14 DIGITAL ASSET RISKS TO REMEMBER

There is no such thing as a risk-free trade or investment. Generally, bigger expected returns come with a greater risk of loss. The more you understand the risks of your investment, the more effectively you can minimize their potential effects. Here are some common risks associated with digital assets:

Operational risks

1. **Unsupervised trading.** Over-the-counter cash-market trading platforms—where you can buy or sell digital assets for dollars—are not supervised by regulators like other exchanges, banks, or brokers.

2. **Inconsistent customer protections.** Some virtual currency platforms may be missing critical system safeguards and customer protections, such as protection against hacks or segregating customer assets. Without adequate safeguards, you may lose some or all of your digital assets.

3. **Commingled customer assets.** Over-the-counter trading platforms are commonly custodians of your assets. When you trade, you trade against the platform and your funds are held and recorded by the platform on its centralized system—not the blockchain. In these situations, your assets may be mixed with other customers' assets, or could be used by the platform for operational purposes. If the platform is hacked, goes bankrupt, or disappears, you may not be able to get your money back.

Only work with trading platforms that are registered to do business in the United States and your individual state to ensure you retain your protections under the law. Registration alone won't protect you from loss, fraud, or other problems, but most scams involve unregistered entities, people, and products. Trading platforms offering services to U.S. customers are required to register as money service businesses (MSBs) with the Financial Crimes Enforcement Network (FinCEN) and many state regulators. To check a platform's registration, visit **fincen.gov/msb-registrant-search** or **csbs.org/nationwide-multistate-licensing-system**. Companies that offer leverage, margin, financing, or derivatives must register with the CFTC and the National Futures Association (check **nfa.futures.org/basicnet/**).

Cybersecurity risks

4. **Most new projects fail.** And, others could be out and out frauds. Take time to research and understand the project, the technology, use-case, demand, competing projects, governance, who's behind the effort, the developers' track records, how your money will be used, and when or if you can get it back. Was the code audited by a reliable third party and security tested? Closely review white papers and other documents. If they don't make sense, or don't exist, walk away.

5. **Hacker attacks.** In a digital environment hacking is always a threat. Hackers generally seek out the greatest amount of money and the least resistance. Only keep funds you are ready to spend or trade in wallets connected to the internet. Keep the rest in a cold (offline) wallet.

6. **Phishing attacks.** If you receive an email or text about your trading account; a transaction; a new product, wallet, or service; or receive an urgent request to contact customer support; **do not click** any links, open attachments or use QR codes. Phishing attacks often pose as popular brands or companies and the links provided in the emails go to imposter sites that steal your account

information or assets. If you receive an urgent email about your account, independently look up the customer service link. For apps or mobile wallets, visit the apps' official website to download the software.

7. **Lost or stolen private keys.** Your private key is your digital signature. If it is lost or stolen you will no longer have access to your assets. You can recreate a private key, with your digital wallet's seed phrase—a string of words that when encrypted create the private key. Never give your private key or seed phrase to anyone.

Market risks

8. **New and novel.** Compared to other forms of investing, digital assets are relatively new. They don't have long, historical track records, which makes it harder to predict how they will react in different market conditions.

9. **High volatility.** Many digital assets are difficult to value. Uncertainty, changes in sentiment, economic conditions, or even a social media comment, can send market values rising or falling sharply.

10. **Liquidity risk**. It may be hard to sell digital assets that aren't commonly traded. Lightly traded assets are also easier to manipulate.

11. **Run risk.** Stablecoins are not insured, and may not actually be supported by all the stabilizing assets they claim. If stablecoin owners lose confidence and rush for the exits, the panic could lock out some customers and leave them with worthless coins. Runs on one stablecoin can also cause ripple effects in other coins or other parts of the digital economy.

12. **Counterparty risk.** Blockchain transactions were designed to be unchangeable. Once your digital asset is sent to another wallet you cannot get it back. This makes knowing exactly who is on the other side of a transaction critically important. There are no do-overs or charge-backs.

Fraud risks

13. **Watch out on social media.** Most digital asset scams begin on social media or messaging apps. Never make digital asset payments to people you meet online. And don't rely solely on tips or claims you see on social media platforms.

14. **Data can be manipulated.** Criminals can hack social media profiles or easily create new aliases. Fraudulent platforms can also control what you see on their websites or trading apps, and can manipulate you to trade or invest more.

LEARN MORE, visit cftc.gov/LearnAndProtect

Commodity Futures Trading Commission
1155 21st Street NW
Washington, DC, 20581
cftc.gov | 866-FON-CFTC (866-366-2382)

education@cftc.gov @CFTC @CFTCgov youtube.com/CFTC