IS BITCOIN RAT POISON? CRYPTOCURRENCY, CRIME, AND COUNTERFEITING (CCC)

Eric Engle[1]

[1] JD St. Louis, DEA Paris II, DEA Paris X, LL.M.Eur., Dr.Jur. Bremen, LL.M. Humboldt. Eric.Engle @ yahoo.com, http://mindworks.altervista.org. Dr. Engle beleives James Orlin Grabbe was the author of bitcoin, and is certain that Grabbe issued the first digital currency and is the intellectual wellspring of cryptocurrency. *Kalliste!*

Introduction

Distributed cryptographic currency, most famously exemplified by bitcoin,[2] is anonymous[3] on-line currency backed by no state.[4] The currency is generated by computation ("mining"), purchase, or trade.[5] It is stored and tracked using peer-to-peer technology,[6] which

[2] *See* Jonathan B. Turpin, Note, *Bitcoin: The Economic Case for A Global, Virtual Currency Operating in an Unexplored Legal Framework*, 21 IND. J. GLOBAL LEGAL STUD. 335, 337-38 (2014) (describing how Bitcoin is a virtual currency).

> Bitcoin is supported by a distributed network of users and relies on advanced cryptography techniques to ensure its stability and reliability. A Bitcoin is simply a chain of digital signatures (i.e., a string of numbers) saved in a "wallet" file. This chain of signatures contains the necessary history of the specific Bitcoin so that the system may verify its legitimacy and transfer its ownership from one user to another upon request. A user's wallet consists of the Bitcoins it contains, a public key, and a private key. The public key is the address to which another party can send Bitcoins, and the private key is what enables the wallet's owner to send his own Bitcoins to someone else. As an analogy, the public key is your street address, and the private key is the key to your front door; others can send mail to your house with no more than your address, but no one can remove your belongings without your permission.

Id.

[3] *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 179 (2012) (commenting on the anonymity of Bitcoin).

> All Bitcoin transactions are public, but are considered anonymous because nothing ties individuals or organizations to the accounts that are identified in the transactions. However, individuals sometimes post account numbers online in ways that can be connected to their online identities. It might be possible, using statistical techniques and some identified accounts, to undo the anonymity of the system. Such unexpected and sudden exposure would obviously be deleterious to Bitcoin's value.

Id.

[4] *See id.* at 204 (commenting on the anonymous nature of digital currencies).

[5] *See* Pamela J. Martinson & Christopher P. Masterson, *Bitcoin and the Secured Lender*, 33 NO. 6 BANKING & FIN. SERVICES POL'Y REP. 13, 13-14 (2014) (listing ways in which one may obtain Bitcoin).

> Users may obtain Bitcoin in three basic ways:
>
> (1) New Bitcoin may be "mined" by users who opt to lend their

can be compared to file sharing[7] systems such as torrent.[8] Because cryptocurrency relies on distributed computing it does not require a central clearing house,[9] unlike government issued currency.[10] Be-

> computational resources to the Bitcoin network to perform the demanding computational work needed to support the system. In return for providing computational resources, such users are rewarded with new Bitcoin based on their share of computation used. These mining operations are increasingly conducted by large-scale GPU farms with multiple graphics processing units (which are better-suited than traditional CPUs (central processing units) to performing Bitcoin operations) working to perform the requisite calculations. The process is somewhat analogous to gold prospectors using their sweat and equipment to mine for gold, hence the term 'mining.'
>
> (2) Bitcoin can be purchased on specialized currency exchanges, in a similar manner to exchanging US dollars for, say, Euros. It should be noted that the exchange rate between Bitcoin and traditional currencies has fluctuated wildly in the past compared to the relatively small movements often seen between traditional currency pairs.
>
> (3) Goods and services may be sold in return for Bitcoin payments. An increasing number of businesses and individuals are conducting transactions in Bitcoin.

Id.

[6] *See* Grinberg, *supra* note 3, at 160 (explaining the technological component of bitcoin). "Bitcoin is a digital, decentralized, partially anonymous currency, not backed by any government or other legal entity, and not redeemable for gold or other commodity. It relies on peer-to-peer networking and cryptography to maintain its integrity." *See* Grinberg, *supra* note 3, at 160.

[7] *See* Vesna Harasic, Note, *It's Not Just About The Money: A Comparative Analysis of the Regulatory Status of Bitcoin Under Various Domestic Securities Laws*, 3 AM. U. BUS. L. REV. 487, 489 (2014) (providing examples of how bitcoin transfers are similar to music sharing systems). "Transfers occur through a network operated by thousands of computers, similar to a music-sharing system like iTunes or Spotify." *Id.*

[8] *See* Andy, *As Bitcoins Roll In, The Pirate Bay Adds Support for Litecoin Donations*, TORRENTFREAK (May 2013), *archived at* http://perma.cc/ZZ7J-ACJ5 (comparing Bitcoin's technology to torrents).

[9] *See* Harasic, *supra* note 7, at 488-89 (stating Bitcoin is the first type of currency that does not require a central payment system). "Bitcoin is the first digital currency that allows two parties to directly exchange single monetary units without going through a central payment system." *See* Harasic, *supra* note 7, at 488-89.

[10] *See* Paul H. Farmer, Jr., Note & Comment, *Speculative Tech: The Bitcoin Legal*

cause the transfer of funds is distributed, decentralized, and encrypted, it is in theory very difficult, and in practice nigh impossible, to trace the funds used in cryptocurrency transactions, whether to buyer or to seller.[11] Anonymity can be further strengthened by use of TOR[12]-onion proxies to obfuscate users' IP addresses[13] and tumbler software to render transactions obscurely.[14]

The anonymity cryptocurrencies offer enables criminality[15]

Quagmire & the Need for Legal Innovation, 9 J. BUS. & TECH. L. 85, 89 (2014) (contrasting the central clearing house requirements between government issued currency and cryptocurrency).

> In a traditional system, like those implemented through online banks and entities like PayPal, the third party keeps track of all of the transactions on their own servers. The public ledger of the Bitcoin network allows records to be kept without the third party, while the "cryptographic proof" maintained in the ledger allows individuals to engage in transactions without oversight. The intent of Bitcoins is based in the removal of a central third party that has control over, and the ability to manipulate, the entire system.

Id.

[11] *See* Conor Desmond, *Bitcoins: Hacker Cash or the Next Global Currency?* 19 PUB. INT. L. REP. 30, 32 (2013) (setting forth the difficulties in tracing funds used in cryptocurrency transactions). "The advantage of such exchanges is that there can be no way to trace the transaction; so long as an individual has the bitcoin program, one can accept the bitcoin anywhere on the planet." *Id.*

[12] *See* Jonathan Lane, *Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation*, 8 CHARLESTON L. REV. 511, 521-22 (2014) (elucidating how TOR networks further the anonymity of Bitcoin users).

[13] *See* Derek A. Dion, Note, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash*, 2013 U. ILL. J.L. TECH. & POL'Y 165, 166 (2013) (addressing how TOR maintains the anonymity of users through the frequently changing of IP addresses).

[14] *See* Lane, *supra* note 12, at 526 (noting how Silk Road used a complex payment system centered on Bitcoin).

> In addition to the anonymity provided by the Tor network and standard Bitcoin use, Silk Road used 'tumbler' software, which processed each payment through various 'dummy transactions' to further frustrate the ability of law enforcement to track a given transaction. This complex payment system, centered on Bitcoin, was the key to the site's success and its ability to maintain transactional anonymity among users.

See Lane, *supra* note 12, at 526.

[15] *See* Desmond, *supra* note 11, at 34 (discussing how Bitcoin's anonymous nature has attracted criminal activity). "[T]heir near anonymous and decentralized nature has also attracted criminals who value few things more than being allowed to oper-

such as arms sales, drug dealing,[16] human trafficking, murder-for-hire,[17] money laundering,[18] sale of child porn,[19] and sanctions busting.[20] Such a network of anonymity and criminality would also be

ate in the shadows." *See* Desmond, *supra* note 11, at 34.

[16] *See* James P. Gerkis & Serafima Krikunova, *Bitcoin and Other Virtual Currencies: Approaching U.S. Regulatory Acceptance,* 39-SPG ADMIN. & REG. L. NEWS 4, 8 (2014) (addressing how Bitcoin enables illegal activity); *see also* Lane, *supra* note 12, at 513-14 (acknowledging Bitcoin's influence on criminal activity).

[17] *See* Gerkis & Krikunova,*supra* note 16, at 8 (explaining how cryptocurrencies enables illegal activities).

> Silk Road was a secret marketplace where illegal goods and services could be purchased online with Bitcoins. The Silk Road operated on a Tor network, which allowed users to conceal their Internet Provider (IP) addresses and identities. Once users gained access to the network, they could purchase various drugs, guns, fake drivers' licenses, pirated media content, malware, computer-hacking services, and even murder for hire or 'hitmen.' As alleged, Ulbricht himself offered an undercover federal agent $80,000 to murder a Silk Road employee who was arrested and whom Ulbricht feared would expose the network. The SDNY criminal complaint charged Ulbricht with narcotics-trafficking conspiracy, computer-hacking conspiracy, and money-laundering conspiracy. The Maryland indictment included counts for conspiracy to distribute a controlled substance and for attempted witness murder and attempted commission of murder-for-hire. Total sales on the Silk Road purportedly generated the equivalent of about $1.2 billion in revenue and $80 million in commissions. The FBI has seized over $164 million worth of Bitcoin from the website. Still, even after the Silk Road shutdown, illicit transactions with Bitcoin have been reported to take place on alternate sites.

See Gerkis & Krikunova,*supra* note 16, at 8.

[18] *See* Desmond, *supra* note 11, at 34 (highlighting the difficulties in combating or tracing illegal financial transactions). "This concern about giving criminals a chance to easily disguise their transactions is a major problem for criminal enforcement agencies since their main weapons to combat organized crime activities is to 'follow the money.'" *See* Desmond, *supra* note 11, at 34.

[19] *See* Grinberg, *supra* note 3, at 161 (examining the dangers of child exploitation in regards to the Bitcoin currency). "Bitcoin's ability, like all digital and anonymous currencies, to facilitate money laundering, tax evasion, and trade in illegal drugs and child pornography." *Id.*

[20] *See* Nicole D. Swartz, Comment, *Bursting the Bitcoin Bubble: The Case to Regulate Digital Currency as a Security or Commodity*, 17 TUL. J. TECH. & INTELL. PROP. 319, 322 (2014) (exposing Iran for utilizing Bitcoin as a means of eluding government economic sanctions). "[B]itcoin is also used in Iran to evade currency sanctions." *Id.*

ideal for state sponsored terrorism.[21] Frankly speaking, the social costs and dangers posed by cryptocurrency far outweigh any potential use of cryptocurrency to fund U.S. or allied intelligence operations secretly as part of the CIA's "black" budget, which is the only potential upside to these facts that one could imagine from a governmental perspective.[22]

Supposedly, cryptocurrency would be at least as efficient as state issued currency[23] and make economies in the market[24] e.g., through reduced transaction costs.[25] However, that usually libertarian[26] argument ignores the central role of currency and finance law in affairs of State, as well as the state as regulator of legal transactions.[27] More "efficient" murder and more "efficient" illegal arms sales are obviously not in the interests of society or of the victims of crime.[28] The terrorist potential for cryptocurrency is bigger than for hawala

[21] *See* Jonathan Chester, *How Questions About Terrorism Challenge Bitcoin Startups*, FORBES (Dec. 2015), *archived at* http:// perma.cc/2VXQ-54T2 (linking Bitcoin with various terrorist operations).

[22] *See* Eamon Javers, *Special Ops grill bitcoin for its terror fight*, CNBC (Sept. 2014), *archived at* http://perma.cc/2RR7-YUY4 (stating that the U.S. government has a special interest in Bitcoin).

[23] *See* David Groshoff, *Kickstarter My Heart: Extraordinary Popular Delusions and the Madness of Crowdfunding Constraints and Bitcoin Bubbles*, 5 WM. & MARY BUS. L. REV. 489, 506 (2014) (analyzing the potential use of Bitcoin in governmental funding). "In the mid-1970s, Friedrich von Hayek, an economics Nobel laureate, stated '[t]here is no reason to doubt that private enterprise would, if permitted, have been capable of providing as good and at least as trustworthy coins." *Id.*

[24] *See id.* at 507 (asserting the implications of Bitcoin as an alternative to government tender).

[25] *See* Turpin, *supra* note 2, at 349 (citing other instances where reduced transaction costs inspired positive development). "In his seminal article, The Problem of Social Cost, Ronald Coase argued that where transaction costs are significant, they may lead to inefficient results if not controlled for." *See* Turpin, *supra* note 2, at 349.; *see also* Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 15-16 (1960) (pointing out that the pitfalls of disregarding transaction cost can lead to uncontrollable costs).

[26] *See* Groshoff, *supra* note 23, at 512 (articulating what the libertarian view regarding the favorable features of virtual currencies).

[27] *See* Groshoff, *supra* note 23, at 523 (displaying libertarians' dismissive attitude towards the state actors in legally regulating virtual transactions).

[28] *See Terrorists and Hawala Banking: Cheap and Trusted*, THE ECONOMIST (Nov. 22, 2001), *archived at* http://perma.cc/W4RG-6DEY (questioning whether virtual money transfers should be shut down after criminals and terrorist have used them because of the legal problems it causes).

banking.[29] Hawala banking, unlike cryptocurrency, must be halal i.e. in conformity with Islamic law.[30] Hawala banking has allegedly been used by terrorist groups such as Al Qaeda: Islamic law specifically prohibits targeting children and other non-combatants right in the Koran itself.[31] Many fatwas issued by respected imams have accordingly declared terrorism unislamic.[32] Cryptocurrency in contrast is not required to conform to Islamic law and unlike hawala banking is completely anonymous and more easily accessible to any terrorist group or organized crime.[33]

As well as enabling all types of crimes and presenting potential for terrorists anywhere, bitcoin[34] and similar distributed cryptocurrencies, such as dogecoin, present a cryptographic risk to United States' national security.[35] Bitcoins are generated and their transfer secured through distributed cryptography.[36] One may rightly ask just what "math problems" bitcoin and other cryptocurrencies are used to

[29] *See id.* (demonstrating how cryptocurrency could assist terrorism more than previous currency exchanges such as hawala).

[30] *See* Burhan, *Question & Answers: Halaal & Haraam*, ISLAMHELPLINE, *archived at* http://perma.cc/ZY9L-B77M (examining whether cryptocurrency is in accordance with Shariah or Islamic law).

[31] *See* Juan Miguel del Cid Gómez, *A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates*, 4 PERSPECTIVES ON TERRORISM 3, 3 n.4 (2010) (displaying how Al-Qaeda's use of hawala vast that it has become practically autonomous in funding their operations); *see also* Heba Aly, *Islamic Law and the Rules of War: More Than a Millennium Before the Codification of the Geneva Conventions, Most of the Fundamental Categories of Protection Could be Found in Islamic Teachings*, MIDDLE EAST EYE (Apr. 29, 2014), *archived at* http://perma.cc/L6PQ-WTRW (stating the Koran prohibits targeting civilians unless under "supreme emergency" to prevent the destruction of Islam).

[32] *See* Aly, *supra* note 31 (indicating that as recently as 2009, al-Qaeda has attempted to correct their members who target civilians).

[33] *See* Burhan, *supra* note 30 (summarizing the benefits of cyber currency over hawala and the lack of ramifications under Shariah or Islamic law).

[34] *See* Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and The Zero-Member LLC+*, 108 NW. U. L. REV. 1485, 1488 (2014) (stating that "[b]itcoin is a peer-to-peer software system, which means, practically speaking, that the entire system is made up of versions of the software that end-users download and run on their personal computers").

[35] *See id.* at 1494-95 (warning of the danger cryptocurrency can create without proper regulation). "This mining process has been explained as users 'solving math problems to earn coins.'" *See* Desmond, *supra* note 11, at 31.

[36] *See* Bayern, *supra* note 34, at 1490 (explaining how cryptography helps users prevent others from using their bitcoins).

solve.[37] Distributed computing to obtain massive brute force computing power for encryption[38] using a public key system[39] to encipher transactions,[40] the backbone of cryptocurrency, can also be used to encipher hostile messages, such as nuclear launching codes, submarine telecommunications, or terrorist attack orders, which renders friendly NSA decryption efforts more difficult than they need to be.[41]

[37] *See* LAISSEZ FAIRE CONTRIBUTORS, A MAN'S RIGHT TO HAPPINESS 96-97 (2013) (suggesting that Bitcoins were developed to verify online transactions by solving complicated algorithms).

[38] *See* Harasic, *supra* note 7, at 489 (explaining that as bitcoin users "use their computers to generate solutions, new bitcoins are issued. However, as the number of users in the system increases, the mathematical proofs become more difficult, which eventually slows down the production of bitcoins over time").

[39] *See* Harasic, *supra* note 7, at 489-90 (discussing how Bitcoin transactions are secured through a system of public and private key encryption).

> Bitcoins are sent from one computer to another through individual messages. Each message has a personal identifier called an 'address,' and each address has an associated pair of public and private keys, consisting of a string of numbers and letters. When an individual transfers bitcoins[,] to a recipient, the recipient sends his or her address to the transferor. The transferor then adds the address and the amount of bitcoins to the transfer message. Finally, the transferor signs the message with his or her private key, and announces the public key to the recipient for signature verification.

See Harasic, *supra* note 7, at 489-90.

[40] *See* Farmer, Jr., *supra* note 10, at 89-90 (explaining how public-key encryption protects user privacy).

> In order to maintain user privacy, all transactions are done through the use of public-key encryption. The encryption generates two different, but related, keys for each network user--one private and one public. The user retains one key and the other is made viewable by those initiating transactions. The private key is used to access funds and approve payments, while the public key is used to receive payments and as the means of record keeping for all transactions compiled in the blocks. If user A has a public key of X, user B has a public key of Y, and they engage in a transaction, it would be recorded as X to Y and not A to B. User A would use their private key to approve the transaction and user B would use theirs to access what was exchanged.

See Farmer, Jr., *supra* note 10, at 89-90.

[41] *See* Alan Brill & Lonnie Keene, *Cryptocurrencies: The Next Generation of Terrorist Financing?*, 6 DEF. AGAINST TERRORISM REV. 7, 16 (2014) (addressing how cryptocurrencies may be beneficial to national financial regulatory systems and detrimental to international security).

Massively distributed cryptanalysis can also be used to decipher U.S. transmissions.[42] Thus, cryptocurrency poses a threat as a potential massively distributed cryptanalysis engine.[43]

To underline the importance of cryptanalysis to United States national security: U.S. decryption of Japanese[44] ciphers and allies',[45] notably British and Polish,[46] decryption of German[47] ciphers was a

[42] *See* James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012), *archived at http://*perma.cc/47JP-9GVP (acknowledging the NSA's ability to cryptanalyze or break complex encryption systems within U.S. computer technology).

[43] *See* David Glance, *NAB's Bitcoin ban a symptom of the digital currency threat*, THE CONVERSATION (Apr. 10, 2014), *archived at* http://perma.cc/5MDV-C6VZ (comparing theoretical threats that cryptocurrencies pose to threats regarding real currencies).

[44] *See* Alberto-Perez, *How the U.S. Cracked Japan's 'Purple Encryption Machine' at the Dawn of World War II*, IO9 (Mar. 22, 2013), *archived at http://* perma.cc/X3D2-BU5Z (recalling that by using the broken "red" cipher as a crib, the U.S. was able to break the new, tougher, "purple" cipher).

[45] *See* WŁADYSŁAW KOZACZUK, ENIGMA: HOW THE GERMAN MACHINE CIPHER WAS BROKEN, AND HOW IT WAS READ BY THE ALLIES IN WORLD WAR TWO 99 (1984) (focusing on how Poland provided France, and then Britain, with a captured German ciphering machine, and British cryptographers led by Alan Turing at Bletchley Park were decisive in the battle of the Atlantic).

[46] *See* B. J. COPELAND, THE ESSENTIAL TURING: SEMINAL WRITINGS IN COMPUTING, LOGIC, PHILOSOPHY, ARTIFICIAL INTELLIGENCE, AND ARTIFICIAL LIFE: PLUS THE SECRETS OF ENIGMA 2 (2004) (providing an exhaustive account of the decisive role Turing played in British cryptanalysis along with the mathematics of cryptography). Hounded with criminal accusation and hormone "treatment" for his homosexuality after the war, Turing was in the end driven to suicide. *See* DAVID A. J. RICHARDS, THE RISE OF GAY RIGHTS AND THE FALL OF THE BRITISH EMPIRE: LIBERAL RESISTANCE AND THE BLOOMBURY GROUP 157 (2013) (explaining the end of Turing's life); *see also* ANDREW HODGES, ALAN TURING: THE ENIGMA 487 (2012) (recalling Alan Turing's death and legacy).

[47] *See* JAMES GANNON, STEALING SECRETS, TELLING LIES: HOW SPIES AND CODEBREAKERS HELPED SHAPE THE TWENTIETH CENTURY 69 (2001) (explaining how British codebreakers interpreted German orders, which allowed for British convoys to be given a timely warning in order to change their course of travel and avoid potential dangers). Although Germany's cryptographic branch, B-Dienst, did in fact break several merchant marine ciphers, most of the cryptographic war was won by the allied countries. *See* HERVIE HAUFLER, CODEBREAKERS' VICTORY: HOW THE ALLIED CRYPTOGRAPHERS WON WORLD WAR II 66-67 (2014) (summarizing how cryptanalysts from Germany and Britain deciphered codes during World War II). Whether due to "traitors" or defectors, bribery or treachery, the German intelligence services were systematically less effective, as can be seen by Hitler's execution of the head of the German intelligence service, Canaris. *See* ALAN

decisive factor in victory in World War II.[48] The ability to quickly decipher hostile messages contributed significantly to victory in battle after battle, most notably at Midway.[49] Consequently, the United States rightly regards cryptographic technology as military technology subject to strict export controls.[50] When German Chancellor Merkel called for a "no spy" treaty,[51] she betrayed herself as at best inexperienced and naïve,[52] at worst as deeply cynical.[53] Although she thought herself in "unchartered territory"[54] she was in reality "lost at

AXELROD, THE REAL HISTORY OF WORLD WAR II: A NEW LOOK AT THE PAST 54 (2008) (providing an overview of Wilhelm Canaris's role during World War II). While Soviet human intelligence efforts were always more effective than those of the Western countries, fascist human intelligence was even less effective than that of the Western allies. *See* MICHAEL WARNER, THE RISE AND FALL OF INTELLIGENCE: AN INTERNATIONAL SECURITY HISTORY 133 (2014) (setting forth the distinction between Soviet human intelligence and Western counterintelligence services throughout World War II); *see also* ABRAM N. SHULSKY & GARY JAMES SCHMITT, SILENT WARFARE: UNDERSTANDING THE WORLD OF INTELLIGENCE 18 (3rd ed. 2002) (recognizing the difficulty in operating Western intelligence services in communist countries).

[48] *See* DAVID KAHN, SEIZING THE ENIGMA: THE RACE TO BREAK THE GERMAN U-BOAT CODES 54-55 (Frontline Books 2012) (elaborating on the cipher systems used during World War II for decryption purposes); *see also* HY ROTHSTEIN & BARTON WHALEY, THE ART AND SCIENCE OF MILITARY DECEPTION 60 (2013) (explaining the decryption strategies used to win World War II).

[49] *See* PATRICK DELAFORCE, BATTLE OF THE BULGE: HITLER'S FINAL GAMBLE 200 (2014) (discussing the interpretation of Enigma machine messages); *see also* RICHARD A. MOLLIN, AN INTRODUCTION TO CRYPTOGRAPHY 13 (2000) (describing the decryption methods used by the United States to defeat Japan in the Battle of Midway).

[50] *See* License Exceptions, 15 C.F.R. § 740.17 (explaining the export and transfer laws regarding encryption items).

[51] *See* Philip Oltermann, *US will Not Enter Bilateral No-Spy Deal with Germany, Reports Media*, THE GUARDIAN (Jan. 14, 2014), *archived at* http://perma.cc/432J-JTEF (noting America's refusal to enter into a no-spy agreement with Germany).

[52] *See* Denver Nicks, *Merkel Denounces "Spying Among Friends,"* TIME (Oct. 24, 2013), *archived at* http://perma.cc/H624-P52D (portraying Chancellor Merkel's view that the U.S. and Germany are allies).

[53] *See id.* (emphasizing Chancellor Merkel's feelings about trust among allies and partners).

[54] *See* Jens Thurau, *PRISM Questions Dominate Merkel Presse*, DW NEWS (July 19, 2013), *archived at* http://perma.cc/9ZHU-K9TJ (highlighting the pros and cons of the Internet in the context of foreign relations). "Das Internet ist für uns alle Neuland, und es ermöglicht auch Feinden und Gegnern unserer demokratischen Grundordnung natürlich, mit völlig neuen Möglichkeiten und völlig neuen Herangehensweisen unsere Art zu leben in Gefahr zu bringen." *Id.* "The Internet

sea" when she claimed: "Spying among friends—that is a no go."[55] As a consequence of the German Federal Chancellor's theatrics[56]

is new-land for all of us, and it naturally enables both enemies and opponents to endanger our orderly democratic foundations with completely new possibilities and completely new methods." *Id.*

[55] *See* David Stubblebine, *Henry Stimson*, WORLD WAR II DATABASE (2016), *archived at* http://perma.cc/H5P6-D3N8 (providing a biography of Henry Stimson and his involvement in World War II). U.S. Secretary of State Henry Stimson closed the U.S. State Departments cryptology department in 1929 stating, "Gentlemen don't read each other's mail." *Id.* Chancellor Merkel could not have been ignorant of that statement, which she decidedly echoed in her claim that "Ausspähen unter Freunden—das geht gar nicht" ("Spying among friends—that is a no go"). *See Merkel ist ihr früheres Zitat zum Abhören nicht peinlich*, WAZ (Aug. 18, 2014), *archived at* https://perma.cc/WY7V-8RK6 (failing to comment on allegations that the BND regularly spied on Turkey in light of her earlier statements against spying on friendly nations). In reality, friendly espionage services spy on each other regularly for at least two reasons: first, to practice tradecraft in safety as tradecraft mistakes against allies do not have deadly consequences, and second, to detect infiltrators (so-called "moles"). It has been exposed that Germany in fact regularly spies on Turkey, Merkel's theatrical indignation against espionage among allies to the contrary. *Id.*; *see also* Spiegel Staff, *Targeting Turkey: How Germany Spies on Its Friends*, SPIGEL ONLINE INT'L (Aug. 18, 2014), *archived at* http://perma.cc/C4XJ-383M (revealing Germany's espionage activities on the Turkish government). That fact is completely unsurprising, given the problems of terrorism and criminality in the Islamic world. However, the spy scandal led to (or was caused by) the exposure of certain moles. *Id.*; *see also* Von Ulrich Claub, *Agenten im befreundeten BND ist ein Sonderfall*, POLITIK GEHEIMDIENSTEXPERTE DIE WELT (July 9, 2014), *archived at* http://perma.cc/9FA7-PTYF (noting that certain more than unfriendly infiltrators may also have been exposed and expelled). Speaking of expulsion, in the end, the CIA station chief in Berlin was expelled, an extremely unusual move. *Id.*; *see also* Allan Hall, *CIA Station Chief Expelled in Berlin Spy Row: Germany Orders Expulsion in Response to Two Cases of Alleged Spying*, DAILY MAIL (July 10, 2014), *archived at* http://perma.cc/WZ8P-5W7L (asserting two incidents regarding spying between the United States and Germany); *see also* David Robarge, *The James Angleton Phenomenon "Cunning Passages, Contrived Corridors": Wandering in the Angletonian Wilderness*, NOTE 4 (Jan. 26, 2010), *archived at* http://perma.cc/4QCS-2MBB (highlighting renounced spies, moles, and double agents throughout history, specifically James Angleton, whose double agent life was chronicled in the novel "The Wilderness of Mirrors").

[56] *See* Alexandra Hudson, *German MP Meets Snowden, Says He Is Willing to Come to Germany for Inquiry*, REUTERS (Oct. 31, 2013), *archived at* http://perma.cc/WZ7Z-PSLP (highlighting the willingness of German lawmaker, Hans-Christian Stroebele, to meet with Edward Snowden). For example, Germany's defense minister stated "it is clear that trust has been broken and this trust must be restored." *Id.* This requires official agreements on which we can depend," after his meeting with U.S. traitor, Edward Snowden. *Id.*; *see also Germany summons*

Germany is not a member of the UK-USA intergovernmental intelligence sharing agreement,[57] which, incidentally, is most definitely *not* a “no spy” agreement.[58] The German chancellor's demand for a no-spy treaty was entirely unrealistic.[59] The much touted “no spy” treaty was never even drafted - because it was totally unrealistic.[60] The U.S. is not a party to *any* “no spy” agreement,[61] not even with *Canada*.[62] In contrast, accession to the UK-USA intelligence sharing treaty *was* a realistic option for Germany, but is now off the table:[63] trust is a

U.S. ambassador over alleged spying on Merkel, CBS NEWS (Oct. 24, 2013), *archived at* http://perma.cc/6PR7-CJLD (discussing German authorities allegations that American intelligence was targeting Chancellor Angela Merkel’s cellphone). The German defense minister was only echoing the very same line as the German Chancellor “such trust now has to be built anew.” *Id.*; *see also Arrival and door-step Merkel (DE)*, NEWSROOM (Oct. 24, 2013), *archived at* https://perma.cc/WRK5-FFAH (speaking about building new trust). Anyone who wishes to dredge through the video of Merkel's speech may find it on the TVNEWSROOM website. *Id.* Obviously, meeting with a spy who has defected to Russia does not help in building trust between countries. For example, Russia has once again covertly invaded a neighboring country, annexing part of that country. Trust has been broken, no?

[57] *See* Carly Nyst & Anna Crowe, *Unmasking the Five Eyes: Global Surveillance Practices,* GISWATCH.ORG (Nov. 2013), *archived at* http://perma.cc/L2NU-CUAP (observing the UK-USA agreements and their implications). The authors here are likely pseudonymous. *Id.*

[58] *See id.* (highlighting the misconceptions that surround the UK-USA agreement).

> While UKUSA is often reported as having created a 'no spy pact' between Five Eyes states, there is little in the original declassified documents from the 1940s and 1950s to support such a notion. Crucially, first and foremost, no clause exists that attempts in any form to create such an obligation.

Id.

[59] *See* Oltermann, *supra* note 51 (noting that the United States does not monitor its communications with Germany, thus making a request for a “no-spy” agreement moot).

[60] *See id.* (implying that a “no spy” agreement was unlikely to occur between the United States and Germany despite an effort to draft one because of the lack of trust between the countries).

[61] *See* Ashley Deeks, *I Spy, You Spy, We All Spy?*, LAWFARE (Sept. 6, 2013), *archived at* http://perma.cc/7XQR-TUYM (refuting notions that the United States has participated in “no spy” agreements with other countries).

[62] *See* Kady O'Malley, *From the Order Paper Question Archives: Do the "Five Eyes" Watch Each Other?,* CBC NEWS (Oct. 10, 2012), *archived at* http://perma.cc/Q4EJ-QANA (indicating Canada will neither admit nor deny their current or past participation in the “Five Eyes” agreement).

[63] *See* Patrick Donahue & John Walcott, *Berlin Spying Prompted U.S. Offer Too*

two-way street.[64]

This shows how important signals intelligence (SIGINT) and cryptography are to the United States.[65] When we understand that cryptocurrency is based on massively distributed cryptography and thus poses an implicit threat to U.S. cryptanalysis, banning cryptocurrency such as bitcoin becomes an even more obvious policy prescription.[66]

Not only is cryptocurrency a threat to national security, cryptocurrency is a bad investment: bitcoin combines elements of a Ponzi scheme [67] with market manipulation[68] and pump-and-dump.[69] Sever-

Late to Sway Merkel, BLOOMBERGBUSINESS (July 12, 2014), *archived at* http://perma.cc/K22V-7ZVL (inferring Germany and the United States may have once agreed to share spying information, but the idea quickly subsided). Although an intelligence sharing agreement was always possible, the United States has not been a party to any "no spy" treaty. *Id.* Furthermore, the "no spy" treaty text was never proposed by governments or even discussed among academics. *Id.*

[64] *See id.* (recognizing the loss of trust between the United States and Germany in regards to surveillance as a result of the spying scandal).

[65] *See* Ronald S. Moultrie, *Signals Intelligence*, NSA (Mar. 2, 2015), *archived at* http://perma.cc/UG35-UYG5 (defining "Signals Intelligence" as intelligence obtained from electronic signals and systems, like communication, radars, and weapon systems).

[66] *See* Brill & Keene, *supra* note 41, at 12, 16 (summarizing the process of buying and creating cryptocurrencies, as well as their potential threat to cryptanalyst).

[67] *See* Complaint at 1, Sec. Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2014 U.S. Dist. Lexis 130781 (E.D. Tex. 2014) (articulating the Securities and Exchange Commission's case against Bitcoin for participating in a Ponzi scheme); *see also* Desmond, *supra* note 11, at 35 (pointing out how cryptocurrency has been used to disguise Ponzi schemes); Groshoff, *supra* note 23, at 520 (juxtaposing the elements of a Ponzi scheme with that of cryptocurrencies); Eric Posner, *Fool's Gold: Bitcoin is a Ponzi Scheme The Internet's Favorite Currency Will Collapse*, SLATE (Apr. 11, 2013), *archived at* http://perma.cc/Z938-SLP5 (suggesting that "[u]nless a bitcoin has value as a currency, it has no value at all, and its price in dollars will fall to zero"). "Bitcoin will collapse when people realize that it can't survive as a currency because of its built-in deflationary features, or because of the emergence of [an alternative], or both." *Id.*

[68] *See* Groshoff, *supra* note 23, at 519 (portraying Bitcoin Trojan horses as evidence of market manipulation).

> For example, evidence of computing risk has occurred, as 'Bitcoin trojan horses already exist.' In addition, cyber-attacks have doubled from 2010 to 2012. Mt.Gox indicated that hackers have targeted the exchange "to 'destabilise Bitcoin' . . . [and] abuse the system for profit." When Mt. Gox, the most popular exchange, was hacked . . . [t]he glut of bitcoins for sale crashed

al Bitcoin exchanges such as Mt. Gox, Tradehill, and Bitcoinica, have been compromised by hackers and fraudsters, with significant losses to investors.[70] These frauds and other pervasive thefts of bitcoins[71] are reflected in the high volatility of bitcoin's value.[72]

> the price from $17.50 to $0.01 within a half hour. The company said, '[a]ttackers ... wait for everybody to panic-sell their Bitcoins, wait for the price to drop to a certain amount . . . and start buying as much as they can.' In late 2010, the Bitcoin system had to fix a 'vulnerability in the system' found when the creation of nearly 185 billion Bitcoins resulted from a verification error and again when an inter-governmental task force wrote that terrorist groups may use digital assets such as Bitcoin.

See Groshoff, *supra* note 23, at 519.

[69] *See* Denis T. Rice, *The Past and Future of Bitcoins in Worldwide Commerce*, BUS. L. TODAY (Nov. 2013), *archived at* http://perma.cc/N24N-3FX5 (describing bitcoins value in the current trading infrastructure).

> The economist Paul Krugman stated earlier this year that, unlike gold or paper fiat currencies, bitcoin derives its value solely from a self-fulfilling expectation that others will accept it as payment. Herb Jaffe cited a Morningstar analyst as having called the Winklevoss ETF 'a total gimmick,' that bitcoins are very illiquid, and that the current trading infrastructure 'is riddled with security/efficiency problems.'

Id.

[70] *See* Groshoff, *supra* note 23, at 519-20 (demonstrating Bitcoins' vulnerability to hackers and the perceived risk for investors).

> Such linkage to international criminal activity may represent a material risk for Bitcoins, as well. In 2011, Silkroad, which was an illegal marketplace for crimes with victims, began permitting Bitcoins as a currency medium. In 2012, more controversy arose: a major market, Tradehill, closed; two additional markets-Bitcoinica and Bitfloor-were hacked; an FBI report became leaked, reporting that the FBI 'fears[ed] . . . Bitcoin as a tool to facilitate the sales of drugs and weapons and assist terrorists;' the closing of 'Bitcoin savings and trust' creating '$5.6 million in debt;' and clients sued Bitcoinica for the alleged loss of deposits. As a result, 'users are anxious about Bitcoin's legal status and the possibility of a government crackdown.'

See Groshoff, *supra* note 23, at 519-20.

[71] *See* Grinberg, *supra* note 3, at 180 (continuing to demonstrate Bitcoins' vulnerabilities by showing how easy it is for hackers to compromise and obtain the secure information).

> Like cash, bitcoins can be lost or stolen. Keeping bitcoins on one's computer can be as dangerous as keeping large sums of cash in one's physical wallet, and each user should take care to backup and secure his Bitcoin wallet. A large-scale theft of

Bitcoin fraud is so common because "the current trading infrastructure 'is riddled with security/efficiency problems:'"[73] "lack of oversight . . . permits anonymous transactions to occur very easily [and] has earned the currency its moniker, 'hackercash.'"[74] Consequently, "bitcoins are very illiquid:"[75] they are difficult to sell.[76] To top it off, investments in cryptocurrency are not insured by the Federal Deposit Insurance Corporation, so cryptocurrency exposes consumers to risk they are unaware of.[77] Even worse to a consumer perspective: cryptocurrency is insecure.[78]

Any cipher is only as secure as its key.[79] Thus, bitcoin transactions are vulnerable to attacks that seek to seize an account's private key.[80] Even cryptologically secure systems are always open to

> bitcoins from many users could create a confidence crisis. Such theft could occur by a virus or Trojan horse that installs itself on a Bitcoin user's computer and sends the wallet file to the criminal who wrote the software.

See Grinberg, *supra* note 3, at 180.

[72] *See* Neil Guthrie, *The End of Cash? Bitcoin, the Regulators and the Courts*, 29 B.F.L.R. 355, 361 (2014) (examining the high volume of fraudulent practices and money-laundering associated with the exchange of Bitcoins do to the Bitcoins' value); *see also* Groshoff, *supra* note 23, at 521 (addressing concerns regarding the volatility in the value of Bitcoins by exemplifying how drastically the value pertaining to Bitcoins changed between February 2013 to June 2013).

[73] *See* Rice, *supra* note 69 (proffering that Bitcoin fraud is prevalent due to inadequacies in security and efficiency within the trading infrastructure of Bitcoins).

[74] *See* Desmond, *supra* note 11, at 31 (explaining the reason why digital money like Bitcoin is nicknamed "hackercash").

[75] *See* Rice, *supra* note 69 (describing how Bitcoin's lacks security to become an efficient form of currency like gold or paper).

[76] *See* Rob Wile, *It's Still Ridiculously Difficult To Buy Bitcoin*, BUS. INSIDER (July 9, 2014), *archived at* http://perma.cc/AC64-JA9Q (addressing difficulties associated with selling Bitcoins).

[77] *See* Swartz, *supra* note 20, at 323 (stressing that Bitcoin transactions generally are not insured due to the anonymity of users and the finality of transactions).

[78] *See* Susanne Posel, *Bitstamp Hack Highlights the Insecurity of Cryptocurrency*, OCCUPY CORPORATISM (Jan. 6, 2015), *archived at* http://perma.cc/72VK-S3M5 (accounting for insecurities associated with cryptocurrencies).

[79] *See* ROTHSTEIN & WHALEY, *supra* note 48 (exemplifying the importance of security in regards to ciphers).

[80] *See* Lane, *supra* note 12, at 516 (suggesting importance of an account's private key and significance behind protecting it from vulnerabilities aforementioned).

> The Bitcoin system is comprised of a network of interconnected computers called 'nodes,' all of which run the Bitcoin client software. The software generates two mathematically related keys,

human intelligence attacks (HUMINT) such as social engineering or the physical seizure of the hard drive where data is recorded.[81] Cryptocurrencies such as bitcoin are also computationally vulnerable to denial of service attacks,[82] trojan horses,[83] and mining by zombie bot-

> one public and one private, that together make up a user's digital signature. The public key, also known as the Bitcoin address, is used to send and accept payments to and from other users, while the private key remains concealed with the user and functions as a password to unlock the transaction. For each public key, or Bitcoin address, there is exactly one matching private key that is mathematically related to it and is designed in a way that the public key may be calculated from it, but not vice-versa. If a private key corresponding to a Bitcoin transaction is lost or stolen, the balance is likely gone forever.

See Lane, *supra* note 12, at 516.

[81] *See* JOSHUA BARON ET AL., NATIONAL SECURITY IMPLICATIONS OF VIRTUAL CURRENCY 56-57 (2015) (cautioning that even the most virtually secure systems are still vulnerable to traditional forms of fraudulent activity).

[82] *See* Grinberg, *supra* note 3, at 180-81 (explaining how Bitcoin is susceptible to denial of service).

> Although Bitcoin is decentralized and generally has no single point of failure, it is nevertheless susceptible to a form of denial of service attack. Individuals with a majority of the computational power in the Bitcoin mining network can effectively preclude any transaction from being processed. Such a sustained attack might significantly depress the exchange rate and lead to a collapse of confidence. Obtaining the necessary computational power is easy, if expensive. Although some question why anyone would do such a thing, several parties might have sufficient interest: governments who want to shut Bitcoin down, individuals with future liabilities in bitcoins, or hackers who want to blackmail a business that relies on bitcoins.

See Grinberg, *supra* note 3, at 180-81.

[83] *See* Groshoff, *supra* note 23, at 519 (explaining the existence of Bitcoin Trojan horses).

> For example, evidence of computing risk has occurred, as 'Bitcoin trojan horses already exist.' In addition, cyber-attacks have doubled from 2010 to 2012. Mt. Gox indicated that hackers have targeted the exchange "to 'destabilise Bitcoin' ... [and] abuse the system for profit.' When 'Mt. Gox, the most popular exchange, was hacked .... [t]he glut of bitcoins for sale crashed the price from $17.50 to $0.01 within a half hour.' The company said, '[a]ttackers ... wait for everybody to panic-sell their Bitcoins, wait for the price to drop to a certain amount ... and start buying as much as they can.' In late 2010, the Bitcoin system had to fix a 'vulnerability in the system' found when the crea-

nets,[84] all of which have occurred with losses to bitcoin's users.[85]

All of these facts make cryptocurrencies such as bitcoin look terrible.[86] To be blunt, bitcoin is rat poison.[87]

"The law and regulation of virtual currencies are currently in a state of flux worldwide".[88] This article argues that the U.S. regulatory approach to cryptocurrency should simply seek to ban cryptocurrencies[89] because distributed encrypted currency enables a wide range of grave crimes, threatens US national security, and because cryptocurrency is more or less a scam.[90] This article will also point out the

> tion of nearly 185 billion Bitcoins resulted from a verification error and again when an inter-governmental task force wrote that terrorist groups may use digital assets such as Bitcoin.

See Groshoff, *supra* note 23, at 519.

[84] *See* Dion, *supra* note 13, at 184-85 (introducing the concept of zombie bot-nets and their role in mining Bitcoins).

[85] *See* Dion, *supra* note 13, at 185 (recognizing the widespread effect of Bitcoin theft).

[86] *See* Paul Vigna, *Buffet: 'Stay Away' From Bitcoin*, WALL ST. J. (Mar. 14, 2014), *archived at* http://perma.cc/8PRV-C4KM (warning, "'[s]tay away from it,' he said, according to a transcript. '[i]t's a mirage basically'").

[87] *See* VW Staff, *Charlie Munger Compares Bitcoin to Rat Poison*, VALUEWALK (May 6, 2013), *archived at* http://perma.cc/2WHT-MEGZ (stating that "it's rat poison").

[88] *See* Brad Jacobsen & Fred Peña, *What Every Lawyer Should Know About Bitcoins*, 27 UTAH B. J. 40, 43 (2014).

[89] *See* Bloomberg News, *China Bans Financial Companies From Bitcoin Transactions*, BLOOMBERG BUS. (Dec. 5, 2013), *archived at* http://perma.cc/BTY3-TM2U (highlighting the risk of digital currencies and how the ban addresses this concern). Bitcoin is sufficiently crooked that even states with weak rule of law such as Russia and China have banned it. *See The People's Bank of China and Five Associated Ministries Notice: "Prevention of Risks Associated with Bitcoin*,*"* BTCC (Dec. 3, 2013), *archived at* http://perma.cc/7XKF-EEZF (providing an English translation describing China's reasons for banning Bitcoin); *see also* Evander Smart, *Russia Plans Bitcoin Ban by 2015*, CRYPTOCOINSNEWS (Sept. 14, 2014), *archived at* http://perma.cc/V2YV-P3NC (explaining Russia's reasons for banning Bitcoin); Ellis Hamburger, *Russia Bans Bitcoin Use*, THE VERGE (Feb. 9, 2014), *archived at* http://perma.cc/PY5G-T4RB (reiterating Russia's suspicion of Bitcoin for its link to illicit activities); *Legality of Bitcoin by Country*, WIKIPEDIA, *archived at* http://perma.cc/5KHE-RGBK (providing an up-to-date list of the worldwide banning of bitcoin).

[90] *See* Nicholas A. Plassaras, Comment, *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*, 14 CHI. J. INT'L L. 377, 390-91 (2013) (listing the potential obstacles of Bitcoin as digital currency).

> [E]conomists are worried about the uncertainty surrounding the operation and growth of digital currencies. 'Because so much of

regulatory mechanisms which can and should be used to ban crypto-currencies: laws against counterfeiting, securities and exchange rules and regulations, and asset forfeiture laws. The Department of State should also coordinate with U.S. allies and friends and encourage them to likewise ban pirate currency.[91]

Universal Jurisdiction for Essential State Functions Such as Currency under International Law

The United States, like most every other government on earth, enjoys a monopoly in emitting coin[92] and currency.[93] The fiscal power – taxation, monetary policy, budgeting - is a core element of state sovereignty, essential to the functioning of the state.[94] The fiscus is also uniquely *state* power, not private power.[95] Consequently, as a matter of public international law, States may lawfully exercise extraterritorial jurisdiction via the protective principle for counterfeiting, whether of currency, obligations, or passports,[96] because

> the data on these currencies is either supplied directly by the issuer or scattered across the Internet, it is difficult for scholars to draw any reliable conclusions on whether--and if so, how and when--these currencies might be widely accepted.' Others criticize digital currencies like Bitcoin on a more theoretical level because they are neither intrinsically valuable, like gold, nor do they have roots in a commodity expressing a certain purchasing power.

Id.

[91] *See* Adrianne Jeffries, *Senator Calls on the US Government to Ban Bitcoin*, THE VERGE (Feb. 26, 2014), *archived at* http://perma.cc/PKB9-UA38 (suggesting a U.S. ban on Bitcoin to follow other international trends).

[92] *See* Juilliard v. Greenman, 110 U.S. 421, 462 (1884) (defining "[t]he meaning of the terms 'to coin money' is . . . to mould metallic substances into forms convenient for circulation and to stamp them with the impress of the government authority indicating their value with reference to the unit of value established by law").

[93] *See id.* at 446 (reinforcing the idea that Congress has a monopoly on currency and coin circulation); *see also* United States v. Falvey, 676 F.2d 871, 876 (1st Cir. 1982) (referencing a statute intending to prevent the circulation of counterfeit coins); United States v. Gellman, 44 F. Supp. 360, 364 (D. Minn. 1942) (interpreting a coin counterfeit statute to prevent the coining of money in competition with the U.S.).

[94] *See Juilliard*, 110 U.S at 442 (acknowledging the authority of the state government with respect to its enumerated powers to create and distribute currency).

[95] *See id.* at 447 (recognizing the state's fiscal powers).

[96] *See* ANTHONY AUST, HANDBOOK OF INTERNATIONAL LAW 44 (2010) (explaining

these functions are indispensable for effective governance.[97] So, despite the recent Supreme Court Decision in *Morrison*,[98] courts ought *not* impose a presumption that U.S. legislation has no extraterritorial effect where extra-territorial jurisdiction under the protective principle is possible.[99] Securing U.S. currency, U.S. financial instruments, and U.S. passports worldwide is the sovereign prerogative of the United States and can be enforced extra-territorially as a matter of ius gentium under protective principle jurisdiction.[100]

Because counterfeiting government instruments can properly be subject to extraterritorial jurisdiction under the protective principle as a matter of international law, the legality of any cryptocurrency transaction on earth can in theory be attacked by any country on earth that regards the use of cryptocurrency as undermining its own financial instruments by abetting counterfeiting and perhaps even in cases of "mere" money laundering.[101] This too shows why cryptocurrency is a bad bet.[102]

Currency Powers under the U.S. Constitution: The Federal Money Monopoly

An essential failing of the articles of confederation of the United States, the constitutional precursor to the current United States constitution, was finance: the articles of confederation provided no independent taxation power to the confederal government, and the

the limits of the protective principal as well as the foreign offense actions); *see also* CHRISTOPHER C. JOYNER, INTERNATIONAL LAW IN THE 21ST CENTURY: RULES FOR GLOBAL GOVERNANCE 150 (2005) (discussing the protective principal and how it applies to state jurisdiction).

[97] *See* JOYNER, *supra* note 96 (acknowledging the importance of the protective principal and the states enforcement powers).

[98] *See* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 250 (2010) (describing the strict presumption against extra-territorial effect of U.S. legislation).

[99] *See id.* at 255 (stating the principle regarding extra-territoriality in the U.S. and its effects on foreign nations).

[100] *See id.* at 256 (giving an example of how the United States can have jurisdiction over matters surrounding the United States economy and actors on foreign soil).

[101] *See* AUST, *supra* note 96 (inferring cryptocurrency may fall under international law regarding a governments right to prevent counterfeiting and money laundering).

[102] *See* Jeffries, *supra* note 91 (highlighting the government's concerns regarding cryptocurrency and crime).

States as co-equal sovereigns and international legal persons had plenary fiscal power, including powers over their own coin and currency.[103] The result was a financial disaster: rampant inflation and federal impotence were the most obvious flaws.[104] To correct these defects, the current Constitution created a federal government with exclusive foreign policy powers and granted powers of taxation, and fairly wide ranging ones, to the federal government.[105] Furthermore, the Constitution transferred all monetary powers aside from chartering of banks and some forms of taxation into the exclusive hands of the Federation.[106] The United States, like most every other country on earth, thus enjoys a monopoly on the creation of money, which shows why cryptocurrency is illegal as an invasion of the federal currency monopoly.[107]

i. Federal Power - Gold, Silver, Fiat

The U.S. Constitution gives the federal government the powers to "coin Money" and "regulate the Value thereof."[108] Money is a generic term, and embraces coinage as well as paper currency.[109] Although a good-faith argument could be made that "coin" indicates specie, only, and "currency" notes, whether fiat or asset-backed, and

[103] *See* NAT'L BUREAU OF ECON. RESEARCH, FOUNDING CHOICES: AMERICAN ECONOMIC POLICY IN THE 1790S 133 (Douglas A. Irwin & Richard Sylla, eds., 2011) (demonstrating the hardship associated with financing the Revolutionary War); *see also* JAMES WILLARD HURST, A LEGAL HISTORY OF MONEY IN THE UNITED STATES, 1774-1970, 5 (2001) (purporting that "[e]xperience under the articles . . . provided base lines from which to measure the later course of law affecting the money supply").

[104] *See Economic and the Articles of Confederation*, HISTORY CENTRAL (2015), *archived at* http://perma.cc/CY8L-5DMV (articulating why one central money creation system is necessary in order for a country's economy to flourish).

[105] *See id.* (explaining why the founders of the Constitution created a centralized treasury with the sole power to create and regulation money).

[106] *See* U.S. CONST. art. I, § 8 (pointing to the powers given to the Federal Government regarding money, taxation, and their regulation).

[107] *See* ANDREI DINU, THE SCARCITY OF MONEY: THE CASE OF CRYPTOCURRENCIES 6 (2014) (explaining how fiat money is similar to cryptocurrency in that it derives its scarcity from government monopoly).

[108] *See* U.S. CONST. art. I, § 8, cl. 5 (stating the U.S. Government's power to create and regulate money).

[109] *See* Hopson v. Fountain, 24 Tenn. 140, 141 (1844) (defining money in the historical context).

that "money" indicates coin and currency alike, the U.S. Constitution does not in fact make these distinctions.[110] Current and historic interpretations of the U.S. Constitution regard coinage, currency and money alike: all are nomisma, units of account posited by the government as media of exchange.[111] Ordinary legislation could and should make those finer distinctions to generate greater legal certainty.[112] However, it appears, after this brief survey of the legislation on counterfeiting, that ordinary federal legislation repeats the constitutional commingling of basic terminology, to the detriment of legal certainty and the rule of law.[113] As a constitution must be comprehensible to ordinary persons and is of general character this terminological error in constitutional law is forgivable.[114] However ordinary legislation naturally plays precisely the role of refinement and clarity in exact definition of the general terms found in constitutions.[115]

The federal government may also lawfully "borrow Money on the credit of the United States"[116] and "provide for the Punishment of counterfeiting the Securities and current Coin of the United States."[117] Thus, the federal government is empowered to issue fiat currency,[118] despite libertarian and tax protestors' tin-foil hat fantasies

[110] *See Coinage Clause*, THE HERITAGE FOUNDATION, *archived at* http://perma.cc/5T9P-JRTU (noting the absence of distinctions between coin and currency).

[111] *See* ARISTOTLE, *Book V*, *in* NICOMACHEAN ETHICS 5 (W. D. Ross trans., 350 B.C.E.) (stating that "money has become by convention a sort of representative of demand; and this is why it has the name 'money' (nomisma)-because it exists not by nature but by law (nomos) and it is in our power to change it and make it useless").

[112] *See* SOFIA RANCHORDÁS, CONSTITUTIONAL SUNSETS AND EXPERIMENTAL LEGISLATION: A COMPARATIVE PERSPECTIVE 126 (2014) (advocating for clearly written laws to promote legal certainty).

[113] *See id.* (suggesting how, without legal certainty, citizens may not know their legal rights).

[114] *See id.* (supporting the fact that citizens need legal certainty).

[115] *See id.* (demonstrating how legal certainty is a critical element of good lawmaking).

[116] U.S. CONST. art. I, § 8, cl. 2.

[117] U.S. CONST. art. I, § 8, cl. 6.

[118] *See* Hepburn v. Griswold, 75 U.S. 603, 614 (1870) (analyzing whether there is an implied power in the Constitution that grants legislators with a power regarding credit currencies); *see also Juilliard*, 110 U.S. at 439 (demonstrating Congress' power over currency and finance); Legal Tender Cases, 79 U.S. 457, 618 (1871) (explaining the overlap of federal and state regulation of currency); Shollenberger v. Brinton, 52 Pa. 9, 33 (1865) (providing an overview of Congress's powers regarding legal tenders).

to the contrary.[119] After all, fiat currency has this advantage over specie: it is lighter and easier to transport.[120]

ii. State power to Tender Gold and Silver, Only.

The U.S. constitution prohibits states from "coin[ing] money"[121] and prohibits the states from "mak[ing] any Thing but gold and silver Coin a Tender in Payment of Debt."[122] Tender is an offer of payment of money.[123] A good faith argument could be made that the States are empowered to emit dollar denominated undiluted specie coins, only, though that is not the argument which has prevailed over time. States are without doubt prohibited from issuing "bills of credit,"[124] i.e. paper currency, whether fiat or specie.[125]

Taken together, the federal power to issue fiat currency and the prohibition to the states to coin money or issue bills of credit indicate that the federal government has the exclusive public power to

[119] *See* Frank Moraes, *Why Libertarians Hate Fiat Money*, FRANKLY CURIOUS (Dec. 29, 2013), *archived at* http://perma.cc/6SQ8-JLZQ (highlighting that Libertarian's belief that taxing is similar to theft).

[120] *See* Mark Harrison, *Did the Gold Standard Work? Economics Before and After Fiat Money*, CFA INST. (Apr. 16, 2013), *archived at* http://perma.cc/C2K3-RYMR (acknowledging the various advantages of fiat currency in comparison to specie).

[121] U.S. CONST. art. I, § 8, cl. 5.

[122] U.S. CONST. art. I § 10, cl. 1.

[123] *See* ALVA ROSCOE HUNT, A TREATISE ON THE LAW OF TENDER, AND BRINGING MONEY INTO COURT NOT ONLY IN SUPPORT OF A PLEA OF TENDER: BUT UNDER THE COMMON RULE: TOGETHER WITH A CHAPTER ON OFFER OF JUDGMENT 3 (2011) (defining tender concerning the payment of money).

[124] *See* Craig v. Missouri, 29 U.S. 410, 432 (1830) (defining bills of credit as "paper intended to circulate through the community for its ordinary purposes as money and redeemable at a future day"); *see also* Briscoe v. Bank of Commonwealth of Ky, 36 U.S. 257, 257 (1837) (defining that "To constitute a bill of credit, within the constitution . . . it must be a paper which circulates on [credit] . . . and so received and used in the ordinary business of life").

[125] *See Briscoe*, 36 U.S. at 337 (Story, J., dissenting) (providing alternative methods of currency).

issue notes which are legal tender, currency.[126] Cryptocurrency, in contrast, is privately issued.[127] Since the principal objects of public law documents such as constitutions are public law persons such as the federal or state government, private power will be regulated in principle by ordinary law, not the constitution.[128]

iii. Private Power to Issue Scrip?

Fiscal law is an instance of public power; thus, there is in principle no private fiscal power.[129] Any private financial capacity is a matter of contract and property, not fiscal law.[130] Of course, the principle of freedom of contract, one of the building blocks of the liberal state, is protected in the U.S. constitution.[131] Thus, the several states may not "impair the obligations of contracts."[132] Likewise, no state may disallow debt owed to a private person or the debt of the state itself - bankruptcy law is exclusively federal.[133]

How may private law persons lawfully arrange their finances? Private persons may lawfully issue coupons, claims for discounted prices or rebates on goods they sell.[134] Private persons may also law-

[126] *See id.* at 257 (discussing the powers of the federal government with respect to creating currency).

[127] *See* Brill & Keene, *supra* note 41, at 24 (acknowledging the private transactions that occur with cryptocurrencies, such as Bitcoin).

[128] *See* Suhana Dhawan, *Difference Between Constitutional Law and Ordinary Law*, SHARE YOUR ESSAYS (2016), *archived at* http://perma.cc/9QE6-EG46 (describing the different roles ordinary law plays in both public and private law).

[129] *See* U.S. Const., art I, § 10, cl. 1 (stating the federal government's sole authority in coining and printing money).

[130] *See id.* (declaring that no state that not pass any law impairing the obligation of contracts).

[131] *See* Thomas G. West, *The Economic Principles of America's Founders: Property Rights, Free Markets, and Sound Money*, THE HERITAGE FOUND. (Aug. 30, 2010), *archived at* http://perma.cc/76VF-JAG7 (explaining the importance and basics of the freedom of contract).

[132] *See* U.S. CONST. art. I, § 10, cl. 1 (articulating the constitutional limitations on states regarding commerce).

[133] *See* U.S. CONST. art. I, § 8 (acknowledging the exclusive federal jurisdiction over bankruptcy litigation).

[134] *See* United States v. Van Auken, 96 U.S. 366, 368-69 (1878) (qualifying that

fully issue tokens representing payment received for services they offer, where such tokens are not intended for general circulation or use as a form of currency.[135] However, there is a recognized federal monopoly on issuance of coins and cash in the United States and that monopoly applies to both public law and private law legal persons.[136] The federal money monopoly exists[137] because otherwise it would be difficult or even impossible for the federal government to levy taxes, to the detriment of all government operations[138] and because, as cryp-

coupons do not constitute money under the Constitution).

[135] *See* Anchorage Centennial Dev. Co. v. Van Wormer & Rodrigues, Inc., 443 P.2d 596, 599-600 (Alaska 1968) (condemning the illegality as a defense to the particular breach of contract claim at issue when tokens are used commemoratively instead of commercially).

[136] *See* Kurt Schuler, *Note Issue by Banks: A Step Toward Free Banking in the United States?*, 20 CATO J. 453 (2001) (explaining why the United States government has a monopoly in issuing bank notes).

[137] *See* United States v. Marigold, 50 U.S. 560, 566-67 (1850) (clarifying the scope of the power to coin money); *see also* Memorandum and Order at 4, United States v. Von Nothaus, No. 5:09CR27-RLV (W.D. N.C. Nov. 10, 2014) (suggesting the federal government's agencies have the sole power to prosecute claims regarding counterfeit money).

[138] *See Marigold*, 50 U.S. at 567 (indicating that without the ability to enforce the government's power to regulate money other government function regarding money would become relatively impossible).

> But the twentieth section of the act of Congress of March 3d, 1825, or rather those provisions of that section brought to the view of this court by the second question certified, are not properly referable to commercial regulations, merely as such; nor to considerations of ordinary commercial advantage. They appertain rather to the execution of an important trust invested by the Constitution, and to the obligation to fulfill that trust on the part of the government, namely, the trust and the duty of creating and maintaining a uniform and pure metallic standard of value throughout the Union. The power to coining money and of regulating its value was delegated to Congress by the Constitution for the very purpose, as assigned by the framers of that instrument, of creating and preserving the uniformity and purity of such a standard of value; and on account of the impossibility which was foreseen of otherwise preventing the inequalities and the confusion necessarily incident to different views of policy, which in different communities would be brought to bear on this subject. The power to coin money being thus given to Congress, founded on public necessity, it must carry with it the correlative power of protecting the creature and object of that power. It cannot be imputed to wise and practical statesmen, nor is it consistent with

tocurrency illustrates, private currency enables criminality.[139]

Private persons can nonetheless emit commercial paper, which is an unconditional promise to tender payment in cash for a sum certain on a determinable date.[140] Although private persons, unlike the several states,[141] may issue bills of credit,[142] cryptocurrency is not a bill of credit[143] because it is not a promise to redeem a debt in cash. Cryptocurrency is not a form of commercial paper because it is not an unconditional promise to pay a sum certain on or before a definite date.[144] Cryptocurrency is however digital scrip, a redeemable token of value.[145] Scrip is a token, usually paper, which claims to

> common sense, that they should have vested this high and exclusive authority, and with a view to objects partaking of the magnitude of the authority itself, only to be rendered immediately vain and useless, as must have been the case had the government been left disabled and impotent as to the only means of securing the objects in contemplation.

Id.

[139] *See id.* at 568 (demonstrating how private currency may result in criminal activity).

[140] *See* Weissman v. Sinorm Deli, 669 N.E.2d 242, 245 (N.Y. 1996) (defining commercial paper as "an instrument for the payment of money only or a judgment"); *see also* U.C.C. § 3-104(a)(1) (indicating that a "negotiable instrument" is a promise or order to pay a particular amount of money and the promise becomes payable when it is issued or comes into possession by the holder).

[141] *See* US. CONST. art. I, § 10, cl. 1 (focusing on the idea that the several states are prohibited from emitting bills of credit, i.e. currency)

[142] *See* Briscoe v. Bank of Commonwealth of Ky., 36 U.S. 257, 348 (1837) (asserting state cannot issue bills of credit as a form of currency); *accord* State *ex rel.* Shiver v. Comptroller Gen., 4 S.C. 185, 209 (1873) (contending that under the Constitution unconstitutional bills of credit are bills issued by a State, issued based on the credit of that State, and must be "intended to circulate as money"); *cf.* Hous. & Tex. Cent. R.R. Co. v. Texas, 177 U.S. 66, 87 (1900) (contrasting that bills of credit are actually promises by the states in paper form pledging the states faith and marking the paper as able to circulate as money).

[143] *See Briscoe*, 36 U.S. at 338 (inferring that because cryptocurrency is not on paper it does not violate the Constitution). A bill of credit is a promissory note designed to circulate as money and redeemable at a future day. *See Craig*, 29 U.S. at 432 (alluding to cryptocurrency not qualifying as a bill of credit because it is not on paper); *accord* Hale v. Huston, 44 Ala. 134, 139 (1870) (stating that the authority of the state defers to the authority of the Supreme Court on the subject).

[144] *See Briscoe*, 36 U.S. at 338 (clarifying one way in which cryptocurrencies differ from traditional exchanges).

[145] *See* Brill & Keene, *supra* note 41, at 11 (explaining how cryptocurrencies may be exchanged for value in traditional forms of currency).

have a redeemable money value.[146]

Currency Laws in Ordinary Federal Legislation

i. The Stamp Act

The Stamp Payments Act is a U.S. Federal law which prohibits circulation of privately issued currency worth less than one dollar:[147] recall, that when the dollar was pegged to gold it was much more valuable than today because coinage had precious metal content and dollars were redeemable in specie.[148] Consequently the specie value of U.S. coinage was greater than the nominal value.[149] This encouraged coin hoarding, depleting the treasury's store of precious metals.[150] Consequently, private persons facing a shortfall in "small change" emitted redeemable tokens denominated as U.S. money to make up for the shortfall.[151] The stamp act was enacted to combat

[146] *See Scrip*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining scrip as a "document that entitles the holder to receive something of value paper money, that is issued for temporary use").

[147]*See* Stamp Payments Act of 1862, 18 U.S.C. § 336 (2012) (introducing the Stamp Payment Act).

> Whoever makes, issues, circulates, or pays out any note, check, memorandum, token, or other obligation for a less sum than $1, intended to circulate as money or to be received or used in lieu of lawful money of the United States, shall be fined under this title or imprisoned not more than six months, or both.

Id.

[148] *See* Seth Lipsky, *What Is a Dollar?*, NAT'L AFFAIRS (2011), *archived at* http://perma.cc/6Z73-BJVM (explaining the formation of the Gold Standard in the United States).

[149] *See id.* (discussing the types of denominations created by the Gold Standard in creating currency).

[150] *See* CRAIG K. ELWELL, CONG. RESEARCH SERV., BRIEF HISTORY OF THE GOLD STANDARD IN THE UNITED STATES 8-9 (2011) (discussing the common occurrence of the "bank panic" which would lead to mass withdrawals and often cause banks to fail); *see also 34 – Executive Order 6102 – Requiring Gold Coin, Gold Bullion and Gold Certificates to Be Delivered to the Government*, THE AM. PRESIDENCY PROJECT, *archived at* http://perma.cc/43MX-9AAF (demanding that all privately owned gold be transferred over to the government due to economic emergency).

[151] *See* ELWELL, *supra* note 150, at 8 (providing an example of the smaller amount of coin used to replace that which had been liquidated from the banks during periods of panic).

coin hoarding: scrip worth less than one dollar is illegal.[152]

Case-law on the stamp act has since provided several factors for seeing when private scrip violates U.S. laws prohibiting counterfeiting, forming legal principles that should apply by analogy to other laws, i.e. scrip *over* one dollar of value.[153] The following factors are relevant when analyzing whether a given scrip is lawful.

*Scrip that only circulates locally, not nationally, is likelier to not violate United States law.[154]

*Scrip that can only be redeemed for goods, is also likely not to be found in violation of laws against counterfeiting.[155]

*Scrip that does not visually resemble U.S. money, is less likely to violate U.S. laws against counterfeiting.[156]

*Finally, scrip that resembles a commercial check is less likely to violate U.S. counterfeiting laws.[157]

While these cases all address the stamp act, logic implies that they would apply to prohibitions against counterfeit generally by legal analogy, and not merely to counterfeits below a value of one dollar, which in fact are de minimis due to the devaluation of the fiat dollar as compared to the gold standard dollar.[158]

ii. The Counterfeiting Statutes

[152] *See* Stamp Payments Act of 1862, 18 U.S.C. § 336 (2012) (setting forth the stamp act's ban on issuing and circulating currency with an equivalency of less than one dollar).

[153] *See* United States v. Van Auken, 96 U.S. 366, 368 (1877) (exemplifying when private scrip violates U.S. laws involving the circulation of currency when the sum of the currency is larger than one dollar).

[154] *See id.* at 367-68 (asserting that scrip is less likely to violate United States currency laws because it does not circulate nationally and it is a miniscule amount).

[155] *See Scrip*, BLACK'S LAW DICTIONARY (10th ed. 2014) (comparing internet scrip to coupons and bonus points, which may be exchanged by a consumer for goods or services, but they have no cash value).

[156] *See* United States v. Monongahela Bridge Co., 26 F. Cas. 1292, 1292 (W.D. Pa. 1863) (determining that scrip that does not resemble U.S. currency is likely to encounter counterfeiting problems).

[157] *See* Stettinius v. United States, 22 F. Cas. 1322, 1324-25 (Cir. Ct. D.C. 1839) (explaining that currency in the form of paper or commercial check is less likely to violate counterfeiting laws).

[158] *See* Jason Fernando, *The Gold Standard Versus Fiat Currency*, INVESTOPEDIA (May 12, 2015), *archived at* http://perma.cc/4B5C-V3XQ (explaining that due to the devaluation of the fiat dollar counterfeiting currency is much harder than when attempting to counterfeit previous forms of currency).

The Stamp Act limits itself to what are now small denominations and covers scrip as well as counterfeit.[159] The federal counterfeiting statute[160] prohibits the creation of larger sums of money.[161] The counterfeiting statute is intended to protect the monopoly of the United States dollar as a means of exchange.[162] Are cryptocurrencies counterfeits?

At least one U.S. court has found bitcoin to be currency,[163] although 18 U.S.C. § 485 requires similarity between the counterfeit object and U.S. money, 18 U.S.C. §. 486 does not require similarity.[164] Thus, "Bitcoin has the potential to be deemed a counterfeit and rendered illegal"[165] because it competes against the dollar as a general medium of exchange and thereby violates the federal money monopoly.[166] If the factors which indicate when scrip is unlawful under the Stamp Act apply by analogy to the federal counterfeiting statute then it is clear that cryptocurrency violates the counterfeiting stat-

[159] *See* Stamp Payments Act of 1862, 18 U.S.C. § 336 (2012) (discussing the Stamp Act's coverage and limitations).

[160] *See* 18 U.S.C. § 470 (2012) (outlining counterfeiting prohibitions and obligations); *see, e.g.*, 18 U.S.C. § 471 (2012) (prohibiting the alteration or counterfeiting of U.S. obligations or other securities). Since U.S. dollars today are fiat, they should be covered by section 471. *Id.*; *see, e.g.*, 18 U.S.C. §§ 485-486 (2012) (governing the counterfeiting of coins and bars).

[161] *See* 18 U.S.C. § 486 (2012) (articulating that counterfeited currency "whether in the resemblance of coins of the United States . . . or of original design" is considered counterfeited monies under the statute).

[162] *See* United States v. Le Mon, 622 F.2d 1022, 1024 (10th Cir. 1980) (suggesting "[t]he manifest purpose of the counterfeiting statute is the protection of all currency and obligations of the United States").

[163] *See* Sec. Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2013 U.S. Dist. LEXIS 110018, at *5 (E.D. Tex. Aug. 6, 2013) (holding that Bitcoin is a "currency or form of money").

[164] *Compare* 18 U.S.C. § 485 (2012) (requiring that counterfeited coins or bars must resemble any currently circulated United States stamped or coined monies in order to be subject to the statute), *with* 18 U.S.C. § 486 (2012) (subjecting punishment for merely attempting to pass counterfeited currency as current circulated money).

[165] Farmer, Jr., *supra* note 10, at 94.

[166] *See* Farmer, Jr., *supra* note 10, at 95 (addressing the applicability of the Stamp Payments Act of 1862 to the concept of Bitcoins in order to prevent alternative domestic currencies from competing with the dollar).

ute.[167] Considering these factors in the case of cryptocurrencies such as bitcoin: bitcoin circulates *globally,* is not *redeemable for goods sold by the emitter* and *competes with the dollar*.[168] Taken together, those facts indicate cryptocurrency should be seen as counterfeit.[169] Although bitcoin does *not* resemble U.S. money, it also does *not* resemble a check because it is not an unconditional promise to pay a sum certain on a determinable date.[170] Cryptocurrency is scrip, but given these factors the logical conclusion is that cryptocurrency is unlawful scrip and is in violation of the federal counterfeiting statute because it competes with the dollar as a general medium of exchange.[171]

iii. Money Laundering

Cryptocurrency also raises the problem of money laundering.[172] Money laundering is the attempt to disguise the source or destination of criminally tainted funds.[173] Money laundering seeks to make dirty money appear clean.[174]

> Generally, money laundering can be divided into three stages: (1) placement; (2) layering; and (3) integration. For the first step, money, usually in the

[167] *See supra* notes 147-158 and accompanying text (discussing the factors associated with making scrip unlawful under the Stamp Act).

[168] *See supra* notes 147-158 and accompanying text (reiterating the specific factors that could make cryptocurrencies unlawful).

[169] *See* Farmer, Jr., *supra* note 10, at 95 (suggesting that Bitcoins could be considered counterfeit currency and a violation of the Stamp Payments Act).

[170] *See* U.C.C § 3-104 (2016) (defining a negotiable instrument as "an unconditional promise or order to pay a fixed amount of money").

[171] *See* Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, The Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 155 (2012) (concluding that Bitcoins could be considered a substitute for currency subjecting it to the federal counterfeiting statute).

[172] *See Dutch Police Arrests Three People in Bitcoin Money Laundering Investigation*, BLOCKCHAIN AGENDA (Oct. 1, 2015), *archived at* http://perma.cc/BRT2-T9Y4 (demonstrating how Bitcoin has been linked to money laundering).

[173] *See* Ruoke Yang, *When is Bitcoin a Security under U.S. Securities Law?*, 18 J. TECH. L. & POL'Y 99, 123-24 (2013) (defining money laundering as the criminal process of mixing dirty money from illegal activities with clean money and redistributing the mixture into circulation).

[174] *See id.* at 124 (explaining how "dirty money" can be integrated into society to appear as ordinary business income).

> form of cash generated from criminal activities, is 'placed' or converted into a less bulky and noticeable form (e.g., diamonds). In the second step, multiple financial transactions are made to create a long and twisted trail, hence putting 'layers' between the origin of the dirty money and its eventual entrance into the clean monetary supply. Finally, through a front business for instance, the dirty money is integrated into mainstream society as part of the front business' income.[175]

Cryptocurrency makes placement and layering easier than it would otherwise be and is an ideal vehicle for money laundering due to anonymity.[176] Money laundering is a federal crime under the Bank Secrecy Act ("BSA")[177] and the Money Laundering Control Act of 1986.[178] We discuss the historical evolution of anti-money laundering laws ("AML") to show why they are somewhat inadequate to govern cryptocurrency transactions and how to strengthen the bans against money laundering so as to prevent and punish use of cryptocurrency as a tool of money laundering.[179]

Money laundering was first outlawed in the United States by the Bank Secrecy Act ("BSA") and then also by the Money Laundering Control Act ("MLCA").[180] The BSA aims at transactions over $10,000, which caused money launderers to circumvent that law by

[175] *Id.*

[176] *See id.* (outlining how cryptocurrency makes the process of money laundering simpler by making it easier to counterfeit and redistribute currency back into commerce).

[177] *See* 12 U.S.C. § 1951 (2012) (noting how the BSA requires businesses to maintain records in order to aid "in criminal, tax, or regulatory investigations or proceedings").

[178] *See* Money Laundering Control Act of 1986, 18 U.S.C. §§ 1956-1957 (2012) (prohibiting people from concealing proceeds generated from illegal activities as proceeds from a lawful financial transaction).

[179] *See* Yang, *supra* note 173, at 124 (providing an example through the Bank Secrecy Act of one of the many anti-money laundering legislative actions taken to aid in the battle against money laundering through cryptocurrency).

[180] *See* Danton Bryans, Note, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J. 441, 455-56 (2014) (highlighting the initial regulation of money laundering, which was the BSA).

engaging in multiple transactions of less than $10,000.[181] The MLCA was enacted to cover that weakness of the BSA.[182]

Money laundering statutes initially targeted organized crime, focusing on the *criminal* and identifying the source of their income in order to cripple organized crime by drying up its stream of revenue.[183] More recently, anti-money laundering laws are also used to combat terrorism.[184] The contemporary institutional approach to money laundering focuses attention on the *institutions* which receive tainted cash[185] rather than the criminal, through reporting requirements and forfeiture statutes,[186] which require only a civil standard of proof and may even shift the burden of proof to the property owner.[187] Due to this shift, which more often focuses on financial institutions, recent AML regulations require financial institutions responsible to "know your customer" ("KYC"),[188] e.g., through "Customer

[181] *See id.* (noting that the BSA's previous $10,000 threshold in regards to addressing money laundering issues).

[182] *See id*. at 459-60 (outlining the federal provisions of the MLCA and providing the requirements for money laundering to be considered a federal crime).

[183] *See* Catherine Martin Christopher, *Whack-A-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Money Laundering*, 18 LEWIS & CLARK L. REV. 1, 2 (2014) (identifying criminals as the targeted group covered by original money laundering statutes).

> Initially, anti-money laundering statutes were enacted in order to hamper the illegal drug trade, though anti-money laundering laws are also used to fight 'corruption, organized crime and transnational criminal activity.' Theoretically, individuals will be less likely to engage in criminal enterprises if they cannot safely (that is, without law enforcement detection) spend the proceeds of their crimes.

Id. at 3-4.

[184] *See id.* at 5 (demonstrating how anti-money laundering laws have been used to prevent terrorist attacks post September 11th).

[185] *See id.* at 23 (characterizing anti-money laundering laws as a type of regulation for financial institutions). "U.S. law enforcement is increasingly turning to regulation and prosecution of financial institutions to enforce anti-money laundering laws, and existing anti-money laundering laws are being stretched to include digital currency exchanges in the group of institutions subject to reporting requirements." *Id.*

[186] *See* Lane, *supra* note 12, at 545 (providing that Bitcoin's anonymity and encryption directly affects forfeiture statutes).

[187] *See* 18 U.S.C. § 981 (2012) (discussing which party has the burden of proof with respect to forfeiture claims).

[188] *See "Know Your Customer" Guidelines Anti Money Laundering Standards,* J&K BANK, *archived at* http://perma.cc/H2LP-2YE6 (defining what a customer is

Identification Programs ("CIP")," [189] to maintain records of transactions[190] and to report suspicious activity.[191] Although the institutional approach is more effective, U.S. money laundering statutes do not focus on the *destination* of *clean* money for a *dirty* transaction.[192] This loophole in the law, having been identified,[193] needs to be closed by legislative amendment.

Money transmitters must have effective anti-money laundering programs to prevent use of their business as a money laundering platform. [194] Although individual bitcoin users are not Money Service Businesses, Bitcoin exchanges can be a money service business and thus subject to SEC regulation and anti-money laundering laws. [195] The U.S. Treasury Department's Financial Crimes Enforcement

with respect to the "KYC" policy).

[189] *See* Rule for Banks, 31 C.F.R. § 1020.220(a)(1) (elaborating on the concept of Customer Identification Programs for credit unions, banks, and trust companies who also have an anti-money laundering compliance program in place).

[190] *See* 12 U.S.C. § 1953(a) (2012) (outlining the requirements for the maintenance of appropriate records for uninsured banks and business institutions).

[191] *See* 31 U.S.C. § 5313 (2012) (noting that "a domestic financial institution . . . shall file a report on the [specified] transaction at the time and in the way the Secretary prescribes").

[192] *See* Yang, *supra* note 173, at 124-25 (noting that United States money laundering statute does not take into account the destination of clean money).

[193] *See* Christopher, *supra* note 183, at 10 (cautioning against the loopholes in current money laundering regulations).

[194] *See* U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES GUIDANCE (2013) [hereinafter APPLICATION OF FINCEN'S REGULATIONS, VIRTUAL CURRENCIES GUIDANCE] (defining FinCEN's idea of a virtual currency user as, anyone who "obtains virtual currency to purchase goods or services").

[195] *See id.* (highlighting that a user of virtual currency does not obtain the status of a money service business just because it uses virtual currency for the exchange of goods); *see also* U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY MINING OPERATIONS (2014) (defining the parameters of when users would be subject to the status as MSBs).

> [FinCEN found that] [t]o the extent that a user mines Bitcoins and uses the Bitcoins solely for the user's own purposes and not for the benefit of another, the user is ***not*** an MSB under [the BSA's (Bank Secrecy Act)] regulations, because these activities involve neither "acceptance" nor "transmission" of the convertible virtual currency and are not the transmission of funds within the meaning of the [BSA's regulations].

Network ("FinCEN" [196]) regards bitcoin administrators[197] as money transmitters[198] and thus obligated to register with FinCen.[199]

Cryptocurrency as a Security

Cryptocurrency's legal classification as a security or currency is somewhat uncertain.[200] Bitcoin has been found to be a security in at least one U.S. court.[201] However, a different U.S. court has found bitcoin to be currency.[202] Currency itself is not a security and thus is

Id.

[196] *See* APPLICATION OF FINCEN'S REGULATIONS, VIRTUAL CURRENCIES GUIDANCE, *supra* note 194 (noting that FinCEN does not regulate virtual currency when a user purchases goods or services through a virtual network).

[197] *See* Gordon Griffin, *Virtual Currencies in the Crosshairs*, 28 FALL CRIM. JUST. 62, 62-63 (2013) (describing two types of bitcoin administrators).

> An exchanger is 'a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency,' while an administrator is 'a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.'

Id.

[198] *See* APPLICATION OF FINCEN'S REGULATIONS, VIRTUAL CURRENCIES GUIDANCE, *supra* note 194 (stating that virtual currency does not fall under FinCEN's regulations as a form of money transmitter).

> A user of virtual currency is not an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations.

Id.

[199] *See* APPLICATION OF FINCEN'S REGULATIONS, VIRTUAL CURRENCIES GUIDANCE, *supra* note 194 (emphasizing that virtual currency is not subject to FinCEN registration).

[200] *See* Harasic, *supra* note 7, at 491 (describing the IRS's categorization of Bitcoin as property rather than currency). "Bitcoin's legal classification remains uncertain." *See* Harasic, *supra* note 7, at 491.

[201] *See* Gerkis & Krikunova, *supra* note 16, at 6 (according to the Securities and Exchange Commission Bitcoin may also be classified as a security).

[202] *See* Sec. Exch. Comm'n v. Shavers, No.4:13-CV-416, 2013 U.S. Dist. LEXIS 110018, at *5 (E.D. Tex. Aug. 6, 2013) (holding that Bitcoin is a "currency or form of money").

not subject to SEC regulation,[203] but currency exchanges and futures on currency are subject to SEC regulation.[204] Cryptocurrency brokers may also be required to register with the SEC.[205]

This paper, consistent with these federal court rulings, argues that cryptocurrency can be both a currency *and* a security. Cryptocurrencies such as bitcoin are rightly subject to laws against counterfeiting *and* laws against stock fraud because of their dual nature as a medium of exchange and as a speculative instrument: the federal case which held bitcoin to be currency is *not* inconsistent with federal case which found bitcoin to be a security.[206] Cryptocurrencies are curren-

[203] *See* 15 U.S.C. § 78c(a)(10) (2012) (originally the Securities Exchange Act of 1934 ch. 404, title I, Sec. 3) (defining securities, specifying which investment vehicles are not deemed securities under the Act). The following are not securities and thus are exempt from SEC regulation: "currency or any note, draft, bill of exchange, or banker's acceptance which has a maturity at the time of issuance of not exceeding nine months, exclusive of days of grace, or any renewal thereof the maturity of which is likewise limited." *Id.*; *accord* Bellah v. First Nat'l Bank of Hereford, Texas, 495 F. 2d 1109, 1114 (5th Cir. 1974) (rejecting the Plaintiff's claim that the note and the ancillary deed of trust are covered securities under the 1934 Act); Procter & Gamble Co. v. Bankers Trust Co., 925 F. Supp. 1270, 1280 n.4 (S.D. Ohio 1996) (stating foreign currency "is not a security as defined in the 1933 and 1934 Acts"). "[I]t is generally acknowledged that currency is not a security." *See* Lewis D. Lowenfels & Alan R. Bromberg, *What is a Security Under the Federal Securities Laws?*, 56 ALB. L. REV. 473, 483 (1993) (exempting currency from being in the security category).

[204] *See* General Rules and Regulations, Securities Exchange Act of 1934, 17 C.F.R. § 240 (2013) (clarifying that the SEC has jurisdiction over foreign currency exchanges).

[205] *See* Letter from Jason Coombs, CEO, Public Startup Company, Inc., to Mary Jo White, Chair, Securities and Exchange Commission (Nov. 15, 2014) (arguing the SEC has declared cryptocurrency a security depending on the facts and circumstances); *see also* John M. Pachkowski, *FinCEN provides guidance to virtual currency miners and investors*, WOLTERS KLUWER L. & BUS. (Jan. 31, 2014), *archived at* http://perma.cc/M6YU-KZHW (discussing measures that those working with cryptocurrency may have to take) "[P]roviding specific brokerage-related services might require the company to be registered with the Securities and Exchange Commission (SEC) or the Commodities and Futures Trading Commission (CFTC), in which case the company would be covered under the BSA as a securities broker-dealer or a commodities or futures trader." *Id.*

[206] *Compare* Sec. Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2013 U.S. Dist. LEXIS 110018, at *5 (E.D. Tex. Aug. 6, 2013) (finding that "Bitcoin is a currency or form of money"), *with* Sec. Exch. Comm'n v. Shavers, No 4:13-CV-416, 2013 U.S. Dist. LEXIS 130781, at *28 (E.D. Tex. Sept. 18, 2014) (finding that the defendant violated Sections 5(a) and 5(c) of the Securities Act, 15 U.S.C. § 77e(a), by

cies, and yet may *also* be subject to SEC jurisdiction as a security, depending on the specific facts of the case at bar.[207] The following hypothetical illustrates the logic of double regulation of the hybrid instrument. If I were to forge federal treasury bonds and negotiate them then I would be in violation of both the anti-fraud provisions of the securities laws and would be guilty of counterfeiting.[208] Counterfeiting and stock fraud are not mutually exclusive crimes; they can be complementary criminal acts.[209] Thus, bitcoin is a currency, yet can also be a security. [210] The fact that cryptocurrency has played a key role in many frauds and other crimes further justifies double regulation. [211]

We now explore the definition of security[212] to see when and

selling a security, not registering the security sold, and used interstate means of sale).

[207] *See* Sec. Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2013 U.S. Dist. LEXIS 130781, at *28 (E.D. Tex. Sept. 18, 2014) (demonstrating under certain facts cryptocurrency like Bitcoin can be deemed a security by a court).

[208] *See* Peter Followill, *Counterfieting Laws and Penalties*, CRIMINAL DEFENSE LAWYER (2016), *archived at* http://perma.cc/P373-J3PY (showing what happens when a person forges currency).

[209] *See id.* (reaffirming that counterfeiting encompasses more than making fake currency).

[210] *Compare* Sec. Exch. Comm'n v. Shavers, No 4:13-CV-416, 2013 U.S. Dist. LEXIS 110018, at *5 (E.D. Tex. Aug. 6, 2013) (holding Bitcoins are money and should be treated as such), *with* Sec. Exch. Comm'n v. Shavers, No 4:13-CV-416, 2013 U.S. Dist. LEXIS 130781, at *28 (E.D. Tex. Sept. 18, 2014) (articulating that cryptocurrencies are also securities).

[211] *See Virtual Currency: Risks and Regulation*, INDEP. CMTY. BANKERS OF AM. (June 23, 2014), *archived at* http://perma.cc/U8D9-NFSN (summarizing various crimes surrounding cryptocurrency).

[212] *See* 15 U.S.C. § 77b(a)(1) (2012) (originally the Securities Act of 1933 ch. 38, title I, Sec. 1, 48 Stat. 74) (describing how the Court has held these statutory definitions as identical). The Securities Act of 1933 defines security as:

> [A]ny note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign

why cryptocurrency is subject to SEC rules and regulations.

i. What is a Security?

Although cryptocurrencies are subject to counterfeiting laws, their purchase or sale can also be a violation of the rules and regulations of the Securities and Exchange Commission.[213] The Securities and Exchange Act defines security as "any note, stock, treasury stock, security future, security-based swap, bond . . . [or] investment contract"[214] and subjects securities to regulation for issuance and compliance.[215]

Does cryptocurrency fall into any of these categories? Is cryptocurrency a security?

The term "security" is to be liberally interpreted in the context of actual economic facts.[216] Notes may be either securities or commercial paper.[217] Notes are presumed to be securities,[218] though the presumption is rebuttable.[219] Commercial paper that falls due within

> currency, or, in general, any interest or instrument commonly known as a 'security', or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.

Id.; *see also* 15 U.S.C. § 78c(a)(10) (2012) (originally the Securities Exchange Act of 1934 ch. 404, title I, Sec. 3) (referencing the definition of "security" in the 1934 act); Landreth Timber Co. v. Landreth, 471 U.S. 681, 685 (1985) (acknowledging the federal definition of security).

[213] *See* Followill, *supra* note 208 (warning that it is "illegal to buy, sell, exchange, transfer, receive or deliver counterfeit securities").

[214] *See* 15 U.S.C. § 77b(a)(1) (2012) (defining the term "security").

[215] *See* 15 U.S.C. § 77c(a)(9)-(10) (2012) (describing the requirements with respect to conditions of security issuance).

[216] *See* Sec. Exch. Comm'n v. Am. Commodity Exch., Inc., 546 F.2d 1361, 1366 (10th Cir. 1976) (describing how the term "security" should be understood through looking an economic viewpoint).

[217] *See* Reves v. Ernst & Young, 494 U.S. 56, 61-62 (1990) (explaining how notes can be many types of instruments in the commercial paper and securities world).

[218] *See Reves*, 494 U.S. at 56 (holding that demand notes do fall under securities).

[219] *See Reves*, 494 U.S. at 67 (indicating that a note is understood to be a security unless that presumption is rebutted).

> Begins with a presumption that any note with a term of more than nine months is a 'security' but allows 'an issuer to rebut the presumption that a note is a security if it can show that the note in question bear[s] a strong family resemblance to an item on the

nine months of issuance is exempted from SEC regulation unlike longer term notes.[220] Bitcoin is not commercial paper because it is not a promise to pay a sum certain by a determinable date.[221] Bitcoin has already been determined in court not to be a stock,[222] because it does not have characteristics associated with stocks[223] such as the right to vote and a claim to dividend payments.[224] Bitcoin is also no promise to pay on occurrence of a given contingency and thus is not a future.[225] Bitcoin is not a promise to repay a principal with interest and so bitcoin is not a bond.[226] However, investment contracts are also subject to SEC regulations as a "security."[227] Cryptocurrencies

> judicially crafted list of exceptions' of notes that 'are obviously not securities'

Id. at 63-65.

[220] *See* 15 U.S.C. § 77c(a)(3) (2012) (originally the Securities Act of 1933 § 3(a)(3)) (noting the timeframe during which commercial paper is not subject to SEC regulation).

> Any note, draft, bill of exchange, or banker's acceptance which arises out of a current transaction or the proceeds of which have been or are to be used for current transactions, and which has a maturity at the time of issuance of not exceeding nine months, exclusive of days of grace, or any renewal thereof the maturity of which is likewise limited.

Id.

[221] *See* Grinberg, *supra* note 3, at 195-96 (emphasizing that bitcoins are not negotiable instruments because they lack the requisite characteristics to be so).

[222] *See* Landreth Timber Co. v. Landreth, 471 U.S. 681, 685 (1985) (implying that currencies like Bitcoin do not qualify as securities); *see also* Jeffrey E. Alberts & Bertrand Fry, *Is Bitcoin a Security?*, 21 B.U. J. SCI. & TECH. L. 1, 9-10 (2015) (analyzing Bitcoin by the courts' definition of a security).

[223] *See* United Hous. Found., Inc. v. Forman, 421 U.S. 837, 851 (1975) (outlining factors used to determine whether an investment is a stock). Factors include: "(i) the right to receive dividends contingent upon an apportionment of profits; (ii) negotiability; (iii) the ability to be pledged or hypothecated; (iv) the conferring of voting rights in proportion to the number of shares owned; and (v) the capacity to appreciate in value." *Id.*

[224] *See id.* (providing two of the key characteristics in a stock).

[225] *See id.* (explaining that one of the common features in stocks is the payout of dividends being dependent upon profit).

[226] *See* Sec. Exch. Comm'n v. Shavers, No 4:13-CV-416, 2013 U.S. Dist. LEXIS 110018, at *2 (E.D. Tex. Aug. 6, 2013) (explaining how Bitcoin is limited as currency that can only be invested by paying actually money).

[227] *See Landreth Timber Co.*, 471 U.S. at 686 (explaining how investment contracts fall within the definition of a "security").

have been found to be "investment contract[s]"[228] under the Howey test[229] and thus subject to regulation the Securities and Exchange Acts,[230] including listing and compliance requirements as well as the risk of liability for fraudulent trades.[231]

The canonical definition of "investment contract" subject to regulation by the SEC is *SEC v. Howey*.[232] Howey defined an investment contract is a "contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or third party"[233] Thus, there are four elements to the *Howey* test:

(1) an investment of money, *and*
(2) in a common enterprise, *and*
(3) which is expected to produce profits, *and*
(4) due to the efforts of others.

Prong four, initially defined as "solely" through the efforts of others has been expanded by later case-law to equate "solely" with "primarily" or "substantially."[234]

Note that these four prongs are connected by conjunction (*A* and *B* and *C* and *D =investment contract).*[235] These prongs are *not*

[228] *See Shavers*, No 4:13-CV-416, 2013 U.S. Dist. LEXIS 110018, at *20 (highlighting a court decision holding that Bitcoin investments meet the definition of securities).

[229] *See* Sec. Exch. Comm'n v. W. J. Howey Co., 328 U.S. 293, 299-300 (1946) (holding that profit sharing in farm worked by others held to be an investment contract and thus subject to the SEA).

[230] *See* 15 U.S.C. § 77b(a)(l) (2012) (stating that investment contracts are a security); *see also* 15 U.S.C. § 78c(a)(10) (2012) (including investment contracts under the category of "security").

[231] *See* 15 U.S.C. § 77e(b) (2012) (setting forth the requirements for compliance with interstate commerce regulations regarding securities).

[232] *See W. J. Howey Co*., 328 U.S. at 298 (stating that the term "investment contract" was at that time undefined by the Securities Act or any relevant legislative reports).

[233] *See id.* at 298-99 (providing a definition of investment contract for purposes of the Securities Act).

[234] *See* Sec. Exch. Comm'n v. Glenn W. Turner Enters., Inc., 474 F.2d 476, 481-82 (9th Cir. 1973) (highlighting the importance of the word "solely" in the *Howey* definition of an investment contract).

[235] *See id.* (stating that all of the elements create the substance of an investment contract).

four alternatives.[236] Nor are they four factors to be weighed in the totality of circumstances, each of which tends to indicate an investment contract.[237] All four elements must coexist for an investment contract to be found.[238]

ii. Cryptocurrency is not a Commodity or Future

Commodities are defined as tangible items.[239] Commodities are not securities.[240] Bitcoin is not a commodity because it is intangible.[241] A future is a promise of a future payment price for a given commodity at or before a given time.[242] Bitcoin is not a future because it is not a promised possibility to purchase a product at a particular price.[243] However, trading in options based on the speculated future value of a cryptocurrency would be subject to the CFTC regulations.[244]

Cryptocurrency and Taxation[245]

Bitcoin also raises tax issues,[246] notably tax evasion,[247] and

[236] *See id.* (pointing to the use of "and" in the definition, which infers that all elements must be present for there to be an investment contract)

[237] *See id.* (highlighting that each factor signals the relevant language of an investment contract).

[238] *See id.* (pointing out that the language in the *Howey* test uses "and" instead of "or," making it clear that all elements must be present).

[239] *See* State *ex. rel* Moose v. Frank, 169 S.W. 333, 336 (Ark. 1914) (stipulating the particular definition of commodity in its commercial usage); *see also Commodity*, BLACK'S LAW DICTIONARY (9th ed. 2009) (providing a definition of commodity).

[240] *See* Lowenfels & Bromberg, *supra* note 203, at 548 (discussing the difference between a security transaction and a commodity).

[241] *See* Comshare, Inc., v. United States, 27 F.3d 1142, 1145 (6th Cir. 1994) (noting that although physical tapes and discs were tangible property, the information on those disks was intangible property).

[242] *See Introduction to the Futures Market,* FUTURES KNOWLEDGE (June 23, 2014), *archived at* http://perma.cc/7WJ5-BZP2 (providing an overview of the futures market).

[243] *See* Swartz, *supra* note 20, at 333 (concluding that bitcoins may fall within the commodity category, but are not futures).

[244] *See* Swartz, *supra* note 20, at 333-34 (stating that bitcoin may be subject to CFTC authority).

[245] *See* INTERNAL REVENUE SERVICE BULLETIN, NOTICE 2014-21 (2014) (outlining the IRS guidelines on taxation of virtual currency).

[246] *See* Bayern, *supra* note 34, at 1487, n. 4 (illustrating possible regulatory issues

can be thought of as a "virtual" offshore tax haven.[248] For tax purposes, cryptocurrency is property, not currency,[249] and should be characterized as ordinary income, and not as a capital asset[250] though the IRS plans to characterize cryptocurrency transactions as capital gains or ordinary income depending on the actual facts of the concrete case.[251] Realization of income from cryptocurrency ordinarily occurs on its conversion into cash.[252]

arising from Bitcoin use).

> Bitcoin raises other problems for legal regulation that need to be addressed in their own right. There are a variety of important but comparatively mundane questions, such as what sort of capital gains treatment, if any, should attend profits from private trading in bitcoins. More subtle is the potential tax treatment of profits from 'mining,' or creating through software processes the valuable units of account in cryptographically backed currency. There are also questions about the interaction between Bitcoin and the securities laws. (citation omitted).

See Bayern, *supra* note 34, at 1487, n. 4.

[247] *See* Patrick McLeod, *Taxing And Regulating Bitcoin: The Government's Game Of Catch Up,* 22 COMMLAW CONSPECTUS 379, 384-85 (2014) (stating regulators concerns that Bitcoin could be used "for the purposes of tax evasion and money laundering").

[248] *See* Omri Y. Marian, *Are Cryptocurrencies Super Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38, 40 (2013) (explaining that "tax havens allow taxpayers to conceal earnings from tax authorities in the taxpayers' home jurisdictions").

[249] *See* INTERNAL REVENUE SERVICE BULLETIN, *supra* note 245, at 2 (discussing that for Federal tax purposes cryptocurrency istreated as property).

[250] *See* INTERNAL REVENUE SERVICE BULLETIN, *supra* note 245, at 3-4 (describing the types of gains or losses taxpayers realize on the sale or exchange of virtual currency).

> [S]tocks, bonds, and other investment property are generally capital assets. A taxpayer generally realizes ordinary gain or loss on the sale or exchange of virtual currency that is not a capital asset in the hands of the taxpayer. Inventory and other property held mainly for sale to customers in a trade or business are examples of property that is not a capital asset.

Id.

[251] *See* INTERNAL REVENUE SERVICE BULLETIN, *supra* note 245, at 2-3 (noting that if a taxpayer receives virtual currency as a form of payment for goods or services, they must include that as general income when calculating their gross income).

[252] *See* Helvering v. Horst, 311 U.S. 112, 115 (1940) (highlighting how the taxation of income in U.S. law is presumed only to occur on its realization into cash; this presumption of realization into cash may be rebutted).

> Admittedly, not all economic gain of the taxpayer is taxable income. From the beginning the revenue laws have been interpret-

Though cryptocurrency violates the governmental currency monopoly and should be seen as illegal, illegal transactions are subject to taxation.[253] For example, prostitution is illegal in U.S. law in most states.[254] However, prostitutes' income, though usually untaxed de facto, is de jure liable to taxation.[255] The tougher issue is whether and when ordinary and necessary business expenses used to generate illegal income may be deducted.[256] "Model's" costumes, incidentally, are ordinary and necessary business expenses and thus deductible from taxable income.[257] Even if illegal, realization of income from

> ed as defining 'realization' of income as the taxable event, rather than the acquisition of the right to receive it. And 'realization' is not deemed to occur until the income is paid. But the decisions and regulations have consistently recognized that receipt in cash or property is not the only characteristic of realization of income to a taxpayer on the cash receipts basis. Where the taxpayer does not receive payment of income in money or property realization may occur when the last step is taken by which he obtains the fruition of the economic gain which has already accrued to him. (citation omitted).

Id.

[253] *See* 26 U.S.C. § 61 (1984) (defining gross income as "all income from whatever source derived" and listing various sources that constitutes income under the statute).

[254] *See* Blevins v. Commissioner, 14 T.C.M 840 (1955) (addressing how prostitution is an immoral and illegal occupation within the United States).

[255] *See id*. (suggesting that income generated from illegal activities is still subject to taxation).

[256] *See* 26 U.S.C § 162(c)(2) (2012) (suggesting that it is unclear whether ordinary and necessary business expenses used in the production of *illegal* income are tax deductible). Internal Revenue Code Section 162(c)(2) prohibits tax deduction of illegal payments generally. *Id.*; *see also* 26 U.S.C § 280E (2012) (prohibiting deductions of expenses in the drug trade). What about prostitutes? First, many prostitutes are also models or strippers, and thus have similar costumes. Thus, de facto, a prostitute can declare her costumes as deductions simply by claiming to be an actress, model, or even stripper, all of which are legal forms of sex work. *See, e.g.*, 26 U.S.C § 162(a) (2012) (indicating that work clothes may constitute necessary and ordinary business expenses).

[257] *See* Tilman v. United States, 644 F. Supp. 2d 391, 403-04 (S.D.N.Y. 2009) ("Under certain circumstances, expenses for work clothes are deductible, pursuant to I.R.C. § 162(a)"); *see also* Donnelly v. Commisioner, 262 F.2d 411, 412 (2d Cir. 1959) (discussing that for clothes to be deductible, they 'must be of a type specifically required as a condition of employment, and they must not be adaptable to general usage as ordinary clothing); *see also* Pevsner v. Commissioner, 628 F.2d 467, 469 (5th Cir.1980) (acknowledging that a taxpayer may deduct the cost of clothing "only if: (1) the clothing is of a type specifically required as a condition of

cryptocurrency is subject to taxation[258] because of the broad definition of "income" in U.S. tax law, which subjects U.S. persons to income tax on their world-wide income (unlike any other country the author is familiar with).[259] Moreover, under the Foreign Accounts Tax Compliance Act ("FATCA"), "foreign financial institutions ("FFIs") are required to identify their U.S. account holders to the IRS. If an FFI fails to do so, it faces a 30 percent gross tax on certain payments received from U.S. sources."[260]

The reader is reminded that the characterization of cryptocurrency for tax law does not, as a matter of law, have to be the same characterization for securities and exchange law,[261] because these are independent branches of administrative law.[262] Although the same term ought to be presumed to have the same meaning when used by the same legislature, this presumption may be rebutted where a contrary intent be proven[263] or where the result would be an absurdity[264]

employment, (2) it is not adaptable to general usage as ordinary clothing, and (3) it is not so worn).

[258] *See* McLeod, *supra* note 247 (stating that the IRS considers Bitcoin is taxable).

[259] *See* De Ganay v. Lederer, 250 U.S. 376, 378-79 (1919) (sustaining federal taxation of income of alien non-resident derived from securities held in this country). Similarly, non-resident's with U.S. sourced income are liable for tax thereon. *Id.*; *see also U.S. Citizens and Resident Aliens Abroad*, INTERNAL REVENUE SERV., *archived at* http://perma.cc/S875-XGT8 (confirming that a U.S. citizen's worldwide income is subject to U.S. income tax).

[260] *See* Marian, *supra* note 248 (stating the repercussions for foreign financial institutions that fail to provide information on their U.S. account holders).

[261] *See* Atlantic Cleaners & Dryers, Inc. v. United States, 286 U.S. 427, 433 (1932) (stating that "[i]t is not unusual for the same word to be used with different meanings in the same act, and there is no rule of statutory construction which precludes the courts from giving to the word the meaning which the legislature intended it should have in each instance"). Of course, constitutional interpretation is somewhat different from ordinary statutory interpretation, since the Constitution must of necessity be comprehensible to citizens of average intelligence. *See* Louisville & Nashville R.R. Co. v. Gaines, 3 F. 266, 274 (1880) (discussing different methods of constitutional interpretation).

[262] *See, e.g.*, *Office of Administrative Law Judges*, U.S. SEC. & EXCH. COMM'N, *archived at* http://perma.cc/AU4D-DCFN (exemplifying the administrative nature of U.S. securities laws proceedings).

[263] *See Atlantic Cleaners & Dryers, Inc.*, 286 U.S. at 434 (indicating that there is a burden shifting rebuttable presumption thatmust be considered).

[264] *See* Lagae v. Lackner, 996 P.2d 1281, 1284 (Colo. 2000) (quoting that "although we must give effect to the statute's plain and ordinary meaning, the General Assembly's intent and purpose must prevail over a literalist interpretation that leads to

because the law is presumed to be self-consistent and rational.[265]

Examples of Cryptocurrency Frauds

As seen, cryptocurrencies enable all kinds of crimes.[266] Thus, it is no surprise that the legal landscape of "alternative" currency is littered with the wreckage of exposed scams.[267] The following cases all exemplify the point that cryptocurrency ought to be outlawed because it enables crime and fraud. They also are examples of the application of the rules described in this article.

i. Liberty dollar - Counterfeiting

Liberty dollars were printed currency and minted coins, purporting to be redeemable for silver and denominated as dollars.[268] The creator of the currency issued coins which looked similar to U.S. coins, with the image of the statue of liberty and the devise "Trust in God."[269] Thus, the coins clearly fell within the terms of the counterfeiting laws.[270] Furthermore, the value of silver in the coins emitted

an absurd result").

> However plain the ordinary meaning of the words used in the statute may be, the courts will reject that meaning when to accept it would lead to a result so plainly absurd that it could not possibly have been intended by the Legislature or would defeat the plain legislative intention.

See Kiriakids v. United Artists Commc'ns, Inc., 440 S.E.2d 364, 366 (S.C. 1994).

[265] *See* City of Cleburne v. Cleburne Living Ctr. 473 U.S. 432, 440 (1985) (stating "[t]he general rule is that legislation is presumed to be valid").

[266] *See* Grinberg, *supra* note 3, at 161 (providing an example of the types of crimes that Bitcoin can facilitate).

[267] *See* Grinberg, *supra* note 3, at 205 (highlighting the scams that often occur in Bitcoin transactions).

[268] *See* Susan Headley, *What are NORFED Liberty Dollar Coins?*, ABOUT.COM (Dec. 15, 2014), *archived at* http://perma.cc/8NBU-RK9D (defining the Liberty Dollar as an attempt at an inflation proof currency backed by silver and gold, but resembled U.S. currency).

[269] *See id.* (commenting on the similarities between the Liberty Dollar and existing U.S. currency).

[270] *See* Alan Feuer, *Prison May Be the Next Stop on a Gold Currency Journey*, N.Y. TIMES (Oct. 24, 2012), *archived at* http://perma.cc/4XTU-RYHY (asserting that the creation of the Liberty Dollar directly violated existing U.S. counterfeiting laws).

was lower than the face value of the coin, and thus fell afoul of laws against fraud too.[271]

[272]

Liberty dollar also issued silver certificates: these warehouse certificates were multicolored, unlike U.S. greenbacks, but somewhat reminiscent of old-school silver certificates[273] which were issued by the United. States in the 20th Century.[274] Liberty dollar's certificates were purportedly backed up by warehoused silver and, like old-school specie currency used the term “silver certificate.”[275]

The issuer, Bernard Von NotHaus, was ultimately convicted of counterfeiting.[276] The government interest in protecting the monopoly position of the dollar for economic and fiscal reasons are justifications of the prohibitions of private currencies.[277]

[271] *See* Demetri Kofinas, *Asheville man charged in alleged Liberty Dollar fraud scheme by Clarke Morrison*, DEMETRIKOFINAS.COM, *archived at* http://perma.cc/S6SW-WD6R (exemplifying a situation in which Liberty Dollars violated laws against fraud).

[272] *See Bernard von NotHaus: Liberty Dollar Trial Update*, FREEDOM’S PHOENIX (Apr. 20, 2011), *archived at* http://perma.cc/SXN6-9EUM.

[273] *See Silver Certificate*, COIN CMTY. FAMILY (2016), *archived at* http://perma.cc/P6W9-J73Q (depicting Silver Certificates as red, brown, and blue in color).

[274] *See id.* (describing the attributes of the basic silver dollar certificate).

[275] *See id.* (highlighting the Silver Standard as providing a note to the holder that allows them to exchange the Silver Certificate for silver held by the Treasury of U.S.).

[276] *See* Farmer, Jr., *supra* note 10, at 94-95 (pointing out that NotHaus’s conviction centered on his creation of counterfeit coins).

[277] *See* Grinberg, *supra* note 3, at 161 (regarding the motivation towards aggressive attacks upon unauthorized minting of currency).

ii. Liberty Reserve – Money Laundering

Similar to Liberty Dollar, Liberty Reserve also created an alternative currency,[278] which, like bitcoin, provided its customers with anonymity, and appears to have been intended to facilitate money laundering.[279] Vladimir Kats, founder of Liberty Reserve, ultimately plead guilty to money laundering[280] for operating "an anonymous digital currency system that provided cybercriminals and others with the means to launder criminal proceeds on an unprecedented scale."[281]

iii. e-Gold

E-Gold, like liberty dollar, claimed to tie real assets (gold) with anonymous on-line accounts, a digital currency like bitcoin.[282] Like Liberty Reserve, e-Gold, was clearly directed toward the object of laundering money, and violated the MLCA.[283] Ultimately, the U.S. government shut it down for violation of money laundering and fraud.[284]

[278] *See* Griffin, *supra* note 197 (describing how Liberty Reserve was able to achieve its goals by not requiring verification for its accounts).
[279] *See* Alexis C. Madrigal, *How to Launder Billions and Billions of Digital Dollars*, THE ATLANTIC (Nov. 4, 2013), *archived at* http://perma.cc/KA9D-PFUV (focusing on the Vladimir Kats and how he used Liberty Reserve to launder money through the digital currency system).
[280] *See* Emily Spaven, *Founder of Liberty Reserve admits guilt and faces 75 years in prison*, COIN DESK (Nov. 1, 2013), *archived at* http://perma.cc/NA9S-AEAT (describing Vladimir Kat's plea involving counts of money laundering, unlicensed money transmitting, receiving child pornography, and marriage fraud).
[281] *Id.*
[282] *See* Daniel McGlynn, *Are Bitcoin and Other New Money Systems Safe?*, CQ PRESS (Sept. 26, 2014), *archived at* http://perma.cc/SPC4-CLY7 (stating how E-Gold allowed users to buy shares of gold in exchange for internet-based credits).
[283] *See* 18 U.S.C. § 1956 (2012), *amended by* North Korea Sanctions and Policy Enhancement Act of 2016, Pub. L. No. 144-122, 130 Stat 93 (defining laundering of monetary instruments).
[284] *See* Grinberg, *supra* note 3, at 161 (highlighting government action against money laundering schemes). "The U.S. government prosecuted and shut down the creators of e-gold, a digital currency backed by gold, under state and federal laws for conspiracy to commit money laundering, and also for providing services to those involved in 'child exploitation, credit card fraud, and wire (investment)

iv. Mount Gox, Bitcoinca

Bitcoin exchanges are yet another example of fraud associated with cryptocurrency.[285] Bitcoin exchange such as Mt. Gox[286] TradeHill[287] and Bitcoinica[288] have all been compromised by computer criminals with the loss of hundreds of thousands of bitcoins.[289] Mt. Gox ultimately went bankrupt.[290]

v. Silk Road – Asset Forfeiture

"Silk Road" is yet another cautionary tale of shady online currency, and a precursor to what will probably happen to bitcoin.[291] "Silk Road was a 'sprawling black-market bazaar, where illegal drugs and other illicit goods and services [were] regularly bought and sold by the site's users.'"[292] The anonymity bitcoin offered enabled the illegal online market which was "Silk Road."[293] Ross Ulbricht, founder of Silk Road, was captured not due to flaws in the system of anonymity but due to Ulbricht's own human errors,[294] which is cause for caution.[295] "Silk Road" (and similar illegal markets) could not have

fraud.'" *Id.* Business just doesn't look too good for criminal entrepreneurs. *Id.*

[285] *See* Sarah Gruber, *Trust, Identity, And Disclosure: Are Bitcoin Exchanges The Next Virtual Havens For Money Laundering And Tax Evasion?*, 32 QUINNIPIAC L. REV. 135, 140 (2013) (acknowledging that bitcoin exchanges have been used to launder money and avoid tax obligations).

[286] *See id.* at 159 (recognizing Mt. Gox as a prominent bitcoin exchange).

[287] *See id.* at 160 (noting the impact of TradeHill, the second largest Bitcoin exchange, on the bitcoin community).

[288] *See id.* (acknowledging Bitcoinica as a previous bitcoin exchange service).

[289] *See id.* at 159-60 (demonstrating how Mt. Gox, TradeHill, and Bitcoinica all lost their money).

[290] *See* Martinson & Masterson, *supra* note 5, at 16 (stating Mt. Gox, the highest profile Bitcoin exchange, filed for bankruptcy in February 2014).

[291] *See* United States v. Ulbricht, 31 F. Supp. 3d 540, 546-47 (S.D.N.Y. 2014) (cautioning against various unlawful uses of cryptocurrency).

[292]*See* Joseph Burleson, *XI. Bitcoin: The Legal Implications Of A Novel Currency*, 33 REV. BANKING & FIN. L. 99, 104 (2013).

[293] *See id.* at 104 (illustrating the anonymous nature of bitcoin as a risk for Silk Road users).

[294] *See* Lane, *supra* note 12, at 527 (highlighting the lack of technical sophistication of investigators in the anonymous Bitcoin system).

[295] *See* Lane, *supra* note 12, at 542 (stating that "[e]ven where transaction records

operated without bitcoin.[296] The FBI seized at least 26,000[297] bitcoins from silk road users,[298]though many more were untraceable, which points out how dangerous cryptocurrency is.[299]

Remedies to Cryptocurrency

Given how toxic cryptocurrency is, a discussion of computational forensics may help law enforcement or legislators.[300] Here we examine some weak-points in cryptocurrency, which can be used to reign in lawlessness.

i. Block Chain Attacks

Supposedly, cryptocurrencies' use of a block-chain[301] to rec-

and corresponding Bitcoin keys are in the possession of law enforcement, as is the case with Silk Road, the difficulty and time required to decode the information and trace transactions through the block chain make it highly unlikely that authorities will be able to develop probable cause to seize users' Bitcoin balances before the users have transferred the balances elsewhere").

[296] *See* Lane, *supra* note 12, at 539 (suggesting cryptocurrency is a key factor to Silk Roads' success).

[297]*See* Burleson, *supra* note 292, at 105 (highlighting the importance of legislation to protect consumers so they do not face losses as a result of the seizure of electronic currency).

[298] *See* Lane, *supra* note 12, at 512-13 (claiming that a different source alleges there are over 100,000 seized Bitcoins). "Within a matter of months, the Federal Bureau of Investigation had shut down the underground website Silk Road, arrested and charged its alleged administrator, and seized from him roughly 170,000 Bitcoins worth an estimated $32 million." *Id.*

[299] *See* Lane, *supra* note 12, at 512-13 (demonstrating how uncertain Congress and law enforcement was about the expansive use of cryptocurreny).

[300] *See* Kaplanov, *supra* note 171, at 118-119 (showing how complex cryptocurrency is and suggesting the need for a forensic specialist dealing with cryptocurrency).

[301] *See* Kaplanov, *supra* note 171, at 118-119 (stating Bitcoins utilize other methods to record various sequences of transactional records).

> A timestamp records the exact time of a transaction and can come in two forms -- the creation of currency or a transaction between two parties. This complete record of all transactions is called a "block chain, which is a sequence of records called blocks." Every computer on the bitcoin network has a copy of the entire block chain, back to the very first transaction, and this information is updated by passing new blocks to other users on the network. Further, each block must meet certain requirements as it passes along the network, making it very difficult to generate a

ord transactions renders trading secure[302] and enables eventual tracing of transactions.[303] Although the block chain does present a poten-

> valid block in order to fraudulently obtain bitcoins. Essentially, each transaction can be thought of as a sentence in a book. Then each block is like a chapter of that book--a catalogue of a sequence of transactions. Each chapter is then combined into separate volumes, or block chains, with all of the volumes making up the publicly available ledger.

Id.; *see also* Nicholas Godlove, Note, *Regulatory Overview of Virtual Currency,* 10 OKLA. J.L. & TECH. 71 (2014) (mentioning how virtual works on a technical level).

> [V]irtual currency is inextricably linked with a public ledger of transfer. In fact, the very foundation of the Bitcoin's existence is bound with a public record of every exchange of every coin between transferors and transferees, published to all other users on the network, forming a chain that can be tracked the creation of the currency. This list of all transfers, going back to the 'Genesis Block' of original Bitcoins, is called the 'Block chain. The Bitcoin peer-to-peer network that allows for miners to generate Bitcoins also serves as a public ledger for all Bitcoin transactions. A timestamp server records the time of creation of each Bitcoin and any other Bitcoin transaction within the network. The full record of transactions is called a block chain, a sequence of records composing a virtual ledger. The computing power delivered to the network by the miners is used to generate the blocks of the chain and keep track of Bitcoin transactions. A useful analogy is to think of the entire network as a handwritten public ledger comprised of sentences, chapters, and volumes. Every transaction is a sentence and each block is a chapter making a 'catalogue of a sequence of transactions.' The chapters are combined into separate volumes and block chains making up the public ledger.

Id.

[302] *See* Harasic, *supra* note 7, at 490-91 (discussing the ease in which individuals can transfer Bitcoins).

> The 'block chain' is a computer-generated, public record of all Bitcoin transactions, back to the very first transaction. Every computer on the Bitcoin network has a copy of the entire block chain. After an hour or two, each transfer is locked in time by the massive amount of user transfers added to the block chain. The use of this time-stamping process ensures that the same bitcoin is not used in more than one transfer. Therefore, each individual bitcoin has an irreversible history of transfers, tracing its movement from one computer to the next.

See Harasic, *supra* note 7, at 490-91.

[303] *See* Godlove, *supra* note 301 (questioning how anonymous Bitcoins are in the public spectrum).

> The block chain is public, meaning that it is possible for anyone

tial route to attack encrypted anonymous on-line transactions, such attacks would be based on social engineering, not the cryptologic security of the peer-to-peer cipher system itself, which is only vulnerable to key recovery or computationally intensive brute force attack.[304]

ii. Digital Wallet Attacks

Another point of attack regulators may wish to consider is the cryptocurrency's "digital wallet", a chink in the hermetic armour of anonymous transactions: "every Bitcoin transaction is facilitated by a digital wallet. Requiring the verification of a wallet holder's identity, maintenance of transaction records, and reporting of suspicious activity allows law enforcement, with valid legal authority, to identify parties to suspected criminal transactions."[305] Failure to maintain such records would enable the police to seize the bitcoin account in ques-

> to see every Bitcoin transaction ever, back to the Genesis block or coinbase transaction. Although Bitcoin addresses aren't immediately associated with real-world identities, computer scientists have done much work figuring out how to de-anonymize 'anonymous' social networks. The block chain is a marvelous target for these techniques. The great majority of Bitcoin users will be identified with relatively high confidence and ease in the near future.
>
> The confidence interval linking block chain transferees and individuals will be enough to achieve probable cause for further investigation of discovered individuals, but not high enough to generate convictions without more evidence. But law enforcement will soon be able to identify likely targets whom they suspect of illegally using virtual currency. Furthermore, identification will be retrospective, meaning that someone who bought drugs on Silk Road in 2011 will still be identifiable on the basis of the block chain whenever these techniques are developed. These de-anonymization techniques are well known to computer scientists, and therefore to the NSA, and likely eventually will be used by law enforcement.

See Godlove, *supra* note 301.

[304] *See* Godlove, *supra* note 301 (describing the potential issues arising from blockchain recipients).

[305] *See* Lane, *supra* note 12, at 554 (describing what is required to identify criminal activity relating to electronic currency).

tion under asset forfeiture law.[306] Prosecutors can also use the federal wire fraud statute, which has broad application "to prosecute just about any scheme, scam, or fraud committed within Bitcoin."[307]

iii. Asset Forfeiture Statutes[308] as a Remedy to Cryptocurrency

As we saw in the case of "Silk Road," asset forfeiture is one response to crime.[309] Asset forfeiture is the simple idea that police may seize property of suspected criminals where said property was used as a criminal instrument or is the proceeds of criminal activity – and that the police may then use these seized assets to fund their own operations.[310] An asset (property) may be said forfeited where it is seized by the state without compensation to the owners.[311] As such, asset forfeiture is an infringement on the fundamental constitutional right to property.[312] Consequently, asset forfeiture statutes ought thus be the subject of strict constitutional scrutiny, and not mere rational review, for a fundamental right is in fact at stake.[313] However, finding a compelling state interest in the suppression of crime is no difficult feat: so the only question is if the asset forfeiture is the least restrictive means available to the state,[314] in which case the law would be constitutional as far as due process goes. Asset forfeiture is con-

[306] *See* Lane, *supra* note 12, at 554 (explaining how transparency in Bitcoin transactions improves law enforcement's abilities to investigate).

[307] *See* Dion, *supra* note 13, at 198 (mentioning what could occur if prosecutors stick with the current legislation).

[308] *See* 18 U.S.C. § 981 (2012) (listing the primary sources for counterfeiting prohibition in the federal statutory law).

[309] *See* United States v. Ulbricht, 31 F. Supp. 3d 540, 546-47 (S.D.N.Y. 2014) (noting the U.S government's allegations as grounds of denying defendant 'silk road' motion for to dismiss the narcotics trafficking conspiracy charges).

[310] *See* MARIAN R. WILLIAMS ET AL., INST. FOR JUSTICE, POLICING FOR PROFIT: THE ABUSE OF CIVIL ASSET FORFEITURE 17 (2010) (arguing that law enforcement agencies have significant incentives regarding asset forfeiture).

[311] *See id.* at 15 (defining civil asset forfeiture).

[312] *See* U.S. CONST. amend. V (guaranteeing that private property shall not be taken for public use without just compensation).

[313] *See* WILLIAMS, *supra* note 310, at 62 (acknowledging the constitutional challenges to asset forfeiture).

[314] *See* Korematsu v. United States, 323 U.S. 214, 223 (1944) (noting the Supreme Court's first application of the strict scrutiny standard); *see also* Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989) (highlighting the least restrictive governmental means to protecting minors).

stitutionally suspect, but courts to present regard asset forfeiture constitutionally admissible.[315] Nevertheless, one can rightly question whether police should be allowed to "eat what they kill" because that leads to the real risk of corruption.[316] Furthermore, the procedural rules on asset forfeiture are at least as draconian as the idea that the police may fund their own operations and thereby become unresponsive to democratic influence.[317] The only infringed interest in asset forfeiture is property, not life or liberty; thus, asset forfeiture is a *civil* remedy, not a criminal remedy.[318] Like any other civil remedy asset forfeiture need only meet a civil standard of proof (more likely than not) as opposed to the criminal standard (beyond reasonable doubt).[319] Furthermore, because asset forfeiture is a civil remedy, the burden of proof may be lawfully placed on the *claimant* to the property that the property in question was neither the instrumentality nor product of criminality.[320]

[315] *See* Bennis v. Michigan, 516 U.S. 442, 456-57 (1996) (affirming the asset forfeiture of property did not violate the due process clause of the Constitution).

[316] *See* Brant C. Hadaway, *Executive Privateers: A Discussion on Why the Civil Asset Forfeiture Reform Act Will Not Significantly Reform the Practice of Forfeiture*, 55 U. MIAMI L. REV. 81, 92 (2000) (discussing the implication of the civil asset forfeiture reform act). "Not since the writs of assistance, which helped to inspire our revolution against the British Crown, has a U.S. government mandated that law enforcement officers be allowed, in essence, to eat what they kill." *Id.*

[317] *See id.* at 94 (pointing out that the previous law was inherently susceptible to corruption).

> [W]ith the help of the federal government, local police departments are able to directly raise cash for what they determine are their priorities, free from accountability to any political process. This has led to the alarming development of law enforcement gaining a pecuniary interest not only in forfeited property, but in the very profitability of the drug market itself. Certainly, this cannot be healthy for a democratic society.

Id.

[318] *Contra id*. at 92 (contrasting that property forfeiture as a method of generating revenue is one of the most critical threats to personal liberty).

[319] *See id*. at 97 (distinguishing between the criminal and civil standards of proof regarding seizing a person's property).

[320] *See* Karis Ann-Yu Chi, *Follow the Money: Getting to the Root of the Problem with Civil Asset Forfeiture in California*, 90 CAL. L. REV. 1635, 1640 (drawing attention to the burden of proof shifting toward the person seeking relief).

> An owner who decides to contest the forfeiture has the burden of showing that . . .the property is not actually connected to criminal activities. . . . [O]nce the government seizes an asset the asset

Forfeiture statutes apply to narcotics crimes,[321] as well as illegal wire transfers;[322] there must be a "substantial connection" between the property and the crime.[323] A direct connection between the crime and the proceeds or object is *not* required.[324] Absence proof of a legitimate source of income is sufficient evidence of substantial connection.[325] There is an "innocent owner" defense to forfeiture,[326] however the claimant to the property bears the burden of proof that the property seized was not in fact a criminal instrument or proceeds of crime.[327]

Asset forfeiture has already yielded thousands of bitcoins to the FBI.[328] Because asset forfeiture laws merely require that the

> cannot be recovered unless the owner, through the use of her limited procedural rights, successfully proves a negative and demonstrates the innocence of her property.

Id.

[321] *See* 21 U.S.C. § 881(a)(1) (2012) (explaining that drug related offenses could result in property seizure).

[322] *See* 18 U.S.C. § 981(a)(1)(A) (2012) (articulating that property forfeiture will occur with certain types of fraud).

[323] *See* 18 U.S.C. § 983(c)(3) (allowing the government to seize property used in criminal actions).

[324] *See id.* (inferring that a direct connection between the crime and the property does not need to exist, but rather they have to be connected substantially).

[325] *See* 18 U.S.C. § 983(c)(3) (2012) (concluding that there needs to be a substantial connection between the property being seized and the crime committed); *see also* United States v. Twenty One Thousand Dollars in U.S. Postal Money Orders, 298 F. Supp. 2d 597, 601, 604 (E.D. Mich. 2003) (illustrating the Government's burden in establishing whether the property is subject to forfeiture).

[326] *See* Calero-Toledo v. Pearson Yacht Leasing Co., 416 U.S. 663, 689-90 (1974) (summarizing the defense of innocent owner as someone "uninvolved and unaware of the wrongful activity" and had taken reasonable steps to prevent their property from being used inappropriately).

[327] *See* Eric Engle, *Libertarianism and Resistance to Civil Asset Forfeiture to the State*, INT. J. OF PUB. L. & POL'Y 8 (July 2012) (discussing extensively a constitutional examination of asset forfeiture law).

[328] *See* Lane, *supra* note 12, at 512-13 (depicting one example of the FBI seizing Bitcoins).

> When the Drug Enforcement Administration announced that it had seized 11.02 bitcoins from Charleston, South Carolina hospitality worker Eric Daniel Hughes in May 2013, the first ever government seizure of its kind, few outside the Bitcoin network could have foreseen the legal implications that followed. Previously, a few informed members of Congress had called for tighter restriction on Bitcoin, but those calls had fallen on the deaf ears

property be the proceeds or object of a criminal transaction at any point in the chain of ownership, cryptocurrencies are inherently in danger of seizure.[329]

Conclusion: The Bitcoin Bubble

In the final analysis, cryptocurrency will prove to be a financial fad, a bubble, which will burst as reality finally catches up to speculation. Market bubbles arise due to psychological biases, which are described by behavioral psychology.[330] Behavioral Finance and Economics (BFE) seeks to understand market activity from an interdisciplinary perspective, drawing especially from psychology and market analyses.[331] Unlike neoclassical economic theory, which postulates that people are rational actors and seek to maximize their well-being, BFE recognizes that people face imperfect information and do not always act in an economically rational manner[332] due to

> of a public with little understanding of the virtually anonymous medium of exchange or the dangers it posed. Within a matter of months, the Federal Bureau of Investigation had shut down the underground website Silk Road, arrested and charged its alleged administrator, and seized from him roughly 170,000 bitcoins worth an estimated $32 million. Suddenly, those dangers became clear as the press began publishing story after story, Congress held hearings regarding the regulation of the virtual currency, and Bitcoin moved toward the forefront of the national consciousness.

See Lane, *supra* note 12, at 512-13.

[329] *See* Lane, *supra* note 12, at 531 (observing property similar to Bitcoins are always in danger of criminal seizure).

[330] *See* Groshoff, *supra* note 23, at 503 (naming the psychological factors contributing to the market bubble). Specifically: anchoring bias (the tendency once committed to stay committed, to "double down" on existing investments), overconfidence (overestimating one's own intelligence; we all think we are above average, and some of us are wrong), hindsight bias (presuming past experiences will be future experiences), and failure to accurately and adequately assess risks—representativeness bias, and finally bandwagon i.e. herd mentality, investors tend to follow the crowd. This is why market bubbles arise, seriously exceed objective valuations, and collapse rapidly. *See* Groshoff, *supra* note 23, at 503.

[331] *See* Groshoff, *supra* note 23, at 498 (suggesting Behavioral Finance and Economics comprises of multiple academic disciplines).

[332] *See* Groshoff, *supra* note 23, at 498 (recognizing that BFE is not limited to financial factors but includes emotional and psychological motivations as well).

emotions and bias,[333] and tend to trade on irrelevant information.[334] These irrational biases generate economic bubbles - and the crash which inevitably follows them.[335] The fact that cryptocurrencies are an unproductive speculative fad is one more explanation why they are a bad investment and ought to simply be outlawed.[336]

Cryptocurrency is a threat to domestic and international security as well as to investors' savings and the market itself by undermining investors' confidence. Consequently, the best regulatory approach will use all legal means at the United State's disposal to make cryptocurrency illegal, subject to asset forfeiture, and to augment transaction costs to cryptocurrency transactions through the SEC.

[333] *See* Groshoff, *supra* note 23, at 499 (explaining how psychological and economic factors play a role in market decisions).

[334] *See* Groshoff, *supra* note 23, at 500 (deducing that some traders focus on what they believe others will view as the best product rather than the quality of the product itself). "[N]oise traders. . . evaluate whether to buy or sell assets based on price trends, emotions, or estimations about what other investors in the market will do." *See* Groshoff, *supra* note 23, at 500.

[335] *See* Groshoff, *supra* note 23, at 502 (stating that because buying is done based on emotional factors, the market often spirals).

[336] *See* R. Joseph Cook, *Bitcoins: Technological Innovation Or Emerging Threat?*, 30 J. INFO. TECH. & PRIVACY L. 535, 537 (2014) (arguing that digital virtual currencies such as bitcoin should be outlawed).