Keep your assets clean: the risks of owning 'dirty' crypto

By Joseph Cioffi, Esq., Adam Levy, Esq., and Christine DeVito, Esq., Davis+Gilbert LLP

SEPTEMBER 11, 2025

Transactions conducted in fiat currency seldom give rise to questions regarding the currency's origins; however, transactions involving digital assets warrant greater scrutiny. There may be legal ramifications for those who unwittingly possess digital assets like Bitcoin that have been connected to a crime, *i.e.*, "dirty" crypto.

Although a crypto holder or investor may not know their crypto is so tainted, the U.S. government just might. It has become increasingly adept at tracking crypto transactions through tracing analysis.

Over the last few years alone, hundreds of billions of dollars in crypto assets have been used in connection with various crimes and frauds. As such, digital asset holders should be aware of the risks of possessing "dirty" crypto, such as losing assets to the government (subject to a court forfeiture order), frozen digital wallets, and possible devaluation of their "dirty" assets.

Potential losses and liability arising from dirty digital assets

Multiple government agencies, including OFAC (Office of Foreign Assets Control) and FinCEN (Financial Crimes Enforcement Network), are tasked with detecting or investigating crimes involving digital assets (including financial fraud, money laundering, confidence schemes, ransomware attacks, and even terrorism). Recent legislation has provided these agencies greater tools to conduct these investigations.

Notably, the IRS increased the reporting obligations of crypto exchanges for the 2025 tax year, which will serve to enhance the government's visibility into crypto transaction histories.

The classic example of tainted crypto is Bitcoin associated with OFAC's Specially Designated Nationals and Blocked Persons (SDN) List. Any individual engaging in transactions with such crypto may expose themselves to possible sanctions or enforcement actions. For example, they may become subject to civil money judgments, be required to provide information to OFAC, or be referred for criminal investigation.

Such penalties are not reserved for highly culpable persons. Rather, any individual who is in receipt of blocked property — even without criminal or nefarious intent — may be at risk of penalties. OFAC's guidelines explain that a "strict lability" legal standard is applied. Further, persons who comply with OFAC's protocol by reporting (initially and annually) on the affected assets fare only slightly better, as the affected assets may still be frozen.

[D]igital asset holders should be aware of the risks of possessing "dirty" crypto, such as losing assets to the government (subject to a court forfeiture order), frozen digital wallets, and possible devaluation of their "dirty" assets.

Crypto may also be tainted by others' violations of the Bank Secrecy Act (BSA), an anti-money laundering (AML) statute. In *United States v. Sterlingov*, the defendant operated Bitcoin Fog, a "mixer" service which increased the privacy of crypto transactions by commingling assets (while there are legitimate uses of the service, it was also an alleged hotbed for money laundering).

In 2024, the District Court for the District of Columbia entered a preliminary forfeiture order covering all assets that were "involved in" defendant's crimes, including lawfully obtained funds (in which defendant never had a proprietary interest) used in the scheme.

How unwitting dirty bitcoin holders can fight back

Although third parties — which could include purchasers of crypto held on a platform — generally can assert an interest in forfeited property by petitioning the court pursuant to 21 U.S.C. 853(n)(2) (or the civil forfeiture corollary, 18 U.S.C. § 983(a)(4)), doing so entails spending time and money with unpredictable results.

Investors can reduce the likelihood of acquiring "dirty" crypto by transacting on Know-Your-Customer (KYC) compliant exchanges that follow proper AML protocols to screen out crypto associated with blocked IP addresses or otherwise filter out blocked assets. However, as the industry was built on an ideal of decentralization, it is not surprising that crypto transactions are more commonly occurring in various contexts outside traditional exchanges. For example, FinCEN has reported that there are over 37,000 virtual currency kiosks in the U.S. as of January 1 of 2025 — a stark increase from about 4,000 in early 2019. *See* Fin-2025-NTC1.

Yet, persons engaging in peer-to-peer crypto transactions, or transacting through non-compliant exchanges, may end up receiving unvetted assets. Unwitting acquirers of dirty digital assets, which become frozen, forfeited, or discounted, may have avenues for legal relief depending on the potentially offending party, including transferors, exchanges, and intermediaries.

When it comes to avoiding "dirty" crypto, the best cure is prevention through diligence and care in choosing exchanges and counterparties.

For instance, they could seek to hold an exchange with insufficient security measures liable for damages based on a negligence theory. In 2023, in *Sarcuni v. bZx DA*, the District Court in the Southern District of California declined to dismiss a negligence action against a crypto exchange, where alleged security failures resulted in the theft of $55 million in crypto.

To the extent that the crypto at issue is deemed a security, a similar claim possibly could be brought against an exchange that made untrue claims regarding its AML protocols. In 2022, for example, in *Karimi v. Deutsche Bank Aktiengesellschaft* the District Court in the Southern District of New York allowed securities fraud claims to proceed based on alleged misrepresentations of a financial institution's AML practices.

To the extent that the contractual language in a user agreement or other contract with the exchange supports it, the user may also seek to hold the exchange liable under any applicable indemnity provisions.

In addition, users of mixers or other privacy services may be able to assert claims based on the implied covenant of good faith and fair dealing (if a user or similar agreement exists) if their assets become implicated in crime. For example, crypto holders could explore such a claim against the service provider where a service meant to shield users from fraud used deposited assets to facilitate criminal activity, potentially undermining the purpose of the agreement.

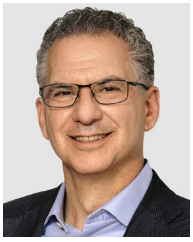
Finally, those who have difficulty disposing of a "dirty" digital asset, leading to a need to discount its value, could explore a suit against the transferor based on a theory of unjust enrichment.

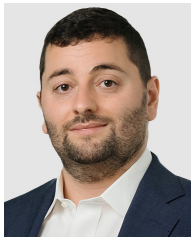
Conclusion

When it comes to avoiding "dirty" crypto, the best cure is prevention through diligence and care in choosing exchanges and counterparties. If despite best practices, an investor becomes an unwitting holder of tainted assets or the subject of a government investigation, they should be aware of the potential liability and create a corresponding game plan for legal action and recovery from the offending party that created the legal exposure.

Joseph Cioffi is a regular contributing columnist on consumer and commercial financing for Reuters Legal News and Westlaw Today.

About the authors





Joseph Cioffi (L) is chief operating partner at **Davis+Gilbert LLP**, where he is also chair of the bankruptcy, creditors' rights and finance practice. He has transactional, insolvency and litigation experience in sectors marked by significant credit and legal risks, such as subprime lending and emerging industries. He can be reached at jcioffi@dglaw.com. **Adam Levy** (C) is an associate in the bankruptcy, creditors' rights and finance group at the firm. He helps creditors resolve their most significant commercial disputes, including fraudulent and preferential transfer actions and financial products litigation. He can be reached at alevy@dglaw.com. **Christine DeVito** (R) is an associate in the bankruptcy, creditors' rights and finance group at the firm. She helps creditors protect their rights in bankruptcy cases and supports borrowers and lenders in negotiating credit agreements. She can be reached at cdevito@dglaw.com. The firm is located in New York.

This article was first published on Reuters Legal News and Westlaw Today on September 11, 2025.