ARTICLE

Implications of the U.S. Government's Plan to Regulate Cryptocurrencies

Government regulation in the U.S. and elsewhere is expected to actively influence the development of digital asset products and markets over the next decade. As the digital assets industry and consumers await regulatory clarity, recent events have exacerbated longstanding concerns about the potential use of cryptocurrency to facilitate illicit activities and sanctions evasion.

Despite the recent market contraction in digital assets, industry market cap still stands at around $1 trillion, up from $14 billion from five years ago.[1, 2, 3] Around 16 percent of adult Americans – approximately 40 million people – have "invested in, traded, or used cryptocurrencies."[4]

On March 9, 2022, President Biden signed an Executive Order directing the federal government to develop a coordinated, interagency plan to oversee digital assets, and assess whether the U.S. should issue a digital equivalent to the dollar.[5] The order directs the U.S. Department of Treasury's Financial Stability Oversight Council to identify and mitigate systematic financial risks posed by digital assets and develop appropriate policy recommendations to address regulatory gaps.[6]

Under the Executive Order, the Department of the Treasury will partner with other agencies and the U.S. intelligence community and collaborate with allies to ensure international frameworks,

1 "Is Crypto Really Worth $3 Trillion? I Ran the Numbers.", Bloomberg, Aaron Brown, Nov. 10, 2021.

2 "The World's Cryptocurrency Is Now Worth More Than $3 Trillion", TIME, Joanna Ossinger, Nov. 8, 2021.

3 "Crypto Winter Is Coming: What You Need To Know", Forbes, Farran Powell, June 14, 2022.

4 "FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets", The White House, March 9, 2022.

5 "Biden moves toward regulating cryptocurrencies", MSN/Boston Globe, Katie Rogers and Ephrat Livni, March 9, 2022.

6 "FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets", The White House, March 9, 2022.

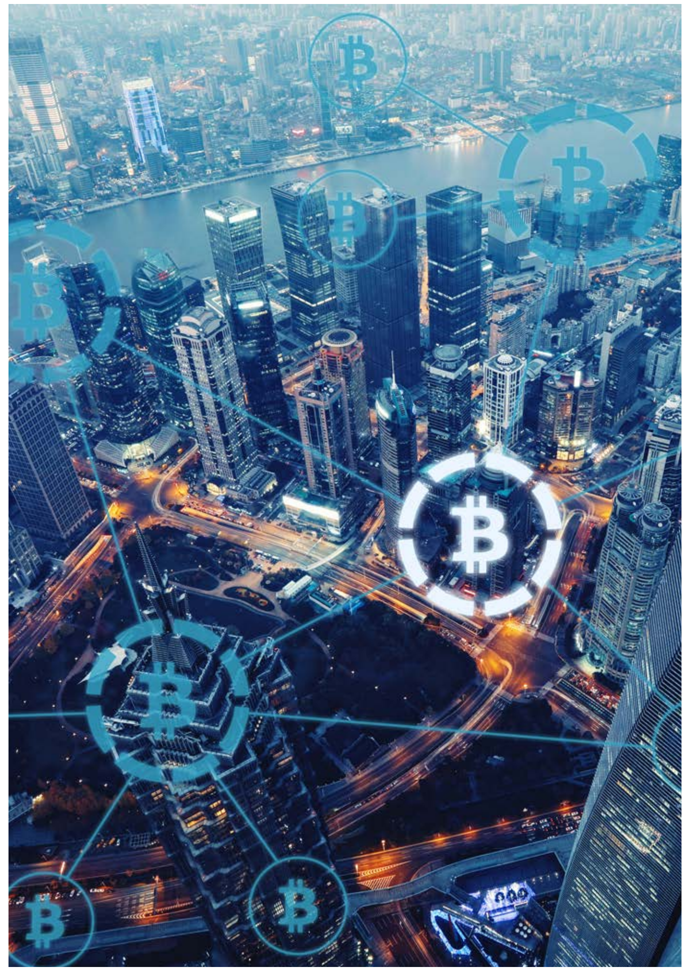
capabilities, and partnerships are aligned and responsive to potential risks.[7] According to the White House, this cooperative approach will help produce a plan to regulate cryptocurrencies, and ensure responsible innovation while mitigating the nexus to illicit finance and risks to consumers, financial stability, and national security.[8]

Cryptocurrency and blockchain technology, while offering benefits such as reducing the cost and increasing the speed of financial transactions, streamlining supply chain management, reducing administrative costs, and bringing financial services to the "unbanked", carry significant risks if not implemented properly. For example, theft of funds and data breaches can result from failure to account for security risks. In addition, cryptocurrency holders are often targeted by bad cyber actors, and as digital currencies become more sought after as a result of sanctions, the targeting can be expected to increase.[9]

Cryptocurrency and Sanctions Evasion

Russia's February 2022 invasion of Ukraine resulted in additional economic sanctions imposed by the U.S. and several of its allies. Among the objectives of the new sanctions is to target the wealth of key political figures and other national security officials, oligarchs, and institutions of Russia.[10]

The Biden Administration is concerned that cryptocurrency may provide an end run around sanctioned Russian money, and that Russian entities could leverage cryptocurrency to blunt the force of U.S. sanctions, including a so-called digital ruble and by launching ransomware attacks.[11] The demanded form of payment in most ransomware attacks is cryptocurrency, creating a potential source of illicit revenue for sanctioned entities.[12]



In further efforts by the U.S. aimed at preventing Russia from using cryptocurrency to evade sanctions, Senator Elizabeth Warren (D-Mass.) introduced a bill ("Digital Asset Sanctions Compliance Enhancement Act of 2022") to make it harder to use cryptocurrency to evade sanctions,[13] and the Treasury Department issued a Financial Crimes Enforcement Network (FinCEN) alert that instructed financial institutions to be "vigilant" of Russian oligarchs and state actors attempting to evade sanctions and other U.S.-imposed restrictions with cryptocurrency.[14]

7 Ibid.

8 Ibid.

9 "Report of the Attorney General's Cyber Digital Task Force", Office of the Deputy Attorney General, Cyber-Digital Task Force, October 2020.

10 "U.S. Treasury Imposes Sanctions on Russian Federation President Vladimir Putin and Minister of Foreign Affairs Sergei Lavrov", U.S. Department of Treasury, February 25, 2022.

11 "Russia could use cryptocurrency to blunt the force of US sanctions", Economic Times/New York Times, Emily Flitter and David Yaffe-Bellany, Feb. 24, 2022.

12 "Report of the Attorney General's Cyber Digital Task Force", Office of the Deputy Attorney General, Cyber-Digital Task Force, October 2020.

13 "Warren crafts bill targeting cryptocurrency in Russia sanctions", Leigh Ann Caldwell, NBC News, March 8, 2022.

14 "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts", FinCEN Alert, March 7, 2022.

The U.S. and its allies will face increasingly complex and interconnected convertible virtual currency (CVC) threats marked by the growing use of decentralized digital assets. These challenges will play out amidst continuing global financial and economic disruptions resulting from Russia's invasion of Ukraine and the Covid-19 pandemic, increasing the potential for disruptions to financial systems. Evolving digital assets technology presents a changing and enduring threat that could potentially undermine sanctions compliance of financial institutions.[15]

Over the past decade, illicit actors such as sanctioned Russian oligarchs and criminal syndicates have diversified their funding sources by incorporating digital assets. Cryptocurrency appeals to sanctioned individuals, entities, or institutions because of:

1. The ability to make rapid transfers without intermediary or geographic limitation,
2. Perceived finality of settlements,
3. Lower transaction costs,
4. The ability to publicly verify transactions,
5. Pseudonymity, and
6. Varying and limited regulatory oversight and requirements.

According to FinCEN, as a result of significant sanctions actions taken by the Department of the Treasury's Office of Foreign Assets Control (OFAC), sanctioned Russian and Belarusian actors may seek to evade sanctions through various means, including via non-sanctioned financial institutions in Russia, Belarus and developing countries.[16] In addition, sanctions evasion activities could be conducted by various actors who retain access to the international financial system, including convertible CVC exchangers and those in geographies outside Russia.[17]

How to Prepare for New Financial Regulations

The U.S. is considered one of the early pioneers and leaders in setting international standards for regulating and supervising digital assets and digital asset service providers for anti-money laundering and countering financing of terrorism (AML/CFT).[18] Although the U.S. urges the international community to implement international standards, poor implementation of those standards abroad can present significant illicit financing risks for the U.S. and global financial systems.[19]

It is incumbent on entities to proactively address common areas of vulnerability today, before regulation is enacted that broadly mandates stronger protections. The Biden Administration's Executive

[15] "FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets", The White House, March 9, 2022.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange", U.S. Department of the Treasury Press Release, Nov. 9, 2021.

Order outlines the need for coordinated regulatory measures to reduce the risks digital assets could pose to consumers, financial stability, national security, and combating illicit financing, among other things.[20] These risks drive three key remediation themes:

1. **Cybersecurity**: Cryptocurrency is already becoming more mainstream and as its popularity grows, cyber attacks intending to steal funds will increase. Regulations implementing Know-Your-Customer (KYC), anti-fraud, and AML requirements will result in policies and procedures that curb a percentage of the attacks (for example, by identifying and suspending transactions that are inconsistent with customers' typical activity and stated account purposes), but the pseudonymity of transactions is likely to remain.[21] This aspect will continue to attract cyber threat actors capable of stealing large sums of cryptocurrency, and cryptocurrency-related attacks, such as ransomware attacks, compelling proper cybersecurity protections.
2. **Consumer Protection**: The increased use of digital assets, exchanges, and trading platforms may increase the risks of crimes targeting consumers such as fraud and theft, other regulatory violations, privacy, and data breaches, unfair and abusive acts or practices. In response, providers of digital asset products and services to consumers must put the proper consumer protections in place.
3. **Detecting Illicit Finance**: Digital assets have facilitated cybercrime-related financial networks and activity, including ransomware, that could pose national security risks. The introduction of digital assets into the financial system may increase the risk of financial crimes such as money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, theft, and corruption.[22] These illicit activities will likely drive greater scrutiny of digital assets. Organizations should review and set their own standards for AML, CFT, KYC, and sanctions programs to mitigate these risks, rather than rely on minimum regulatory standards.

The Biden Administration's Executive Order also further lays the groundwork for increased U.S. regulation,[23] and members of Congress have authored multiple bills this year. The industry and consumers continue to cope with uncertainty in the rulemaking process which is unfortunately likely to persist for some time. In the interim many organizations are developing more risk management muscle on their own.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals.

[20] "FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets", The White House, March 9, 2022.
[21] "Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework", Anthony M. Shults et al, October 2020.
[22] "FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets", The White House, March 9, 2022.
[23] Ibid.

JACO SADIE
Senior Managing Director
+1 415 283 4230
jaco.sadie@fticonsulting.com

TODD RENNER
Senior Managing Director
+1 404 460 6200
todd.renner@fticonsulting.com

AMBER VITALE
Managing Director
+1 646 453 1269
amber.vitale@fticonsulting.com

PAUL FELDMAN
Senior Director
+1 212 499 3687
paul.feldman@fticonsulting.com

RYAN MCHALE
Director
+1 312 252 9306
ryan.mchale@fticonsulting.com

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm. ©2022 FTI Consulting, Inc. All rights reserved. **www.fticonsulting.com**

07192022 | VN02243-v09