Bitcoin Policy Institute

November 3, 2022
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220
RE: Ensuring Responsible Development of Digital Assets; Request for Comment

Bitcoin As a Strategic Asset for National Security

About Bitcoin Policy Institute

The Bitcoin Policy Institute (BPI) is a non-partisan, non-profit research center working to study the policy and societal implications of emerging monetary networks. Our researchers include economists, lawyers, climate scientists, philosophers, and technologists with decades of combined experience studying Bitcoin and digital assets. We are pleased to submit the following comment in response to the U.S. Department of the Treasury's request for comment.

Introduction

U.S. policymakers have long recognized the strategic value in providing pathways for global citizens to connect to our society and capital markets when they would otherwise be blocked by hostile governments. The political economies of our nation's greatest adversaries have continuously relied on restricting the access of their citizens to the free world. As former Secretary of State and Treasury Secretary George Shultz stated, *"Open political and economic systems have been gaining ground, and there's a good reason for it. They work better."* Dictators and autocrats rely on strict surveillance and control over the flow of information and capital because human beings in their innate yearning for self-determination will universally choose freedom over repression. Without such restrictions, these closed societies would evolve as citizens gained awareness of and access to the American way of life.

In the post-war era, an open international system has been featured as a key U.S. policy objective for every administration, Democrat or Republican. The past 70 years have been marked by the success of efforts to champion free speech and free trade across the globe. Indeed, America won the Cold War in large part through attraction – by tearing down the physical, ideological, and commercial walls of communist states and exposing their citizens to capitalism and democratic society. For example, government-funded initiatives like Voice of America and Radio Free Europe stripped authoritarians of their monopoly on information and demonstrated the value of free speech. Exposure to western goods revealed the benefits of capitalism. The attractiveness of free and open societies did the rest.

Amidst the increasing digitization of political and economic life, today's tyrants have erected powerful technological tools to monitor, censor, and restrict the open flow of information and value. To win, America must continue its tradition of promoting even more powerful technologies that render the closed systems of our adversaries impotent.

The American Legacy of Strong Encryption

The Tor network (short for "The Onion Router") enables anyone to communicate over the internet anonymously. Since its public release in 2003, individuals have used Tor for both legitimate and illicit activities. Tor offers unrestricted communication and connection for salutary purposes – for example, to domestic violence victims, foreign dissidents, whistleblowers, and the intelligence agencies of our allies; but it also is available to foreign adversaries and criminal or other malign actors.

Enabled by strong encryption, Tor is a powerful technology that greatly diminishes the U.S. government's ability to monitor or block the open flow of information. Despite this, Tor was born out of the United States Naval Research Laboratory, open-sourced to the world by U.S. intelligence agencies, and it continues to receive most of its funding from the U.S. government. Responding to mounting calls for the government to crack down on strong encryption, former NSA and CIA Director Michael Hayden quipped "*Why would you weaken a powerful cyber tool…even for a legitimate law enforcement need over here?*" Before addressing the topic of digital assets, it is worth reflecting on the question of why we not only allow, but actively promote, unrestricted global internet access.

A modern authoritarian regime is only as strong as its control over information and capital. For the past two decades, Tor and the promotion of encrypted communications have allowed dissidents to undermine closed societies from within by enabling anyone living under dictatorship to access western media and ideas, communicate freely, and organize – all outside the purview of their government.

At its core, permissionless strong encryption has digitally enshrined key civil liberties and human rights, like freedom of speech, assembly, association, and the press, for anyone connected to the internet. From Tor's use in facilitating the 2009 Iranian uprising and punching through China's Great Firewall to Facebook and Twitter's role in the Arab spring, we observe a clear pattern of the open flow of information strengthening our open society's interests. Emphasizing this point in a 2016 interview, then Defense Secretary Ash Carter explained how strong encryption strengthens US national security, stating, *"Russia and China openly defy all the values of freedom of speech, of free and open Internet. If they write the rules, they won't be consistent with the values of the United States."* It is widely understood that permissionless access to and unstoppable transmission of information inevitably benefits open societies and undermines illiberal states. In much the same way, bitcoin's adoption globally represents a force empowering the individual over repressive states and a tool for the marginalized to gain self-determination.

Bitcoin: The Next Chapter of Our Open System

Bitcoin allows anyone in the world with an internet connection to store and send value in a manner that cannot be reversed, frozen, or seized. It is open and permissionless. It is distinct from other cryptocurrencies in that it is credibly neutral, widely-decentralized, uncontrolled by any leadership or founding team, and optimized for resisting censorship. In keeping with the basic liberal principle of limited government and our legal system's presumption of innocence, Bitcoin, like cash, ensures that while anyone can make a payment, no one is shielded from the consequences of their payment. America and other open societies can thrive by recognizing that crime must be discovered before it is prosecuted. Illiberal, closed societies follow different, repressive rules.

Like Tor, Bitcoin is used for both lawful and illicit activities, relies on encryption developed and open-sourced by U.S. intelligence agencies, and offers unrestricted access to its users. On a per capita basis, Bitcoin is most widely used in nations with authoritarian governments, weak respect for property rights, and strict capital controls. Human rights groups have documented that dissidents in countries like China, Russia, Iran, Nigeria, and Venezuela increasingly turn to Bitcoin to finance their resistance. Just as Tor enabled tens of millions of people to see and access the freedom of open societies, Bitcoin enables tens of millions to escape the capital controls of authoritarian states and connect to the western financial system. Just as Tor digitally enshrines and exports the right to communicate freely across the globe, Bitcoin digitally enshrines and exports free trade and the right to transact. While the freedoms Bitcoin affords its users align well with longstanding U.S. policy objectives, these same freedoms present a unique threat to our greatest adversaries.

There is a reason China has been among the most Bitcoin-hostile governments in the world, banning Bitcoin mining and making all cryptocurrency transactions illegal. Bitcoin allows citizens of illiberal states to vote with their money, to participate in our financial markets, and to deploy capital without the blessing of the state. Following in the footsteps of Radio Free Europe and Tor, Bitcoin continues the

American thesis that when given the opportunity to choose between open and closed societies, global citizens will choose the former.

Assessing Risks

Ransomware

Criminal groups (some state-sponsored) have dramatically increased the scale, sophistication, and severity of ransomware operations. As a result, attacks are becoming more frequent and the payouts (demanded in cryptocurrency) are growing. The U.S. National Security Council is focused on this issue and has directed a whole of government approach to counter ransomware groups and bolster public and private sector resilience to attacks. The Colonial Pipeline ransomware incident in May 2021 elevated this topic from a cybersecurity-specific issue to a high-priority national security issue.

While most criminal groups still accept Bitcoin (as the most highly valued crypto-asset), they are increasingly demanding ransomware payment in "Anonymity Enhanced Cryptocurrencies" (specifically Monero). Unlike Bitcoin (whose transparent ledger makes transactions trivial to track), AECs like Monero are designed for privacy, obscuring all transactions from public view. As a result, some ransomware groups charge a premium (~10-20%) for Bitcoin vs. Monero, with the latter denominating the majority of ransomware demands. DHS and the IRS have put out contracts for firms that claim to be able to potentially track Monero transactions, but the specific technical capabilities are not public.

Illicit Finance

Cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, but the market correction in the first half of 2022 has seen illicit transaction volumes falling 15% y-o-y (*Figure 1*).

In April 2022, U.S. and German law enforcement conducted a joint operation to take down and sanction Hydra, the largest Darknet market, as well as a Russian crypto exchange. As a result, Darknet market revenue is also down significantly in 2022, and is currently 43% lower than where it was through July in 2021 (*Figure 2*).

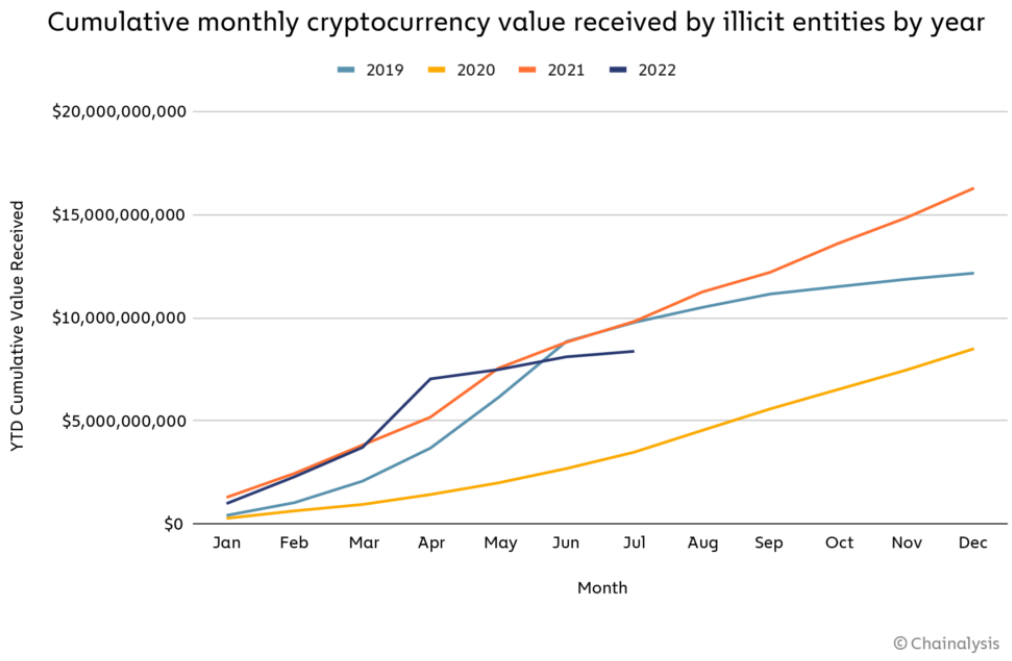

Figure 1

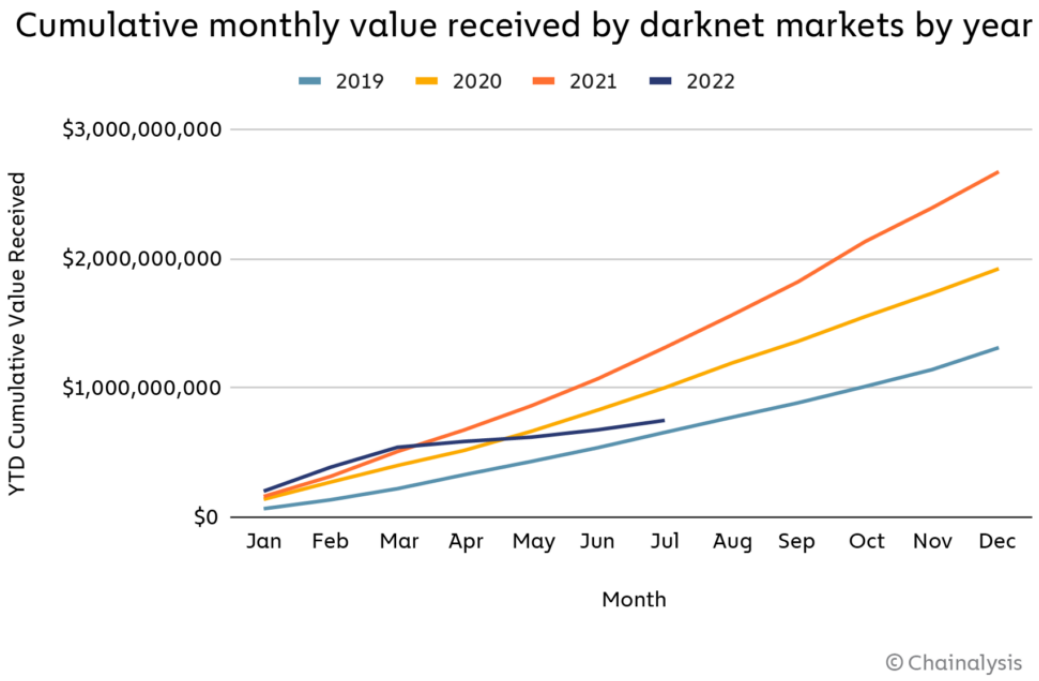

Figure 2

Chainalysis stated it well when they said "the decline in darknet market revenue — and indeed, cryptocurrency value received by all criminal categories — following Hydra's shutdown shows the tangible impact of law enforcement's growing ability to fight cryptocurrency-based crime."

In addition to Darknet revenue, revenue from cryptocurrency scams are also falling, with the cumulative number of individual transfers to scams so far in 2022 the lowest since 2018. As the market has matured in recent years, the number of inexperienced users has likely fallen, making participants somewhat less susceptible to scams, which have cost naive users in billions in fraud in previous years.

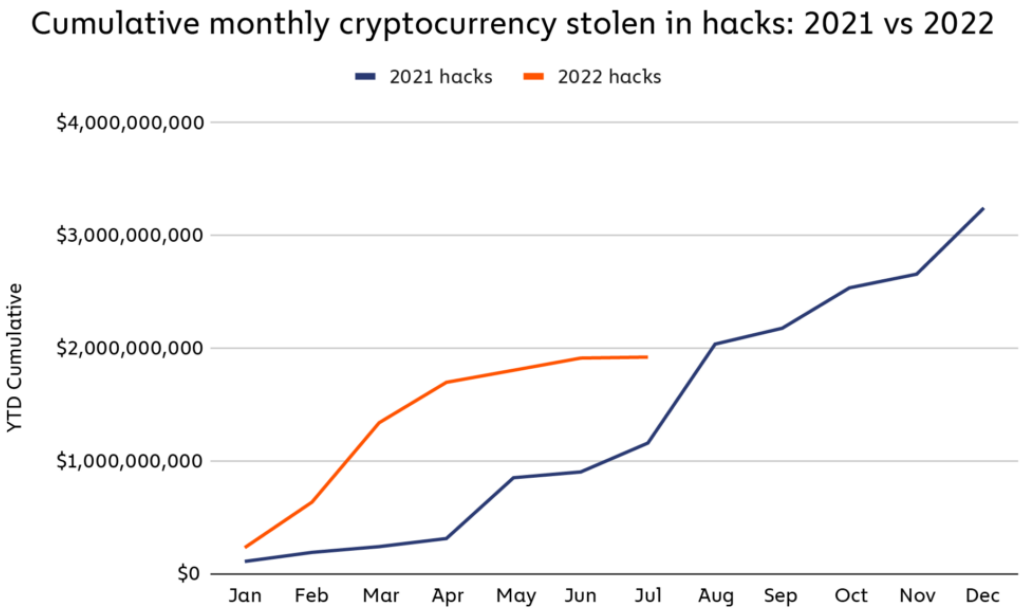

Figure 3

However, revenue from hacking and theft are on the rise, principally driven by the dramatic increase in funds stolen from decentralized finance ("DeFi") protocols. This portion of the crypto-ecosystem inherits the "move fast and break things" ethos of silicon valley and their open source code is a ripe target for hackers to exploit and reap very large bounties.

The Lazarus Group (a hacking group controlled by the North Korean intelligence service) is the dominant exploiter of DeFi protocols, stealing an estimated $1 billion from these insecure projects in the first half of 2022 alone. Their use of the Ethereum-based mixer Tornado Cash to launder their stolen assets led OFAC to issue an unprecedented sanction of smart contract public addresses (in addition to the standard entity and property designations on the SDN list), an act that precipitated widespread consternation in the crypto-community and will likely be challenged in U.S. court.

Sanctions Evasion

It has been a common refrain that Bitcoin is a useful tool for rogue nations and entities to evade U.S. sanctions. This concern was raised in the immediate aftermath of Russia's invasion of Ukraine, but thus far, no significant use of Bitcoin to evade sanctions has materialized.

On March 2, 2022, Attorney General Merrick Garland announced the launch of Task Force KleptoCapture, an interagency law enforcement task force dedicated to enforcing sanctions and restrictions placed in response to Russia's actions in Ukraine. The mission of the Task Force will specifically include "targeting efforts to use cryptocurrency to evade U.S. sanctions, launder proceeds of foreign corruption, or evade US responses to Russian military aggression." OFAC issued guidance in an FAQ released on March 11, 2022, confirming that compliance with the expansive Russian sanctions is required "regardless of whether a transaction is denominated in traditional fiat currency or virtual currency."

It is unlikely that any cryptocurrency will provide a meaningful way for the Russian institutions, officials, oligarchs subject to specific sanctions to accomplish widespread asset flight, and no illicit flows have been seen to-date.

FinCEN states that it is unlikely that the Russian government can use cryptocurrency to mitigate or circumvent the impact of sanctions in any meaningful way, finding that "large scale sanctions evasion using CVC by a government such as the Russian Federation is not necessarily practicable." Additionally, FinCEN Acting Director Him Das said the agency had "not seen widespread evasion of our sanctions using methods such as cryptocurrency." This echoes the sentiment expressed by Carol House, Director of Cybersecurity at the National Security Council, when she stated, "[t]he scale that the Russian state would need to successfully circumvent all U.S. and partners' financial sanctions would almost certainly render cryptocurrency as an ineffective primary tool for the state."

U.S. Treasury officials themselves "are not overly worried about crypto undermining the effort to choke off the Kremlin's access to capital. Laundering large amounts of money through a dizzying array of digital wallets and exchanges is expensive, time-consuming and would likely be visible in the broader crypto market, given the massive investment portfolios of individuals and institutions named in the sanctions."

Strategic Principles

Several strategic principles should guide the US approach to crafting digital asset policy, that mitigate risk, while maximizing the promise of these emerging technologies.

1. A balanced, net assessment of the broad implications of Bitcoin and other digital assets networks is required to ensure that the U.S. takes maximum advantage of these technologies while mitigating risks.
2. Policy should not be narrowly drawn to address a particular risk (e.g., illicit finance) without considering the larger strategic interests at stake.
3. We should learn from the encryption battles of the 90s and avoid making premature, heavy-handed policy decisions that overweight apparent national security interests at the expense of open innovation and technology leadership.
4. Policy making processes should recognize that truly decentralized digital asset networks by definition have no leader or governing body and are likely to be underrepresented in the political process relative to other stakeholders with a more concentrated interest.
5. As the world's most attractive capital market, our cross-border tax policies and accounting rules should make it easier for US entities to receive Bitcoin as investment and as payment for exports.

President Biden rightly framed this decade as "a battle between the utility of democracies in the 21st century and autocracies… We've got to prove democracy works." The values of an open society, now under threat by revanchist authoritarian states, rest at the center of our strategic interest in promoting liberal democracy around the world. Open digital assets that empower individuals can help advance the cause of freedom, stymie the objectives of authoritarian adversaries, and help advance a core national security interest. Peer-to-peer systems like Bitcoin represent the essence of autonomy, voluntary cooperation, and liberal values that our country was built on.

As with any new technology, bad actors will exploit these systems and their growing pains will result in new policy questions and challenges. However, the U.S. should take a strategic view for the long-term promise these technologies hold and work to encourage their flourishing in our country and around the world.

Sincerely,

David Zell, Co-Executive Director, Bitcoin Policy Institute
dz@btcpolicy.org

Matthew Pines, National Security Fellow, Bitcoin Policy Institute
pines@ks.group