# THE CRISIS OF CRYPTOCURRENCY: EXECUTIVE BRANCH AUTHORITY TO ADDRESS THE WORLD'S MOST POTENT FINANCIAL THREAT

*Robert J. DeNault*[*]

## INTRODUCTION

The golden age of technology brought novel threats to American national security along with it. Chief among them are non-state actors who pose grave threats to civilians, governments, and civilized society. These non-state actors, sometimes referred to colloquially as terrorists, perpetrate violence on innocent people, force economies into disarray, and apply immeasurable pressure to the norms that serve as cornerstones of global peacekeeping. Since the September 11th terrorist attacks in 2001, the Executive Branch of the United States Government has undertaken ground, air, naval and cyber operations to address this new concern. One significant area of interest for the Executive Branch has been regular endeavors to cut off terrorist financing abroad and within the U.S.[1] But emerging technologies now threaten to subvert those efforts and endanger the national security of the U.S. economy in the process. The Executive faces difficult questions about how to maintain the integrity of the U.S. economic system in light of rampant money laundering and ransomware attacks—hallmarks of terrorists' digital presence—made possible by anonymous cryptocurrency transactions. Bitcoin, the most popular cryptocurrency format in the world, has become a preferred means for terrorists[2] and money launderers to obtain cash quick.

There is no question the Executive Branch must address the national security threat Bitcoin poses. Evaluating which constitutional tools the Executive Branch possesses to counter Bitcoin's role in facilitating terrorist and criminal activity in the U.S. economy invokes legal questions on the limits of Executive Branch authority and constitutional rights of American

---

[*] Robert J. DeNault is a juris doctor candidate and Class of 1986 Scholar enrolled in the Duke University School of Law Class of 2021. A special gratitude is owed to Major General Charles J. Dunlap, Jr. USAF for his help an assembling this paper.

[1] *See e.g.*, Nathan Reiff, *Leaked Photo Suggests NSA Infiltrated Cryptocurrencies*, INVESTOPEDIA (Jun. 25, 2019), https://www.investopedia.com/news/did-nsa-infiltrate-cryptocurrencies-0/; Juan Zuarte, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, Sept. 10, 2013 (Public Affairs 1st Ed.).

[2] Anthonia Isichei, *FBI Director: Cryptocurrencies Pose Threats to National Security*, BTC MANAGER (Nov. 8, 2019), https://btcmanager.com/fbi-director-cryptocurrencies-national-security/?q=/fbi-director-cryptocurrencies-national-security/&.

citizens. This paper will address the national security concerns Bitcoin presents and offer a viable course of action available to the President to counter its utilization by terrorists and bad actors. It will then analyze legal sources of authority to pursue such actions, and finally evaluate constitutional arguments that may cut against the constitutionality of Executive actions against cryptocurrency.

## I. BACKGROUND: THE CRYPTOCURRENCY THREAT

Common understanding of cryptocurrency is sparse. Most Americans, including lawyers, hear words like "Bitcoin," "blockchain" and "cryptocurrency" and make a variety of incorrect assumptions about their meaning. However, the basics of cryptocurrency are not extraordinarily complex. Bitcoin's fundamental structure itself presents a national security concern.[3] The best explanation of Bitcoin starts with an academic paper which served as the foundation for all cryptocurrency theory.[4] This paper outlines the basic formula all cryptocurrencies now rely upon, and describes Bitcoin as a "purely peer-to-peer version of electronic cash" which allows "electronic payments to be sent directly from one party to another without going through a financial institution."[5] Put plainly, Bitcoin allows users to send money to one another but never withdraw funds, write a check, or register an expense on a bank account.

There is no record of money moving between parties except a small series of numbers in a long list, called a blockchain. As Bitcoin transactions happen across the world each day, a network "timestamps transactions by hashing them," creating a lengthy record that "cannot by changed without redoing the proof-of-work"[6] that renders review by people like tellers unnecessary. Each hash contains a series of unique numbers, flanked on either side by *another* specific set of numbers representing the Public Key of the sender and the Private Key of the recipient. As signatures pile up, hashes are bundled into a long chain—a blockchain. Bitcoins are made of blockchains, and the value of coins is determined by how frequently users

---

[3] Billy Bambrough, *Bitcoin and Crypto Suddenly Branded a 'National Security Issue'*, FORBES (Jul. 16, 2013), https://www.forbes.com/sites/billybambrough/2019/07/16/Bitcoin-and-crypto-suddenly-branded-a-national-security-issue/#52920ed21a59.

[4] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*,

[5] *Id.* at 1.

[6] *See id.* (explaining the non-corruptible character of Bitcoin by asserting that a long series of numbers cannot be altered by fraudulent actors without undermining the entire chain, making such fraud impossible) (emphasis added).

cash out their Bitcoins and the size of transactions.[7] Alarming estimates indicate these transactions involve at least $72 billion in criminal activity.[8]

An anonymous, unregulated banking system poses a litany of national security concerns. Public Key and Private Key signatures might sound like avenues for removing anonymity in Bitcoin transactions, but the signatures are actually specially formulated to keep identities hidden. The academic paper addresses Bitcoin's inability to offer the kind of privacy guaranteed by "traditional banking," due to the necessity to announce transactions publicly in the blockchain system.[9] However, the paper asserts "privacy can still be maintained by breaking the flow of information in another place: *keeping public keys anonymous*."[10] The blockchain records a person sending money to someone else, but does not display information about who is involved in the transaction. The paper compares this to "information released by stock exchanges," in that the time and size of transactions are public, but the identities of parties involved remain private.[11] However, the key difference here is that stock transactions are regulated by the Securities and Exchange Commission; there is no similar regulator for cryptocurrency. The academic paper also instructs users on how to keep transactions *more* invisible, recommending new key pairs be used for every transaction to "keep them from being linked to a common owner."[12]

The Bitcoin system is essentially shadow banking, and as such it is easy to understand how it quickly transformed into a stock trade for criminal activity. Almost all ransomware attacks—which involve government or private sector tech operations being hacked, locked down and made inoperable until ransoms are paid—include Bitcoin as the preferred means of demand payment.[13] Cities like Baltimore, [14] Newark, Atlanta, and San Diego[15] have all been struck by ransomware attacks where hackers shut down government operations and demanded payment in Bitcoin. Ransomware

---

[7] *Id.* at 3. (emphasis added).

[8] Hillary J. Allen, $ =<euro>=BITCOIN?, 76 MD. L. REV. 877, 904 (2017).

[9] Nakamoto supra, n. 4 at 9.

[10] *Id.* (emphasis added).

[11] *Id.*

[12] *Id.*

[13] Coveware Q1 Ransomware Marketplace Report, *Ransom amounts rise 90% in Q1 as Ryuk increases*, COVEWARE, https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases (last visited Oct. 26, 2019).

[14] *See* Ian Duncan, *Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts*, THE BALT. SUN (May 29, 2019) https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html.

[15] Grand Jury Indictment, *U.S. v. Savandi*, *et al*, Nov. 26, 2018 (D.C. N.J.).

attacks are on pace to become a "$1 billion a year crime,"[16] threatening to create an environment where sophisticated organizations must pay hackers in order to keep shareholders happy and customers content. But ransomware attacks are not the only cryptocurrency activity threatening the integrity of the U.S. economy. International money laundering now involves a significant amount of Bitcoin. In 2018, a private firm estimated $2.5 billion of criminal money was laundered using Bitcoin payments.[17] That same private firm indicated that, should anti-money laundering regulations be enacted with cryptocurrency in mind, "opportunities to launder cryptocurrencies [would] be greatly reduced."[18] It is not a viable option for the U.S. to do nothing about these threats, a reality Treasury Secretary Steven Mnuchin recognized this year.[19]

It did not take long for terrorists and global criminals to see Bitcoin's potential. Silk Road, an internet marketplace for drugs and weapons which was taken down in 2013, conducted all financial transactions through Bitcoin.[20] Peripheral actors deepened these problems by developing methods to make Bitcoin transactions *more* obscured. In 2014, a group of coders calling themselves 'unSystem' released an application called 'Dark Wallet.'[21] The program thwarted "impending Bitcoin regulations that seek to tie . . . identities to Bitcoin ownership."[22] Framing the program as one designed to avoid pesky transparency requirements, one of the creators described the app's genuine purpose during a debate in New York City: "[I]t's just money laundering software."[23] The program mixes two transactions, one innocuous and one unlawful, to create confusion.[24]

---

[16] Survey Report, "Understanding the Depth of the Global Ransomware Problem," MALWAREBYTES, https://go.malwarebytes.com/OstermanRansomwareSurvey.html (last visited Oct. 26, 2019).

[17] CipherTrace, *Cryptocurrency Anti-Money Laundering Report*, CipherTrace Cryptocurrency Intelligence, (2018).

[18] *Id.*

[19] *See* White House Press Briefing by Treasury Secretary Steven Mnuchin on Regulatory Issues Associated with Cryptocurrency, July 15, 2019, *available at* home.treasury.gove/news/press-releases/sm731 (emphasizing U.S. national security concerns with Bitcoin as based upon the preserving the "integrity" of the economy).

[20] Aaron Brantly, *Financing Terrorism Bit by Bit*, COMBATING TERRORISM CTR. AT WEST POINT, Vol. 7 No. 10 (Oct. 2014).

[21] Andy Greenberg, *'Dark Wallet' is About to Make Bitcoin Money Laundering Easier than Ever*, WIRED (Apr. 29, 2014), https://www.wired.com/2014/04/dark-wallet/.

[22] *Id.*

[23] Debate with Cody Wilson on Design and Violence I: Open Source, Museum of Modern Art (Mar. 27, 2014).

[24] *See* Greenberg *supra*, n. 21 (explaining how Dark Wallet obfuscates user identities by pairing transactions so suspicious ones cannot be isolated).

Similarly, Hamas, the militant Palestinian group designated a terrorist organization by the U.S., recently developed a website for the express purpose of receiving donations via Bitcoin.[25] The website contains an explicit instruction video which explains how to acquire and send Bitcoin without tipping off authorities.[26] Months earlier, British journalist Richard Hall reported other jihadi groups connected to al-Qaeda in Syria were also promoting Bitcoin in order to raise funds.[27] These were not the first instances of terrorist reliance on Bitcoin. "As early as 2014," Hall writes, "ISIS supporters had posted tutorials online about how to make Bitcoin donations to the group."[28] Terrorist use of Bitcoin funds do not yet account for a majority of Bitcoin transactions or even a majority of criminal activity associated with Bitcoin.[29] However, authorities stress an increase in the sophistication of terrorist reliance on Bitcoin in recent months.[30] By summer 2019, U.S. government agencies acknowledged Bitcoin was being utilized by terrorist groups and hostile nation states[31] around the world. Treasury Secretary Steve Mnuchin noted in a White House press briefing that cryptocurrencies "have been exploited to support billions of dollars in illicit activity like cybercrime, tax evasion, extortion, ransomware, illicit drugs, human trafficking" in addition to serving as a funding source for terrorist groups.[32] Characterizing Bitcoin in a new way, Secretary Mnuchin answered a critical question: "This is indeed a national security issue."[33]

While Mnuchin acknowledged technological innovation is important, he noted the "overriding goal" of the U.S. is to maintain the integrity of the

---

[25] Nathaniel Popper, *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*, N.Y. TIMES, Aug. 19, 2019 at B1, *available at* http://www.nytimes.com/2019/08/18/technology/terrorists-Bitcoin.html.

[26] *Id.*

[27] Richard Hall, *Jihadists in Syria Turn to Bitcoin for Needed Funds*, THE INDEPENDENT (Apr. 17, 2019) https://www.independent.co.uk/news/world/middle-east/Bitcoin-syria-terror-funding-al-qaeda-hayat-tahrir-al-sham-a8873996.html.

[28] *Id.*

[29] *See* Popper *supra*, n. 25 (characterizing the amount of Bitcoin traced to terrorists as being in the "tens of thousands").

[30] *Id.*

[31] See, e.g., Jason Brett, U.*S. Authorities Arrest Virgil Griffith for Teaching Cryptocurrency and Blockchain in North Korea*, FORBES (Nov. 29, 2019), https://www.forbes.com/sites/jasonbrett/2019/11/29/us-authorities-arrest-virgil-griffith-for-teaching-cryptocurrency-and-blockchain/#7dd8ad3142cb; Daniel Palmer, *North Korea Plans Bitcoin-Like Cryptocurrency to Sidestep Sanctions*, COINDESK (Sept. 19, 2019), https://www.coindesk.com/north-korea-plans-Bitcoin-like-cryptocurrency-to-sidestep-sanctions.

[32] White House Press Briefing *supra* n. 19.

[33] *Id.*

American financial system and protect it from abuse.[34] Widespread criminality is now associated with Bitcoin—so much so that the SEC, CFTC, FinCEN recently issued a joint statement reminding financial operators that transactions involving cryptocurrencies like Bitcoin are subject to anti-money laundering laws and obligations.[35] In the face of a rapidly growing national security threat to the U.S. economy, the Executive Branch is faced with a complicated, dangerous and impersonal adversary.

## II. A PROPOSED EXECUTIVE ACTION

The President could dismantle Bitcoin by issuing two separate Executive Orders. The first would authorize the use of force by the U.S. military in the form of cyberattacks against Bitcoin platform operators, Bitcoin ATM's which provide cash for Bitcoin, and blockchain technology. The second would authorize the U.S. Department of Treasury to ban Bitcoin websites and financial services from U.S. access. Each order would be designed to neutralizing Bitcoin's operations domestically and abroad. This paper will analyze sources of power the Executive Branch might rely on to issue such orders, as well as Constitutional arguments against them.

## III. LEGAL ANALYSIS OF EXECUTIVE ACTION

Executive Branch powers[36] in the field of national security have been interpreted differently by different presidents.[37] Some presidents interpret their national security authority as inherent to the job, virtually unbounded except by Constitutional prohibitions; others take the position that Executive authority can only be derived from specific language in the Constitution or a statute passed by Congress.[38] In evaluating the former proposition, the President's inherent authority here centers on two assertions. First, the President's unique foreign relations powers give him the latitude to protect

---

[34] *Id.*

[35] Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets, Oct. 11, 2019, *available at*, https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets.

[36] John Reed Stark, *Roadmap for President Trump's Crypto-Crackdown*, John Reed Stark Consulting (Aug. 6, 2019), https://corpgov.law.harvard.edu/2019/08/06/a-roadmap-for-president-trumps-crypto-crackdown/.

[37] *Compare* William H. Taft, *Our Chief Magistrate and His Powers*, 139–140 (1925) ("the President can exercise no power which cannot be fairly and reasonably traced to some specific grant of power") *with* Theodore Roosevelt, *Autobiography*, 372 (1914) ("[It is] not only [the President's] right but his duty to do anything that the needs of the Nation demand, unless such action [is] forbidden by the Constitution or by law").

[38] *Id.*

American financial interests that intersect with global affairs. Second, the President's Commander-in-Chief authority enables him to protect the U.S. from terrorist attacks. Both justify elimination of Bitcoin as a legitimate threat to national security.

Most presidents instead interpret their authority in the latter, more limited fashion and prefer to justify their actions with specific statutory delegations from Congress. Fortunately for the President, Congress has lavished the Executive Branch with an assortment of tools to fight terrorism, keep American markets free from fraud and criminality, and prevent foreign powers from exploiting vulnerabilities in the American economy. Most relevant for our purposes are the Patriot Act,[39] the Authorized Use of Military Force (AUMF),[40] and the International Economic Emergency Powers Act (IEEPA).[41] Given the extensive body of evidence that Bitcoin facilitates terrorist activity and rampant criminal behavior, the Executive Branch could use these statutes collectively to justify targeting Bitcoin.

The following sections will explore each of these arguments in turn, beginning with the inherent power considerations, followed by potential sources of statutory authority. Ultimately, the conclusion will aggregate all these powers to determine that the Executive Branch likely has authority to eliminate Bitcoin for national security purposes.

### *A. The President's Inherent Powers*

#### 1. The Foreign Relations Power

Alexander Hamilton, in the early days of the U.S., extrapolated on the rationale for the powers granted to the Executive Branch:

> "Energy in the executive is a *leading character of good government*. It is essential to the *protection of the community against foreign attacks*: It is not less essential to the steady administration of the laws, to the *protection of property against those irregular and high handed combinations* which sometimes interrupt the ordinary course of justice, to the security of liberty against the enterprises of ambition, of faction and of anarchy."[42]

---

[39] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT Act) Act of 2001*, 107 P.L. 56, 115 Stat. 272 §§ 311–330 (2001).

[40] Authorized Use of Military Force, 50 U.S.C. § 1541–49 (2019).

[41] International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1708 (2019).

[42] THE FEDERALIST NO. 70 (Alexander Hamilton) (emphasis added).

Hamilton's early focus on protecting American communities and property from foreign "high handed combinations" suggests a wide capacity for the Executive Branch to act in instances where those concerns are implicated.[43] The contours of this authority must be understood in light of the "marked difference between foreign affairs and domestic affairs," the former of which grants the President a wider latitude to act in the nation's best interests.[44]

One president quietly stretched the bounds of Executive national security authority in foreign relations and economics. In 1971, President Richard Nixon signed a series of executive orders which transformed the American economic system. They included wage and price freezes, surcharges on imports, and, most importantly, the unilateral cancellation of international convertibility of the U.S. dollar to gold.[45] Nixon's Treasury Secretary justified the implementation of the Executive Orders as an effort to disrupt the "[well-manicured] playing fields of international finance,"[46] espousing a rationale which invoked the President's foreign relations powers implicating national security concerns.[47] Nixon's orders were intended to close the window for "foreign governments [to] exchange their dollars for gold."[48] Nixon's rationale bears resemblance to Hamilton's notion of an Executive responsibility to protect against high-handed combinations such as a flood of dollar-gold conversions meant to crash U.S. markets.[49]

Bitcoin in many respects resembles a high-tech attempt to return to the days of the gold standard.[50] Bitcoin proponents are wary of central bank management and intervention in the valuation of money, similar to advocates of a return to gold-backed currency.[51] Creators of Bitcoin have also limited

---

[43] *Id.*

[44] United States v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936).

[45] Paul Lewis, *Nixon's Economic Policies Return to Haunt the G.O.P.*, N. Y. TIMES, Aug. 15, 1976 at 93, *available at*, https://www.nytimes.com/1976/08/15/archives/nixons-economic-policies-return-to-haunt-the-gop-nixons-economic.html.

[46] *Id.*

[47] Stephen Dycus, Arthur Berney, William Banks, Peter Raven-Hansen, & Stephen Vladeck, *National Security Law*, p. 54, Aspen Casebook Series (2016) (connecting the President's national security powers to foreign relations).

[48] Sandra Kollen Ghizoni, *Nixon Ends Convertibility of US Dollars to Gold and Announces Wage/Price Controls, Federal Reserve History*, FEDERAL RESERVE HISTORY, https://www.federalreservehistory.org/essays/gold_convertibility_ends (last visited Dec. 5, 2019).

[49] THE FEDERALIST NO. 70 (Alexander Hamilton).

[50] *See* Allen *supra*, n. 8 at 904.

[51] *Id.* at 904–5. The number of Bitcoins that may be released is capped at 21,000,000, which ensures that it is "not susceptible to the type of monetary policy intervention central banks deploy to maintain price stability." *Id.*

the supply of available Bitcoins without regard to increases or decreases in demand for other goods and services, a quintessential defect of gold that was a key rationale for abandoning it.[52] Whether or not these kinds of defects are properly characterized as within the ambit of Presidential national security authority depends in large part upon Bitcoin's vulnerability to hostile foreign interference. For example, if the growth of cryptocurrency in the American economy was exacerbated by powers like China and Russia,[53] the President could make a compelling argument that such growth presented a direct threat to the U.S. national security in that it exposed the U.S. markets to interference by those countries.[54] The President could make a secondary argument that Bitcoin subverts Nixon's departure from the Bretton Woods system and re-entangles American economics with foreign activity which threatens U.S. national security and encroaches upon the President's foreign relations authority.[55]

Unregulated cryptocurrencies usurp the role of payment systems traditionally provided by banks, warranting fear that they represent international shadow banking[56] or property exchanges built on criminal activity.[57] As noted above, studies estimate between 2013–2016 there was a five-fold increase in large-scale illegal operations on the Bitcoin blockchain.[58] Bitcoin remains almost entirely unregulated despite its rapid

---

[52] *Id.* at 905.

[53] Anna Baydakova, *Millions in Crypto is Crossing the Russia-China Border Daily. There, Tether is King*, COINDESK (Jul. 30, 2019), https://www.coindesk.com/tether-usdt-russia-china-importers.

[54] *See* Lewis *supra*, n. 45 at 93 (writing that Treasury Secretary John Connally acknowledged part of the rationale behind Nixon's Executive Orders was to disrupt international actors' abilities to affect the American market).

[55] *See generally* U.S. v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936). In *Curtiss-Wright*, Justice Sutherland quoted Chief Justice John Marshall speaking to the House of Representatives in 1800: "the President is the sole organ of the nation its external relations, and its sole representative with foreign nations." *Curtiss-Wright* is oft-cited for the proposition that the "President . . . manages [American] concerns with foreign nations." While the extent of what Presidential activity is covered by *Curtiss-Wright* is subject to debate, President Nixon's Executive Orders withdrawing the U.S. from the Bretton Woods system have never been subject to a constitutional challenge.

[56] *Id.* at 911.

[57] Sean Foley, Jonathan R. Karlsen, Talis J. Putnin, *Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrency?*, REVIEW OF FINANCIAL STUDIES, (Dec. 14, 2018). The authors conclude up to $76 billion of illegal activity per year involves Bitcoin and comprises 46% of Bitcoin transactions.

[58] Rachel Wolfson, *Tracing Illegal Activity Through the Bitcoin Blockchain to Combat Cryptocurrency-Related Crimes*, FORBES (Nov. 26, 2018), https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-Bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/#51fe90a833a9.

growth in popularity in the wake of the 2008 economic crisis.[59] The more cryptocurrency seizes upon the traditional role played by banks, the greater the domestic harm is posed by cryptocurrency's increasing dependency on criminal and terrorist activity.[60] As Hamilton noted, amongst the President's core duties is the obligation to protect the people from the assault of anarchy.[61] It is difficult to imagine something more anarchical than a currency whose value is based in large part on the crimes it facilitates.

Yet valid arguments could be made that Congress specifically left cryptocurrency unaddressed as it reauthorized the Patriot Act in 2019,[62] meaning they did not want to delegate authority to the President to address it. This argument is likely to fail in light of recent Supreme Court decisions affirming the Executive Branch enjoys some inherent, exclusive powers in the sphere of foreign relations, and can even contradict Congress in some instances.[63] If the President enjoys unilateral authority to contradict Congress on some foreign relations matters, it is likely he maintains authority to protect the American economy where Congress is *silent* on a particular matter.[64] Furthermore, Nixon's unilateral abandonment of the gold standard was never challenged by Congress, indicating Congress historically accepted its validity.[65] The U.S. national security interest in keeping its economy free from dependence on foreign criminal activity goes in many respects to the root of Presidential authority.[66] It is the President's duty to avail himself of every appropriate means not forbidden by law to ensure federal laws are faithfully executed.[67] The complex system of American financial law empowers the federal government to collect taxes, prevent money laundering, discourage fraud, and weaken criminal markets, all in order to diminish illicit financial behavior. These objectives are subverted by cryptocurrencies which

---

[59] *See* Allen *supra*, n. 8 at 911.

[60] *Id.*

[61] THE FEDERALIST NO. 70 (Alexander Hamilton).

[62] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT Act) Act of 2001*, 107 P.L. 56, 115 Stat. 272 §§ 311–330 (2001).

[63] *See* Zivotofsky ex rel. Zivotofsky v. Kerry, 135 S. Ct. 2076 (2015) (holding that the President alone effects the formal act of recognition).

[64] The Steel Seizure Case, (Jackson, J. concurring) ("Congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility.")

[65] *Id.* (Frankfurter, J. concurring) (acknowledging that consistent practices known to Congress and left unaddressed are likely valid exercises of Executive authority).

[66] CONST., Art. II. sec. 3. The phrase "[the President] shall take Care that the Laws be faithfully executed" has been construed by the Supreme Court to require the President to "avail himself of every appropriate means not forbidden by law" in fulfilling his duties. *U.S. v. Tingey*, 30 U.S. 115, 117 (1831).

[67] Tingey, 30 U.S. 115, 117.

facilitate $72 billion in criminal activity.[68] The President's responsibility to protect the economy under his foreign relations power serves as a compelling source of legal authority for the Executive Branch to eliminate Bitcoin.[69]

2. Commander-in-Chief Power

The President's Commander-in-Chief powers are never spelled out in the Constitution. Instead, they exist under the rubric of the Commander-in-Chief clause and the gloss history U.S. national security history painted upon it.[70] Presidents are bound by the Constitution to respond to attacks or invasions from foreign parties without waiting for special legislative authority,[71] suggesting the Executive Branch plays a critical role in repelling potential threats to the country. *The Prize Cases* present a salient example of Presidential authority to disrupt international economic activities where those activities finance a war effort of an enemy of the U.S..[72] President Lincoln, in an attempt to stymie nascent fortification of Confederate armies, ordered a blockade of Southern ports. The system worked like this: U.S. naval vessels intercepted ships traveling to and from ports, warning them not to do so again.[73] If they returned, naval vessels captured them and sold them for prize money.[74] The Court held this exercise of power was legitimate where evidence indicates a state of war exists between the U.S. and another entity.[75]

Declared enemy terrorist groups in Syria, Iraq and elsewhere promote the use of Bitcoin to followers in order to fund terrorist attacks.[76] The President, in his role as Commander-in-Chief,[77] can explore the elimination

---

[68] Allen *supra* n. 8 at 911.

[69] Michael del Castillo, *Trump Executive Order Banning a Cryptocurrency Could Mutate into Far-Reaching Law*, FORBES (Sept. 14, 2019), https://www.forbes.com/sites/michaeldelcastillo/2019/09/14/trump-executive-order-banning-a-cryptocurrency-could-mutate-into-far-reaching-law/#169155ee55d2.

[70] Stephen Dycus, Arthur Berney, William Banks, Peter Raven-Hansen, & Stephen Vladeck, *National Security Law*, p. 81, Aspen Casebook Series (2016).

[71] The Prize Cases, 67 U.S. 635, 668. (1863). While *The Prize Cases* dealt with the Civil War and not a foreign invasion, the Court took particular care to state that "whether the hostile party be a foreign invader, or States organized in rebellion, it is none the less a war." *Id.*

[72] *See id.* (holding that the President "had a right, *jure belli*, to institute a blockade of ports in possession of the States in rebellion.")

[73] Dycus, et al *supra*, n. 47 at 82.

[74] *Id.*

[75] *See* The Prize Cases, 67 U.S. 635, 671 ("The proclamation of the blockade is itself official and conclusive evidence to the Court that a state of war existence which demanded and authorized a recourse to such a measure, under the circumstances peculiar to the case.")

[76] *See* discussion *supra*, Sec. II. (highlighting the proliferation of Bitcoin as terrorist financing in recent years).

[77] *Report on the Legal and Policy Frameworks Guiding U.S.' Use of Military Force and*

of Bitcoin operators as a means of destroying a financial resource for terrorists. Bitcoin's similarities to the seized trading vessels in *The Prize Cases* is notable. As Americans intentionally or inadvertently send Bitcoin payments to terrorists in places like Syria[78] and Palestine,[79] the President must consider whether a digital blockade is a legitimate military objective. The fact Bitcoin operators are not themselves terrorist organizations is not of particular significance; the merchants on trade vessels in *The Prize Cases* were not Confederate rebels, either.[80] Consistent with the prerogatives cited by President Lincoln, an executive order to eliminate Bitcoin could be justified on the grounds that it targets a funding source for an enemy against whom we are in a state of war. However, it is important to note that, in this gray area of international law, President Barack Obama acknowledged that "great care is taken to adhere to the principle of proportionality [the legal principle requiring force be proportional to the threat it targets] in both planning and execution to ensure that collateral damage is kept to a minimum."[81]

The President's capacity to launch cyberattacks, especially against non-military targets, is not boundless. The President's discretion is limited by Department of Defense rules of engagement regarding cyber operations.[82] Cyberattacks are not permitted to destroy computer systems ostensibly part of "civilian infrastructure;" however, such systems can lawfully become targets if they can be categorized as a legitimate "military objective."[83] Any cyber operation that would "seize or destroy enemy property" would have to be "imperatively demanded" by necessities of war.[84] Bitcoin cyberattacks fall into these categories, so it is unlikely the President enjoys unilateral authority to launch them based solely on Commander-in Chief authority.

Under *The Prize Cases* framework, a President enjoys authority to order the military to disrupt economic activity benefiting an enemy of the U.S. with whom the U.S. is in armed conflict.[85] Department of Defense guidelines allow the President explore cyberattacks against cryptocurrency operators as a non-violent means of cutting off terrorist funding, but also limit the extent he may target civilian infrastructure. While inherent authority to

---

*Related National Security Operations*, p. 7, White House (Dec. 2016) (hereinafter "White House Report").

[78] Hall *supra*, n. 27.

[79] Popper supra, n. 25.

[80] The Prize Cases, 67 U.S. 635, 669.

[81] *See* White House Report *supra*, n. 77 at 21.

[82] Dep. Of Defense, Law of War Manual, § 16.5.1: Cyber Operations and *Jus in Bello* (June, 2015).

[83] *Id.*

[84] *Id.*

[85] The Prize Cases, 67 U.S. at 669.

protect the U.S. economy and cut off terrorist funding are based on national security concerns, it is unlikely those authorities alone justify targeting *all* Bitcoin operations.

### *B. The President's Statutory Powers*

The President's inherent powers are supplemented by a series of statutory delegations to the Executive Branch. The most relevant statutes are the Patriot Act, the AUMF, and the IEEPA.

#### 1. The Patriot Act

The Patriot Act, a wide-ranging piece of legislation enacted in the wake of September 11th, is oft-referred to with derision and scorn by Americans. This is in large part due to intelligence gathering powers it grants to Executive Branch agencies, viewed by many U.S. citizens with suspicion. However, intelligence gathering was not the only focus of the legislation. The Patriot Act generated a sea change in the area of money laundering law. It implemented requirements for banking institutions to flag transactions for money laundering, making it harder to mask the identities of individuals or groups conducting transactions or opening accounts in the U.S. and prohibiting U.S. institutions from doing business with foreign shell banks.[86] The legislation increased criminal penalties for financial crimes, specifically with an eye toward combatting corruption,[87] directly associating these concerns with the broader U.S. national security interest of maintaining the integrity of the American economy.

The legislation had practical elements, too. Financial institutions were given legal immunity from liability for disclosure of suspicious transactions or activity to authorities,[88] incentivizing cooperation between banks and the government in the fight against terrorism and global organized crime. Importantly for the purposes of this paper, one section was devoted entirely to "MSB's"—money services businesses.[89] These include "any person who engages as a business in an informal money transfer system or any network of people who engage in the business in facilitating the transfer of money domestically or internationally outside of the conventional financial

---

[86] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT Act) Act of 2001*, 107 P.L. 56, 115 Stat. 272 §§ 311–330 (2001).

[87] *Patriot Act* § 329 introduced criminal penalties for bribery and targets corrupt officials with potential prison sentences of 15 years.

[88] *Id.* § 351.

[89] *Id.* § 359.

institutions system."[90] These words, written years before the inception of cryptocurrency, presciently apply the Patriot Act to channels of financial exchange which might operate entirely outside the banking system—i.e., Bitcoin.

Other provisions impose reporting requirements on financial institutions where currency or coin value received by an individual or entity exceeds $10,000.[91] However, the provision defines currency as "foreign currency" or "any monetary instrument with a face amount of not more than $10,000."[92] The IRS defines Bitcoin and other forms of cryptocurrency as property, not currency.[93] While property could be regarded as a monetary instrument, the federal government has not applied this provision to Bitcoin transactions exceeding $10,000.

The Patriot Act armed the Executive Branch with an array of tools to fight criminal activity like money laundering. The Patriot Act bestows authority upon the President to determine whether an "organization" has "planned, authorized, aided, or engaged in such hostilities or attacks" against the U.S and subject it to scrutiny under new restrictions.[94] The President could determine specific Bitcoin operators aided terrorists by facilitating Bitcoin transactions to fund attacks. However, terrorists use apps like DeepWallet[95] (the app described by its creators as "money laundering software")[96] to make it harder for law enforcement to follow transactions. DeepWallet targets one of few transparent elements of Bitcoin—public signatures, discussed above[97]—by "integrating laundering . . . into every payment its user makes."[98] Cody Wilson, the man behind the money laundering software comment, admits his app enables crimes but simply explains that in his view, "[l]iberty is a dangerous thing."[99]

Liberty to create apps is important, yes; but the right to be liberated from terrorists, money launders, drug cartels and organized crime is probably more compelling. While freedom to act creates some danger to all, to invoke the merits of liberty while defending the enabling of criminal activity flies in

---

[90] *Id.*

[91] *Patriot Act* § 365 (amending 53 U.S.C. 31).

[92] *Id.*

[93] Notice 2014-21, *Section 4. Frequently Asked Questions*, Internal Revenue Service (2014).

[94] *Patriot Act* § 106.

[95] *See* Greenberg *supra* at n. 21.

[96] *Id.*

[97] *See* discussion *supra* at Section II.

[98] *See* Greenberg *supra* at n. 21. Explaining how DarkWallet functions, Greenberg writes: "Every time a user spends Bitcoins, his or her transaction is combined with that of another user chosen at random who's making a payment around the same time."

[99] *Id.*

the face of the very system which pairs liberty with justice for all. There are several ways the President could rely on the Patriot Act to support Executive Orders designed to protect the liberty of innocent citizens from terrorist and criminal organizations. The President could order the IRS to change its definition of cryptocurrency from property to currency, and then subject it to the provisions of the Patriot Act which require banks to obtain information about withdrawals of over $10,000.[100] The President could define cryptocurrency exchanges as MSB's and utilize that characterization to take targeted action toward them to obstruct their proliferation. This qualification may also assist the President in utilizing his powers under another statute, the IEEPA, which will be discussed later. Finally, the President could go so far as to block availability of apps like DeepWallet in the U.S., consistent with Patiot Act provisions which empower him to punish those who conspire to assist money launderers.[101]

It is almost certain that a Presidential ban on cryptocurrency would invite arguments that such an action violates separation-of-powers principles, as the President appears to be "legislating" from the Executive Branch.[102] While it is true the Patriot Act does not enumerate a total prohibition of alternative financial systems, its purpose and design support the assertion that Congress has determined money laundering and terrorist financing to be critical national security issues. This reality would be helpful to the President, as he could argue that it places him well within the second category of Justice Jackson's famous separation-of-powers framework from *Youngstown Sheet & Tube Co. v. Sawyer*.[103] In his *Youngstown* concurrence, which is not formal law but has informed Supreme Court separation-of-powers jurisprudence, Justice Jackson contemplated three categories of authority for Presidential acts: acts specifically authorized by statute or the Constitution, acts not specifically authorized by any statute or language but justified by concurrent authority between the Executive Branch and Congress, and acts contrary to Congressional intent without authorization from Congress but authorized by exclusive Presidential power.[104] It appears President's acts to target Bitcoin exist in the second category, as Congress created a framework for addressing money laundering concerns and did so to empower the Executive Branch to combat terrorism and financial crime. It is critical the President argue he remains within the second category of Justice Jackson's framework—and,

---

[100] *Patriot Act* § 365 (amending 53 U.S.C. 31).

[101] *Id.* § 359.

[102] *See* The Steel Seizure Case, 343 U.S. 579, 579 (1951) (a divided opinion regarding the President's ability to conduct legislative-like activity in the national security context).

[103] *Id.* at 634 (Jackson, J. concurring).

[104] *Id.*

more importantly, outside of dangerous limitations of the third.[105] Given Justice Jackson's prose that any actual test of power is likely to depend on "imperatives of events" rather than abstract theories of law, the threats Bitcoin poses would play a significant role in evaluating the Presidential activity in question and would likely lead to a favorable result for the Executive Branch.[106] However, any approach to the third category would almost certainly result in a loss for the Executive Branch under *Youngstown*.[107]

The Patriot Act, in providing an expansive means to the Executive Branch to address national security concerns like terrorist financing and money laundering, offers significant support for the argument the Executive Branch has legal justification for eliminating Bitcoin. The provisions—taken in conjunction with the other statutes and the President's inherent authorities discussed *supra*—would probably convince the Supreme Court the President's acts were justified under the second category of the *Youngstown* framework.

2. The AUMF

The broadest authority the President has to launch military cyberattacks against Bitcoin operators based on national security concerns is the Authorized Use of Military Force (AUMF). The AUMF was passed by Congress three days after September 11th.[108] The joint resolution authorizes the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, committed, or aided" the September 11th attacks, or "harbored such organizations or persons, in order to prevent any future acts of international terrorism against the U.S.."[109] While the AUMF does not authorize the President to use force against all groups that commit terrorist acts, the U.S. military has taken action against a number of groups under the AUMF's authority, including al Qaeda, the Taliban, al-Shabaab, and individuals associated with al Qaeda in Libya and Syria, as well as the Islamic State (IS).[110]

Courts broadly construe the AUMF to cover Executive actions fundamentally accepted as an "incident of war."[111] The Supreme Court determined the AUMF authorizes the Executive Branch to engage in the

[105] *Id.* (describing the third category of Executive power as the "lowest ebb" of Presidential authority).
[106] *Id.*
[107] *Id.*
[108] Authorization for Use of Military Force, 115 Stat. 224 (2001).
[109] AUMF § 2(a).
[110] White House Report *supra*, n. 77 at 5.
[111] Hamdi v. Rumsfeld, 542 U.S. 507, 519 (2004).

detention of U.S. citizens who associate with enemy combatants or organizations covered by the AUMF.[112] In *Hamdi v. Rumsfeld*, the Supreme Court held that such detentions were a "fundamental incident of waging war."[113] Subsequent cases permitted similar detentions, in part because the Government developed a process for evaluating them.[114] That the Court considers an activity as restrictive as detention of U.S. citizens by the Executive Branch as authorized by the AUMF likely envelopes similar, less-restrictive activities as authorized.

If the President enjoys the power to detain U.S. citizens abroad who associate with terrorist groups under the AUMF, he or she almost certainly possesses authority to order cyberattacks on cryptocurrencies which regularly fund with terrorist groups. As noted by the Court in *The Prize Cases*, blockades of enemy resources itself suggests the existence of a state of war,[115] suggesting such acts are *de facto* fundamental incidents of waging war.[116] Recent efforts by President Trump to maintain control over the oil fields in Syria[117]—civilian infrastructure related to economics, not warfare—signal that the Executive Branch has already adopted this understanding. While it is true cryptocurrency disruption might affect innocent civilians in a way that oil field seizure would not, the seizure of productive oil fields will likely disturb oil markets in a direct manner, too. If courts showed an unwillingness to reject the President's seizure of oil fields, they would probably be unwilling to address the targeting of cryptocurrencies.

3. IEEPA

Perhaps the most compelling statutory authorization the President could rely on to justify Executive action banning Bitcoin and dismantling its international operators is the International Emergency Economic Powers Act (IEEPA).[118] The act empowers the President to "investigate, regulate or

---

[112] *Id.*

[113] *Id.*

[114] *See* Hamdan v. Rumsfeld, 548 U.S. 557, 678 (2006) (referring to legislation that created an avenue "for consideration of petitioner's claims" which did not exist under prior case law to justify detention).

[115] *See* The Prize Cases, 67 U.S. 635, 671 ("The proclamation of the blockade is itself official and conclusive evidence to the Court that a state of war existence which demanded and authorized a recourse to such a measure, under the circumstances peculiar to the case.")

[116] Hamdi, 542 U.S. at 519.

[117] Scott Horsley, *Fact Check: President Trump's Plans for Syrian Oil*, NPR (Oct. 28, 2019), https://www.npr.org/2019/10/28/774053444/fact-check-president-trumps-plans-for-syrian-oil.

[118] *See* Pub. L. No. 95–223, 91 Stat. 1626 (codified as amended at 50 U.S.C. § 1701–08 (2019)).

prohibit" transactions in foreign exchange, transfers of payments between any banking institution, or the importing or exporting of currency by any person subject to the jurisdiction of the U.S..[119] The authority granted may be "exercised to deal with any unusual or extraordinary threat . . . to the national security, foreign policy, or economy of the U.S.."[120] The only other conditions that must be satisfied for the President to lawfully exercise these powers are that the U.S. be engaged in armed hostilities or undergo attack by a foreign country or foreign nationals, and that the President declare a national emergency with respect to such threat—a sharp signal of IEEPA's strong connection to national security concerns.

The IEEPA has already been used to block assets of terrorist organizations.[121] President George W. Bush issued an Executive Order which authorizes the Departments of Treasury and Justice to designate and block assets of entities that provide support, services, or assistance to, or otherwise associate with terrorists and terrorist organizations.[122] Both President Barack Obama and President Donald Trump renewed this Executive Order, and President Trump has relied on the IEEPA to introduce tariffs on Mexican exports in response to the national security threat of unlawful border immigration from Mexico.[123] President Trump has also relied on the IEEPA to pressure U.S. companies from doing business with China while he engages in a trade dispute.[124]

If tariffs on exports, an economic activity tangentially related to the issue of border security, qualify as a lawful target of Executive activity under the IEEPA, Bitcoin operators would almost certainly come within the scope of the President's powers. Cryptocurrency represents more than a threat to traditional banking; it poses an existential peril to the economy and government of the country. Could there exist a more potent threat to the U.S., a large republic composed of small republics which all govern through the passage of laws, than a global property exchange valued in large part by how much *unlawful* activity it enables? Criminals are already recognizing Bitcoin makes them untouchable: cybersecurity firms estimate ransomware attacks—in which 98% of attackers demand Bitcoin as payment[125]—are on track to

---

[119] 50 U.S.C. § 1702 (a)(1)(A) (2019).

[120] § 1701 (a).

[121] *Executive Order 13224*, 66 FR 49079 (Sept. 27, 2001).

[122] *Id.*

[123] *Trump to Hit Mexico with Tariffs in Anti-immigration Measure*, BBC NEWS (May 31, 2019), https://www.bbc.com/news/world-us-canada-48469408.

[124] *Trump can use these powers to pressure US companies to leave China*, REUTERS (Aug. 24, 2019) https://www.cnbc.com/2019/08/24/trump-can-use-these-powers-to-pressure-us-companies-to-quit-china.html.

[125] Coveware Q1 Ransomware Marketplace Report *supra*, n. 13.

become a $1 billion-per-year industry.[126]

Given the unusual and extraordinary statistics which paint a bleak picture of Bitcoin's facilitation of rampant international criminal activity, there is almost no doubt that the President could legitimately declare a cryptocurrency emergency and issue Executive Orders pursuing its disruption consistent with the IEEPA. Importantly, however, the President may not suspend the claims of those who might lose property or suffer harm by the operations.[127] If claims are efforts to establish liability and they do not focus on property within the jurisdiction, they must be permitted to proceed through U.S. courts if they are otherwise legitimate.[128] Constitutional arguments against the President's authority to issue the Executive Orders would almost certainly follow, along with other lesser claims regarding property or monetary loss. These claims will be addressed in more detail in Section V.

4. Taking the Statutes Together

The IEEPA allows the President to declare a cryptocurrency emergency with respect to the financing of terrorism, or money laundering, or international criminal activities. He or she could then issue Executive Orders to disrupt blockchain activities, knock out Bitcoin operators and ban websites, banks and retailers from accepting Bitcoin payments. The question of whether the President would *need* to take the step of declaring such an emergency may be moot, given the existence of the AUMF and its recognition that the Executive Branch is already in a state of hostilities with terrorist actors. The existence of the AUMF signals the importance of terrorist groups as a national security concern of the U.S., further supporting the notion that threats posed by terrorist use of cryptocurrency are unusual and extraordinary.

The remaining question is whether Executive Orders targeting Bitcoin and cryptocurrency operators violate constitutional rights of American citizens. It is in this context that the Patriot Act does significant work. The President can argue moderate encroachment on constitutional rights is permissible here because the Executive Branch is fulfilling its

---

[126] Survey Report, *Understanding the Depth of the Global Ransomware Problem*, MALWAREBYTES, https://go.malwarebytes.com/OstermanRansomwareSurvey.html (last visited Oct. 26, 2019).

[127] *See* Dames & Moore v. Regan, 453 U.S. 654, (1981) (holding that although the IEEPA authorized President Carter's nullification of American-Iranian contracts, it cannot be read to authorize the suspension of American claims against Iranians in American courts because the "claims of American citizens against Iran are not in themselves transactions involving Iranian property" or "efforts to exercise any rights with respect to such property.")

[128] *Id.*

constitutional duties to enforce laws duly passed by Congress. With respect to constitutional authorization, the Executive Branch probably can issue the Executive Orders, empowered by a combination of inherent and statutory delegations to target cryptocurrencies based on national security concerns about terrorist financing and maintaining the integrity of the U.S. economy.

## IV. CONSTITUTIONAL ANALYSIS

Similar to any law passed by Congress, Executive Orders are subject to constitutional challenges by American citizens or organizations with proper standing and claims that meet federal jurisdictional requirements. A variety of individuals and entities would have proper standing—established when a party can show that a government action will cause them irreparable harm and immediate injury—to bring a claim seeking to undo the Executive Orders. A thornier legal question is whether the federal courts have jurisdiction over the issue. In the realm of national security law, Article III courts are reluctant to hear cases that implicate political questions; that is, issues that could be resolved between the other two branches of government or at the ballot box.[129] The Executive Branch would attempt to divert any claim from heading to the courts by arguing the question presented by the case is inherently political: Congress afforded the Executive Branch a variety of tools to address money laundering and terrorist financing, and the President's discretionary implementation of that authority is a political question. Whether the Supreme Court would agree remains unclear. However, the Court has, in recent years, avoided wading into separation-of-powers questions when the President is acting within the general scope of a statute.[130] This paper assumes a citizen has established proper standing and that there exists federal jurisdiction to hear arguments about the President's exercise of power targeting Bitcoin. This section focuses on constitutional arguments *against* the Executive Orders with reference to the above-mentioned case law and statutory authority to show how the arguments for and against the Orders may interact.

---

[129] Baker v. Carr, 369 U.S. 186 (1962). The Court articulated six factors that might invoke the political question doctrine, but the most frequently cited are the first two: "[p]rominent on the surface of any case held to involve a political question is found a textually demonstrable constitutional commitment of the issue to a coordinate political department; or a lack of judicially discoverable and manageable standards for resolving it."

[130] *But see* Dep. of Commerce, et al v. N.Y., et al, (2019) SLIP CITE (holding that the Executive Branch was not acting in good faith in its invocations of the political question doctrine to defend a citizenship question it added to the 2020 Census).

### *A. Due Process Concerns*

The strongest argument against the Executive actions dismantling Bitcoin and other forms of cryptocurrency is founded upon the due process clauses of the Fourth, Fifth and Fourteenth Amendments.[131] As noted above, the IRS categorizes cryptocurrency as property, not currency.[132] In the absence of any evidence connecting *specific* money to criminal activity, the seizure of property implicates due process protections against unreasonable seizures.[133] However, the hallmark of property protected by due process is an individual entitlement grounded in state law.[134] Most states have not yet enacted regulations addressing Bitcoin,[135] and while private sector entities increasingly accept Bitcoin as payment, there is no statutory scheme in any state which regulates Bitcoin as property or quantifies its value with legal recognition. The few states that have addressed Bitcoin are mixed on whether it is currency, data, or property.[136]

The federal government, however, has issued guidance on Bitcoin and in doing so legitimized it to some extent. The Financial Crimes Enforcement Network (FinCEN) published letters stating cryptocurrency issuers were money transmitters required to follow federal regulations.[137] A few states have attempted to enact similar comprehensive regulations, but in almost every instance the result was a total exodus of cryptocurrency operators,[138] a result the Executive Branch in this hypothetical would be pleased with. In light of the messy understanding about precisely what Bitcoin is—virtual currency or property—plaintiffs must argue their Bitcoin amounted to property seized unlawfully by the government and hope the Supreme Court

---

[131] U.S. CONST. Am. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); Am. V ("No person shall . . . be deprived of life, liberty or property, without due process of law"); Am. XIV ("No State shall . . . deprive any person of life, liberty or property, without due process of law; nor deny to any person equal protection of the laws.").

[132] Notice 2014-21 *supra* n. 93.

[133] Burden of Proof and Presumptions in Tracing Currency, Bank Account or Cash Equivalent to Illegal Drug Trafficking so as to Permit Forfeiture, or Declaration as Contraband, Under State Law, 104 A.L.R.5th 229, § 11. (emphasis added).

[134] Logan v. Zimmerman Brush Co., 455 U.S. 422, 430–31 (1982).

[135] Matthew E. Kohen and Justin S. Wales, *State Regulations on Virtual Currency and Blockchain Technologies*, CARLTONFIELDS, https://www.carltonfields.com/insights/publications/2018/state-regulations-on-virtual-currency-and-blockchain-technologies (last visited Nov. 29, 2019).

[136] *Id.*

[137] *Id.*

[138] *Id.*

agrees with them, a tall order for nine justices not known for their familiarity with emerging technology.

Ultimately the government could counter this issue in several ways. First, the Treasury Department could offer a window for Bitcoin owners to cash out their property before implementing the ban. While Bitcoin owners might complain that the announcement of the ban spun the price of their property into a downward spiral, there is no legitimate claim over every new law which negatively affects a business's value. An accommodation window would go a long way to quell due process concerns, because it would allow the government to argue the property was never *seized*, but rather subject to financial regulations prohibiting internet operators and financial entities from facilitating its conversion to cash. While removing the ability to cash out would likely itself implicate due process concerns,[139] the due process required of the government in that instance would be diminished by the lower value of the mere ability to cash out as opposed to the value of the coin itself.

Engaging in hypothetical due process arguments about a stream of data which no government has adequately or clearly defined is near-impossible to do. It is likely plaintiffs would be able to make out some due process right to a cash equivalency of their cryptocurrency; however, offering a window to convert their property to cash before eliminating that possibility would likely meet due process requirements under the Fourth, Fifth and Fourteenth Amendments.

### *B. First Amendment Issues*

Bitcoin proponents also wield the First Amendment as an shield from regulation of cryptocurrency. The creators of DeepWallet, the money-laundering software app designed to further obfuscate Bitcoin's already-deficient efforts at transparency,[140] invoked First Amendment principles to defend their program shortly after acknowledging it was designed to facilitate criminal activity.[141] Scholars advocating First Amendment protections for source code, however, acknowledge that it, "like any other language or form of speech, may receive full, partial or no First Amendment coverage" similar to obscene materials or the solicitation of crimes.[142] The question presented here is twofold: does First Amendment protection exist for source code; if so,

---

[139] *See* Logan, 455 U.S. at 430–31 ("[T]he types of interests protected as property are varied and, as often as not, intangible, relating 'to the whole domain of social and economic fact.'")

[140] Argument *supra*, Pt. II.

[141] Greenberg *supra* n. 21.

[142] Jorge R. Roig, *Decoding First Amendment Coverage of Computer Source Code in the Age of Youtube, Facebook, and the Arab Spring*, 68 N.Y.U. ANN. SURV. AM. L. 319, 328 (2012).

does that protection apply when source code facilitates transactions on the internet? While the answer to the first is probably some (albeit nuanced) protections for source code, the answer to the second is much more challenging to discern.

Despite characteristics which distinguish it from spoken or written language, source code can be written, read, and understood by humans.[143] Furthermore, technical compositions like patent applications[144] or even brief statements like trademarks[145] are considered speech for First Amendment purposes, albeit heavily regulated speech. Source code generates software that is utilized for expressive or associational purposes, similar to a large body of protected First Amendment activity like parades, protests, or other forms of organizational conduct.[146] Comparable to spoken language, however, some source codes are more connected to First Amendment principles than others. The source code for Facebook or Twitter, which creates a forum for First Amendment expression, presents a close connection to free speech principles. The source code for a banking app, however, does not implicate the same values. In light of the Supreme Court's extensively deferential First Amendment jurisprudence, it is unlikely it would conclude source code is *entirely* undeserving of First Amendment protection. However, the Court is specific in its First Amendment jurisprudence[147] and would probably stop short of extending all First Amendment protections to source code which creates Bitcoin or apps like Dark Wallet.

Which raises the second question: whether the First Amendment also applies to cryptocurrency once it goes live as a transaction platform. Plaintiffs could argue Bitcoin and cryptocurrency embody a disagreement with traditional banking that should enjoy protection under the First Amendment. While the Court has shown remarkable deference to individual and corporate First Amendment rights,[148] it is unlikely a "purely peer-to-peer version of

---

[143] *See* Roig *supra*, n. 142 at 327.

[144] Matal v. Tam, 137 S.Ct. 1744, 1757–58 (2017).

[145] Id.

[146] *See, e.g.*, Hurley v. Irish-Am. Gay, Lesbian and Bisexual Group of Bost. 515 U.S. 557 (1995) (parade permitting to exclude LGBT organization); Tex. v. Johnson, 491 U.S. 397 (1989) (protest flag burning protected by First Amendment); Spence v. State of Wash., 418 U.S. 405 (1974) (privately owned flag display protected expression).

[147] *Compare* Wooley v. Maynard (determining New Hampshire license plates containing the phrase "Live Free or Die" amounted to government speech triggering traditional First Amendment analysis) *with* Walker v. Tex. Div., Sons of Confederate Veterans Inc. (alternatively concluding that similar displays trigger "forum analysis" in the event private parties submit the designs).

[148] *See, e.g.*, Am. Legion v. Am. Humanist Ass'n, 139 S. Ct. 2067, 2089 (permitting a Latin cross to stand on government land because it was a traditional monument to soldiers); Matal, 137 S.Ct. at 1757–58 (describing Walker as the "outer bounds of the government-speech doctrine" in permitting offensive trademarks); Burwell v. Hobby Lobby Stores, Inc.,

electronic cash" allowing "electronic payments to be sent directly from one party to another without going through a financial institution"[149] itself qualifies as First Amendment expression. The prohibition at issue here eliminates unregulated transactions, not the suppression of ideas. Bitcoin advocates are free to express support for cryptocurrency in whatever fashion they like—they are simply prohibited from offering financial services that use it. Software involving commercial transactions, not a forum for individual expression, is only distantly related to the "marketplace of ideas" which undergirds First Amendment jurisprudence.[150] The Court is unlikely to buy an argument that cryptocurrency itself represents a First Amendment expression.

Bitcoin advocates may argue transactions should be protected under the commercial speech doctrine. The First Amendment accords commercial speech with a limited measure of protection, commensurate with its "subordinate position in the scale of First Amendment values."[151] While commercial speech usually applies to advertising or warning labels, the Court may find the test useful in instances where technological commercial activity is implicated. The test for whether commercial speech should be protected is whether the imposed restriction is justified by a substantial government interest, whether it directly advances that interest, and whether it is more extensive than necessary to serve that interest.[152] The first and second prongs of the test are easily answered: the government's national security interest represents an "urgent objective of the highest order"[153] and is clearly advanced by a prohibition of cryptocurrency. Analysis of the final element, however, is less certain.

A total prohibition on cryptocurrency appears presumptively expansive, and Bitcoin advocates would cite a parade of horribles about thousands of lawful transactions now prohibited to indicate the overbreadth of the Executive Orders. However, the Court has permitted expansive statutory schemes, even when they implicate First Amendment concerns, where the government invokes national security interests to defend them.[154] For example, in *Holder v. Humanitarian Law Project*,[155] the Court addressed

---

573 U.S. 682, 736 (establishing religious exercise rights for for-profit corporations).

[149] Nakamoto supra, n. 4 at 1.

[150] *See* Walker v. Texas Div., Sons of Confederate Veterans, Inc., (2015) (holding that First Amendment rules are designed to protect the marketplace of ideas).

[151] Ohralik v. Ohio State Bar Ass'n. 436 U.S. 447, 456 (1978).

[152] Central Hudson Gas & Elec. V. Public Serv. Comm'n 447 U.S. 557, 564 (1980).

[153] Holder v. Humanitarian L. Project, 561 U.S. 1, 4–5 (2010) (writing that stopping terrorist funding is an interest of the "highest order" and likely a compelling one).

[154] *See id.* (affirming Congress's criminalization of non-monetary contributions to terrorist organizations and holding it did not violate the First Amendment).

[155] 561 U.S. 1.

whether a statute prohibiting material support for terrorism violated the First Amendment when applied to the transmission of supplies or aid.[156] Chief Justice Roberts explained that the government "considered and rejected the view that ostensibly peaceful aid would have no harmful effects" and that, where the government is justified in such a rejection, it may criminalize otherwise peaceful activity.[157] The notion that the activity might "[free] up other resources within the organization that may be put to violent ends" as well as the understanding that the activity lends legitimacy to foreign terrorist groups both justified the decision.

A similar rationale could be applied to cryptocurrency. Plaintiffs conducting transactions on unregulated blockchains associated with $72 billion in criminal activity[158] extend legitimacy to an enterprise which itself projects national security concerns. The Executive Branch may suffer in not having a particular Congressional statute to rely upon as it did in *Holder*, but for First Amendment purposes the main concern is whether the government action is authorized, not which branch is authorized to undertake it.[159] In the end, on both the question of source code protection that guarantees a right to operate cryptocurrency and a protection of cryptocurrency as expression, plaintiffs are unlikely to make a winning First Amendment argument here.

## CONCLUSION

There is abundant evidence indicating cryptocurrency poses two critical national security threats. Its operation as a cyber money laundering system implicates concerns about whether the government can successfully maintain the integrity of the American economy, and its rapidly rising use by terrorist organizations makes terrorist attacks more likely. The President would be derelict in his duty to protect from high-handed schemes and combinations[160] if he ignored the threats Bitcoin poses.

The President enjoys inherent foreign relations and Commander-in-Chief powers which, supplemented by statutory grants of authority to address money laundering, terrorism and international economic emergencies, present strong support for Executive authority in this area. While there is some merit to the argument that prohibiting cryptocurrency may violate due process, a simple cash out window would likely be enough to bring the action

---

[156] *Id.*
[157] *Id.*
[158] Allen *supra*, n. 8 at 904.
[159] *See* N. Y. Times Co. v. United States, 403 U.S. 713 (1971) (addressing Executive agency activity in a First Amendment analysis as "government power" indistinguishable from Congressional authority).
[160] Hamilton supra, n. 42.

into compliance with the Fourth, Fifth and Fourteenth Amendments. The First Amendment, while broad, does not offer the remedy Bitcoin proponents presume it will. Ultimately, the Executive Branch is well-positioned to act against cryptocurrency. It need only develop the requisite gumption to do so.