BITCOIN

BankThink The US government is now a bitcoin whale. That has consequences

By Michael Diaz Jr, Ishmael Green, Prince-Alex Iwu June 05, 2025, 10:00 a.m. EDT 4 Min Read

AMERICAN BANKER

The creation of a Strategic Bitcoin Reserve creates a tempting target for bad actors, and raises the stakes for everyone in the areas of anti-money laundering, cybersecurity, market-volatility and sanctions-screening, write Michael Diaz, Ishmael Green and Prince-Alex Iwu, of Diaz, Reus &

Targ. *Adobe Stock*

Washington's 2025 crypto pivot has made the federal government both the world's newest bitcoin whale and a primary shaper of digital-asset rules. With a Strategic Bitcoin Reserve, the SEC's rollback of custody-accounting penalties, and an imminent stablecoin bill, Treasury is shifting from regulator to market participant. For banks, that collision of policy and market power ushers in a fresh mix of anti-money-laundering, cybersecurity, market-volatility and sanctions-screening risks that demand immediate attention.

First, on March 6, 2025, an executive order created the Strategic Bitcoin Reserve, aggregating seized bitcoin into Treasury-controlled wallets as national assets. Treasury's digital asset holdings create attractive targets for cyberattacks. Unlike commercial exchanges such as Binance, whose mix of hot and cold wallets offers only partial on-chain visibility, every Strategic Bitcoin Reserve address that becomes publicly known is fully traceable on-chain. That transparency is a double-edged sword: It aids forensic monitoring but also lets adversaries track balances and time their attacks.

These wallets, likely worth billions, are publicly traceable on blockchain ledgers, making them especially tempting to cybercriminals. For comparison, the government previously seized 69,370 BTC ($4.4 billion) from Silk Road and 94,000 BTC ($3.6 billion) from the Bitfinex hack. This visibility mirrors the vulnerabilities seen in the Mt. Gox ($470 million, 2014) and Binance ($40 million, 2019) hacks. While the executive order does not prescribe how Treasury wallets must be structured, any bank that wins a custodial mandate will need robust multiparty computation or other multi-signature controls. If a custodian maintains even a limited online balance in a hot wallet, it must budget for costly insurance. In short, encryption is table stakes, multi-signature is mandatory and cyber-insurance premiums are only going up.

Secondly, whenever a reserve address is identified by on-chain analysts, its visibility can trigger volatility and market-manipulation risks. Crypto markets rely on real-time wallet-tracking tools

such as Whale Alert and Arkham Intelligence. Traders already react sharply to movements in wallets tagged "U.S. government," as shown when bitcoin slipped toward $60,000 after a government wallet moved roughly $240 million in Silk Road-linked BTC on June 26, 2024. Even routine flows — for asset liquidation, restitution payments or custody shuffles — may be misread as policy signals, sparking automated selling or front-running. Banks providing custody or execution services must therefore reinforce liquidity-management playbooks and upgrade market-surveillance systems to spot spoofing and sudden order-book imbalances as soon as flagged reserve wallets start to move.

Additionally, compliance obligations are becoming more complex. Because Treasury-controlled wallets are explicitly covered by OFAC sanctions guidance and Fincen's proposed record-keeping rules for large crypto transfers, any transaction touching those addresses triggers heightened know-your-customer and sanctions-screening obligations. Banks must verify transactions carefully to comply with sanctions laws and restrictions detailed by Treasury guidelines, significantly increasing the operational compliance burden.

CRYPTOCURRENCY

Market structure bill gets off to rocky start at hearing

House lawmakers discussed the recently introduced market structure bill, with Democrats expressing concerns that the bill could enable banks to evade securities laws.

By Claire Williams

June 4

The SEC's recent Staff Accounting Bulletin No. 122 (SAB 122) reverses the 2022 guidance that forced banks to hold crypto assets on balance sheet. By scrapping that costly capital treatment, SAB 122 finally makes crypto custody economically viable for regulated institutions. Several banks have already relaunched pilot programs, signaling a renewed rush into digital assets. The compliance stakes, however, remain high: AML requirements did not soften. Wallets handled by banks must still be screened against OFAC's ever-lengthening list of sanctioned addresses, including Hezbollah and Houthi-linked clusters that moved millions in stablecoins to evade sanctions.

Furthermore, bipartisan momentum behind the STABLE Act, which is now advancing through Congress, will add statutory muscle to stablecoin oversight. The bill would impose bank-level prudential standards and explicit AML/KYC duties on any institution that issues, holds or clears fiat-backed tokens. That is not hypothetical: Banks already processing stablecoins such as Tether (USDT) must detect illicit activity like Venezuela's 2024 use of USDT to bypass oil sanctions in a market where stablecoins powered 63% of all illicit crypto volume in 2024. Transaction-monitoring engines and screening rule sets therefore need to evolve quickly, well before the STABLE Act takes effect, to flag sanctions-evading flows and keep compliance programs exam-ready.

Why should banks care? Treasury's Strategic Bitcoin Reserve turns government wallets into high-value targets, reshaping AML, sanctions and cybersecurity expectations across the industry. Whether launching or expanding crypto-custody services under SAB 122, banks must invest in real-time blockchain analytics, sanctions screening and robust cyber controls. Falling short could invite regulatory enforcement, market losses and reputational damage; a risk underscored by the Federal Reserve's 2024 enforcement action against Customers Bank for "significant deficiencies" in its digital-asset AML controls. Integrating these tools is now table stakes for accurately attributing wallet activities, screening sanctions exposure and spotting mixer flows that illicit actors use to obscure funds.