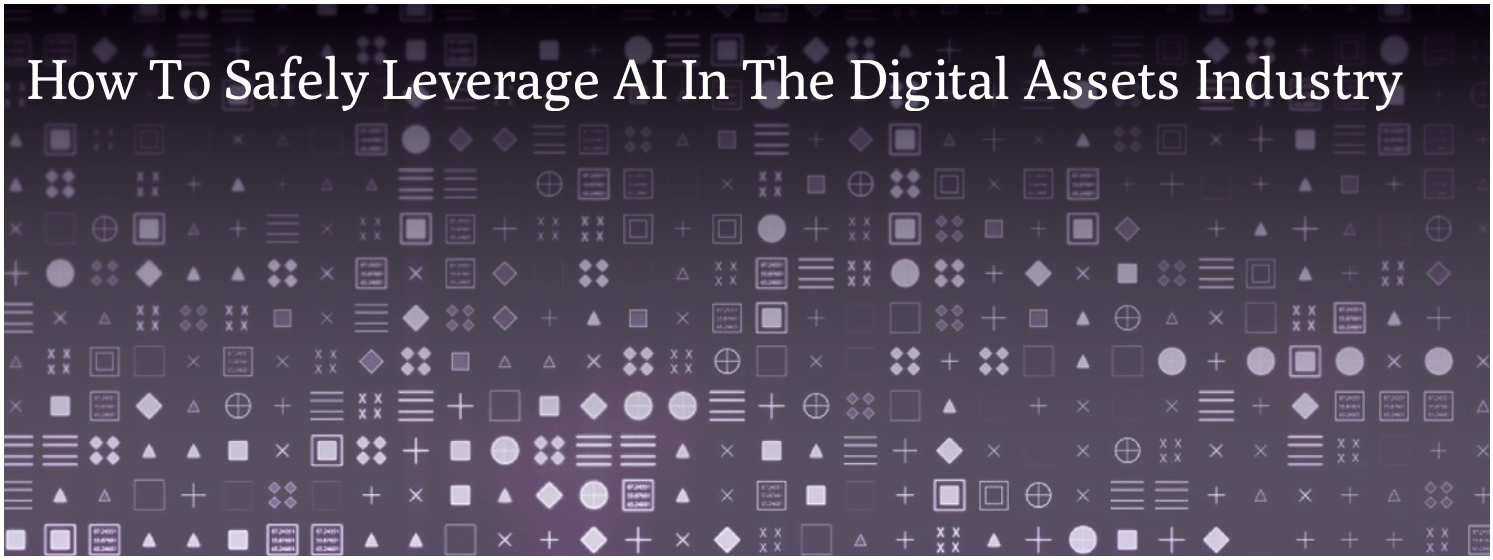
WINSTON & STRAWN LLP

ARTICLE

How To Safely Leverage AI In The Digital Assets Industry



NOVEMBER 21, 2024

This article was originally published in Law360. Reprinted with permission. Any opinions in this article are not those of Winston & Strawn or its clients. The opinions in this article are the authors' opinions only.

Artificial intelligence has been integrated into various industries, but it is uniquely destined to form a close relationship with the digital assets space.

The decentralized and data-driven nature of digital assets offers fertile ground for AI to analyze complex patterns, predict market trends and streamline processes, making the combination of AI and digital assets particularly synergistic.

Digital asset businesses have begun to leverage AI to reduce costs, meet market demands, increase efficiency, facilitate scalability and more effectively manage and control risk.

Major digital-asset-focused companies have revealed ambitious plans to integrate AI into cryptocurrency markets, including BlackRock's AI-powered digital dollar project announced in October, which is expected to drive the value of cryptocurrencies like Bitcoin and Ethereum.[1]

This article discusses advantages offered to digital asset businesses by integrating AI, and certain related legal and regulatory risks that have been identified by government agencies, particularly regarding privacy, cybersecurity and bias. It also attempts to provide practical considerations for digital-asset-related businesses that may use AI and associated technologies.

USES AND BENEFITS OF AI AND DIGITAL ASSETS

In the digital assets space, as in others, AI can play a key role in fraud detection, risk assessment, algorithmic trading and customer service. It can also assist in market analysis and enable proactive trading.

AI-driven chatbots and virtual assistants may provide continuous customer support, handling inquiries in real time, and enhancing customer satisfaction through sentiment analysis. AI may help to mitigate operational risks by analyzing user behavior and detecting anomalies that might go unnoticed by humans, providing early warnings against potential fraud or security breaches.

Meanwhile, automated trading benefits from AI's ability to monitor markets 24/7, execute trades swiftly and offer personalized trading strategies, giving its users a competitive edge.

Digital assets are primarily built on blockchain technologies, which generate and store vast amounts of data — from market transactions, trading volumes, price movements and user interactions — by recording transaction information in a public, transparent, decentralized, immutable ledger.

Unlike traditional financial systems, digital assets operating on blockchains facilitate peer-to-peer transactions without relying on traditional third parties and validate transactions in a decentralized manner. AI offers a powerful tool for extracting actionable insights and trends from large volumes of data.

LEGAL AND REGULATORY RISKS OF AI USAGE

The confluence of new generative AI tools and increased popularity for digital assets can amplify risks of each technology and raise important regulatory questions for policymakers. Those policymakers, however, are challenged to create comprehensive laws and regulations for the digital asset space, let alone any that contemplate the intersection of AI and digital assets.

While comprehensive regulation remains elusive, regulators have issued several pronouncements specific to the intersection of digital assets and AI that should be considered by businesses considering these technologies, as discussed below.

Risks in Customer Support

The use of chatbots and self-service technologies fueled by AI to provide customer service has become quite widespread.

Federal agencies do not view chatbots as inherently problematic; many government agencies have adopted these tools to meet their own service demands. The concern with customer support tools that utilize generative AI is the risk of misrepresentations and privacy violations.

The Federal Trade Commission has previously highlighted the privacy concerns associated with AI use in chatbots. The FTC typically enforces privacy rights under the Federal Trade Commission Act, Section 45, prohibiting unfair and deceptive practices.[2]

In a June "Business Blog" update, the FTC outlined several ways in which a company's use of AI chatbots could be considered unfair and deceptive.[3]

First, firms may not misrepresent what the AI chatbot is, or what the bot can do. Thus, it could be considered deceptive if a business fails to inform its customers that its customer service tools are powered by AI.

Further, the FTC has suggested that these tools could be considered deceptive if they "lack scientific support" or "apply only to certain types of users or under certain conditions."[4]

This is particularly relevant as generative AI is known to have so-called hallucination problems, which occur when large language models perceive patterns or objects that don't exist and generate inaccurate, nonsensical or irrelevant information. This can lead to several risks, such as generating information that sounds plausible but is based on fabricated or erroneous data, making its outputs unreliable.

Further, if AI's accuracy or functionality depends on specific data inputs or certain types of users, it may inadvertently provide misleading information to others.

From a privacy perspective, digital asset businesses should not use AI chatbots to collect data that exceeds the scope of the consumer's consent.

The FTC has suggested that only informing consumers of changes in their data practices — for example, sharing consumers' data with third parties or using that data for AI training — through a retroactive amendment to its terms of service or privacy policy adopting permissive data practices may be considered an unfair or deceptive practice.[5]

AI chatbots, without strict data governance controls, could lead to data misuse, breaches of privacy or unfair profiling. However, AI can also mitigate this risk by being designed with privacy features, such as automatically limiting data collection to only what is necessary, implementing strong consent-management protocols, and ensuring transparency in how consumer data is used.

While generative AI tools rely on training data — potentially based on real customer data and interactions — to learn or enhance their accuracy, this practice may increase the risk of exposure of sensitive customer financial and private information stored by digital asset businesses in ways that may violate FTC privacy standards and company legal obligations.

The FTC has outlined strict penalties for noncompliance with its privacy standards, including significant monetary penalties [6] and mandatory refunds to consumers. [7]

Risks in Fraud Detection

While AI tools can be utilized to help detect fraud, a number of commentators have observed that they also have the potential to introduce bias and discrimination into the process of fraud detection. New uses of AI may inherit bias by using biased training data.

In a joint statement on "Enforcement Efforts Against Discriminations and Bias in Automated Systems," the Consumer Financial Protection Bureau, the U.S. Department of Justice, the U.S. Equal Employment Opportunity Commission and the FTC stressed the danger of discrimination in these outcomes when the datasets used "incorporate historical bias, or ... contain other types of errors." [8]

This can lead to fraud detection algorithms potentially correlating data with protected classes and disproportionately targeting specific groups with allegations of fraudulent behavior without justification.

Similarly, AI systems may act without any explanation or transparency on how the system produces its output or reaches certain decisions.

The joint statement also stated that:

Many automated systems are "black boxes" whose internal workings are not clear to most people and, in some cases, even the developer of the tool. This lack of transparency often makes it all the more difficult for developers, businesses, and individuals to know whether an automated system is fair. [9]

Digital asset businesses regulated by the U.S. Securities and Exchange Commission may face unique risks if integrating AI into their products.

SEC Chair Gary Gensler has been adamant about combatting so-called AI washing, or the purposeful mischaracterization of a company's AI capabilities to exaggerate the innovation or technological advancement of its products.

In the last year, the SEC has issued contentious new cybersecurity rules [10] and predictive data analytics proposals related to brokerages. [11] In July 2023, the SEC proposed a rule requiring broker-dealers to address conflicts of interest in the use of AI in trading to prevent potentially fraudulent activity. [12]

Risks in Automatic Trading Options

The perpetual availability of trading on digital asset markets contributes to their volatility and unpredictability. This makes trading bots, which use AI to automatically buy and sell digital assets, a potentially appealing option.

However, the SEC and the U.S. Commodity Futures Trading Commission have previously issued warnings to investors looking to invest in programs that "operate advisory and trading businesses related to digital assets," including, potentially, programs using AI. [13]

In January, the CFTC also released a customer advisory, titled "AI Won't Turn Trading Bots into Money Machines," which focused on protecting investors from trading platforms that claim AI-created algorithms can guarantee huge

returns.[14]

The SEC has also taken action against schemes promising profits from the trading activities of a purported crypto-asset trading bot.[15]

Additionally, in May, the DOJ indicted two brothers — Anton and James Peraire-Bueno — for using so-called crypto bots in a front-running scheme to obtain nearly $25 million in transactions on the Ethereum network.[16]

However, enforcement actions typically target bad actors and involve fraudulent conduct; thus, ambiguity remains on the liability of digital asset businesses using AI trading programs that turn out merely to be faulty.

AI trading has caught the interest of lawmakers, and features in several congressional bills.

In September 2023, the Algorithmic Accountability Act of 2023 was reintroduced to provide the FTC new authority to create protections for people targeted by AI-generating decisions affecting high-impact uses, including in financial services.[17]

Fundamentally, the act requires companies to conduct impact assessments of the decision processes of their AI systems, and creates a public database housed within the FTC, allowing consumers to access and review the decisions that have been automated by companies.[18]

Skeptics fear that many AI systems operate in opaque black boxes, without explanation or transparency as to the processes leading to their outputs. If an AI model lacks transparency, it would be difficult — if not impossible — to verify the accuracy of its results, thus creating opportunities for biased and inaccurate outputs that could, in turn, raise consumer protection concerns.

Explanations would be particularly important in automated digital asset trading, given the significant market fluctuations and perpetually open markets. Without transparency, it will be challenging to verify the efficacy and validity of AI trading model decisions, with mass-programmed decision-making having the potential to destabilize markets.

Further, while it may sound intuitive, in the age of buzzwords like “machine learning” and “deep learning,” digital asset businesses should make sure that the AI trading algorithms used are actually powered by AI.

In March 2024, the SEC prosecuted its first AI fraud case against two investment advisers, Delphia Inc. and Global Predictions Inc., for overstating the role of their “predictive algorithmic model[s]” for asset selection.[19]

These enforcement actions demonstrate that the SEC will not wait for an AI-specific rule to charge AI-related disclosure and other violations; it will effectively apply existing federal securities laws to hold parties accountable for making misrepresentations about the use of AI in their services or products.

CONCLUSION

While the use of AI by digital asset businesses can provide several key benefits, AI integration into these businesses also presents legal and regulatory risks that should be proactively addressed.

Digital asset businesses that use or plan to implement AI should assess their risk management frameworks to ensure that AI-related risks are effectively mitigated in compliance with applicable laws, regulations and guidance from regulatory bodies.

Achieving AI readiness involves establishing strong data governance and security practices, training employees on AI and data privacy requirements, and implementing transparency and interpretability mechanisms.

As AI systems evolve, businesses should also have robust regulatory change-management processes in place to monitor updates from regulators and adjust their controls as needed to meet evolving consumer protection standards and supervisory expectations.

Digital asset businesses should remain proactive by conducting thorough impact assessments of their AI tools, implementing rigorous data protection measures, and ensuring that AI-driven processes adhere to ethical guidelines.

They should also clearly disclose, perhaps in their terms of service agreements, how AI will affect user accounts, especially regarding automated decisions on transactions or risk profiling. Entities may opt to obtain explicit consent from users for specific AI functions, especially those that involve data processing, profiling or predictions.

While AI can streamline processes, human oversight remains crucial, especially for high-risk decisions. Digital asset companies should ensure that human reviewers can intervene when AI makes critical judgments, like transaction monitoring or fraud alerts.

Digital asset businesses may also regularly audit AI models for biases that could unfairly affect certain groups of users, such as during risk assessments or onboarding processes.

By striking a balance between innovation and compliance, digital asset businesses can harness the full potential of AI while safeguarding their companies against legal challenges and regulatory enforcement actions.

---

[1] Billy Bambrough, Digitizing the Dollar: BlackRock CEO Reveals His Radical Plan for AI-Powered Crypto That's Predicted to Blow Up the Price of Bitcoin and Ethereum, Forbes (Oct. 13, 2024), https://www.forbes.com/sites/digital-assets/2024/10/13/digitizing-the-dollar-blackrock-ceo-reveals-his-radical-plan-for-ai-powered-crypto-thats-predicted-to-blow-up-the-price-of-bitcoin-and-ethereum/.

[2] 15 U.S.C. § 45.

[3] Michael Atleson, Succor Borne Every Minute, FTC Business Guidance Blog (June 11, 2024), https://www.ftc.gov/business-guidance/blog/2024/06/succor-borne-every-minute (hereinafter "FTC June Blog Post").

[4] Michael Atleson, Keep your AI claims in check, FTC Business Guidance Blog (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check.

[5] AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive, Federal Trade Commission (Feb. 13, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive.

[6] See Federal Trade Commission, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads, (May 25, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

[7] See Federal Trade Commission, FTC Sends Refunds to Ring Customers Stemming from 2023 Settlement over Charges the Company Failed to Block Employees and Hackers from Accessing Consumer Videos, (Apr. 23, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-sends-refunds-ring-customers-stemming-2023-settlement-over-charges-company-failed-block.

[8] CFPB et al., Joint Statement on Enforcement Efforts Against Discriminations and Bias in Automated Systems (Apr. 25, 2023) at 3, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

[9] Id.

[10] Securities and Exchange Commission, Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Release No. 34-97142, 88 Fed. Reg. 20212 (2023), https://www.sec.gov/files/rules/proposed/2023/34-97142.pdf.

[11] Securities and Exchange Commission, Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, Release No. 34-97990, 88 Fed. Reg. 23625 (2023), https://www.sec.gov/files/rules/proposed/2023/34-97990.pdf.

[12] Id.

[13] Commodity Futures Trading Commission, Investor Alert: Watch Out for Fraudulent Digital Asset and "Crypto" Trading Websites, (2019), https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/watch_out_for_digital_fraud.html.

[14] AI Won't Turn Trading Bots into Money Machines, Commodity Futures Trading Commission (2024), https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/AITradingBots.html.

[15] See SEC v. Braga, No. 2022-201, Complaint, U.S. Securities and Exchange Commission, https://www.sec.gov/files/litigation/complaints/2022/comp-pr2002-201-braga.pdf; see also SEC v. Tetreault, No. 2022-201, Complaint, U.S. Securities and Exchange Commission, https://www.sec.gov/files/litigation/complaints/2022/comp-pr2002-201-tetreault.pdf.

[16] See United States v. Anton Peraire-Bueno, Indictment, U.S. District Court Southern District of New York (2024), https://www.justice.gov/opa/media/1351996/dl; see also Press Release, U.S. Dep't of Justice, Two Brothers Arrested for Attacking Ethereum Blockchain and Stealing $25M in Cryptocurrency (May 2024), https://www.justice.gov/opa/pr/two-brothers-arrested-attacking-ethereum-blockchain-and-stealing-25m-cryptocurrency.

[17] S. 2892, 118th Cong. (2023 — 2024).

[18] Id.

[19] Securities and Exchange Commission, SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence (March 18, 2024), https://www.sec.gov/newsroom/press-releases/2024-36.

10+ Min Read

Related Capabilities

Artificial Intelligence (AI) | Cryptocurrencies, Digital Assets & Blockchain Technology

Related Professionals

Carl Fornaris

Daniel T. Stabile

Kimberly A. Prior

Janelle E. Rodriguez-Mena