NOVEMBER 2022

KEY POLICY CONSIDERATIONS AND RECOMMENDATIONS **FOR CRYPTOCURRENCY**

NSI on the Hill represents the views of a number of the National Security Institute's experts—many with longstanding experience working on crypto-related matters—and it identifies key considerations and recommendations for Congress to consider regarding potential legislative action to regulate this emerging technology.

OVERVIEW

The advent of Bitcoin, and subsequently other digital currencies, along with other Web3 elements like decentralized finance (DeFi) has introduced new considerations regarding how the United States should treat economic policy and, by extension, national security. Crypto's continued innovation is creating significant implications for the U.S. national security community, including anti-money laundering and countering the financing of terrorism (AML/CFT) efforts, sanctions enforcement, and criminal investigations, particularly the growing ransomware epidemic. While well-intentioned, some U.S. regulators and policymakers are attempting to apply existing ill-fitting rules to this new industry in ways that could severely stifle the ability of the United States to remain at the forefront of this transformative technology, which is key to maintaining U.S. leadership of the global financial system.

NSI seeks to promote policies that are pro-innovation while supporting the development of new paradigms for achieving key U.S. national security objectives, including those around AML/CFT, law enforcement investigations, financial intelligence collection, and sanctions viability. This paper provides a roadmap of recommendations for Congress to consider as it begins to tackle the question of regulating the crypto industry.

KEY RECOMMENDATIONS FOR CONGRESS:

- Congress could pass bipartisan legislation to provide broad policy guidance and a market-friendly regulatory framework to govern digital assets that clears away conflicting state and local law, as well as provides increased funding to federal, state, and local law enforcement agencies to better understand and interdict illegal activity traced to blockchains.
- Congress could amend the Bank Secrecy Act (BSA) to include non-fungible tokens (NFTs) in AML/CFT guidance to make explicit how these novel instruments are treated by financial regulators.
- Congress could direct the Treasury Department to institute a risk-based approach to reporting requirements for unhosted/self-hosted wallets, which would empower individual financial freedom through self-custody of financial assets while allowing for appropriate oversight of national security concerns.
- Congress could incentivize increased cooperation, specifically detailed information sharing and threat reporting, between federal agencies and the private sector regarding ransomware and other cyber-based threats.

BACKGROUND

AML/CFT REGULATIONS

- U.S. regulators charged with designing and enforcing AML/CFT regulatory frameworks, chiefly the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN), have been on the leading edge of digital currency policy for several years as they have worked to address money laundering, terrorist financing, and other criminal efforts leveraging these new digital technologies.
  - Industry participants have debated whether existing laws provide authority for these actions and have argued that new, clearer standards need to be written into law by Congress to create a more effective regulatory regime that accounts for the novelty of the technology underlying digital currencies and decentralized finance (DeFi) protocols.
  - Currently, regulatory enforcement is driven by multiple federal statutes and a patchwork of state-level regulations.
    - This escalates the cost of doing business in U.S.-based jurisdictions, despite having the most open and dynamic investment environment in the world.
      - Despite being the financial capital of the United States (and arguably the world), New York State's Department of Financial Services' BitLicense program, which allows virtual asset service providers (VASPs) to operate in New York, has driven away businesses due to high compliance costs.
    - American entrepreneurs must have the ability and opportunity to innovate, or the U.S. risks losing key industry players to other countries, giving those foreign jurisdictions a freer hand in dictating the rules of the road for this technology and its development.

SANCTIONS

- The evolution of digital assets has introduced new challenges for sanctions authorities in the United States, chiefly, how should software, including source code, be treated by existing sanctions law and will digital assets make it easier for America's adversaries to evade its sanctions regimes.

- As financial technology continues to evolve, particularly with the increasing number of digital assets and blockchain applications in the crypto ecosystem, it is critical that OFAC, along with law enforcement agencies, be able to effectively use the tools at their disposal to prevent criminal activity, particularly where, as here, there is a significant nexus with national security.
  - We have already seen the Treasury Department start to take direct action against alleged bad actors in this space, for example, through the recent imposition of significant sanctions on Tornado Cash.
  - While some may argue that the decentralized nature of autonomous-running applications (like Tornado Cash) makes it difficult (if not impossible) to implement appropriate controls, particularly with existing laws, because there is no claimed financial or legal ownership of the application nor any individual claiming ownership, the fact is that numerous blockchain applications have developed capabilities to limit their use for illicit purposes.

- Despite initial concerns from policymakers, it does not appear that the Russian government or large Russian corporations have used digital currencies at scale to evade U.S. and EU sanctions since the beginning of the Russia-Ukraine war.
  - Our assessment, however, is that this is not for lack of interest but rather because there is no developed foreign exchange market for fiat-crypto currency trading pairs, since most cryptocurrencies are traded while pegged to stablecoins (another form of digital currency) rather than convertible fiat currency, keeping funds on the blockchain ecosystem. Two, it remains difficult to move a large amount of money off major blockchains—as a nation-state would need to—while still obscuring the "cash-out" destination.

UNHOSTED/SELF-HOSTED WALLETS

- The U.S. government, led by the Treasury Department, has been debating how to regulate unhosted wallets for several years. (An unhosted/self-hosted wallet is software or hardware that allows a user to maintain possession of digital currency off of an exchange or other third-party platform. In the absence of targeted regulations, such tools allow their users to remain anonymous or pseudonymous in the course of financial transactions.)
  - Initial attempts to require wallet providers to broadly collect counter-party information for all transactions was considered a non-starter by industry, including the inherent design of open-source, non-custodial wallets, which are intentionally created to make financial intermediaries redundant and, consequently, make the collection of customer information unnecessary.
  - While the rule-making process is still underway at the Treasury Department, other jurisdictions have taken steps to address how to regulate unhosted wallets by crafting their own rules, such as in the UK, the EU, or Switzerland, which could provide a pathway for U.S. regulators, or for Congress, to step in sooner.
    - For instance, in the UK, the government applies significant information requirements for unhosted wallet transfers on a risk-sensitive basis and requires limited information to be provided for counterparties for cross-border transfers above a de minimis level while protecting this information through its data protection regulations.
    - In the EU, under new rules proposed by the Markets in Crypto-Assets (MiCA) framework, **negotiators have agreed upon a reporting threshold of €1,000 for transactions involving unhosted wallets** (which is notably less than the $10,000 required for cash transactions in the United States under the Bank Secrecy Act).
    - More so than the UK or EU, **Switzerland has moved in a more enforcement-friendly direction**.
      - Swiss financial authorities have implemented an automated protocol that allows users to automatically share proof of ownership of a cryptocurrency wallet with regulators when conducting transactions.

RANSOMWARE & CYBER THREATS

- The spread of ransomware has reached epidemic proportions, with criminals targeting a broad range of victims and an expanding list of potential threats to governments, emergency services, and critical infrastructure.
  - Blockchain-based currencies have played a key role in the spread of ransomware as criminal actors have sought to use the ostensible anonymity that blockchain-based currencies provides to hide their transactions.
  - At the same time, the development of sophisticated blockchain analytics, coupled with the public and immutable nature of the blockchain, also provide new and evolving capabilities to trace criminal activity, disrupt it, and recover illicit gains.

- According to one ransomware activity report, hackers received nearly $700 million in cryptocurrency extorted from ransomware attacks in 2020, a more than 300% increase from the prior year.
  - The same study said that approximately 74% of global ransomware revenue went to entities either located in Russia or likely controlled by the Russian government.

- According to Chainalysis' annual report in 2022, even though the use of crypto for illicit purposes as a percentage of overall blockchain traffic has decreased as the number of users engaging in crypto-based financial transactions has increased over 500% from 2020 to 2021, the overall amount of money stolen or otherwise fraudulently obtained has increased significantly, to the tune of $14 billion in illicit crypto-based proceeds.

- In many ways, undertaking criminal activity on the blockchain is akin to leaving certain types of forensic evidence at the scene of the crime, giving investigators a potential blueprint to follow—essentially a digital money trail—for tracking down bad actors.

- Law enforcement agencies from the Secret Service to the IRS, have successfully carried out investigations and prosecutions—oftentimes in collaboration with rapidly innovating private-sector firms and without the need for the use of traditional law enforcement investigative tools like subpoenas—using sophisticated analytics and transaction details available on public blockchains.
- At the same time, current technology does limit the ability to monitor transactions on the major blockchains (like Bitcoin, Ethereum, Solana, and a few others) because existing blockchain intelligence firms are limited in their ability to monitor transactions on newer, lesser used blockchains.

- There is also an emerging enforcement problem—similar to the jurisdictional issues seen in cybersecurity—because there is no single agency in charge of all matters related to the crypto ecosystem; agencies ranging from the FBI, Department of Justice, Intelligence Community, to the Treasury Department, the SEC, and the CFTC—not to mention state agencies—all play different roles and seek to assert jurisdiction to potentially regulate or police the crypto economy.
  - This lack of clear agency leadership makes it difficult for victims to know where to turn for assistance and makes it nearly impossible for even well-meaning actors to comply with the wide range of (sometimes conflicting) guidance and regulation.

RECOMMENDATIONS FOR CONGRESS

AML/CFT REGULATIONS

- Congress ought to take up bipartisan legislation that provides broad policy guidance and a market-friendly regulatory framework to govern digital assets and that clears away conflicting state and local law, and provides increased funding to federal, state, and local law enforcement agencies to better understand and interdict illegal activity.
  - Such a framework would also allow the United States to put down a marker to the rest of the world and signal our position as the continued leader of the international financial system and help promote further international coordination on AML/CFT frameworks regarding digital assets between the United States and much of the G7, including through the Financial Action Task Force (FATF).

- To put the United States in a position of regulatory leadership, Congress could introduce legislation to establish and fund AML/CFT training programs in digital assets for U.S. allies, particularly the G7, where close financial linkages already exist.

- Congress could create a new federal grant program exclusively for training related to cryptocurrency investigations for law enforcement agencies.
  - This would help narrow the gap, as intelligence firms have noted, between “traceability and retrievability,” to help police find ways to not only find stolen digital assets but to get them back as well.

- NFTs also represent an AML risk because they can be moved on and off exchange-based marketplaces just as easily as cryptocurrencies and could act as a store of value that might escape regulation.
  - **A Treasury Department report from February 2022** on money laundering in the art world reflects the difficulty with classifying NFTs, due to their opaque nature and differing characteristics therein.
  - **According to Elliptic**, a blockchain intelligence firm, digital assets owned by sanctioned entities have been used to buy NFTs and have also been linked to Tornado Cash, “the laundering tool of choice,” for purchases in NFT marketplaces.

- Congress could amend the BSA to codify that rules governing virtual assets also apply to NFTs.
  - Using **FATF's most recent guidance on the subject**, FinCEN could classify NFTs as virtual assets when they are "used for payment or investment purposes" and apply existing AML/CFT rules.
  - **While Treasury continues to study the issue of NFTs**, and in the absence of comprehensive, bipartisan legislation with appropriate executive branch input, Congress could act to ensure that existing NFT platforms, and other digital art marketplaces, are treated as regulated entities within the crypto ecosystem, as opposed to the **opaque treatment NFTs currently receive in most jurisdictions**.

SANCTIONS

- In order to gain clarity of legal issues surrounding the designation of computer code, Congress could direct the Department of Justice's Office of Legal Policy to issue a report providing its legal opinion as to the constitutionality of applying sanctions under the existing International Emergency Economic Powers Act (IEEPA) statute to software and how this interpretation may be affected by the Ninth Circuit Court's ruling in *Bernstein v. Department of Justice* that computer code is considered speech protected by the First Amendement.

- To better understand the dynamics of sanctions evasion in an era of digital money, Congress could direct the Treasury Department, in coordination with the State Department, Intelligence Community, and other agencies as appropriate, to issue a report, to include a classified annex, detailing how nation-states use cryptocurrencies, blockchain platforms, and other elements of Web3 to evade U.S. sanctions.

UNHOSTED/SELF-HOSTED WALLETS

- Congress could instruct the Treasury Department, specifically FinCEN, to institute a risk-based approach to reporting requirements for unhosted/self-hosted wallets.
  - This risk-based approach would mirror **steps taken by the United Kingdom**, our closest ally and, arguably, most like-minded partner in the global financial system, to update U.S. rules on unhosted wallets.
    - Given the evolutionary state of VASPs, and the crypto ecosystem more broadly, U.S. policymakers should consider whether it is best to implement risk-based guidelines, as opposed to mandatory requirements, to ensure that technological innovation is not prematurely crimped.

- During proposed rulemakings for VASPs, U.S. regulators could propose rules that allow said providers to utilize available private-sector tools, including those developed by **Chainalysis**, **Eastnets**, **Elliptic**, and **TRM Labs**, to ensure compliance with Treasury sanctions and rules promulgated by OFAC and FinCEN.
  - These tools can be used to verify that wallet addresses are verified and cross-checked against the Treasury's Specially Designated Nationals and Blocked Persons (SDN) List for compliance with current sanctions regimes.

- Congress could also encourage the establishment of de minimis rules, which have been considered by non-U.S. jurisdictions.
  - Such a regulation would set a baseline above which increased scrutiny or reporting requirements on virtual assets transactions would kick in and be aligned with **FATF's standards**.
    - For instance, if a transaction were to take place involving an unhosted wallet, whereby there could be a lack of personally identifiable information of the sender or receiver of virtual assets, the VASP would collect the names and wallet addresses of the beneficiary, as well as the originator.

RANSOMWARE & CYBER THREATS

- Congress could incentivize increased cooperation, specifically detailed information sharing and threat reporting, between federal agencies and the crypto industry regarding ransomware and other cyber-based threats, before more **aggressive reporting regimes being considered** by the Securities and Exchange Commission (SEC) are adopted.
  - Financial institutions are already permitted to share information under **Section 314(b)** of the USA Patriot Act.
  - Congress can signal its regulatory intent most effectively by providing clear and broad liability and regulatory protections for organizations that provide detailed information and cooperate deeply with the government.
  - Major crypto players could form an organization like the FS-ISAC for the purposes of sharing finance-related AML, CFT, and other threat information.
    - Such an organization may already exist in the form of the **Cryptocurrency Compliance Cooperative**, an association of industry players, largely specializing in offering blockchain analytics services.
    - Formalizing the organization into an ISAC, coupled with appropriate regulatory and liability protection, could serve as the industry's organized intake for government interaction on AML/CFT rules and proposed regulatory rulemaking.
      - Such a public-private interface would raise awareness, inform business owners, and be a place for the government to flow information to the private sector.
  - This body could be used as a triage center, intaking information regarding financial hacking techniques and attack vectors, while also directing victims to the best state or federal agency equipped to assist with their specific issue and coordinating the regulatory efforts of various players.
    - A crypto ISAC would benefit from the Treasury Department serving as the lead government representative to industry given Treasury's staff unique subject matter expertise regarding financial instruments. Treasury could loop in other regulators, like the SEC, CFTC, and Office of the Comptroller of the Currency, on an as-needed basis.
      - Treasury's lead in this space is reinforced by **Presidential Policy Directive 21**, which designated Treasury as the sector-specific agency for the financial services industry, which can be reasonably extended to VASPs and other blockchain-based entities that provide financial services to customers.
- Like the iterative process that has taken several years by which the cybersecurity industry has become embedded with government efforts to secure networks, critical infrastructure, and other network-based assets, the crypto industry needs to acknowledge its role as the first line of defense when it comes to protecting its platforms from illicit users.

MOVING FORWARD

- There are significant economic and national security benefits to the United States for ensuring that key blockchain-based innovation continues to take place in the United States and allied nations, including ensuring that such technologies provide for increased financial inclusion for those who have been unable to access the traditional financial system and do not empower authoritarian regimes to exert additional control over their own populations and to export repression abroad. In addition, keeping blockchain innovation remains here will ensure that the U.S. government can take appropriate, limited action to help prevent fraud and financial crimes, including money laundering and terrorism financing.
  - Moreover, the fact that all major digital currencies, including most major stablecoins, currently derive their value relative to the dollar, gives the United States leverage in setting the rules of the road for crypto regulations, including how to best utilize sanctions to prevent or punish illicit activity.
  - However, if the United States overregulates, we could very well push developers and users abroad, as industry participants seeks regulatory arbtriage opportunities in other jurisdictions, including potentially denominating their cryptocurrencies against fiat currencies backed by non-market economies.