$ 2,662	\$ 547,736	\$ 51,131,377
Less: Transaction expenses	49,807,846	—	61,881	49,869,727
Less: Impairment of digital assets	319,317	—	118,291	437,608
Adjusted gross profit	\$ 453,816	\$ 2,662	\$ 367,564	\$ 824,042

Nine Months Ended September 30, 2024				
(in thousands)	Digital Assets	Data Centers	Treasury and Corporate	Total
Revenues and gains / (losses) from operations	\$ 26,852,394	\$ —	\$ 553,030	27,405,424
Less: Transaction expenses	26,583,046	—	76,015	26,659,061
Less: Impairment of digital assets	67,198	—	123,741	190,939
Adjusted gross profit	\$ 202,150	\$ —	\$ 353,274	\$ 555,424

The following table presents a reconciliation of Adjusted EBITDA to the most directly comparable GAAP measure, Net income / (loss):

(in thousands)	Digital Assets	Data Centers	Treasury and Corporate	Three Months Ended September 30, 2025
Net income / (loss)	\$ 234,392	\$ 2,104	\$ 268,561	\$ 505,057
Add back:				
Equity based compensation	11,989	1,645	8,423	22,057
Notes interest and other expense	—	—	14,415	14,415
Taxes	—	—	40,145	40,145
Depreciation and amortization expense	3,812	—	3,585	7,397
Unrealized (gain) / loss on notes payable – derivative	—	—	—	—
Mining related impairment loss / loss on disposal	—	—	38,027	38,027
Settlement expense	—	—	1,810	1,810
Other (income) / expense, net	(272)	(90)	(595)	(957)
Reorganization and reorganization merger costs	—	—	1,401	1,401
Adjusted EBITDA	\$ 249,921	\$ 3,659	\$ 375,772	\$ 629,352

(in thousands)	Digital Assets	Data Centers	Treasury and Corporate	Three Months Ended September 30, 2024
Net income / (loss)	\$ 8,855	\$ (1,875)	\$ (40,310)	\$ (33,330)
Add back:				
Equity based compensation	11,128	—	6,585	17,713
Notes interest and other expense	—	—	9,107	9,107
Taxes	—	—	(7,885)	(7,885)
Depreciation and amortization expense	3,568	1,875	7,565	13,008
Mining related impairment loss / loss on disposal	—	—	—	—
Unrealized (gain) / loss on notes payable – derivative	—	—	2,858	2,858
Other (income) / expense, net	—	—	(781)	(781)
Reorganization and reorganization merger costs	—	—	1,227	1,227
Adjusted EBITDA	\$ 23,551	\$ —	\$ (21,634)	\$ 1,917

(in thousands)	Digital Assets	Data Centers	Treasury and Corporate	Nine Months Ended September 30, 2025
Net income / (loss)	\$ 235,386	\$ (795)	\$ 5,725	\$ 240,316
Add back:				
Equity based compensation	29,757	2,115	18,997	50,869
Notes interest and other expense	—	—	42,726	42,726
Taxes	—	—	45,503	45,503
Depreciation and amortization expense	10,927	1,251	15,290	27,468
Mining related impairment loss / loss on disposal	—	—	95,057	95,057
Unrealized (gain) / loss on notes payable – derivative	—	—	35,544	35,544
Reorganization and reorganization merger costs	—	—	8,687	8,687
Settlement expense	—	—	7,344	7,344
Other (income) / expense, net	(148)	(90)	(2,185)	(2,423)
Adjusted EBITDA	\$ 275,922	\$ 2,481	\$ 272,688	\$ 551,091

(in thousands)	Digital Assets	Data Centers	Treasury and Corporate	Nine Months Ended September 30, 2024
Net income / (loss)	\$ 17,601	\$ (5,349)	\$ 216,949	\$ 229,201
Add back:				
Equity based compensation	41,875	—	19,626	61,501
Notes interest and other expense	—	—	26,564	26,564
Taxes	—	—	(12,602)	(12,602)
Depreciation and amortization expense	8,057	5,349	20,058	33,464
Mining related impairment loss / loss on disposal	—	—	—	—
Unrealized (gain) / loss on notes payable – derivative	—	—	15,144	15,144
Reorganization and reorganization merger costs	—	—	2,564	2,564
Other (income) / expense, net			\$ (2,606)	(2,606)
Adjusted EBITDA	\$ 67,533	\$ —	\$ 285,697	\$ 353,230

Key Factors Affecting Our Performance

The growth and success of our business as well as our financial condition and operating results have been, and will continue to be, affected by a number of factors, including:

Price and volatility of digital assets

Values of digital assets have been highly volatile. Effects from speculation regarding the future appreciation or depreciation in the value of digital assets, making their market prices more volatile, may materially and adversely affect the value of our digital asset inventory. Changing investor confidence and resultant fluctuations in the price of various digital assets may cause uncertainty in the market and could negatively impact trading volumes of digital assets, which would negatively impact our business and operating results.

Adoption of digital assets

The cryptoeconomy experienced rapid growth in 2021 driven by the simultaneous widespread adoption of digital assets, expanded use of cryptocurrencies and broader blockchain innovations including DeFi and the growth of non-fungible tokens (“NFTs”) as a prominent form of tokenization. After a retreat in 2022, cryptocurrency markets started to rally in 2023, which continued through December 2024. After a brief retreat in the first quarter of 2025, the price of bitcoin stayed above \$100,000 throughout the third quarter of 2025 and reached another all-time high, temporarily exceeding \$126,000 on October 6, 2025. The initially retail-driven adoption of cryptocurrencies has evolved to include institutional holders, utilizing digital assets as both a store of value and for commercial applications. The lead up to the launch of the spot-based bitcoin ETFs in the U.S. in the first quarter of 2024 followed by the U.S. Presidential election in November 2024 provided a boost to bitcoin. According to the Crypto Market Sizing Report released by Crypto.com, the number of worldwide individual cryptocurrency users rose to 708 million as of September 2025, up from 659 million as of December 31, 2024 and 580 million in December 2023. Moreover, bitcoin’s trailing five-year compounded annual growth rate reached 60% as of September 30, 2025. However, historical trends are not indicative of future adoption, and it is possible that the adoption of digital assets and blockchain technology may slow, take longer to develop, or never be broadly adopted, which would negatively impact our business and operating results.

Strategic acquisitions and investments

We intend to continue to use our scale, expertise and balance sheet to identify and execute on acquisitions across our business lines. A series of acquisitions has diversified our product offerings and revenue sources. This includes the acquisition of the Helios bitcoin mining facility and its operations from Argo Blockchain in December 2022. In February 2023, we completed the acquisition of GK8, a developer of secure technology solutions for self-custody of digital assets by institutions, from the Chapter 11 bankruptcy estates of Celsius Network, LLC and its affiliated debtors in possession (the “Celsius Estate”). In July 2024, we acquired the assets of CMF, a blockchain node operator that provides trusted, secure services to decentralized protocols across the digital asset ecosystem. In December 2024, we acquired Fierce, a financial application software provider that we relaunched in October 2025 as GalaxyOne. See “—Recent Developments”. Any such acquisitions of, or investments in, companies with complementary products and technologies may affect our future operating results.

Regulation in U.S. and international markets

Our financial prospects and continued growth depend in part on our ability to continue to operate in a manner compliant with regulations. Our business is subject to the oversight of numerous regulatory agencies in the U.S. and other jurisdictions, including, but not limited to, FinCEN, the SEC and the Commodities Futures Trading Commission (“CFTC”). Many of these agencies have issued consumer advisories regarding the risks posed by digital assets to investors. Our strategy is to continue to invest significantly in our finance, legal, compliance, and security functions in order to remain at the forefront of digital asset policy initiatives and regulatory trends. We primarily service institutional customers potentially mitigating some of the compliance risks. However, as the industry matures, we may experience fluctuations in our operating results as a result of changes in the laws and regulations that are applicable to our business.

Critical Accounting Policies and Estimates

Our unaudited condensed consolidated financial statements are prepared in accordance with GAAP. In preparing the condensed consolidated financial statements, we apply accounting policies and estimates that affect the reported amounts and related disclosures. Inherent in such policies are certain key assumptions and estimates made by management, which we believe best reflect our underlying business and economic conditions. Our estimates are based on historical experience and various other factors and assumptions that we believe are reasonable under the circumstances. We regularly re-evaluate our estimates used in the preparation of the condensed consolidated financial statements based on our latest assessment of the current and projected business and economic environment. By their nature, these estimates and judgments are subject to an inherent degree of uncertainty and actual results could differ materially from the amounts reported based on these estimates.

There have been no material changes to our critical accounting policies and estimates as compared to the critical accounting policies and estimates included in the Company’s Quarterly Report on Form 10-Q for the quarter ended June 30, 2025.

Components of Results of Operations

Revenue

- Digital assets sales: Gross sales proceeds from sales of digital intangible assets.
- Fees: Performance and management fees for unconsolidated funds, for which the Company acts as the general partner and / or manager. Additionally, this includes fees received for investment advisory services including mergers and acquisition advisory, as well as fees earned through technology licensing, mining hosting operations, and mining equipment lease income.
- Blockchain rewards: Gross amount of blockchain generated digital assets and transaction fees earned for proof-of-stake validation, also referred to as staking.
- Proprietary mining: Bitcoin rewards from proprietary digital asset mining.
- Lending: The return that is earned from digital assets and fiat currencies lent to counterparties.

Gains / (losses) from operations

- Net gain / (loss) on digital assets: Realized and unrealized gains / (losses) from changes in the fair value of digital assets that are measured using fair value in accordance with our accounting policies. This includes net gains resulting from the return of Digital intangible assets borrowed and Collateral payable. Digital assets borrowed and Collateral payable digital asset liabilities each contain an embedded derivative that is valued based on the market prices of the underlying digital assets; certain corresponding Digital intangible assets may be held at the lower of cost or lowest observable fair value. Upon repayment of the digital asset loans, the impaired digital intangible assets would have a lower carrying value than the liabilities, resulting in a gain on extinguishment of the Digital asset loans payable. Other digital asset balances such as Digital assets receivable, digital assets posted as collateral, and Digital assets loan receivable, net of allowance are also measured at the fair value of the underlying digital assets and the resulting fluctuations are also included in Net gain / (loss) on digital assets.
- Net gain / (loss) on investments: Gains / (losses) from the changes in fair value of investments, as well as the gain / (loss) from sales of investments held by the Company.

- Net gain / (loss) on derivatives trading: Change in fair value of derivative assets and liabilities, resulting from contracts held by the Company for trading and hedging purposes.

Operating expenses

Operating expenses consist of transaction expenses, impairment of digital assets, compensation and benefits, general and administrative (inclusive of depreciation and amortization), technology, professional fees, and exchangeable notes interest expense.

Transaction expenses

Transaction expenses consist of the following:

- Digital assets sales costs: Carrying value of digital assets sold, net of impairment if applicable, allocated on a first-in-first-out basis.
- Blockchain reward distributions: As a principal in the provision of staking services, the Company recognizes the amount of staking rewards earned by third-parties utilizing the Company's validation infrastructure as part of its operating expenses.
- Borrowing costs: Costs of borrowing digital assets and fiat from clients and counterparties. Borrowed digital assets and fiat are utilized in our trading and lending operations.
- Mining and hosting costs: Mining power costs, including realized and unrealized gains and losses on power purchase agreements, hosting fee expense and costs of mining equipment recognized through sales-type finance leases.
- Other transaction expenses: Trading commissions, custody, and exchange fees incurred by the Company.

Impairment of digital assets

Impairment loss from digital intangible assets which have been marked to the lower of cost or lowest observable fair value in the current period.

Results of Operations

Below is a discussion of our results of operations for the three and nine months ended September 30, 2025 compared to the three and nine months ended September 30, 2024. The results of operations presented below should be reviewed in conjunction with Galaxy's consolidated financial statements and notes thereto included elsewhere in this Quarterly Report on Form 10-Q.

Three and Nine Months Ended September 30, 2025 Compared to Three and Nine Months Ended September 30, 2024

The table below presents our results of operations for the three and nine months ended September 30, 2025 and 2024.

(in millions)	Three Months Ended September 30,				Nine Months Ended September 30,			
	2025	2024	\$ Change	% Change	2025	2024	\$ Change	% Change
Revenues.....	\$ 28,401.9	\$ 8,570.7	\$ 19,831.2	231 %	\$ 50,039.6	\$ 26,788.9	\$ 23,250.7	87 %
Gains / (losses) from operations	817.0	141.6	\$ 675.3	477 %	1,091.7	616.5	\$ 475.2	77 %
Revenues and gains / (losses) from operations	29,218.9	8,712.3	20,506.6	235 %	51,131.4	27,405.4	23,726.0	87 %
Operating expenses:								
Transaction expenses.....	28,292.8	8,536.1	19,756.6	231 %	49,869.7	26,659.1	23,210.7	87 %
Impairment of digital assets.....	197.7	108.5	89.2	82 %	437.6	190.9	246.7	129 %
Compensation and benefits	85.0	57.3	27.8	49 %	207.0	179.6	27.4	15 %
General and administrative	58.7	23.9	34.8	146 %	164.5	65.9	98.6	150 %
Technology	11.5	7.6	3.9	51 %	33.0	21.4	11.6	54 %
Professional fees	14.5	10.9	3.5	32 %	58.0	38.2	19.8	52 %
Notes interest expense	14.4	7.1	7.3	103 %	42.7	21.1	21.6	102 %
Total operating expenses	28,674.6	8,751.4	19,923.2	228 %	50,812.6	27,176.3	23,636.3	87 %
Other income / (expense):								
Unrealized gain / (loss) on notes payable – derivative	—	(2.9)	2.9	100 %	(35.5)	(15.1)	(20.4)	(135) %
Other income / (expense), net.....	1.0	0.8	0.2	25 %	2.5	2.6	(0.1)	(4) %
Total other income / (expense)	1.0	(2.1)	3.0	143 %	(33.0)	(12.5)	(20.5)	(164) %
	\$ 545.2	\$ (41.2)	\$ 586.4	1,423 %	\$ 285.8	\$ 216.6	\$ 69.2	32 %
Income taxes expense / (benefit)	40.1	(7.9)	48.0	608 %	45.5	(12.6)	58.1	461 %
Net income / (loss)	\$ 505.1	\$ (33.3)	\$ 538.4	1,617 %	\$ 240.3	\$ 229.2	\$ 11.1	5 %

Revenues and gains from operations

Revenue

(in millions)	Three Months Ended September 30,				Nine Months Ended September 30,			
	2025	2024	Change	% Change	2025	2024	Change	% Change
Digital assets sales	\$ 28,199.0	\$ 8,464.8	\$ 19,734.2	233 %	\$ 49,613.6	\$ 26,507.7	\$ 23,105.9	87 %
Fees.....	104.3	20.7	83.6	404 %	132.8	75.4	57.4	76 %
Blockchain rewards.....	52.2	48.1	4.1	9 %	164.5	96.1	68.4	71 %
Proprietary mining	1.2	11.4	(10.3)	(90) %	13.4	47.9	(34.5)	(72) %
Revenues from contract with customers	\$ 28,356.7	\$ 8,545.0	\$ 19,811.6	232 %	\$ 49,924.3	\$ 26,727.1	\$ 23,197.2	87 %
Blockchain rewards from non-customers ⁽¹⁾	2.6	1.9	0.7	37 %	13.2	5.5	7.7	140 %
Lending	42.6	23.6	19.0	81 %	102.2	56.4	45.8	81 %
Total revenues	\$ 28,401.9	\$ 8,570.5	\$ 19,831.3	231 %	\$ 50,039.7	\$ 26,789.0	\$ 23,250.7	87 %

(1) Includes blockchain rewards earned from decentralized finance protocols and third-party staking infrastructure.

Total revenues were \$28.4 billion and \$50.0 billion, an increase of \$19.8 billion and an increase of \$23.3 billion, or 231% and 87%, respectively, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. The increase for the three months ended September 30, 2025 was primarily driven by a \$19.7 billion increase in Digital assets sales. The increase for the nine months ended September 30, 2025 was primarily driven by a \$23.1 billion increase in Digital assets sales. Galaxy recognizes revenue from transactions with customers, which include centralized trading platforms, and the corresponding Digital asset sales cost, on a gross basis because of its

role as principal in sales and purchases of digital intangible assets. The significant volume of Galaxy's digital intangible asset transactions results in significant Digital assets sales revenue with corresponding significant digital asset sales cost reflected in Transaction expenses. As a result, the magnitude of changes in Revenue on the Company's statement of operations overshadow other parts of the business, but are predominantly offset by Transaction expenses in Net income.

Digital assets sales were \$28.2 billion and \$49.6 billion, an increase of \$19.7 billion and increase of \$23.1 billion, or 233% and 87%, respectively, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. The increase for the three months ended September 30, 2025, was primarily driven by increased trade volumes resulting from a significant trade execution in the third quarter of 2025, supplemented by higher average digital asset prices in 2025. The increase for the nine months ended September 30, 2025, was also driven by the significant trade execution in the third quarter of 2025 and supplemented by higher average price of digital assets in 2025. Digital assets sales associated with external customer facing trades are reflected in the Digital Assets segment.

Sales of bitcoin, ether and tether made up 86% and 86%, versus 87% and 89%, of Digital assets sales for the three and nine months ended September 30, 2025 and three and nine months ended September 30, 2024, respectively. Approximately 52% of Digital asset sales revenue for the three months ended September 30, 2025 was comprised of the sale of bitcoin, compared to 51% of Digital assets sales revenue for the three months ended September 30, 2024. Approximately 15% of Digital asset sales revenue for the three months ended September 30, 2025 was comprised of the sale of ether, compared to 14% of Digital assets sales revenue for the three months ended September 30, 2024. Approximately 53% of Digital asset sales revenue for the nine months ended September 30, 2025 was comprised of the sale of bitcoin, compared to 58% of Digital assets sales revenue for the nine months ended September 30, 2024. Approximately 14% of Digital asset sales revenue for the nine months ended September 30, 2025 was comprised of the sale of ether, compared to 14% of Digital assets sales revenue for the nine months ended September 30, 2024.

Fee revenue was \$104.3 million and \$132.8 million, an increase of \$83.6 million and \$57.4 million, or 404% and 76%, respectively, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. For the three and nine months ended September 30, 2025, the increase was primarily attributable to the investment banking fees earned from us acting as placement agent in a private placement (the "Forward PIPE Transaction") by Forward Industries, Inc., a global design company that initiated a Solana focused treasury strategy ("Forward Industries"), as well as additional asset management fees earned during the quarter due to increased assets under management. The increase was partially offset by the cessation of mining hosting contracts at the Helios site during the first quarter of 2025 in anticipation of the data center conversion. No mining hosting revenue was generated for the three and nine months ended September 30, 2025, as compared to mining hosting revenue of \$7.0 million and \$24.9 million during the three and nine months ended September 30, 2024.

Blockchain rewards from customers were \$52.2 million and \$164.5 million, an increase of \$4.1 million and \$68.4 million, or 9% and 71% respectively, for the three and nine months ended September 30, 2025 compared to the three and nine months ended September 30, 2024. The increase was attributable to both increased assets under stake and a higher average price of digital assets during the 2025 periods. Galaxy launched proof of stake ("PoS") validation infrastructure services (reflected within the Digital Assets segment) in late 2023 to which third party and proprietary digital assets may be bonded on PoS networks to generate blockchain rewards. The delegation of staked digital assets to Galaxy-operated validation infrastructure by a number of digital asset treasury companies starting in the second quarter of 2025 contributed to the increased Blockchain rewards from customers earned in the three and nine months ended September 30, 2025 as compared to the three and nine months ended September 30, 2024. The net portion of the blockchain rewards retained by Galaxy earned on third party digital assets bonded to Galaxy validator nodes was between 5% and 10% as of September 30, 2025. Blockchain rewards generated by the Digital Assets segment on Treasury and Corporate digital assets are eliminated on consolidation within the Treasury and Corporate segment. Blockchain rewards earned from non-customers are primarily generated from participation in various decentralized finance protocols. The yield generated from these activities are primarily driven by the value of the underlying digital asset at the time of receipt and the various incentives provided by the protocols to participants.

Proprietary mining was \$1.2 million and \$13.4 million, a decrease of \$10.3 million and \$34.5 million, or 90% and 72%, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. The decrease for the three and nine months ended September 30, 2025 was attributable to the cessation of proprietary mining at the Helios site at the end of the first quarter of 2025 and to lower hash price that resulted from the halving of the bitcoin network in April 2024. Mining activities are reflected within the Treasury and Corporate segment.

Lending revenues were \$42.6 million and \$102.2 million, an increase of \$19.0 million and \$45.8 million, or 81% and 81%, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. This increase was primarily attributable to the increased size of the loan book. The average loan book size for the

three and nine months ended September 30, 2025 was \$1.8 billion and \$1.3 billion compared to \$668.1 million and \$566.1 million for the three and nine months ended September 30, 2024. Counterparty loan originations were \$493.2 million and \$2.2 billion for the three and nine months ended September 30, 2025 compared to \$825.8 million and \$1.4 billion for the three and nine months ended September 30, 2024. External lending revenue is reflected within the Digital Assets segment.

Gains / (losses) from operations

(in millions)	Three Months Ended September 30,				Nine Months Ended September 30,			
	2025	2024	Change	% Change	2025	2024	Change	% Change
Net gain / (loss) on digital assets	\$ 453.8	\$ 112.0	\$ 341.8	305.2 %	\$ 570.5	\$ 436.4	\$ 134.1	30.7 %
Net gain / (loss) on investments	297.8	13.3	\$ 284.5	2,139.1 %	360.0	(25.2)	\$ 385.2	1,528.6 %
Net gain / (loss) on derivatives trading	65.4	16.3	\$ 49.1	301.2 %	161.2	205.3	\$ (44.1)	(21.5)%
Net gain / (loss) from operations	\$ 817.0	\$ 141.6	\$ 675.4	477 %	\$ 1,091.7	\$ 616.5	\$ 475.2	77 %

Net gain / (loss) on digital assets was \$453.8 million and \$570.5 million for the three and nine months ended September 30, 2025, compared to a Net gain / (loss) on digital assets of \$112.0 million and \$436.4 million for the three and nine months ended September 30, 2024. The net gain on digital assets during the nine months ended September 30, 2025 was driven by net gains of approximately \$325.1 million on bitcoin including associated DeFi assets, net gains of approximately \$122.9 million on SOL, including associated DeFi assets as well as restricted tokens, and net gains of approximately \$116.6 million on ether including associated DeFi assets, partially offset by net losses of approximately \$57.9 million on certain restricted digital assets including TIA and SPEC and net losses of approximately \$17.2 million on digital assets receivable. The net gain on digital assets during the three months ended September 30, 2025 was primarily driven by net gains on bitcoin including associated DeFi assets of approximately \$182.6 million, net gains on ether including associated DeFi assets of approximately \$135.5 million, and net gains on SOL, including associated DeFi assets as well as restricted tokens of approximately \$100.4 million. Galaxy transacts significantly in and holds net long positions predominantly in bitcoin, which increased in value by 6% and 22%, respectively, in the three and nine months ended September 30, 2025, and in ether, which increased in value by 67% and 24%, respectively, in the three and nine months ended September 30, 2025. The net gain or loss on digital assets not measured at fair value depends on the difference in value of the underlying digital asset between the time of recognition and derecognition. Net loss on digital financial assets in the three and nine months ended September 30, 2025 was driven by decreased valuations for digital assets from Galaxy's net borrowed positions in these assets, which include certain tokenized financial instruments. Net gain / (loss) on digital assets is reflected in both the Digital Assets and Treasury and Corporate segments depending on the underlying activity.

The primary drivers for the net gains and losses on digital assets were as follows:

(in millions)	Three months ended September 30,				Nine months ended September 30,			
	2025	2024	Change	% Change	2025	2024	Change	% Change
Net gain/(loss) on digital intangible assets measured at fair value	\$ 279.4	\$ 179.1	\$ 100.4	56.1 %	\$ 127.4	\$ 316.5	\$ (189.0)	(59.7)%
Net gain/(loss) on digital intangible assets not measured at fair value ⁽¹⁾	202.8	(66.8)	269.6	403.6 %	472.6	119.8	352.8	294.5 %
Net gain/(loss) on digital financial assets measured at fair value ⁽²⁾	(28.5)	(0.3)	(28.2)	n/m	(29.5)	0.1	(29.6)	n/m
Net gain/(loss) on digital assets	\$ 453.8	\$ 112.0	\$ 341.8	305.2 %	\$ 570.5	\$ 436.4	\$ 134.1	30.7 %

(1) Includes gain on derecognition of impaired digital assets.

(2) Includes gains and losses on tokenized financial assets such as U.S. Treasuries as well as tokenized variable debt tokens.

Net gain on investments was \$297.8 million and \$360.0 million for the three and nine months ended September 30, 2025, respectively, compared to a Net gain on investments of \$13.3 million and Net loss on investments of \$25.2 million for the three and nine months ended September 30, 2024, respectively. The net gain for the three months ended September 30, 2025 was primarily attributable to net unrealized gains on Ripple Labs, Inc., Bullish Global and Bitcoin ETFs as well as realized gains on the sponsored Galaxy Digital Crypto Vol Fund, which holds Solana and AVAX, Bullish Global, and

bitcoin ETFs. The net gain for the nine months ended September 30, 2025 was primarily attributable to unrealized gains on Ripple Labs, Inc., Bullish Global, and bitcoin ETFs as well as realized gains on bitcoin ETFs, Xapo and the sponsored Galaxy Digital Crypto Vol Fund. The net gain for the three months ended September 30, 2024 was primarily attributable to realized gains earned on the distribution of bitcoin and cash from investments including Mt. Gox Investment Fund LP, partially offset by unrealized losses on short positions. The net loss for the nine months ended September 30, 2024 was primarily attributable to realized losses on short positions partially offset by realized gains on distributions of digital assets, including bitcoin, and cash received from investments including Mt. Gox Investment Fund LP and the FTX bankruptcy claims, as well as unrealized gains on the Company's investments in BTC ETFs and the sponsored Galaxy Digital Crypto Vol Fund LLC. Net gains and losses on proprietary investments are reflected in the Treasury and Corporate segment.

Net gain on derivatives trading was \$65.4 million and \$161.2 million, an increase of \$49.1 million and a decrease of \$44.1 million, or 301% and (21)%, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024, respectively. Derivatives trading gains include proprietary trading and hedging activities. The increase for the three months ended September 30, 2025 was primarily attributable to a \$53.0 million increase of realized and unrealized gains on settled and unsettled digital asset derivatives, partially offset by a decrease of \$13.0 million in realized and unrealized gains on settled and unsettled interest rate derivatives. The decrease for the nine months ended September 30, 2025 was primarily attributable to a \$52.0 million decrease of realized and unrealized gains on settled and unsettled digital asset derivatives, partially offset by a \$17.1 million increase in realized and unrealized gains on settled and unsettled foreign currency derivatives. Net gain / (loss) on derivatives is reflected in both the Digital Assets and Treasury and Corporate segments dependent on the underlying activity.

Net derivative gain represents gains / (losses) from settled derivative trades and gains / (losses) on open derivatives. It was driven by the following free-standing derivatives:

(in thousands)	Three Months Ended September 30, 2025			Nine Months Ended September 30, 2025		
	Gains / (losses) on open derivatives	Gains / (losses) from settled derivative trades	Net gain on derivatives trading	Gains / (losses) on open derivatives	Gains / (losses) from settled derivative trades	Net gain on derivatives trading
Digital assets ⁽¹⁾	\$ 14,390	\$ 54,052	\$ 68,442	\$ 97,400	\$ 30,715	\$ 128,115
Foreign currencies	(3,308)	(1,913)	(5,221)	(1,571)	20,722	19,151
Interest rates	(228)	(2,305)	(2,533)	(900)	1,397	497
Equity securities	(577)	(1,134)	(1,711)	(4,941)	8,868	3,927
Commodities	1,173	5,265	6,438	1,307	8,240	9,547
Total	\$ 11,450	\$ 53,965	\$ 65,415	\$ 91,295	\$ 69,942	\$ 161,237

- (1) Galaxy actively hedged its exposure to restricted digital assets and digital asset receivables, which contributed \$30.3 million and \$94.7 million to Net derivative gain in the three and nine months ended September 30, 2025, respectively.

(in thousands)	Three Months Ended September 30, 2024			Nine Months Ended September 30, 2024		
	Gains / (losses) on open derivatives	Gains / (losses) from settled derivative trades	Net gain on derivatives trading	Gains / (losses) on open derivatives	Gains / (losses) from settled derivative trades	Net gain on derivatives trading
Digital assets ⁽¹⁾	\$ 7,848	\$ 7,561	\$ 15,409	\$ 27,692	\$ 152,383	\$ 180,075
Foreign currencies	(5,783)	4,754	(1,029)	1,951	64	2,015
Interest rates	853	9,618	10,471	(2,765)	7,194	4,429
Equity securities	2,406	(10,874)	(8,468)	(13,605)	22,827	9,222
Commodities	684	(727)	(43)	(581)	10,142	9,561
Total	\$ 6,008	\$ 10,332	\$ 16,340	\$ 12,692	\$ 192,610	\$ 205,302

- (1) Galaxy actively hedged its exposure to restricted digital assets and digital asset receivables, which contributed \$1.1 million and \$22.3 million to Net derivative gain in the three and nine months ended September 30, 2024, respectively.

Operating expenses

Transaction expenses

(in millions)	Three Months Ended September 30,				Nine Months Ended September 30,			
	2025	2024	Change	% Change	2025	2024	Change	% Change
Digital assets sales costs	\$28,186.5	\$ 8,454.2	\$ 19,732.3	233 %	\$49,572.4	\$26,471.6	\$ 23,100.8	87 %
Blockchain reward distributions	41.7	39.3	2.3	6 %	131.5	69.5	62.0	89 %
Borrowing costs	51.5	26.6	24.9	94 %	127.1	63.3	63.8	101 %
Mining costs	0.8	10.0	(9.2)	(92)%	7.1	35.7	(28.6)	(80)%
Other transaction expenses	12.2	6.0	6.2	103 %	31.7	18.9	12.8	68 %
Transaction expenses	\$ 28,292.7	\$ 8,536.1	\$ 19,756.5	231 %	\$ 49,869.8	\$ 26,659.0	\$ 23,210.8	87 %

Digital assets sales costs were \$28.2 billion and \$49.6 billion, an increase of \$19.7 billion and \$23.1 billion, or 233% and 87%, respectively, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. This was primarily driven by increased trade volumes resulting from a significant trade execution in the third quarter of 2025, supplemented by higher average digital asset prices in 2025. Digital assets sales costs must be analyzed in conjunction with Impairment of digital assets and Net gain/(loss) on digital assets. As a percentage of Digital assets sales and Net gain/(loss) on digital assets, Digital assets sales costs and Impairment of digital assets collectively were approximately 100% for each of the three and nine months ended September 30, 2025 and 2024. Digital assets sales cost associated with external customer facing trades are reflected in the Digital Assets segment.

Blockchain reward distributions were \$41.7 million and \$131.5 million, an increase of \$2.3 million and \$62.0 million, or 6% and 89%, respectively, for the three and nine months ended September 30, 2025 compared to \$39.3 million and \$69.5 million for the three and nine months ended September 30, 2024, respectively. Galaxy launched validators in 2023 (reflected within the Digital Assets segment) to which third party and proprietary digital assets may be bonded on PoS networks to generate blockchain rewards. Blockchain reward distributions represent the staking rewards earned on third party assets staked on Galaxy validators which are passed on to the third parties, net of the fees which Galaxy charges. The delegation of staked digital assets to Galaxy-operated validation infrastructure by a number of digital asset treasury companies starting in the second quarter of 2025 contributed to the increased Blockchain rewards and associated Blockchain reward distributions in the three and nine months ended September 30, 2025 as compared to the three and nine months ended September 30, 2024. The net portion of the blockchain rewards retained by Galaxy earned on third party digital assets bonded to Galaxy validator nodes, including the CPO, was between 5% and 10% as of September 30, 2025. Blockchain reward distributions generated by the Digital Assets segment on Treasury and Corporate digital assets are eliminated on consolidation within the Treasury and Corporate segment.

Borrowing costs were \$51.5 million and \$127.1 million, an increase of \$24.9 million and \$63.8 million, or 94% and 101%, respectively, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024, primarily due to higher average borrowing volumes supporting increased operational activity.

Mining costs were \$0.8 million and \$7.1 million, a decrease of \$9.2 million and \$28.6 million, or 92% and 80%, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. The decrease is attributable to the cessation of mining hosting contracts during the first quarter of 2025 and the elimination of proprietary mining at the Helios site at the end of the first quarter of 2025 in anticipation of the data center conversion. Power costs make up the majority of mining business expense. Galaxy had hashrate under management (“HUM”) attributable to its remaining bitcoin mining machines of 0.2 exahash as of September 30, 2025 compared to HUM of 6.2 exahash as of September 30, 2024. Mining activities are reflected within the Treasury and Corporate segment.

Other transaction expenses were \$12.2 million and \$31.7 million, an increase of \$6.2 million and \$12.8 million, or 103% and 68%, for the three and nine months ended September 30, 2025, respectively, compared to the three and nine months ended September 30, 2024. Other transaction expenses include exchange, custodial and trading fees.

Impairment of digital assets was \$197.7 million and \$437.6 million, an increase of \$89.2 million and \$246.7 million, or 82% and 129%, respectively, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. This increase was primarily attributable to the mix of digital intangible assets with

which the Company transacted; specifically higher exposure to digital assets which convey enforceable rights to Galaxy over the underlying assets, such as digital assets from many decentralized finance protocols and wrapped tokens, during the three and nine months ended September 30, 2025, as compared to the same period last year, resulted in higher impairment as the associated assets typically do not qualify for fair value treatment under ASU 2023-08. Impairment of digital assets includes expense associated with digital intangible assets held at lower of cost or market that were sold during the period and those digital intangible assets still held by Galaxy at the end of the period.

Compensation and benefits were \$85.0 million and \$207.0 million, an increase of \$27.8 million and \$27.4 million, or 49% and 15%, respectively, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. The increase for the three months ended September 30, 2025 was due to an increase in headcount and an increase of the cash settled share based deferred bonus awards liability due to an increase in Galaxy's share price.

General and administrative expenses were \$58.7 million and \$164.5 million, an increase of \$34.8 million and an increase of \$98.6 million, or 146% and 150%, respectively, for the three and nine months ended September 30, 2025, compared to the three and nine months ended September 30, 2024. The increase for the three months ended September 30, 2025 was primarily driven by additional impairment of \$38.0 million on proprietary mining equipment and infrastructure. The increase for the nine months ended September 30, 2025 was primarily driven by loss on disposal and impairment of mining equipment of \$95.1 million incurred during the period. Depreciation and amortization of \$7.4 million and \$27.5 million was included in General and administrative expenses for the three and nine months ended September 30, 2025, which decreased by \$5.6 million and \$6.0 million compared to \$13.0 million and \$33.5 million for the three and nine months ended September 30, 2024 due to the lower cost basis and write-off of mining equipment and infrastructure in anticipation of the data center conversion.

Net Income/(Loss)

Galaxy generated Net income of \$505.1 million and Net income of \$240.3 million for the three and nine months ended September 30, 2025, respectively, compared to Net loss of \$33.3 million and Net income of \$229.2 million for the three and nine months ended September 30, 2024, respectively. The primary drivers of Net income for the three and nine months ended September 30, 2025 were gains on our investment and digital assets portfolios, as well as significant revenues recognized from structuring the Forward PIPE Transaction, partially offset by an increase in operating expenses, specifically from loss on disposal and impairment of our mining equipment and infrastructure. Galaxy transacts significantly in bitcoin which increased in value by 6% and 22% during the three and nine months ended September 30, 2025, respectively, and ether which increased in value by 67% and 24% during the three and nine months ended September 30, 2025, respectively. Net trading gains and gains on our net long digital assets position were the drivers of Net income during the three and nine months ended September 30, 2024.

The following table represents select financial data and a discussion of significant changes for the past eight quarters:

(in millions)	September 30, 2025	June 30, 2025	March 31, 2025	December 31, 2024	September 30, 2024	June 30, 2024	March 31, 2024	December 31, 2023
Net gain / (loss) on digital assets	\$ 453.8	\$ 134.9	\$ (18.2)	\$ 198.2	\$ 112.0	\$ (22.0)	\$ 346.4	\$ 281.2
Net gain / (loss) on investments	\$ 297.8	\$ 195.4	\$ (133.2)	\$ 284.0	\$ 13.3	\$ (101.5)	\$ 63.0	\$ 37.6
<i>Quarter over quarter fluctuation</i>								
Bitcoin	6%	30%	(12)%	48%	1%	(12)%	69%	57%
Ether	67%	36%	(45)%	28%	(24)%	(6)%	60%	37%
Cryptocurrency market capitalization	16%	24%	(18)%	51%	(4)%	(14)%	64%	53%
Bitcoin price ⁽¹⁾	\$114,056	\$107,144	\$82,549	\$93,429	\$63,329	\$62,678	\$71,334	\$42,265
Ether price ⁽¹⁾	\$4,146	\$2,486	\$1,823	\$3,333	\$2,603	\$3,433	\$3,648	\$2,281
Cryptocurrency market capitalization ⁽²⁾	\$3,993,636	\$3,429,992	\$2,766,428	\$3,393,595	\$2,250,803	\$2,332,883	\$2,702,110	\$1,647,895

(1) Represents coinmarketcap.com quoted price as of 23:59 UTC for bitcoin and ether. Presented in whole dollars.

(2) Represents market capitalization data from coinmarketcap.com through September 30, 2024 and from coingecko.com starting with the period ended December 31, 2024.

Net gain / (loss) on digital assets and investments have historically been correlated with fluctuations in the prices of bitcoin and ether as demonstrated in the table above. As Galaxy’s operating businesses in the Digital Assets and Data Center segments mature, digital asset prices are anticipated to have a proportionally less significant impact on Net income in the future.

Components of Financial Position

The following represents selected financial data and a discussion of significant changes.

(in millions)	As of		Change	% Change
	September 30, 2025	December 31, 2024		
Digital intangible assets ⁽¹⁾	\$ 3,841.6	\$ 2,568.6	\$ 1,273.0	50 %
Digital financial assets	322.9	359.7	(36.8)	(10) %
Digital assets loans receivable	1,299.7	579.5	720.2	124 %
Assets posted as collateral — digital assets	712.8	277.1	435.7	157 %
Digital assets receivable ⁽¹⁾	21.4	60.7	(39.3)	(65) %
Digital assets subtotal	6,198.4	3,845.6	\$ 2,352.8	61 %
Digital assets borrowed ⁽¹⁾	3,064.8	1,497.6	1,567.2	105 %
Collateral payable — digital assets	2,525.0	1,324.7	1,200.3	91 %
Digital asset liabilities subtotal	5,589.8	2,822.3	\$ 2,767.5	98 %
Investments ⁽¹⁾	2,106.2	1,643.5	462.7	28 %
Property and equipment	874.1	237.0	637.1	269 %
Total assets	\$ 11,522.7	\$ 7,119.9	\$ 4,402.8	62 %
Total liabilities	\$ 8,350.4	\$ 4,925.5	\$ 3,424.9	70 %

⁽¹⁾ Includes current and non-current portion.

As of September 30, 2025, our digital asset balances were \$6.2 billion, an increase of \$2.4 billion from December 31, 2024. This increase was driven by a significant increase in Digital assets borrowed to support increased operations, an increase in digital asset collateral payable due to the increased size of our loan portfolio, as well as increases in digital asset prices. These same drivers also drove the increase of \$2.8 billion in our digital assets liabilities balances which totaled \$5.6 billion as of September 30, 2025. The Company’s largest digital asset holding as of both September 30, 2025 and December 31, 2024 was bitcoin. During the nine months ended September 30, 2025, the price of bitcoin increased by 22%.

Investments increased \$462.7 million during the nine months to \$2.1 billion as of September 30, 2025. This increase was primarily due to investments in Forward Industries, as well as unrealized gains of \$156.7 million on investments still held at September 30, 2025. As of September 30, 2025, Galaxy’s largest investments were bitcoin and ether spot ETF investments of \$640.8 million, limited partner interests in Galaxy-sponsored funds totaling \$359.6 million, Forward Industries of \$255.6 million, and Ripple Labs, Inc. of \$170.8 million. As of December 31, 2024, Galaxy’s largest investments were bitcoin and ether spot ETF investments of \$669.2 million and limited partner interests in Galaxy-sponsored funds totaling \$398.4 million.

Property and equipment increased \$637.1 million during the nine months to \$874.1 million as of September 30, 2025. The increase was primarily due to investment in AI/HPC infrastructure to build out our data center hosting facility at Helios in West Texas, partially offset by an \$87.3 million impairment of mining equipment and related infrastructure and \$12.3 million of disposals of mining equipment net carrying value associated with the data center conversion of our Helios campus. We capitalize costs, including direct labor and materials, associated with the development and construction of our AI/HPC data center infrastructure while the assets are being prepared for their intended use.

Total assets increased by \$4.4 billion during the nine months to \$11.5 billion as of September 30, 2025, primarily due to the \$637.0 million increase in Property and equipment and \$2.4 billion increase in digital assets balances described above.

Total liabilities increased by \$3.4 billion during the nine months to \$8.4 billion as of September 30, 2025, primarily due to the \$1.6 billion and \$1.2 billion increase in digital assets borrowed and digital asset collateral payable, respectively, as described above.

Liquidity and Capital Resources

We held \$1.1 billion in cash and cash equivalents as of September 30, 2025, an increase of \$675.3 million, or 146.1%, as compared to December 31, 2024. The following table provides a breakdown of the Company's cash and cash equivalents balances by location:

(in millions)	September 30, 2025	December 31, 2024
Digital asset trading platforms	154.6	64.7
Other financial institutions ⁽¹⁾	982.8	397.4
Total	\$ 1,137.4	\$ 462.1

(1) Includes banks, other trading platforms, and broker-dealers

Working capital (current assets less current liabilities) was \$2.3 billion and Total equity was \$3.2 billion as of September 30, 2025, compared to working capital of \$2.0 billion and Total equity of \$2.2 billion as of December 31, 2024. As of September 30, 2025 and December 31, 2024, we held total gross digital assets with a carrying value of \$4.2 billion and \$2.9 billion, respectively.

On August 15, 2025, Galaxy Helios I LLC entered into the Credit Agreement with Deutsche Bank AG providing for a senior secured term loan facility in an aggregate principal amount of up to \$1.4 billion. The intended use for this facility is to finance the construction and development of a data center project in Dickens County, Texas and related costs. As of September 30, 2025, the outstanding amount drawn under the Credit Agreement was \$433.5 million, which is recognized within Notes payable in the Company's condensed consolidated interim statements of financial position. See Note 18 of the Company's consolidated financial statements included elsewhere in this Quarterly Report on Form 10-Q for additional information on the Credit Agreement.

In June 2025, the Company and certain selling stockholders sold 35,980,967 shares of Class A common stock in an underwritten public offering, of which 26,400,000 shares were offered by the Company and the remaining sold by the selling stockholders (including pursuant to the underwriter's option to purchase additional shares), at an offering price of \$19.00 per share. Net proceeds to the Company from the offering were approximately \$477.8 million after deducting underwriting discounts and offering costs. We are utilizing the net proceeds from this offering to finance the continued expansion of our AI/HPC infrastructure at the Helios data center campus and general corporate purposes.

In November 2024, Galaxy issued \$402.5 million of 2.500% Exchangeable Senior Notes due 2029. From time to time and subject to the terms of the indenture governing the 2029 Exchangeable Notes, the 2029 Exchangeable Notes are exchangeable for shares of Class A common stock. We are utilizing the net proceeds from the offering to support the build-out of high-performance computing infrastructure at our Helios data center in West Texas and for general corporate purposes. See Note 18 of the Company's condensed consolidated interim financial statements included elsewhere in this Quarterly Report on Form 10-Q for additional information on the 2029 Exchangeable Notes.

In April 2024, Galaxy raised C\$169.4 million from a syndicate of underwriters, led by Canaccord Genuity Corp. Galaxy issued 12,100,000 ordinary shares pursuant to the transaction. We are utilizing the net proceeds for working capital and general corporate purposes.

In the general course of business, we make commitments to invest in our managed funds and to purchase equipment. As we grow our business, we expect our operating expenses to increase. In addition, we make investments in early-stage companies and coin networks in the digital assets space. Individual investments tend to be small but in the aggregate, these investments can constrain our liquidity. We consider our liquidity position and projected liquidity needs when committing to new investments.

From time to time we receive cash inflows from our investments via strategic disposal and redemptions, as well as via distributions. On a net cash basis, we expect to continue to make investments in our sectors as we find compelling opportunities, balanced by conservatively managing our liquidity.

The \$978 million increase in Total equity during the nine months ended September 30, 2025 was primarily due to our public offering of shares in June 2025 and the impact of the Reorganization Transactions, as well as Net income during the period of \$240 million.

(in thousands)	September 30, 2025	December 31, 2024
Total assets	\$ 11,522,716	\$ 7,119,855
Total liabilities	\$ 8,350,397	\$ 4,925,503
Total equity	3,172,319	2,194,352

As of September 30, 2025 and through the date of this filing, we have not experienced any difficulties meeting counterparty requests to return loans or collateral.

To meet our estimated capital expenditure requirements related to the conversion of the existing bitcoin mining infrastructure at our Helios campus to AI/HPC data center infrastructure, we will need to obtain additional debt, equity and/or equity-linked financing. The final terms and availability of any such financing will depend on various factors, including market conditions at the time. Beyond the Helios campus conversion, we believe that our existing cash and cash equivalents and cash flows from operations will be sufficient to support working capital requirements for at least the next 12 months. We expect these sources will be sufficient to fund our long-term contractual obligations and capital needs. However, this is subject, to a certain extent, to general economic, financial, competitive, regulatory, and factors that are beyond our control. See “Risk Factors—Risks Related to our Operations—Our expansion into the AI/HPC data center business will require substantial additional capital. We may be unable to obtain additional financing for this or for other areas of business development on acceptable terms or at all” in this Quarterly Report on Form 10-Q. In the event there is insufficient working capital to support the growth of the business, we may sell digital assets to generate cash to meet obligations as they come due, or may exit all or a portion of an investment if an exit price is advantageous to us. We may also seek additional sources of financing in the future, including but not limited to, issuing equity, convertible notes or a debt facility.

Refer to Note 17 of Galaxy’s consolidated financial statements included in this Quarterly Report on Form 10-Q for further information on commitments and contingencies and Note 15 of Galaxy’s consolidated financial statements for further information on the Company’s lease obligations. A table summarizing our contractual obligations is included in “Contractual Obligations” below. As of September 30, 2025 and December 31, 2024, we did not have any other off-balance sheet arrangements that have, or are reasonably likely to have, a current or future effect on our results of operations or financial position.

Cash Flows

(in thousands)	For the Nine Months Ended	
	September 30, 2025	September 30, 2024
Net cash provided by (used in) operating activities	756,948	172,735
Net cash provided by (used in) investing activities	(710,469)	(457,566)
Net cash provided by (used in) financing activities	628,844	240,198

Nine Months Ended September 30, 2025

Cash and cash equivalents for the nine months ended September 30, 2025 increased from \$462.1 million to \$1.1 billion. The Company utilized \$710.5 million for its investing activities, which was primarily due to purchases of investments of \$2.5 billion and purchases of property, equipment and intangible assets of \$634.5 million partially offset by proceeds and distributions from investments of \$2.6 billion. Net cash provided by financing activities was \$628.8 million primarily due to \$522.5 million, net of costs, from share issuances and \$416.2 million of proceeds from Notes payable, net of issuance costs, partially offset by \$178.4 million net cash used for margin loans payable. Operating activities provided an additional \$756.9 million.

Nine Months Ended September 30, 2024

Cash and cash equivalents during the nine months ended September 30, 2024 decreased from \$316.6 million to \$272.0 million. The Company used \$457.6 million for its investing activities, which was primarily due to purchases of investments of \$2.8 billion partially offset by proceeds and distributions from investments of \$2.4 billion. Net cash provided by financing activities was \$240.2 million primarily due to \$122.6 million, net of costs, from share issuances and \$391.8 million of proceeds from loans payable partially offset by \$236.0 million repayment of loans payable. Operating activities provided an additional \$172.7 million.

Contractual Obligations

The following table presents a summary of our contractual obligations as of September 30, 2025:

(in thousands)	Payments Due by Period				
	Total	Less than 1 year	1 - 3 years	4 - 5 years	After 5 years
Loans and collateral payable ⁽¹⁾	\$ 5,928,857	\$ 5,919,277	\$ 9,580	\$ —	\$ —
Lease obligations	14,524	1,427	8,719	4,378	—
Notes payable	1,288,254	440,754	445,000	402,500	—
Data center commitments	908,089	908,089	—	—	—
Legal settlement	160,000	40,000	120,000	—	—
Other obligations ⁽²⁾	137,333	2,081	135,252	—	—
Total Contractual Obligations	\$ 8,437,057	\$ 7,311,628	\$ 718,551	\$ 406,878	\$ —

⁽¹⁾ Includes fiat and digital asset payables. Loans and collateral with terms of less than one year and those without a prespecified maturity date are included in the Less than 1 year category. However, these balances are generally extended and rolled into new loans and/or collateral.

⁽²⁾ Includes obligations to fund capital commitments to seven portfolio companies. Excludes other liabilities related to goods and services required in the ordinary course of business.

Item 3. Quantitative and Qualitative Disclosures About Market Risk

Market risk is the risk associated with changes in the market value of assets and liabilities resulting from broad market movements, such as changes in the general level of interest rates, equity prices, foreign exchange rates, and commodity prices. The Company's material market risks are outlined below.

Digital Asset Price Risk

We have invested a significant portion of our capital in digital assets. This includes Digital intangible assets, Digital financial assets, Digital assets loan receivable, net of allowance, Assets posted as collateral, Digital assets receivable, and Derivative assets. Offsetting our digital assets balances, we have digital asset related liabilities including Collateral payable, Digital assets borrowed, and Derivative liabilities. As discussed in Note 2 to our consolidated financial statements included elsewhere in this Quarterly Report on Form 10-Q, while the majority of our digital assets are measured at fair value starting from January 1, 2023, we continue to account for a material portion of our digital assets as indefinite-lived intangible assets, which are subject to impairment losses if the fair values of our digital assets decrease below their carrying values at any time since their acquisition. Our digital assets related liabilities are accounted for using the fair value of the underlying digital assets, and are sensitive to changes in market prices.

Management's estimate of the effect of digital asset price risk on our Treasury and Corporate digital asset portfolio due to a +/- 20% change in the market prices of digital assets, with all other variables held constant, was +/- \$260.9 million and \$247.3 million as of September 30, 2025 and December 31, 2024, respectively.

Equity Price Risk

Equity price risk is the risk that the value of equity interests in private or public entities will fluctuate as a result of changes in equity prices (other than those arising from interest rate risk or foreign currency risk), whether caused by factors specific to an individual investment, its issuer, or all factors affecting all instruments traded in a market or market segment. All investments present a risk of loss of capital. The maximum risk resulting from financial instruments is equivalent to their fair value. Our investments are susceptible to other market risk arising from uncertainties about future prices of the

instruments. We moderate this risk through the various investment strategies within the parameters of our investment guidelines.

Management’s estimate of the effect of equity price risk on investments due to a +/- 20% change in the market prices of our investments and investments sold short, with all other variables held constant, was +/- \$378.5 million and \$327.4 million as of September 30, 2025 and December 31, 2024, respectively.

Credit and Counterparty Risk

Our cash and cash equivalents, digital assets, derivatives, receivables (including digital assets receivables) and loans receivable (including digital asset loans receivable) are exposed to credit and counterparty risk. There are two main activities or processes in which we participate which give rise to credit and counterparty risk: lending and posting risk margin with trading platforms.

Galaxy transacts in digital assets with third parties for lending, borrowing, and derivative trading purposes. These activities expose Galaxy to credit and counterparty risk. We mitigate this risk by requiring counterparties to provide collateral assets. Collateral that we accept is assessed based on its liquidity, volatility, correlation to the counterparty, and overall risk profile at the time of the transaction. Collateral accepted for digital asset loans is typically other denominations of digital assets or U.S. dollars. We only accept digital assets as collateral which are internally approved for trading. However, permissible collateral does not include all digital assets that are approved for trading. On termination of the loan, the borrower is required to return the digital assets to us, and any gains or loss in the market price during the loan would inure to us. In the event of a bankruptcy of the borrower, we could experience delays in recovering our digital assets. In addition, to the extent that the value of the digital assets increases during the term of the loan, the value of the digital assets may exceed the value of collateral provided to us, exposing us to credit risks with respect to the borrower and potentially exposing us to a loss of the difference between the value of the digital assets and the value of the collateral. If a counterparty defaults under its obligations with respect to a loan of digital assets or an open derivative position, including by failing to deliver additional collateral when required or by failing to return the digital assets upon the termination of the loan or settlement of the derivative, we may expend significant resources and incur significant expenses in connection with efforts to enforce the relevant agreement, which may ultimately be unsuccessful.

Galaxy participates in DeFi protocols as part of its operations. DeFi is built on smart contracts that facilitate transactions without traditional intermediaries. The counterparty risk is elevated in decentralized finance environments due to the pseudonymous nature of blockchain transactions. Furthermore, the collateralization mechanisms in DeFi, often involving volatile digital assets, can lead to liquidity issues, especially in market downturns. The lack of a central authority or regulated framework to enforce contractual obligations or provide depositor insurance also increases our risk, as we have limited recourse in the event of defaults or platform failures. Additionally, smart contract risks, such as code vulnerabilities or execution failures, can result in significant financial losses. We have implemented monitoring procedures to both identify potentially malicious counterparties and minimize our exposure to any individual decentralized protocol.

We post risk margin in the form of digital assets and U.S. dollars with digital asset trading platforms to participate in activities within the trading platform. The posting of risk margin is required to utilize leverage for spot, futures and derivative trading with regards to digital assets. Certain trading platforms will accept digital assets as collateral while other venues will only accept U.S. Dollars.

Below is a list of digital asset trading platforms, including their location and type of collateral posted, where Galaxy posted more than a de minimis amount of risk margin as of September 30, 2025:

Entity	Entity Type	Entity Domicile	Collateral Type
Binance	Digital asset trading platform	Cayman Islands	Digital assets
Maple	Digital asset trading platform	Australia	Digital assets
Fidelity	Digital asset trading platform	United States	Digital assets
Coinbase	Digital asset trading platform	United States	Digital assets

As of September 30, 2025, the total amount of digital assets on the digital asset trading platforms listed above was \$1.1 billion, of which \$374.3 million was held at Binance, \$307.3 million was held at Maple, \$214.4 million was held at Fidelity, and \$172.3 million was held at Coinbase.

In addition to the above, Galaxy maintained past relationships with Bakkt, Bitfinex, Bitmex, Bitstamp, Blockchain (PITX), Bybit, Huobi, Kraken, LMAX, OKX and Wootrade, all of which are digital asset trading platforms. Galaxy may re-engage with the foregoing digital asset trading platforms or other trading platforms at some point in the future. Galaxy

also, in the regular course of business, posts margin at financial institutions and other trading platforms outside of digital asset trading platforms.

Some of these digital asset trading and digital asset derivatives platforms (collectively referred to in this Quarterly Report on Form 10-Q as “digital asset trading platforms”) are unregulated and are not subject to regulatory oversight. Furthermore, certain digital asset trading platforms engage in the practice of commingling their clients’ assets in omnibus platform wallets. When digital assets are commingled, transactions are not recorded on the applicable blockchain ledger but are only recorded by the digital asset trading platform. Therefore, there is risk around the occurrence of transactions or the existence of period end balances held at these digital asset trading platforms, and digital assets held at such digital asset trading platforms are subject to the risk of loss in the event of a bankruptcy, liquidation or similar event involving the trading platform.

We limit our credit risk by placing our cash and digital assets with financial institutions and trading platforms on which we have performed internal due diligence procedures. Our due diligence procedures around trading platforms include, but are not limited to, internal control procedures around on-boarding new platforms which includes review of their anti-money laundering (“AML”) and know-your-client (“KYC”) policies by our Chief Compliance Officer (centralized platform specific); obtaining a security report by an independent third-party, if available; regular review of market information specifically regarding the trading platforms’ security and solvency risk, including reviewing wallets that interact with decentralized platforms (decentralized platform specific); setting balance limits for each platform account based on risk exposure thresholds and preparing daily asset management reports to ensure limits are being followed; and having a fail-over plan to move cash and digital assets held on a platform in instances where risk exposure significantly changes.

While we intend to only transact with counterparties or platforms that we believe to be creditworthy, there can be no assurance that a counterparty will not default and that we will not sustain a material loss on a transaction as a result.

Item 4. Controls and Procedures

Our disclosure controls and procedures are designed to ensure that information we are required to disclose in reports that we file or submit under the Exchange Act, is recorded, processed, summarized, and reported within the time periods specified in SEC rules and forms, and that such information is accumulated and communicated to our management, including our CEO and Chief Financial Officer (“CFO”), as appropriate, to allow timely decisions regarding required disclosure.

Our management, with the participation and supervision of our CEO (our principal executive officer) and our CFO (our principal financial officer), has evaluated the effectiveness of our disclosure controls and procedures (as defined in Rules 13a-15(e) and 15d-15(e) under the Exchange Act) as of September 30, 2025. Based on such evaluation, our CEO and CFO have concluded that as of September 30, 2025, our disclosure controls and procedures were, in design and operation, effective at a reasonable assurance level.

Changes in Internal Control over Financial Reporting

There were no changes in our internal control over financial reporting (as such term is defined in Rules 13a-15(f) and 15d-15(f) of the Exchange Act) during the most recent fiscal quarter that have materially affected, or are reasonably likely to materially affect, our internal control over financial reporting.

PART II - OTHER INFORMATION

Item 1. Legal Proceedings

In the ordinary course of business, the Company and its subsidiaries and affiliates may be threatened with, named as defendants in, or made parties to pending and potential legal actions, including class actions, arbitrations and other disputes. The Company and its subsidiaries and affiliates are also subject to oversight by numerous regulatory and other governmental agencies and may receive inspection requests, investigative subpoenas and requests from regulators for documents and information, which could lead to enforcement investigations and actions.

The Company reviews any lawsuits, regulatory investigations, and other legal proceedings on an ongoing basis and provides disclosure and records loss contingencies in accordance with its accounting policies. Except as discussed below, the Company does not believe that the ultimate resolution of existing legal and regulatory outstanding matters will have a material effect upon our financial condition or liquidity. However, in light of the uncertainties inherent in these matters, it is possible that the ultimate resolution of one or more of these matters may have a material adverse effect on the Company's results of operations for a particular period, and future changes in circumstances or additional information could result in additional accruals or resolution in excess of established accruals, which could adversely affect the Company's results of operations, potentially materially.

Luna matters: On March 27, 2025, Galaxy reached an agreement with the New York State Attorney General to resolve civil claims related to certain investments, trading, and public statements made in connection with the LUNA digital asset from late 2020 to 2022. As of September 30, 2025 and December 31, 2024, the Company had accrued a legal provision of \$149 million and \$182 million, respectively. The accrued amounts include the impact of discounting the estimated cash flows at a rate of approximately 4.3%. The undiscounted settlement was \$200 million and payable between 2025 and 2028, with a payment of \$40 million in each of 2025 and 2026, and a payment of \$60 million in each of 2027 and 2028. Under the terms of the settlement, Galaxy also agreed to, among other things, compliance enhancements related to public statements about cryptocurrency and purchases and sales of cryptocurrency.

In December 2022, a proposed class action was filed in the Ontario Superior Court of Justice against GDH Ltd., our Chief Executive Officer and our former Chief Financial Officer asserting various claims including alleged misrepresentations relating to our public disclosure regarding investments and trading in the LUNA digital asset. The class action purports to be brought on behalf of a proposed class of persons and entities who acquired our securities on the secondary market from May 17, 2021 to and including May 6, 2022. The class action seeks unspecified damages and various declaratory relief, including leave to proceed with the right of action for misrepresentation under statutory securities provisions. These proceedings are still in early stages and have not been certified to proceed as a class action. The plaintiff's motion for leave and certification is scheduled to be heard in April 2026. Based on the stage of the case, the outcome remains uncertain, and the Company cannot estimate the potential impact, if any, on its business or financial statements at this time.

See "Item 1A. Risk Factors—Risks Related to our Operations—We or our subsidiaries and affiliates are and may continue to be subject to substantial litigation, including individual and class action lawsuits, and regulatory risks" for additional information about the risks related to the Luna matters.

Item 1A. Risk Factors

Investing in our Class A common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below, together with all of the other information in this Quarterly Report on Form 10-Q, including the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations" and the condensed consolidated financial statements and related notes. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of or that we deem immaterial may also become important factors that adversely affect our business. If any of the following risks occur, our business, operating results, financial condition, and future prospects could be materially and adversely affected. Many risks affect more than one category, and the risks are not in order of significance or probability of occurrence because they have been grouped by categories. The market price of our Class A common stock could decline, and you could lose part or all of your investment due to any of these risks. Some statements in this Quarterly Report on Form 10-Q, including statements in the following risk factors, constitute forward-looking statements. See the section titled "Special Note Regarding Forward-Looking Statements."

Summary Risk Factors

Below is a summary of the principal factors that make an investment in our Class A common stock risky. This summary does not address all of the risks that we face. Additional discussion of the risks summarized here, and other risks that we face, can be found following this summary and should be carefully considered, together with other information in this Quarterly Report on Form 10-Q, before making investment decisions regarding our Class A common stock:

- We have limited operating history. Our business lines are nascent, unproven and subject to material legal, regulatory, operational, reputational, tax and other risks in every jurisdiction and are not assured to be profitable.
- Our operating results have and will significantly fluctuate due to a variety of factors, including the highly volatile nature of cryptocurrency.
- A determination that a digital asset is a “security,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could adversely affect the value of that digital asset and potentially digital assets generally, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock.
- A determination that a digital asset is a “security,” or a “security-based swap,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could have adverse regulatory consequences for us, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock.
- Our process for analyzing whether or not a particular digital asset is a security for purposes of the federal securities laws may not yield results that are consistent with subsequent determinations by the SEC or federal courts, or with similar determinations made by our competitors.
- We are highly dependent on our key personnel, including our Founder, which exposes stockholders to material and unpredictable “key man” risk.
- If we fail to develop, maintain and enhance our brand and reputation, our business operating results and financial condition may be adversely affected.
- We operate in highly competitive industries; and we compete against unregulated or less regulated companies and companies with greater financial and other resources; and our business, operating results, and financial condition may be adversely affected if we are unable to respond to our competitors effectively.
- We or our subsidiaries and affiliates are and may continue to be subject to substantial litigation, including individual and class action lawsuits, and regulatory risks.
- Our business relies on third-party service providers and subjects us to risks that we may not be able to control or remediate.
- Because our long-term success depends, in part, on our ability to expand our sales to customers outside the United States, our business is susceptible to risks associated with international operations.
- Managing different business lines could present conflicts of interest.
- Our strategy to expand into the AI/HPC data center business may not be successful and may result in adverse consequences to our business, financial condition and results of operations.
- Our AI/HPC data center business model is predicated, in part, on establishing and maintaining a customer base that will generate a recurring stream of revenues. If that recurring stream of revenues is not maintained or does not increase as expected, our operating results may be adversely affected.
- We are subject to risks in connection with our mining business and AI/HPC data center business, including risks associated with counterparties.
- Digital assets represent a new and rapidly evolving industry, and the market price of our Class A common stock has in the past and may in the future be impacted by the acceptance of bitcoin and other digital assets.
- Our and our third-party service providers’ failure to safeguard and manage our and our customers’ funds and digital assets could adversely impact our business, operating results and financial condition.

- Legislative or regulatory changes or actions by the U.S. Congress or any U.S. federal or state agencies could restrict the use of one or more digital assets, the ability to enter into transactions referencing digital assets, validating or mining activity, the operation of digital asset networks or digital asset trading platforms in a manner that adversely affects our business.
- Cybersecurity incidents and other issues related to our information systems, technology and data may materially and adversely affect us.
- Any failure to obtain, maintain, protect, defend or enforce our intellectual property and other proprietary rights could adversely affect our business, financial condition and results of operations.
- GDI's principal asset is its direct ownership interest in GDH LP. GDI is accordingly dependent upon distributions from GDH LP to pay dividends, if any, and taxes, make payments under the Tax Receivable Agreement and pay other expenses.
- Our Founder controls a significant portion of our voting power and his interests may be different from those of stockholders and may prevent new investors from influencing significant corporate decisions, including mergers, consolidations, or the sale of us or all or substantially all of our assets.
- The market price and trading volume of our Class A common stock may be volatile, which may affect the value of an investment in our Class A common stock and could subject us to litigation.
- Substantial future sales of shares of our Class A common stock in the public market could cause the market price of our Class A common stock to fall.
- The tokenization of our Class A common stock may introduce risks and uncertainties that adversely affect the market for, and the trading price of, our Class A common stock, among other potential consequences.
- We face challenges, increased costs and administrative responsibilities as a newly listed U.S. company, and management devotes substantial time to related compliance initiatives.
- Our management team has limited experience managing a U.S. public company and some members of senior management are new to our company and our industry. Our business could be adversely affected if our management team is not successfully integrated or does not execute our business plan and developmental strategies.

Risks Related to Our Operations

We have limited operating history. Our business lines are nascent, unproven and subject to material legal, regulatory, operational, reputational, tax and other risks in every jurisdiction and are not assured to be profitable.

We and our subsidiaries have limited operating history on which an investor might evaluate our performance. We began operations in 2018, and publicly introduced new products and services, including buying and selling of select cryptocurrencies (our “trading” business), managing capital on behalf of third parties (our “asset management” services), our financial, investment and strategic financial services (our “investment banking” services), our balance sheet venture investments portfolio (managed by our “crypto ventures” team), our suite of products and services related to bitcoin mining (our “mining” services) in 2020, our self-custody technology business in 2023, our validator services business in 2024 and our GalaxyOne platform in 2025. As a result, we are subject to many of the risks common to early-stage enterprises, including under-capitalization, cash shortages, limitations with respect to personnel, financial and other resources and lack of revenues, any of which could have a material adverse effect on us and may force us to reduce or curtail operations. Due to our limited operating history, our business model has not been fully proven and we have limited financial data that can be used to evaluate our current business and future prospects, which subjects us to a number of uncertainties, including our ability to plan for, model and manage future growth and risks. Our historical revenue growth should not be considered indicative of our future performance. There is no assurance that we will be successful in achieving a return on stockholders’ investment and the likelihood of success must be considered in light of the early stage of operations. Even if we accomplish these objectives, we may not generate the anticipated positive cash flows or profits. No assurance can be given that we will ever be successful in our operations and operate profitably.

Furthermore, our business lines are nascent, unproven and subject to material legal, regulatory, operational, reputational, tax and other risks in every jurisdiction and are not assured to be profitable. We may fail to be able to implement our investment or trading strategies, achieve our investment objectives, effectively operate our digital asset

mining sites, develop our business lines or produce a return for our investors. We have chosen to pursue a number of different businesses in this evolving industry. It is possible that some of these businesses may be difficult to enter and/or it may become evident that a particular business is not a productive use of capital or time. In particular, it is possible that existing laws and regulations (as interpreted going forward), and newly-enacted laws and regulations that have not yet become effective or been proposed, could make it impractical or impossible for us to enter into new business lines and may require us to stop engaging in certain business activities that we already perform that may currently be profitable. These difficulties and legal restrictions could lead us to modify our businesses and focus. In particular, we may become involved in investments and projects that are not directly related to the digital asset or blockchain industry. These projects are likely to relate to industries and clients that we believe will benefit in the future from blockchain technology and our experience and network in the digital assets industry.

From time to time, we may also launch new lines of business, offer new products and services within existing lines of business or undertake other strategic projects. For example, we are currently in the process of converting the infrastructure at our Helios mining campus to AI/HPC data center infrastructure and operations. While we have experience in providing computing power, we have no experience in developing, retrofitting and offering AI/HPC data centers, and there can be no assurance that these or any other modifications to our business model and strategy will be successful or will not result in harm to our business. See “—Risks Related to Our Business Lines—Our strategy to expand into the AI/HPC data center business may not be successful and may result in adverse consequences to our business, financial condition and results of operations” for more information on the risks relating to our transition to the AI/HPC business. There are substantial risks and uncertainties associated with these efforts and we expect to invest significant capital and resources in such efforts. Regulatory requirements can affect whether initiatives are able to be brought to market at all and, even if so, in a manner that is timely and attractive to our customers. Initial timetables for the development and introduction of new lines of business, products or services and price and profitability targets may not be met. Furthermore, our revenues and costs may fluctuate due to start-up costs associated with new businesses or products and services (including for legal or regulatory reasons) while revenues may take time to develop, which may adversely impact our results of operations. If we are unable to successfully manage our business while reducing expenses, our ability to continue in business could depend on our ability to raise sufficient additional capital, obtain sufficient financing and/or monetizing assets. The occurrence of any of the foregoing risks would have a material adverse effect on our financial results, business and prospects.

Our operating results have and will significantly fluctuate due to a variety of factors, including the highly volatile nature of cryptocurrency.

Our leading sources of revenue are dependent on digital assets and the broader cryptoeconomy. Our operating results have and will significantly fluctuate due to a variety of factors, including the highly volatile nature of cryptocurrency. Significant positive or negative changes in cryptocurrency asset prices (whether individually or in the aggregate) will not necessarily result in similar benefit or impairment to our operating results and financial condition. For example, the cumulative market capitalization of cryptocurrencies decreased approximately 57% during the three months ended June 30, 2022, while the value of GDH LP limited partners’ capital decreased 23% during the same period. Our operating results will continue to fluctuate significantly as a result of a variety of factors, many of which are unpredictable and in certain instances are outside of our control, including:

- our dependence on offerings that are dependent on digital asset trading activity, including trading volume and the prevailing trading prices for digital assets, whose trading prices and volume can be highly volatile;
- our ability to attract, maintain, and grow our customer base and engage our customers;
- changes in the legislative or regulatory environment, or actions by governments or regulators, including fines, orders, or consent decrees;
- legislative or regulatory changes that impact our ability to offer certain products or services;
- the impact of environmental, social and governance concerns surrounding digital assets;
- pricing for our products and services;
- investments we make in the development of products and services as well as technology offered to our ecosystem partners, international expansion, and sales and marketing;
- our ability to utilize, utilization of and dependence on centralized digital asset trading platforms and OTC markets that are approved primarily based on our diligence review;
- macroeconomic conditions, including decreased trading in global markets or decreased demand for financial services products generally;

- disputes with our customers or regulators, adverse legal proceedings or regulatory enforcement actions, judgments, settlements, or other legal proceeding and enforcement-related costs;
- the development and introduction of existing and new products and services by us or our competitors;
- increases in operating expenses that we expect to incur to grow and expand our operations and to remain competitive;
- the timing and amount of noncash expenses, such as stock-based compensation and asset impairment;
- system failure or outages, including with respect to third-party cryptocurrency networks, decentralized finance protocols, breaches of security or privacy or any inaccessibility of the third-party cryptocurrency networks or decentralized finance protocols due to our or third-party actions;
- changes in the overall tax rate for our business, changes in tax laws or judicial or regulatory interpretations of tax laws;
- changes in accounting standards, policies, guidance and interpretations or principles;
- changes in requirements imposed on us by regulators or by our counterparties, including net capital requirements imposed by the SEC and the Financial Industry Regulatory Authority (“FINRA”) on our broker-dealers;
- our ability to attract and retain talent;
- our ability to compete with our competitors; and
- general economic conditions in either domestic or international markets, including the impact of pandemics, global economic slowdowns, domestic and foreign regulatory uncertainty, changes in trade policies, including the imposition of tariffs, trade controls and other trade barriers, actual or perceived global banking and finance related issues, increased risk of inflation, potential uncertainty with respect to the federal debt ceiling and budget and potential or actual government shutdowns, related thereto, interest rate volatility, and potential global recession.

As a result of these factors, it is difficult for us to forecast growth trends accurately and our business and future prospects are difficult to evaluate, particularly in the short term. In light of the rapidly evolving nature of our business and the cryptoeconomy, period-to-period comparisons of our operating results may not be meaningful, and you should not rely upon them as an indication of future performance. Quarterly and annual expenses reflected in our financial statements may be significantly different from historical or projected rates. Our operating results in one or more future quarters may fall below the expectations of securities analysts and investors. As a result, the market price of our Class A common stock may increase or decrease significantly.

Our operating results are dependent on the prices of digital assets and volume of transactions that we conduct. If such price or volume declines, our business, operating results, and financial condition would be adversely affected.

Any declines in the volume of digital asset transactions, the price of digital assets, or market liquidity for digital assets generally may adversely affect our operating results. We have significant investments in digital assets. As of September 30, 2025, we held digital intangible assets of \$3.8 billion, digital financial assets of \$322.9 million, and bitcoin and ether spot ETF investments of \$640.8 million. Changes in the value of digital assets will generally have a significant impact on our results. Our operating results will be impacted by the revenues and profits we generate from the purchase, sale, and trading of digital assets and financial contracts linked to digital assets. The price of digital assets and associated demand for buying, selling, and trading of digital assets have historically been subject to significant volatility. For instance, in 2017 and 2021, the value of certain digital assets, including bitcoin, experienced steep increases in value, followed by steep declines in 2018 and 2022. After recovering from the 2018 decline and reaching record highs in December 2021, the value of the total crypto market cap declined by approximately 64% in the twelve months ended December 31, 2022. The collapse of several companies in the digital asset industry such as Celsius, Voyager and FTX impacted digital assets prices in 2022 and the majority of 2023. We believe that the approval and launch of spot-based Bitcoin ETFs in the U.S. in the first quarter of 2024 and the election of President Donald Trump in the fourth quarter of 2024 drove up the crypto market cap again in 2024, but the crypto market generally declined in the first quarter of 2025 before increasing again in the second quarter of 2025. The price and trading volume of any digital asset is subject to significant uncertainty and volatility, and may significantly decline in the future, without recovery. Such uncertainty and volatility depend on a number of factors, including:

- market conditions across the cryptoeconomy;
- changes in liquidity, volume, and trading activities;

- trading activities on digital asset trading platforms worldwide, many of which may be unregulated, and may include manipulative activities;
- investment and trading activities of highly active retail and institutional users, speculators, miners, and investors;
- the speed and rate at which cryptocurrency is able to gain adoption as a medium of exchange, utility, store of value, consumptive asset, security instrument, or other financial assets worldwide, if at all;
- decreased user and investor confidence in digital assets and digital asset trading platforms;
- negative publicity and events relating to the cryptoeconomy;
- unpredictable social media coverage or “trending” of digital assets;
- the ability for digital assets to meet user and investor demands;
- the functionality and utility of digital assets and their associated ecosystems and networks, including digital assets designed for use in various applications;
- consumer preferences and perceived value of digital assets and digital asset markets;
- increased competition from other payment services or other digital assets that exhibit better speed, security, scalability, or other characteristics;
- regulatory (including enforcement) or legislative changes and updates affecting the cryptoeconomy;
- the characterization of digital assets under the laws of various jurisdictions around the world;
- the maintenance, troubleshooting, and development of the blockchain networks underlying digital assets, including by miners, validators, and developers worldwide;
- the ability for cryptocurrency networks to attract and retain miners or validators to secure and confirm transactions accurately and efficiently;
- ongoing technological viability and security of digital assets and their associated smart contracts, applications and networks, including vulnerabilities against hacks and scalability;
- fees and speed associated with processing digital asset transactions, including on the underlying blockchain networks and on digital asset trading platforms;
- financial strength of market participants;
- the availability and cost of funding and capital;
- the liquidity of digital asset trading platforms;
- interruptions in service from or failures of major digital asset trading platforms;
- availability of an active derivatives market for various digital assets;
- availability of banking and payment services to support cryptocurrency-related projects;
- level of interest rates and inflation;
- monetary policies of governments, trade restrictions, and fiat currency devaluations; and
- national and international economic and political conditions.

There is no assurance that any digital asset will maintain its value or that there will be meaningful levels of trading activities. For example, in 2022, we witnessed dampened demand for trading digital assets in the wake of industry turmoil, impacting our operating results. In the event that the price of digital assets or the demand for trading digital assets decline, our business, operating results, and financial condition could be adversely affected.

Our operating results are dependent on the prices of digital assets and volume of transactions that we conduct, which have historically been volatile and are subject to social media and publicity risks.

Activities in bitcoin and other digital assets also receive a high degree of public scrutiny, both from traditional media sources and through social media and other forums. Unfavorable publicity regarding bitcoin has adversely affected the price of bitcoin, as has unfavorable publicity involving other digital assets or digital asset-focused firms. Bitcoin has in the past, and may in the future, be the target of media criticism, including regarding the market value, utility and environmental effects of bitcoin. Such unfavorable media coverage could continue to materially impact decisions to buy, hold, or trade bitcoin and, as a result, impact the price of bitcoin.

In addition, social media posts and other statements and actions by prominent individuals, including Elon Musk and Michael Saylor, have resulted in outsized movements in the market price of bitcoin and other cryptocurrencies. It is possible that future statements by Mr. Musk, Mr. Saylor and other individuals concerning bitcoin and other cryptocurrencies will have disproportionate impacts on the market price of bitcoin and other digital assets.

A determination that a digital asset is a “security,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could adversely affect the value of that digital asset and potentially digital assets generally, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock.

Depending on the facts and circumstances, a digital asset may be considered a “security,” or an activity in which we engage may be deemed to involve a “securities transaction,” under the federal or state securities laws. The test for determining whether a particular digital asset is a “security,” or whether a particular activity involves a “securities transaction,” is complex and difficult to apply, and the outcome is difficult to predict. Public, though non-binding, statements by senior officials at the SEC have indicated that the SEC did not consider bitcoin or ether to be securities, and does not currently consider bitcoin to be a security. Moreover, the staff of the SEC’s Division of Corporation Finance has published statements that it does not consider, under certain circumstances, “meme coins” or some stablecoins to be securities. However, such statements may be withdrawn at any time without notice and comment by the staff of the Division of Corporation Finance at the SEC or the SEC itself. In addition, the SEC, through delegated authority approving the exchange rule filings to list shares of trusts holding ether as commodity-based ETFs, appears to have implicitly taken the view that ether is not a security, and through delegated authority has approved exchange rule filings to list shares of trusts holding ether as commodity-based exchange traded products that are not registered as investment companies. The SEC staff has also authored informal, non-binding “no-action” letters to the promoters of a handful of digital assets to the effect that the staff would not recommend enforcement action to the SEC on the basis that transactions in such digital assets, as described to the staff by their respective promoters, are securities transactions. On the other hand, the SEC under the prior administration brought enforcement actions against the issuers and promoters of several other digital assets on the basis that the digital assets in question are securities. Under the prior administration, the SEC also brought enforcement actions against digital asset trading platforms for allegedly operating unregistered securities exchanges, brokers, and clearing agencies on the basis that certain of the digital assets that they facilitate trading and settlement of through their platforms are securities. In January 2025, the SEC launched a crypto task force dedicated to developing a comprehensive and clear regulatory framework for digital assets led by Commissioner Hester Peirce. Subsequently, Commissioner Peirce announced a list of specific priorities to further that initiative, which included pursuing final rules related to a digital asset’s security status, a revised path to registered offerings and listings for digital assets-based investment vehicles, and clarity regarding digital asset custody, lending, and staking. However, the efforts of the crypto task force have only just begun, and how or whether the SEC regulates digital asset activity in the future remains to be seen.

Whether a digital asset is a security or offers and sales of a digital asset are securities transactions under the federal securities laws depends on whether it is included in the lists of instruments making up the definition of “security” in the Securities Act, the Exchange Act, the Investment Advisors Act and the Investment Company Act (collectively, “federal securities laws”). Digital assets as such do not appear in any of these lists, although each list includes the terms “investment contract” and “note,” and the SEC has typically analyzed whether a particular digital asset is a security by reference to whether it meets the tests developed by the federal courts interpreting these terms, known as the *Howey* and *Reves* tests, respectively. For many digital assets, whether or not the *Howey* or *Reves* tests are met is difficult to resolve definitively, and substantial legal arguments can often be made both in favor of and against a particular digital asset qualifying as a security under one or both of the *Howey* and *Reves* tests. Adding to the complexity, the SEC staff has indicated that the security status of a particular digital asset can change over time as the relevant facts evolve, though the SEC has not further addressed this theory in its ongoing litigation.

Certain state regulators or attorneys general have also alleged that certain digital assets are securities under relevant state laws and that digital asset trading platforms' activities violate state securities laws.

Any enforcement action by the SEC or a state securities regulator asserting that a digital asset is a security or sold in a securities transaction or related derivatives contract, or a court decision to that effect, would be expected to have an immediate material adverse impact on the trading value of that digital asset, and depending on the specific characteristics of the digital asset, could have adverse spillover effects on the trading values of other digital assets perceived to share similar characteristics. This is because the business models behind most digital assets are incompatible with U.S. regulations applying to transactions in securities. If a digital asset is determined to be a security, it is likely to become difficult or impossible for the digital asset to be traded, cleared or custodied in the United States through the same channels used by non-security digital assets. For example, all transactions in such digital asset would have to be registered with the SEC and potentially state securities regulators, or conducted in accordance with exemptions from registration, which could severely limit its liquidity and usefulness. Moreover, the network on which such digital asset is utilized may be subject to regulation as an intermediary in the securities markets, which could effectively render the network impracticable for its intended purposes. In addition to materially and adversely affecting the trading value of the digital asset, any such consequences are likely to significantly impact its liquidity and market participants' ability to convert the digital asset into U.S. dollars. Any assertion that a digital asset is a security or securities transaction by the SEC or another regulatory or judicial authority may have similar effects.

The SEC's positions on the federal securities law status of particular digital assets are closely watched and can have dramatic effects, whether or not the SEC's positions prevail in federal court. For example, in 2020 the SEC filed a complaint against the promoters of XRP alleging that they raised more than \$1.3 billion through XRP sales that should have been registered under the federal securities laws, but were not. In the weeks following the filing of the SEC's complaint, XRP's market capitalization fell to less than \$10 billion, which was less than half of its market capitalization in the days prior to the complaint. Subsequently, in July 2023, the District Court for the Southern District of New York held that while XRP is not a "security," certain sales of XRP to certain buyers (but not other types of sales to other buyers) amounted to "investment contracts" under the *Howey* test and therefore securities. The District Court entered a final judgment in the case on August 7, 2024. On January 15, 2025, the SEC filed an appeal against the judgment with the United States Court of Appeals for the Second Circuit (the "Second Circuit"). In late March 2025, senior executives of the promoters of XRP announced on social media platforms that the SEC has agreed to drop its appeal without conditions in connection with its settlement agreement with the SEC, which is subject to finalization. On April 10, 2025, the promoters of XRP and the SEC filed a joint motion to pause the judicial proceedings. On April 16, 2025, the Second Circuit granted the joint motion and ordered the SEC to file a status report within 60 days. On May 8, 2025 the promoters of XRP and the SEC entered into a settlement agreement, which provided that, among other things, the parties would jointly request the district court to issue an indicative ruling as to whether it would dissolve the August 7, 2024 injunction and order the escrow account to be released, with \$50 million ultimately being paid by the promoters of XRP as a civil penalty to the SEC.

Likewise, in the days following the announcement of SEC enforcement actions against certain digital asset issuers and trading platforms, the prices of various digital assets declined significantly and may continue to decline if or as such cases advance through the federal court system. Furthermore, the decisions in cases involving digital assets have resulted in seemingly inconsistent views of different district court judges, including one that explicitly disagreed with the analysis underlying the decision regarding XRP, which underscore the continuing uncertainty around which digital assets or transactions in digital assets are securities and what the correct analysis is to determine each digital asset's status. For example, the conflicting district court opinions and analyses demonstrate that factors such as how long a digital asset has been in existence, how widely held it is, how large its market capitalization is, the manner in which it is offered, sold or promoted and whether it has actual use in commercial transactions, ultimately may have limited to no bearing on whether the SEC, a state securities regulator or any particular court will find it to be a security.

In June 2023, the SEC brought an action against Binance (the "Binance Complaint") and Coinbase (the "Coinbase Complaint") alleging that they solicited U.S. investors to buy, sell, and trade "crypto asset securities" through their unregistered trading platforms and operated unregistered securities exchanges, brokerages and clearing agencies. Binance subsequently announced that it would be suspending USD deposits and withdrawals on Binance.US and that it planned to delist its USD trading pairs. In November 2023, the SEC brought similar charges against Kraken (the "Kraken Complaint"), alleging that it operated as an unregistered securities exchange, brokerage and clearing agency. In February 2025, March 2025 and May 2025, respectively, each of Coinbase, Kraken and Binance entered into a court-approved joint stipulation with the SEC to dismiss each of the SEC's lawsuits with prejudice. Several other digital assets market participants have also announced that the SEC informed them that the SEC was terminating its investigation or

enforcement action into their firm. The effect of these lawsuits on the broader digital asset ecosystem and the reputation impact on industry participants, remain uncertain. As part of our trading business, we have in the past and in some cases continue to provide clients and counterparties access to certain digital assets that the SEC in these complaints has alleged to be securities, or the subject of securities transactions. We carefully consider the implications of these allegations as well as other developments relating to the digital assets to which we may provide clients and counterparties access.

As described under “—A determination that a digital asset is a “security,” or a “security-based swap,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could have adverse regulatory consequences for us, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock,” the determination that a digital asset is a security under the federal securities laws could also have adverse U.S. regulatory consequences for us. But even if there were no such adverse U.S. regulatory consequences, we may nevertheless decide to terminate our services relating to that digital asset and liquidate our holdings of that digital asset while we believe a liquid market still exists, which could result in us selling that digital asset at depressed prices.

To the extent we hold any digital asset that is impacted by an assertion or finding of securities status, or we engage in any economic arrangement in respect of a digital asset that is deemed to be a securities transaction, our business, financial condition and results of operations would be adversely impacted, as they would to the extent we earn revenues from transacting or facilitating transactions in that digital asset. Depending on which digital asset or activities are impacted, these adverse impacts could be material to us and to the market price of our Class A common stock.

A determination that a digital asset is a “security,” or a “security-based swap,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could have adverse regulatory consequences for us, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock.

In addition to the potential for adverse consequences to our business, financial condition and results of operations described under “—A determination that a digital asset is a “security,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could adversely affect the value of that digital asset and potentially digital assets generally, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock,” the classification of a digital asset as a security under the federal securities laws has wide-ranging implications for the regulatory obligations that flow from the offer, sale, trading, clearing and holding of such assets. In 2023, the SEC brought the Coinbase Complaint, the Binance Complaint and the Kraken Complaint, alleging that a number of digital assets are securities and that, as a result, each of these companies had failed to register with the SEC in a number of capacities as required under the federal securities laws. Although the complaints against Binance, Coinbase, and Kraken have been dismissed, in the days following the complaints, one of the digital asset trading platform’s publicly traded stock price fell by 10%. Although we take the implications that our digital assets could be treated as securities for federal securities law purposes into account, for a digital asset that we previously treated as not being a security for federal securities law purposes, the implications could include the following, any of which could have adverse consequences to our business, financial condition and results of operations as well as the market price of our Class A common stock:

- Liability for participating in unregistered securities offerings. In the United States, securities generally may not be offered or sold unless the offer or sale is registered with the SEC or an exemption from registration is available. If a digital asset or any of our transactions in or referencing digital assets is determined to be a security and we offered or sold that digital asset, or engaged in that digital asset transaction, without a valid exemption from SEC registration requirements, we could incur liability to purchasers as well as SEC monetary fines and other penalties, including restrictions on our ability to conduct business.
- Liability for acting as an unregistered broker-dealer, national securities exchange or clearing agency. A person in the business of effecting transactions in securities or security-based swaps in the United States is generally subject to registration with the SEC as a “broker,” “dealer,” or “security-based swap dealer.” A platform that brings together purchasers and sellers to trade securities (or certain securities-related derivatives) in the United States is generally subject to registration as a national securities exchange or as a security-based swap execution facility, or must qualify for an exemption, such as by being operated by a registered broker-dealer as an alternative trading system. A person that facilitates clearing and settlement of securities or that acts as a securities depository may be subject to registration with the SEC as a clearing agency. If a digital asset is determined to be a security and we transacted in that digital asset or engaged in a transaction referencing that digital asset in a manner implicating any of the foregoing SEC registration requirements or other related registrations without being so registered or without

a valid registration exemption, we could incur SEC monetary fines and other penalties, including restrictions on our ability to conduct business.

- Liability for operating as an unregistered investment company. A person in the business of investing in securities in the United States is subject to registration and regulation as an investment company under the Investment Company Act, unless a valid exemption from such registration applies. The laws and regulations applicable to registered investment companies, including limitations on debt and other forms of leverage, restrictions on transactions with affiliates and other limitations on business activities generally make it impractical for an operating company such as us. If one or more digital assets is determined to be a security and we had been relying on such digital assets as not being securities for Investment Company Act purposes, we could incur SEC monetary fines and other penalties, including restrictions on our ability to conduct business. In addition, counterparties to contracts to which we are party could seek to avoid their obligations under those contracts on grounds that contracts with illegally unregistered investment companies are unenforceable.
- Obligation to restructure our operations in order to avoid operating as an unregistered investment company. We intend to conduct our operations so that we will not be deemed to be an investment company under the Investment Company Act. If we determined that we risked becoming subject to registration as an investment company under the Investment Company Act, we would explore alternatives for avoiding this status, which may include disposing of digital asset securities, or one or more of our balance sheet venture investments, or acquiring businesses or assets that are not securities, and we may be required to effect such dispositions or acquisitions under unfavorable market conditions. See “—Risks Related to Our Organizational Structure and Ownership of our Class A Common Stock—If we are deemed to be an investment company under the Investment Company Act, applicable restrictions could make it impractical for us to continue our business as contemplated and could have a material adverse effect on our business.”
- Liability for acting as an unregistered investment adviser. A person in the business of advising others, for compensation, with respect to securities in the United States or to U.S. clients is subject to registration and regulation as an investment adviser under the Advisers Act, unless a valid exemption from such registration applies. If a digital asset is determined to be a security and we advised clients as to that digital asset in a manner implicating Advisers Act registration requirements without being so registered or without a valid registration exemption, we could incur SEC monetary fines and other penalties, including restrictions on our ability to conduct business.

Similar, though not identical, concerns would arise if a digital asset or a digital asset transaction is determined to be a security-based swap.

We may be able to take steps in order to bring our operations into compliance with the federal securities laws following a determination that one or more digital assets in which we transact are securities or security-based swaps, but there is no guarantee that we would be able to take such actions as may be necessary to ensure that our future activities comply with applicable law, which could force us to discontinue some or all of our business activities. In general, any steps we are able to take in order to ensure future compliance with applicable laws would not insulate us from liability for past violations.

While the above description of adverse regulatory consequences focuses on the federal securities laws, the various U.S. states and jurisdictions outside the United States also intensively regulate securities transactions, and so a U.S. state’s or other jurisdiction’s determination that a particular digital asset is a security or security-based swap could have similarly adverse consequences to our business, financial condition and results of operations as well as the market price of our Class A common stock.

Our process for analyzing whether or not a particular digital asset is a security for purposes of the federal securities laws may not yield results that are consistent with subsequent determinations by the SEC or federal courts, or with similar determinations made by our competitors.

We have procedures designed to analyze whether each digital asset that we seek to transact in or develop could be deemed to be a “security” under the federal securities laws. We have adapted our process for determining the federal securities law status of digital assets over time, as the specific steps in the process have evolved in light of the developing regulatory environment. Prior to 2018, our activities primarily involved Bitcoin and Ethereum and their various forks. Beginning in January 2018, we implemented a procedure whereby before transacting in a new digital asset, our trading desk would seek approval from the legal department; and the legal department would generally discuss the digital asset with other Galaxy employees to determine whether the digital asset appeared to have a consumptive use, as opposed to a merely speculative investment use, and if so, approve it for transactions. Beginning in January 2019, our legal department

introduced a New Product Approval form in order to standardize the process that was initiated the previous year, and responsibility for approving and categorizing new digital assets was assigned to a risk committee later renamed the “Token Committee” composed of senior executives, including members of the legal department, and advised by the legal department. The Token Committee is currently comprised of our President, Chief Financial Officer, Chief Operating Officer, General Counsel, Head of Trading, Head of Technology, Head of Research, Head of Operations, Chief Compliance Officer, Deputy Chief Compliance Officer and Deputy General Counsel. In August 2020, with the benefit of several months’ experience using the Token Committee approval process, our legal department updated the New Product Approval form to more closely align with the analysis being conducted by the Token Committee with advice of the legal department. In August 2021, the Token Committee introduced an element to the approval process in addition to the New Product Approval form, generally requiring a third-party assessment of a digital asset’s federal securities law status, which may include a legal analysis prepared by external lawyers. In 2025, the process was further updated to also require an assessment as to whether a digital asset could be deemed a security under New York state securities laws.

As part of our federal securities law analytical process, we take into account a number of factors, including the various definitions of “security” under the federal securities laws and federal court decisions interpreting elements of these definitions, such as the U.S. Supreme Court’s decisions in the *Howey* and *Reves* cases and their progeny, as well as reports, orders, press releases, public statements and speeches by the SEC, its commissioners and its staff providing guidance on when a digital asset may be a security for purposes of the federal securities laws. To the extent any such court rulings, reports, orders, press releases, public statements, speeches or other developments we become aware of implicate a digital asset that we have previously sorted into the “No Restrictions” category, we endeavor to reassess the federal securities law status of such digital asset. In certain circumstances, our categorization of particular digital assets has changed, and may in the future change, in light of new information. For example, if a digital asset in which we transact in the United States or with U.S. clients or counterparties were alleged to be a security in credible private litigation, an SEC enforcement order or in a statement or speech by an SEC official, we would consider any new findings of facts, legal analyses and other circumstances involving such digital asset that are relevant to whether such digital asset may be a security, and determine whether our classification of such digital asset should be modified. Conversely, certain digital assets that were once offered in a manner that led us to sort them into the “Non-U.S.” category (i.e., because they did not meet the criteria for inclusion in the “No Restrictions” category at the time of such determination), may later be re-analyzed based on developing facts and circumstances. Under certain circumstances, we may determine that we have reasonable grounds for concluding that such a digital asset is not a security under the federal securities laws, and re-categorize such digital asset into the “No Restrictions” category. We also evaluate any broader impact that such court rulings, reports, orders, press releases, public statements and speeches may have on our overall business strategy, in particular the scope of our trading business. We continue to monitor the U.S. and global regulatory environment, and we expect our process to continuously evolve to take into account case law, facts, and developments in technology, as regulatory guidance evolves. However, because of the inherent uncertainties associated with such an analysis, we acknowledge that a particular digital asset that we transact in or develop may in the future be found by a federal court or alleged by the SEC or a private plaintiff to be a security notwithstanding our prior conclusion, and such prior conclusion, even if reasonable under the circumstances, would not preclude legal or regulatory action based on the presence of a security. We recognize that the application of securities laws to the specific facts and circumstances of digital assets may be complex and subject to change and differing judicial opinions.

We conduct a re-evaluation of our prior determinations regarding the federal securities law status of a digital asset in which we may transact when we become aware of new findings of facts or other changed circumstances implicating such digital asset, and a member of the Token Committee considers there to be a reasonable likelihood that such development could impact our prior determination with respect to the federal securities law status of such digital asset. In that event, we would re-evaluate such digital asset under our then-current procedures, taking into consideration such new development, before continuing to transact in such digital asset in a manner that would implicate our compliance with federal securities laws. We do not always re-examine our prior determinations regarding the federal securities law status of the digital assets in which we may transact solely because there has been an update or enhancement to our policies and procedures. Because of this, there is a possibility that a digital asset we have approved for trading under our prior policies and procedures might not gain approval under our policies and procedures as updated or enhanced. If we were to determine, as a result of a re-examination of our prior determination or otherwise, that a digital asset in which we have previously transacted on a “No Restrictions” basis is a security, we would take all actions that we deem necessary in order to comply with law, including but not limited to ceasing to trade such digital asset in the United States or with U.S. clients or counterparties.

Because of complexities in applying the federal securities laws to digital assets and the fact that different companies doing business in the digital asset industry take varying approaches to digital asset analyses, we expect that competitors may reach different conclusions from us on the securities-law status of a particular digital asset or digital asset category. Although we anticipate that these differences will narrow over time as the SEC and federal courts address the securities-law status of larger numbers of individual digital assets, or as Congress enacts relevant legislation, until that occurs, where

competitors conclude that they have the ability to transact in digital assets in ways that we do not permit because of these different conclusions, some competitors may have business and revenue opportunities that are not available to us.

We believe that our process reflects a thoughtful analysis that is reasonably designed to facilitate consistent application of available legal guidance to digital assets to determine whether a particular digital asset is a security under the federal securities laws. However, we recognize that the application of securities laws to the specific facts and circumstances of digital asset transactions is complex and subject to change and differing judicial opinions, and therefore legal and regulatory risk will be an inherent feature of our business model until greater legal and regulatory certainty becomes possible. Because our process may be considered “risk based” in the sense that it is not capable of entirely eliminating risks associated with a particular digital asset being found to be a security and because it does not address a state-by-state securities law analysis, and because of the fact that our determinations (and similar determinations by other industry participants) are not binding upon the SEC, any state regulator or attorney general, a private plaintiff, or any federal or state court, we acknowledge that a particular digital asset that we transact in may in the future be found by a federal or state court or alleged by the SEC, a state regulator or attorney general, or a private plaintiff to be a security notwithstanding our prior determination. We also acknowledge that the SEC, any state regulator or attorney general, a private plaintiff, or any federal or state court may determine that a digital asset is a security based on factors that are difficult to predict and/or are outside of our control, potentially including the actions of a third-party promoter. In that case, our prior determination, even if reasonable under the circumstances, would not preclude legal or regulatory enforcement action, or lawsuits brought by our clients and counterparties, based on the presence of a security. We have received, and might in the future receive, from time to time, SEC inquiries regarding specific digital assets in which we transact. To the extent the SEC, a state regulator or attorney general, a private plaintiff or a court asserts or determines that any digital assets in which we transact are securities, that assertion or determination could prevent us from continuing to transact in such digital assets and could result in regulatory enforcement penalties, sanctions, injunctions, cease and desist orders, reputational harm and financial losses.

If the SEC or any other party alleges that our non-custodial staking services involve unregistered offers and sales of securities or unregistered securities broker-dealer activity in violation of the Securities Act or the Exchange Act and the courts agree, we may be required to cease our non-custodial staking activities and may be subject to monetary and other penalties or other liabilities.

In several enforcement actions filed by the SEC under the prior administration in federal courts in New York, California, and Washington D.C., the SEC alleged that certain companies have offered staking services to retail customers for various digital assets as unregistered securities or acted as unregistered securities broker-dealers in facilitating offers or sales of third-party staking services in violation of the registration provisions of the Securities Act or the Exchange Act. For example, in 2023 the SEC charged Kraken, Coinbase and Binance with offering and selling digital asset staking-as-a-service programs to retail customers as unregistered investment contract schemes in violation of the Securities Act. In June 2024, the SEC charged Consensys Software Inc. with acting as an underwriter of unregistered securities in violation of the Securities Act and as an unregistered broker in violation of the Exchange Act by marketing the Lido and Rocket Pool third-party liquid staking-as-a-service programs to retail customers through Consensys’ “Metamask Staking” platform. As noted above, the complaints against Binance, Coinbase, and Kraken have been dismissed, as has the complaint against Consensys. In May 2025, the staff of the SEC Division of Corporation Finance released a statement taking the view that “protocol staking” activities described therein do not involve the offer or sale of a security (the “Staff staking statement”). While we believe our non-custodial staking services are within the activities described in the Staff staking statement, the Staff staking statement is not a rule or other statement of the SEC and is not binding on any party—including the SEC or a court.

For many of the reasons similar to those discussed in the Staff staking statement, we believe that our non-custodial staking businesses do not offer or sell any “securities” subject to the securities laws or SEC regulations. We further believe that, even if they could be alleged to involve securities, our staking activities would in any event qualify for exemptions from Securities Act or Exchange Act requirements. For example, we believe our provision of non-custodial staking validator node infrastructure to accredited investors through privately arranged transactions and our operation of back-end validator node support to third-party staking operations such as Lido do not fall within the purview of the securities laws or SEC regulations, and that even if they did, they would qualify for one or more exemptions from those laws or regulations. However, we do not know if the SEC or a court would ultimately agree with our interpretation of those laws or regulations. If the SEC or a private litigant were to prevail on claims that our non-custodial staking businesses violate the Securities Act or Exchange Act or similar state laws, we may be subject to monetary penalties, liabilities, reputational harm, and may be required to cease offering these services.

We may suffer losses due to staking, delegating, and other related services.

Blockchain networks which utilize PoS or similar consensus mechanisms to validate transactions enable holders of certain digital assets to stake or delegate those assets with validator nodes to secure the network and participate in transaction validation activities on their underlying blockchain networks. We currently stake certain digital assets and operate validator nodes on blockchain networks through our blockchain infrastructure operations. Some PoS networks require the digital assets to be transferred on the underlying blockchain networks into smart contracts which are not under our or anyone's control, or to a validator node directly, to participate in staking. Other PoS networks enable users to delegate certain rights or powers associated with the relevant digital assets to a validator node, while custody of the digital asset itself remains entirely with the user. If our validator nodes or relevant smart contracts fail to behave as expected, suffer cybersecurity attacks, experience security issues, or encounter other problems, our or our clients' digital assets may be irretrievably lost. In addition, most PoS blockchain networks dictate requirements for participation in the relevant staking activity, such as requiring a minimum amount of staked digital assets before being able to operate as a validator node. If those requirements are not met, the blockchain network or other validator nodes may impose penalties, referred to as "slashing," such as if the validator node operator acts maliciously on the network, "double signs" any transactions, or experiences extended downtimes. Slashing penalties can also apply due to prolonged inactivity on a blockchain network and inadvertent errors such as coding, computing or hardware issues, as well as more serious behavior such as intentional malfeasance. If Galaxy-operated validator nodes or any other validator nodes that we may use are subject to slashing in the future in accordance with the rules of an underlying blockchain network, our or our clients' staked digital assets may be confiscated, withdrawn, or burnt by the network, resulting in permanent losses. Any loss of digital assets, penalties or slashing events could damage our brand and reputation, cause us to suffer financial losses, and adversely impact our business.

Our issuance of the Galaxy Premium Yield Investment Note through our GalaxyOne platform exposes us to additional regulatory, litigation, and financial risk.

We offer the Galaxy Premium Yield Investment Note (the "Note") as an investment product through our GalaxyOne platform. The Note is not a bank deposit or other obligation of, or guaranteed by, any bank. It is not insured by the FDIC or any other governmental agency. The Note is unsecured, and investors may lose some or all of their principal. Galaxy Digital LP offers the Note only to accredited investors, as defined by the SEC under Rule 501 of its Regulation D, which includes individuals permitted to invest in certain private securities offerings not registered with the SEC. Should the SEC disagree with our classification of the Note, or if Galaxy Digital LP were unable to meet its obligations to investors pursuant to the terms of the Note, customers may bring claims or litigation against us that would be costly to address and may adversely affect our business.

Our relationship with our bank partner, Cross River Bank, is important to our GalaxyOne business, and if we are unable to maintain our relationship, it may adversely affect such business and its financial performance.

We rely on Cross River Bank to provide the banking services offered through the GalaxyOne platform, such as opening and maintaining customer high-yield demand deposit accounts and issuing GalaxyOne-branded debit cards. Our relationship with Cross River Bank is an important part of our GalaxyOne business as we do not have a banking license.

Our relationship with Cross River Bank is governed by several agreements. These agreements give Cross River Bank discretion in approving aspects of our business practices, including our application and qualification procedures for customers and the products we introduce pursuant to such partnerships, and require us to comply with certain risk management standards and other regulations. If we lose our relationship with Cross River Bank and we are not able to switch to another bank partner, we will not be able to operate our business in its current form. If Cross River Bank terminates any of these agreements or is unable or unwilling to process customer transactions for any reason, including for regulatory reasons, we will likely be unable to switch some or all of our customer transactions or accounts from Cross River Bank to another bank because customers hold their accounts directly with Cross River Bank rather than one of our affiliates. Moreover, switching a significant portion or all of our member accounts handled by Cross River Bank to another bank partner or partners, including contracting with an additional bank or banks, may take time and increase the complexity of our operations, resulting in significant additional costs and diverting management's attention from other aspects of our business.

More specifically, we partner with Cross River Bank pursuant to a master program services agreement (as amended, the "CRB MPSA"), and a credit card and debit card amendment to the CRB MPSA. The CRB MPSA has an initial term of three years, beginning in October 2022, and shall continue for two successive terms each for two year periods (each a "Renewal Term"), unless prior to the expiration of the initial term or any Renewal Term, either Cross River Bank or GalaxyOne gives the other party not less than ninety days' written notice of its election not to renew the CRB MSA. The

Initial Term of the CRB MPSA ends in October 2025 and GalaxyOne intends to maintain the relationship through the upcoming first Renewal Term. Cross River Bank may terminate or suspend individual demand deposit accounts at any time in Cross River Bank's sole discretion; however, a suspension of a majority of accounts for a period exceeding thirty days without written approval by GalaxyOne will be deemed a termination of the CRB MPSA. Cross River Bank and GalaxyOne may both terminate the CRB MPSA early for cause upon the occurrence of certain events, including but not limited to certain regulatory changes, regulatory termination, and insolvency by either party. Cross River Bank may also elect to suspend the CRB MPSA, during which time new account openings are suspended, until such time as the parties are able to correct the aspects of the program leading to the suspension. Upon the termination or expiration of the CRB MPSA, GalaxyOne may elect to transition the program to a successor banking provider, at which time Cross River Bank and GalaxyOne are contractually obligated to work together during the wind-down period to wind down the program or transition the program to the successor as soon as reasonably possible and in no event later than one year after expiration or termination of the CRB MPSA, but we cannot guarantee the outcome of such a transition or wind down.

Partnerships between banks and financial technology companies have been the subject of increased and evolving scrutiny from regulators and legislators over the past several years. Federal banking regulators have, in some cases, required increased oversight by banks of their partners or restricted banks' abilities to offer or expand programs. Accordingly, we or Cross River Bank may face external pressures that could impose additional compliance costs on us or Cross River Bank, impact Cross River Bank's ability to process transactions, and affect our relationship over time. The potential for increased regulatory scrutiny may cause Cross River Bank to reassess its partnership with us and may deter new potential bank partners from entering a partnership with us. For more information related to these regulatory matters, see the section titled "Business—Regulatory Environment."

In addition, our reliance on Cross River Bank exposes us to its economic performance, such as any liquidity constraints, insolvency, or other factors impacting Cross River Bank's ability to provide banking services through the GalaxyOne platform, and to any events, circumstances, or risks affecting Cross River Bank or the banking system generally. If Cross River Bank's stability deteriorates, if it does not maintain appropriate regulatory compliance, or if GalaxyOne's business or economic relationship with Cross River Bank deteriorates for any reason, we will likely be unable to transfer customer accounts (or, if we are able, may incur substantial costs to do so) to a new bank partner and may have difficulty finding additional bank partners; in addition, our GalaxyOne products may be disrupted, the GalaxyOne brand may be harmed, and its business and financial performance may be adversely affected.

We are highly dependent on our key personnel, including our Founder, which exposes stockholders to material and unpredictable "key man" risk.

We are highly dependent on the services of our senior management team, including members of our executive team, and other key employees and personnel across product, engineering, risk management, compliance and legal, finance and marketing. Because we operate in a relatively new industry that requires highly skilled and technical personnel, our future success is highly dependent on the talents and contributions of our senior management and other key personnel. The loss of any such key personnel could disrupt our operations and have a material adverse effect on our business.

In particular, we are highly dependent on the services of Michael Novogratz, our Founder, CEO and, through his direct and indirect ownership, the largest beneficial owner of our common stock, for conducting our businesses, implementing investment and trading strategies and establishing and maintaining relationships with key business counterparties. If the services of our Founder were to become unavailable for any reason including a voluntary decision by our Founder to no longer continue with the business, it would have a material adverse effect on our business and investment decisions, financial results and returns to our stockholders.

Our Founder, other members of senior management or other key personnel could engage in activities outside of Galaxy or could leave their positions at Galaxy in favor of other pursuits. Neither our Founder nor any other key personnel are contractually required to continue to provide services to us. While all of our key personnel have entered into employment agreements with us which contain covenants that they will not compete with us and applicable laws may prevent such personnel from engaging in certain directly competitive activities to the extent that they are members of our board of directors, such laws will not guarantee to stockholders that such personnel will devote their full time, attention or efforts to us. For example, if our Founder were to cease to provide services to us, he could engage in other pursuits, which may relate to digital assets or investing, while remaining our largest owner, an outcome that may be unfavorable to stockholders. Our Founder may also continue to manage significant non-digital assets outside of us, which may consume some of his time, attention and efforts.

Our Founder’s public profile makes it more likely that we will attract material regulatory scrutiny, which would be costly and distracting regardless of whether we have engaged in any unlawful conduct.

Our Founder has been a vocal and visible proponent of digital assets, in some cases attracting controversy in connection with his views and statements as expressed on social media or otherwise. Further, due to our Founder’s public profile, his views, statements and conduct could be subject to scrutiny by both the public at large and governmental and regulatory bodies, which could adversely affect our business and our reputation. These considerations make it foreseeable that we could attract material regulatory scrutiny driven in part by the visibility of our Founder, irrespective of whether we have engaged in any unlawful conduct. Regulatory scrutiny may take the form of requests for information or responses, examinations, meetings or other types of interactions that may proceed to a formal enforcement action, suit, fine or other formal negative sanction, consume a material amount of management’s time, attention and efforts, lead to material spending on legal and other advisors or cause other negative consequences (including, for example, certain of the matters discussed under “Item 1. Legal Proceedings.”).

If we fail to develop, maintain and enhance our brand and reputation, our business operating results and financial condition may be adversely affected.

Our brand and reputation are key assets and a competitive advantage, and maintaining a strong brand and reputation will be an important factor in our success and our development of our business. Protecting and enhancing our brand depends largely on the success of our marketing efforts, ability to provide consistent, high-quality, and secure products, services, features, and support. Thus, maintaining, protecting, and enhancing our reputation is also important to our development plans and relationships with our partners and counterparties. Furthermore, we believe that the importance of our brand and reputation may increase as competition in the financial services industry, the digital asset industry and the AI industry further intensifies. Our brand and reputation could be harmed if we fail to achieve these objectives or if our public image were to be tarnished by negative publicity, unexpected events, or actions by third parties. Unfavorable publicity regarding, for example, the quality of or changes to our products and services, litigation or regulatory activity, privacy practices, data security compromises or breaches, terms of service, intellectual property matters, employment matters, the use of our products, services, or supported digital assets for illicit or objectionable ends, the actions of our clients, customers, employees, or the actions of other companies that provide similar services to ours, has in the past, and could in the future, adversely affect our reputation and our business.

We receive a high degree of media coverage in the industries in which we operate and around the world. Additionally, because we are a founder-led company, actions by, or unfavorable publicity about our Founder, may adversely impact our brand and reputation. Such negative publicity also could have an adverse effect on the size and engagement of our customers and could result in decreased revenue, which could have an adverse effect on our business, operating results, and financial condition. Further, we may in the future be the target of social media campaigns criticizing actual or perceived actions or inactions that are disfavored by our customers, employees, or society at-large, which campaigns could materially impact our customers’ decisions to engage with our products and services.

More broadly, because the digital asset, blockchain technology and AI sectors are relatively nascent, public opinion is underdeveloped and will continue to evolve over time. For example, there has been focus on the environmental, social and governance considerations regarding the use of electricity and other resources for digital asset mining operations. The same environmental considerations are also applicable to the AI/HPC sector.

Public debate regarding the regulation of all facets of the digital asset sector will continue to take shape as regulators and lawmakers make their positions known. Moreover, in 2022, each of Celsius Networks, Voyager Digital, Three Arrows Capital and FTX declared bankruptcy. In particular, in November 2022, FTX—which was at the time one of the world’s largest and most popular digital asset trading platforms—became insolvent, and it was revealed that the platform had been misusing customer assets, resulting in a loss of confidence in participants of the cryptoeconomy and negative publicity surrounding crypto more broadly. Additionally, in February 2025, the digital asset trading platform, Bybit, lost approximately \$1.5 billion in ether through a hacker-induced transfer from its cold wallet to a wallet address associated with the Lazarus Group. Unfavorable media coverage in relation to the cryptoeconomy, including the societal impact of digital assets and the infrastructure that supports them and/or the viability of any particular cryptocurrency, digital asset trading platform, or firm engaged in digital asset-related businesses, could have a cascading impact on digital assets as an investable asset class, or even the cryptoeconomy at large, and adversely impact our business, our operating results and the value of any investment in us.

If we fail to protect our brand image or reputation, we may experience material adverse effects to the size, demographics, engagement, and loyalty of our customers and counterparties, resulting in decreased revenue. In addition, if securities analysts or investors perceive any media coverage of us, or of the industries in which we operate more broadly, to

be negative, the price of our Class A common stock may be adversely affected. Any such negative publicity could have an adverse effect on the size, activity, and loyalty of our customers and counterparties, and result in a decrease in revenue, which could adversely affect our business, operating results, and financial condition. See “—Risks Related to Cryptocurrencies and Digital Assets—Due to a lack of familiarity and some negative publicity associated with digital asset trading platforms, existing and potential customers, counterparties and regulators may lose confidence in digital asset trading platforms” and “—Risks Related to Our Business Lines—Our strategy to expand into the AI/HPC data center business may not be successful and may result in adverse consequences to our business, financial condition and results of operations” for further discussion of these risks.

If we are unable to successfully identify, hire and retain qualified individuals, we will not be able to implement our growth strategy successfully.

Our future success depends on the continuing efforts of our key employees and our ability to attract and retain highly skilled personnel and senior management. We currently depend on the continued services and performance of our key personnel, including our Founder. Our growth strategy is based, in part, on our ability to attract and retain highly qualified individuals. Competition presented by other firms may create difficulty for us in recruiting and retaining professionals of a caliber consistent with our business strategy. If we are unable to successfully identify hire, develop, motivate and retain qualified professionals, this failure could materially and adversely affect our investment and trading strategies, the value of our assets and the value of any investment in us. If one or more of our executive officers or key employees were unable or unwilling to continue their employment with us, we might not be able to replace them easily, in a timely manner, or at all. The risk that competitors or other companies may poach our talent increases as we continue to build our brands and become more well-known. Our key personnel have been, and may continue to be, subject to poaching efforts by our competitors and other fintech, internet and high-growth companies, including well-capitalized players in the digital asset space. The loss of key personnel, including members of management as well as key engineering, product development, marketing, and sales personnel, could disrupt our operations and have a material adverse effect on our business. The success of our brand also depends on the commitment of our key personnel to our mission. To the extent that any of our key personnel act in a way that does not align with our mission, our reputation could be materially adversely affected.

Our future success will depend upon our continued ability to identify, hire, develop, motivate and retain highly skilled individuals across the globe, with the continued contributions of our senior management being especially critical to our success. Competition for well-qualified, highly skilled employees in the industries in which we operate is intense and our continued ability to compete effectively depends, in part, upon our ability to attract and retain new employees. While we have established programs to attract new employees and provide incentives to retain existing employees, particularly our senior management, we cannot guarantee that we will be able to attract new employees or retain the services of our senior management or any other key employees in the future. Additionally, we believe that our culture and core values have been, and will continue to be, a key contributor to our success and our ability to foster the innovation, creativity and teamwork we believe we need to support our operations. If we fail to effectively manage our hiring needs and successfully integrate our new hires, or if we fail to effectively manage remote work arrangements, our efficiency and ability to meet our forecasts and our ability to maintain our culture, employee morale, productivity and retention could suffer, and our business, financial condition and results of operations could be materially adversely affected.

We operate in highly competitive industries and we compete against unregulated or less regulated companies and companies with greater financial and other resources, and our business, operating results, and financial condition may be adversely affected if we are unable to respond to our competitors effectively.

Both the cryptoeconomy and the AI economy are highly innovative, rapidly evolving, and characterized by healthy competition, experimentation, changing customer needs, frequent introductions of new products and services, and subject to uncertain and evolving industry and regulatory requirements. We expect competition to further intensify in the future as existing and new competitors introduce new products or enhance existing products. We compete against a number of companies operating both within the United States and abroad, and both those that focus on traditional financial services, those that focus on crypto-based services and those that focus on AI/HPC-based services. Our competitive landscape is varied across two operating business segments: Digital Assets, which includes our Global Markets and Asset Management & Infrastructure Solutions businesses, and Data Centers, which includes our scalable high performance computing infrastructure.

Digital Assets: Our Digital Assets operating business segment integrates trading, investment banking, asset management, and staking services, which compete with a diverse array of traditional and decentralized market participants.

Data Centers: Our Data Centers operating business segment competes with a range of infrastructure providers that are building or repurposing facilities to support the rapidly growing demand for AI and compute-intensive workloads. This

includes traditional data center operators expanding into HPC, cloud infrastructure providers scaling capacity, and former crypto mining operators pivoting to meet the needs of AI workloads.

We believe our primary source of competition to date has been from companies, in particular those located outside the U.S., who are either subject to significantly less stringent regulatory and compliance requirements in their local jurisdictions or have interpreted the regulatory requirements to which they are subject in a manner that is different from our interpretation. Some of such companies' business models rely on being unregulated or only regulated in a small number of lower compliance jurisdictions, whilst also offering their products in highly regulated jurisdictions, including the United States, without necessarily complying with the relevant regulatory requirements in such jurisdictions.

To date, encouraged by limited but growing enforcement by U.S. and foreign regulators, many of these competitors have been able to operate from offshore while offering large numbers of products and services to consumers, including in the U.S., Europe, and other highly regulated jurisdictions, without complying with the relevant licensing and other requirements in these jurisdictions, and seemingly without penalty. Due to our regulated status in several jurisdictions and our commitment to legal and regulatory compliance, we have not been able to offer many popular products and services, including products and services that our unregulated or less regulated competitors are able to offer to a group that includes many of our customers, which may adversely impact our business, financial condition, and results of operations.

In recent years, our commitment to compliance and the attendant customer-facing requirements, including customer due diligence requirements, may have had a competitive impact on us as these unregulated or less compliance-focused competitors have attracted more business. We also have expended significant managerial, operational, and compliance costs to meet the legal and regulatory requirements applicable to us in the United States and other jurisdictions in which we operate, and expect to continue to incur significant costs to comply with these requirements, which these unregulated or less regulated competitors have not had to incur.

Additionally, due to the broad nature of our products and services, we also compete with, and expect additional competition from, traditional financial services companies. We also face competition from companies that may target a wider range of customers, including retail customers, which could result in such competitors gaining broader recognition and market acceptance relative to our primarily institutional customer approach.

The rapid pace of blockchain and AI innovation means that new products are constantly emerging. Keeping pace will require investment in technology adoption and development. Many innovative start-up companies and larger companies have made, and continue to make, significant investments in research and development, and we expect these companies to continue to develop similar or superior products and technologies that compete with our products. Further, more traditional financial and non-financial services businesses may choose to offer crypto-based services in the future as the digital assets industry grows and as greater legal and regulatory certainty emerges. Our current and potential competitors may establish cooperative relationships among themselves or with third parties that may further enhance their resources, or may otherwise have certain competitive advantages over us.

Our existing competitors have, and our potential competitors are expected to have, competitive advantages over us, such as:

- the ability to offer products and services that we do not support or offer (due to constraints from regulatory authorities, our banking partners, and other factors);
- greater name recognition, longer operating histories, larger customer bases, and larger market shares;
- larger sales and marketing budgets and organizations;
- more established marketing, banking, and compliance relationships;
- greater customer support resources;
- greater resources to make acquisitions;
- lower labor, compliance, risk mitigation, and research and development costs;
- larger and more mature intellectual property portfolios;
- greater number of applicable licenses or similar authorizations;

- established core business models outside of the industries that we operate in, allowing them to operate on lesser margins or at a loss;
- operations in certain jurisdictions with lower compliance costs and greater flexibility to explore new product offerings;
- substantially greater financial, technical, and other resources;
- more efficient hardware;
- greater data center capabilities (for example, through adoption of proprietary technology);
- more timely introduction of new technologies;
- preferred relationships with suppliers, including of hardware for HPC solutions and other equipment;
- better access to more competitively priced power;
- greater reliability in electricity supply and cooling resources, whether as a result of a greater number of backup sources of power or otherwise; and
- more reliable internet connections as a result of the location of their data centers to key internet connections.

If we are unable to compete successfully, or if competing successfully requires us to take costly actions in response to the actions of our competitors, our business, operating results, and financial condition could be adversely affected.

Due to the unregulated nature and lack of transparency surrounding the operations of many digital asset trading platforms, they may experience fraud, security failures or operational problems, which may adversely affect the value of digital assets traded on those digital asset trading platforms and decentralized finance protocols and, consequently, our investments and our Class A common stock.

Digital asset trading platforms and decentralized finance protocols are relatively new and, in some cases, unregulated. Furthermore, while some digital asset trading platforms provide information regarding their ownership structure, management teams, private key management, hot/cold storage policies, capitalization, corporate practices and regulatory compliance, many other digital asset trading platforms do not. A lack of transparency provided could result in us underestimating the risk of a potential loss in balances, which could include the loss of a material portion of the value of the digital assets we own or invest in on such digital asset trading platforms. Digital asset trading platforms do not appear to be subject to regulation in a similar manner as other regulated trading platforms, such as national securities exchanges or designated contract markets. As a result, the marketplace may lose confidence in the less transparent or unregulated digital asset trading platforms, including prominent digital asset trading platforms that handle a significant volume of trading in these assets.

Many digital asset trading platforms are unlicensed, unregulated, operate without extensive supervision by governmental authorities, and do not provide the public with significant information regarding their ownership structure, management team, corporate practices, cybersecurity, and regulatory compliance. In particular, those located outside the United States may be subject to significantly less stringent regulatory and compliance requirements in their local jurisdictions. As a result, trading activity on or reported by these digital asset trading platforms is generally significantly less regulated than trading in regulated U.S. securities and derivatives markets, and may reflect behavior that would be prohibited in regulated U.S. trading venues. Additionally, some of these non-U.S. digital asset trading platforms offer customers high leverage and/or a small or no insurance fund, which could result in potential losses being socialized to customers and a reduction in the value of our assets on digital asset trading platform.

We do not insure the digital assets that we hold. While our third-party custodians have indicated to us that they maintain insurance coverage that is intended to cover losses of the digital assets they custody on behalf of their clients to some extent, there can be no assurance that the loss of any digital asset is at all or fully insured against, and we may have limited rights of legal recourse in the event of loss caused by a third party. Consequently, a loss may be suffered with respect to our digital assets that is not covered by insurance and for which no person is liable for damages. For example, in 2021 there were reports claiming that over 70% of bitcoin trading volume on digital asset trading platforms was falsified or non-economic in nature, with specific focus on unregulated digital asset trading platforms located outside of the United States. Such reports may indicate that the bitcoin exchange market is significantly smaller than expected and that the United States makes up a significantly larger percentage of such market than is commonly understood. Nonetheless, any actual or perceived false trading in digital asset trading platforms, and any other fraudulent or manipulative acts and

practices, could adversely affect the value of digital assets and/or negatively affect the market perception of such assets. Further, a number of digital asset trading platforms, including certain digital asset trading platforms with which we engage, do not obtain or perform comprehensive Services Organization Controls (“SOC”) 1 and SOC 2 evaluations of their systems on a regular basis, if at all. SOC 1 evaluations of a digital asset trading platform assess whether transactions are properly secured and segregated, and that the information provided to traders and investors is complete, accurate and timely. SOC 2 evaluations assess the design and implementation of a digital asset trading platform’s security, availability, and confidentiality controls. Moreover, there are two types of such SOC evaluations: type 1 evaluates the processes at a particular point in time, while type 2 evaluations can test that the system controls across both the platform and its custody products, if applicable, have been operating effectively over a period of time. If digital asset trading platforms do not perform SOC evaluations, we may be unable to confirm that such platforms’ financial reporting is accurate or whether it has taken proper steps to secure its information technology infrastructure against internal and external threats, which could expose us to additional risks that may have been identified and remediated had such platforms obtained or performed SOC evaluation. Engaging with such digital asset trading platforms and decentralized finance protocols could materially impact our reputation and the actual or perceived security of our investments. Any engagement with digital asset trading platforms that do not obtain or perform SOC examinations exposes us to greater risks than companies that engage solely with digital asset trading platforms that maintain thorough SOC examination processes. As of September 30, 2025, we held approximately \$1.8 billion in digital assets at digital asset trading platforms and decentralized finance protocols or custodians that do not have service organization controls reporting available. In addition, over the past several years, some digital asset trading platforms have been closed due to fraud and manipulative activity, business failure or security breaches. In many of these instances, the customers of such digital asset trading platforms were not compensated or made whole for the partial or complete losses of their account balances or were made whole in dollar terms that did not enable customers to benefit from the market value growth of the original digital asset balances. For example, in November 2022, FTX—which was at the time one of the world’s largest and most popular digital asset trading platforms—became insolvent, and it was revealed that the platform had been misusing customer assets. While smaller digital asset trading platforms are less likely to have the infrastructure and capitalization that make larger digital asset trading platforms more stable, larger digital asset trading platforms are more likely to be appealing targets for hackers and malware and may be more likely to be targets of regulatory enforcement action.

Negative perception, a lack of stability in these digital asset trading platforms, fraud or misconduct, and the temporary or permanent closure of such trading platforms due to fraud, business failure, hackers or malware, or government-mandated regulation may reduce confidence in the digital asset marketplace in general and result in a reduction in the value of our assets and greater volatility in the price of digital assets (including bitcoin), as well as increase scrutiny on our activities and increase the likelihood of unfavorable government regulation and the risks of litigation against us. These potential consequences could materially and adversely affect the profitability of our bitcoin mining operations, our investment and trading strategies, the value of our assets and the value of any investment in us and, therefore, the market price of our Class A common stock.

In the event that our employees, contractors or any of our affiliates engage in misconduct or commit errors, it may materially adversely impact our business, operating results and our reputation.

Misconduct or error by our employees or our business partners could subject us to legal liability, financial losses, and regulatory sanctions and could seriously harm our reputation and negatively affect our business. Such misconduct could include engaging in improper or unauthorized transactions or activities, misappropriation of customer funds, insider trading and misappropriation of information, failing to supervise other employees or service providers, improperly using confidential information, as well as improper trading activity such as spoofing, layering, wash trading, manipulation and front-running.

Galaxy’s reputation is critical to maintaining and developing relationships with existing and prospective investors, as well as the numerous third parties with which the Company or a client does business. In recent years, there have been a number of highly publicized cases involving fraud, conflicts of interest or other misconduct by individuals in the financial services industry, and in particular the digital assets sector, and there is a risk that an employee of or contractor to the Company or any of its affiliates could engage in misconduct that adversely affects the investment strategies implemented by the Company, or that an employee or contractor of a service provider could engage in such misconduct. It is not always possible to deter such misconduct, and the precautions the Company (or any service provider) takes to detect and prevent such misconduct may not be effective in all cases. Misconduct by such individuals, or even unsubstantiated allegations of such misconduct, could result in both direct financial harm to the Company and a client, as well as harm to the reputations of the Company and the client, or, in certain circumstances, lead to increased skepticism of the digital asset markets generally, which would have a materially adverse effect on a client.

The inappropriate and/or unauthorized use of social media platforms, including weblogs (or blogs), social media websites and other forms of internet-based communications, which allow individuals access to a broad audience of consumers and other interested persons by our clients or employees could increase our costs, cause damage to our brand, lead to litigation or result in information leakage. In addition, negative or inaccurate posts or comments about us on any social networking platforms could damage our reputation, brand image and goodwill. Despite our efforts to clearly define our mission and strategy and accurately characterize our products and service offerings, our employees, contractors or affiliates may engage in activities either in their official capacity as members of the Galaxy ecosystem, or in their unofficial capacities, that are in conflict with or are incongruent with Galaxy's values, positions or strategies. Any instance of such discontinuity could negatively impact our client and/or counterparty relationships, our reputation and the market price of our Class A common stock or otherwise have a materially adverse effect on a client.

Employee or service provider errors, including mistakes in executing, recording, or processing transactions for customers, could expose us to the risk of material losses even if the errors are detected. Although we have implemented processes and procedures and provide trainings to our employees and service providers to reduce the likelihood of misconduct and error, these efforts may not be successful. There may be confusion among employees, business partners and service providers, particularly in a fast growth company like ours, with respect to compliance obligations, particularly including confidentiality, data access, trading, and conflicts.

Moreover, we frequently engage in a wide variety of transactions and maintain relationships with a significant number of projects in the industries in which we operate, including the blockchain technology sector, their developers, members of their ecosystem, and investors. These transactions and relationships could create potential conflicts of interest in management decisions that we make. For instance, certain of our officers, directors, and employees may be active investors in crypto projects themselves, and may make investment decisions in respect of projects that they have personally invested in.

It is not always possible to deter misconduct, and the precautions we take to prevent and detect this activity may not be effective in all cases. If we were found to have not met our regulatory oversight and compliance and other obligations, we could be subject to regulatory sanctions, financial penalties, and restrictions on our activities for failure to properly identify, monitor and respond to potentially problematic activity and seriously damage our reputation. Our employees, contractors, and agents could also commit errors that subject us to financial claims for negligence, as well as regulatory actions, or result in financial liability. Further, allegations by regulatory or criminal authorities of improper trading activities could affect our brand, reputation and credibility of our Company may be adversely affected.

We or our subsidiaries and affiliates are and may continue to be subject to substantial litigation, including individual and class action lawsuits, and regulatory risks.

We may be party to lawsuits and legal proceedings in the ordinary course of business. These matters are often expensive and disruptive to normal business operations. We have faced, currently face, and may from time to time face allegations, lawsuits, regulatory inquiries, actions, requests, audits or investigations including with regards to contractual disputes with our business partners and other service providers, disputes with our clients and customers, disputes with our employees, agents or affiliates and data privacy, data security, or intellectual property infringement disputes. As an enterprise whose material business lines include financial services, we or our subsidiaries and affiliates, depend to a significant extent on our relationships with our clients and counterparties and our reputation for integrity and high-caliber professional services. As a result, if a client is not satisfied with our services, a counterparty has a dispute or if there are allegations of improper conduct by private litigants or regulators, whether the ultimate outcome is favorable or unfavorable to us, or if there is negative publicity and press speculation about us, whether or not valid, our reputation may be harmed and may be more damaging to our businesses than to businesses in other non-financial industries.

We or our subsidiaries and affiliates have been and could be the subject of any number of inquiries, investigations, lawsuits and proceedings by counterparties, clients, other third parties and regulatory and other governmental agencies in the United States and abroad, which could lead to increased expenses and harm to our reputation, business, financial condition and the market price of our Class A common stock. Responding to inquiries, investigations, lawsuits and proceedings, regardless of the ultimate outcome of the matter, is time-consuming and expensive and can divert the attention of senior management. Adverse outcomes with respect to allegations, lawsuits, regulatory inquiries, audits, or investigations may result in significant settlement costs or judgments, penalties and fines, or require us to modify our services or require us to stop serving certain customers or geographies, any of which could negatively impact our business. The outcome of such proceedings, and the related expenses, may be difficult to predict or estimate until late in the proceedings, which may last a number of years and be costly for us to maintain.

For example, in December 2022, a proposed class action was filed in the Ontario Superior Court of Justice against GDH Ltd., our CEO and our former Chief Financial Officer asserting various claims including alleged misrepresentations relating to our public disclosure regarding investments and trading in the LUNA digital asset. The class action seeks unspecified damages and various declaratory relief, including leave to proceed with the right of action for misrepresentation under statutory securities provisions. These proceedings are still in early stages and have not been certified to proceed as a class action. The plaintiff's motion for leave and certification is scheduled to be heard in April 2026.

In addition, on March 27, 2025, Galaxy reached an agreement with the New York State Attorney General to resolve certain civil claims relating to certain investments, trading, and public statements made in connection with the LUNA digital asset from late 2020 to 2022. Under the terms of the settlement, Galaxy (i) accrued a legal provision of \$149.4 million as of September 30, 2025 (the undiscounted amount of which is \$160 million, payable on a pre-determined schedule over the course of four years) and (ii) has agreed to, among other things, compliance enhancements related to public statements about cryptocurrency and purchases and sales of cryptocurrency.

If Galaxy fails to comply with the terms of that agreement or violates applicable laws, the office of the New York State Attorney General may commence a subsequent investigation, civil action, or proceeding to enforce the agreement, for violations of the agreement, or for other violations, which may result in further settlement costs or judgments, penalties and fines, or require us to modify our services or require us to stop serving certain customers or geographies, any of which could negatively impact our business. Further, the agreement with the New York State Attorney General may have an impact on other current or contemplated litigation. The agreement may also result in stricter oversight or scrutiny of our business and operations by other regulators (in the form of further allegations, lawsuits, regulatory inquiries, actions, requests, audits or investigations).

The scope, determination, and impact of claims, lawsuits, government and regulatory investigations, enforcement actions, disputes, and proceedings to which we are subject cannot be predicted with certainty, and may result in:

- substantial payments to satisfy judgments, fines, or penalties;
- substantial outside counsel legal, advisor and consultant fees and costs;
- additional compliance and licensure requirements;
- the imposition of independent monitors or consultants;
- loss or non-renewal of existing licenses or authorizations, or prohibition from or delays in obtaining additional licenses or authorizations, required for our business;
- loss of our ability to conduct business in certain jurisdictions;
- increased regulatory scrutiny of our business;
- loss of productivity and high demands on employee time;
- criminal sanctions or consent decrees;
- termination of certain employees, including members of our executive team;
- barring of certain employees from participating in our business in whole or in part;
- orders that restrict our business or prevent us from offering certain products or services;
- changes to our business model and practices;
- delays to planned transactions, product launches or improvements; and
- damage to our brand and reputation.

Certain of our subsidiaries are subject to periodic examination by regulatory authorities. If compliance failures or other violations are found during an examination, a regulatory agency could initiate actions and impose sanctions for violations, including, for example, regulatory agreements, cease and desist orders, civil monetary penalties or termination of a license and could lead to litigation by investors or clients, any of which could adversely impact us.

If we and/or any governmental agency believe that we have accepted capital contributions by, or are otherwise holding assets of, any person or entity that is acting directly or indirectly, in violation of U.S., international or other anti-money laundering laws, rules, regulations, treaties or other restrictions, or on behalf of any suspected terrorist or terrorist organization, suspected drug trafficker or senior foreign political figure(s) suspected in engaging in foreign corruption, we and/or such governmental agency may “freeze the assets” of such person or entity. We may also be required to report and remit or transfer those assets to a governmental agency.

We are also subject to the risk of claims under applicable U.S. securities laws. Volatility in our stock price increases the risk of such claims. Actions against us could be brought by sizable classes of customers who may claim large monetary damages, even if the alleged per-customer harm is small or non-existent. Regardless of the outcome, any such matters can have an adverse impact, which may be material, on our business, operating results, or financial condition because of legal costs, diversion of management resources, reputational damage, and other factors.

For more information about litigation matters and other regulatory and legal proceedings in which we are involved, see “Item 1. Legal Proceedings.”

If we cannot keep pace with rapid industry changes to provide new and innovative products and services, the use of our products and services, and consequently our revenue, could decline, which could adversely impact our business, operating results, and financial condition.

The industries in which we operate have been characterized by many rapid, significant, and disruptive products and services in recent years. These include decentralized applications, which allow yield farming, staking, token wrapping, governance tokens, innovative programs to attract customers such as transaction fee mining programs, initiatives to attract traders such as trading competitions, airdrops and giveaways, staking reward programs, and novel cryptocurrency fundraising and distribution schemes. We expect new services and technologies to continue to emerge and evolve, which may be superior to, or render obsolete, the products and services that we currently provide. We cannot predict the effects of new services and technologies on our business. However, our ability to grow our customer base and revenue will depend in part on our ability to innovate and create successful new products and services, both independently and in conjunction with third parties. In particular, developing and incorporating new products and services into our business may require substantial expenditures, take considerable time, and ultimately may not be successful. Any new products or services could fail to attract customers, generate revenue, or perform or integrate well with third-party applications and platforms. In addition, our ability to adapt and compete with new products and services may be inhibited by regulatory requirements and general uncertainty in the law, constraints by our banking partners and payment processors, third-party intellectual property rights, or other factors. Moreover, we must continue to enhance our technical infrastructure and other technology offerings to remain competitive and maintain a platform that has the required functionality, performance, capacity, security, and speed to attract and retain customers. We are entering into the AI/HPC data center market, and as a result, we expect to expend significant costs and expenses to develop and upgrade our technical infrastructure to meet the evolving needs of the industry, including in connection with the conversion of our Helios mining campus to AI/HPC data center infrastructure and operations. Our success will depend on our ability to develop and incorporate new offerings and adapt to technological changes and evolving industry practices. If we are unable to do so in a timely or cost-effective manner, our business and our ability to successfully compete, retain existing customers, and attract new customers may be adversely affected.

We are exposed to a concentration of assets in a particular asset class, which could increase volatility, investment and market risk.

We primarily trade, invest, advise on and hold digital assets and investments in the blockchain space and conduct related businesses. We may accumulate significant positions in, or otherwise have significant exposure to, a single digital asset or asset type. If we choose to invest in concentrated positions, we could increase the volatility of investment results over time and exacerbate the risk that a loss in any position would have a material and adverse effect on our investment and trading strategies, the value of our assets and the value of any investment in us.

We are exposed to significant market risk based on our positions in digital assets, securities, commodities and other assets. The prices or values of digital and non-digital assets in which we may invest or trade have been, and likely will continue to be, highly volatile. We are also subject to the risk of loss of any cash or digital assets that we hold on digital asset trading platforms. For example, on November 8, 2022, FTX, a digital asset trading platform on which we held cash and digital assets, suspended customer withdrawals. FTX subsequently filed for Chapter 11 bankruptcy protection on November 11, 2022. As of December 31, 2022, we had a net loss of approximately \$68 million related to our previously disclosed FTX exposure. The Company subsequently repurchased its FTX bankruptcy claims for \$18.5 million and recorded unrealized gains of \$26.4 million during the year ended December 31, 2023. We divested these claims during the year ended December 31, 2024. Events such as these within the digital asset industry are continuing to develop and it is not

possible to predict at this time all of the risks that they may pose to Galaxy, our service providers or to the digital asset industry as a whole. Sustained market declines and periods of significant market volatility may limit our ability to produce positive investment and trading results, and there can be no assurance that our strategies will be successful in the markets and assets in which we invest or trade.

Our business relies on third-party service providers and subjects us to risks that we may not be able to control or remediate.

Our operations could be interrupted if our third-party service providers experience operational or other systems difficulties, terminate their services or fail to comply with regulations. We outsource some of our operational activities and accordingly depend on relationships with many third-party service providers. Specifically, we rely on third parties for certain services, including, but not limited to, legal, accounting, custodial and other financial operations, trade related activity, IT infrastructure and systems, trade reconciliation, and margin and collateral movement. Our business depends on the successful and uninterrupted functioning of our information technology and telecommunications systems and third-party service providers. The failure of these systems, a cybersecurity breach involving any of our third-party service providers or the termination or change in terms of a third-party software license or service agreement on which any of these systems is based could interrupt our operations. Because our information technology and telecommunications systems interface with and depend on third-party systems, we could experience service denials if demand for such services exceeds capacity or such third-party systems fail or experience interruptions. Replacing vendors or addressing other issues with our third-party service providers could entail significant delay, expense and disruption of service. As a result, if these third-party service providers experience difficulties, are subject to cybersecurity breaches, or terminate their services, and we are unable to replace them with other service providers, particularly on a timely basis, our operations could be interrupted. If an interruption were to continue for a significant period, our business, financial condition and results of operations could be adversely affected. Should we be required to replace third-party service providers, it may be at a higher cost to us, which could adversely affect our business, financial condition and results of operations.

We host certain of our mining equipment at third-party data centers. The providers oversee maintenance, up-time and other important elements of mining productivity. There is a service agreement that guarantees hash rate performance and system up-time and contractual consequences if the hosts do not meet these requirements. To the extent that a host does not meet these requirements for extended periods of time, the revenue from this business could be less than anticipated. Additionally, to the extent power costs increase, it could affect the future profitability of the business.

Unexpected market disruptions may cause major losses for us.

We may incur major losses in the event of disrupted markets and other extraordinary events in which market behavior diverges significantly from historically recognized patterns. The risk of loss in such events may be compounded by the fact that in disrupted markets, many positions become illiquid, making it difficult or impossible to close out positions against which markets are moving. Market disruptions caused by unexpected political, military and terrorist events may from time to time cause dramatic losses for us. Any such disruptions and events may have a material and adverse effect on our investment and trading strategies and on any investment in us.

Operational risk may materially and adversely affect our performance and results and we may not be effective in mitigating any such risk.

Any issue or adverse circumstance surrounding our operational risks may have a material and adverse effect on our performance and results. Operational risk is the risk of an adverse outcome resulting from inadequate or failed internal processes, people, systems or from external events. Our exposure to operational risk arises from routine processing errors, as well as extraordinary incidents, such as major systems failures or legal and regulatory matters. As we operate trading, lending, investment and other businesses that are reliant on both technology and human expertise and execution, we are exposed to material operational risk arising from a number of factors, including, but not limited to, human error, processing and communication errors, errors of our service providers, counterparties or other third parties, failed or inadequate processes and technology or system failures.

Digital asset transfers are typically not reversible without the consent and active participation of the recipient of the transaction. Once a transaction has been verified and recorded in a block that is added to the blockchain, an incorrect transfer or theft of digital assets generally will not be reversible and we may not be capable of seeking compensation for any such transfer or theft. Although we have processes and procedures in place to limit any such transfers, it is possible that, through computer or human error, or through theft or criminal action, our digital assets could be subject to these operations errors and transferred from our accounts in incorrect amounts, or to unauthorized third parties, or to uncontrolled accounts. To the extent that our business lines expand to include trust companies, custody services will expose

us to greater risk of loss from irreversible operational errors, such as collateral transferred from a custody account in incorrect amounts or to unauthorized third parties, or to uncontrolled accounts. Operational errors or significant operational delays could materially negatively impact our ability to conduct our business or service our clients, which could adversely affect results of operations due to potentially higher expenses and lower revenues, create liability for us or our clients or negatively impact our reputation. Recurring operational issues may raise concerns among regulators regarding our governance and control environment.

We seek to mitigate risk and have established policies responsive to the types of risk to which we are subject, including operational risk, credit risk, market risk, counterparty risk, exchange risk and liquidity risk. However, there are inherent limitations to our current and future risk management strategies, including risks that we have not appropriately anticipated or identified. Accurate and timely enterprise-wide risk information is necessary to enhance management's decision-making in times of crisis. If our risk management framework proves ineffective or if our enterprise-wide management information is incomplete or inaccurate, we could suffer unexpected losses, which could materially adversely affect our business, results of operations and financial condition. We continually assess our risk profile and risk management processes across the firm to identify opportunities for improvement and to consider whether we need to address new technologies and innovations in our risk management processes and policies. While we have not identified any material gaps with respect to recent digital asset market events, we cannot guarantee that our risk management processes will continue to be effective in preventing or mitigating losses from future market events.

Our expansion into the AI/HPC data center business will require substantial additional capital. We may be unable to obtain additional financing for this or for other areas of business development on acceptable terms or at all.

The conversion of our Helios campus or any future campus to AI/HPC data center development and operations will be capital-intensive projects that will require substantial additional capital to complete. Furthermore, continued development in other areas of our business may require additional financing. The failure to raise or procure such additional funds when needed or the failure to achieve or maintain positive cash flow could result in the delay or indefinite postponement of our AI/HPC data center development or our other business objectives. There can be no assurance that additional capital or other types of financing will be available if needed or that, if available, will be on terms acceptable to us. If additional funds are raised by offering equity securities or equity-linked securities, existing shareholders could suffer significant dilution. We may require additional financing to fund our operations in certain periods until positive cash flow is achieved.

We may not be able to generate sufficient cash to service all of our indebtedness and may be forced to take other actions to satisfy our obligations under our indebtedness, which may not be successful.

Our ability to make scheduled payments on or refinance our debt obligations depends on our financial condition and operating performance, which are subject to prevailing economic and competitive conditions and to certain financial, business, legislative, regulatory and other factors beyond our control. We may be unable to maintain a level of cash flows from operating activities sufficient to permit us to pay the principal, premium, if any, and interest on our indebtedness.

If our cash flows and capital resources are insufficient to fund our debt service obligations, we could face substantial liquidity problems and could be forced to reduce or delay investments and capital expenditures or to dispose of material assets or operations, seek additional debt or equity capital or restructure or refinance our indebtedness. We may not be able to effect any such alternative measures, if necessary, on commercially reasonable terms or at all and, even if successful, those alternative actions may not allow us to meet our scheduled debt service obligations. Agreements relating to our future indebtedness may also restrict our ability to raise debt or equity capital to be used to repay other indebtedness when it becomes due. We may not be able to obtain proceeds in an amount sufficient to meet any debt service obligations then due.

Our inability to generate sufficient cash flows to satisfy our debt obligations, or to refinance our indebtedness on commercially reasonable terms or at all, would materially and adversely affect our financial position and results of operations and our ability to satisfy our obligations under our indebtedness.

If we cannot make scheduled payments on our debt, we will be in default and holders of our indebtedness could declare all outstanding principal and interest to be due and payable, and we could be forced into bankruptcy, liquidation or reorganization, and our assets would be used to satisfy obligations with respect to such indebtedness before any payment could be made to you as a holder of shares of our Class A common stock. In addition, we may incur substantial additional indebtedness, including secured indebtedness. The terms of the indentures governing the Exchangeable Notes do not restrict us from incurring additional indebtedness. If new debt or other liabilities are added to our current debt levels, the related risks could intensify.

The Project Financing Documents contain certain financial and other covenants that may limit our operating flexibility. The violation of one or more of these covenants could result in an event of default, which, if not cured or waived, could result in our being required to repay these borrowings before their due date or in the need to refinance.

On August 15, 2025, Galaxy Helios I entered into the Project Financing Documents. Subject to customary exceptions, the Project Financing Documents contain certain limitations on the ability of Galaxy Helios I to engage in certain activities, including incurring indebtedness and liens, making investments, entering into affiliate transactions and undergoing fundamental changes. The Project Financing Documents also contain a financial maintenance covenant, requiring Galaxy Helios I to maintain a minimum debt service coverage ratio of 1.40 beginning with the first full quarter after Stabilization (as defined in the Credit Agreement) and a maximum loan-to-cost ratio of 80% on the closing date and each fiscal quarter thereafter until Stabilization. GDH LP is required to maintain tangible net worth of at least the Loan Amount tested on a quarterly basis and to maintain liquidity of at least 10% of the aggregate outstanding Loan Amount at all times (reduced to 5% upon satisfaction of certain conditions).

The Project Financing Documents contain customary events of default, including, without limitation, payment defaults, covenant defaults, breaches of certain representations and warranties, cross defaults to certain indebtedness, certain events of bankruptcy and insolvency, certain judgments, change of control, certain ERISA events, the termination of certain contracts, the misuse of funds and the invalidity of the loan documents.

The terms of any future indebtedness we may incur could include similar or more restrictive covenants. We cannot ensure that we will be able to maintain compliance with these covenants in the future and, if we fail to do so, that we will be able to obtain waivers from the lenders and/or amend the covenants.

Our failure to comply with the restrictive or financial covenants described above as well as the terms of any future indebtedness could result in an event of default, which, if not cured or waived, could result in our being required to repay these borrowings before their due date. If we are forced to refinance these borrowings on less favorable terms or are unable to refinance these borrowings, our business, operating results, financial condition, and prospects could be materially adversely affected.

Because our long-term success depends, in part, on our ability to expand our sales to customers outside the United States, our business is susceptible to risks associated with international operations.

We currently have subsidiaries and operations in jurisdictions such as the Cayman Islands, the U.K., Hong Kong, Canada, Israel, the Bahamas and Japan as well as the United States. We plan to enter into or increase our presence in additional markets around the world, and any inability or failure to adequately exploit opportunities for international expansion, may harm our business and our adversely affect our revenue. We have a limited operating history outside North America, and our ability to manage our business and conduct our operations internationally requires considerable management attention and resources and is subject to particular challenges of supporting a rapidly growing business in an environment of diverse cultures, languages, customs, tax laws, legal systems, alternate dispute systems and regulatory systems. As we continue to expand our business and customer base outside the United States, we will be increasingly susceptible to risks associated with international operations. These risks and challenges include:

- difficulty establishing and managing international operations and the increased operations, travel, infrastructure and legal and compliance costs associated with locations in different countries or regions;
- the need to understand and comply with local laws, regulations and customs in multiple jurisdictions, including laws and regulations governing broker-dealer practices, some of which may be different from, or conflict with, those of other jurisdictions, and which might not permit us to operate our business or collect revenues in the same manner as we do in such other jurisdictions;
- our interpretations of local laws and regulations, which may be subject to challenge by local regulators;
- difficulties or delays in obtaining and/or maintaining the regulatory permissions, authorizations, licenses or consents that may be required to offer certain products in one or more international markets;
- difficulties in managing multiple regulatory relationships across different jurisdictions on complex legal and regulatory matters;
- if we were to engage in any merger or acquisition activity internationally, this is complex and would be new for us and subject to additional regulatory scrutiny;

- the need to vary products, pricing and margins to effectively compete in international markets;
- the need to adapt and localize products for specific countries, including obtaining rights to third-party intellectual property used in each country;
- increased competition from local providers of similar products and services;
- the challenge of positioning our products and services to meet a demand in the local market (also known as “product-market fit”);
- the ability to obtain, maintain, protect, defend and enforce intellectual property rights abroad;
- the need to offer customer support and other aspects of our offering (including websites, articles, blog posts and customer support documentation) in various languages;
- compliance with anti-bribery laws, such as the Foreign Corrupt Practices Act and equivalent anti-bribery and anti-corruption requirements in local markets, by us, our employees and our business partners, and the potential for increased complexity due to the requirements on us as a group to follow multiple rule sets;
- complexity and other risks associated with current and future legal requirements in other countries, including laws, rules, regulations and other legal requirements related to cybersecurity and data privacy frameworks and labor and employment laws;
- the need to enter into new business partnerships with third-party service providers in order to provide products and services in the local market, which we may rely upon to be able to provide such products and services or to meet certain regulatory obligations;
- varying levels of internet technology adoption and infrastructure, and increased or varying network and hosting service provider costs and differences in technology service delivery in different countries;
- fluctuations in currency exchange rates and the requirements of currency control regulations, which might restrict or prohibit conversion of other currencies into U.S. dollars;
- taxation of our international earnings and potentially adverse tax consequences due to requirements of or changes in the income and other tax laws of the United States or the international jurisdictions in which we operate, as well as the impact of tariffs; and
- political or social unrest or economic instability in a specific country or region in which we operate.

We have limited experience with international regulatory environments and market practices, and we may not be able to penetrate or successfully operate in the markets we choose to enter. In addition, we may incur significant expenses as a result of our international expansion, and we may not be successful. We may launch products that lack local product-market fit, face local competition from pre-existing companies offering similar products and/or face limited brand recognition in certain parts of the world, any of which could lead to non-acceptance or delayed acceptance of our products and services by customers in new markets. Product adoption and growth rates may vary significantly across different markets. We are subject to income taxes and other taxes in the United States and other countries in which we transact or conduct business, and such laws and tax rates vary by jurisdiction. We are subject to review and audit by U.S. federal, state, local and non-U.S. tax authorities. Such tax authorities may disagree with tax positions we take, and if any such tax authority were to successfully challenge any such position, our financial condition or results of operations could be materially and adversely affected. Our failure to successfully manage these risks, or any failure to quickly exploit any opportunity for international expansion could harm our international operations in the markets we choose to enter and have an adverse effect on our business, financial condition and results of operations.

Fluctuations in currency exchange rates could harm our operating results and financial condition.

Revenue generated and expenses incurred from our international operations are often denominated in the currencies of the local countries. Accordingly, changes in the value of foreign currencies relative to the U.S. dollar can affect our revenue and operating results reflected in our U.S. dollar-denominated financial statements. Our financial results are also subject to changes in exchange rates that impact the settlement of transactions in non-local currencies. As a result, it could be more difficult to detect underlying trends in our business and operating results. To the extent that fluctuations in currency exchange rates cause our operating results to differ from expectations of investors, the market price of our Class A

common stock could be adversely impacted. Even if we use derivatives to hedge exposure to fluctuations in foreign currency exchange rates, the use of such hedging activities may not offset any or more than a portion of the adverse financial effects of unfavorable movements in foreign exchange rates over the limited time the hedges are in place, and may introduce additional risks if we are unable to structure effective hedges with such instruments.

We may be adversely affected by global conflict.

The continued conflict between Ukraine and Russia and the evolving conflict in the Middle East is likely to continue to create, impacts on global economic markets that are unpredictable. Furthermore, certain Galaxy operations are headquartered in Israel, with primary offices located in Tel Aviv. Approximately 60 Galaxy employees are physically located in Israel, a number of whom have military reserve service obligations. There has been no material impact from the ongoing conflict in the Middle East on our operations in the region. Galaxy management is monitoring the situation including implementing business continuity plans to mitigate future potential risk.

Adverse developments affecting financial institutions could adversely affect our industry and business.

Adverse developments that affect financial institutions, such as events involving liquidity that are rumored or actual, have in the past and may in the future lead to bank failures and market-wide liquidity problems. For example, on March 10, 2023, Silicon Valley Bank (“SVB”), was closed by the California Department of Financial Protection and Innovation, which appointed the FDIC as receiver. Similarly, on March 12, 2023, the New York Department of Financial Services took possession of Signature Bank and appointed the FDIC as receiver of the bank. The U.S. Department of the Treasury, the Federal Reserve and the FDIC released a statement that indicated the FDIC would complete its resolution of SVB and Signature Bank in a manner that fully protects all depositors. The U.S. Department of Treasury, FDIC and Federal Reserve Board also announced a program to provide up to \$25 billion of loans to financial institutions secured by certain of such government securities held by financial institutions to mitigate the risk of potential losses on the sale of such instruments, widespread demands for customer withdrawals or other liquidity needs of financial institutions. We have in the past deposited funds with Signature Bank and Silvergate Bank. We have diverse U.S. banking relationships with most of our deposits at large, systemically important financial institutions. Although Galaxy did not experience any losses or other material impact from our banking relationships with Silvergate Bank and Signature Bank, to the extent that we have deposited funds with banking institutions that fail and are not otherwise protected, we would lose the amount of our deposits over the then current FDIC insurance limit. The loss of our deposits could reduce the amount of cash we have available to operate our business and have an adverse impact on our investment and trading strategies, the value of our assets, the value of any investment in us, financial condition and results of operations.

Risks Related to Our Business Lines

Managing different business lines could present conflicts of interest.

There are certain inherent and potential conflicts of interest in managing different business lines and the presence of any such conflict of interest could materially adversely affect our business, reputation, results of operations and financial condition. We seek to build a full service, institutional-quality financial services business through our two operating business segments: Digital Assets and Data Centers. Subject to applicable regulatory approvals, we may also launch additional business lines from time to time. Due to the broad scope of our businesses, potential conflicts of interest include situations where our services to a particular client or our own investments or other interests conflict, or are perceived to conflict, with the interests of another client, as well as situations where one or more of our businesses have access to material non-public information that may not be shared with our other businesses and situations where we may be an investor or creditor of an entity with which we also have an advisory or other relationship. For example, our subsidiaries may provide corporate advisory services to companies that are also investee companies of our asset management business or within our venture portfolio. In such circumstances, we may not be able to conduct transactions relating to investments in portfolio companies, for example, due to the inability of our asset management business to use to material non-public information in buying or selling securities to us. In ordinary course of business, we may also make loans to protocols and receive the native token as collateral. Accordingly, there may be situations where we are compelled or forced to liquidate the token even though we may have investments in such protocol or token, or other relationships across the Company. Furthermore, the allocation of investment opportunities among us, our funds and our clients could also present conflicts of interest. Providing custody services while managing other funds and accounts can present certain conflicts of interest as those funds and accounts might have similar or different investment objectives or strategies as trust accounts, or otherwise hold, purchase or sell investments that are eligible to be held, purchased or sold by the trust accounts, or may take positions that are opposite in direction from those taken by the trust accounts. In managing these different conflicts, fiduciary duty obligations may require us to resolve conflicts in favor of clients over our Company or other third parties. For example, our asset management business may be engaged to provide advice to a client that is considering entering into a transaction with

us, and may advise the client not to pursue the transaction with us, or otherwise in connection with a potential transaction provide advice to the client that would be adverse to us. Employees and executives, including our Founder, may also have conflicts of interest in allocating their time and activity between the business lines. While we manage conflicts of interest through a number of ways, appropriately identifying and dealing with conflicts of interest is complex and difficult, and our reputation could be damaged and the willingness of clients to enter into transactions with us may be affected if we fail, or appear to fail, to identify, disclose and deal appropriately with conflicts of interest. In addition, potential or perceived conflicts, or the failure to make appropriate disclosures to clients regarding such conflicts, could give rise to litigation or regulatory enforcement actions. A failure to appropriately identify and address potential conflicts of interest could adversely affect our businesses, results of operations and financial condition.

Changes in the value levels of the assets may cause our AUM, revenue and earnings to decline.

Our asset management business, which is conducted through one or more subsidiaries, is primarily comprised of fees based on a percentage of the value of AUM and, in some cases, performance fees which are normally expressed as a percentage of returns to the client. Numerous factors, including price movements in the assets in the markets in which we manage assets, could cause:

- the value of AUM, or the returns that we realize on AUM, to decrease;
- the withdrawal of funds from any products offered by us in favor of products offered by competitors; or
- a decrease in the value of seed or co-investment capital or a decrease in the amount of such capital available to invest.
- Liquidation of third-party bankruptcy estate assets under mandates to do so may also reduce AUM.

The occurrence of any of these events may cause our AUM, revenue and earnings, if any, to decline and may negatively impact the success of our asset management business, results of operations and financial condition.

The asset management business is highly regulated and regulators may apply or interpret these regulations with respect to digital assets in novel and unexpected ways.

Asset management is a highly regulated business subject to numerous legal and regulatory requirements. These regulations are intended to protect customers whose assets are under management and, as such, may limit our ability to develop, expand or carry out our asset management business in the intended manner. We are guided in significant part by regulatory regimes that are not clear or are not yet developed. To the extent that there is any ambiguity as to whether an asset under management is a security, the applicability of many regulations to our asset management business will not be clear. Furthermore, we must address conflicts of interest, as well as the perception of conflicts of interest, between ourselves (including our other business lines) and our clients and funds. In particular, we are required to act in the best interest of our clients and funds, which may include allocating opportunities to our clients and funds rather than to our own principal business lines. In addition, regulators have substantial discretion in determining what is in the best interest of a client of a fund and have increased their scrutiny of potential conflicts as well as the disclosure of such conflicts to an asset manager's clients. Appropriately dealing with conflicts of interest is complex and if we fail, or appear to fail, to deal appropriately with any of these conflicts of interest, we may face reputational damage, litigation, regulatory proceedings, or penalties, fines or sanctions, any of which may have a material and negative impact on our asset management business. In addition, to the extent that we are required to obtain client or investor consent in connection with any potential conflict, any failure or delay in obtaining such consent may have a material and negative impact on our ability to take advantage of certain business opportunities.

Increased competition may cause our AUM, revenue and earnings to decline.

The asset management industry is highly competitive and has relatively low barriers to entry. We currently expect that, as digital assets become more mainstream, additional competitors, potentially in large numbers, may begin providing asset management services with respect to digital assets. We compete based on a number of factors including: investment performance, the level of fees charged, the quality and diversity of services and products provided, name recognition and reputation, and the ability to develop new investment strategies and products to meet the changing needs of investors. In addition, the introduction of new technologies, as well as regulatory changes, may significantly alter the competitive landscape for investment managers in digital assets. This could lead to fee compression or require us to spend more to modify or adapt our product offerings to attract and retain customers and remain competitive with products and services offered by new competitors in the industry. Increased competition on the basis of any of these factors, including competition leading to fee reductions, may cause our AUM, revenue and earnings to decline and materially and negatively

impact the success of our asset management business and affect our overall business, results of operations and financial condition.

Our venture investments, managed by our crypto ventures team within the Digital Assets segment, including any associated lending activities, are subject to substantial risk.

Our investments may be very risky and highly speculative and our venture investments managed by our crypto ventures team within the Digital Assets segment are subject to substantial risk, including risks related to third-party investment managers, operational risk, conflicts of interest, asset performance and regulatory compliance, that, if realized, could result in significant damage to our business and operating results.

Moreover, our due diligence processes may fail to uncover all of the problems, liabilities or other challenges, including fraud, material deficiencies, regulatory or compliance issues in connection with our prospective portfolio companies or our third-party investment managers. This could result in an increased risk of unanticipated or unknown issues or liabilities including with respect to compliance and regulatory matters, and our mitigation strategies may not be effective. Further, our valuations and projections in connection with our prospective investments may be inaccurate, which could result in a loss of all or substantially all of our investments and could adversely impact our financial condition and our business.

We generally do not take controlling equity positions in our portfolio companies. To the extent that we do not hold a controlling equity interest in a portfolio company, we are subject to the risk that a portfolio company may make business decisions with which we disagree, and the stockholders and management of a portfolio company may take risks or otherwise act in ways that are adverse to our interests. Due to the lack of liquidity for the debt and equity investments that we typically hold in our portfolio companies, we may not be able to dispose of our investments in the event we disagree with the actions of a portfolio company, and may therefore suffer a decrease in the value of our investments. Further, our portfolio companies may be highly leveraged.

Our strategy to expand into the AI/HPC data center business may not be successful and may result in adverse consequences to our business, financial condition and results of operations.

Our growth strategy includes expanding and diversifying our revenue sources into new markets and technologies, including using some of our existing bitcoin mining infrastructure for AI/HPC data center development. However, our success in this area may not develop as anticipated and may be affected by factors such as the ability to obtain sufficient financing to convert our existing bitcoin mining infrastructure to AI/HPC data center infrastructure, the expense and timing of new infrastructure development, and our initial reliance on CoreWeave as our single AI/HPC customer.

We do not have experience in developing and offering AI/HPC data center infrastructure. We may experience difficulties with the infrastructure development and modification of AI/HPC campuses, including the Helios campus, due to factors beyond our control. For example, there may be difficulties in integrating new equipment into our existing infrastructure, constraints on our ability to connect to or procure the expected electricity supply capacity at the campus, supply chain disruption (including as a result of local labor availability, severe weather, tariffs or otherwise), defects in design, construction or installed equipment, inability to procure the necessary equipment on commercially acceptable terms or at all, diversion of management resources, insufficient funding or other resource constraints, or actual costs for development may exceed our planned budget. See “—We are subject to risks in connection with our mining business and AI/HPC data center business, including risks associated with counterparties.” Our focus on developing the Helios campus and any other future campuses to offer AI/HPC data center infrastructure may also disrupt our business by diverting our resources and requiring significant management attention that would otherwise be available for utilization within, and development of, our existing businesses.

Our ability to grow our AI/HPC data center business in the future is also dependent on the overall market for AI/HPC data centers. The broader adoption, use, and commercialization of AI technology, and the continued rapid pace of developments in the AI industry, are inherently uncertain. For example, certain AI technology is under public scrutiny for creating inaccurate, incomplete or misleading content, unintended biases and other discriminatory or unexpected results, errors or inadequacies and may be, or be perceived to be, deficient, inaccurate, biased, unethical or otherwise flawed. Therefore, it is difficult to predict the demand for AI/HPC data center capacity, the size and growth rate for this market, the entry of competitive products, or the success of any existing or future products that may compete with any AI/HPC data centers we may develop. In addition, we cannot assure you that we will be able to keep up with the changing AI landscape or in developing services or infrastructure that can meet our customers’ evolving needs in a timely manner, if at all. There is an increasing number of competitors providing AI/HPC data centers, which will result in competition and pricing pressure. Meanwhile, if there is a reduction in demand for any AI/HPC data centers, whether caused by a lack of customer acceptance, a slowdown in demand for computational power, a downturn in the AI industry, an overabundance of unused

computational power, advancements in technology, technological challenges, competing technologies and solutions, decreases in corporate and customer spending, weakening economic conditions or otherwise, the growth of our AI/HPC data center business could be slowed or curtailed, or we may need to make certain changes to our Helios campus, including transitioning AI/HPC infrastructure services to other services, which could require significant and costly operational changes, impose substantial additional costs and divert management attention. For example, rapid technological advancements in the AI industry, such as developments of more efficient AI models that reduce the demand for high-end hardware and, by extension, the data centers that house them, could significantly reduce demand for AI/HPC data centers.

AI and related industries are under increasing scrutiny from regulators due to their concerns about market concentration, anti-competitive practices, and the pace of partnerships and acquisitions involving generative AI startups. As the AI industry continues to grow, transactions and business conduct will likely continue to draw scrutiny from regulators. Therefore, our investments in developing and offering AI/HPC data centers may also result in new or enhanced governmental or regulatory scrutiny, litigation, confidentiality or security risks, ethical concerns or other complications that could adversely affect our business, reputation, results of operations or financial condition.

Our AI/HPC data center business model is predicated, in part, on establishing and maintaining a customer base that will generate a recurring stream of revenues. If that recurring stream of revenues is not maintained or does not increase as expected, our operating results may be adversely affected.

We expect that our AI/HPC data center business will initially be highly dependent on a single customer, CoreWeave, and may continue to derive a significant portion of the revenue of our Data Center operating business segment from such single customer for the foreseeable future. Therefore, the success of our AI/HPC data center business will be highly dependent on our continued relationship with CoreWeave, pursuant to the terms of the Lease Agreement. Any cancellation or non-renewal of our data center business, including the Lease Agreement, in the future, could have a material adverse effect on our business, financial condition and results of operations.

Our ability to grow our AI/HPC data center business in the future will be dependent, in large part, on our ability to maintain and grow our customer base. There can be no assurances that our customer will renew or sign a further contract when its initial contract expires in 2040. In addition, our customer may terminate its agreement with us in certain circumstances, including if we fail to achieve certain milestones within the time periods prescribed therein. In addition, there is no assurance that we will be able to attract additional customers on favorable terms, if at all. Customers may prefer to enter into on-demand or other short-term arrangements with us, particularly if we are not able to compete effectively to assure potential customers as to the reliability of our AI/HPC data center infrastructure and operations. As a result, there can be no assurance that we will retain our existing customer, or that we will attract new customers that will enter into long-term service contracts with us or on contract terms that generate recurring revenue. If we are unable to successfully market our AI/HPC data center business and maintain and grow our existing customer base, then the potential success of our entry into the AI/HPC data center industry may be less than we anticipate, which could have an adverse impact on our business, prospects and operations.

We are subject to risks in connection with our mining business and AI/HPC data center business, including risks associated with counterparties.

In December 2022, we acquired the Helios campus and its bitcoin mining operations, expanding our infrastructure. In furtherance of these objectives, our mining business has procured bitcoin mining equipment to be utilized for proprietary bitcoin mining operations and resale. Our expansion into AI/HPC data center infrastructure requires equipment specifically designed for AI/HPC workloads, which typically comes from different suppliers than bitcoin mining equipment. There are a limited number of AI/HPC data center equipment suppliers in the market today, and the market price and availability of equipment can be volatile based on market supply and demand dynamics. Moreover, our suppliers themselves rely on a complex network of third-party suppliers for semiconductor manufacturing, hardware components, and other critical inputs, which introduces additional risks to our supply chain. There can be no assurance that additional supplies of AI/HPC data center equipment will be available on terms that are acceptable to us, or at all, or that any supplier would be able to provide sufficient equipment to us to meet our requirements.

Governments have limited or may limit the shipment of products in and out of their jurisdictions or impose tariffs on products, which could negatively impact our ability to receive bitcoin mining and AI/HPC data center equipment from our suppliers. Our third-party manufacturers, suppliers, sub-contractors and customers have been and will continue to be disrupted by worker absenteeism, quarantines, restrictions on employees' ability to work, office and factory closures, severe weather, disruptions to ports and other shipping infrastructure, border closures, or other travel or health-related restrictions. Depending on the magnitude of such effects on our supply chain, shipments of parts for our existing bitcoin mining and AI/HPC data center equipment, as well as any new bitcoin mining and AI/HPC data center equipment we

purchase, may be delayed. As our bitcoin mining and AI/HPC data center equipment require repair or become obsolete and require replacement, our ability to obtain adequate replacements or repair parts from the third-party manufacturers may therefore be hampered. Supply chain disruptions could therefore negatively impact our operations.

In addition, our expansion into AI/HPC is expected to be highly dependent on a single customer. The risk that such customer or any future customer of our AI/HPC data center operations may fail to renew, terminate, default on or underperform their contractual obligations would curtail the growth of our AI/HPC data center business and may adversely affect the results of our operations. For a more detailed discussion of this risk, see “—Our AI/HPC data center business model is predicated, in part, on establishing and maintaining a customer base that will generate a recurring stream of revenues. If that recurring stream of revenues is not maintained or does not increase as expected, our operating results may be adversely affected.”

Further, bitcoin mining operations can consume, and our AI/HPC data center operations are expected to consume, significant amounts of electricity. There has been increased focus on, and public debate surrounding, the negative environmental, social and governance considerations associated with such operations. For a more detailed discussion of these risks, see “—Risks Related to Regulation, Information Systems and Privacy Matters—Legislative or regulatory changes or actions in foreign jurisdictions may affect our business or restrict the use of one or more digital assets, transactions referencing digital assets, mining activity or the operation of their networks or the digital asset trading platform market in a manner that adversely affects our business” and “Risks Related to Regulation, Information Systems and Privacy Matters—If regulators or public utilities take actions that restrict or otherwise impact mining activities, there may be a significant decline in such activities, which could adversely affect digital asset networks, our business and the market price of our Class A common stock.”

Any problems accessing electricity sources or increased costs to procure power may result in adverse consequences to our business, financial condition and results of operations.

Our digital asset mining operations and our AI/HPC data center operations can consume significant amounts of electricity and are dependent on our ability to maintain reliable and economical sources of power. Our inability to secure sufficient power or any power outages, shortages, supply chain issues, capacity constraints, or significant increases in the cost of securing power could have an adverse effect on our business, operating results, financial condition, and future prospects. Specifically, our Helios campus could be, from time to time, affected by problems accessing electricity sources, such as planned or unplanned power outages and limitations on transmission or distribution of power. Unplanned power outages, including, but not limited to those relating to large storms, earthquakes, fires, tsunamis, cyberattacks, physical attacks on utility infrastructure, war, and any failures of electrical power grids more generally, and planned power outages by public utilities, could harm customers of our Data Center operating business segment, as well as our business, operating results, financial condition, and future prospects.

The global energy market is currently experiencing inflation and volatility pressures. Various macroeconomic and geopolitical factors are contributing to the instability and global power shortage, including the war in Ukraine, severe weather events, governmental regulations, government relations, and inflation. We expect the cost for power to continue to be volatile and unpredictable and subject to inflationary pressures, which could materially affect our financial forecasting, business, operating results, financial condition, and future prospects. We have undertaken certain processes, such as hedging, in order to reduce the risks of electricity price fluctuations. However, fluctuations in the prices and availability of sufficient power could affect our ability to profitably engage in our digital asset mining and AI/HPC data center operations.

The digital asset mining industry has seen rapid growth and innovation, and is becoming increasingly competitive, and our mining business may be unable to compete effectively.

The digital asset mining industry has seen rapid growth and innovation, and our mining business may be unable to compete effectively. Our mining business’ expenses may be greater than we anticipate, and our investments to make our mining business more efficient or to gain digital asset mining market share may not outpace monetization efforts. Bitcoin miners and other necessary hardware are also subject to malfunction, technological obsolescence, the global supply chain and difficulty, cost in obtaining new hardware and global energy prices. Any major malfunction out of the typical range of downtime for normal maintenance and repair could cause a significant disruption in our ability to continue mining, which could result in lower yields and harm our digital asset mining market share. New miners can be costly and may be in short supply. There can be no assurances that the most efficient mining hardware will be readily available when we identify the need for it. We face competition in acquiring mining machines from major manufacturers and, at a given time, mining machines may only be available for pre-order months in advance. As a result of competition for the latest generation mining machines, or if we unexpectedly need to replace our mining machines due to a faulty shipment or other failure, we may not be able to secure replacement machines at reasonable costs on a timely basis. Furthermore, fluctuations in global

energy prices have in the past, and may in the future, have a material impact on our mining business' operations and financial results. In particular, rising global energy prices could have a material negative impact on our mining business' profits, both directly and indirectly as a result of our exposure to counterparty risks. While our mining business intends to enter into business arrangements that allow us to hedge against global energy prices, there can be no guarantee that we are able to do so effectively, if at all.

Our mining business strategy currently focuses on mining bitcoin (as opposed to other digital assets), and our hardware is limited to mining using current "proof-of-work" protocols. There could be developments in proof-of-work protocols, or other competing validation methods or processes, that negatively impact our current business strategy or render such business strategy obsolete. Proof-of-stake is an alternative method of validating digital asset transactions on other popular blockchain networks. Proof-of-stake methodology does not rely on resource intensive calculations to validate transactions and create new blocks in a blockchain; instead, the validator of the next block is determined, sometimes randomly, based on a methodology in the blockchain software. Rewards, and sometimes penalties, are issued based on the amount of digital assets a user has "staked" in order to become a validator. Should bitcoin shift from a proof-of-work validation method to a proof-of-stake or other method, the transaction verification process (i.e., "mining" or "validating") may render our mining business materially less competitive or less profitable. In addition, in the general course of our business outside of our mining business, we participate in networks with proof-of-stake consensus algorithms, and we may earn rewards in the form of the native token of the network. Depending on the protocol, we also may permit third parties to "delegate" their digital assets to our validator. The third party earns rewards net of a commission earned by Galaxy. The value of any staked digital assets is subject to market volatility, and any such rewards we may earn as a validator could be offset by a loss in value of the staked digital assets. In addition, to the extent we participate in a proof-of-stake network but fail to remain current in any updates or upgrades to the network, we may become temporarily unable to earn rewards as a validator with respect to any staked digital assets on such network, or could have staked digital assets taken from us ("slashed"), to the extent we are deemed to be deviating from acting in the best interest of the network.

In addition, the aggregate computing power of the global Bitcoin network has generally grown over time and we expect it to continue to grow in the future. The barriers to entry for new bitcoin miners are relatively low, which can give rise to additional capacity from competing bitcoin miners. As the hash rate in the Bitcoin network increases, the amount of bitcoin earned per unit of hash rate decreases. The Bitcoin protocol responds to increasing total hash rate by increasing the "difficulty" of bitcoin mining. If this "difficulty" increases at a significantly higher rate, we would need to increase our hash rate at the same rate in order to maintain market share and generate equivalent block rewards. Therefore, in order to maintain or increase our market share, we may be required to make significant capital expenditures.

Any decrease in our mining business' effective market share would result in a reduction in our share of block rewards and transaction fees, which could adversely affect our financial performance and financial position.

If we choose to hedge our exposures, such hedging transactions may be ineffective or reduce our overall performance.

From time to time, we may use a variety of financial instruments and derivatives, such as options, swaps, and forward contracts, for risk management purposes, including to: protect against possible changes in the market value of our investment or trading assets resulting from fluctuations in cryptocurrency markets or securities markets and changes in interest rates; protect our unrealized gains in the value of our investments or trading assets; facilitate the sale of any such assets; enhance or preserve returns, spreads or gains on any trade or investment; hedge the interest-rate or currency-exchange risk on any of our liabilities or assets; protect against any increase in the price of any assets that we anticipate purchasing at a later date; or to any other end that we deem appropriate. The success of any hedging activities by us will depend, in part, on our ability to correctly assess the degree of correlation between the performance of the instruments used in the hedging strategy and the performance of the assets being hedged. Since the characteristics of many assets change as markets change or time passes, the success of our hedging strategy will also be subject to our ability to continually recalculate, readjust and execute hedges in an efficient and timely manner. In addition, while we may enter into hedging transactions to seek to reduce risk, such transactions may actually increase risk or result in a poorer overall performance for us than if we had not engaged in such hedging transactions.

We may fail to develop and execute successful investment or trading strategies.

The success of our investment and trading activities will depend on the ability of the investment team to identify overvalued and undervalued investment opportunities and to exploit price discrepancies. This process involves a high degree of uncertainty. No assurance can be given that we will be able to identify suitable or profitable investment opportunities in which to deploy our capital. The success of the trading activities also depends on our ability to remain competitive with other OTC traders and liquidity providers. Competition in trading is based on price, offerings, level of service, technology, relationships and market intelligence. The success of investment activities depends on our ability to

source deals and obtain favorable terms. Competition in investment activities is based on relationships, the ability to offer strategic advice to portfolio companies and reputation. The barrier to entry in each of these businesses is very low and competitors can easily and will likely provide similar services in the near future. The success of our venture investments and trading business could suffer if we are not able to remain competitive.

We may make, or otherwise be subject to, trade errors.

Errors may occur with respect to trades executed on our behalf. Trade errors can result from a variety of situations, including, for example, when the wrong investment is purchased or sold or when the wrong quantity is purchased or sold. Trade errors frequently result in losses, which could be material. To the extent that an error is caused by a third party, we may seek to recover any losses associated with the error, although there may be contractual limitations on any third party's liability with respect to such error.

Our trading orders may not be timely executed.

Our investment and trading strategies depend on the ability to establish and maintain an overall market position in a combination of financial instruments. Our trading orders may not be executed in a timely and efficient manner because of various circumstances, including, for example, trading volume surges or systems failures attributable to us or our counterparties, brokers, dealers, agents or other service providers. In such an event, we might only be able to acquire or dispose of some, but not all, of the components of our positions, or if the overall positions were to need adjustments, we might not be able to make such adjustments. As a result, we would not be able to achieve our desired market position, which may result in a loss. In addition, we can be expected to rely heavily on electronic execution systems (and may rely on new systems and technology in the future), which may be subject to certain systemic limitations or mistakes, causing the interruption of trading orders made by us.

The success of our investment banking business will depend on our ability to generate and maintain ongoing, profitable client demand for our services and our ability to remain competitive in the digital asset investment banking space.

The success of our investment banking business, which is conducted through Galaxy Digital Partners LLC, one of our FINRA registered broker-dealers, and Galaxy Digital Labs LLC, depends on creating and sustaining a demand for our financial and strategic advisory services with respect to the digital asset, cryptocurrency and blockchain technology sector while maintaining favorable margins. The ability to realize and maintain this demand could be negatively affected by numerous factors, many of which will be beyond our control and unrelated to our future work product.

Developments in the digital asset industry, which are expected to be rapid, could shift demand to new services and solutions. If, as a result of new technologies or changes in the industries we serve, our clients demand new services that we do not or are unable to provide, we may be less competitive in these new areas or need to make significant investment to meet that demand. Our strategy for developing our investment banking business focuses on responding to these types of developments by driving innovation that will enable us to expand our investment banking business into new growth areas. If we do not sufficiently invest in new technology and adapt to industry developments or evolve and expand our business at sufficient speed and scale, the success or even the viability of our investment banking business would be negatively affected.

We may become involved in advisory projects that are not directly related to the digital asset or blockchain industry. These projects are likely to relate to industries and clients that we believe will benefit in the future from blockchain technology and our experience and network in the digital assets industry, however there can be no assurance that any such projects are successful. Further, as our investment banking business continues to develop and evolve, especially with regards to our investments in companies operating within the digital asset industry and the blockchain technology sector generally, we could be subject to unintended or unforeseen regulatory oversight, or come into the purview of regulators who seek to target us for our role in such transactions, which could expose us to regulatory actions, which may be inconsistently applied across jurisdictions.

The success of our investment banking business may be significantly affected by our ability to price our services properly. If we are not able to obtain favorable pricing for our services, the success of our investment banking business may materially suffer. The rates we charge for our services may be affected by a number of factors, including: general economic and political conditions, the competitive environment in our industry and the procurement practices of clients and their use of third-party advisors. In particular, because Galaxy Digital Partners LLC is a broker-dealer and advises on mergers and acquisitions, we may be unable to purchase errors and omissions insurance without incurring material costs to our business. Therefore, we may become subject to a securities class-action lawsuits in connection with our advice on a public merger or acquisition and be without recourse from insurance.

The barrier to entry to digital asset investment banking services is very low and competitors can easily and will increasingly compete with our offerings. As a result, the success of our investment banking business, results of operations and financial condition could suffer if we are not able to remain competitive. The less we are able to differentiate our services and solutions or clearly convey the value of our services and solutions, the more risks we will face in winning new work in sufficient volumes and at target pricing, which could materially negatively impact the success or viability of our investment banking business. In addition, the introduction of new services or products by competitors could reduce our ability to obtain favorable pricing and impact the overall economics for the services or solutions offered.

Because of regulatory uncertainty regarding how transactions in digital assets or digital securities by broker-dealers are or should be regulated, none of our broker-dealer subsidiaries currently engage in underwriting services, private placement services, or otherwise facilitate customer transactions with respect to offerings involving digital assets, tokens, cryptocurrencies, digital securities or initial coin offerings, nor do they accept digital assets, tokens, cryptocurrencies or digital securities as payment for broker-dealer related services.

Pursuant to its membership agreement with FINRA, Galaxy Digital Partners LLC—the entity through which we operate aspects of investment banking—is authorized as a broker-dealer to engage in business relating to underwriting or selling group participation (corporate securities other than mutual funds); private placements of securities; business advisory services concerning mergers and acquisitions, debt financing, equity financing, leveraged buy-outs and distressed corporate advisory; and referrals of broker-dealers, hedge funds and investors to unaffiliated broker-dealers for order execution, clearance and settlement. Despite its focus on providing services to companies in the digital assets space, however, because of regulatory uncertainty regarding how transactions in digital assets by broker-dealers are to be regulated, Galaxy Digital Partners LLC does not currently engage in underwriting services or private placement services involving tokens, digital securities, digital assets, initial coin offerings or other digital representations of securities or property on a blockchain. As a result, because we are unable or unwilling to provide broker-dealer services to prospective clients in connection with offerings involving tokens, digital assets, digital securities, initial coin offerings or other digital representations of securities or property on a blockchain, we may face challenges in winning new work in sufficient volumes and at target pricing from new or existing clients, which could negatively impact the success or viability of our advisory services business.

FIN2, LLC (“FIN2”), the entity through which we provide retail brokerage accounts through GalaxyOne, also does not currently facilitate customer transactions in digital assets, although these are offered through GalaxyOne through a separate affiliate.

Additionally, because of regulatory uncertainty regarding how transactions in digital assets and digital securities by broker-dealers are or should be regulated, none of our broker-dealer subsidiaries currently accept cryptocurrencies, digital assets or digital securities as payment for broker-dealer services, which could negatively impact, our financial condition, profitability and results of operations if the value of such foregone digital asset consideration materially appreciates over time relative to cash consideration.

Our trading business and the various activities we undertake expose us to counterparty credit risk.

Credit risk is the risk that an issuer of a security or a counterparty on a transaction will be unable or unwilling to satisfy payment or delivery obligations when due. In addition to the risk of an issuer of a security in which we invest failing or declining to perform on an obligation under the security, we are exposed to the risk that third parties, including trading counterparties, clearing agents, trading platforms, decentralized finance protocols, clearinghouses, custodians, administrators and other financial intermediaries that may owe us money, securities or other assets will not perform their obligations. Any of these parties might default on their obligations to us because of bankruptcy, lack of liquidity, operational failure, fraud or other reasons, in which event we may lose all or substantially all of the value of any such investment or trading transaction. When we trade on digital asset trading platforms that specialize in digital asset futures and derivatives, we are exposed to the credit risk of that digital asset trading platform.

In the case of loans that are secured by collateral, while we generally expect the value of the collateral to be greater than the value of such loans, the value of the collateral could actually be equal to or less than the value of such loans or could decline below the outstanding amount of such loans. This risk is heightened given that some portion of the collateral for these loans is expected to be digital assets, and thus subject to the volatility, liquidity and other risks detailed herein. Our ability to have access to the collateral could be limited by bankruptcy and other insolvency laws. Our security interest in the collateral could be challenged under commercial laws. Under certain circumstances, the collateral could be released with the consent of the lenders or pursuant to the terms of the underlying loan agreement with the borrower. There is no assurance that the liquidation of the collateral securing a loan would generate sufficient funds to satisfy the borrower’s obligation in the event of non-payment of scheduled interest or principal, or that the collateral could be readily liquidated.

As a result, we might not receive the full payment to which we are entitled on a secured loan and thereby could experience a decline in the value of, or a loss on, the investment.

We may co-invest with third parties, including parties related to our Founder, through joint ventures or other entities. Such investments may include risks in connection with such third-party involvement, including the possibility that a third-party co-venturer may have financial difficulties, may have interests or goals that are inconsistent with ours or may be in a position to take action in a manner contrary to our investment objectives. We and our subsidiaries have loaned money to other companies as part of the balance sheet venture investment business and lending business. The return of principal of such loans will depend in large part on the creditworthiness and financial strength of the issuers of such loans. While we perform extensive due diligence on our investments and loans, nonetheless defaults are possible. In the event of a default by a borrower underlying an investment or loan, we might not receive payments to which we are entitled and thereby could experience a decline in the value of our investments in or loans to the borrower.

We may purchase and write put and call options on digital or non-digital assets. These are highly specialized activities that entail greater-than-ordinary investment risks. An uncovered call writer's loss is theoretically unlimited. Unlike exchange-traded options, which are standardized with respect to some or all of the underlying instrument, expiration date, contract size and strike price, the terms of OTC options (options not traded on exchanges) are generally established through negotiation with the other party to the option contract. While this type of arrangement allows greater flexibility to tailor an option, OTC options generally involve greater credit risk than exchange-traded options, which are typically guaranteed by a clearing organization, frequently affiliated with the exchanges on which they are traded. As of the date of this Quarterly Report on Form 10-Q, the availability of exchange-traded and OTC options on digital assets is extremely limited, so terms may be unfavorable and risks may be greater in comparison to those available for more firmly established types of options.

We may also enter into other derivatives, such as perpetual futures contracts on digital assets. These too are highly specialized activities that may pose material market and credit risks to us.

The failure or bankruptcy of any of our clearing brokers or futures commission merchants ("FCMs"), or the clearinghouses at which we clear financial transactions, could result in a substantial loss of our assets. For example, if a clearing broker fails to appropriately segregate or account for customer assets in accordance with law, customers may be subject to risk of loss of their funds in the event of that clearing broker's bankruptcy. In such an event, the clearing broker's customers, such as us, may be entitled to recover, even in respect of property specifically traceable to them, only a proportional share of all property available for distribution to all of that clearing broker's customers.

We provide certain technological solutions which are novel and may present risks.

Galaxy's self-custody technology solution licenses self-custody software technology to customers that allows customers to generate and store the private keys to their digital assets, as well as to generate multi-signature backup keys, in a secure cold storage vault. Self-custody technology is novel and complex, and as with any new technology, we may encounter technical issues, disruptions or security weaknesses. As such, there is no assurance that our self-custody technology solution will continue to perform as expected. In the event that the technology does not perform appropriately or its security is compromised, our reputation could be adversely affected. Any number of technical changes, software upgrades, cybersecurity incidents or other changes to the technology may occur or be required from time to time, and if we are unable to troubleshoot and resolve any such issues successfully, it could adversely impact our business, financial condition and results of operations.

Risks Related to Cryptocurrencies and Digital Assets

The continuing development and acceptance of digital assets and distributed ledger technology are subject to a variety of risks.

Cryptocurrencies, such as bitcoin, and the other types of digital assets in which we invest and trade involve a new and rapidly evolving industry of which blockchain technology is a prominent, but not unique, part. The growth of the digital asset industry in general, and distributed ledger technology that supports digital assets, is subject to a high degree of uncertainty. The factors affecting the further development of the digital asset industry, as well as distributed ledger technology, include:

- continued worldwide growth in the adoption and use of digital assets;
- the limited operating histories of many cryptocurrency networks, which have not been validated in production and are still in the process of developing and making significant decisions that will affect the design, supply, issuance, functionality, and governance of their respective digital assets and underlying blockchain networks;

- government and quasi-government regulation of digital assets and their use, or restrictions on or regulation of access to and operation of applicable distributed ledger technology or systems that facilitate their issuance and secondary trading;
- the taxation, and tax-related reporting, of transactions involving digital assets by the United States and other jurisdictions;
- the maintenance and development of the open-source software protocols of certain blockchain networks used to support digital assets;
- advancements in technology, including computing power, that may adversely affect the respective cryptocurrency networks, render existing distributed ledger technology obsolete, inefficient, or fail to remediate or introduce new bugs and security risks;
- the use of the networks supporting digital assets for developing smart contracts and distributed applications;
- development of new technologies for mining and staking and the rewards and transaction fees for miners or validators on digital asset networks;
- changes in consumer demographics and public tastes and preferences;
- the availability and popularity of other forms or methods of buying and selling goods and services, including new means of using fiat currencies; and
- general economic conditions and the regulatory environment relating to digital assets.

Many digital asset networks, including Bitcoin and Ethereum, operate on open-source protocols maintained by groups of core developers. The open-source structure of these network protocols means that certain core developers and other contributors may not be compensated, either directly or indirectly, for their contributions in maintaining and developing the network protocol. A failure to properly monitor and upgrade network protocol could damage digital asset networks. As these network protocols are not sold and their use does not generate revenues for development teams, core developers may not be directly compensated for maintaining and updating the network protocols. Consequently, developers may lack a financial incentive to maintain or develop the network, and the core developers may lack the resources to adequately address emerging issues with the networks. There can be no guarantee that developer support will continue or be sufficient in the future. To the extent that material issues arise with certain digital asset network protocols and the core developers and open-source contributors are unable or unwilling to address the issues adequately or in a timely manner, such digital asset networks, and any corresponding digital assets held may be adversely affected.

Digital assets represent a new and rapidly evolving industry, and the market price of our Class A common stock has in the past and may in the future be impacted by the acceptance of bitcoin and other digital assets.

Digital assets built on blockchain technology were only introduced in 2008 and remain in the early stages of development. The Bitcoin network was first launched in 2009 and bitcoins were the first cryptographic digital assets created to gain global adoption and critical mass. Cryptographic and algorithmic protocols governing the issuance of digital assets represent a new and rapidly evolving industry that is subject to a variety of factors that are difficult to evaluate. Because our results of operations and the market price of our Class A common stock may be closely correlated with the acceptance and perception of bitcoin and/or other digital assets, the realization of one or more of the following risks could materially adversely affect the market price of our Class A common stock:

- Bitcoins have only recently become selectively accepted as a means of payment by some retail and commercial outlets, and use of bitcoins by consumers to pay such retail and commercial outlets remains limited. Banks and other established financial institutions may refuse to process funds for bitcoin transactions; process wire transfers to or from digital asset trading platforms, bitcoin-related companies or service providers; or maintain accounts for persons or entities transacting in bitcoin. As a result, the prices of bitcoins are largely determined by speculators and miners, thus contributing to price volatility that makes retailers less likely to accept it as a form of payment in the future.
- Banks may choose to not provide banking services, or may choose to cut off banking services, to businesses that provide digital asset-related services or that accept digital assets as payment, which could dampen liquidity in the market and damage the public perception of digital assets generally or any one digital asset in particular, such as

bitcoin, and their or its utility as a payment system, which could decrease the price of digital assets generally or individually.

- Certain privacy-preserving features have been or are expected to be introduced to some digital asset networks and digital asset trading platforms or businesses that facilitate transactions in digital assets, including bitcoin may be at an increased risk of having banking services cut off if there is a concern that these features interfere with the performance of anti-money laundering duties and economic sanctions checks.
- Users, developers and miners may otherwise switch to or adopt certain digital assets at the expense of their engagement with other digital asset networks, which may negatively impact those networks, including the Bitcoin network.
- In August 2017, the Bitcoin network underwent a hard fork that resulted in the creation of a new digital asset network called Bitcoin Cash. This hard fork was contentious, and as a result some users of the Bitcoin Cash network may harbor ill will toward the Bitcoin network. Any future hard fork could be similarly contentious and some users may attempt to negatively impact the use or adoption of the Bitcoin network or other digital asset networks, as may those involved in contentious hard forks of other digital assets.

Digital assets are a new asset class and represent a technological innovation and they are subject to a high degree of uncertainty. The adoption of digital assets will require growth in usage and in the blockchain technology generally for various applications. Adoption of digital assets will also require greater regulatory clarity. A lack of expansion in use of digital assets and blockchain technologies would adversely affect our financial performance. In addition, there is no assurance that digital assets generally will maintain their value over the long term. The value of digital assets is subject to risks related to our use. If growth in the use of digital assets generally occurs in the near or medium term, there is no assurance that such use will continue to grow over the long term. A contraction in use of digital assets may result in increased volatility or a reduction in digital asset prices, which would materially and adversely affect our investment and trading strategies, the value of our assets and the value of any investment in us.

The prices of digital assets are extraordinarily volatile.

Values of digital assets have historically been highly volatile. The value of cryptocurrencies is based in part on market adoption and future expectations, which may or may not be realized. Fluctuations in the price of various cryptocurrencies may cause uncertainty in the market and could negatively impact trading volumes of cryptocurrencies, which would adversely affect the success of our business, financial condition and results of operations. A decline in the value of the digital assets that we hold would negatively impact our financial position. A significant portion of demand for digital assets is generated by speculators and investors seeking to profit from the short- or long-term holding of these assets. Speculation regarding future appreciation in the value of a digital asset may inflate and make more volatile the price of that digital asset.

Several factors may affect the price of digital assets, particularly cryptocurrencies, including, but not limited to:

- Global cryptocurrency supply and demand, which can be influenced by the growth or decline of retail merchants' and commercial businesses' acceptance of cryptocurrencies as payment for goods and services, the security of online digital asset trading platforms and digital wallets that hold cryptocurrencies, the perception that the use and holding of digital currencies is safe and secure and regulatory restrictions on their use.
- The development and launch timeline of new digital asset networks, and forthcoming upgrades designed to improve network scalability.
- Changes in the software, software requirements or hardware requirements underlying a blockchain network, such as a fork. Forks in the future are likely to occur and there is no assurance that such a fork would not result in a sustained decline in the market price of cryptocurrencies.
- Changes in the rights, obligations, incentives or rewards for the various participants in a blockchain network. For digital assets that rely on miners or validators, sophisticated miner groups may become unduly influential over time if system or bandwidth requirements become too high. Where a single personality or entity exerts an outsize influence, an adverse event impacting that individual or entity, such as an insolvency proceeding, could result in a reduction in the price of a digital assets.

- Concentration of ownership in certain digital assets by an individual or small group of holders or those within one or a small number of jurisdictions. Large sales or distributions by such holders could have an adverse effect on the market price of such digital assets.
- The maintenance and development of the software protocol of cryptocurrencies.
- Digital asset trading platforms' deposit and withdrawal policies and practices, liquidity on such trading platforms and interruptions in service from or failures of such trading platforms.
- Regulatory measures and expected regulatory measures, if any, that affect the use and value of digital assets.
- Judicial pronouncements related to digital assets, including the treatment of digital assets in certain types of insolvencies.
- The taxation, and tax-related reporting, of transactions involving digital assets by the United States and other jurisdictions.
- Competition for and among various cryptocurrencies that exist and market preferences and expectations with respect to adoption of individual currencies.
- Actual or perceived manipulation of the markets for cryptocurrencies.
- Actual or perceived threats that cryptocurrencies and related activities such as mining have adverse effects on the environment or are tied to illegal activities, or on the other hand, the correlation of the price of certain digital assets to the price of bitcoin in particular.
- Social media posts and other public communications by high-profile individuals relating to specific cryptocurrencies, or listing or other business decisions by cryptocurrency companies relating to specific cryptocurrencies.
- Investors' expectations with respect to the rate of inflation, in the economy, monetary policies of governments, trade restrictions and currency devaluations and revaluations.
- Investors' overall confidence in the digital asset ecosystem and the safety and reliability of digital asset trading platforms.
- Activities of stablecoin issuers, the ability of stablecoin issuers to substitute underlying assets to back the stablecoins or the decline in value of those underlying assets and future actions relating to the regulatory or accounting treatment of stablecoins.

Additionally, some purportedly decentralized digital assets may be more centralized than widely believed, or may become more centralized over time, increasing the risk that an adverse event impacting an individual personality or entity could result in a reduction in the price of digital assets. While digital assets networks are typically decentralized and do not need to rely on any single government or institution to create, transmit and determine value, in reality a single personality or entity may have the ability to exert centralized authority over a network.

There are also volatility risks related to stablecoins, which are designed to have a relatively stable price relative to an underlying physical asset, most commonly a fiat currency, such as U.S. dollars, or an exchange-traded commodity. The stability of a stablecoin results from the underlying assets backing the stablecoin that are held by the stablecoin's issuer in reserve accounts, among other factors such as the ability of a holder to redeem the stablecoin from its issuer at par. The issuers of certain stablecoins currently retain broad discretion to determine the composition and amounts of assets held in the issuers' accounts backing those stablecoins, and to substitute assets other than the fiat currency that is initially deposited. The composition of backing assets varies considerably across popular stablecoins, with some stablecoins backed entirely by off-chain assets including cash or short-term, highly liquid assets, and others backed by assets significantly less liquid than cash or cash equivalents. For example, Circle, which issues USDC, reports that it holds cash and short-term cash equivalents to back its USDC stablecoins. Meanwhile, Tether, which issues USDT, publishes a report on a quarterly basis which includes a breakdown of the consolidated total assets comprising its reserves backing USDT as of a given reporting date, and according to such reports, its reserves have included commercial paper and certificates of deposit, cash and bank deposits, reverse repo notes, money market funds, treasury bills, secured loans, corporate bonds, funds and precious metals, and other investments (including digital tokens). We regularly transact in and hold stablecoins; as of September 30, 2025, USDC, USDT and USDS were the only stablecoins that we held in material amounts. A lack of applicable law and regulation has afforded discretion to certain stablecoin issuers to determine the composition and

amounts of assets backing those stablecoins. There is a risk that an issuer may be unable to liquidate enough backing assets if it were to face mass redemptions of its stablecoin, which could cause the price of the stablecoin to deviate from the price of the underlying fiat currency or other asset with which the stablecoin is designed to align in price. In extreme cases, such as a request to immediately redeem all or substantially all of a particular stablecoin in circulation, even stablecoins backed by reserves comprised primarily of cash and cash equivalents may be subject to instability or an inability of the stablecoin issuer to meet all redemption requests, as the market for short-dated U.S. government obligations might not be sufficiently price stable. Market participants have increasingly shown concern about the actual underlying liquidity and reserves for dollar stablecoins such as USDT and USDC. For example, according to reports, Circle had more than \$3 billion of its USDC reserve funds on deposit at SVB which became temporarily inaccessible when SVB was placed into FDIC receivership in March 2023. Although these funds were ultimately made available, concerns related to Circle's access to these funds caused USDC to temporarily fall below its \$1.00 peg, and the total market capitalization of USDC decreased following this temporary depegging. If a stablecoin issuer were to fail to honor its redemption obligations, this could undermine public confidence in stablecoins and in digital assets more broadly, which could have a widespread impact on the cryptoeconomy, causing the prices of other stablecoins and digital assets to become more volatile.

Some have argued that some stablecoins, particularly tether, are (or at least were previously) improperly issued without sufficient backing, and have also argued that those associated with certain stablecoins may be involved in laundering money. On February 17, 2021, the New York Attorney General entered an agreement with Tether's operators, requiring them to cease any further trading activity with New York persons and pay \$18.5 million in penalties for false and misleading statements made regarding the assets backing tether. Volatility in stablecoins, operational issues with stablecoins (for example, technical issues that prevent settlement), concerns about the sufficiency of any reserves that support stablecoins, or regulatory concerns about stablecoin issuers or intermediaries, such as crypto asset spot markets, that support stablecoins, could have a significant impact on the global crypto market and may adversely affect our business.

Because stablecoins purport to be backed by underlying reserve assets, a fundamental issue in the event of the bankruptcy or insolvency of the issuer of a given stablecoin is which party possesses beneficial ownership of the underlying reserve assets: the holder of the stablecoin, or the issuer. If a particular stablecoin were structured in a manner that entitles its holder only to a contractual right to payment from the issuer (even if such payments are to be derived from the underlying assets), then the assets underlying the stablecoins may be considered to be the property of the issuer's bankruptcy estate, such that all of the issuer's creditors would be entitled to their pro rata share of such assets, with the stablecoin holder being treated as an unsecured creditor of the issuer. In such an event, if the issuer were to have insufficient funds or assets to satisfy the claims of its creditors, then the holder of a stablecoin would likely receive only a partial recovery, and not the full purported value of its stablecoin holdings. Conversely, if a particular stablecoin were structured in a manner that entitles its holder to absolute beneficial ownership of the underlying reserve assets, whereby the issuer holds bare legal title to the underlying assets but has no beneficial interest or property rights in such assets, then the holders would likely have a stronger claim on the underlying assets in the event of a bankruptcy or insolvency of the issuer. However, due to the novelty of stablecoins, courts have not yet considered the treatment of underlying reserve assets in the context of a bankruptcy or insolvency of a stablecoin issuer, and there can be no certainty as to a court's determination in such circumstances.

Some digital assets may be more difficult to value than other investments because such assets may not have a liquid or transparent trading market. For example, some digital asset trading platforms have created their own digital assets and used them in opaque and potentially fraudulent manners to facilitate transactions and trading relationships. In certain circumstances, such digital assets are thinly traded, making it difficult to ascertain the true value of such assets. We may not be able to sell a digital asset promptly or at a reasonable time or price. Although there may be an institutional market for certain digital assets, it is not possible to predict exactly how the market for such assets will develop or whether it will continue to exist. A digital asset that was liquid at the time of purchase may subsequently become illiquid, and its value may decline as a result.

There is no assurance that cryptocurrencies will maintain their long-term value in terms of purchasing power in the future, or that acceptance of cryptocurrency payments by mainstream retail merchants and commercial businesses will continue to grow. Only a limited number of cryptocurrencies, including bitcoin, have become sometimes accepted as a means of payment for some goods and services, and use of cryptocurrencies by consumers to pay at retail and commercial outlets remains very limited. In part, this is because cryptocurrencies face significant scaling obstacles that can lead to high fees or slow transaction settlement times and attempts to increase the volume of transactions may not be effective. A lack of expansion by cryptocurrencies into retail and commercial markets, or a contraction of such limited use as has developed to date, may result in increased volatility or a reduction in the value of that cryptocurrency or cryptocurrencies generally, which has in the past, and could materially and adversely affect our investment and trading strategies, the value of our assets and the value of any investment in us.

Due to a lack of familiarity and some negative publicity associated with digital asset trading platforms, existing and potential customers, counterparties and regulators may lose confidence in digital asset trading platforms.

Since the inception of the cryptoeconomy, numerous digital asset trading platforms have been sued, investigated, or shut down due to fraud, manipulative practices, business failure, and security breaches. In many of these instances, customers of these platforms were not compensated or made whole for their losses. Larger platforms like ours are more appealing targets for hackers and malware, and may also be more likely to be targets of regulatory enforcement actions. For example, in February 2021, Bitfinex settled a long-running legal dispute with the State of New York related to Bitfinex’s alleged misuse of over \$800 million of customer assets and, in October 2023, hackers were reported to have stolen \$570 million from the BNB Smart Chain, a blockchain linked with Binance, one of the world’s largest platforms. Further, in 2022 and 2023, each of Celsius Networks, Voyager Digital, Three Arrows Capital, FTX and Genesis declared bankruptcy. In particular, in November 2022, FTX—which was at the time one of the world’s largest and most popular digital asset trading platforms—became insolvent, and it was revealed that the platform had been misusing customer assets, resulting in a loss of confidence in participants of the cryptoeconomy and negative publicity surrounding crypto more broadly.

In December 2022, Galaxy Bahamas Ltd. received approval from the Securities Commission of The Bahamas for registration as a digital asset business under the Digital Assets and Registered Exchanges Act, 2020. Galaxy Bahamas Ltd. physically operates out of the Bahamas and serves as an extension of our trading business and GalaxyOne Prime LLC (“GPL”), one of the subsidiaries through which we operate our trading business. It also offers market making services in spot digital assets and digital assets derivatives. In light of the FTX bankruptcy and surrounding controversies, customers, counterparties and regulators may view operations within the Bahamian cryptoeconomy as riskier than operations in other jurisdictions. See “—Risks Related to Regulation, Information Systems and Privacy Matters—Legislative or regulatory changes or actions in foreign jurisdictions may affect our business or restrict the use of one or more digital assets, transactions referencing digital assets, mining activity or the operation of their networks or the digital asset trading platform market in a manner that adversely affects our business” for a further discussion of these risks.

Further, in June 2023, the SEC initiated lawsuits against Coinbase and Binance alleging, among other things, that such firms were operating as unregistered securities exchanges in the United States, and identifying a number of digital assets that the SEC alleges to be unregistered securities. In addition, in November 2023, the SEC filed a complaint against Kraken and brought similar charges, including an allegation that Kraken operated as an unregistered securities exchange, brokerage and clearing agency. In February 2025, March 2025 and May 2025, respectively, each of Coinbase, Kraken and Binance entered into a court-approved joint stipulation with the SEC to dismiss each of the SEC’s lawsuits with prejudice. Several other digital assets market participants have also announced that the SEC informed them that the SEC was terminating its investigation or enforcement action into their firm. In November 2023, Binance pleaded guilty to the Justice Department’s investigations into violations relating to the BSA, failure to register as a money transmitting business and the International Emergency Economic Powers Act, and the founder of Binance pleaded guilty to failing to maintain an effective AML program in violation of the BSA. As part of the settlement, Binance separately reached resolutions with the CFTC, FinCEN and OFAC; however, its case against the SEC’s allegations remains ongoing, and Coinbase and Kraken have also denied the SEC’s allegations. The Justice Department in April 2025 issued a memorandum indicating that it will prioritize cases related to digital assets’ use in crimes of fraud, terrorism, drugs and human trafficking, organized crime, hacking, and gang financing, while other sorts of cases related to digital assets will be deprioritized. As a result, the outcome of these lawsuits and other lawsuits (to the extent not yet dismissed), their effect on the broader cryptoeconomy and the reputational impact on industry participants, remain uncertain.

In addition, there have been reports that a significant amount of trading volume on digital asset trading platforms is fabricated and false in nature. Such reports may indicate that the market for digital asset trading platform activities is significantly smaller than otherwise understood.

Negative perception, a lack of stability and standardized regulation in the cryptoeconomy, and the closure or temporary shutdown of digital asset trading platforms due to fraud, business failure, hackers or malware, or government mandated regulation, and associated losses suffered by customers may reduce confidence in the cryptoeconomy and result in greater volatility of the prices of assets, including significant depreciation in value. Any of these events could have an adverse impact on our reputation, financial condition and our business.

Many digital asset transactions are irrevocable and stolen or incorrectly transferred digital assets may be irretrievable. As a result, any incorrectly executed digital asset transactions could adversely affect the price of our Class A common stock.

Digital asset transactions are typically not reversible without the consent and active participation of the recipient of the transaction. Once a transaction has been verified and recorded in a block that is added to the blockchain, an incorrect transfer or theft of a digital asset generally will not be reversible and we may not be capable of obtaining compensation for

any such transfer or theft. Although transfers of digital assets that we hold and/or that are custodied on behalf of our customers will regularly be made to or from our custody accounts, it is possible that, through computer or human error, or through theft or criminal action, such digital assets could be transferred from our custody accounts in incorrect amounts or to unauthorized third parties, or to uncontrolled accounts.

Such events have occurred in connection with digital assets in the past. For example, in September 2014, the digital asset trading platform Huobi announced that it had sent approximately 900 bitcoins and 8,000 Litecoins (worth approximately \$400,000 at the prevailing market prices at the time) to the wrong customers. In February 2025, the digital asset trading platform Bybit lost approximately \$1.5 billion in ether through hacker-induced transfer from its cold wallet to a wallet address associated with the Lazarus Group. Although Bybit announced that their reserve guarantee ensured that client assets remained fully intact for such incident, there is no assurance we or other participants in the industry may be able to protect against similar types of losses. To the extent that we are unable to seek a corrective transaction with such third party or are incapable of identifying the third party which has received our digital assets through error or theft, we will be unable to revert or otherwise recover incorrectly transferred digital assets. We will also be unable to convert or recover the digital assets transferred to uncontrolled accounts. To the extent that we are unable to seek redress for such error or theft, such loss could have a material adverse effect on us.

The U.S. federal income tax treatment of transactions in digital assets is unclear.

Due to the new and evolving nature of digital assets and the absence of comprehensive guidance with respect to digital assets, many significant aspects of the U.S. federal income tax treatment of digital assets are uncertain. Our operations and dealings, in or in connection with digital assets, as well as transactions in digital assets generally, could be subject to adverse tax consequences in the United States, including as a result of development of the legal regimes surrounding digital assets, and our operating results, as well as the price of digital assets, could be adversely affected thereby.

Many significant aspects of the U.S. federal income tax treatment of digital assets (including with respect to the amount, timing and character of income recognition) are uncertain. In 2014, the U.S. Internal Revenue Service (the “IRS”) released a notice (the “Notice”) discussing certain aspects of digital assets for U.S. federal income tax purposes and, in particular, stating that such digital assets (1) are “property,” (2) are not “currency” for purposes of the rules relating to foreign currency gain or loss and (3) may be held as a capital asset. In 2019, the IRS released a revenue ruling and a set of “Frequently Asked Questions” (the “Ruling & FAQs”) that provide some additional guidance, including guidance to the effect that, under certain circumstances, hard forks of digital assets are taxable events giving rise to ordinary income and guidance with respect to the determination of the tax basis of digital assets. Moreover, in 2023, the IRS released a revenue ruling that provided guidance on digital asset staking, including guidance to the effect that staking rewards will, under certain circumstances, be treated as giving rise to taxable income (the “Staking Guidance”). However, the Notice, the Ruling & FAQs, and the Staking Guidance do not address other significant aspects of the U.S. federal income tax treatment of digital assets. For example, for a Non-U.S. Holder (as defined below), there currently is no guidance directly addressing whether or in what circumstances engaging in certain activities to generate yield on digital assets, including Staking, could give rise to income that is effectively connected with a trade or business in the United States. We do not intend to request a ruling from the IRS on these issues, and we will take positions on these and other U.S. federal income tax issues relating to digital assets that we believe to be reasonable. There can be no assurance that the IRS will agree with the positions we take, and it is possible that the IRS will successfully challenge our positions.

There can be no assurance that the IRS will not alter its position with respect to digital assets in the future or that a court would uphold the treatment set forth in the Notice and the Ruling & FAQs. It is also unclear what additional guidance on the treatment of digital assets for U.S. federal income tax purposes may be issued in the future. Any such alteration of the current IRS positions or additional guidance could result in adverse tax consequences for us and could have an adverse effect on the value of bitcoin or other digital assets. Because of the evolving nature of digital assets, it is not possible to predict potential future developments that may arise with respect to digital assets. Such developments may increase the uncertainty with respect to the treatment of digital assets for U.S. federal income tax purposes. For example, the Notice addresses only digital assets that are “convertible virtual currency,” and it is conceivable that we will hold certain types of digital assets that are not within the scope of the Notice.

On November 15, 2021, former President Biden signed into law the Infrastructure Investment and Jobs Act (the “IIJA”). The IIJA implements a set of comprehensive tax information reporting rules that will apply to persons, including digital asset trading platforms and custodians, that regularly effect transfers of digital assets on behalf of other persons. In particular, these rules will require digital asset trading platforms and custodians to report certain digital asset transactions (including sales, exchanges and other transfers) effected on behalf of other persons on an annual return, in a manner similar to the current reporting rules for brokers that effect stock and other securities transactions on behalf of customers. In addition, the IIJA extends the reporting requirements for businesses that receive more than \$10,000 in cash in a transaction

(or related transactions) to transactions involving the receipt of digital assets with a fair market value of more than \$10,000. However, such extension to transactions involving the receipt of digital assets has been postponed pending the issuance of regulations.

In July 2024, the IRS and the U.S. Department of the Treasury released final regulations to implement certain of these reporting rules (the “July 2024 final regulations”). The July 2024 final regulations’ definition of the term “broker” is broad and, in a number of respects, is unclear in scope, but generally requires custodial brokers and brokers acting as principals to perform information reporting and backup withholding functions. Under the July 2024 final regulations and a notice released contemporaneously by the IRS and the U.S. Department of the Treasury, such reporting of cost basis information and backup withholding generally will apply in respect of transactions occurring on or after January 1, 2025, but certain transitional relief may be available for transactions occurring prior to January 1, 2026. The July 2024 final regulations do not address all aspects of the IIJA information reporting regime and their application is uncertain in a number of respects, including with respect to the collection and reporting of cost basis information for digital assets and the scope of transactions subject to reporting. In December 2024, the IRS and the U.S. Department of the Treasury issued separate final regulations describing information reporting rules for non-custodial industry participants (the “December 2024 final regulations”), including the requirement to file information returns and furnish payee statements reporting gross proceeds on dispositions of digital assets effected for customers in certain sale or exchange transactions. The December 2024 final regulations were repealed on April 10, 2025, under the Congressional Review Act. Regulations repealed under the Congressional Review Act generally may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law subsequently enacted. The impact on the IIJA information reporting regime of the repeal of the December 2024 final regulations is unclear and there can be no assurance that the same or similar regulations will not be authorized by future law.

The effects of the IIJA reporting regime and its application to us may depend in significant part on future Congressional action and further regulatory or other guidance from the IRS and could create significant compliance burdens and uncertainties for us and our customers, and could affect the price of digital assets, which could have an adverse effect on our business.

The state, local and non-U.S. tax treatment of digital assets is unclear.

The taxing authorities of certain states (i) have announced that they will follow the Notice with respect to the treatment of digital assets for state income tax purposes and/or (ii) have issued guidance exempting the purchase and/or sale of digital assets for fiat currency from state sales tax. It is unclear what further guidance on the treatment of digital assets for state tax purposes may be issued in the future. Any future guidance on the treatment of digital assets for state or local tax purposes could result in adverse tax consequences to us and could adversely affect the price of digital assets.

The treatment of digital assets for tax purposes by non-U.S. jurisdictions may differ from the treatment of digital currency for U.S. federal, state or local tax purposes. It is possible, for example, that a non-U.S. jurisdiction would impose sales tax or value-added tax on purchases and sales of digital assets for fiat assets. For instance, if a foreign jurisdiction with a significant share of the market of bitcoin users imposes onerous tax burdens on digital asset users, or imposes sales or value-added tax on purchases and sales of digital assets for fiat assets, such actions could result in decreased demand for digital currency in such jurisdiction, which could adversely affect the price of digital assets.

You are urged to consult your own tax advisors regarding the tax treatment of digital assets and the consequences of investing in us, given the nature of our business.

Political or economic crises may motivate large-scale sales of digital assets, which would result in a reduction in values and materially and adversely affect us.

Cryptocurrencies, as an alternative to fiat currencies that are backed by central governments, are subject to supply and demand forces based upon the desirability of an alternative, decentralized means of buying and selling goods and services, and it is unclear how such supply and demand will be impacted by geopolitical events. For example, political or economic crises could motivate large-scale acquisitions or sales of digital assets either globally, regionally or locally. Large-scale sales of certain digital assets would result in a reduction in their value and could materially and adversely affect our investment and trading strategies, the value of our assets and our value.

The value of cryptocurrencies and other digital assets may be subject to momentum pricing risk.

Momentum pricing typically is associated with growth stocks and other assets whose valuation, as determined by the investing public, accounts for anticipated future appreciation in value. Cryptocurrency and other digital asset market prices are determined primarily using data from various digital asset trading platforms, OTC markets, and derivative platforms.

Momentum pricing may have resulted, and may continue to result, in speculation regarding future appreciation in the value of cryptocurrencies and other digital assets, inflating and making their market prices more volatile, and such effects may be material and adverse. As a result, cryptocurrencies and other digital assets may be more likely to fluctuate in value due to changing investor confidence in future appreciation (or depreciation) in their market prices, which could adversely materially affect the value of our cryptocurrency and other digital asset inventory and thereby affect the market price of our Class A common stock.

Short sales and borrowings of digital assets pose additional risks.

We engage in short sales and borrowings of digital assets. In a short sale, we sell digital assets that we do not own, typically borrowed from a third party. We also borrow digital assets for various other purposes including but not limited to general liquidity purposes, such as for our capital and treasury operations, and as inventory for our trading business, counterparty trade settlement, collateral management and lending. Borrowing and lending markets for digital assets are currently limited and are unlikely to become as developed and stable as those for securities or other established assets in the near term, if ever, which exposes us to risks.

Because we would remain liable to return any digital assets that we borrowed, whether in connection with a short sale or otherwise, we would be required to purchase an equivalent amount of digital assets prior to the date on which delivery to the third-party lender is required. We will incur a loss as a result of a short sale of a digital asset and may incur a loss as a result of borrowing a digital asset, depending on how we use it, if the price of the digital asset increases between the date of the short sale or borrowing and the date on which we close the relevant position. The amount of any loss will be increased by the amount of the premium or interest that we may be required to pay in connection with a short sale or borrowing. Short selling and borrowing exposes us to unlimited risk with respect to the borrowed digital assets because of the lack of an upper limit on the prices to which those digital assets can rise. Purchasing digital assets to close out a short position can itself cause the price of the digital assets to rise further, thereby exacerbating any losses. Under adverse market conditions, we may have difficulty purchasing digital assets to meet our short sale delivery obligations and may have to sell other digital assets to raise the necessary capital at a time when it would be unfavorable to do so. If a request for return of borrowed assets occurs at a time when other short sellers are receiving similar requests, a “short squeeze” can occur, and we may be compelled to replace borrowed digital assets previously sold short with purchases on the open market at the most disadvantageous time, possibly at prices significantly in excess of the proceeds received in originally selling the assets short. In addition, we may have difficulty purchasing assets to meet our delivery obligations if the assets sold short or borrowed by us have a limited daily trading volume or limited market capitalization. Short sales by us and “short” derivative positions are forms of investment leverage, and the amount of our potential loss is theoretically unlimited.

Additionally, in various contexts, the SEC and state securities regulators have alleged that programs where firms borrow digital assets in exchange for a promise to return those assets, plus a yield, were unlawfully unregistered securities offerings. We do not believe that our borrowing activities constitute the offer or sale of a security. Among other things, unlike in the circumstances where this has been alleged against others, our borrowing activities are not “yield” products widely offered as an investment vehicle to the general public. Instead, we borrow digital assets from institutional counterparties through individually negotiated transactions, and/or through one or more DeFi protocols. While we do not believe our borrowing activities constitute securities offerings, there is a risk that the SEC or state securities regulators could take a contrary view. In that case, our prior determination, even if reasonable under the circumstances, would not preclude legal or regulatory enforcement action, or lawsuits brought by our clients and counterparties, based on the presence of a security. See “—Risks Related to Our Operations—A determination that a digital asset is a “security,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could adversely affect the value of that digital asset and potentially digital assets generally, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock,” for more information.

Lending of digital assets poses additional risks.

We lend digital assets to third parties, including affiliates. On termination of the loan, the borrower is required to return the digital assets to us; any gains or losses in the market price during the loan would inure to us. In the event of the bankruptcy of the borrower, we could experience delays in recovering our digital assets and may, in certain circumstances, recover only some or none of our lent digital assets. In addition, to the extent that the value of the digital assets increases during the term of the loan, the value of the digital assets may exceed the value of collateral provided to us (if any), exposing us to credit risks with respect to the borrower and potentially exposing us to a loss of the difference between the value of the digital assets and the value of the collateral. There may also be legal, operational and technological impediments to our ability to foreclose on collateral posted to us in a timely manner or at all. If a borrower defaults under its obligations with respect to a loan of digital assets, we may expend significant resources and incur significant expenses in

connection with efforts to enforce the loan agreement or our interests in the collateral, which may ultimately be unsuccessful. Moreover, we have in the past, and may in the future, engage in unsecured lending of digital assets, which exposes us to losses amounting to the full value of any such digital assets, including the appreciation of such digital assets during the pendency of the loan. In addition, there is significant operational infrastructure required to scale the borrowing and lending of digital assets. The failure to appropriately implement the infrastructure related to the lending business could lead to operational risk and have a material adverse effect on us. In addition, our lending operations may be subject to regulatory risk. See “—We currently offer services involving, and expect to continue to support, certain smart contract-based digital assets. If the underlying smart contracts for these protocols do not operate as expected, they could lose value and our business could be adversely affected,” “—We engage in DeFi activities and may suffer losses if the DeFi protocols, or our activities thereon, do not function as expected,” “—The emergence of DeFi subjects us to evolving risks and uncertainties relating to our investments and our services” and “—DeFi protocols and digital assets used in DeFi protocols pose heightened regulatory concerns even beyond those that face digital asset networks and digital assets generally.”

While there is no U.S. federal law that requires registration or licensing for lending activities, some digital asset lending arrangements have been found to be securities. See “—Risks Related to Our Operations—A determination that a digital asset is a “security,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could adversely affect the value of that digital asset and potentially digital assets generally, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock.” If we were to originate consumer or commercial loans in the United States, we would be subject to federal laws including the Truth-in-Lending Act, the Equal Credit Opportunity Act, the Consumer Protection Act, the Fair Credit Reporting Act and the Fair Debt Collection Practices Act. Further, some U.S. state laws may, under certain circumstances, require us to obtain a license from the relevant regulatory authority or authorities in a given state before conducting those lending activities.

Blockchain networks, digital assets and the digital asset trading platforms on which these assets are traded are dependent on internet and other blockchain infrastructure and susceptible to system failures, security risks and rapid technological change.

The success of cryptocurrency-based blockchain and other digital asset platforms will depend on the continued development of a stable public infrastructure, with the necessary speed, data capacity and security, and the timely development of complementary products such as high-speed modems for providing reliable internet access and services. Digital assets have experienced, and are expected to continue to experience, significant growth in the number of users and amount of content. Blockchains will continue to be increasingly interconnected with other blockchains and real-world applications. As services and applications continue to be built on top of blockchains, they will place increased reliance on third-party infrastructure providers, including in connection with cross-chain bridges and messaging, liquidity providers, wallets, data feeds and oracles. Reliance on any of these third-parties introduces additional risks and points of failure. There is no assurance that the relevant digital asset infrastructure will continue to be able to support the demands placed on it by this continued growth or that the performance or reliability of the technology will not be adversely affected by this continued growth. There is also no assurance that the infrastructure or complementary products or services necessary to make digital assets a viable product for their intended use will be developed in a timely manner, or that such development will not result in the requirement of incurring substantial costs to adapt to changing technologies. The failure of these technologies or platforms or their development could materially and adversely affect our investment and trading strategies, the value of our assets and the value of any investment in us. Any number of anticipated or unforeseen technical changes, software upgrades, soft or hard forks, cybersecurity incidents or other changes to the underlying blockchain network may occur from time to time, causing incompatibility, technical issues, disruptions or security weaknesses to our systems. If we or our third-party providers are unable to identify, troubleshoot and resolve any such issues successfully, we may no longer be able to support certain cryptocurrencies or blockchain networks, our customers’ assets may be frozen or lost, the security of our hot or cold wallets may be compromised and our systems and technical infrastructure may be affected, all of which could adversely impact the success of our business, financial condition and results of operations. Cryptocurrencies are created, issued, transmitted, and stored according to protocols run by computers in the cryptocurrency network. It is possible these protocols have undiscovered flaws or could be subject to network scale attacks which could result in losses to us. Advancements in quantum computing could break the cryptographic rules of protocols which support certain of our assets.

If the digital asset award for mining or validating blocks and transaction fees for recording transactions on a digital asset network is not sufficiently high to incentivize miners, or if certain jurisdictions continue to limit mining activities, miners may cease expanding processing power or demand high transaction fees, which could negatively impact the value of the digital asset and the market price of our Class A common stock.

If the digital asset rewards for mining blocks or the transaction fees for recording transactions on a digital asset network are not sufficiently high to incentivize miners, or if certain jurisdictions continue to limit mining activities, miners may cease expending processing power to mine blocks and confirmations of transactions on the digital asset's blockchain could be slowed. We pay miner fees in connection with our digital asset transactions. Miner fees can be unpredictable. For instance, in 2024, bitcoin miner fees decreased from approximately \$0.08 per transaction in January 2024 to approximately \$0.05 per transaction in December 2024. For example, the realization of one or more of the following risks could materially adversely affect the market price of our Class A common stock:

- Over the past several years, digital asset mining operations have evolved from individual users mining with computer processors, graphics processing units and first generation application specific integrated circuit machines to “professionalized” mining operations using proprietary hardware or sophisticated machines. If the profit margins of digital asset mining operations are not sufficiently high, including due to an increase in electricity costs, digital asset miners are more likely to immediately sell tokens earned by mining, resulting in an increase in liquid supply of that digital asset, which would generally tend to reduce that digital asset's market price.
- A reduction in the processing power expended by miners on a digital asset network could increase the likelihood of a malicious actor disrupting or obtaining control of the network. See “—Risks Related to Cryptocurrencies and Digital Assets—If a malicious actor or botnet obtains control of more than 50% of the processing power on a digital asset network, or otherwise obtains control over a digital asset network through its influence over core developers or otherwise, such actor or botnet could manipulate the blockchain of such digital asset to adversely affect the market price of our Class A common stock or our ability to operate.”
- Miners have historically accepted relatively low transaction confirmation fees on most digital asset networks due to income skewed toward the block reward. If miners demand higher transaction fees for recording transactions in the blockchain or a software upgrade automatically charges fees for all transactions on a digital asset network, the cost of using such digital asset may increase and the marketplace may be reluctant to accept such digital asset as a means of payment. Alternatively, miners could collude in an anti-competitive manner to reject low transaction fees on a digital asset network and force users to pay higher fees, thus reducing the attractiveness of the digital asset network. Higher transaction confirmation fees resulting from collusion or other factors may reduce the attractiveness of the digital asset network, the value of the digital asset, and could materially and adversely affect our investment and trading strategies, the value of our assets and the market price of our Class A common stock. Losses associated with the payment of miner fees in excess of what we charge our customers, could result in adverse impacts on our operating results.
- To the extent that any miners cease to record transactions that do not include the payment of a transaction fee in mined blocks or do not record a transaction because the transaction fee is too low, such transactions will not be recorded on the blockchain of a digital asset until a block is mined by a miner who does not require the payment of transaction fees or is willing to accept a lower fee. Any widespread delays in the recording of transactions could result in a loss of confidence in a digital asset network.
- Digital asset mining operations can consume significant amounts of electricity, which may have a negative environmental impact as a result of associated greenhouse gas emissions and depletion of water resources, and give rise to public opinion against allowing, or government regulations restricting, the use of electricity for mining operations. Additionally, miners may be forced to cease operations during an electricity shortage or power outage.

From time to time, we may encounter technical issues in connection with changes or upgrades to the underlying digital asset networks of supported cryptocurrencies or protocols, and more broadly, such changes or upgrades may be delayed or unsuccessful, any of which could materially and adversely affect our investments and trading strategies, our financial condition and results of operations.

Rising adoption of blockchain networks leads to network congestion, as space on decentralized ledgers is inherently scarce. From a design standpoint, striking a balance between security, decentralization, and scalability (or transactional throughput) is subject of great debate among innovators and has led to the creation of a variety of networks that make different trade-offs to achieve different outcomes. If network congestion rises to the point where transaction fees make it

prohibitively expensive for average users to operate on the network, those users may stop using the network, and application developers may seek to build on other networks where users can afford to transact.

Any number of anticipated or unforeseen technical changes or software upgrades, soft or hard forks, cybersecurity incidents or other changes to the underlying blockchain network may cause incompatibility, technical issues, disruptions or security weaknesses to our systems. If we or our third-party providers are unable to identify, troubleshoot and resolve any such issues successfully, we may no longer be able to support certain cryptocurrencies or blockchain networks, our customers' assets may be frozen or lost, the security of our hot or cold wallets may be compromised and our technical infrastructure may be affected, all of which could adversely impact the success of our business, financial condition and results of operations.

Changes in the governance of a digital asset network may not receive sufficient support from users and miners or validators, which may negatively affect that digital asset network's ability to grow and respond to challenges.

The governance of decentralized networks, such as the Bitcoin and Ethereum networks, is by voluntary consensus and open competition. As a result, there may be a lack of consensus or clarity on the governance of any particular decentralized digital asset network, which may stymie such network's utility and ability to grow and face challenges. The foregoing notwithstanding, the protocols for some decentralized networks, such as the Bitcoin network, are informally managed by a group of core developers that propose amendments to the relevant network's source code. Core developers' roles evolve over time, largely based on self-determined participation. If a significant majority of users and miners adopt amendments to a decentralized network based on the proposals of such core developers, such network will be subject to new protocols that may adversely affect the value of the relevant digital asset.

As a result of the foregoing, it may be difficult to find solutions or marshal sufficient effort to overcome any future problems, especially long-term problems, on digital asset networks.

A temporary or permanent "fork" could adversely affect an investment in us.

Many public blockchain networks, including the Bitcoin network, operate using open-source protocols, meaning that any user can download the software, modify it and then propose that the users and miners of bitcoin, for example, adopt the modification. The development team for a network might propose and implement amendments to a network's source code through software upgrades altering the original protocol, including fundamental ideas such as the irreversibility of transactions and limitations on the validation of blockchain software distributed ledgers. Such changes to original protocols and software could materially and adversely affect our investment and trading strategies, the value of our assets and the value of any investment in us.

When a modification is introduced and a substantial majority of users and miners consent to the modification, the change is implemented and the network remains uninterrupted. However, if less than a substantial majority of users and miners consent to the proposed modification, and the modification is not compatible with the software prior to its modification, the consequence would be what is known as a "hard fork" of the Bitcoin network, with one group running the pre-modified software and the other running the modified software. The effect of such a fork would be the existence of two versions of Bitcoin running in parallel, yet lacking interchangeability. Both Bitcoin and Ethereum networks have experienced "forks." A fork can lead to a disruption of networks and our information technology systems, which can further lead to temporary or even permanent loss of customer assets. For example, in August 2017, Bitcoin "forked" into Bitcoin and a new blockchain, Bitcoin Cash, as a result of a several-year dispute over how to increase the rate of transactions that the Bitcoin network can process.

Forks may also occur as a network community's response to a significant security breach. For example, in June 2016, an anonymous hacker exploited a smart contract running on the Ethereum network to syphon approximately \$60 million of ether held by The DAO, a distributed autonomous organization ("DAO"), into a segregated account. In response to the hack, most participants in the Ethereum community elected to adopt a "fork" that effectively reversed the hack. However, a minority of users continued to develop the original blockchain, now referred to as "Ethereum Classic" with the digital asset on that blockchain now referred to as Ether Classic. Ether Classic now trades on several digital asset trading platforms.

A fork may also occur as a result of an unintentional or unanticipated software flaw in the various versions of otherwise compatible software that users run. Such a fork could lead to users and miners abandoning the digital asset with the flawed software. It is possible, however, that a substantial number of users and miners could adopt an incompatible version of the digital asset while resisting community-led efforts to merge the two chains. This could result in a permanent fork, as in the case of ether and Ether Classic.

In addition, many developers have previously initiated hard forks in the Bitcoin blockchain to launch new digital assets, such as Bitcoin Cash, Bitcoin Gold, Bitcoin Silver and Bitcoin Diamond. Later, the Bitcoin Cash blockchain was again forked to launch a new digital asset, Bitcoin Satoshi's Vision. To the extent such digital assets compete with a digital asset held by Galaxy, such competition could impact demand for such digital asset and could adversely impact the market price of our Class A common stock. Furthermore, a hard fork can lead to new security concerns. For example, when the Ethereum and Ethereum Classic networks split in July 2016, replay attacks, in which transactions from one network were rebroadcast to nefarious effect on the other network, plagued Ethereum trading platforms through at least October 2016. An Ethereum trading platform announced in July 2016 that it had lost 40,000 Ether Classic, worth about \$100,000 at that time, as a result of replay attacks. Another possible result of a hard fork is an inherent decrease in the level of security due to significant amounts of mining power remaining on one network or migrating instead to the new forked network. After a hard fork, it may become easier for an individual miner or mining pool's hashing power to exceed 50% of the processing power of the digital asset network that retained or attracted less mining power, thereby making digital assets that rely on proof-of-work more susceptible to attack.

A hard fork may adversely affect the price of the digital asset at the time of announcement or adoption. For example, the announcement of a hard fork could lead to increased demand for the pre-fork digital asset, in anticipation that ownership of the pre-fork digital asset would entitle holders to a new digital asset following the fork. The increased demand for the pre-fork digital asset may cause the price of the digital asset to rise. After the hard fork, it is possible the aggregate price of the two versions of the digital asset running in parallel would be less than the price of the digital asset immediately prior to the fork.

The Ethereum network regularly implements software upgrades and other changes to its protocol. For example, in September 2022, the Ethereum network activated the long-awaited upgrade from a proof-of-work to proof-of-stake consensus protocol (the "Merge"). The Merge effectively swapped Ethereum's consensus mechanism away from proof-of-work to proof-of-stake. A digital asset network's consensus mechanism is a material aspect of its source code, and any failure to properly implement such a change could have a material adverse effect on the value of digital assets that rely on the Ethereum network, including some of which we hold, and the market price of our Class A common stock. Although the Merge appears to be successful thus far, it is possible that the Merge introduced a currently undiscovered error or vulnerability. It is expected that further developments and forks for the Ethereum network are forthcoming.

Any future forks could adversely affect our business and the market price of our Class A common stock.

We engage in DeFi activities and may suffer losses if the DeFi protocols, or our activities thereon, do not function as expected.

We engage in various DeFi activities. As of September 30, 2025, Galaxy's digital assets associated with decentralized finance protocols was \$1,008.0 million. DeFi protocols achieve their purposes through self-executing smart contracts. Some of these DeFi protocols allow users to, for example, transfer digital assets to a pool from which other users can borrow without requiring an intermediate party to facilitate these transactions. Digital assets transferred to a pool generally earn interest to the lender, based on the rates at which borrowers repay the loan, and can generally be withdrawn with no restrictions. However, these DeFi protocols pose heightened regulatory concerns and are subject to various risks, including the risk that the underlying smart contract is insecure, the risk that borrowers may default and the lender will not be able to recover its digital assets, the risk that any underlying collateral may experience significant volatility, and the risk that certain core developers with protocol administration rights can make unauthorized or harmful changes to the underlying smart contract. If any of these risks materialize, our digital assets in these DeFi protocols may be adversely impacted and we may lose some or all of our digital assets.

The emergence of DeFi subjects us to evolving risks and uncertainties relating to our investments and our services.

DeFi refers to a variety of blockchain-based applications or protocols that provide for peer-to-peer financial services using smart contracts and other technology rather than such services being offered by central intermediaries. There are various DeFi applications and protocols, each with its own unique risks and uncertainties. Common DeFi applications include borrowing/lending digital assets and providing liquidity or market making in digital assets and derivatives referencing digital assets. DeFi applications and ecosystems are demonstrating how public blockchains and smart contracts can revolutionize financial services, but the nascent technology comes with several risks that could materially and adversely affect our investments and trading strategies. It is difficult to quantify the amount of leverage that exists within the DeFi ecosystem and price volatility can result in deleveraging that moves asset prices dramatically. In addition, smart contracts may contain bugs which put funds at risk of theft or loss. Furthermore, in certain decentralized protocols, it may be difficult or impossible to verify the identity of a transaction counterparty necessary to comply with any applicable anti-money laundering, countering the financing of terrorism, or sanctions regulations or controls.

The complexity and interconnectedness of digital asset networks, applications, and economic systems enables new forms of malicious attacks that leverage a feature or vulnerability of one system to attack another. Such an attack may take the form of a temporary manipulation of the price of certain digital assets that trigger second order behaviors, such as automatic collateral liquidations on decentralized applications or digital asset trading platforms. Such an attack could adversely affect investments. A malicious actor can exploit the structure of one or a series of smart contracts or applications in ways that do not technically constitute exploitation of a “bug” or flaw in the smart contract or application. For example, such an exploit has occurred repeatedly in the Ethereum DeFi ecosystem, whereby a decentralized trading platform or lending application is designed to reference an external pricing source of a particular digital asset to determine when to liquidate collateral. By manipulating the price of the particular digital asset on a third-party platform (such as a digital asset trading platform), the pricing source used by the decentralized trading platform or application is consequently manipulated, which then leads to uneconomic collateral liquidations on the decentralized trading platform or application. Such liquidations may be processed automatically and could have a material adverse effect on our investments and trading strategies.

DeFi protocols and digital assets used in DeFi protocols pose heightened regulatory concerns even beyond those that face digital asset networks and digital assets generally.

The U.S. financial system is extensively regulated at both the federal and state levels with a particular focus on intermediaries such as banks, broker-dealers, swap dealers, futures commission merchants, investment funds, investment advisers, trading platforms, clearinghouses and custodians. U.S. laws and regulations impose specific obligations on financial services intermediaries both for the protection of their customers and for the protection of the U.S. financial system as a whole. These include capital requirements, activities restrictions, reporting and disclosure requirements and obligations to monitor the activities of their customers and to ensure that the intermediaries’ activities and the activities of their customers are conducted in accordance with applicable laws and regulations. Non-U.S. laws and regulatory requirements may impose similar obligations. By seeking to eliminate or substantially limit the role of traditional financial services intermediaries in lending, brokering, advisory, trading, clearing, custodying and other financial services activities, DeFi protocols pose numerous challenges to the longstanding oversight framework developed under U.S. law and used by U.S. and other regulators. For example, one former commissioner of the CFTC has publicly stated that he believes certain DeFi protocols and activities operating without regulatory licensing likely violates the Commodity Exchange Act. Moreover, in June 2023, a federal judge ruled that the CFTC had sufficiently pleaded that a DAO operates a DeFi protocol that has not registered as a futures commission merchant (“FCM”) and thereby illegally offers leveraged retail commodity transactions in digital assets, engages in activities only registered FCMs can perform, and has failed to adopt a customer identification program as part of a BSA compliance program, as required of FCMs, such that the judge granted the CFTC’s motion for default judgment against the DAO. In an accompanying settled enforcement order, the CFTC found the two founders, as token holders who voted their DAO tokens to govern the DAO, personally liable for the DAO’s violations of the Commodity Exchange Act and regulations promulgated thereunder. While the scope of liability for persons associated with a DAO, or its accompanying DeFi protocol, are currently unclear notwithstanding the default judgment entered against the DAO, it is possible that regulatory agencies may consider other DeFi token holders, or users of a DeFi protocol, liable for potential violations of the DeFi protocol. Separately, in September 2024, the CFTC settled with Uniswap Labs, the developer of the Uniswap decentralized exchange, for illegally offering leveraged or margined retail commodity transactions in digital assets through a front-end interface operated by Uniswap Labs.

There has also been an increase in SEC oversight, at least under the prior administration, including reported SEC subpoenas of teams behind DeFi platforms, which indicates that the SEC believed DeFi activities may in themselves implicate federal securities laws. In April 2023, the SEC under the prior administration reopened the comment period and provided supplemental information for its proposed amendments to the definition of “exchange” under the Exchange Act. In the supplemental information, the SEC stated that it believed DeFi protocols, and the parties that develop them, could be exchanges subject to federal securities laws if they facilitate the trading of digital asset securities. In announcing the reopening, then-Chair Gensler stated “calling yourself a DeFi platform is not an excuse to defy the securities laws.” Although in March 2025 then Acting SEC Chairman Uyeda said he had asked SEC staff for options on abandoning the digital assets-related elements of the proposal, it is not possible to predict how or when these developments will be resolved or what the impact on specific DeFi protocols will be. Because it is unclear both which digital assets on a DeFi platform may be deemed securities and which DeFi activities in themselves may implicate the federal securities laws, it is likely that the DeFi industry will face a prolonged period of regulatory uncertainty. It is possible that some DeFi protocols, including those using digital assets that we invest in, will be subjected to costly and burdensome compliance regimes or even prohibited outright.

In addition, traditional financial services intermediaries bear significant and ongoing costs to comply with financial services regulation, and individually or through trade associations may actively oppose legislative or regulatory efforts to

accommodate DeFi activities that compete with their core service offerings. Traditional financial services intermediaries may instead actively encourage policymakers and regulatory authorities to take actions that impede the development and use of DeFi protocols. DeFi protocols that significantly improve on traditional financial services offerings by making transactions more efficient and inexpensive, including those using digital assets, can be expected to draw the most attention and potential opposition from traditional financial services intermediaries, the associations that represent them, and their legislative allies.

Further, most DeFi activities rely on users maintaining “self-hosted” wallets, and DeFi protocols generally do not engage in AML and KYC or other customer identification and due diligence processes, each of which have raised concerns for regulators, including international standard-setting bodies such as the Financial Action Task Force.

Legislative bodies and regulators may be required to adapt their regulatory models to accommodate decentralized financial activities, or take novel steps to supervise, limit or even prohibit decentralized financial activities.

Any action taken by federal, state or international policymakers or regulators to address risks and perceived risks to the public or to the U.S. and other countries’ financial systems from decentralized financial activities, or the threat of such action, could have a material adverse impact on one or more digital assets and therefore materially and adversely impact our investments, our revenue and the market price of our Class A common stock.

If a malicious actor or botnet obtains control of more than 50% of the processing power on a digital asset network, or otherwise obtains control over a digital asset network through its influence over core developers or otherwise, such actor or botnet could manipulate the blockchain of such digital asset to adversely affect the market price of our Class A common stock or our ability to operate.

If a malicious actor or botnet (a volunteer or hacked collection of computers controlled by networked software coordinating the actions of the computers) obtains a majority of hash rate on a proof-of-work system, or otherwise controls a sizeable portion of supply in a proof-of-stake system, it can maliciously disrupt the blockchain, either by halting functionality, censoring transactions, or even double-spending coins. If such an actor or botnet obtains a majority of the processing power dedicated to mining on a particular digital asset network, it may be able to alter the relevant blockchain on which transactions in that digital asset rely by constructing fraudulent blocks or preventing certain transactions from completing in a timely manner, or at all. The malicious actor or botnet could also control, exclude or modify the ordering of transactions. Although the malicious actor or botnet would not be able to generate new tokens or transactions using such control, it could “double-spend” its own tokens (i.e., spend the same tokens in more than one transaction) and prevent the confirmation of other users’ transactions for so long as it maintained control. To the extent that such malicious actor or botnet did not yield its control of the processing power on the relevant digital asset network or the digital asset community did not reject the fraudulent blocks as malicious, reversing any changes made to the relevant blockchain may not be possible. Further, a malicious actor or botnet could create a flood of transactions in order to slow down the relevant digital asset network.

For example, in August 2020, the Ethereum Classic Network was the target of two double-spend attacks by an unknown actor or actors that gained more than 50% of the processing power of the Ethereum Classic Network. The attacks resulted in reorganizations of the Ethereum Classic Blockchain that allowed the attacker or attackers to reverse previously recorded transactions in excess of over \$5.0 million and \$1.0 million.

In addition, in May 2019, the Bitcoin Cash network experienced a 51% attack when two large mining pools reversed a series of transactions in order to stop an unknown miner from taking advantage of a flaw in a recent Bitcoin Cash protocol upgrade. Although this particular attack was arguably benevolent, certain individuals believe it negatively impacted the Bitcoin Cash network.

Further, a malicious actor or botnet could create a flood of transactions in order to slow down the relevant digital asset network. For example, on June 2, 2018, the Horizen network was the target of a double-spend attack by an unknown actor that gained more than 50% of the processing power of the Horizen network. The attack was the result of delayed submission of blocks to the Horizen network. The core developers of Zen have implemented mitigation procedures to significantly increase the difficulty of attacks of this nature by introducing a penalty for delayed block submissions.

The crossing of the 50% threshold indicates a greater risk that a single mining pool or small group of mining pools could exert authority over the validation of digital asset transactions, and this risk is heightened if over 50% of the processing power on the network falls within the jurisdiction of a single governmental authority. To the extent that such events occur on the network of a digital asset that we hold, if the network participants, including any core developers and administrators of mining pools, do not ensure greater decentralization of mining processing power of such network, the

feasibility of a malicious actor obtaining control of the processing power on such network will increase, which may adversely affect our business.

More generally, the practice of Maximum Extractable Value (“MEV”), has become standard and widespread across proof-of-stake-based smart contracting platforms like Ethereum. MEV also refers to “Miner Extractable Value” for proof-of-work-based platforms like the Bitcoin Network. MEV is the practice by which miners and validators exploit their role in a particular digital asset network in order to extract value from transactors by censoring, frontrunning, backrunning or otherwise executing arbitrage strategies against transactors. MEV can reduce the effectiveness of certain blockchain transactions and in turn increase the cost of transacting on networks, which may discourage users from transacting on such networks altogether. There are currently no means to completely mitigate the effects of MEV, and to the extent that we transact on these blockchains, whether for proprietary purposes or on behalf of our clients, we may be unable to protect ourselves or our clients from the effects or impacts of MEV, which could include a reduction in the speed, quality and/or security of our trades. Furthermore, if any one digital asset network’s user experience is harmed at scale, the value of the digital assets carried on that network could decline. The occurrence of any of the aforementioned risks associated with MEV could adversely affect the value of our transactions and investments, our ability to operate efficiently and the market price of our Class A common stock.

A malicious actor may also obtain control over the Bitcoin network through its influence over core developers by gaining direct control over a core developer or an otherwise influential programmer. To the extent that the Bitcoin ecosystem does not grow, the possibility that a malicious actor may be able to obtain control of the processing power on the Bitcoin network in this manner will remain heightened.

Any of the above events could materially and adversely affect certain of our investments and trading strategies, the value of our assets and the value of any investment in us.

Any inability to maintain adequate relationships with affiliates, third-party banks and trading venues with respect to, and any inability to settle customer trades related to, our cryptocurrency offerings, may adversely affect our business, financial condition and results of operations.

We rely on our affiliates, third-party banks and trading venues to provide our cryptocurrency products and services to our customers. The cryptocurrency market operates 24 hours a day, seven days a week. The cryptocurrency market does not have a centralized clearinghouse, and transactions in cryptocurrencies rely on direct settlements between third parties after trades are executed. Accordingly, we rely on our affiliates and third-party banks to facilitate cash settlements between customers and us and rely on the ability of our trading venues to complete cryptocurrency settlements. In addition, we must maintain cash assets in our bank accounts sufficient to meet the working capital needs of our business, which includes deploying available working capital to facilitate cash settlements between us and our customers or us and our trading venues. If our affiliates, third-party banks or trading venues have operational failures and cannot perform and facilitate our routine cash and cryptocurrency settlement transactions, we will be unable to support normal cryptocurrency trading operations and these disruptions could have an adverse impact on our business, financial condition and results of operations. Similarly, if we fail to maintain cash assets in our bank accounts sufficient to meet the working capital needs of our business and necessary to complete routine cash settlements related to our trading activity, such failure could impair our ability to support normal trading operations and these disruptions could have an adverse impact on our business, financial condition and results of operations.

We may also be harmed by the loss of any of our banking partners and trading venues. As a result of the many regulations applicable to cryptocurrencies, the risks of digital assets generally, and pressure from their regulators, many financial institutions have decided or been forced, and other financial institutions may in the future decide, to not provide bank accounts (or access to bank accounts), payments services or other financial services to companies providing cryptocurrency products, including us. Similarly, a number of such companies have had their existing bank accounts closed by their banks. Banks may refuse to provide bank accounts and other banking services to digital asset-related companies, including us, for a number of reasons, such as perceived compliance risks or costs. Galaxy has in the past held accounts at Silvergate Bank and Signature Bank. We have diverse U.S. banking relationships, with most of our deposits at large, systemically important financial institutions. Although Galaxy did not experience any losses or other material impact from our banking relationships with Silvergate Bank and Signature Bank, any inability to procure or keep banking services would have a material and adverse effect on us. Similarly, continued general banking difficulties may decrease the utility or value of digital assets or harm public perception of those assets. In addition to banks, other third-party service providers including accountants, lawyers and insurance providers may also decline to provide services to companies engaged in digital asset-related businesses because of the perceived risk profile associated with such businesses or the lack of regulatory certainty. Consequently, if we or our trading venues cannot maintain sufficient relationships with the banks that provide these services, banking regulators restrict or prohibit banking of cryptocurrency businesses, or if these banks

impose significant operational restrictions, it may be difficult for us to find alternative business partners for our cryptocurrency offerings, which may result in a disruption of our business and could have an adverse impact on our reputation, business, investment and trading strategies, the value of our assets, the value of any investment in us, financial condition and results of operations.

GalaxyOne is subject to risks associated with the execution, transfer, and custody of cryptocurrency, specifically through our partnership with Paxos, which may adversely affect its business and financial performance.

Retail customers can use the GalaxyOne platform to access GalaxyOne Crypto, a technology platform that connects GalaxyOne customers (“End Users”) to Paxos via API to buy, sell, hold, and transfer cryptocurrency. We partner with Paxos for execution, transmission, and custody of End Users’ cryptocurrency. Paxos is a New York State-chartered trust company, overseen by the NYDFS, supporting cryptocurrency custody for End Users. Paxos is also registered as a money service business with FinCEN and maintains money transmitter licenses in a number of states in order to effect aspects of its trading business, including execution and transmission of cryptocurrency for End Users.

As further detailed under “—Risks Related to Our Business Lines,” the laws and regulations applicable to cryptocurrency are evolving and subject to interpretation and change, and GalaxyOne Crypto relies substantially on Paxos to comply with the requirements. Therefore, our current and future cryptocurrency services may be or become subject to additional licensing and regulatory requirements by other state and federal authorities, whether those requirements are imposed on us, Paxos, or both. Failure by Paxos to comply with these requirements may result in, among other things, revocation of required licenses or registrations, loss of approved status, private litigation, administrative enforcement actions, sanctions, civil and criminal liability, and constraints on our ability to continue our partnership, all of which could materially impact our business, our ability to grow or to continue to operate, and could result in client dissatisfaction and reputational harm and expose us to client claims for damages.

In addition to the other risks disclosed under “—Risks Related to Our Business Lines,” there may be additional risks associated with our custody arrangements with Paxos, its obligations and limitations as a regulated New York State-chartered trust company, and with respect to federal or state law, our contractual relationship with the trust company, and other obligations of the trust company that may impact its ability to provide the products and services to our customers described herein.

Competing industries may have more influence with policymakers than the digital asset industry, which could lead to the adoption of laws and regulations that are harmful to the digital asset industry and our business.

The cryptoeconomy is relatively novel and until recently did not have the same access to policymakers and lobbying organizations in many jurisdictions compared to industries with which digital assets may be seen to compete, such as banking, payments and consumer finance. Competitors from other, more established industries may have greater access to and influence with governmental officials and regulators and may be successful in persuading these policymakers that digital assets require heightened levels of regulation compared to the regulation of traditional financial services. As a result, new laws and regulations may be proposed and adopted in the United States and elsewhere, or existing laws and regulations may be interpreted in new ways, that disfavor or impose compliance burdens on the cryptoeconomy or digital asset platforms, which could adversely impact the digital assets in which we invest and therefore the value of any investment in our business.

As digital assets have grown in both popularity and market size, various U.S. federal, state, and local and foreign governmental organizations, consumer agencies and public advocacy groups have been examining the operations of cryptocurrency networks, users and platforms, with a focus on how digital assets can be used to launder the proceeds of illegal activities, fund criminal or terrorist enterprises in the United States, and the safety and soundness of platforms and other service providers that hold digital assets for users. Many of these entities have called for heightened regulatory oversight, and have issued consumer advisories describing the risks posed by digital assets to users and investors.

For instance, on September 16, 2022, the U.S. Treasury and Justice Departments released regulatory and legislative recommendations and priorities to address illicit finance risks connected to the digital assets ecosystem, following former President Biden’s executive order on the regulation of digital assets. The reports reflect the proactive posture that both the U.S. Treasury and Justice Departments have taken towards the enforcement and implementation of AML standards in the digital asset ecosystem. As part of its AML efforts, the U.K.’s Financial Conduct Authority (“FCA”) requires cryptoasset businesses to be duly registered with the FCA under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The FCA has also introduced rules to address harm to retail customers arising from the sale of derivatives and exchange-traded notes that reference certain types of cryptoassets, contending that they are “ill-suited” to retail consumers due to extreme volatility, valuation challenges and association with financial

crimes. The rules, which entered into force on January 6, 2021, prohibit the sale, marketing and distribution to retail clients in the U.K. of derivatives and exchange traded notes that reference certain types of unregulated, transferable cryptoassets. The prohibition applies to investment firms, credit institutions and branches in the U.K. of third-country firms (among others) that market, distribute or sell digital asset-derivatives or digital asset trading platform traded notes in, or from, the U.K. to retail clients. Many types of cryptoassets, including popular cryptocurrencies such as bitcoin, are also subject to the U.K.'s financial promotions regime. It is a criminal offense for these products to be marketed in the U.K. unless the relevant financial promotion has been approved by an FCA authorized firm or an exemption applies. The exemptions are narrow and will generally only be available to sophisticated investors. The FCA is currently finalizing additional rules in this space and is likely to introduce new requirements on industry participants in fiscal years 2025 to 2026, including new regulations for stablecoin providers and cryptocurrency trading venues. To the extent other U.S. and foreign regulatory authorities or legislative bodies adopt other or additional regulations or legislation applicable to the digital asset industry or any other aspect of our business, we could face a heightened risk of potential regulatory violations and could be required to make significant changes to our business model and practices, which changes might not be successful. Any of these outcomes could have an adverse effect on our business, financial condition and results of operations.

We currently offer services involving, and expect to continue to support, certain smart contract-based digital assets. If the underlying smart contracts for these protocols do not operate as expected, they could lose value and our business could be adversely affected.

We currently offer services involving, and expect to continue to support, various digital assets that represent units of value through the use of smart contracts deployed on a blockchain. Smart contracts are programs that store and transfer value and execute automatically when certain conditions are met. Since smart contracts typically cannot be stopped or reversed, vulnerabilities in their programming and design can have damaging, and even permanent, ramifications. For instance, in April 2018, a batch overflow bug was found in many Ethereum-based ERC20-compatible smart contract tokens that allowed hackers to create a large number of smart contract tokens, causing multiple digital asset platforms worldwide to shut down ERC20-compatible token trading. Similarly, in March 2020, a design flaw in the MakerDAO smart contract caused forced liquidations of digital assets at significantly discounted prices, resulting in millions of dollars of losses to users who had deposited digital assets into the smart contract. If any such vulnerabilities or flaws come to fruition, smart contract-based digital assets may suffer negative publicity, be exposed to security vulnerabilities, decline significantly in value, and lose liquidity over a short period of time. As smart contract-based digital assets continue to develop and evolve, we may be subject to unintended or unforeseen regulatory risks and regulatory actions, which may be inconsistently applied across jurisdictions.

In some cases, smart contracts can be controlled by one or more “admin keys” or users with special privileges, or “super users.” These users have the ability to unilaterally make changes to the smart contract, enable or disable features on the smart contract, change how the smart contract receives external inputs and data, and make other changes to the smart contract. For smart contracts that hold a pool of assets, these users may also be able to extract funds from the pool, liquidate assets held in the pool, or take other actions that decrease the value of the assets held by the smart contract in reserves. Even for smart contracts that have adopted a decentralized governance mechanism, such as smart contracts that are governed by the holders of a governance token, such governance tokens can be concentrated in the hands of a small group of core community members, who would be able to make similar changes unilaterally to the smart contract. If any such super user or group of core members unilaterally make adverse changes to a smart contract, the design, functionality, features and value of the smart contract, its related digital assets may be harmed. In addition, assets held by the smart contract in reserves may be stolen, misused, burnt, locked up or otherwise become unusable and irrecoverable. These super users can also become targets of hackers and malicious attackers. If an attacker is able to access or obtain the super user privileges of a smart contract, or if a smart contract’s super-users or core community members take actions that adversely affects the smart contract, our customers who hold and transact in the affected digital assets may experience decreased functionality and value of the applicable digital assets, up to and including a total loss of the value of such digital assets. Although we do not control these smart contracts, any such events could cause customers to seek damages against us for their losses, result in reputational damage to us, or in other ways adversely impact our business.

We currently engage in transactions on DeFi protocols involving the provision of and access to liquidity of various types of digital assets using liquidity pools, which subjects us to a number of risks and uncertainties, each of which could adversely affect our business.

We currently engage in transactions on DeFi protocols involving the provision of and access to liquidity of various types of digital assets using liquidity pools. Liquidity pools enable borrowing, lending, and trading of digital assets directly with smart contract platforms. Interacting with smart contracts is subject to certain risks and uncertainties that could adversely affect our business. See “—We currently offer services involving, and expect to continue to support, certain

smart contract-based digital assets. If the underlying smart contracts for these protocols do not operate as expected, they could lose value and our business could be adversely affected.” In addition, liquidity pools are relatively new and do not appear to be subject to specific regulation in the same manner as traditional trading platforms. Furthermore, while some digital asset trading platforms provide information regarding their ownership structure, management teams, private key management, hot/cold storage policies, capitalization, corporate practices and regulatory compliance, the creators of liquidity pools within DeFi protocols typically do not. Such lack of transparency could result in us underestimating or otherwise misunderstanding the functionality of a specific liquidity pool and thus increase the risk of a potential loss in balances, which could include the loss of a material portion of the value of the digital assets we own or lend using such liquidity pools. Such loss could also be incurred through a bad actor taking advantage of the underlying smart contract’s operations, which could involve manipulating the DeFi protocol’s underlying digital assets or the pricing of trading pairs of digital assets. As a result, some DeFi protocols and liquidity pools may be used beyond their intended use case for fraud or other dishonest or illicit behaviors.

Liquidity pools generally do not seek to, or cannot, comply with regulation in a similar manner as digital asset trading platforms or regulated trading platforms, such as national securities exchanges or designated contract markets. As a result, the marketplace may lose confidence in unregulated liquidity pools and DeFi protocols, including prominent liquidity pools and DeFi protocols we use. Because liquidity pools use Automated Market Makers (“AMMs”), which allow for continuous trading based on supply and demand dynamics, a loss of confidence in a given DeFi protocol or liquidity pool could materially impact the price of digital assets within that DeFi protocol or liquidity pool. In addition, when digital assets are sent to a liquidity pool, they are provided at a set ratio with the goal of ensuring liquidity for trading at all times. The pricing of assets within the pools is determined algorithmically based on the balance of assets in those pools. Any changes in prices of digital assets in liquidity pools could lead to temporary losses, commonly referred to as impermanent loss. Impermanent loss occurs when the value of digital assets in a liquidity pool diverges from their initial ratio and may diverge from other market prices for such digital assets, such that holding the liquidity provider token representing a share in the liquidity pool may be worth less than simply holding the underlying assets directly. Furthermore, using liquidity pools may sometimes require us to lock digital assets in smart contracts. As a result, we may not be able to quickly unlock such digital assets and sell them, whether in response to a vulnerability or price volatility, or at a time when we may otherwise desire liquidity for any number of reasons.

Additionally, market fluctuations affect the value of rewards that we can earn when engaging in yield farming. As a relatively new phenomenon, the prices of digital assets that are subject to yield farming can be extremely volatile. The volatility of such digital assets itself causes a risk that our positions in liquidity pools become liquidated if we have borrowed from liquidity pools against a digital asset that decreases in value and we cannot provide enough additional collateral in time prior to automatic liquidation being triggered. Also, a single event or exploit within one relevant DeFi protocol or liquidity pool can trigger a cascading effect across multiple platforms, causing widespread selling activity and further exacerbating volatility.

Yield farming and the use of liquidity pools are also subject to regulatory uncertainty. Yield farming typically involves a number of different transactions and interactions with multiple protocols (lending, borrowing, and receiving digital assets that represent a share of a liquidity pool) that may individually or taken together fall under the purview of a number of state or federal regulatory authorities. However, the extent to which any such regulation applies to these activities remains an area of significant uncertainty. Because there is uncertainty regarding how yield farming, liquidity pools and DeFi protocols should be regulated, and the extent to which such activities are subject to existing regulations, participating in such activities poses heightened regulatory concerns. See “—DeFi protocols and digital assets used in DeFi protocols pose heightened regulatory concerns even beyond those that face digital asset networks and digital assets generally.”

The value of NFTs, any investment in NFTs, and the regulation of NFTs are uncertain and may subject us to unforeseeable risks.

We have developed and invest, directly and indirectly through our sponsored funds, in NFTs. We also invest in companies that create and support NFTs. NFTs are unique, one-of-a-kind digital assets made possible by certain digital asset network protocols. Because of their non-fungible nature, NFTs introduce digital scarcity and have become popular as online “collectibles,” similar to physical rare collectible items, such as trading cards or art. Like real world collectibles, the value of NFTs may be prone to “boom and bust” cycles as popularity increases and subsequently subsides. Certain metadata pertaining to NFTs or the collectible itself (such as digital art) represented by the NFT may be stored “offchain,” i.e., not on a decentralized digital asset network. If the entity behind an NFT project or its third-party hosting service or platform ceases hosting relevant data relating to NFTs, such NFTs may become worthless. If any of these events were to occur, it could adversely affect the value of certain of our future investments and strategies. In addition, because NFTs generally rely on the same types of underlying technologies as digital assets, most risks applicable to digital assets

(including phishing, hacking and blockchain risks) are also applicable to NFTs and hence any investment into NFTs will be subject to general digital assets risks as described elsewhere in these risk factors. We have also developed and released our own NFTs. Prior to developing and releasing an NFT, we consult external legal counsel to gain comfort that the NFTs we develop and release are not securities under the federal securities laws. However, we recognize that the application of the securities laws to NFTs is particularly uncertain, as most guidance related to the application of the federal securities laws to digital assets has been applied to more fungible forms of digital assets, such as cryptocurrencies. Any determination that the NFTs we develop and release are securities under the federal securities laws would adversely affect us. See “—Risks Related to Our Operations—A determination that a digital asset is a “security,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could adversely affect the value of that digital asset and potentially digital assets generally, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock.”

Private keys are required to access or transfer cryptocurrencies held in custody for GPL and GPL customers and the loss or destruction of such private keys may cause complete loss of the ability to retrieve or transfer such cryptocurrencies. If our custodian is unable to access the private keys and any backups thereto or if it experiences a cybersecurity breach, hack or other data loss that would restrict its ability to access any cryptocurrencies held in custody, we could become subject to reputational harm, legal claims, regulatory scrutiny, and other losses.

Cryptocurrency assets are typically controlled by the holder of the unique private key for the cryptocurrency wallet in which the cryptocurrency assets are held. While public addresses are generally published when used in a transaction on a blockchain, private keys are required to access, retrieve or transfer the cryptocurrency assets in the wallet. Therefore, protection and safekeeping of private keys is necessary to prevent unauthorized third party access to or control over the cryptocurrency assets held in a cryptocurrency wallet. The custodian for digital assets stored on behalf of GPL or GPL customers maintains at all times at least one backup set of keys for this wallet. If any of the private keys for these wallets are stolen, destroyed, lost or otherwise compromised or unavailable, and if the backup versions of these private keys are not available at the time or have been otherwise stolen or compromised, our custodian will not be able to access the digital assets held in the omnibus wallets. Blockchain technologies that hold digital assets, such as wallets and smart contracts, can be hacked or otherwise subject to security breaches and other malicious activities, which may result in, among other things, malicious actors obtaining the ability to retrieve, transfer and otherwise misappropriate the digital assets held in custody for GPL and GPL customers. Destruction, loss or theft of private keys for, or hack or other compromise or unavailability of, the wallets holding digital assets held for GPL and GPL customers could adversely affect customers’ ability to retrieve, access or transfer the digital asset, could require the relevant custodian to pay reimbursements to customers and/or other third parties for their losses, and could subject such custodian to significant liabilities and financial losses in addition to losing trust of customers and other market participants. For these reasons, any destruction, loss or theft of private keys due to a hack, misconduct or error, or any other compromise of the security and confidentiality of the private keys for the cryptocurrency wallets holding digital assets could harm our brand and reputation, could result in significant legal liability or other financial losses, and could adversely impact our business.

Risks Related to Regulation, Information Systems and Privacy Matters

The financial services industry is subject to government regulation in the United States, and our failure or inability to comply with these regulations or regulatory action against us could adversely affect our results of operations, financial condition or business.

The financial services industry is among the most extensively regulated industries in the United States. We operate a commodity trading advisor/commodity pool operator, an investment adviser, and three broker-dealers, each of which is subject to a specific and extensive regulatory scheme. In addition, our subsidiary Galaxy Derivatives LLC (“GDL”) is a registered CFTC-regulated swap dealer. We are subject to numerous state and federal laws and regulations of general application. It is very difficult to predict the future impact of the legislative and regulatory requirements affecting our business and our clients’ businesses.

Our businesses may require regulatory licenses and qualifications that we do not currently have and that may be costly and time-consuming to obtain and, if obtained, may subsequently be revoked. Although we have the authorizations and licenses that we believe are necessary to operate our business in all material respects, with respect to certain jurisdictions, we take the view that we are not conducting regulated activities requiring specific licenses. We acknowledge that relevant regulators in such jurisdictions may take a different view, and changes in regulators’ interpretation of existing licensing statutes or regulations, or disagreement by a regulatory authority with our interpretation of such statutes or regulations, could require additional registrations or licenses, limit certain of our business activities until they are appropriately licensed, and expose us to financial penalties or other non-monetary penalties, or could damage our reputation. We consult with external counsel regarding changes in the relevant laws or regulations and refresh our assessment on a regular basis.

Our subsidiary Galaxy Digital Capital Management LP (“GDCM LP”) is registered as an “investment adviser” with the SEC under the Advisers Act and is regulated thereunder. GDCM LP, and certain affiliates, also manage several funds that do not invest in securities and therefore GDCM LP, and such affiliates, do not manage such funds in a registered investment adviser capacity. GDCM LP also intends to provide advice to funds that are registered as “investment companies” under the Investment Company Act. Moreover, the Advisers Act mandates that if a registered adviser has custody of client funds and securities, it must maintain them with a Qualified Custodian. Given the characteristics of digital assets and the relative immaturity of the asset class, there are limited numbers of Qualified Custodians available at this time (if any) and there can be no assurance that we will ourselves qualify as, or be successful in maintaining client funds and securities with, a Qualified Custodian. Difficulties in finding a Qualified Custodian could have a material adverse effect on the asset management business, including potentially causing it to liquidate a substantial portion of our asset management portfolio. There is also a risk that the SEC determines that certain custodians used are not, regardless of their representations to the contrary, Qualified Custodians, which would potentially require the asset management group to move certain digital assets and/or subject it to regulatory action. The uncertainty and potential difficulties associated with this question and related questions could materially and adversely affect our asset management business. The Advisers Act and the Investment Company Act, together with related regulations and interpretations of the SEC, impose numerous obligations and restrictions on investment advisers and mutual funds, including requirements relating to the safekeeping of client funds and securities, limitations on advertising, disclosure and reporting obligations, prohibitions on fraudulent activities, restrictions on certain transactions between an adviser and its clients, and between a mutual fund and its advisers and affiliates, and other detailed operating requirements, as well as general fiduciary obligations.

Our subsidiary Galaxy DBL LLC is a CFTC-regulated commodity trading advisor and commodity pool operator and is a member of the NFA. In addition, our subsidiary GDL is a registered CFTC-regulated swap dealer. As such, Galaxy DBL LLC and GDL are subject to regulatory requirements under the Commodity Exchange Act, CFTC regulations and NFA bylaws and regulations. These include disclosure, recordkeeping, cybersecurity and reporting requirements, restrictions on advertising, registration and licensing of certain personnel and conduct and anti-fraud requirements, among others. Failure to comply with these regulations could result in injunctions, cease and desist orders, as well as civil monetary penalties, fines, and disgorgement, as well as reputational harm. In addition, Galaxy’s customers may face additional costs for transactions with Galaxy (such as certain requirements related to margin posting and collection) that may make those customers less willing to trade swaps with Galaxy.

Galaxy Digital Partners LLC (“GDP”), Galaxy Securities, LLC (“GSL”) and FIN2, our broker-dealer subsidiaries, are subject to regulatory restrictions and requirements imposed by the SEC, FINRA, state securities regulators, and other relevant governmental authorities and self-regulatory organizations in the jurisdictions in which we operate. U.S. government agencies and self-regulatory organizations, including U.S. state securities commissions, are empowered to enforce the regulatory restrictions and requirements applicable to us and conduct administrative proceedings that can result in censure, fine, the issuance of cease-and-desist orders or the suspension or expulsion of a broker-dealer from registration or membership. GDP is registered as a broker-dealer in 53 U.S. states and territories, and each of GSL and FIN2 are registered broker-dealers in 51 U.S. states and territories. GDP, GSL and FIN2 are all members of, and are subject to periodic examinations and investigations by, FINRA. Further, GDP, GSL and FIN2 are subject to the Bank Secrecy Act, as amended by the USA PATRIOT Act of 2001, and the implementing regulations thereunder, which require financial institutions, including broker-dealers, to establish AML compliance programs, file suspicious activity and other reports with the U.S. government and maintain certain records. Broker-dealers and mutual funds must also implement related customer identification procedures and beneficial ownership identification procedures.

Our KYC and onboarding processes are designed to verify the identity of our customers, manage associated risks and prevent offers and sales of some digital assets and other products and services to certain persons, it is nevertheless possible that customers could intentionally and fraudulently provide us with false information, act contrary to, or otherwise circumvent, our KYC and onboarding policies or procedures. Any improper provision of false information or circumvention of our KYC policies or procedures could result in unintended offering or sale of our services and products to parties that we intend to restrict from our services or products and one or more regulators deeming our KYC policies and procedures inadequate and not in compliance with relevant laws and regulations. We also have policies and procedures relating to the safeguarding of digital assets, which are designed to prevent conflicts of interest, including the comingling of assets. See “—Our and our third-party service providers’ failure to safeguard and manage our and our customers’ funds and digital assets could adversely impact our business, operating results and financial condition” below for additional information. Any circumvention or failure of our policies could, among other things, require changes to our business practices and scope of operations or harm our reputation, which, in turn could have a material adverse effect on our results of operations, financial condition or business.

Our subsidiary GalaxyOne Prime LLC is registered as a money service business with FinCEN and has money transmitter licenses in a number of states in order to effect aspects of its trading business. GalaxyOne Prime NY LLC, which has applied for a BitLicense and a money transmitter license in New York State, also recently became a FinCEN-registered money services business. As a money services business, GPL is subject to the applicable anti-money laundering rules and any other laws and regulations applicable to a money services business. Furthermore, a number of U.S. states have adopted specific statutory provisions, or have issued guidance, regarding the treatment of virtual currencies under the money transmitter requirements of that U.S. state, and California has enacted the Digital Financial Assets Law (the “DFAL”), which will come into effect on July 1, 2026, that is broadly similar to the BitLicense regulation in New York State.

In addition, due to our business activities, we are subject to ongoing examinations, oversight, and reviews by U.S. federal and state regulators, and financial service regulators, which each have broad discretion to audit and examine our business. We are periodically subject to audits and examinations by these regulatory authorities. As a result of findings from these audits and examinations, regulators have, are, and may in the future require us to take certain actions, including amending, updating, or revising our compliance measures from time to time, limiting the kinds of customers which we provide services to, changing, terminating, or delaying the introduction of our existing or new product and services, and undertaking further external audits or being subject to further regulatory scrutiny. We have received, and may in the future receive, examination reports citing violations of rules and regulations, inadequacies in existing compliance programs, and requiring us to enhance certain practices with respect to our compliance program, including due diligence, monitoring, training, reporting, and recordkeeping. Implementing appropriate measures to properly remediate these examination findings may require us to incur significant costs, and if we fail to properly remediate any of these examination findings, we could face civil litigation, significant fines, damage awards, forced removal of certain employees including members of our executive team, barring of certain employees from participating in our business in whole or in part, revocation of existing licenses, limitations on existing and new products and services, reputational harm, negative impact to our existing relationships with regulators, exposure to criminal liability, or other regulatory consequences. Further, should strict legal and regulatory requirements and additional regulatory investigations and enforcement occur or intensify, it may continue to result in changes to our business, as well as increased costs, and supervision and examination for both us and our agents and service providers. Moreover, new laws, regulations, or interpretations may result in additional litigation, regulatory investigations, and enforcement or other actions, including preventing or delaying us from offering certain products or services offered by our competitors or could impact how we offer such products and services. Adverse changes to, or our failure to comply with, any laws and regulations have had, and may continue to have, an adverse effect on our reputation and brand and our business, operating results, and financial condition. Such additional requirements could cause us to incur extraordinary expenses, possibly materially and adversely affecting our investment and trading strategies, the value of our assets and the value of any investment in us.

All of the foregoing laws and regulations, as well as any other laws and regulations we are or may become subject to, are complex and we are required to expend significant resources to monitor and maintain our compliance with such laws and regulations. It is also possible that a new Administration and a new Congress in the United States implements new laws and regulations that we may be required to expend significant resources on understanding and complying with. Any failure on our part to comply with these and other applicable laws and regulations could result in regulatory fines, suspensions of personnel or other sanctions, including revocation of our registration or that of our subsidiaries as an investment adviser, broker-dealer, commodity pool operator, commodity trading adviser, swap dealer (if and when granted) or trust company, as the case may be, which could, among other things, require changes to our business practices and scope of operations or harm our reputation, which, in turn could have a material adverse effect on our results of operations, financial condition or business.

In addition, financial services regulation is constantly changing, and new laws or regulations, or new interpretations of existing laws or regulations, could have a materially adverse impact on our ability to operate as currently intended, or require us to obtain additional or newly-created registrations or licenses in the future and cause us to incur significant expense in order to ensure compliance. It is not currently clear to what extent federal and state financial services regulators will continue enforcing existing laws, regulations, and rules and will continue to enhance their supervisory expectations regarding the management of legal and regulatory compliance risks. These regulatory changes and uncertainties make our business planning more difficult and could result in changes to our business model and potentially adversely impact our results of operations.

Proposals to change the statutes affecting financial services companies are frequently introduced in Congress and state legislatures that, if enacted, may affect their operating environment and the registrations or licenses Galaxy requires in substantial and unpredictable ways. In addition, numerous federal and state regulators have the authority to promulgate or change regulations that could have a similar effect. We cannot determine with any degree of certainty whether any such

legislative or regulatory proposals will be enacted and, if enacted, the ultimate impact that any such potential legislation or implementing regulations, or any such potential regulatory actions by federal or state regulators, would have upon our business.

Our subsidiary Galaxy Digital UK Limited (“GD UK”) is authorized by the FCA and has permission to carry on a range of regulated activities, including, but not limited to, advising on certain investments, arranging deals in certain investments and dealing in certain investments as principal and agent. For example, GD UK’s permissions mean that it can enter into derivatives with customers that are professional clients and eligible counterparties. GD UK has been authorized by the FCA since December 17, 2024. As an FCA authorized firm, GD UK is subject to a range of laws and regulations, including, but not limited to, U.K. AML requirements, the FCA’s conduct of business obligations, regulatory reporting requirements and corporate governance obligations. Failure by GD UK to comply with these obligations may result in investigations and enforcement action by the FCA or other regulatory authorities in the U.K.

New laws, regulations, policy or changes in enforcement of existing laws or regulations applicable to our business, or reexamination of current practices, could adversely impact our profitability, limit our ability to continue existing or pursue new business activities, require us to change certain of our business practices or the registrations or licenses we are required to hold or obtain, affect retention of key personnel, or expose us to additional costs (including increased compliance costs and/or customer remediation). These changes also may require us to invest significant resources, and devote significant management attention, to make any necessary changes and could adversely affect our business.

We are subject to risks related to the banking ecosystem, including through our GalaxyOne bank partnerships, FDIC regulations and policies, and other regulatory obligations, which may adversely affect our GalaxyOne business and financial performance.

The GalaxyOne platform, through GalaxyOne Holdings LLC, offers access to FDIC-insured high-yield demand deposit accounts offered by our bank partner Cross River Bank, Member FDIC. Customers who open a demand deposit account with Cross River Bank may also be issued debit cards by Cross River Bank. The Cross River Bank Deposit Account Agreement signed by our customers states that funds held by our customers in their Cross River Bank demand deposit account are eligible for insurance from the FDIC, up to the applicable limit.

We believe the demand deposit accounts offered by Cross River Bank through GalaxyOne and Cross River Bank currently comply and will continue to comply with all applicable requirements for each eligible customer’s deposits made through our platform to be covered by FDIC insurance. However, because Cross River Bank is a member of the FDIC instead of us, it is ultimately the responsible party for ensuring that customer funds held at the bank remain eligible for FDIC insurance up to the applicable limit.

If we or a non-bank third party that we work with (such as card networks and payment processors) were to fail or file for bankruptcy, FDIC deposit insurance would not cover any losses associated with that failure and receivership proceedings would not be entered into under the Federal Deposit Insurance Act (“FDIA”), because we are not a bank, nor are the non-bank third parties we work with. For example, if Cross River Bank were to fail and enter receivership proceedings under the FDIA (regardless of whether we or any of the non-bank third parties we work with also fail or file for bankruptcy) and if customers’ deposits were not covered by FDIC insurance, customers may seek to hold us liable for the full amount of their uninsured deposit losses, and any such claims or litigation could be costly to address. Additionally, if we, a non-bank third party we work with, or Cross River Bank were to fail (regardless of whether the deposits are covered by FDIC insurance), or if there were concerns of any of the foregoing, our customers may seek to withdraw their funds, or may not be able to withdraw all their funds in a timely manner, which may adversely affect our GalaxyOne business and financial performance, including by leading to claims or litigation that may be costly to address and harm our reputation.

Additionally, through contractual obligations to Cross River Bank in connection with this program, we are subject to risk management standards for third-party relationships in accordance with federal bank regulatory guidance and examinations by the federal banking regulators. Should we or Cross River be unable to satisfy these standards, we may have to discontinue certain products or the entirety of the relationship, and our GalaxyOne business and financial performance may be adversely affected.

In addition to the other risks disclosed under “—Risks Related to Our Operations,” there may be additional risks associated with our partnership with Cross River Bank, including but not limited to its operations, its obligations and limitations as a regulated bank under federal or state law, our contractual relationship with Cross River Bank, and other obligations of Cross River Bank that may impact its ability to provide the products to our customers described herein.

GalaxyOne is subject to risks associated with the regulation of broker-dealers, including through our partnership with DriveWealth, which may adversely affect its business and financial performance.

GalaxyOne, through FIN2, a registered broker-dealer and member of FINRA, offers traditional brokerage accounts to retail customers. FIN2 operates as an introducing broker on a fully-disclosed basis, with accounts being carried by DriveWealth, an unaffiliated registered broker-dealer and member of FINRA and various other self-regulatory organizations. GalaxyOne's brokerage services also offer customers a stock lending ("GalaxyOne Rewards") program through FIN2, with clearing and custody services provided by DriveWealth. Through the GalaxyOne Rewards program, FIN2 customers make certain fully paid or excess customer margin securities available for lending to other market participants.

As registered broker-dealers, FIN2 and our other two affiliate broker-dealers are subject to regulations that cover all aspects of their businesses, including sales practices, customer disclosures, AML and KYC obligations, use and safekeeping of customers' funds and securities, capital adequacy, recordkeeping and the conduct of directors, officers, employees, representatives and associated persons. FINRA and the SEC conduct periodic examinations of the operations of broker-dealers. Violation of applicable regulations can result in the suspension or revocation of a broker-dealer's registration, the imposition of censures or fines and the suspension or expulsion of the broker-dealer from FINRA.

In addition to the other risks disclosed under "—Risks Related to Our Operations," there may be additional risks associated with our clearing arrangement with DriveWealth, upon whom FIN2 relies to provide clearing services and carry FIN2's brokerage customers accounts. These risks include those arising from FIN2's operations, obligations and limitations as a registered broker-dealer under federal or state law, our contractual relationship with DriveWealth and other obligations of DriveWealth that may impact its ability to provide the products to us and our customers described herein.

For example, to the extent DriveWealth is unwilling or unable to perform its usual functions coupled with the unavailability of alternative arrangements, which may be due to market volatility, uneconomic trading conditions, capacity constraints, financial constraints, system failures, unanticipated trading halts invoked by securities exchanges, market closures, or other reasons, GalaxyOne customer transactions may go unexecuted or unsettled. Our inability to get client orders executed or settled because of the unwillingness or inability of DriveWealth to perform its usual functions could result in client dissatisfaction and reputational harm and expose us to client claims for damages.

In addition, in connection with the GalaxyOne Rewards program, DriveWealth offers certain GalaxyOne customers with a brokerage account at DriveWealth access to its Fully Paid Securities Lending program ("FPSL"). FPSL allows Galaxy customers to loan fully-paid securities in their DriveWealth brokerage account to investors and institutions. In return, customers receive a portion of the market-driven interest rate paid by the counterparty as consideration for the loaned security. In accordance with regulatory requirements, in exchange for loaned securities, DriveWealth is required to cause cash or other forms of eligible collateral to be pledged to customers when a customer loans securities. Sharp changes in market values of substantial amounts of securities in a short period of time and the failure by parties to the lending or borrowing transactions to honor their commitments (including DriveWealth's commitment to cause collateral to be pledged to the customer) could result in substantial losses, which could result in client losses, dissatisfaction and reputational harm and expose us to client claims for damages.

Our and our third-party service providers' failure to safeguard and manage our and our customers' funds and digital assets could adversely impact our business, operating results and financial condition.

We may from time to time deposit, transfer and hold in custody with third-party custodians customer funds and digital assets. Our policies, procedures, operational controls and controls over financial reporting are designed to protect us from material risks surrounding commingling of assets, conflicts of interest and the safeguarding of digital assets and customer funds deposited, transferred or held in custody with third-party custodians across jurisdictions. In addition, our security technology is designed to prevent, detect, and mitigate inappropriate access to our systems, by internal or external threats.

Furthermore, our KYC and onboarding processes are designed to verify the identity of our customers, manage associated risks and prevent offers and sales of some digital assets and other products and services to certain persons. We have tailored our AML and KYC protocols to each of our business lines. For our asset management business, there are two main processes and protocols utilized by our funds: the majority of our funds outsource AML and KYC to an industry-standard fund administrator, which requires all investors to undergo a diligence process similar to that of broker-dealers, while our other funds rely on a combination of in-house personnel and an external fund administrator, with in-house personnel collecting documentation required for investor onboarding for the external fund administrator, which performs AML diligence using those materials. For the balance sheet venture investments reflected in our Treasury and Corporate segment, which cover investments made with our firm capital, we utilize a combination of background checks and

representations and warranties, whereby we initially conduct background checks on relevant parties and may perform additional procedures, such as obtaining representations and warranties, as a result of our assessment of such background checks. For our franchise trading and investment banking business, we apply different AML and KYC policies and procedures to sub-segments; for example, our counterparty-facing trading businesses have their own separate AML and KYC regimes, which are handled in-house and modeled after policies similar to the robust procedures that apply to money services businesses. Our investment banking business has implemented AML and KYC policies as outlined by FINRA as a registered broker-dealer. While we do not have one comprehensive set of policies and procedures that apply across this segment, the protocols that are in place are designed to comply with customer due diligence requirements and to address the specific needs of our counterparty-facing and investment banking businesses. Our data center business and our mining business operate similarly, with separate AML and KYC regimes applying to hosting clients and mining finance clients within our mining business, with such in-house regimes being modeled after the procedures that apply to money services businesses and complying with customer due diligence requirements. We do not have a formal policy in place for our GK8 business, but rather deal with any diligence needs on a case-by-case basis consistent with the level of robustness that we apply to our other business lines. We believe we have developed and maintained administrative, technical, and physical safeguards designed to comply with applicable legal requirements and industry standards.

While we have implemented the foregoing AML and KYC protocols within each of our business lines, due to the nature of the digital assets industry and technology, including the pseudonymous nature of blockchain transactions, we may inadvertently or without our knowledge engage in transactions with persons named on OFAC's Specially Designated Nationals list or other blocked or sanctioned persons in connection with our interactions with a blockchain (including through our current or historical proprietary mining activities, for which we rely on the mining pool operators with whom we contract from time to time). Further, fraudulent and illegal transactions and prohibited status could be difficult or impossible for us and our partners, suppliers and vendors to detect in some circumstances. Therefore, there can be no assurance that our AML and KYC protocols will be sufficient to prevent or detect all inappropriate practices, fraud or violations of such laws, regulations and requirements by the Company's affiliates, employees, directors, officers, partners, agents and service providers, in connection with our operations. In the event that our AML and KYC protocols are insufficient to prevent or detect such instances, we could become subject to legal proceedings, inquiries, examinations, investigations, and other regulatory or civil actions, which may subject us to, among other things, fines, penalties, and monetary settlements.

As our business continues to grow, we must continue to strengthen our associated internal controls and ensure that our third-party custodians and other service providers do the same. Our success and the success of our product offerings require significant confidence in our and our third-party service providers' ability to properly custody and manage digital asset balances and handle large and growing transaction volumes and amounts of customer funds. In addition, we are dependent on our third-party service providers' operations, liquidity, and financial condition for the proper custody, maintenance, use and safekeeping of these customer assets. Any material failure by us or such third-party service providers to maintain the necessary controls, policies, safeguarding procedures, perceived or otherwise, or to manage the digital assets we or they hold for or on behalf of our customers or for our own investment and operating purposes could also adversely impact our business, operating results, and financial condition. Further, any material failure by us or our third-party service providers to maintain the necessary controls or to manage customer digital assets and funds appropriately and in compliance with applicable regulatory requirements could result in reputational harm, significant financial losses, lead customers to discontinue or reduce their use of our and our third-party service providers' products and services, and result in significant penalties and fines and additional restrictions, which could adversely impact our business, operating results, and financial condition.

We hold digital assets of the customers of Galaxy Prime, our prime brokerage offering, in omnibus custodial accounts at one or more third party custodians appointed by Galaxy Prime. These custodial accounts are maintained in Galaxy Prime's name for the benefit of its customers. No Galaxy proprietary assets are held in these custodial accounts. In furtherance of our goal of safekeeping customer assets, our Galaxy Prime customer agreements contain an express election intended to apply the protections of Article 8 of the Uniform Commercial Code, as in effect in New York ("Article 8"), to the digital assets held by Galaxy Prime for its customer by providing that all property and assets held in or credited from time to time to a customer's account on Galaxy Prime's books and records will be treated as "financial assets" for purposes of Article 8. If Article 8 applies, we believe that in the event of a bankruptcy of Galaxy Prime the digital assets credited to these customer accounts should not be considered the property of Galaxy Prime's bankruptcy estate and not subject to the claims of its general creditors. However, due to the novelty of digital assets, there can be no certainty as to a bankruptcy court's treatment of these customer assets in such circumstances. As such, there is a risk that such digital assets could be considered to be the property of Galaxy Prime and, in the event of our bankruptcy, customers could be treated as general unsecured creditors of Galaxy Prime with respect to these assets. In addition, the Article 8 election does not apply to digital assets that have been staked through Galaxy's staking services or, if a customer elects to obtain margin financing Galaxy

Prime, to customer margin assets that have been rehypothecated by Galaxy Prime pursuant to an express contractual right to do so.

Furthermore, it is possible that hackers, employees or service providers acting contrary to our or our third-party custodians' policies, or others could circumvent these safeguards to improperly access our systems or documents, or the systems or documents of our third-party service providers or agents, and improperly access, obtain, and misuse customer digital assets and funds. The methods used to obtain unauthorized access, disable, or degrade service or sabotage systems are also constantly changing and evolving and may be difficult to anticipate or detect for long periods of time. Our and our third-party custodians' insurance coverage for such impropriety is limited and may not cover the extent of loss nor the nature of such loss, in which case we may be liable for the full amount of losses suffered, which could be greater than all of our assets. Our and our third-party custodians' ability to maintain insurance is also subject to the insurance carriers' ongoing underwriting criteria. Any loss of customer funds or digital assets could result in a subsequent lapse in insurance coverage, which could cause a substantial business disruption, adverse reputational impact, inability to compete with our competitors, and regulatory investigations, inquiries, or actions. Additionally, transactions undertaken through electronic channels may create risks of fraud, hacking, unauthorized access or acquisition, and other deceptive practices. Any security incident resulting in a compromise of customer assets could result in substantial costs to us and require us to notify impacted customers, and in some cases regulators, of a possible or actual incident, expose us to regulatory enforcement actions, including substantial fines, limit our ability to provide services, subject us to litigation, significant financial losses and adversely impact our brand, reputation, business, results of operations, financial condition and prospects.

Our operations are reliant on technology provided by third parties which are out of our direct control.

Certain strategies and critical aspects of our operations are reliant on technology, including hardware, software and telecommunications systems. Significant parts of the technology used in the management of each client may be provided by third parties and are therefore beyond our direct control. Forecasting, trade execution, data gathering, risk management, portfolio management, information technology infrastructure and support, compliance and accounting systems all are designed to depend upon a high degree of automation and computerization. Although we seek, on an ongoing basis, to ensure adequate backups of software and hardware where possible and will attempt to conduct adequate due diligence and monitoring of providers, such efforts may be unsuccessful or inadequate, and software or hardware errors or failures may result in errors, data loss and/or failures in trade execution, risk management, portfolio management, compliance or accounting. Errors or failures may also result in the inaccuracy of data and reporting or the unavailability of data or vulnerability of data to the risk of loss or theft. Errors may occur gradually and once in the code may be very hard to detect and can potentially affect results over a long period of time. If an unforeseeable software or hardware malfunction or problem is caused by a defect, virus or other outside force, our clients and our business may be materially adversely affected.

In particular, we may rely on cloud (including private and public cloud-based) technology for certain operations, including data storage. Cloud-based technology, like any electronic data storage or processing technology, is not fail-safe. It may be subject to certain defects, failures or interruptions of service beyond our direct control. It is also possible that such technology could be compromised by a third party, including through the use of malicious software or programs, such as viruses, which may expose the Company and a client to theft (of data or other assets) and/or significant business interruption. Our third-party technology providers have, from time to time, experienced security incidents in connection with systems that we use. In addition, a software provider may cease operations or be relatively thinly capitalized and our and a client's ability to be made whole after any loss may be compromised as a result.

Legislative or regulatory changes or actions by the U.S. Congress or any U.S. federal or state agencies could restrict the use of one or more digital assets, the ability to enter into transactions referencing digital assets, validating or mining activity, the operation of digital asset networks or digital asset trading platforms in a manner that adversely affects our business.

As digital assets have grown in both popularity and market size, the U.S. Congress and a number of U.S. federal and state agencies and self-regulatory organizations (including FinCEN, OFAC, SEC, CFTC, FINRA, NFA, the Consumer Financial Protection Bureau, the Department of Justice, the Department of Homeland Security, the Federal Bureau of Investigation, the IRS, the Office of the Comptroller of the Currency, the FDIC, the Federal Reserve and state financial institution and securities regulators) have been examining the operations of digital asset networks, digital asset users and the digital asset markets, with particular focus on the extent to which digital assets can be misused to launder the proceeds of illegal activities, evade sanctions, or fund criminal or terrorist enterprises, and generally the safety and soundness of digital asset trading platforms and other service providers that hold digital assets for users. Many of these regulatory bodies have issued consumer advisories regarding the risks posed by digital assets to investors. Ongoing and future regulatory

actions with respect to digital assets generally or any digital asset that we hold or invest in may alter, perhaps to a materially adverse extent, the nature of an investment in us or our ability to continue to operate.

At times, the leadership of the SEC, at least under the prior administration, took the view that the digital asset ecosystem requires more explicit regulatory oversight and that the SEC should have more explicit regulatory authority over the digital asset ecosystem. For example, in August 2021, the former Chair of the SEC stated that he believed investors using digital asset trading platforms are not adequately protected, and that activities on the platforms can implicate the securities laws, commodities laws and banking laws, raising a number of issues related to protecting investors and consumers, guarding against illicit activity, and ensuring financial stability. The former Chair repeatedly expressed a need for the SEC to have additional authorities to prevent transactions, products, and platforms from “falling between regulatory cracks,” as well as for more resources to protect investors in “this growing and volatile sector.” The former Chair called for federal legislation centering on digital asset trading, lending, and decentralized finance platforms, seeking “additional plenary authority” to write rules for digital asset trading and lending. The former Chair then stated that he believed the law as applied to digital assets and digital asset market participants is clear and that there is no need for additional explicit authorities. As part of this shift, the SEC and the former Chair of the SEC alleged that certain digital asset market participants are not in compliance with existing regulations applicable to them. For example, in May 2024, the former Chair of the SEC said, “The crypto industry’s record of failures, frauds, and bankruptcies is not because we don’t have rules or because the rules are unclear,” but rather, “it’s because many players in the crypto industry don’t play by the rules.” Moreover, the SEC under the prior administration pursued a number of enforcement actions against market participants across the digital asset ecosystem based on alleged violations of existing laws and regulations. See “—Risks Related to Our Operations—A determination that a digital asset is a “security,” or that an activity in which we engage involves a “securities transaction” for purposes of the federal securities laws could adversely affect the value of that digital asset and potentially digital assets generally, and could therefore adversely impact our business, financial condition and results of operations as well as the market price of our Class A common stock.”

The SEC under the prior administration also took steps to interpret its existing authorities as covering various digital asset activities. In December 2022, the SEC proposed Regulation Best Execution, which would establish an SEC-level best execution regulatory framework for brokers, dealers, government securities brokers, government securities dealers, and municipal securities dealers. The proposed rule release stated that the proposed Regulation Best Execution would apply to all securities, including what the SEC views as digital asset securities. In February 2023, the SEC proposed amendments to the custody rules under Rule 206(4)-2 of the Advisers Act. The proposed rule changes would amend the definition of a “Qualified Custodian” under Rule 206(4)-2(d)(6) and expand the current custody rule in 206(4)-2 to cover digital assets (whether or not securities) and related advisory activities. In April 2023, the SEC reopened for comment a proposed amendment to the definition of an “exchange” under Exchange Act Rule 3b-16. In the reopening release, the SEC provided supplemental information regarding trading systems for digital asset securities that explained that the proposed rule could apply to DeFi protocols to the extent they meet the definition of “exchange.” In February 2024, the SEC adopted a rule that expands the definition of “dealer” and “government securities dealer” under Rules 3a5-4 and 3a44-2 of the Exchange Act. In the final rule release, the SEC confirmed that the new rule applies to activities involving digital asset securities.

Although the former Acting Chairman of the SEC Mark Uyeda has suggested that certain of these rule amendments would be dropped and Commissioner Peirce’s Crypto Task Force is taking a different approach to regulating the digital asset industry, if enacted as proposed, these rules would likely impose additional regulatory requirements with respect to the trading in, custody and storage of digital assets and could lead to additional regulatory oversight of the digital asset ecosystem more broadly.

There have been several bills introduced in Congress that propose to establish additional regulation and oversight of the digital asset markets. On July 18, 2025, President Trump signed the first of these bills, the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), into law, establishing the first comprehensive regulatory scheme for payment stablecoins in the United States. Other related bills continue to be contemplated in the relevant committees, as well as the full House of Representatives and Senate. It is difficult to predict whether, or when, any of these developments will lead to Congress granting additional authorities to the SEC or other regulators, what the nature of such additional authorities might be, how additional legislation and/or regulatory oversight might impact the ability of digital asset markets to function or how any new regulations or changes to existing regulations might impact the value of digital assets generally and those held by us specifically. The consequences of increased federal regulation of digital assets and digital asset activities could have a material adverse effect on our business and the market price of our Class A common stock.

Furthermore, changes in U.S. political leadership and economic policies may create uncertainty that materially affects the price of digital assets. For example, on March 6, 2025, President Trump signed an Executive Order to establish a

Strategic Bitcoin Reserve and a United States Digital Asset Stockpile. Pursuant to this Executive Order, the Strategic Bitcoin Reserve will be capitalized with bitcoin owned by the Department of Treasury that was forfeited as part of criminal or civil asset forfeiture proceedings, and the Secretaries of Treasury and Commerce are authorized to develop budget-neutral strategies for acquiring additional bitcoin, provided that those strategies impose no incremental costs on American taxpayers. Conversely, the Digital Asset Stockpile will consist of all digital assets other than bitcoin owned by the Department of Treasury that were forfeited in criminal or civil asset forfeiture proceedings, but the U.S. government will not acquire additional assets for the U.S. Digital Asset Stockpile beyond those obtained through such proceedings. The anticipation of a U.S. government-funded strategic cryptocurrency reserve had motivated large-scale purchases of various digital assets in the expectation of the U.S. government acquiring those digital assets to fund such reserve, and the market price of some digital assets decreased significantly as a result of the ultimate content of the Executive Order. Any similar action or omission by the U.S. federal administration or other government authorities may negatively and significantly impact the price of digital assets.

Law enforcement agencies have often relied on the transparency of blockchains to facilitate investigations. However, certain privacy-enhancing features have been, or are expected to be, introduced to a number of digital asset networks, and these features may provide law enforcement agencies with less visibility into transaction-level data. Europol, the European Union’s law enforcement agency, released a report in October 2017 noting the increased use of privacy-enhancing digital assets like Zcash and Monero in criminal activity on the internet. The U.S. Department of the Treasury made a similar finding in its February 2022 National Money Laundering Risk Assessment. In August 2022, OFAC prohibited transactions by U.S. persons or persons in the United States involving Tornado Cash, a digital asset protocol designed to obfuscate blockchain transactions, by adding Tornado Cash and certain Ethereum wallet addresses associated with the protocol to its Specially Designated Nationals and Blocked Persons List. A large portion of validators globally, as well as notable industry participants such as Circle, the issuer of the USDC stablecoin, have reportedly complied with the sanctions and blacklisted the sanctioned addresses from interacting with their networks or digital assets. In October 2023, FinCEN issued a notice of proposed rulemaking that identified convertible virtual currency (“CVC”) mixing as a class of transactions of primary money laundering concern and proposed requiring covered financial institutions to implement certain recordkeeping and reporting requirements on transactions that covered financial institutions know, suspect, or have reason to suspect involve CVC mixing within or involving jurisdictions outside the United States. In April 2024, the DOJ arrested and charged the developers of the Samurai Wallet mixing service with conspiracy to commit money laundering and conspiracy to operate an unlicensed money transmitting business. In May 2024, a co-founder of Tornado Cash was sentenced to more than five years imprisonment in the Netherlands for developing Tornado Cash on the basis that he had helped launder more than \$2 billion worth of digital assets through Tornado Cash. Additional regulatory action with respect to privacy-enhancing digital assets is possible in the future.

Legal or regulatory changes or interpretations of our existing and planned activities (including those of our subsidiaries or our portfolio companies), including the mere buying and selling of digital assets, could require the registration or licensing of us and/or our subsidiaries in additional, costly and constraining capacities, such as a money services business under the regulations promulgated by the FinCEN under the authority of the Bank Secrecy Act, the BitLicense scheme adopted by the NYDFS, the DFAL in California, or pursuant to applicable current or future laws and regulations or the laws of other jurisdictions, and would therefore require us and/or our subsidiaries to comply with applicable regulatory, licensing, examination and supervision requirements. See “Item 1. Legal Proceedings” for more information.

The effect of any future regulatory change on our business or the digital assets we hold is impossible to predict, but such change could be substantial and adverse to the utility of our products and services, our investment and trading strategies, the value of our assets and the value of any investment in us.

Legislative or regulatory changes or actions in foreign jurisdictions may affect our business or restrict the use of one or more digital assets, transactions referencing digital assets, mining activity or the operation of their networks or the digital asset trading platform market in a manner that adversely affects our business.

Various foreign jurisdictions have adopted, and may continue to adopt laws, regulations or directives that affect a digital asset network, the digital asset markets, and their users, particularly digital asset trading platforms and service providers that fall within such jurisdictions’ regulatory scope.

A number of foreign jurisdictions have recently taken regulatory action aimed at digital asset activities, including as a result of energy consumption concerns. China has made transacting in cryptocurrencies illegal for Chinese citizens in mainland China, and additional restrictions may follow. China’s central bank has further restricted digital asset-related activities, stating that activity by overseas digital asset trading platforms, and services offering trading, order matching, and token issuance and derivatives, constitute illegal activity. Both China and South Korea have banned initial coin offerings entirely (although South Korean regulators have indicated they may replace the outright ban with regulations in the future)

and regulators in other jurisdictions, including Canada, Singapore and Hong Kong, have opined that initial coin offerings may constitute securities offerings subject to local securities regulations. Kosovo and Angola have prohibited domestic digital asset mining as a result of associated energy use, and other jurisdictions have banned further expansion of such operations for similar reasons. A number of countries continue to have absolute or implicit bans on digital assets.

Foreign laws, regulations or directives, as well as the assertion of jurisdiction by foreign regulators and other government entities over digital assets and digital asset markets, may conflict with those of the United States. Such conflicts may negatively impact the acceptance of one or more digital assets by users, merchants and service providers outside the United States and may therefore impede the growth or sustainability of the digital asset economy in the European Union, China, Japan, Russia, the Bahamas and the United States and globally, or otherwise negatively affect the value of digital assets that we invest in. While the European Union’s digital asset regulations are effectively uniform, the laws and regulations in other regions are disparate, conflicting and subject to regular change and reinterpretation. The effect of any future regulatory change on our business or the digital assets that we invest in is impossible to predict, but such change could be substantial and adverse to our investment and trading strategies, the value of our assets and the value of any investment in us.

If regulators or public utilities take actions that restrict or otherwise impact mining activities, there may be a significant decline in such activities, which could adversely affect digital asset networks, our business and the market price of our Class A common stock.

Concerns have been raised about the amount of electricity required to secure and maintain certain digital asset networks. For example, as of September 30, 2025 over 1000 exa-hashes per second, using a 7-day moving average, are performed in connection with mining on the Bitcoin network. Although measuring the electricity consumed by this process is difficult because these operations are performed by various machines with varying levels of efficiency, the process consumes a significant amount of energy. The operations of other digital asset networks may also consume significant amounts of energy. Further, in addition to the direct energy costs of performing calculations on any given digital asset network, there are indirect costs that impact a network’s total energy consumption, including the costs of cooling the machines that perform these calculations.

Driven by concerns around energy consumption and the impact of digital asset mining on electric utilities, various states and cities have implemented, or are considering implementing, moratoriums on mining activity in their jurisdictions. Such actions could increasingly cause cryptocurrency networks or protocols to adopt “proof of stake” methods of validation rather than “proof of work,” which would have an adverse impact on our mining business. In addition, a significant reduction in mining activity as a result of such actions could adversely affect the security of a digital asset network by making it easier for a malicious actor or botnet to manipulate the relevant blockchain. See “—If a malicious actor or botnet obtains control of more than 50% of the processing power on a digital asset network, or otherwise obtains control over a digital asset network through its influence over core developers or otherwise, such actor or botnet could manipulate the blockchain of such digital asset to adversely affect the market price of our Class A common stock or our ability to operate.” If regulators or public utilities take action that restricts or otherwise impacts mining activities, such actions could result in decreased security of a digital asset network and consequently adversely impact our revenues, our business and the market price of our Class A common stock.

Many of the digital assets and transactions referencing digital assets in which we facilitate trading are subject to regulatory authority by the CFTC. Any fraudulent or manipulative trading activity in such an instrument could subject us to increased regulatory scrutiny, regulatory enforcement, and litigation.

The CFTC has stated and judicial decisions involving CFTC enforcement actions have confirmed that at least some digital assets, including bitcoin, fall within the definition of a “commodity” under the U.S. Commodity Exchange Act of 1936 (“CEA”). As a result, the CFTC takes the view that it has wide jurisdiction over derivatives referencing many digital commodities. In addition, the CFTC has general enforcement authority to police against manipulation and fraud in at least some spot digital asset markets. From time to time, manipulation, fraud, and other forms of improper trading by market participants have resulted in, and may in the future result in, CFTC investigations, inquiries, enforcement actions, and similar actions by other regulators, government agencies, and civil litigation. Such investigations, inquiries, enforcement actions, and litigation may cause us to incur substantial costs and could result in negative publicity.

Certain transactions in digital assets may constitute “leveraged retail commodity transactions” subject to regulation by the CFTC as futures contracts. If digital asset transactions we facilitate are deemed to be such retail commodity transactions, we would be subject to additional regulatory requirements, licenses and approvals, and potentially face regulatory enforcement, civil liability, and significant increased compliance and operational costs.

Any transaction in a commodity, including a digital asset, entered into with or offered to retail investors on a leveraged, margined, or financed basis (a “leveraged retail commodity transaction”) is subject to CFTC regulation as a futures contract unless such transaction results in actual delivery within 28 days. In March 2020, the CFTC adopted guidance addressing what constitutes “actual delivery” of a digital asset. To the extent that digital asset transactions that we facilitate or facilitated are deemed leveraged retail commodity transactions, including pursuant to current or subsequent rulemaking or guidance by the CFTC, we may be subject to additional regulatory requirements and oversight, and we could be subject to judicial or administrative sanctions if we do not or did not at a relevant time possess appropriate registrations. The CFTC has previously brought enforcement actions against entities, including DAOs and DeFi development labs, engaged in leveraged retail commodity transactions without appropriate registrations.

Particular digital assets or transactions in which we engage are or could be deemed “commodity interests” (e.g., futures, options on non-security commodities, swaps) or security-based swaps subject to regulation by the CFTC or SEC, respectively. For such transactions, we are subject or would be subject to various regulatory regimes, which could require us to obtain additional regulatory requirements, licenses and approvals, which could impose significant increased compliance and operational costs. If we do not hold such licenses or approvals or do not otherwise meet the requirements of these regulatory regimes, we could potentially face regulatory enforcement or liability.

Activities in “commodity interests” (as such term is defined by the CEA and CFTC rules and regulations), including certain futures contracts, options on futures contracts, options on non-security commodities, swaps and retail leveraged commodity transactions (among other instruments), are subject to extensive supervisory oversight by the CFTC. This includes licensing of entities engaged in, and platforms offering, commodity interest transactions. GDL, Galaxy’s registered CFTC-regulated swap dealer, engages in dealing activity in swaps. To the extent that other transactions we engage in involving digital assets are deemed to fall within the definition of a commodity interest, whether as a swap or otherwise and including pursuant to subsequent rulemaking or guidance by the CFTC, we may be subject to additional regulatory requirements and oversight and could be subject to judicial or administrative sanctions if we do not or did not at a relevant time possess appropriate registrations as an exchange (for example, as a designated contract market for trading futures or options on futures, or as a swap execution facility for trading swaps) or as a registered intermediary (for example, as a futures commission merchant or introducing broker). Such actions could result in injunctions, cease and desist orders and revocation of existing licenses, as well as civil monetary penalties, fines, and disgorgement, as well as reputational harm. The CFTC has previously brought enforcement actions against entities engaged in digital asset activities for failure to obtain appropriate exchange or intermediary registrations. In addition, Galaxy’s customers may face additional costs for transactions with Galaxy (such as certain requirements related to margin posting and collection) that may make those customers less willing to trade swaps with Galaxy.

In 2024, GDL’s dealing activity in swaps exceeded the applicable Dodd-Frank de minimis registration threshold. As a result, GDL was required to apply for registration as a swap dealer with the CFTC and NFA, which registration was approved in May 2025. As a registered swap dealer, GDL is subject to additional regulatory requirements, including, but not limited to, capital requirements, margin requirements, risk management requirements, supervision requirements, business conduct standards, and transaction reporting requirements. Galaxy has experienced a significant increase in costs to appropriately comply with swap dealer requirements, with such additional costs factored into broader business planning exercises. In addition, Galaxy’s customers may face additional costs for transactions with Galaxy (such as certain requirements related to margin posting and collection) that may make those customers less willing to trade swaps with Galaxy. To the extent that digital asset transactions that we facilitate or facilitated are deemed leveraged retail commodity transactions, including pursuant to current or subsequent rulemaking or guidance by the CFTC, we may be subject to additional regulatory requirements and oversight related to them.

Additionally, any failure to adequately comply with applicable CFTC rules and requirements may result in investigation and enforcement actions, as well as potential monetary fines, sanctions and/or reputational damage.

If a digital asset is deemed to be a security, certain derivatives referencing that digital asset (including a perpetual futures contract on that digital asset) could constitute a security-based swap subject to SEC regulation rather than a swap subject to CFTC regulation. To the extent that transactions we engage in involving digital assets are deemed to fall within the definition of a security-based swap, including pursuant to rulemaking or guidance by the SEC, we may be subject to additional regulatory requirements and oversight by the SEC and could be subject to judicial or administrative sanctions, particularly if we had not previously treated such transactions as being security-based swaps. For example, we may be

required to register the offer and sale of the security-based swap with the SEC, or register ourselves with the SEC as a security-based swap dealer to the extent we engage in more than a de minimis amount of security-based swap dealing activity, register ourselves with the SEC as a major security-based swap participant to the extent we meet quantitative thresholds requiring registration as such, or we may be required to register with the SEC as a national securities exchange or security-based swap execution facility to the extent we facilitate certain types of security-based swap transactions. We are not currently registered with the SEC in any capacity on the basis of security-based swap activity and could be subject to enforcement actions if we were found to have failed to timely register. This could result in injunctions, cease and desist orders, as well as civil monetary penalties, fines, and disgorgement, as well as reputational harm.

If we register with the CFTC or SEC in any additional capacity as a result of swap or security-based swap activity, respectively, we would be subject to additional supervision and regulatory requirements, including, but not limited to, capital requirements, margin requirements, risk management and diligent supervision requirements, and business conduct standards, as applicable. We may experience a significant increase in costs to comply with these requirements, and we may incur significant fines or restrictions on our activities if we fail to comply with these requirements, to the extent they were deemed applicable to us.

Even where we are not required to be registered with the CFTC or SEC, we are required to accurately report swap and security-based swap transactions to registered data repositories if we are the designated reporting party for such transactions. Failure to comply with applicable CFTC and/or SEC reporting rules could subject the Company to investigation and enforcement and possible monetary fines and sanctions.

The AI industry is subject to developing and evolving regulatory frameworks globally, which are expected to become increasingly complex as AI continues to evolve, and our efforts to comply with such legislation or regulation could be costly and our failure or inability to comply with these regulations or regulatory action against us could adversely affect our results of operations, financial condition or business.

The rapid pace of innovation in the field of AI has led to developing and evolving regulatory frameworks globally, which are expected to become increasingly complex as AI continues to evolve. U.S. and foreign regulators and lawmakers have started proposing and adopting, or are currently considering, regulations and guidance specifically on the use of AI. For example, in October 2023, the former Presidential Administration signed an executive order (the “October 2023 Executive Order”) that established new standards for AI safety and security. However, in January 2025, the current Presidential Administration signed an executive order that rescinded the October 2023 Executive Order and requires the development of an AI action plan that is consistent with the current Presidential Administration’s policy within 180 days thereof. Meanwhile, in Europe, the EU AI Act became effective on August 1, 2024 and will be fully applicable after a two-year transitional period. The EU AI Act aims to ensure AI systems are safe, respect fundamental rights, and foster innovation, while also establishing a risk-based approach to AI regulation, with bans on certain AI practices and specific requirements for high-risk applications. Following the EU AI Act, Colorado passed a Consumer Protections for Artificial Intelligence bill introducing state-level oversight of “high-risk” AI systems, which mirrors language and several provisions appearing in the EU AI Act. In September 2024, California enacted various AI bills relating to transparency, privacy, entertainment, election integrity, and government accountability. It is possible that new laws and regulations will be adopted in the U.S. and in non-U.S. jurisdictions, or that existing laws and regulations may be interpreted, in ways that would affect our operations. We may not be able to adequately anticipate or respond to these evolving laws and regulations, and we may need to expend additional resources to adjust our offerings in certain jurisdictions if applicable legal frameworks are inconsistent across jurisdictions. Further, the cost to comply with such laws or regulations could be significant and would increase our operating expenses, which could adversely affect our business, financial condition and results of operations.

Increased regulations and regulatory scrutiny in the AI industry could also lead to a decrease in demand for AI/HPC infrastructure, which may adversely affect our business, operating results, financial condition, and future prospects. See “—Risks Related to Our Business Lines—Our strategy to expand into the AI/HPC data center business may not be successful and may result in adverse consequences to our business, financial condition and results of operations” for further information relating to the potential impacts of decreased market demand on our AI/HPC data center business.

Cybersecurity incidents and other issues related to our information systems, technology and data may affect us materially and adversely.

Cybersecurity incidents and cyberattacks have been occurring globally at a more frequent and severe level and will likely continue to increase in frequency in the future. The digital asset and AI industries are a particular target for cybersecurity incidents, which may occur through intentional or unintentional acts by individuals or groups having authorized or unauthorized access to our systems or our clients’ or counterparties’ information, which may include

confidential information. These individuals or groups include employees, vendors and customers, as well as hackers. The information and technology systems used by us and our service providers, and other third parties, are vulnerable to damage or interruption from, among other things: hacking, ransomware, malware and other computer viruses; denial of service attacks; network failures; computer and telecommunication failures; phishing attacks; infiltration by unauthorized persons; security breaches; usage errors by their respective professionals; power outages; terrorism; and catastrophic events such as fires, tornadoes, floods, hurricanes and earthquakes.

We and our third party service providers have experienced cybersecurity incidents in the past, and expect to experience cybersecurity incidents in the future. While we take efforts to protect our systems and data, including establishing internal processes and implementing technological measures designed to provide multiple layers of security, and contract with third-party service providers to take similar steps, we have experienced cybersecurity breaches in the past, and there can be no assurance that our safety and security measures (and those of our third-party service providers) will prevent damage to, or interruption or breach of, our information systems, data (including personal data) and operations. We have recently taken steps to expand and enhance our cybersecurity controls and practices and, as cybersecurity-related threats continue to evolve, we may be required to expend significant additional resources to continue to modify or enhance our protective measures or to investigate and remediate any information security vulnerabilities. Nevertheless, it is possible we could suffer an impact or disruption that could materially and adversely affect us. Our operational infrastructure may be breached due to the actions of outside parties, error or malfeasance of our employee, or otherwise, and, as a result, an unauthorized party may obtain access to our accounts, private keys, data, or digital assets. Additionally, outside parties may attempt to fraudulently induce our employees to disclose sensitive information in order to gain access to our infrastructure. As the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently, or may be designed to remain dormant until a predetermined event, and often are not recognized until launched against a target, we may be unable to anticipate these techniques or implement adequate preventative measures. Additionally, in the occurrence of a pandemic or similar event, there is an increased risk that we may experience cybersecurity-related incidents as a result of our employees, service providers and other third parties working remotely on less secure systems and environments. Controls employed by our information technology department and our customers and third-party service providers, including cloud vendors, could prove inadequate. If an actual or perceived breach of any of our digital asset account occurs, the market perception of our effectiveness could be harmed.

Moreover, there could be public announcements regarding any cybersecurity-related incidents and any steps we take to respond to or remediate such incidents, and if securities analysts or investors perceive these announcements to be negative, it could, among other things, have a substantial adverse effect on the price of our common stock. Further, any publicized security problems affecting our businesses or those of third parties with whom we are affiliated or otherwise conduct business may discourage consumers from doing business with us, which could have a material and adverse effect on our business, financial condition and results of operations.

It is difficult or impossible to defend against every risk being posed by changing technologies, as well as criminals' intent to commit cybercrime, and these efforts may not be successful in anticipating, preventing, detecting or stopping attacks, or reacting in a timely manner. The increasing sophistication and resources of cybercriminals and other non-state threat actors and increased actions by nation-state actors make it difficult to keep up with new threats and could result in a breach of security. Such threats may see their frequency increased, and effectiveness enhanced, by the use of artificial intelligence. Further, cybersecurity risks may be heightened as a result of ongoing global conflicts such as the Russia-Ukraine conflict or the ongoing Israel-Hamas conflict. Additionally, we cannot guarantee that our insurance coverage would be sufficient to cover any such losses.

To the extent the operation of our systems relies on our third-party service providers, through either a connection to, or an integration with, third parties' systems, the risk of cybersecurity attacks and loss, corruption, or unauthorized access to or publication of our information or the confidential information and personal data of customers and employees may increase. Third-party risks may include insufficient security measures, data location uncertainty, and the possibility of data storage in inappropriate jurisdictions where laws, security measures or other controls may be inadequate or in which there are uncertainties regarding governmental intervention and use of such data, and our ability to monitor our third-party service providers' data security practices are limited. Although we generally have agreements relating to cybersecurity and data privacy in place with our third-party service providers, they are limited in nature and we cannot guarantee that such agreements will prevent the accidental or unauthorized access to or disclosure, loss, destruction, disablement or encryption of, use or misuse of or modification of data (including personal data) or enable us to obtain adequate or any reimbursement from our third-party service providers in the event we should suffer any such incidents. Due to applicable laws and regulations or contractual obligations, we may be held responsible for any information security failure or cybersecurity attack attributed to our vendors as they relate to the information we share with them. A vulnerability in or related to a third-party service provider's software or systems, a failure of our third-party service providers' safeguards, policies or

procedures, or a breach of a third-party service provider's software or systems could result in the compromise of the confidentiality, integrity or availability of our systems or the data housed in our third-party solutions.

The security of the information and technology systems used by us and our service providers may continue to be subjected to cybersecurity threats that could result in material failures or disruptions in our business. If these systems are compromised, become inoperable for extended periods of time or cease to function properly, we or a service provider may have to make a significant investment to fix or replace them. The failure of these systems or of disaster recovery plans for any reason could cause significant interruptions in operations and result in a failure to maintain the security, confidentiality or privacy of sensitive data, including personal information relating to stockholders (and the beneficial owners of stockholders). Such a failure could harm our reputation, subject us to legal claims and otherwise materially and adversely affect our investment and trading strategies and our value.

We obtain and process sensitive customer data. Any real or perceived improper use of, disclosure of, or access to such data could harm our reputation, as well as have an adverse effect on our business.

We obtain and process sensitive data, including personal data related to our customers and their transactions, such as their names, addresses, trading data, tax identification, and bank account information. We face risks, including to our reputation, in the handling and protection of this data, and these risks will increase as our business continues to expand. Federal, state, and international laws and regulations governing privacy, data protection, and e-commerce transactions require us to safeguard our customers', employees', and service providers' personal data.

We have administrative, technical, and physical security measures and controls in place and maintain a robust information security program. However, our security measures may be inadequate or breached as a result of third-party action, employee or service provider error, malfeasance, malware, phishing, hacking attacks, system error, trickery, advances in computer capabilities, new discoveries in the field of cryptography, inadequate facility security or otherwise, and, as a result, someone may be able to obtain unauthorized access to sensitive information, including personal data, on our systems. Additionally, privacy and data protection laws are evolving, and it is possible that these laws may be interpreted and applied in a manner that is inconsistent with our data handling safeguards and practices that could result in fines, lawsuits, and other penalties, and significant changes to our or our third-party partners' business practices and products and service offerings.

To the extent that the measures we or our third-party business partners have taken prove to be insufficient or inadequate, we may become subject to litigation, breach notification obligations, or regulatory or administrative sanctions, which could result in significant fines, penalties, damages, harm to our reputation, or loss of customers. If our own confidential business information or sensitive customer information were improperly disclosed, our business could be adversely affected. Additionally, a party who circumvents our security measures could, among other effects, appropriate customer information or other proprietary data, cause interruptions in our operations, or expose customers to hacks, viruses, and other disruptions.

Depending on the nature of the information compromised, in the event of a data breach or other unauthorized access to our customer data, we may also have obligations to notify customers and regulators about the incident, and we may need to provide some form of remedy, such as a subscription to credit monitoring services, pay significant fines to one or more regulators, or pay compensation in connection with a class-action settlement (including under the private right of action under the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020, the "CCPA"), which has resulted in an increase of security breach litigation). Such breach notification laws continue to evolve and may be inconsistent from one jurisdiction to another. Complying with these obligations could cause us to incur substantial costs and could increase negative publicity surrounding any incident that compromises customer data. Additionally, the financial exposure from the events referenced above could either not be insured against or not be fully covered through any insurance that we may maintain, and there can be no assurance that the limitations of liability in any of our contracts would be enforceable or adequate or would otherwise protect us from liabilities or damages as a result of the events referenced above. Any of the foregoing could have an adverse effect on our business, reputation, operating results, and financial condition.

Furthermore, we may be required to disclose personal data pursuant to demands from individuals, regulators, government agencies, and law enforcement agencies in various jurisdictions with conflicting privacy and security laws, which could result in a breach of privacy and data protection policies, notices, laws, rules, court orders, and regulations. Additionally, changes in the laws and regulations that govern our collection, use, and disclosure of customer data could impose additional requirements with respect to the retention and security of customer data, could limit our marketing activities, and have an adverse effect on our business, operating results, and financial condition.

We are subject to stringent laws, rules, regulations, policies, industry standards and contractual obligations regarding data privacy and security and may be subject to additional related laws and regulations in jurisdictions into which we expand. Many of these laws and regulations are subject to change and reinterpretation and could result in claims, changes to our business practices, monetary penalties, increased cost of operations or other harm to our business.

We and our third-party service providers are subject to a variety of federal, state, local, and non-U.S. laws, directives, rules, policies, industry standards and regulations, as well as contractual obligations, relating to privacy and the collection, protection, use, retention, security, disclosure, transfer and other processing of personal data and other data, including Section 5(c) of the Federal Trade Commission Act, the Gramm Leach Bliley Act of 1999 and the CCPA. The regulatory framework for data privacy and security worldwide is continuously evolving and developing and, as a result, interpretation and implementation standards and enforcement practices are likely to remain uncertain for the foreseeable future. New laws, amendments to or reinterpretations of existing laws, regulations, standards and other obligations may require us to incur additional costs and restrict our business operations, and may require us to change how we use, collect, store, transfer or otherwise process certain types of personal data and to implement new processes to comply with those laws and our customers' exercise of their rights thereunder.

In the United States, federal law restricts certain collection, processing, storage, use and disclosure of personal data, requires notice to individuals of privacy practices and provides individuals with certain rights to prevent the use and disclosure of certain non-public or otherwise legally protected information. These rules also impose requirements for the safeguarding and proper destruction of personal data through the issuance of data security standards or guidelines. There is also a risk of enforcement actions in response to rules and regulations promulgated under the authority of federal agencies and state attorneys general and legislatures and consumer protection agencies. In addition, privacy advocates and industry groups have proposed and may propose new and different self-regulatory standards that either legally or contractually apply to us. If we fail to follow these security standards, even if no customer information is compromised, we may incur significant fines or experience a significant increase in costs.

Numerous states have enacted or are in the process of enacting state-level data privacy laws and regulations governing the collection, use, and other processing of state residents' personal data. For example, the CCPA, which took effect on January 1, 2020, established a new privacy framework for covered businesses such as ours, and has required us, and may require us in the future, to modify our data processing practices and policies and incur compliance related costs and expenses. The CCPA provides new and enhanced data privacy rights to California residents, such as affording California residents the right to access and delete their information and to opt out of certain sharing and sales of personal information. The law also prohibits covered businesses from discriminating against California residents (for example, charging more for services) for exercising any of their CCPA rights. The CCPA imposes severe civil penalties and statutory damages as well as a private right of action for certain data breaches that result in the loss of personal information. This private right of action has increased the likelihood of, and risks associated with, data breach litigation. Numerous other states also have enacted, or are in the process of enacting or considering, comprehensive state-level data privacy and security laws and regulations that share similarities with the CCPA.

The effects of the CCPA and other similar state or federal laws and other future changes in laws or regulations relating to privacy, data protection and information security, particularly any new or modified laws or regulations that require enhanced protection of certain types of data or new obligations with regard to data retention, transfer or disclosure, are significant and may require us to modify our data processing practices and policies and could greatly increase the cost of providing our offerings, require significant changes to our operations or even prevent us from providing certain offerings in jurisdictions in which we currently operate and in which we may operate in the future or incur potential liability in an effort to comply with such legislation.

The CCPA has led, and may lead, other states to pass comparable legislation, with potentially greater penalties and more rigorous compliance requirements relevant to our business. For example, many state legislatures have adopted legislation that regulates how businesses operate online, including measures relating to privacy, data security, data breaches and the protection of sensitive and personal information. Laws in all 50 states require businesses to provide notice to customers whose personally identifiable information has been disclosed as a result of a data breach. The laws are not consistent, as certain state laws may be more stringent or broader in scope, or offer greater individual rights, with respect to sensitive and personal information than federal, international or other state laws, and such laws may differ from each other, which may complicate compliance efforts. Compliance in the event of a widespread data breach may be costly.

The NYDFS also issued Cybersecurity Requirements for Financial Services Companies, which took effect in 2017, and which require banks, insurance companies and other financial services institutions regulated by the NYDFS, to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of New York State's financial services industry. The cybersecurity regulation adds specific requirements for these institutions'

cybersecurity compliance programs and imposes an obligation to conduct ongoing, comprehensive risk assessments. Further, on an annual basis, each institution is required to submit a certification of compliance with these requirements. We may in the future become subject to such NYDFS regulations and requirements, which could subject us to additional investigations and examinations of our compliance programs.

We make public statements about our use, collection, disclosure and other processing of personal data through our privacy policies, information provided on our website and press statements. Although we endeavor to comply with our public statements and documentation, we may at times fail to do so or be alleged to have failed to do so. The publication of our privacy policies and other statements that provide promises and assurances about data privacy and security can subject us to potential government or legal action if they are found to be deceptive, unfair or misrepresentative of our actual practices. Any failure or perceived failure by us or our third-party service providers to comply with our posted privacy policies or with any applicable federal, state or similar foreign laws, rules, regulations, industry standards, policies, certifications or orders relating to data privacy and security, or any compromise of security that results in theft, unauthorized access, acquisition, use, disclosure, or misappropriation of personal data or other customer data, could result in significant awards, fines, civil and/or criminal penalties or judgments, proceedings or litigation by governmental agencies or customers, including class action privacy litigation in certain jurisdictions and negative publicity and reputational harm, one or all of which could have an adverse effect on our reputation, business, financial condition and results of operations. All of these evolving compliance and operational requirements impose significant costs, such as costs related to organizational changes, implementing additional protection technologies, training employees and engaging consultants, which are likely to increase over time. In addition, such requirements may require us to modify or restrict our data processing practices and policies, distract management or divert resources from other initiatives and projects, all of which could have a material adverse effect on our business, financial condition, results of operations and prospects.

We may face particular privacy, data security, and data protection risks as our business expands into the U.K. and the EU in connection with the GDPR and other data protection regulations.

International presence in the U.K. and the EU, as well as the fact that some of our customers are residents of the U.K. and the EU, subjects us or may subject us to the EU General Data Protection Regulation (“GDPR”), which became effective in May 2018, supplemented by national laws and further implemented through binding guidance from the European Data Protection Board, which regulates the collection, control, sharing, disclosure, use and other processing of personal data and imposes stringent data protection requirements with significant penalties, and the risk of civil litigation, for non-compliance. As described further below, following Brexit, we also are subject to the United Kingdom General Data Protection Regulation (“U.K. GDPR”) (i.e., a version of the GDPR as implemented into U.K. law). Among other requirements, the GDPR regulates transfers of personal data subject to the GDPR to third countries that have not been found to provide adequate protection to such personal data, including the United States.

One of the primary safeguards that allowed U.S. companies to import personal data from Europe had been certification to the EU-U.S. Privacy Shield and Swiss U.S. Privacy Shield frameworks administered by the U.S. Department of Commerce. However, the Court of Justice of the EU (“CJEU”), invalidated the EU U.S. Privacy Shield, in a case known as “Schrems II.” Following this decision, the United Kingdom government has similarly invalidated use of the EU U.S. Privacy Shield as a mechanism for lawful personal data transfers from the United Kingdom to the United States under the U.K. GDPR and the Swiss Federal Data Protection and Information Commissioner announced that the Swiss-U.S. Privacy Shield does not provide adequate safeguards for the purposes of personal data transfers from Switzerland to the United States. The CJEU’s decision in Schrems II also raised questions about whether one of the primary alternatives to the EU-U.S. Privacy Shield, namely, the European Commission’s standard contractual clauses, can lawfully be used for personal data transfers from Europe to the United States or other third countries that are not the subject of an adequacy decision of the European Commission. On July 10, 2023, the European Commission adopted an adequacy decision concluding that the U.S. ensures an adequate level of protection for personal data transferred from Europe to the United States under the EU-U.S. Data Privacy Framework (followed on October 12, 2023, with the adoption of an adequacy decision in the United Kingdom for the U.K.-U.S. Data Bridge). The adequacy decision does not foreclose, and has faced and is likely to continue to face, legal challenges, and the ongoing legal uncertainty may increase our costs and our ability to efficiently process personal data imported from Europe and the U.K. If we are unable to implement a valid mechanism for personal data transfers from Europe and the U.K., we will face increased exposure to regulatory actions, substantial fines and injunctions against processing personal data from Europe and the U.K. Inability to export personal data may also: restrict our activities outside Europe and the U.K.; limit our ability to collaborate with partners as well as other service providers, contractors and other companies outside of Europe and the U.K.; and/or require us to increase our processing capabilities within Europe and the U.K. at significant expense or otherwise cause us to change the geographical location or segregation of our relevant systems and operations—any or all of which could adversely affect our operations or financial results. Additionally, other countries outside of Europe and the U.K. have enacted or are considering enacting similar cross-border

data transfer restrictions and laws requiring local data residency, which could increase the cost and complexity of delivering our services and operating our business. The type of challenges we face in Europe and the U.K. will likely also arise in other jurisdictions that adopt regulatory frameworks of equivalent complexity. While we have taken steps to mitigate the impact on us with respect to transfers of data, such as implementing standard contractual clauses, the efficacy and longevity of these transfer mechanisms remains uncertain.

The enactment of the GDPR also introduced numerous privacy-related changes for companies operating in the EU, including greater control for data subjects (including, for example, the “right to be forgotten”), increased data portability for EU consumers, data breach notification requirements, and increased fines. In particular, the GDPR includes obligations and restrictions concerning the consent and rights of individuals to whom the personal data relates, the transfer of personal data out of the European Economic Area (the “EEA”) or the U.K., security breach notifications and the security and confidentiality of personal data. Under the GDPR, fines of up to €20 million or up to 4% of the annual global revenue of the noncompliant company, whichever is greater, could be imposed for violations of certain of the GDPR’s requirements. Such penalties are in addition to any civil litigation claims by customers and data subjects. The GDPR requirements will likely apply not only to third-party transactions, but also to transfers of information between us and our subsidiaries, including employee information.

Further, the U.K.’s vote in favor of exiting the EU, often referred to as Brexit, and ongoing developments in the U.K. have created uncertainty with regard to data protection regulation in the U.K. Following the expiry of transitional arrangements agreed to between the U.K. and EU, data processing in the U.K. is governed by the U.K. GDPR, exposing us to two parallel regimes, each of which authorizes similar fines and other potentially divergent enforcement actions for certain violations. With respect to transfers of personal data from the EEA to the U.K. on June 28, 2021, the European Commission issued an adequacy decision in respect of the U.K.’s data protection framework, enabling data transfers from the EEA to the U.K. to continue without requiring organizations to put in place contractual or other measures in order to lawfully transfer personal data between the territories. While it is intended to last for at least four years, the European Commission may unilaterally revoke the adequacy decision, at any point, and if this occurs, it could lead to additional costs and increase our overall risk exposure.

Other countries have also passed or are considering passing laws requiring local data residency or restricting the international transfer of data. These changes may lead to additional costs and increase our overall risk exposure. Any inability to adequately address data privacy or security-related concerns, even if unfounded, or to comply with applicable laws, regulations, standards and other obligations relating to data privacy and security, could result in litigation, breach notification obligations, regulatory or administrative sanctions, additional cost and liability to us, harm to our reputation and brand, damage to our relationships with customers and have an adverse effect on our business, financial condition and results of operations.

Our use of technology, proprietary and non-proprietary software, data and intellectual property may be subject to substantial risk.

We rely heavily on the use of technology, proprietary and non-proprietary software, data and intellectual property, including that of third parties in both the digital asset sector and otherwise. The reliance on this technology and data is subject to a number of important risks. Much of the existing technology for the financial services businesses was not built to service digital assets, which require a unique set of considerations. We are working with numerous service providers to help develop technology to service the industry. If these platforms and technology solutions do not work as planned, or do not meet the level of quality we require, it may make transacting business less efficient, more expensive and potentially prone to errors.

The operation of any element of the digital assets network or any other electronic platform may be severely and adversely affected by the malfunction of its technology and the technology of third parties. For example, an unforeseen software or hardware malfunction could occur as a result of a virus or other outside force, or as result of a design flaw in the design and operation of the network or platform. Furthermore, if our software, hardware, data or other intellectual property is found to infringe on the rights of, or our rights therein are found to be infringed upon by, any third party, the underlying value of our assets could be materially and adversely affected.

Third parties with which we do business or that facilitate our business activities, including digital asset trading platforms, financial intermediaries or vendors that provide services or security solutions for our operations, could also expose us to technology risk, including from breakdowns or failures of their own systems or capacity constraints or other services that impair our ability to process transactions and communicate with customers and counterparties. In addition, we are exposed to the risk that a technology disruption or other information security event at a vendor to our third-party

service providers could impede their ability to provide products or services to us. We may not be able to effectively monitor or mitigate operational risks relating to the use of vendors by third-party service providers.

Failure to maintain adequate recordkeeping of electronic communications could expose us to regulatory risks, operational liabilities and reduce our ability to address legal actions.

Failure to maintain comprehensive records of written communications, especially those conducted through off-channel means (such as personal phones, private email accounts, or other devices), poses significant risks for us. Inadequate recordkeeping violates regulatory requirements set forth by the SEC. The inability to produce complete and accurate records during examinations can result in enforcement actions, fines, or even revocation of registration. For example, in prior years, the members of the staff of the SEC's Division of Enforcement raised whether off-channel communications were appropriately captured. In February 2024, we received termination letters concluding these investigations without charges, but there is no assurance that we will not be subject to SEC inquiries, investigations or enforcement actions in the future. See "Item 1. Legal Proceedings."

Also, without proper documentation, we may face legal challenges. In the event of disputes, investigations, or litigation, the absence of records can weaken our legal position and hinder effective defense. Failing to capture texts, emails, instant messages, and other off-channel communications also creates operational vulnerabilities. These gaps may lead to misunderstandings, misrepresentations, or unauthorized actions that may cause harm to us, our reputation or our clients. Finally, personal devices used for off-channel communications may lack the same security protocols as firm-managed systems. This increases the risk of data breaches, leaks, or unauthorized access.

The need to adopt technology in response to changing security threats poses a challenge to the safekeeping of our digital asset holdings and our operations.

Holders of digital assets must adapt to technological change to secure and safeguard accounts. As technological change occurs, the security threats to our digital asset holdings and our custody technology will likely adapt, and previously unknown threats may emerge. Furthermore, we may become a greater target of security threats as our size and reputation increases. If we are unable to identify and mitigate or stop new security threats, our assets may be subject to theft, loss, destruction or other attack, which could result in a loss of our assets or materially and adversely affect our investment and trading strategies, the value of our assets and the value of any investment in us. Similarly, our custody technology business may become a greater target of security threats as the size of custodied assets increases. If we are unable to identify and mitigate or stop new security threats to our custody technology, custodied assets may be subject to theft, loss, destruction or other attack, which could materially and adversely affect the value of any investment in us.

Any failure to obtain, maintain, protect, defend or enforce our intellectual property and other proprietary rights could adversely affect our business, financial condition and results of operations.

Our success and ability to compete depend in part upon our ability to obtain, maintain, protect, defend and enforce our intellectual property and other proprietary rights and technology. Unauthorized use of our intellectual property or a violation of our intellectual property and other proprietary rights by third parties may damage our brand and our reputation. We rely on a combination of trademark, patent, copyright, and trade secret laws in the United States and internationally, our terms and conditions, other contractual provisions and technological measures to protect our intellectual property rights from infringement, misappropriation or other violation to maintain our brand and competitive position. Various factors outside our control pose a threat to our intellectual property rights, as well as to our products, services and technologies.

The steps we take to protect our intellectual property rights may not be sufficient to effectively prevent third parties from infringing, misappropriating, diluting or otherwise violating our intellectual property rights or to prevent unauthorized disclosure or unauthorized use of our trade secrets or other confidential information. We make business decisions about when to seek patent protection for a particular technology and when to rely upon trade secret protection, and the approach we select may ultimately prove to be inadequate. There can be no assurance our intellectual property rights will be sufficient to protect against unauthorized parties offering products or services that are substantially similar to ours and compete with our business or attempting to copy aspects of our technology and use information that we consider proprietary.

In addition to registered intellectual property rights, we rely on non-registered information and technology, such as trade secrets, confidential information and know-how. We attempt to protect our intellectual property, technology, and confidential information by requiring our employees, contractors, consultants, corporate collaborators, advisors and other third parties who develop intellectual property on our behalf to enter into confidentiality and invention assignment agreements, and third parties we share information with to enter into nondisclosure and confidentiality agreements. We

cannot guarantee that we have entered into such agreements with each party who has developed intellectual property on our behalf and each party that has or may have had access to our confidential information, know-how and trade secrets. These agreements may be insufficient or breached, or may not effectively prevent unauthorized access to or unauthorized use, disclosure, misappropriation or reverse engineering of our confidential information, intellectual property, or technology. Moreover, these agreements may not provide an adequate remedy for breaches or in the event of unauthorized use or disclosure of our confidential information or technology, or infringement of our intellectual property. Enforcing a claim that a party illegally disclosed or misappropriated a trade secret or know-how is difficult, expensive, and time consuming, and the outcome is unpredictable. In addition, trade secrets and know-how can be difficult to protect and some courts inside and outside the United States are less willing or unwilling to protect trade secrets and know-how. If any of our trade secrets were to be lawfully obtained or independently developed by a competitor or other third party, we would have no right to prevent them from using that technology or information to compete with us, and our competitive position would be materially and adversely harmed.

The loss of trade secret protection could make it easier for third parties to compete with our products and services by copying functionality. Additionally, individuals not subject to invention assignment agreements may make adverse ownership claims to our current and future intellectual property, and, to the extent that our employees, independent contractors or other third parties with whom we do business use intellectual property owned by others in their work for us, disputes may arise as to the rights in related or resulting know-how and inventions.

We will not be able to protect our intellectual property rights if we do not detect unauthorized use of our intellectual property rights. We also may fail to maintain or be unable to obtain adequate protections for certain of our intellectual property rights in the United States and certain non-U.S. countries, and our intellectual property rights may not receive the same degree of protection in non-U.S. countries as they would in the United States because of the differences in non-U.S. patent, trademark, copyright, and other laws concerning intellectual property and proprietary rights. Any of our intellectual property rights may be successfully challenged, opposed, diluted, misappropriated or circumvented by others or invalidated, narrowed in scope or held unenforceable through administrative process or litigation in the United States or in non-U.S. jurisdictions. Furthermore, legal standards relating to the validity, enforceability and scope of protection of intellectual property rights are uncertain and any changes in, or unexpected interpretations of, intellectual property laws may compromise our ability to enforce our trade secrets and other intellectual property rights.

In order to protect our intellectual property and other proprietary rights, we may be required to expend significant resources to apply for, maintain, monitor and protect these rights. Litigation brought to protect and enforce our intellectual property rights could be costly, time-consuming and distracting to management and could result in the impairment or loss of portions of our intellectual property. Furthermore, because of the substantial amount of discovery required in connection with intellectual property litigation, there is a risk that some of our confidential information could be compromised by disclosure during this type of litigation. Our efforts to enforce our intellectual property rights may be met with defenses, counterclaims and countersuits attacking the validity and enforceability of our intellectual property rights. Accordingly, we may not be able to prevent third parties from infringing upon or misappropriating our intellectual property. An adverse outcome in such litigation or proceedings may therefore expose us to a loss of our competitive position, expose us to significant liabilities or require us to seek licenses that may not be available on commercially acceptable terms, if at all. Our failure to secure, protect and enforce our intellectual property rights could seriously damage our brand and have an adverse effect on our business, financial condition and results of operations.

Third parties may initiate legal proceedings alleging that we are infringing, misappropriating or otherwise violating their intellectual property rights, the outcome of which would be uncertain and could have a material adverse effect on our business, financial condition and results of operations, or adversely affect the operations of portfolio companies and digital asset networks.

Our commercial success depends, in part, on our ability to develop and commercialize our services and use our internally developed technology without infringing, misappropriating or otherwise violating the intellectual property or proprietary rights of third parties. In recent years, there has been considerable patent, copyright, trademark, domain name, trade secret and other intellectual property development activity in the cryptoeconomy, as well as litigation, based on allegations of infringement or other violations of intellectual property, including by large financial institutions. We may become subject to intellectual property disputes, whether or not such allegations have merit. Intellectual property disputes can be costly to defend and may cause our business, operating results and financial condition to suffer. As the cryptoeconomy expands and more patents are issued, the risk increases that there may be patents or other intellectual property rights owned by third parties that relate to our technology, and of which we are not aware or that we must challenge to continue our operations as currently contemplated. Whether merited or not, we may face allegations that we, our partners or parties indemnified by us have infringed, misappropriated, or otherwise violated the patents, trademarks,

copyrights or other intellectual property rights of third parties. Such claims may be made by competitors seeking to obtain a competitive advantage or by other parties. For example, in recent years, individuals and groups have begun purchasing intellectual property assets for the purpose of making claims of infringement and attempting to extract settlements from companies like ours. It may also be necessary for us to initiate litigation in order to determine the scope, enforceability or validity of third-party intellectual property or proprietary rights, or to establish our intellectual property rights. We may not be able to successfully settle or otherwise resolve such adversarial proceedings or litigation. If we are unable to successfully settle future claims on terms acceptable to us, we may be required to engage in or to continue litigation. Regardless of whether third-party claims have merit, litigation can be time consuming, divert management's attention and financial resources, and can be costly to evaluate and defend. Some third parties may be able to sustain the costs of complex litigation more effectively than we can because they have substantially greater resources. Results of any such litigation are difficult to predict and may require us to stop commercializing or using our technology, obtain licenses and pay royalties, modify our services and technology while we develop non-infringing substitutes, or incur substantial damages, settlement costs, or face a temporary or permanent injunction prohibiting us from marketing or providing the affected services.

With respect to any third-party claims regarding intellectual property rights, we may have to seek a license to continue operations found to be in violation of such rights. If we require a third-party license, it may not be available on commercially reasonable terms or at all, and we may have to pay substantial royalties, upfront fees or grant cross-licenses to our intellectual property rights. We may also have to redesign our technology or services so they do not infringe such third-party intellectual property rights, which may not be possible or may require substantial expenditures of money and time, during which our technology may not be available for commercialization or use. Even if we are party to an agreement pursuant to which a third party must indemnify us against such costs, the indemnifying party may be unable or otherwise unwilling to uphold its contractual obligations. If we cannot or do not obtain relevant third-party licenses, or cannot obtain such licenses on commercially reasonable terms, obtain similar technology from another source, or design new technology that is not infringing, our revenue and earnings could be adversely impacted.

We also license software from third-party vendors. Third parties may claim that our use of such licensed software infringes upon their intellectual property rights. Although we seek to secure indemnification protection from our software vendors to protect us against potential third-party infringement claims in connection with our use of such license software, not all of our vendors agree to provide us with sufficient indemnification protection, and in the instances where we do secure indemnification protection from our vendors, it is possible such vendors may not honor such indemnification obligations.

Third parties may assert intellectual property claims relating to portfolio companies or digital asset networks and their source code. Regardless of the merit of any claim, any threatened action that reduces confidence in portfolio companies or digital asset networks could materially and adversely affect our investment and trading strategies, the value of our assets and the value of any investment in us. Additionally, a meritorious intellectual property claim could lead to a loss of value in the impacted portfolio company or prevent us or other end users from accessing a specific blockchain network or holding or transferring their digital assets, which could force the liquidation of certain digital assets in which we have an interest or cause the value of such digital assets to decline significantly. As a result, an intellectual property claim against a portfolio company or large participants on certain blockchain networks could materially and adversely affect our investment and trading strategies, the value of our assets and the value of any investment in us.

Even if resolved in our favor, litigation or other legal proceedings relating to intellectual property may cause us to incur significant expenses, and could distract our technical and management personnel from their normal responsibilities. In addition, there could be public announcements of the results of hearings, motions or other interim proceedings or developments, and if securities analysts or investors perceive these results to be negative, such announcements could have a material adverse effect on the price of our Class A common stock. Moreover, any uncertainties resulting from the initiation and continuation of any legal proceedings could have a material adverse effect on our ability to raise the funds necessary to continue our operations. Assertions by third parties that we violate their intellectual property rights could therefore have a material adverse effect on our business, financial condition and results of operations.

Our business depends on our ability to effectively invest in, implement improvements to, and properly maintain the uninterrupted operation, security and integrity of, our operating platform and other information technology and business systems.

Our business is highly dependent on maintaining effective information technology systems as well as the integrity and timeliness of the data we use to serve our customers, support our partners and operate our business. It is possible that hardware failures or errors in our systems could result in data loss or corruption, or cause the information that we collect to be incomplete, or contain inaccuracies that our customers regard as significant. Because of the large amount of data that we

collect and manage, if our data were found to be inaccurate or unreliable, or became inaccessible, whether due to failures, errors, or other reasons, or if we, or any of our third-party service providers, especially our third-party dialing and routing software systems, were to fail to effectively maintain such information systems and data integrity, we could experience operational disruptions that may impact our customers, individuals and partner teams, and hinder our ability to provide services, establish appropriate pricing for services, retain and attract customers, establish reserves, report financial results timely and accurately and maintain regulatory compliance, among other things.

Our information technology strategy and execution are critical to our continued success. We must continue to invest in long-term solutions that will enable us to anticipate customer needs and expectations, enhance our customer experience, act as a differentiator in the market, comply with applicable laws, and protect against cybersecurity risks and threats. Our success is dependent, in large part, on maintaining the effectiveness of existing technology systems and continuing to deliver and enhance technology systems that support our business processes in a cost-efficient and resource-efficient manner and enable us to analyze and manage data in a comprehensive manner. Increasing and shifting regulatory and legislative requirements are likely to place additional demands on our information technology infrastructure that could have a direct impact on resources available for other projects tied to our strategic initiatives.

Also, in the event of damage or interruption, our insurance policies may not adequately compensate us for any losses that we may incur. System failures or outages, including any potential disruptions due to significantly increased global demand on certain cloud-based systems during a pandemic, could compromise our ability to perform these functions in a timely manner, which could harm our ability to conduct business or delay our financial reporting. Such failures could adversely affect our operating results and financial condition. In addition, certain of our third-party service providers are required to notify us if they experience a security breach or unauthorized disclosure of certain personal information, or, in some cases, confidential data or information of ours or our billers, partners or consumers, and their failure to timely notify us of such a breach or disclosure may cause us to incur significant costs or otherwise harm our business. Additionally, we may make critical transactions on behalf of our customers, and any errors, defects or other infrastructure problems could result in damage to such consumers. These consumers could seek significant compensation from us for their losses and our insurance policies may be insufficient to cover a claim. Even if unsuccessful, this type of claim may be time-consuming and costly for us to defend.

Furthermore, prolonged interruption in the availability, or reduction in the speed or other functionality, of our systems, products or services could materially harm our reputation and business. Frequent or persistent interruptions in accessing our systems and services could cause consumers to believe that our systems and services are unreliable, leading them to switch to our competitors or to avoid our systems and services, and could permanently harm our reputation and business.

Connectivity and interoperability among technologies is becoming increasingly important. As a result, we must also develop new systems to meet current market standards and keep pace with continuing changes in information processing technology, evolving industry and regulatory standards and customer needs. Failure to do so may present compliance challenges and impede our ability to deliver services in a competitive manner. Further, system development projects are long term in nature, may be more costly than expected to complete and may not deliver the expected benefits upon completion. In addition, we may not be able to adequately assess the functionality, and data integrity and security impacts, of new or significantly changed products, services, business processes or infrastructure that we use. Our failure to effectively invest in, implement improvements to and properly maintain the uninterrupted operation and integrity of our information technology and other business systems, as well as any write-downs in connection with the obsolescence of our technology, could materially and adversely affect our business, financial condition and results of operations.

Disruptions of the information technology systems or infrastructure of certain of our third-party vendors and service providers could also disrupt our businesses, damage our reputation, increase our costs, and have a material adverse effect on our business, financial condition and results of operations.

We rely heavily on the communications and information systems of third parties to conduct our business. For instance, we rely on computing infrastructure operated by Amazon Web Services (“AWS”) and Microsoft Azure (“Azure”) to host or operate some or all of certain key products or functions of our business. Our customers need to be able to access our systems at any time, without interruption or degradation of performance. Our technological infrastructure depends, in part, on the virtual cloud infrastructure hosted in AWS and Azure. Although we have disaster recovery plans that utilize multiple AWS and Azure locations, any incident affecting their infrastructure could adversely affect our cloud-native platform. A prolonged AWS or Azure service disruption affecting our cloud-native platform would adversely impact our ability to service our customers and could damage our reputation with current and potential customers, expose us to liability, result in substantial costs for remediation, could cause us to lose customers, or otherwise harm our business, financial condition and results of operations. We may also incur significant costs for using alternative hosting sources or taking other actions in preparation for, or in reaction to, events that damage the AWS or Azure services we use. Additionally, in the event that our

AWS or Azure service agreements are terminated, or there is a lapse of service, elimination of AWS or Azure services or features that we utilize, or damage to such facilities, we could experience interruptions in access to our systems as well as significant delays and additional expenses in arranging for or creating new facilities or re-architecting our systems for deployment on a different cloud infrastructure service provider, which would adversely affect our business, financial condition, and results of operations.

As expectations regarding operational and information security practices have increased, our operating systems and infrastructure, and those of our third-party service providers, must continue to be safeguarded and monitored for potential failures, disruptions, breakdowns, and attacks. Our data processing systems, or other operating systems and facilities, and those of our third-party service providers, may stop operating properly or become disabled or damaged as a result of a number of factors, including events that are wholly or partially beyond our and our third-party service providers' control. For example, there could be electrical or telecommunication outages; software bugs and defects; server malfunctions; human error; natural disasters such as earthquakes, tornadoes, or hurricanes; disease pandemics and related government orders; events arising from local or larger scale political or social matters, including terrorist acts; cyberattacks and other data security incidents, including ransomware, malware, phishing, social engineering, including some of the foregoing that target the cryptoeconomy in particular. These incidents can range from individual attempts to gain unauthorized access to information technology systems to more sophisticated security threats involving cybercriminals, hacktivists, cyberterrorists, nation-state actors, or the targeting of commercial financial accounts. These events can also result from internal compromises, such as human error or malicious internal actors, of our workforce or our vendors' personnel.

While we have business continuity, disaster recovery and other policies and procedures designed to prevent or limit the effect of the failure, interruption or security breach of our information systems, there can be no assurance that any such failures, interruptions or security breaches will not occur or, if they do occur, that they will be adequately addressed. Furthermore, if such failures, interruptions or security breaches are not detected immediately, their effect could be compounded. Our risk and exposure to these matters remains heightened because of the evolving nature of these threats and our use of third-party service providers with access to our systems and data. As a result, cybersecurity and the continued development and enhancement of our controls, processes, and practices designed to protect our systems, computers, software, data, and networks from attack, damage or unauthorized access remain a focus for us. Disruptions or failures in the physical infrastructure or operating systems that support our businesses and customers, or cyberattacks or security breaches of our networks, systems or devices, or those that our customers or third-party service providers use to access our products and services, could result in customer attrition, financial and trading losses, reputational damage, reimbursement or other compensation costs, and/or remediation costs, any of which could have a material effect on our results of operations or financial condition.

Some of our products and services contain open source software, which may pose particular risks to our proprietary software, products and services in a manner that could harm our business.

We use open source software in our products and services and anticipate using open source software in the future. Some open source software licenses require those who distribute open source software as part of their own software product to publicly disclose all or part of the source code to such software product or to make available any derivative works of the open source code on unfavorable terms or at no cost, and we may be subject to such terms. The terms of many open source licenses to which we are subject have not been interpreted by U.S. or foreign courts, and there is a risk that open source software licenses could be construed in a manner that imposes unanticipated conditions or restrictions on our ability to provide or distribute our products or services. We could face claims from third parties claiming ownership of, or demanding release of, the open source software or derivative works that we developed using such software, which could include our proprietary source code, or otherwise seeking to enforce the terms of the applicable open source license. These claims could result in litigation and could require us to make our software source code freely available, purchase a costly license or cease offering the implicated products or services unless and until we can reengineer them to avoid infringement, which may be a costly and time-consuming process. While we monitor our use of open source software and try to ensure that none is used in a manner that would require us to disclose our proprietary source code or that would otherwise breach the terms of an open source agreement, such use could inadvertently occur, or could be claimed to have occurred, in part because open source license terms are often ambiguous. Any actual or claimed requirement to disclose our proprietary source code or pay damages for breach of contract could harm our business and could help third parties, including our competitors, develop products and services that are similar to or better than ours.

Additionally, the use of certain open source software can lead to greater risks than use of third-party commercial software, as open source licensors generally do not provide warranties or controls on the origin of software. There is typically no support available for open source software, and we cannot ensure that the authors of such open source software will implement or push updates to address security risks or will not abandon further development and maintenance. Many

of the risks associated with the use of open source software, such as the lack of warranties or assurances of title or performance, cannot be eliminated, and could, if not properly addressed, negatively affect our business. Any of these risks could be difficult to eliminate or manage and, if not addressed, could have an adverse effect on our business, financial condition and results of operations.

Disruptions in our, or our service providers', disaster recovery systems or management continuity planning could limit our ability to operate our business effectively.

Our information technology systems facilitate our ability to conduct our business. While we have disaster recovery systems and business continuity plans in place, any disruptions in our, or our service providers', disaster recovery systems or the failure of these systems to operate as expected could, depending on the magnitude of the problem, adversely affect our operating results by limiting our capacity to effectively conduct our operations. Despite our implementation of a variety of security measures, our information technology systems could be subject to physical or electronic compromises and similar disruptions from unauthorized tampering, or to weather-related disruptions where our systems are hosted. In addition, in the event that a significant number of our personnel were unavailable in the event of a disaster or we failed to recover office facilities or systems, our ability to effectively conduct business could be adversely affected. Any of the foregoing could have a material adverse effect on our business, financial condition and results of operations.

If we fail to comply with our obligations under license or technology agreements with third parties or are unable to license rights to use technologies on reasonable terms, we may be required to pay damages and could potentially lose license rights that are critical to our business.

We license certain intellectual property, including technologies, data, content and software from third parties, that is important to our business, and in the future, we may enter into additional agreements that provide us with licenses to valuable intellectual property or technology. If we fail to comply with any of the obligations under our license agreements, we may be required to pay damages and the licensor may have the right to terminate the license. Termination by the licensor would cause us to lose valuable rights and could prevent us from selling our products and services, or inhibit our ability to commercialize future products and services. Our business would suffer if any current or future licenses terminate, if the licensors fail to abide by the terms of the license, if the licensed intellectual property rights are found to be invalid or unenforceable, or if we are unable to enter into necessary licenses on acceptable terms. Moreover, our licensors may own or control intellectual property that has not been licensed to us and, as a result, we may be subject to claims, regardless of their merit, that we are infringing or otherwise violating the licensor's rights.

In the future, we may identify additional third-party intellectual property we may need to license in order to engage in our business. However, such licenses may not be available on acceptable terms or at all. The licensing or acquisition of third-party intellectual property rights is a competitive area, and several more-established companies may pursue strategies to license or acquire third-party intellectual property rights that we may consider attractive or necessary. In addition, companies that perceive us to be a competitor may be unwilling to assign or license rights to us. Even if such licenses are available, we may be required to pay the licensor substantial royalties based on sales of our products and services. Such royalties are a component of the cost of our products or services and may affect the margins on our products and services. In addition, such licenses may be nonexclusive, which could give our competitors access to the same intellectual property licensed to us. Any of the foregoing could have a material adverse effect on our competitive position, business, financial condition and results of operations.

We may be subject to claims that we have wrongfully hired an employee from a competitor, or that our employees, consultants or independent contractors have wrongfully used or disclosed confidential information of third parties or that our employees have wrongfully used or disclosed alleged trade secrets of their former employers.

Many of our employees, consultants and advisors, or individuals that may in the future serve as our employees, consultants and advisors, are currently or were previously employed at companies including our competitors or potential competitors. Although we try to ensure that our employees, consultants, independent contractors and advisors do not use the confidential or proprietary information, trade secrets or know-how of others in their work for us, we may be subject to claims that we have, inadvertently or otherwise, used or disclosed confidential or proprietary information, trade secrets or know-how of these third parties, or that our employees, consultants or, independent contractors or advisors have, inadvertently or otherwise, used or disclosed confidential information, trade secrets or know-how of such individual's current or former employer. If we fail in defending any such claims, in addition to paying monetary damages, we may lose valuable intellectual property rights or personnel. Litigation may be necessary to defend against these claims. Even if we are successful in defending against these claims, and whether or not such claims have merit, litigation could result in substantial cost and be a distraction to our management and employees. We cannot predict whether we would prevail in any such actions. Moreover, intellectual property litigation, regardless of its outcome, may cause negative publicity and

could prohibit us from marketing or otherwise commercializing our offerings and technology. Claims that we, our employees, consultants or advisors have misappropriated the confidential or proprietary information, trade secrets or know-how of third parties could therefore have a material adverse effect on our business, financial condition and results of operations.

If we are unable to protect the confidentiality of our trade secrets, know-how and other proprietary and internally developed information, the value of our technology could be adversely affected.

We may not be able to protect our trade secrets, know-how and other internally developed information adequately. Although we use reasonable efforts to protect this internally developed information and technology, our employees, consultants and other parties (including independent contractors and companies with whom we conduct business) may unintentionally or willfully disclose our information or technology to competitors. Enforcing a claim that a third party illegally disclosed or obtained and is using any of our internally developed information or technology is difficult, expensive and time consuming, and the outcome is unpredictable. We rely, in part, on nondisclosure, confidentiality and assignment-of-invention agreements with our employees, independent contractors, consultants and companies with whom we conduct business to protect our trade secrets, know-how and other intellectual property rights and internally developed information. These agreements may not be self-executing, or they may be breached and we may not have adequate remedies for such breach. Moreover, third parties may independently develop similar or equivalent proprietary information or otherwise gain access to our trade secrets, know-how and other internally developed information. Additionally, as with other potential information security breaches, our trade secrets could also be compromised. Any of these events could materially and adversely affect our business, financial condition and results of operations.

Risks Related to Our Organizational Structure and Ownership of our Class A Common Stock

GDI's principal asset is its direct ownership interest in GDH LP. GDI is accordingly dependent upon distributions from GDH LP to pay dividends, if any, and taxes, make payments under the Tax Receivable Agreement and pay other expenses.

GDI's principal asset is its direct ownership of limited partnership units of GDH LP ("LP Units"). GDI has no independent means of generating revenue. GDH LP is treated as a partnership for U.S. federal income tax purposes and, as such, is not subject to U.S. federal income tax. Instead, the taxable income of GDH LP is allocated to holders of LP Units, including GDI. Accordingly, GDI incurs U.S. federal income taxes on its allocable share of any net taxable income of GDH LP. It also incurs expenses related to its operations, and has obligations to make payments under the Tax Receivable Agreement. As the sole general partner of GDH LP, GDI intends to cause GDH LP to make distributions to the holders of LP Units in amounts sufficient to (i) cover all applicable taxes payable by GDI and the other holders of LP Units, (ii) allow it to make any payments required under the Tax Receivable Agreement, (iii) fund dividends to its stockholders in accordance with its dividend policy to the extent that its board of directors declares such dividends and (iv) pay its expenses.

Deterioration in the financial conditions, earnings or cash flow of GDH LP and its subsidiaries for any reason could limit or impair their ability to pay such distributions. Additionally, to the extent that GDI needs funds and GDH LP is restricted from making such distributions to GDI under applicable law or regulation or as a result of covenants in its debt agreements or otherwise, GDI may not be able to obtain such funds on terms acceptable to it, or at all, and, as a result, could suffer a material adverse effect on its liquidity and financial condition.

Our Founder controls a significant portion of our voting power and his interests may be different from those of stockholders and may prevent new investors from influencing significant corporate decisions, including mergers, consolidations, or the sale of us or all or substantially all of our assets.

As of October 31, 2025, our Founder owned, indirectly through entities controlled by him, shares of our Class A common stock and Class B common stock entitling him to approximately 49.2% of our total voting power.

Accordingly, our Founder has significant influence over matters that require approval of our stockholders, including the election of members of the board of directors. This concentration of ownership and voting power may also delay, defer or prevent an acquisition by a third party or other change of control of Galaxy and may make some transactions more difficult or impossible without the support of our Founder even if they are in the best interests of the stockholders. This could have the effect of discouraging transactions in which you as a holder of shares of our Class A common stock might otherwise receive a premium for your shares over the then-current market price. Collectively, these considerations may have a negative effect on the price of our Class A common stock.

Our Founder's interests may not be fully aligned with those of other holders of our Class A common stock which, given our Founder's power and influence, could lead to actions that are not in the best interests of stockholders. For example, our Founder may have a different tax position from the Company and holders of our Class A common stock, especially in light of the existence of the Tax Receivable Agreement, which could influence decisions regarding whether and when we should dispose of assets or incur new, or refinance existing, indebtedness, or whether and when we should undergo certain changes of control for purposes of the Tax Receivable Agreement or terminate the Tax Receivable Agreement. In addition, the structuring of future transactions may take into consideration these tax or other considerations even where no similar benefit would accrue to us. Our Founder might also be motivated to take actions to retain his significant stake in Galaxy at the expense of maximizing the overall value of Galaxy (and therefore the market price of our Class A common stock). Our Founder's fiduciary duties may serve as a check on any such motivation, but holders of our Class A common stock cannot be assured that the potential divergence of our Founder's interests and theirs might not hurt the market price of our Class A common stock.

In certain circumstances, GDH LP is required to make distributions to GDI and the other holders of LP Units, and the distributions that GDH LP may be required to make could be substantial.

Under the amended and restated limited partnership agreement of GDH LP (the "Amended LP Agreement"), GDH LP is generally required from time to time to make pro rata distributions in cash to GDI and the other holders of LP Units at certain assumed tax rates in amounts that are intended to be sufficient to cover the U.S. federal income taxes on our and the other GDH LP limited partners' respective allocable shares of the taxable income of GDH LP. The distributions GDH LP may be required to make could be substantial, including as a result of the future recognition of capital gains associated with contributions by GDH LP to qualified opportunity zones. As a result of (i) potential differences in the amount of net taxable income allocable to GDI and the other GDH LP limited partners, (ii) the lower income tax rate applicable to corporations than individuals and (iii) the use of an assumed tax rate (based on the income tax rate applicable to individuals, or, if higher, corporations) in calculating GDH LP's distribution obligations, GDI may receive tax distributions significantly in excess of its tax liabilities and obligations to make payments under the Tax Receivable Agreement. GDI's board of directors will determine the appropriate uses for any excess cash so accumulated, which may include, among other uses, dividends, repurchases of its Class A common stock, or purchases of additional LP Units (either of which may be accompanied by a pro rata adjustment to the number of LP Units held by the other GDH LP limited partners in order to preserve the intended one-to-one correspondence between LP Units held by GDI and outstanding shares of our Class A common stock), the payment of obligations under the Tax Receivable Agreement and the payment of other expenses. GDI has no obligation to distribute such cash (or other available cash other than any declared dividend) to its stockholders. No adjustments to the redemption or exchange ratio of LP Units for shares of Class A common stock will be made as a result of either (i) any cash distribution by GDI or (ii) any cash that GDI retains and does not distribute to its stockholders. To the extent that GDI does not distribute such excess cash as dividends on its Class A common stock and instead, for example, hold such cash balances or lend them to GDH LP, holders of LP Units would benefit from any value attributable to such cash balances as a result of their ownership of Class A common stock following a redemption or exchange of their LP Units.

The market price and trading volume of our Class A common stock may be volatile, which may affect the value of an investment in our Class A common stock and could subject us to litigation.

The market price and trading volume of our Class A common stock may be volatile and will likely continue to be subject to significant fluctuations in response to, among other factors: developments in the industries in which we operate; market fluctuations in digital assets generally or changes in the underlying values and trading volumes of the digital assets that we hold or trade; our financial performance and prospects or changes in the financial performance and prospects of companies engaged in businesses that are similar to our businesses; changes in laws or regulations, including tax laws, or new interpretations or applications of laws and regulations, that are applicable to our businesses; sales of our Class A common stock by our existing stockholders, including Class A common stock issued upon redemption or exchange of any LP Units; general economic trends and other external factors, including those resulting from war, incidents of terrorism or responses to such events; speculation in the press or investment community regarding our or our business or investments, or factors or events that may directly or indirectly affect our businesses or investments; and further issuances of our Class A common stock or LP Units.

The price of our Class A common stock also could be subject to wide fluctuations in response to the risk factors described in this Quarterly Report on Form 10-Q and others beyond our control, including:

- the number of shares of our Class A common stock publicly owned and available for trading;
- overall performance of the equity markets or publicly-listed financial services and technology companies;

- our actual or anticipated operating performance and the operating performance of our competitors;
- changes in the projected operational and financial results we provide to the public or our failure to meet those projections;
- failure of securities analysts to initiate or maintain coverage of us, changes in financial estimates by any securities analysts who follow our company, or our failure to meet the estimates or the expectations of investors;
- any major change in our board of directors, management, or key personnel;
- if we issue additional shares of capital stock, including in the form of blockchain tokens, in connection with customer reward or loyalty programs;
- rumors and market speculation involving us or other companies in our industry;
- announcements by us or our competitors of significant innovations, new products, services, features, integrations or capabilities, acquisitions, strategic investments, partnerships, joint ventures, or capital commitments;
- changes or proposed changes in laws or regulations or differing interpretations or enforcement thereof affecting our business;
- litigation or other proceedings involving us, our industry or both, or investigations by regulators into our operations or those of our competitors;
- the global political, economic, and macroeconomic climate; and
- other events or factors, including those resulting from pandemic, war, incidents of terrorism, or responses to these events.

In recent years, stock markets have experienced significant price and volume fluctuations, which have had a significant impact on the market price of securities issued by many companies, irrespective of the operating performance of the affected companies. Moreover, the prices of the digital assets that we hold or trade have historically been, and will likely continue to be, highly volatile. Accordingly, the price of our Class A common stock could fluctuate based upon factors that have little or nothing to do with us or our operating performance, which could materially and adversely affect the value of any investment in our Class A common stock.

In addition, in the past, following periods of market volatility, shareholders have instituted securities class action litigation against various issuers. If we were to become involved in such securities litigation, it could have a substantial cost and divert resources and the attention of executive management from our business regardless of the outcome of such litigation, which may adversely affect the market price of our Class A common stock and our business, financial condition and results of operation.

Moreover, the market price and trading volume of our Class A common stock may be subject to even greater volatility now that our Class A common stock is listed on Nasdaq. Prior to the consummation of the Reorganization Transactions, GDHL was limited in its ability to offer its ordinary shares to U.S. investors or to avail itself of the U.S. capital markets. Our consummation of the Reorganization Transactions and subsequent listing on Nasdaq has enabled individual investors, retail investors and others who may have not previously been permitted to trade in GDHL's ordinary shares to trade in our Class A common stock. These factors could cause volatility in the market price of our Class A common stock and an unsustainable market price if, for example, institutional investors believe our Class A common stock is worth less than retail investors, in which case the price of our Class A common stock may fluctuate and/or decline over time. Further, if the public price of our Class A common stock is above the level that investors determine is reasonable for our Class A common stock, some investors may attempt to short our Class A common stock, which would create additional downward pressure on the public price of our Class A common stock. Moreover, to the extent that there is a lack of consumer awareness among retail investors, or there is insufficient demand for our Class A common stock among U.S. investors more generally, such events could reduce the market price of our Class A common stock and cause volatility in the market price of our Class A common stock.

There can be no assurance that an active trading market on the TSX or Nasdaq for our Class A common stock will be maintained or develop. The lack of a liquid market for our Class A common stock could also result from the relatively small percentage of our Class A common stock that is beneficially owned by public shareholders and available for trading,

with a relatively large percentage of our Class A common stock beneficially owned by holders of LP Units (and therefore not available for trading absent the redemption or exchange of such LP Units). If an active market does not develop or is not maintained, you may have difficulty selling any shares of our Class A common stock that you own. An inactive market may also impair our ability to raise capital by selling shares of our Class A common stock and may impair our ability to acquire or make investments in companies, products or technologies for which we may issue equity securities to pay for such acquisition or investment. In the absence of an active trading market relatively small sales may result in a significant negative effect on the price of our Class A common stock.

Changes in law could cause our Class A common stock to be de-listed from the TSX or Nasdaq or any other exchange on which we are listed or may be listed in the future, or cause us to undergo costly restructuring, liquidation or sale. Further, we may need or want to raise additional capital, but we may be unable to do so due to changes in law, regulation or interpretation.

Apart from the numerous material legal and regulatory risks to us described elsewhere in this section, we could be adversely affected by changes in law, regulation, interpretation of such law or regulation or regulator or exchange discretion. Such changes are difficult to predict but could conceivably lead to a cease-trade or the de-listing of our Class A common stock, the inability to list our Class A common stock in other jurisdictions or a costly restructuring or even liquidation of Galaxy.

If, whether by reason of changes in law, regulation or interpretation, or by reason of our or our conduct, we became unable to sell securities to investors in particular jurisdictions, the liquidity and market price of our Class A common stock would be negatively impacted, which would make it more difficult for us to sell additional Class A common stock or otherwise raise capital. Such difficulties could lead to our bankruptcy or insolvency, which may lead to material or complete losses for holders of Class A common stock.

The market price of our Class A common stock may be subject to downward pressure due to redemptions or exchanges of LP Units for shares of Class A common stock, exercises of outstanding options, exchanges of Exchangeable Notes or from additional issuances of our Class A common stock.

The majority of the economic interest in GDH LP remains represented by LP Units and each GDH LP limited partner may redeem all or a portion of their LP Units for newly issued shares of Class A common stock (or, if we elect, cash of equivalent value) on a one-for-one basis with the number of LP Units redeemed. At our option, we may also effect a direct exchange of such LP Units for shares of Class A common stock (or, if we elect, cash of equivalent value). Upon any such redemption or exchange, shares of Class B common stock held by GDH LP limited partners will be cancelled on a one-for-one basis with every LP Unit redeemed or exchanged. As and to the extent LP Units are redeemed or exchanged for newly issued shares of Class A common stock, the economic interest of then-current holders of our Class A common stock will decrease proportionately (though the direct economic interest of the Company in GDH LP will increase proportionately). Such redemptions or exchanges would increase the market supply of Class A common stock, which could lead to a decrease in the market price of Class A common stock, especially since it is foreseeable that many redemptions or exchanges may closely precede sales, and could result in significant dilution for holder of our Class A common stock.

Furthermore, GDH LP issued \$500 million aggregate principal amount of 3.00% Exchangeable Senior Notes due 2026 (the “2026 Exchangeable Notes”) on December 9, 2021, \$402.5 million aggregate principal amount of 2.500% Exchangeable Senior Notes due 2029 (the “2029 Exchangeable Notes”) on November 25, 2024 and \$1.30 billion aggregate principal amount of 0.50% Exchangeable Senior Notes due 2031 (the “2031 Exchangeable Notes” and, together with the 2026 Exchangeable Notes and the 2029 Exchangeable Notes, the “Exchangeable Notes”) on October 30, 2025. From time to time and subject to the terms of the indentures governing the Exchangeable Notes, the Exchangeable Notes are exchangeable for shares of our Class A common stock at the option of the holders thereof. The maximum number of shares of our Class A common stock issuable upon the exchange of all outstanding 2026 Exchangeable Notes, all 2029 Exchangeable Notes and all 2031 Exchangeable Notes is approximately 74.2 million, subject to certain adjustments as set forth in the indentures. On or after September 15, 2026 and prior to the close of business on the second scheduled trading day immediately preceding their maturity date, holders may exchange their 2026 Exchangeable Notes, in multiples of \$250,000 principal amount, at their option at any time. On or after September 1, 2029, and prior to the close of business on the second scheduled trading day immediately preceding their maturity date, holders may exchange their 2029 Exchangeable Notes, in multiples of \$250,000 principal amount, at their option at any time. On or after February 1, 2031, and prior to the close of business on the second scheduled trading day immediately preceding their maturity date, holders may exchange their 2031 Exchangeable Notes, in multiples of \$1,000 principal amount, at their option at any time. Holders may exchange their 2026 Exchangeable Notes, 2029 Exchangeable Notes and 2031 Exchangeable Notes prior to the close of business on the business day immediately preceding September 15, 2026, September 1, 2029, and February 1, 2031, respectively, only under certain circumstances. As of September 30, 2025, there was \$1,281.0 million in principal

outstanding of the Exchangeable Notes. To the extent that we elect to settle exchanges of the Exchangeable Notes in whole or in part in shares of Class A common stock, it will result in a dilution of the value of a stockholder's interests in our Class A common stock, and any such dilution may be material. Similarly, if we issue additional shares of Class A common stock, then-current holders of Class A common stock will be diluted. For example, on October 17, 2025, we issued 9,027,778 shares of Class A common stock as part of the October Private Placement. The potential for the issuance of additional shares of our Class A common stock could have a material adverse effect on the market price of our Class A common stock.

Substantial future sales of shares of our Class A common stock in the public market could cause the market price of our Class A common stock to fall.

Sales of a substantial number of shares of our Class A common stock in the public market, or the perception that these sales might occur, could adversely affect the market price of our Class A common stock and may make it more difficult for you to sell your Class A common stock at a time and price that you deem appropriate. If GDH LP limited partners or any holders of our Class A common stock (or LP Units that are redeemable or exchangeable for our Class A common stock) sell, or indicate an intention to sell, substantial amounts of our Class A common stock in the public market after any legal restrictions on resale lapse, the market price of our Class A common stock could substantially decline. As of October 31, 2025 our Founder owned, indirectly through entities controlled by him, shares of our Class A common stock and Class B common stock entitling him to approximately 49.2% of our total voting power. If our Founder alone were to sell a substantial portion of the shares he beneficially owns, it could cause the market price of our Class A common stock to decline.

All shares of our Class A common stock into which the ordinary shares of GDHL converted by operation of law in connection with the Reorganization Transactions and all the shares of our Class A common stock that were sold in our June 2025 underwritten public offering are freely tradable in the public market without restriction or further registration under the Securities Act, other than shares held by our "affiliates," as that term is defined in Rule 144 under the Securities Act ("Rule 144").

The remaining outstanding shares of Class A common stock (as well as any additional shares of our Class A common stock issuable (i) upon redemption or exchange of outstanding LP Units held by GDH LP limited partners or (ii) upon the exchange of outstanding Exchangeable Notes by the holders thereof) are, unless registered under the Securities Act, and shares of Class A common stock underlying outstanding RSUs or subject to outstanding stock options will be (unless covered by a registration statement on Form S-8) on issuance, deemed to be "restricted securities" as defined in Rule 144. We have filed an immediately effective registration statement on Form S-8 under the Securities Act covering all shares of Class A common stock subject to stock options outstanding and reserved for issuance under our equity incentive plans. We also have an effective resale registration statement on Form S-1 in respect of the shares of Class A common stock issuable upon the redemption or exchange of outstanding LP Units and upon the exchange of outstanding Exchangeable Notes. In addition, we have filed a resale registration statement on Form S-1 covering the offer and sale from time to time of 12,777,778 shares of Class A common stock issued in the October Private Placement. The shares issued in the October Private Placement are subject to a lock-up period of 90 days following the closing of the October Private Placement. Upon the expiration of such lock-up period, all such shares will be eligible for resale in the public market, subject to compliance with applicable federal securities laws.

In the future, we may issue additional shares of Class A common stock or other equity or debt securities convertible into or exercisable or exchangeable for shares of our Class A common stock in connection with a financing, strategic investment, litigation settlement or employee arrangement or otherwise.

If such shares of our Class A common stock are sold, or if it is perceived that they will be sold in the public market, the market price of our Class A common stock could decline.

If we are deemed to be an investment company under the Investment Company Act, applicable restrictions could make it impractical for us to continue our business as contemplated and could have a material adverse effect on our business.

Under Sections 3(a)(1)(A) and (C) of the Investment Company Act, a company generally will be deemed to be an "investment company" for purposes of the Investment Company Act if (i) it is, or holds itself out as being, engaged primarily, or proposes to engage primarily, in the business of investing, reinvesting or trading in securities or (ii) it engages, or proposes to engage, in the business of investing, reinvesting, owning, holding or trading in securities and it owns or proposes to acquire investment securities having a value exceeding 40% of the value of its total assets (exclusive of U.S. government securities and cash items) on an unconsolidated basis.

We do not believe that we are an “investment company,” as such term is defined in either of those sections of the Investment Company Act. As the sole general partner of GDH LP, we control and operate GDH LP. On that basis, we believe that our interest in GDH LP is not an “investment security” as that term is used in the Investment Company Act. However, if we were to cease participation in the management of GDH LP, our interest in GDH LP could be deemed an “investment security” for purposes of the Investment Company Act. We intend to conduct our operations so that we will not be deemed to be an investment company under the Investment Company Act or otherwise conduct our business in a manner that does not subject us to the registration and other requirements of the Investment Company Act. In order to ensure that we are not deemed to be an investment company, we may be limited in the assets that we may continue to own and, further, may need to dispose of or acquire certain assets at such times or on such terms as may be less favorable to us than in the absence of such requirement.

For example, certain of our venture investments may be considered investment securities and we might be required to dispose of one or more of them, or to limit the extent of our venture investments business (such as by foregoing otherwise attractive balance sheet venture investment opportunities), in order not to become an investment company. Further, certain of our operating subsidiaries rely on specific exemptions from the Investment Company Act to operate their businesses. In particular, we operate our digital asset financing business so as to comply with the exemption under Section 3(c)(2) of the Investment Company Act for businesses primarily engaged in, among other things, acting as a market intermediary with respect to financial contracts relating to commodities or currencies. If our digital asset financing business was to fail to comply with this exemption, it could result in our being unable to conduct such business and it could also cause us to be deemed an investment company as our own status under the Investment Company Act depends in part on that of our operating subsidiaries that conduct our businesses. If anything were to happen which would cause us to be deemed to be an investment company under the Investment Company Act (such as the classification of digital assets held by us as securities for purposes of the Investment Company Act, or significant changes in the value of our investments or other assets), the requirements imposed by the Investment Company Act could make it impractical for us to continue our business as currently conducted, which would materially adversely affect our business, financial condition and results of operations. In addition, if we were to become inadvertently subject to the Investment Company Act, any violation of the Investment Company Act could subject us to material adverse consequences, including potentially significant regulatory penalties and the possibility that certain of our contracts could be deemed unenforceable.

In addition, if anything were to happen which would cause us to be deemed to be an investment company under the Investment Company Act, it will become more difficult and costly for us to comply with the applicable requirements of the securities legislation and regulations thereunder of each province and territory of Canada (“Canadian Securities Laws”).

Our stockholders will generally not benefit from protections of investment company statutes in various jurisdictions, and may suffer from the restrictions that such statutes place on the liquidity of our Class A common stock and on our fundraising, businesses or other activities.

We are not an investment fund and do not intend to operate as an investment fund in the future. Nonetheless, it is possible that we may effectively be classified as the equivalent of a commodity pool (to the extent that digital assets are deemed to fall within the definition of a “commodity interest” under the Commodity Exchange Act) or an investment fund under the investment company laws of various jurisdictions, including the European Union Alternative Investment Fund Managers Directive.

Our business is designed to comply with exemptions from the application of such laws, which means that holders of Class A common stock do not and will not benefit from the investor protections provided by such laws. At the same time, we may be constrained by such laws from raising additional capital in certain jurisdictions, to the potential detriment of the value and liquidity of Class A common stock, and we may be restricted or precluded from operating in certain jurisdictions without additional financial registrations or licenses that we do not currently have.

Furthermore, if, whether by reason of changes in law, regulation or interpretation or by reason of our conduct, we no longer qualify for applicable exemptions from commodity pool or investment company laws, the results may materially adversely affect us and could lead to our liquidation or sale, which may lead to material or complete losses for holders of Class A common stock.

We will be required to indemnify our directors and certain officers or other agents against a wide range of potential liabilities and these indemnification obligations could be material.

Our amended and restated certificate of incorporation and amended and restated bylaws (together, our “organizational documents”) provide for customarily broad rights of indemnification for our directors, officers, employees and certain other agents to the fullest extent authorized by the Delaware General Corporation Law (the “DGCL”). The organizational

documents also provide for the possibility of advancement of expenses to such indemnified persons. In addition, we have entered into indemnification agreements with our directors and officers. While rights of indemnification are typically viewed as a key protection and inducement for indemnified persons to serve in senior roles in which they may be exposed to liability, indemnification payments and advancement of expenses may be material and may have an adverse effect on us. Furthermore, indemnified persons may be subject to derivative or other similar claims brought by the stockholders or us, which claims would generally be expected to be covered by rights of indemnification and, potentially, advancement of expenses. In certain circumstances, subject to applicable laws in the relevant jurisdictions, indemnified persons may be entitled to indemnification even if their liabilities arose from their own negligence or unlawful conduct. We have incurred, and are expected to continue to incur, significant expense to procure directors and officers liability insurance that both supports our potential indemnification obligations and, in some cases, provides indemnified persons with additional protection beyond the scope of these obligations. If we are unable to maintain adequate insurance, there could be adverse consequences.

We are required to pay GDH LP limited partners who redeem or exchange LP Units for shares of Class A common stock for certain tax benefits that we may claim, and the amounts that we may pay could be material.

We are party to the Tax Receivable Agreement with certain present and former limited partners of GDH LP (the “TRA Parties”) that provides for the payment by us to the TRA Parties of 85% of the amount of cash savings, if any, in U.S. federal, state and local income tax or franchise tax that we actually realize as a result of (i) any increase in tax basis in GDH LP’s assets resulting from redemptions or exchanges by those holders of LP Units for shares of Class A common stock in accordance with the terms of the LP Units and payments made under the Tax Receivable Agreement, and (ii) deductions in respect of interest with respect to payments made under the Tax Receivable Agreement, as and when such tax benefits are realized. We are required to make similar payments to GDH LP limited partners who previously exchanged their partnership interests in GDH LP for GDHL ordinary shares. The payment obligations under the Tax Receivable Agreement are our obligations and are not the obligations of GDH LP.

The actual increase in tax basis, as well as the amount and timing of any payments under the Tax Receivable Agreement, varies depending upon a number of factors, including the timing of redemptions or exchanges by the TRA Parties, the price of Class A common stock at the time of the exchange, the extent to which such exchanges are taxable, the amount and timing of the taxable income that we generate in the future, the tax rate then applicable and the portion of our payments under the Tax Receivable Agreement that constitute imputed interest. The payments that we will be required to make under the Tax Receivable Agreement could be material. The payments are not conditioned upon the other TRA Parties’ continued ownership of Class A common stock.

Payments under the Tax Receivable Agreement are based on the tax reporting positions we determine, and the IRS or another tax authority may challenge all or a part of the tax basis increases, or other tax attributes subject to the Tax Receivable Agreement, and a court could sustain such challenge. Further, the parties to the Tax Receivable Agreement will not reimburse us for any payments previously made if such tax attributes are subsequently disallowed, except that any excess payments made to a TRA Party will be netted against future payments otherwise to be made to such TRA Party under the Tax Receivable Agreement, if any, after our determination of such excess. In addition, upon the occurrence of certain changes of control, the actual U.S. federal, state, local and/or non-U.S. tax savings we may realize may be different than the amount of such tax savings we are deemed to realize under the Tax Receivable Agreement, which will be based on the U.S. federal, state, local and/or non-U.S. tax rates in effect on the date of the change of control and certain assumptions, including that we would have sufficient taxable income to fully utilize the deductions arising from the tax basis increases and other tax attributes subject to the Tax Receivable Agreement. In both such circumstances, we could make payments to the TRA Parties that are greater than our actual cash tax savings and we may not be able to recoup those payments, which could negatively impact our liquidity. The Tax Receivable Agreement provides that (1) in the event that we breach any of our material obligations under the Tax Receivable Agreement or (2) if, at any time, we elect an early termination of the Tax Receivable Agreement, our obligations under the Tax Receivable Agreement (with respect to all LP Units, whether or not LP Units have been redeemed or exchanged before or after such transaction) would accelerate and become payable in a lump sum amount equal to the present value of the anticipated future tax benefits calculated based on certain assumptions, including that we would have sufficient taxable income to fully utilize the deductions arising from the tax basis increases and other tax attributes subject to the Tax Receivable Agreement. The change of control provisions in the Tax Receivable Agreement may result in situations where GDH LP limited partners have interests that differ from or are in addition to those of our other stockholders.

Finally, our ability to make payments under the Tax Receivable Agreement depends on the ability of GDH LP to make distributions to us. To the extent that we are unable to make payments under the Tax Receivable Agreement for any reason, such payments will be deferred and will accrue interest until paid. Non-payment may in certain circumstances constitute a

breach of a material obligation under the Tax Receivable Agreement and therefore accelerate payments due under the Tax Receivable Agreement, which could negatively impact our results of operations and could also affect our liquidity in periods in which such payments are made.

The holding of, or trading in, our Class A common stock may be, or become, illegal in certain countries or other jurisdictions.

One or more countries or jurisdictions, including but not limited to China, Russia, South Korea, the United States and Canada, may take regulatory actions now or in the future that severely restrict the right to acquire, own, hold, sell or use digital assets. Such actions or restrictions may also result in the restriction of holding or trading in our Class A common stock or cause the price of any affected digital asset to decrease, possibly substantially. Such actions or restrictions would likely materially and adversely affect the effectiveness of our investment and trading strategies, the value of our assets and the value of any investment in us. Stockholders are urged to consult legal advisors in their own relevant jurisdictions with respect to the current and prospective lawfulness of their purchasing, holding or selling our Class A common stock.

We do not anticipate paying any cash dividends in the foreseeable future.

We currently intend to retain our future earnings, if any, for the foreseeable future, to fund the development and growth of our business. Accordingly, we do not currently intend to pay any cash dividends to holders of our Class A common stock for the foreseeable future. As a result, capital appreciation in the price of our Class A common stock, if any, will be your only source of gain on an investment in our Class A common stock.

However, under the Amended LP Agreement, GDH LP is generally required from time to time to make pro rata distributions in cash to us and the other holders of LP Units at certain assumed tax rates in amounts that could be significant. See “—In certain circumstances, GDH LP is required to make distributions to us and the other holders of LP Units, and the distributions that GDH LP may be required to make could be substantial.”

If securities analysts do not publish or cease publishing research or reports about our business or if they downgrade our stock or our sector, or if there is any fluctuation in our credit rating, the price of our Class A common stock price and trading volume could decline.

The trading market for our Class A common stock will rely in part on the research and reports that industry or financial analysts publish about us or our business. We do not control these analysts. If securities or industry analysts drop coverage of our company or fail to commence coverage of us, the market price of our shares would likely be negatively impacted. Furthermore, if one or more of the analysts who do cover us downgrade our stock or our industry, or the stock of any of our competitors, or publish inaccurate or unfavorable research about our business, the price of our Class A common stock could decline. If one or more of these analysts stops covering us or fails to publish reports on us regularly, we could lose visibility in the market, which, in turn, could cause our stock price or trading volume to decline.

Additionally, any fluctuation in the credit rating of us or our subsidiaries may impact our ability to access debt markets in the future or increase our cost of future debt, which could have a material adverse effect on our operations and financial condition, which in return may adversely affect the market price of shares of our Class A common stock.

The tokenization of our Class A common stock may introduce risks and uncertainties that adversely affect the market for, and the trading price of, our Class A common stock, among other potential consequences.

Since September 2025, we enable Tokenized GLXY, a natively tokenized version of our Class A common stock. While Tokenized GLXY provides an additional mechanism for investors to hold and transfer shares in the Company, which may improve settlement efficiency and increase accessibility, it may also introduce new risks and uncertainties that could adversely affect the market for, and the trading price of, both Tokenized GLXY and Traditional GLXY.

Although we have not yet enabled trading of Tokenized GLXY on automated market maker decentralized exchanges, we may do so in the future, and we understand that decentralized mechanisms have emerged that facilitate on-chain bilateral trading between “Allowlisted” wallets. The market for tokenized securities is nascent, and there can be no assurance that a liquid or orderly market for Tokenized GLXY will develop or be sustained. Blockchain-based mechanisms, like decentralized exchanges, may have significantly less liquidity, volume, transparency or regulatory oversight compared to national securities exchanges, such as Nasdaq. This could fragment liquidity across platforms, impair price discovery, widen bid-ask spreads, and lead to prolonged price discrepancies between Tokenized and Traditional GLXY—especially where arbitrage is limited by operational or regulatory constraints.

On May 20, 2025, we entered into a Digital Transfer Agency Agreement with Superstate Services LLC as our digital asset transfer agent, pursuant to which it has agreed to create and maintain an “Allowlist” of wallet addresses of individuals and entities who have completed onboarding requirements and are permitted to hold, transfer and facilitate transfers of Tokenized GLXY. As a result, access to Tokenized GLXY is restricted to holders who meet the onboarding requirements of our digital transfer agent, potentially limiting investor participation and market depth, and resulting in greater price volatility.

Furthermore, market intermediaries may face unclear or evolving obligations when interacting with tokenized securities such as Tokenized GLXY, and the application of the U.S. federal securities laws and other regulations to the transfer of tokenized securities remains uncertain. This may prevent or discourage market intermediaries from holding, transacting, or facilitating transactions in Tokenized GLXY, further limiting liquidity. Reduced liquidity in Tokenized GLXY, whether due to general investor unfamiliarity, uncertain demand, operational friction, inefficient linkages between the markets for Tokenized GLXY and Traditional GLXY or otherwise, could result in lower trading prices for Tokenized GLXY, and such negative price signaling from the market for Tokenized GLXY could adversely impact the trading price of Traditional GLXY. In addition, if regulatory authorities determine that the platforms, mechanisms or participants involved in the secondary trading of Tokenized GLXY do not comply with applicable law, we or such intermediaries could face enforcement actions or fines, or be required to unwind or restructure aspects of the project. These risks could lead to diminished investor confidence, reduced participation in transactions of Tokenized GLXY, and corresponding negative effects on the trading price, volatility and/or liquidity of Traditional GLXY.

Tokenized GLXY is also subject to the broader risks associated with digital assets, including cybersecurity, technological failures, and operational risks, which could affect our reputation, financial condition, and operating results. See “—Risks Related to Cryptocurrencies and Digital Assets.”

Risks Related to Financial Reporting and Accounting

The nature of our business requires the application of complex financial accounting rules, and there is limited guidance from accounting standard setting bodies. If financial accounting standards undergo significant changes, our operating results could be adversely affected.

The accounting rules and regulations that we must comply with are complex and subject to interpretation by the Financial Accounting Standards Board (the “FASB”) and the SEC, and recent actions and public comments from the SEC have focused on the integrity of financial reporting and internal controls. In addition, many companies’ accounting policies are being subjected to heightened scrutiny by regulators and the public. Further, there have been limited precedents for the financial accounting of digital assets and related valuation and revenue recognition, and while the SEC has issued certain staff interpretations regarding the accounting of certain digital asset transactions, there remains significant uncertainty on how companies can account for digital assets transactions, digital assets, and related revenue. For example in December 2023, FASB adopted an accounting standards update which requires certain digital assets to be reported at fair value; however, this update excludes a material portion of digital assets with which we transact. Uncertainties in or changes to regulatory or financial accounting standards could result in the need to change our accounting methods and/or recast our financial statements and could impair our ability to provide timely and accurate financial information, which could adversely affect our financial statements, result in a loss of investor confidence, and more generally impact our business, operating results, and financial condition.

Our historical financial statements do not reflect the full extent of the potential variability in earnings that we may experience in the future relating to digital asset holdings.

The prices of digital assets have historically been subject to dramatic price fluctuations and are highly volatile. While we adopted ASU 2023-08 in fiscal year 2023, which requires us to measure a significant portion of our digital assets at fair value, we still have a material amount of digital assets that are measured at the lower of cost or impaired value basis. We determine the fair value of the majority of our digital assets based on quoted (unadjusted) prices on the active digital asset trading platform that we have determined is our principal market for such digital asset. We perform an analysis each quarter to identify whether events or changes in circumstances, principally decreases in the quoted (unadjusted) prices on the active digital asset trading platform, indicate that it is more likely than not that certain of our digital assets are impaired. In determining if an impairment has occurred, we consider the lowest price of one such digital asset quoted on the active digital asset trading platform at any time since acquiring the specific digital asset held. If the carrying value of any such digital asset exceeds that lowest price at any time during the quarter, an impairment loss is deemed to have occurred with respect to that digital asset in the amount equal to the difference between its carrying value and such lowest price, and subsequent increases in the price of such digital asset will not affect the carrying value of our holdings of such digital asset. Such increases in the price of digital assets are not recorded until realized upon sale. In determining the gross profit to be

recognized upon sale, we calculate the difference between the sale price and carrying value of the specific digital asset sold immediately prior to sale.

As a result, any decrease in the fair value of certain digital assets below our carrying value for such assets at any time since their acquisition requires us to incur an impairment charge, and such charge could be material to our financial results for the applicable reporting period, which may create significant volatility in our reported earnings and decrease the carrying value of our digital assets, which in turn could have a material adverse effect on the market price of our Class A common stock.

We may sell or purchase additional digital assets in future periods and correspondingly decrease or increase our overall holdings of digital assets, and the proportion of our total assets represented by digital asset holdings may increase in the future. As a result, volatility in our earnings in future periods may be significantly more than what we experienced in prior periods.

We are exposed to losses due to lack of perfect information. Valuation involves significant risks and uncertainties, including the fact that methodologies involve subjective judgments.

As a trader in digital assets, we will trade in a variety of assets with a number of different counterparties on both an anonymous and disclosed basis. We may at times trade with others who have information that is more accurate or complete than ours, and as a result we may accumulate unfavorable positions at unfavorable prices preceding large price movements in a given instrument. If the frequency or magnitude of these events increases, our losses would likely increase correspondingly, which could have a material and adverse effect on the effectiveness of our investment or trading strategies and on any investment in us.

Digital assets, including but not limited to, bitcoin, can fluctuate dramatically in value and can lose a material portion of their value in a short period of time. There can be no assurance as to the value of our portfolio as of any date in the future. Any future valuation could diverge from previous estimates as a result of market fluctuations or additional third-party valuations of underlying assets using different and potentially inconsistent methods, financial reporting requirements under GAAP or other factors.

For the purposes of GAAP-compliant financial reporting, our assets and liabilities are valued in accordance with GAAP. Accordingly, we are required to follow a specific framework for measuring the fair value of our assets and liabilities and, in our audited financial statements, to provide certain disclosures regarding the use of fair value measurements.

The fair value measurement accounting guidance establishes a hierarchical disclosure framework that ranks the observability of market inputs used in measuring assets and liabilities at fair value. The observability of inputs depends on a number of factors, including the type of asset or liability, the characteristics specific to the asset or liability and the state of the marketplace, including the existence and transparency of transactions between market participants. Assets and liabilities with readily quoted prices, or for which fair value can be measured from quoted prices in active markets, generally will have a high degree of market price observability and less judgment applied in determining fair value.

We hold certain assets, such as privately placed equity, debt, warrants or options, digital asset receivables and certain restricted digital assets, that will not have readily assessable market values. In such instances, we will determine the fair value of such assets based on various factors. In connection with assets for which no external pricing information is available, we may rely on internal pricing models or third-party valuation agents. Such valuations may vary from similar valuations performed by other independent third parties for similar types of assets. The valuation of illiquid assets is inherently subjective and subject to increased risk that the information used to value the asset or to create the price models may be inaccurate or subject to other error. Inaccurate valuations may, among other things, hinder us from effectively managing our investment portfolios and risks.

The value of our portfolio may also be affected by changes in accounting standards, policies or practices. From time to time, we will be required to adopt new or revised accounting standards or guidance. It is possible that future accounting standards that we are required to adopt could materially change the valuation of our assets and liabilities.

Because of a wide variety of market factors and the nature of assets held by us, there is no guarantee that the value determined by us or a third-party valuation agent will represent the value that will be realized by us on the eventual disposition of the asset or that would, in fact, be realized upon an immediate disposition of the asset. Moreover, the valuations to be performed by us or a third-party valuation agent are inherently different from the valuation of our assets that would be performed if we were forced to liquidate all or a significant portion of our assets, which liquidation valuation could be materially lower.

Changes in, or the development of guidance relating to, accounting standards governing the preparation of our financial statements and future events could have a material impact on our reported financial condition, results of operations, cash flows and other financial data.

Preparation of financial statements in conformity with GAAP requires management to make estimates based upon assumptions about future economic and market conditions which affect reported amounts and related disclosures in our financial statements. If subsequent events occur that are materially different than the assumptions and estimates we used, our reported financial condition, results of operation and cash flows may be materially negatively impacted.

We supplement our GAAP financial statements from time to time with certain non-GAAP measures. However, such non-GAAP measures are not a replacement for our GAAP results, and are subject to important additional risks and uncertainties. The accounting for, and audit standards relating to, digital assets remain subject to further guidance. To the extent that such guidance imposes obligations on audit firms that they are not able to meet with respect to the review of digital assets, we could have difficulty in obtaining an audit opinion, filing audited financial statements in a timely manner or obtaining an unqualified opinion.

Further, from time to time, regulators change the financial accounting and reporting standards governing the preparation of our financial statements or the interpretation of those standards. These changes are difficult to predict and can materially impact how we record and report our financial condition, results of operations, cash flows and other financial data. In some cases, we may be required to apply a new or revised standard retroactively or to apply an existing standard differently, also retroactively, in each case potentially resulting in a change to prior period financial statements and related disclosures, which could have a material adverse effect on the market price of our Class A common stock.

Our internal control over financial reporting may not be effective and our independent registered public accounting firm may not be able to certify as to its effectiveness, which could have a significant and adverse effect on our business and reputation.

We are not currently required to publish a formal assessment of the effectiveness of our internal control over financial reporting under the SEC rules that implement Section 404 of the Sarbanes-Oxley Act, and will not be required to do so until we file our second annual report on Form 10-K, and our independent auditors will be required to issue an attestation report on the effectiveness of our internal control over financial reporting when we file our second report on Form 10-K. We may incur significant expenses and devote substantial management effort in the process of ensuring compliance with the attestation requirements of the Sarbanes-Oxley Act.

When evaluating our internal control over financial reporting, we may identify material weaknesses that we may not be able to remediate in time to meet the applicable deadline imposed upon us for compliance with the requirements of Section 404 of the Sarbanes-Oxley Act. In addition, if we fail to achieve and maintain the adequacy of our internal controls, as such standards are modified, supplemented or amended from time to time, we may not be able to ensure that we can conclude on an ongoing basis that we have effective internal control over financial reporting in accordance with Section 404 of the Sarbanes-Oxley Act. Further, any failure to develop or maintain effective controls or any difficulties encountered in their implementation or improvement could harm our business or cause us to fail to meet our reporting obligations on a timely basis and may result in material misstatements in our consolidated financial statements. We cannot be certain as to the timing of completion of our evaluation, testing and any remediation actions or the impact of the same on our operations. If we are not able to implement the requirements of Section 404 of the Sarbanes-Oxley Act in a timely manner or with adequate compliance, our independent auditors may issue an adverse opinion due to ineffective internal control over financial reporting, and we may be subject to sanctions or investigation by regulatory authorities, such as the SEC. As a result, there could be a negative reaction in the financial markets due to a loss of confidence in the reliability of our financial statements. In addition, we may be required to incur costs in improving our internal controls system and the hiring of additional personnel. Any such action could negatively affect our results of operations and cash flows.

Risks Related to Being a U.S. Public Company

We face challenges, increased costs and administrative responsibilities as a U.S. public company, and management devotes substantial time to related compliance initiatives.

We incur significant levels of legal, accounting and other expenses in respect of our status as a public company in Canada and in the United States. We are required to comply with, and incur the associated costs of compliance with, the Sarbanes-Oxley Act and the Dodd-Frank Wall Street Reform and Consumer Protection Act, as well as rules and regulations implemented by the SEC and Nasdaq. The expenses incurred by U.S. public companies generally for reporting and corporate governance purposes have been increasing. In addition, we remain listed on the TSX, and as such, continue

to be subject to Canadian Securities Laws and the listing requirements of the TSX, which impose significant requirements relating to disclosure controls and procedures and internal control over financial reporting. Compliance with these rules and regulations has increased our legal and financial compliance costs, has required us to hire additional personnel, and has made some activities more time consuming and costly. Our management has devoted, and will continue to devote, a substantial amount of time to ensure that we comply with all of these requirements, diverting the attention of management away from revenue-producing activities. These laws and regulations also could make it more difficult or costly for us to obtain certain types of insurance, including director and officer liability insurance, and we may be forced to accept reduced policy limits and coverage or incur substantially higher costs to obtain the same or similar coverage. These laws and regulations could also make it more difficult for us to attract and retain qualified persons to serve on our board of directors, our board committees or as our executive officers.

As a result of our increased compliance obligations as a U.S. public company, we have needed, and will continue needing, to:

- institute a more comprehensive compliance framework;
- update, evaluate and maintain a system of internal controls over financial reporting in compliance with the requirements of Section 404 of Sarbanes-Oxley and the related rules and regulations of the SEC, as and when such requirements, rules and regulations become applicable to us;
- prepare and distribute periodic public reports in compliance with our obligations under the U.S. federal securities laws;
- revise our existing internal policies, such as those relating to disclosure controls and procedures and insider trading;
- comply with SEC rules and guidelines requiring registrants to provide their financial statements in interactive data format using eXtensible Business Reporting Language;
- involve and retain to a greater degree outside counsel and accountants in the above activities; and
- enhance our investor relations function.

In addition, as a company in the digital assets industry, we may experience higher-than-anticipated operating expenses as well as higher independent auditor and consulting fees and may need to hire additional qualified personnel to continue to satisfy these public-company requirements. We are required to expend considerable time and resources with respect to our compliance with public company regulations, and we will continue to incur significant expenses. If we are unable to satisfy our obligations as a public company, we could be subject to de-listing of our Class A common stock on Nasdaq and/or the TSX, fines, sanctions or other detrimental regulatory actions or civil litigation.

Our management team has limited experience managing a U.S. public company and some members of senior management are new to our company and our industry. Our business could be adversely affected if our management team is not successfully integrated or does not execute our business plan and developmental strategies.

Our management team has limited experience managing a U.S. public company, interacting with U.S. public company investors, and complying with the increasingly complex laws pertaining to U.S. public companies. Our management team may not successfully or efficiently manage our transition to being a U.S. public company subject to significant regulatory oversight and reporting obligations under the federal securities laws and the continuous scrutiny of securities analysts and investors. In addition to Nasdaq, we are listed on the TSX, and we expect to continue to be subject to certain Canadian Securities Laws requiring us to file reports and other information on SEDAR for the foreseeable future, and are therefore subject to multiple, additional, and at times, competing, governance and reporting obligations. These obligations and constituents require significant attention from our senior management and could divert their attention away from the day-to-day management of our business, which could adversely affect our business, operating results, and financial condition.

Further, some members of our management team have recently joined our company and will need to be successfully integrated in order to effectively execute our business plan and developmental strategies. Our management team therefore has limited historical experience with our clients, our business and our industry and the process of transitioning our new members into our business is complex and time consuming. This may impact our ability to collectively respond to issues in a quick and efficient manner. If our management team is unable to develop a business strategy that can be executed in a successful manner, it could materially adversely impact business and our revenue.

Certain statutory provisions generally afforded to stockholders of a Delaware corporation are not applicable to us.

Certain statutory provisions generally afforded to stockholders of a Delaware corporation are not applicable to us. For example, our amended and restated certificate of incorporation, or our certificate of incorporation, contains a provision renouncing our interest and expectancy in certain corporate opportunities, such that any members of the board of directors who are not also employees of the Company, GDH LP or any of their respective subsidiaries do not have any duty to refrain from engaging in the same or similar business activities or lines of business as us. Our certificate of incorporation provides that, to the fullest extent permitted by applicable law, we renounce our right to certain business opportunities, and that any such member of our board of directors has no duty to communicate or offer such business opportunity to us and is not liable to us or any of our stockholders for breach of any fiduciary or other duty under statutory or common law, as a director, officer or controlling stockholder, or otherwise, by reason of the fact that any such individual pursues or acquires such business opportunity, directs such business opportunity to another person or fails to present such business opportunity, or information regarding such business opportunity, to us. Our organizational documents waive any corporate opportunity doctrine and similar claims against any non-employee directors (other than to the extent any corporate opportunity is offered to a non-employee director in his or her capacity as a director).

In addition, pursuant to our certificate of incorporation, we have opted out of Section 203 of the DGCL with respect to certain existing shareholders (including our Founder), which prohibits a publicly held Delaware corporation from engaging in a business combination transaction with an “interested stockholder” (as defined in Section 203 of the DGCL) for a period of three years after the interested stockholder became such unless such transaction fits within an applicable exemption, such as board approval of the business combination or the transaction in which resulted in such stockholder becoming an interested stockholder.

Further, pursuant to the director nomination agreement with GGI (the “Director Nomination Agreement”), GGI has the right to nominate one director to our board of directors for so long as GGI continues to beneficially own at least 25% of our Class A common stock. This right will be deemed to have been exercised for so long as our Founder remains on our board of directors. As the sole owner of GGI, our Founder is able to designate himself or another nominee for election to our board of directors; provided that the right of any director designated by our Founder to serve on a committee is subject to applicable laws and Nasdaq independence rules.

Provisions in our organizational documents and Delaware law, and certain rules imposed by regulatory authorities, might discourage, delay or prevent a change of control of our company or changes in our management and, therefore, depress the market price of our Class A common stock.

Our organizational documents contain provisions that could depress the market price of our common stock by acting to discourage, delay or prevent a change in control of our company or changes in our management that the stockholders of our company may deem advantageous. These provisions include:

- the ability of our board of directors to amend our amended and restated bylaws which may allow our board of directors to take additional actions to prevent an unsolicited takeover and inhibit the ability of an acquirer to amend our bylaws to facilitate an unsolicited takeover attempt;
- that, subject to the rights granted pursuant to the Director Nomination Agreement, vacancies and newly created directorships may be filled only by the remaining directors;
- the ability of our board of directors to prevent the transfer of capital stock, or the exercise of rights with respect to our common stock, if the effect of such transfer or exercise of rights would result in a stockholder holding more than 9.9% of the total voting power of our common stock on a fully diluted basis;
- the limitation of the liability of, and the indemnification of, Galaxy’s directors and officers;
- controlling the procedures for the conduct and scheduling of board of directors and stockholder meetings;
- advance notice procedures with which stockholders must comply to nominate candidates to the our board of directors or to propose matters to be acted upon at a stockholders’ meeting, which could preclude stockholders from bringing matters before annual or extraordinary general meetings of stockholders and delay changes in our board of directors and also may discourage or deter a potential acquirer from conducting a solicitation of proxies to elect the acquirer’s own slate of directors or otherwise attempting to obtain control of us; and
- require super majority approvals to remove the protective provisions in our organizational documents listed above or to amend our bylaws.

Such provisions could impede any merger, consolidation, takeover or other business combination involving our company or any of our subsidiaries or discourage a potential acquirer from making a tender offer or otherwise attempting to obtain control of us or our subsidiaries.

In addition, a third party attempting to acquire us or a substantial position in our common stock may be delayed or ultimately prevented from doing so by change in ownership or control regulations to which our regulated broker-dealer subsidiary is subject. FINRA Rule 1017 generally provides that FINRA approval must be obtained in connection with any transaction resulting in a single person or entity owning, directly or indirectly, 25% or more of a member firm's equity and would include a change of control of a parent company. The foregoing and any other applicable regulations relating to changes in control of us or our regulated subsidiaries could further have the effect of delaying or deterring a change in control of us.

Our certificate of incorporation designates a state or federal court located within the State of Delaware as the exclusive forum for substantially all disputes between the Company and its stockholders, and the federal district courts of the United States as the exclusive forum for the resolution of any complaint asserting a cause of action under the Securities Act or the Exchange Act, which could limit the ability of a holder of Class A common stock to choose the judicial forum for certain lawsuits against us or our directors, officers, or employees.

Our certificate of incorporation provides that, unless we consent in writing to the selection of an alternative forum, to the fullest extent permitted by law, the sole and exclusive forum for (i) any derivative action or proceeding brought on our behalf, (ii) any action or proceeding asserting a claim of breach of a fiduciary duty owed by any of our directors, officers or other employees to us or our stockholders, (iii) any action or proceeding arising pursuant to, or seeking to enforce any right, obligation or remedy under, any provision of the DGCL, or our organizational documents, (iv) any action or proceeding seeking to interpret, apply, enforce or determine the validity of our organizational documents, (v) any action or proceeding asserting a claim that is governed by the internal affairs doctrine or (vi) any action or proceeding as to which the DGCL confers jurisdiction on the Court of Chancery of the State of Delaware shall be the Court of Chancery of the State of Delaware (or, if the Court of Chancery does not have subject matter jurisdiction, another state court sitting in the State of Delaware (or, if no state court located within the State of Delaware has jurisdiction, the federal district court for the District of Delaware)), in all cases subject to the court having jurisdiction over indispensable parties named as defendants. Additionally, our certificate of incorporation states that the foregoing provision does not apply to claims arising under the Securities Act, the Exchange Act or other federal securities laws for which there is exclusive federal or concurrent federal and state jurisdiction. Our certificate of incorporation provides that, unless we consent in writing to the selection of an alternative forum, the federal district courts of the United States is the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act, the Exchange Act or other U.S. federal securities laws for which there is exclusive federal or concurrent federal and state jurisdiction.

Any person or entity purchasing or otherwise acquiring or holding any interest in any of our securities shall be deemed to have notice of and consented to these provisions. These exclusive forum provisions may limit a stockholder's ability to bring a claim in a judicial forum of its choosing for disputes with us or our directors, officers, or other employees, which may discourage lawsuits against us and our directors, officers, and other employees. The enforceability of similar choice of forum provisions in other companies' charter documents has been challenged in legal proceedings, and it is possible that a court could find these types of provisions to be inapplicable or unenforceable. For example, in December 2018, the Court of Chancery of the State of Delaware determined that a provision stating that federal district courts of the United States are the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act is not enforceable. Although this decision was reversed by the Delaware Supreme Court in March 2020, courts in other states may still find these provisions to be inapplicable or unenforceable. If a court were to find the exclusive forum provisions in our certificate of incorporation to be inapplicable or unenforceable in an action, we may incur additional costs associated with resolving the dispute in other jurisdictions, which could adversely affect our results of operations.

Our disclosure controls and procedures may not prevent or detect all errors or acts of fraud.

We are subject to the periodic reporting requirements of the Exchange Act. We designed our disclosure controls and procedures to provide reasonable assurance that information we must disclose in reports we file or submit under the Exchange Act is accumulated and communicated to management, and recorded, processed, summarized and reported within the time periods specified in the rules and forms of the SEC. We believe that any disclosure controls and procedures, no matter how well conceived and operated, can provide only reasonable, not absolute, assurance that the objectives of the control system are met. These inherent limitations include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of a simple error or mistake. Additionally, controls can be circumvented by the individual acts of some persons, by collusion of two or more people or by an unauthorized override of the controls.

Accordingly, because of the inherent limitations in our control system, misstatements due to error or fraud may occur and not be detected.

General Risk Factors

Pandemics or other market events with impacts on the global economy may materially and adversely affect us.

We face risks related to health epidemics and other outbreaks of communicable diseases, which could significantly disrupt our operations and may materially and adversely affect our business and financial conditions. For example, in December 2019, a novel strain of the coronavirus COVID-19 emerged as a global pandemic. As a result, during the first quarter of 2020, global financial markets experienced a period of sharp decline and volatility due in large part to the real and perceived economic impact of the COVID-19 pandemic. The public health impact of the coronavirus, as well as the steps taken by governments and businesses around the world to combat its spread, impacted the global economy in a variety of ways, including causing many businesses to close and significant supply chain disruptions.

During the global financial crisis of 2007 to 2008, various sectors of the global financial markets experienced an extended period of adverse conditions featuring market uncertainty, reduced liquidity, greater volatility, general widening of credit spreads and a lack of price transparency. In addition, governments from time to time during times of crisis intervene, directly and by regulation in ways that are unpredictable. Such intervention is often intended to directly influence prices and may, together with other factors, cause all of such markets to move rapidly in the same direction. To the extent that similar marketplace events were to occur in the future, either as a result of a pandemic or otherwise, these events may have an adverse impact on our investments or our business operations.

We intend to continue to execute on our strategic plans and operational initiatives; however, future pandemics or market disruptions, including due to global economic slowdowns, domestic and foreign regulatory uncertainty, changes in trade policies, including the imposition of tariffs, trade controls and other trade barriers, actual or perceived global banking and finance related issues, increased risk of inflation, potential uncertainty with respect to the federal debt ceiling and budget and potential or actual government shutdowns, related thereto, interest rate volatility, and potential global recession, may result in delays or modifications to these plans and initiatives. Business activities could also be materially adversely impacted as the fundraising for asset management products and advisory transactions may be delayed during such situations and the delivery of AI/HPC data center equipment may be disrupted due to supply chain interruptions. In particular, a pandemic could materially and adversely impact our business including without limitation, employee health, workforce productivity, increased expenses and other factors that will depend on future developments beyond our control, which may have a material and adverse effect on our business, financial condition, results of operations and cash flows. Such adverse effect could be rapid and unexpected.

The ultimate extent of the impact of any epidemic, pandemic, or other health crisis, or any other market disruption on our business will depend on multiple factors that are highly uncertain and cannot be predicted, including its severity, location and duration, and actions taken to contain or prevent further its spread. Additionally, pandemics could increase the magnitude of many of the other risks described in this Quarterly Report on Form 10-Q, and may have other material adverse effects on our operations that we are not currently able to predict. If our business and the markets in which we operate experience a prolonged occurrence of adverse public health conditions it could materially adversely affect our business, financial condition, and results of operations.

We may be adversely affected by natural disasters and other catastrophic events, and by man-made problems such as terrorism, that could disrupt our business operations, and our business continuity and disaster recovery plans may not adequately protect us from a serious disaster.

Natural disasters or other catastrophic events may also cause damage or disruption to our operations, international commerce, and the global economy, and could have an adverse effect on our business, operating results, and financial condition. Our business operations are subject to interruption by natural disasters, severe weather, fire, power shortages, and other events beyond our control. Further, acts of terrorism, labor activism or unrest, and other geo-political unrest could cause disruptions in our business or the businesses of our partners or the economy as a whole. In the event of a natural disaster or other severe weather, including a major earthquake, blizzard, or hurricane, or a catastrophic event such as a fire, power loss, or telecommunications failure, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in development of our platform, lengthy interruptions in service, breaches of data security, and loss of critical data, all of which could have an adverse effect on our future operating results. Natural disasters and other severe weather may occur with increased frequency and severity in the future as a result of climate change. We do not maintain insurance sufficient to compensate us for the potentially significant losses that could result from disruptions to our services. Additionally, all the aforementioned risks may be further increased if we do not implement a

disaster recovery plan or our partners' disaster recovery plans prove to be inadequate. To the extent natural disasters or other catastrophic events concurrently impact data centers or mining equipment that we rely on, our operations may be delayed and we may suffer losses, both financial and otherwise.

Item 2. Unregistered Sales of Equity Securities and Use of Proceeds

None.

Item 3. Defaults Upon Senior Securities

None.

Item 4. Mine Safety Disclosures

Not applicable.

Item 5. Other Information

Director and Officer Trading Arrangements

During the three months ended September 30, 2025, none of our directors or officers (as defined in Rule 16a-1(f) under the Exchange Act) adopted, modified or terminated a "Rule 10b5-1 trading arrangement" or "non-Rule 10b5-1 trading arrangement," as each term is defined in Item 408(a) of Regulation S-K.