SMU | Dedman School of Law

SMU Law Review

Volume 72 | Issue 4 Article 17

2019

"WWW" Marques the Spot: Privateering as a Solution to Cryptocurrency Theft

Joshua Parisi
Southern Methodist University, Dedman School of Law, jparisi@mail.smu.edu

"WWW" Marques the Spot: Privateering as a Solution to Cryptocurrency Theft

*Joshua Parisi**

TABLE OF CONTENTS

* Lead Articles Editor, SMU Law Review Association. Candidate for Juris Doctor 2020, SMU Dedman School of Law; B.S.B.A. & B.A. 2013, University of Arkansas. The author would like to thank his fiancée, family, and friends for all of their love and support. Additional thanks to the staff of *SMU Law Review* for their comments and help.

I. INTRODUCTION

OVER the last three decades, global commerce has been irrevocably changed by the digital revolution. The widespread proliferation of affordable computers, the introduction of the internet, and the growth of mobile-phone technology have changed the way that companies and individuals purchase many of their goods and services. Unfortunately, these advances have come in tandem with a host of new challenges, culminating in the birth and quick rise of "cybercrime." In 2017 alone, the perpetration of cybercrime cost consumers around the globe a whopping $172 billion.[1] Consumers are not the only targets of cybercrime. In 2012, a prolific hacker announced plans to rob a large number of the United States' leading banks in an act that was seen as a protest against the rich.[2] A reputable computer security firm estimated that these attacks could cause losses of "hundreds of millions of dollars," and it was later confirmed that the hacker had "claimed at least 500 cyber victims."[3] Experts have estimated that cybercrime could cost the global economy more than $6 trillion annually by 2021.[4]

Despite the growing cost of cybercrime to the U.S. economy, the government response remains woefully inadequate. The government has advised victims of cyberattacks to merely "contact[ ] the system administrator from the attacking computer to request assistance."[5] Meanwhile, victimized American institutions have spent millions to try to rebuff cybercrime and have begun to actively call for the ability to address cybercriminals with offensive—rather than defensive—measures.[6] While many might suggest that the U.S. military or law enforcement agencies should be responsible for any attempts at aggressive retribution, it is clear that even though "there are numerous individuals with hacking or other computer-savvy abilities, most of these individuals are not within" the armed forces or law enforcement communities.[7] Besides, the Department of Defense has made it clear that its cybersecurity personnel are focused on national security and the protection of government network infra-

1. *2017 Norton Cyber Security Insights Report*, SYMANTEC CORP. 4 (2017), https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf [https://perma.cc/GWD6-PAS3].

2. Christopher M. Kessinger, *Hitting the Cyber Marque: Issuing a Cyber Letter of Marque to Combat Digital Threats*, ARMY LAW., Aug. 2013, at 4, 12.

3. *Id.*

4. Abigail Summerville, *Protect Against the Fastest-Growing Crime: Cyber Attacks*, CNBC, https://www.cnbc.com/2017/07/25/stay-protected-from-the-uss-fastest-growing-crime-cyber-attacks.html [https://perma.cc/3D5E-8JT5] (last updated July 26, 2017, 3:53 PM).

5. Kessinger, *supra* note 2, at 12 (quoting U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 180 (2007), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf [https://perma.cc/T88C-DL5P]).

6. *Id.*

7. SAMUEL P. MOWERY, DEFINING CYBER AND FOCUSING THE MILITARY'S ROLE IN CYBERSPACE 13 (2013); B. Nathaniel Garrett, Comment & Case Note, *Taming the Wild Wild Web: Twenty-First Century Prize Law and Privateers as a Solution to Combating Cyber-Attacks*, 81 U. CIN. L. REV. 683, 698 (2012).

structure, rather than the interests of private companies and individuals.[8] Practically speaking, "The current law, and seemingly political position, is basically forcing U.S. companies to 'just stand and take a beating.'"[9]

Recently, cybercrime has undergone new developments influenced by the growing popularity and accessibility of "cryptocurrency." Cryptocurrencies are "unique, typically encrypted, computer files that can be converted to or from a government-backed currency to purchase goods and services from merchants that accept virtual currencies."[10] In the last ten years, the development of cryptocurrency has threatened to further disrupt the commercial space by fundamentally changing the way that consumers and businesses conceptualize and use money. Even the least tech-savvy have heard of one of the most widely used cryptocurrencies: Bitcoin. Bitcoin is an "anonymous, on-line currency . . . generated by computation ('mining'), purchase, or trade."[11] While Bitcoin does offer a secure alternative payment option for online businesses, it too comes with negatives, like all of the technological advances before it. The anonymity provided by Bitcoin transactions has enabled a whole host of criminal activities to be committed online, including "arms sales, drug dealing, human trafficking, murder-for-hire, money laundering, sale of child porn, and sanctions busting."[12] Bitcoin has also been subject to speculation. While a Bitcoin (using the ticker BTC) could be purchased for roughly $2 in late 2011,[13] the exchange rate shot up to nearly $20,000 per BTC in 2017 before quickly cratering back to an average of around $7,500 per BTC in 2018.[14] As of this writing, Bitcoin's exchange rate is still high relative to its mid-2010 beginnings, as a single Bitcoin can be purchased for approximately $8,000.[15]

Despite Bitcoin's budding potential for criminality and seeming price instability, "it is clear that not only have thousands of blockchain applications been launched, but the biggest firms in many industries are invest-

---

8. *See* Molly Picard, Comment, *Cyberspace: The 21st-Century Battlefield Exposing Soldiers, Sailors, Airmen, and Marines to Potential Civil Liabilities*, 4 NAT'L SEC. L.J. 125, 139–41 (2015).

9. Kessinger, *supra* note 2, at 12–13 (quoting Jeff Bardin, *Caution: Not Executing Offensive Actions Against Our Adversaries Is High Risk*, CSO (Nov. 29, 2012), https://www.csoonline.com/article/2136485/caution—not-executing-offensive-actions-against-our-adversaries-is-high-risk.html [https://perma.cc/6VR6-6BMQ]).

10. Sumit Agarwal, Note, *Bitcoin Transactions: A Bit of Financial Privacy*, 35 CARDOZO ARTS & ENT. L.J. 153, 158 (2016) (quoting *What You Should Know About Virtual Currencies*, CAL. DEP'T OF BUS. OVERSIGHT (Apr. 2014), https://dbo.ca.gov/wp-content/uploads/sites/296/2019/02/Virtual_Currencies_0414.pdf [https://perma.cc/AQ2Z-LK72]).

11. Eric Engle, *Is Bitcoin Rat Poison? Cryptocurrency, Crime, and Counterfeiting (CCC)*, 16 J. HIGH TECH. L. 340, 341 (2016).

12. *Id.* at 333–44.

13. Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 160 (2012).

14. Michael Rosenblat, *Bitcoin Price Speculation for 2019*, YAHOO FIN. (Dec. 27, 2018), https://finance.yahoo.com/news/bitcoin-price-speculation-2019-103004792.html [https://perma.cc/P74P-93ZY].

15. *United States Dollar to Bitcoin (USD to BTC)*, MKTS. INSIDER, https://markets.businessinsider.com/currency-converter/united-states-dollar_btc [https://perma.cc/H63R-CWL6] (last visited Sept. 29, 2019).

ing substantial amounts of resources in blockchain-related efforts."[16] This, in combination with the rapid appreciation of Bitcoin value in the last five years, has caused an enormous upswing in the frequency of Bitcoin theft, or cyber piracy. By 2014, over $500 million worth of Bitcoin had been lost or stolen by cybercriminals,[17] and in just the first half of 2018 cybercriminals stole over $1.1 billion of cryptocurrency.[18] Businesses were targeted the second most in 2018, bearing twenty-one percent of the losses generated by cryptocurrency theft.[19] The United States bore the brunt of cryptocurrency-related thefts, with over twenty-four separate instances reported in 2018.[20] Cryptocurrency theft has become a large problem in the international community too, as one of the world's top Bitcoin exchanges by volume traded was ransacked by cybercriminals for over $30 million worth of cryptocurrencies in June 2018.[21] In the January 2017 hack of Japanese cryptocurrency exchange Coincheck, hackers made off with approximately $500 million worth of cryptocurrencies.[22] Because cryptocurrency theft is only going to become a more prevalent problem as more vendors and larger parts of society accept the technology, many scholars have sought legal methods for victims of cybercrime to fight back.

This paper aims to present a viable method for businesses and individuals to combat cyber piracy through a mechanism that is already present in the U.S. Constitution. Under Article I, Section Eight, "Congress shall have Power To . . . grant Letters of Marque and Reprisal."[23] Traditionally, a letter of marque authorized a private citizen to capture the naval vessels and property of ships sailing under an enemy flag during times of escalated hostilities between two nations.[24] From the fifteenth century until the mid-nineteenth century, letters of marque and reprisal were also used by different nations to augment their naval forces in the struggle against piracy on the high seas through the use of privateers.[25] At the time of the American Revolutionary War, it was generally accepted that a "priva-

16. Benito Arruñada, *Blockchain's Struggle to Deliver Impersonal Exchange*, 19 MINN. J.L. SCI. & TECH. 55, 56 (2018).

17. 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, 324 (2014).

18. Kate Rooney, *$1.1 Billion in Cryptocurrency Has Been Stolen This Year, and It Was Apparently Easy to Do*, CNBC (June 7, 2018, 9:08 AM), https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html [https://perma.cc/RYD2-M9QW].

19. *Id.*

20. *Id.*

21. Jethro Mullen, *Top Bitcoin Exchange Says Over $30 Million in Cryptocurrencies Stolen*, CNN BUS. (June 20, 2018, 5:54 AM), https://money.cnn.com/2018/06/19/technology/bithumb-bitcoin-cryptocurrencies-theft/index.html [https://perma.cc/7W63-NBKL].

22. *Id.*

23. U.S. CONST. art. I, § 8, cl. 11.

24. J. Gregory Sidak, *The Quasi War Cases—And Their Relevance to Whether "Letters of Marque and Reprisal" Constrain Presidential War Powers*, 28 HARV. J.L. & PUB. POL'Y 465, 473 (2005).

25. *See* William Young, Note, *A Check on Faint-Hearted Presidents: Letters of Marque and Reprisal*, 66 WASH. & LEE L. REV. 895, 900, 907 (2009).

teer . . . was a ship armed and fitted out at private expense for the purpose of preying on the enemy's commerce to the profit of her owners, and bearing a commission, or letter of marque, authorizing her to do so, from the Government."[26] Other scholars have noted that "the rules concerning private actor responses to piracy and other unlawful behavior on the high seas" are quite likely "the closest historical analog for today's private sector response to unlawful cyber activity."[27] This is true because, "[l]ike the high seas, the cyber realm is not confined within the territory of individual states . . . [and] it has become a vital pathway of commerce and communication."[28] Privateers were a necessary tool to supplement national navies because "[t]he vastness of seas [allowed] pirates [to] easily commit their crimes undetected."[29]

While the power to issue letters of marque and reprisal has lain dormant since the War of 1812,[30] Congress should revive the practice to effectively authorize "cyber privateers" that would efficiently and cheaply address the growing problem of cyber piracy related to cryptocurrency in private commerce. Part II of this paper addresses the general history of privateering and specifically focuses on past usage of letters of marque and reprisal by the United States. Part III covers the basic characteristics of Bitcoin as the most widespread cryptocurrency and further examines exactly how Bitcoin is stolen. Part IV recommends a theoretical framework for the use of letters of marque to create cyber privateers, and addresses the important role that Bitcoin would serve as the incentive for private entities to operate as cyber privateers. Finally, Part V concludes by analyzing the legal and practical concerns that have been raised by critics of the revival of privateering and discusses several of the possible solutions to these issues.[31]

II. A REMARQUEABLE HISTORY

A. Origins and Golden Age of Privateers

Letters of marque and reprisal have a long and storied history, first originating in the fifth century as the remnants of the Western Roman Empire disintegrated and piracy became more common in the Mediterra-

26. *Id.* at 896–97 (quoting Edgar Stanton Maclay, A History of American Privateers 7 (1899)).

27. Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 Stan. J. Int'l L. 103, 110 (2014).

28. Jeremy Rabkin & Ariel Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea*, 14 Chi. J. Int'l L. 197, 202 (2013).

29. Jennifer J. Rho, Comment, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable Under the Alien Tort Statute*, 7 Chi. J. Int'l L. 695, 713 (2007) (quoting Eugene Kontorovich, *Implementing* Sosa v. Alvarez-Machain*: What Piracy Reveals About the Limits of the Alien Tort Statute*, 80 Notre Dame L. Rev. 111, 152 (2004)).

30. Young, *supra* note 25, at 897.

31. This paper will not consider the military and national security uses of cyber privateering or the possibility of cyber privateers being used to "hack back" in the case of a data breach.

nean Sea.[32] Scholars have theorized that the use of privateers reflected the power vacuum left by the Roman Empire as the feudal European states struggled to provide "private redress and protection of commerce."[33] These proto-letters of marque and reprisal "authorized private merchant ships to carry arms in self-defense."[34] Privateering was widely recognized as separate from piracy, with piracy often carrying harsh punishments while "acts of privateering were explicitly authorized and governed by the rule of law."[35] In the leadup to the Italian Renaissance, as trade began to flourish again in the Mediterranean, privateering authorizations evolved to include many of the restrictions and stipulations that would continue to be used through the decline of privateering.[36] These later examples showed a shift away from use of privateering authorizations as a self-defense measure, as they allowed privateers to "act on [the government's] behalf and seize property belonging to an enemy government, usually in the form of ships and cargo."[37] They often included strict limits on "the amount that could be captured" and frequently "contained an expiration date, after which any capture would be deemed piracy."[38] This practice of authorizing private individuals to attack enemy commerce and combat piracy spread to "the rest of Western Europe by the end of the fourteenth century."[39]

The very first modern letters of marque and reprisal were created by English statute around 1354.[40] While the letters would often be combined into a single document in later usage, letters of marque and letters of reprisal initially had separate meanings.[41] "A letter of marque authorized seizures outside of the sovereign's local jurisdiction" while "a letter of reprisal allowed privateers to capture property within the immediate jurisdiction of the sovereign."[42] Once a privateer had captured an enemy vessel, the privateer would be required to return the vessel and its cargo to one of the letter issuers' ports.[43] The captured vessel would be turned over to that nation's prize courts, which would evaluate the claims of ownership and determine whether the vessel was lawfully taken within the authorization provided by the privateer's letter of marque.[44] If the capture was legitimate, the vessel would be condemned and sold, and the privateer would retain a portion of the proceeds from the sale (as outlined in their letter of marque) while the rest would be seized by the

32. Young, *supra* note 25, at 900.
33. *Id.*
34. Kessinger, *supra* note 2, at 6.
35. Garrett, *supra* note 7, at 688.
36. Young, *supra* note 25, at 900.
37. Kessinger, *supra* note 2, at 6.
38. Garrett, *supra* note 7, at 688.
39. Young, *supra* note 25, at 900.
40. Garrett, *supra* note 7, at 688.
41. *See id.* at 688–89.
42. *Id.* at 689.
43. *Id.* at 688.
44. *Id.*

state.[45] This procedure was replicated by the major European powers and was used extensively during the fifteenth and sixteenth centuries.[46] By 1625, privateers were a common and accepted part of the naval military seascape.[47]

B. Privateers in the American Revolution

While the larger European states had already begun to reduce their reliance on privateers in the late eighteenth century due to their ability to project naval military power on a wider scale, the thirteen American colonies "possessed little in the way of financial resources or naval might during the Revolutionary War."[48] During the war, both the Continental Congress and several of the individual states authorized privateers to plunder British ships in the Caribbean and wider Atlantic Ocean.[49] The young American nation rapidly became "the world's biggest proponent of privateering."[50] Thomas Jefferson encouraged extensive use of privateers and urged the public that "[e]very possible encouragement should be given to privateering in time of war."[51] Jefferson's belief that privateers should be used to supplement the American navy was likely well founded, as the thirteen colonies "had just sixty-four ships in [the] official navy and commissioned only twenty-two 'men of war' during the conflict."[52] Privateers filled in the naval ranks as the Continental Congress and state governments together authorized around 2,000 ships throughout the Revolution.[53] Three thousand eighty-seven British ships and over $10 million in goods were captured under American letters of marque and reprisal during the war, which caused "a great deal of harm to British commerce."[54] Privateering efforts further hindered the British war effort through the capture of "thousands of British seamen" which "depressed the morale of the British public" and ultimately contributed to the shift in sentiment against continuing the war.[55]

Besides their overwhelmingly effective use as an offensive tool, the Americans realized that letters of marque and reprisal were also useful as a means to provide their merchant fleet with the legal authorization for self-defense. Thomas Jefferson wrote:

---

45. Sidak, *supra* note 24, at 473.

46. *Id.* at 468.

47. *See* Hugo Grotius, The Rights of War and Peace 163 n.3 (Richard Tuck ed., Liberty Fund 2005) (1625).

48. Young, *supra* note 25, at 900–02 (citing Harry M. Ward, The American Revolution: Nationhood Achieved 1763–1788, at 184 (1995)).

49. Kessinger, *supra* note 2, at 6–7.

50. Robert P. DeWitte, Note, *Let Privateers Marque Terrorism: A Proposal for a Reawakening*, 82 Ind. L.J. 131, 134 (2007).

51. *Id.*

52. Young, *supra* note 25, at 902.

53. *Id.*

54. *Id.*

55. *Id.*

> The ship Jane is an English merchant vessel . . . employed in the commerce between Jamaica and these States. She brought here a cargo of produce . . ., and was to take away . . . flour. Knowing of the war when she left Jamaica, and that our coast was lined with small French privateers, she armed for her defense[sic], and took one of those commissions usually called letters of marque. She arrived here safely . . . . Can it be necessary to say that a merchant vessel is not a privateer? That though she has arms to defend herself in time of war, in the course of her regular commerce, this no more makes her a privateer, than a husbandman following his plough in time of war, with a knife or pistol in his pocket, is thereby made a soldier? The occupation of a privateer is attack and plunder, that of a merchant vessel is commerce and self-preservation.[56]

Overwhelmingly though, American privateers were motivated not by self-defense but by the nearly limitless profit potential of privateering as an enterprise.[57] George Washington, Thomas Paine, and Benjamin Franklin all owned shares in different privateering ventures during the war.[58] Privateers provided the American public with goods and luxury items that were not generally available due to the British blockade, which bolstered the economy and improved the public morale.[59] Privateers had an amazingly positive effect on American war efforts, which makes it unsurprising that their authorization and legality would be assured in the newly created federal government.

C. Constitutional Recognition and Later Use

Both the Articles of Confederation and later the Constitution provided mechanisms for the new American federal government to issue letters of marque and reprisal. The Articles of Confederation granted the Continental Congress the power to "grant[ ] letters of marque and reprisal in times of peace" and to create "rules for deciding, in all cases, what captures on land or water shall be legal, and in what manner prizes taken by land or naval forces in the service of the United States, shall be divided or appropriated."[60] While the Articles of Confederation are noted for reserving many powers to the states, the framers here were clear that privateering was exclusively a federal-government concern, as they explicitly prohibited the states from issuing letters of marque and reprisal without the consent of the Continental Congress.[61] In 1787, the Constitutional Convention convened in Philadelphia, Pennsylvania, to address some of

56. Theodore T. Richard, *Reconsidering the Letter of Marque: Utilizing Private Security Providers Against Piracy*, 39 Pub. Cont. L.J. 411, 437 (2010) (quoting Letter from Thomas Jefferson to Gouverneur Morris (Aug. 16, 1793), *in* III Thomas Jefferson, Memoir, Correspondence, and Miscellanies, from the Papers of Thomas Jefferson 275 (Thomas Jefferson Randolph ed., 1829)).

57. Young, *supra* note 25, at 903.

58. Kessinger, *supra* note 2, at 7.

59. Young, *supra* note 25, at 903.

60. Articles of Confederation of 1781, art. IX, para. 1.

61. *Id.* art. VI, para. 5.

the issues caused by the Articles of Confederation.[62] A representative from Massachusetts proposed that Congress be granted the power to issue letters of marque and reprisal, and the addition was approved by a unanimous committee vote.[63] Scholars have suggested that the framers may have included this provision as a method "for the sovereign to redress the injuries of its citizens when a declaration of war 'may not be deemed either expedient or necessary.'"[64]

Just under a decade after the ratification of the new Constitution in 1789, Congress had the occasion to issue its first letters of marque and reprisal during the Quasi-War of 1798 against France.[65] However, the impact of the new congressional power to authorize a privateering fleet was not fully brought to bear until the breakout of the War of 1812 with Britain.[66] At the start of the war, the British Navy outnumbered the active American vessels by over sixty-two to one.[67] In response to this dire situation, Congress authorized the issuance of letters of marque and reprisal that would complement the American war effort while also applying tight regulations on the activities of privateers that wished to retain a legally protected status.[68] This legislation required each applicant to "list specific details about the ship, crew, and owners, and 'Ample security' submitted to ensure compliance with both international and United States law."[69] Additionally, each privateer was required to keep a detailed logbook of their daily activities for inspection by any United States Navy vessel met at sea or by the prize courts when returning to port.[70] Specifically, these logs demanded "a true and exact account of . . . the prizes he shall take; the nature and probable value of such prizes; [and] the times and places, when and where taken, and how and in what manner he shall dispose of the same."[71] Any failure to follow these requirements would result in forfeiture of the bond and possible prosecution for piracy.[72] Throughout the conflict, "privateers 'proved to be the only effective American offensive weapon' of a war in which few, if any, significant American war aims were accomplished."[73] American privateers were once again able to inflict huge losses on the British merchant fleet as they captured prizes worth around $39 million at the time.[74]

---

62. *See* Young, *supra* note 25, at 905.
63. Sidak, *supra* note 24, at 477.
64. Young, *supra* note 25, at 906 (quoting JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES 411 (Carolina Academic Press 1987) (1833)).
65. *Id.* at 897 (citing ALEXANDER DECONDE, THE QUASI-WAR: THE POLITICS AND DIPLOMACY OF THE UNDECLARED WAR WITH FRANCE, 1797–1801, at 124 (1966)).
66. Kessinger, *supra* note 2, at 7.
67. *Id.*
68. An Act Concerning Letters of Marque, Prizes, and Prize Goods, ch. 107, § 9, 2 Stat. 759, 761 (1812) [hereinafter 1812 Privateering Act].
69. Kessinger, *supra* note 2, at 7.
70. *Id.* (citing 1812 Privateering Act, § 9, 2 Stat. at 761).
71. 1812 Privateering Act, § 10, 2 Stat. at 762.
72. Kessinger, *supra* note 2, at 7.
73. Young, *supra* note 25, at 907 (quoting DOROTHY DENNEEN VOLO & JAMES M. VOLO, DAILY LIFE IN THE AGE OF SAIL 235 (2002)).
74. Kessinger, *supra* note 2, at 7.

D. Decline of Privateering and the Paris Declaration of 1856

In the late eighteenth and early nineteenth centuries, privateering entered a slow but steady decline.[75] As the major European powers expanded their territories, "the need for private protection and reprisal diminished; the sovereign was able to protect the interests of its subjects without resort to private warfare."[76] While privateers remained active well into the nineteenth century, in 1778, France was the last European power to issue a letter of marque.[77] In the United States, the end of the War of 1812 saw the final authorization of privateers by the federal government.[78] While President Andrew Jackson proposed the use of privateers against another quasi-conflict with France in the 1830s, Congress never enacted the measure.[79] However, during the Texas War of Independence, the Texas legislature issued letters of marque for privateers to "protect the coast, harass Mexican shipping, and bring prizes that could be auctioned off, with part of the proceeds going to the public treasury."[80] Even in this instance though, the usage of privateers was greatly diminished compared to the American Revolution and War of 1812, as the Texans only granted six letters of marque and reprisal for the entirety of the six-month-long war.[81]

At the Congress of Paris in 1856, several of the major European powers met to settle the peace terms for the recently ended Crimean War.[82] Damage to the shipping and commerce interests of all nations involved led the negotiating parties to consider the termination of privateering as an internationally accepted part of naval warfare.[83] In particular, British naval authorities feared that "[t]he Maritime population of the United States . . . might furnish to Russia the elements of a fleet of privateers, which attached to its service by Letters of Marque and covering the seas with a network would harass and pursue [their] commerce even in the most remote waters."[84] After their experiences at the hands of privateers during the American Revolution and the War of 1812, the British were keenly aware of the power of privateers to augment the navies of weaker nations in a challenge to their own naval supremacy.[85]

---

75. Young, *supra* note 25, at 901, 907.
76. *Id.* at 900–01.
77. *Id.* at 901.
78. *Id.* at 907.
79. Kessinger, *supra* note 2, at 7 (citing Francis H. Upton, The Law of Nations Affecting Commerce During War: With a Review of the Jurisdiction, Practice and Proceedings of Prize Courts 175 (1863)).
80. *Id.* at 7–8.
81. *Id.* at 8 (citing *Fortune Favors the Brave—The Story of the Texas Navy: Texas Privateers*, Tex. State Library & Archives Comm'n, https://www.tsl.texas.gov/exhibits/navy/privateers.html [https://perma.cc/PD6Z-CG7U] (last modified June 24, 2019)).
82. Garrett, *supra* note 7, at 689.
83. Rosenzweig, *supra* note 27, at 112.
84. Travers Twiss, Belligerent Right on the High Seas, Since the Declaration of Paris (1856), at 10 (1884).
85. Kessinger, *supra* note 2, at 8.

The parties eventually settled on the final language of the Paris Declaration of 1856, which essentially forbade signatories from issuing new letters of marque and reprisal.[86] The relevant parts of this agreement read:

> The above-mentioned Plenipotentiaries, being duly authorized, resolved to concert among themselves as to the means of attaining this object; and, having come to an agreement, have adopted the following solemn Declaration: (1) Privateering is, and remains, abolished; (2) The neutral flag covers enemy's goods, with the exception of contraband of war; (3) Neutral goods, with the exception of contraband of war, are not liable to capture under enemy's flag; (4) Blockades, in order to be binding, must be effective, that is to say, maintained by a force sufficient really to prevent access to the coast of the enemy.[87]

Importantly, the drafters of the Paris Declaration were careful to make certain that the agreement only bound the signatory nations.[88] Eventually forty-five other nations joined the original signatories to the treaty, but the United States refused to be bound by the agreement.[89] American naval authorities seemed to believe that the Paris Declaration was merely a tool for the European powers, and specifically the British, to suppress the seafaring capabilities of smaller nations.[90] Secretary of State William L. Marcy later voiced his opinion that "the United States could not forgo the right to send out privateers, which in the past had proved her most effective maritime weapon in time of war, and which, since she had no large navy, were essential to her fighting power."[91] American diplomats also worried that the Paris Declaration did not provide for the absolute "protection of all non-contraband private property from capture at sea."[92] Both of these concerns weighed heavily enough on American diplomats to reject the Paris Declaration, which left the United States free to continue issuing letters of marque and reprisal in the future.[93]

The final chapter of naval privateering in American history was written during the Civil War. In April 1861, Confederate President Jefferson Davis "issued letters of marque against Northern shipping" with the approval of the newly formed Confederate Congress.[94] While the Confederacy openly embraced privateering, Union diplomats initially made it widely known that they would honor the Paris Declaration and even attempted to join the United States as a signatory.[95] Commentators have suggested that Union leaders may have feared "the involvement of the

86. *See* Paris Declaration Respecting Maritime Law, Apr. 16, 1856, *available at* https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=473FCB0F41DCC63BC12563CD0051492D [https://perma.cc/HK9L-F7FC].

87. *Id.*

88. Kessinger, *supra* note 2, at 8.

89. Garrett, *supra* note 7, at 689.

90. Kessinger, *supra* note 2, at 8 (citing EPHRAIM DOUGLASS ADAMS, GREAT BRITAIN AND THE AMERICAN CIVIL WAR 141 (1925)).

91. ADAMS, *supra* note 90, at 141.

92. Kessinger, *supra* note 2, at 8.

93. Garrett, *supra* note 7, at 689.

94. Kessinger, *supra* note 2, at 8–9.

95. *Id.* at 9.

British or French navies in the conflict," a condition that could have exposed the Union to a much broader conflict on the international stage.[96] These efforts were ultimately futile; British vessels entered the conflict, and the Union subsequently authorized its own letters of marque and declared that any privateers sailing under the Confederate flag would be treated like pirates if captured.[97] Here, the legacy of the Paris Declaration was called into question, as an international tribunal asked to determine the liability of Britain for damages caused by a privateer operating under a Confederate letter of marque "found no issue with a non-signatory (the Confederacy) issuing letters of marque to a signatory (Britain) 'to construct, furnish, and crew ships to be used in commerce raids against a non-signatory, the United States.'"[98]

Even though Congress has not exercised its power to grant letters of marque and reprisal since the conclusion of the Civil War, this inactivity is not reflective of a general acceptance of a prohibition of privateering. During the Spanish-American War, the idea of again turning to privateer forces was acknowledged by President McKinley, who announced that the United States would voluntarily comply with the provisions of the Paris Declaration while retaining the legal right to issue letters of marque if needed.[99] At the Hague Peace Conference in 1907, the United States continued to insist on its unrestrained right to authorize privateers because "[i]t [was] well known that the Government of the United States of America has not adhered to that Declaration."[100] Doubtless, the United States still has the power to issue new letters of marque and reprisal and could utilize this power to enable lawful cyber privateers without violating existing international law.

III. CRYPTOCURRENCY AS CONTEMPORARY DOUBLOONS

A. General Characteristics of Bitcoin and Blockchain

The need for cyber privateers derives from the widespread adoption of cryptocurrency, and specifically Bitcoin, by modern businesses and consumers. As discussed above, a "Bitcoin is a digital, decentralized, partially anonymous currency, not backed by any government or other legal entity,

96. *Id.*

97. An Act Concerning Letters of Marque, Prizes, and Prize Goods, ch. 85, 12 Stat. 758, 759 (1863); *see* James Russell Soley, The Blockade and the Cruisers 170 (1883) (noting the Union never issued a letter of marque during the Civil War and that captured Confederate privateers would be subject to execution after conviction).

98. Kessinger, *supra* note 2, at 9 (quoting Todd Emerson Hutchins, Comment, *Structuring a Sustainable Letters of Marque Regime: How Commissioning Privateers Can Defeat the Somali Pirates*, 99 Calif. L. Rev. 819, 857 (2011)).

99. Alexander Porter Morse, *Rights and Duties of Belligerents and Neutrals from the American Point of View*, 46 Am. L. Reg. 657, 660 (1898).

100. United States, The Second International Peace Conference, Held at the Hague from June 15 to October 18, 1907: Instructions to and Report from Delegates of the United States, Conventions and Declarations, Final Act, with Draft of Convention Relative to the Conventions 40 (1908).

and not redeemable for gold or other commodity."[101] Supporters of Bitcoin have embraced it because it is highly liquid, generally has low transaction costs, can be used to make micropayments across the internet, and affords buyers and sellers a degree of anonymity that is not usually attainable through the use of traditional currencies or credit cards.[102] Bitcoin draws its origins to the early 1990s, when certain online groups disdainful of government currency regulations desired a decentralized and private method of exchange that would enable cooperation amongst pseudonymous users.[103] A workable solution was eventually developed in the form of Bitcoin, which creator Satoshi Nakamoto (a pseudonym) released to the internet at large in the late 2000s.[104] Nakamoto believed that Bitcoin would address "the inherent weaknesses of the trust based model" that serves as a basis for the modern global commerce framework because Bitcoin is "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[105]

Nakamoto's major breakthrough came in the form of the blockchain protocol that allowed Bitcoin to function. At a high level, blockchain provides a sort of ledger where all transactions involving a Bitcoin are "publicly announced" and each exchange cannot proceed until "participants [in the network] . . . agree on a single history of the order in which they were received."[106] This prevents a Bitcoin from being spent more than one time by any participant in the system.[107] Once a transaction has been verified, it is recorded as a "block" in the chain of data that records the movement of all available coins within the system.[108] This ledger allows the public to see that Bitcoins are being exchanged amongst different users of the system but also provides for relative anonymity by associating only a "public key" with the users sending and receiving Bitcoin.[109] These public keys protect the identities of their holders like usernames on a website so that the public ledger is more "similar to the level of information released by stock exchanges, where the time and size of individual trades, the 'tape', is made public, but without telling who the parties were."[110] Blockchain essentially allows Bitcoins to be transferred to and from different users without the need for government control and pre-

101. Grinberg, *supra* note 13, at 160.
102. *Id.*
103. *Id.* at 162.
104. *Id*; *see* Bernard Marr, *A Short History of Bitcoin and Crypto Currency Everyone Should Read*, FORBES (Dec. 6, 2017, 12:28 AM), http://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#7e0cba413f27 [https://perma.cc/TZK6-S6TN]. *See generally* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN, http://bitcoin.org/bitcoin.pdf [https://perma.cc/P9DF-TAN9] (last visited Sept. 9, 2019).
105. Nakamoto, *supra* note 104, at 1.
106. *Id.* at 2.
107. *Id.*
108. *Id.* at 3–4.
109. *Id.* at 6.
110. *Id.*

vents users from being forced to reveal their identities to the counterparty or to the general public.

Individual Bitcoins are created through a complex set of computations known as mining.[111] When participants in the system "opt to lend their computational resources to the Bitcoin network to perform the demanding computational work needed to support" the verification of transactions on the blockchain, they are rewarded for their efforts by the distribution of new Bitcoins based on their share of the work.[112] Nakamoto designed the system to incentivize users to provide the extensive amounts of computational power that would be needed to run the network and as "a way to initially distribute coins into circulation, since there is no central authority to issue them."[113] While the early mining efforts were the product of individual early adopters attempting to make the system work, enterprising individuals soon realized that mining operations could be more efficiently "conducted by large-scale GPU farms with multiple graphics processing units . . . working to perform the requisite calculations."[114] The entire process is rather similar "to gold miners expending resources to add gold to circulation," leading to the adoption of the term "mining."[115] To protect the value of Bitcoin from rampant inflation, Nakamoto included a mechanism that increased the difficulty of the computations as the number of miners increased, which effectively acts to cap the number of Bitcoins that can possibly be created.[116] In 2012, approximately fifty Bitcoins were issued every ten minutes.[117] This rate has slowed since then, and the total supply of Bitcoin will eventually be capped near 21 million coins.[118] Similar to the U.S. dollar, Bitcoins are divisible, although they can be subdivided out to eight decimal places instead of only two.[119]

Individuals and businesses have several different options to obtain Bitcoins. As detailed above, Bitcoins can be mined, although the enormous amounts of electricity and computing power necessary to generate a single coin have largely rendered this unprofitable for individuals in the last five years.[120] Alternatively, Bitcoin can be obtained through the purchase and sale of goods and services.[121] Many different online vendors now accept Bitcoin, including auction sites, web hosts, technology consulting firms, non-profit organizations, and even retail establishments.[122]

---

111. Engle, *supra* note 11, at 341.
112. *Id.* at 347 n.5 (quoting Pamela J. Martinson & Christopher P. Masterson, *Bitcoin and the Secured Lender*, 33 BANKING & FIN. SERVS. POL'Y REP. 13, 13–14 (2014)).
113. Nakamoto, *supra* note 104, at 4.
114. Engle, *supra* note 11, at 347 n.5 (quoting Martinson & Masterson, *supra* note 112, at 13–14).
115. Nakamoto, *supra* note 104, at 4; Engle, *supra* note 11, at 347 n.5.
116. Grinberg, *supra* note 13, at 163.
117. *Id*.
118. *Id.*
119. *Id.*
120. *Id.* at 167; *see* Nakamoto, *supra* note 104, at 4.
121. Engle, *supra* note 11, at 341.
122. Grinberg, *supra* note 13, at 165–66.

The anonymity afforded by Bitcoin has given rise to its popularity as a method of exchange for online casinos and adult novelty shops, and it has unfortunately also been used in illegal marketplaces to trade for illicit drugs, firearms, and even certain criminal services.[123] Finally, Bitcoins can be purchased for government-backed currency (like the U.S. dollar, the Euro, or the Japanese yen) or for other forms of cryptocurrency on specialized Bitcoin exchanges.[124] These exchanges allow Bitcoin to be traded for a relatively similar value across the globe, although the "exchange rate between Bitcoin and traditional currencies has fluctuated wildly . . . compared to the relatively small movements often seen between traditional currency pairs."[125] The Mt. Gox online exchange, which at one time was the largest Bitcoin exchange in existence, recorded daily trading volumes of approximately $10,000 worth of Bitcoin per day in March 2011.[126] Unlike traditional foreign currency trading, Bitcoin exchanges generally do not offer futures trading although options can be purchased over the counter.[127]

Generally, Bitcoins can be accessed through the use of a computer program known as a "Bitcoin client" or through the creation of an account on one of the many websites that runs this program for their clients in an easier-to-navigate interface.[128] The string of code that makes up a Bitcoin is saved to a file known as a "Bitcoin wallet," which must be kept secure.[129] This wallet file contains the public key, discussed above, and also a private key that a user must enter into the Bitcoin client to access the Bitcoins stored in the file.[130] Many of the major exchanges offer "transaction services, allowing individuals to keep, send, and receive [B]itcoins without ever running the Bitcoin client on their own computers."[131] These services are convenient for the common consumer, but they have been plagued with a serious problem: cyber piracy.[132]

B. The Growing Threat of Bitcoin Theft

For the last decade, cyber pirates have targeted both individual holders of Bitcoin and Bitcoin exchanges at an alarming rate. Since their creation, Bitcoins have been subject to loss and theft similar to traditional currency.[133] The blockchain itself is resistant to tampering, but individual

123. *Id.* at 165; Engle, *supra* note 11, at 343–44.
124. Engle, *supra* note 11, at 341 n.5 (quoting Martinson & Masterson, *supra* 114, at 13–14).
125. *Id.*
126. Grinberg, *supra* note 13, at 166.
127. *Id.*
128. *Id.* at 162–63.
129. *Id.* at 163.
130. 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).
131. Grinberg, *supra* note 13, at 167.
132. Engle, *supra* note 11, at 353.
133. *Id.*; Grinberg, *supra* note 13, at 180.

wallet files are not.[134] Bitcoins can only be stolen from individual holders "when someone completes an unauthorized transfer out of the authorized user's wallet by stealing the user's private access key."[135] While the necessity of both the public and private key to access a wallet file does provide a modicum of security, hackers have found increasingly refined ways "to seize an account's private key."[136] Owners of Bitcoin have been consistently warned to "backup and secure [their] Bitcoin wallet[s]," if they keep their wallet files on their personal computers.[137] However, personal computers have been particularly vulnerable to viruses that install themselves onto a user's computer and then automatically allow the cyber pirate who created the virus to access that user's wallet.[138] In early 2011, one Russian scammer was able to steal over 150 Bitcoins from unwary users.[139] The victims had each installed a program that purported to back up their wallet files for added security but was actually transmitting each victim's Bitcoins to the scammer.[140]

Although Bitcoin exchanges and transaction services providers should arguably be able to provide more security to their clients, they have fallen prey to some of the most ambitious thefts yet perpetrated. In fact, the largest Bitcoin thefts on record occurred when hackers attacked exchanges, rather than individual owners of Bitcoin.[141] Cyber pirates are responsible for raids on several different exchanges, including TradeHill, Bitcoinica, and Mt. Gox, to the tune of millions of dollars' worth of cryptocurrency plunder.[142] Some commentators have argued that exchanges are frequently targeted because "the current trading infrastructure 'is riddled with security/efficiency problems,'"[143] and a significant "lack of oversight . . . permits" exchanges to operate without the safeguards necessary to prevent criminals from easily infiltrating their internal networks.[144] Unlike when an FDIC-insured bank is robbed, when exchanges are hacked, their customers bear the brunt of the losses because "Bitcoin transactions are not insured against loss."[145] Scholars have noted that this is one of the major areas where Bitcoin falls behind traditional currencies, as it currently offers little chance of recovery.[146]

---

134. Arruñada, *supra* note 16, at 98 n.3.
135. Swartz, *supra* note 17, at 323.
136. Engle, *supra* note 11, at 354.
137. Grinberg, *supra* note 13, at 180.
138. *Id.* at 180, 184 n.88.
139. *Id.* at 184 n.88.
140. *Id.*
141. Daniel Shane, *$530 Million Cryptocurrency Heist May be Biggest Ever*, CNN (Jan. 29, 2018, 11:55 AM), http://www.money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html [https://perma.cc/RB5G-MGEN].
142. Engle, *supra* note 11, at 385.
143. Denis T. Rice, *The Past and Future of Bitcoins in Worldwide Commerce*, BUS. L. TODAY, Nov. 2013, at 1, 4.
144. Conor Desmond, *Bitcoins: Hacker Cash or the Next Global Currency?*, 19 PUB. INT. L. REP. 30, 31 (2013).
145. Swartz, *supra* note 17, at 324.
146. *Id.*

The cautionary tale of the Mt. Gox exchange is one of the largest publicity hits ever suffered by a Bitcoin exchange. The Mt. Gox exchange was founded in 2010 and, for the first half of the 2010s, dominated the market for Bitcoin transaction services.[147] While Mt. Gox was attacked once in 2011, that breach was relatively small, and the exchange was able to keep the story from spreading widely across the Bitcoin community.[148] By 2013, the Mt. Gox exchange was handling an estimated eighty percent of the world's Bitcoin transactions.[149] During February 2014, customers of the Mt. Gox exchange were shocked as the exchange first suspended withdrawals from user accounts, then suspended trading entirely, and finally closed the platform before filing for bankruptcy protection in Japan.[150] Documents were eventually leaked, which showed that cyber pirates were able to make off with around $473 million worth of cryptocurrency with the exchange's customers bearing nearly ninety percent of the loss.[151]

The repercussions of the Mt. Gox hack still affect the Bitcoin economy today, as the CEO of the exchange is facing criminal charges in Japan, and Bitcoin exchanges have since been subjected to higher levels of regulatory scrutiny than ever before.[152] However, even as nations have started to bring their regulatory power to bear on the problems presented by Bitcoin, one major issue has evaded a workable solution—How can Bitcoins that have been stolen by cyber pirates be returned to their rightful owners?

IV. HOW CYBER PRIVATEERS CAN CRUSH THE BLACKBEARDS OF THE MODERN AGE

A. Adapting Letters of Marque to Cyberspace

Congress can exercise its constitutional power to issue letters of marque and reprisal to authorize a new force of cyber privateers. Victims of Bitcoin piracy could seek out these specialists, who would then provide cheap and efficient redress. Article I, Section Eight of the Constitution states, "Congress shall have Power To . . . grant Letters of Marque and Reprisal."[153] As discussed above, the United States has retained this ability despite the agreement of other nations to forgo the practice.[154] This section argues how letters of marque should be adapted to provide legal authorization for cyber privateers to recover stolen digital assets, how existing prize court legislation for naval captures could be implemented in a

147. Darryn Pollock, *The Mess That Was Mt. Gox: Four Years On*, Cointelegraph (Mar. 9, 2018), https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on [https://perma.cc/CMU6-3284].
148. *See id.*
149. *Id.*
150. *Id.*
151. *Id.*
152. *Id.*
153. U.S. Const. art. I, § 8, cl. 11.
154. *See supra* Part II.D.

cyber context, and how Bitcoin would play an extremely important role as the profit motive to incentivize private parties to partake in the new framework.

1. Issuing Cyber Letters of Marque and Supervising Cyber Privateers

A legislative basis for the issuance of new cyber letters of marque and subsequent supervision of the cyber privateers can be found in the authorizations made for privateers on the high seas during the Revolutionary War and the War of 1812. Congress could either grant the power to issue letters of marque and reprisal to the President, or it could delegate that power directly to a new or existing administrative agency.[155] Congress could then lay out the requirements that any applicant for a cyber letter of marque would have to satisfy before approval. In the 1812 Privateering Act, Congress required "[t]hat all persons applying for letters of marque and reprisal . . . shall state in writing the name . . . and force of the vessel, and the name and place of residence of each owner concerned therein, and the intended number of the crew."[156] Modern legislation might require that each applicant name the computer security firm that is applying for the letter of marque, the owners of said firm, and the number of computer specialists that the firm intends to set to work on recovering stolen assets. Other commentators have suggested that a "central government database . . . would provide the supervising agency with a means of . . . policing cyber privateers and holding them accountable."[157]

Additionally, the 1812 Privateering Act required that each "owner . . . of the ship . . . and the commander thereof, for the time being, shall give bond to the United States . . . with condition that the owners, officers, and crew . . . will observe the treaties and laws of the United States."[158] Congress could demand that each applicant put up a bond, which would serve the dual purposes of (1) screening out smaller, undercapitalized firms that may not have the financial resources to provide redress in the case of any improper captures; and (2) ensuring that each cyber privateer has sufficient "skin in the game" to discourage illegal activity. The bond should be large enough to deal a severe financial blow to the firm should it ever be forfeited. With the immense amount of profit that these firms stand to make, a bond in the low millions of dollars would likely suffice.

Finally, Congress could require that each member of the modern "crew" have a requisite level of education in computer science before allowing them to operate as cyber privateers. While the 1812 Privateering Act did not give any training requirements for the seamen that may be aboard a privateering vessel, an education requirement would provide the supervising agency another opportunity to preemptively vet all of the firm's personnel. Like demanding a bond, setting a minimum educational

155. *See* 1812 Privateering Act, ch. 107, § 1–2, 2 Stat. 759, 759 (1812).
156. *Id*. § 2.
157. Kessinger, *supra* note 2, at 19.
158. 1812 Privateering Act, § 3, 2 Stat. at 759.

threshold would also operate to "keep the cyber cutthroats out of this business" by making sure that only those computer technicians "with the requisite discretion and technical expertise are . . . acting with congressional authority as a cyber privateer."[159]

Once a cyber letter of marque has been issued, Congress could require that each computer-security firm keep a log of the individual technician's actions online, back up any capture by evidence of attribution, and immediately declare each capture to the supervisory agency. The 1812 Privateering Act set out that each "commanding officer of every vessel having a commission . . . shall keep a regular journal" of their daily sailing activities and the specific details of any prizes that were taken.[160] The commander was required to turn over this log to any U.S. naval officer whom he might encounter while at sea and also to present his log to naval authorities when the vessel returned to port after a voyage.[161] This could easily be applied to cyber privateers who would merely be asked to keep a record of their online activity, and specifically, facts relating to any seizure of digital assets. This would allow the supervisory agency to police the privateers and would serve as another deterrent to prevent them from acting outside of their letter of marque.

A unique issue presented by cyber privateering, and specifically the recovery of cryptocurrency like Bitcoin, is the problem of attribution. To prove that the digital assets being seized by a cyber privateer are actually stolen, it would be necessary for the original theft to be attributed to the actor being attacked by the privateer.[162] This issue is similar to that presented by identifying an enemy naval ship but can be much more difficult. While it is theoretically easy to track an individual's online activity, in practice it can present several difficulties, especially in an asset-recovery context.[163] In the past, the anonymity provided by Bitcoin transactions made it very difficult, if not impossible, for the activities of hackers and thieves to be monitored on a large scale.[164] However, recent advances in the analysis of the blockchain ledgers have led researchers to conclude that "[B]itcoin transactions are . . . pseudonymous, not anonymous."[165] Because all Bitcoin transactions are recorded in a manner allowing all users to see the public keys associated with any given exchange, some scholars have suggested that modern computer science techniques might allow authorities to identify all users of Bitcoin in the near future.[166] Even cyber pirates must have public keys that can "accept" stolen

159. Kessinger, *supra* note 2, at 20.
160. 1812 Privateering Act, § 10, 2 Stat. at 761–62.
161. *Id.* § 11, 2 Stat. at 762.
162. *See* Rosenzweig, *supra* note 27, at 116.
163. *See* Rabkin, *supra* note 28, at 236–37 (explaining that perpetrators of cybercrime "can be hard to locate with precision or with perfect confidence").
164. *See* Agarwal, *supra* note 10, at 157.
165. *Id.* at 160.
166. Engle, *supra* note 11, at 393 n.303 (quoting Nicholas Godlove, Note, *Regulatory Overview of Virtual Currency*, 10 OKLA. J.L. & TECH. 71, 82 (2014)). Nicolas Godlove stated:

Bitcoin for the transaction to be recorded in the ledger. These advances would allow cyber privateers to track the movement of stolen Bitcoins from their rightful owner to the public keys of the pirates, who could then be identified. Congress could require that this evidence be collected and presented with the prize at the time of "capture," which would mitigate the chances of any erroneous seizures.

Privateers of old were commanded to bring their prizes to U.S. ports, where the prize would be turned over to the prize courts for condemnation.[167] Similarly, Congress could demand that cyber privateers immediately declare any capture to the supervisory agency and then refer the seizure to prize courts for official condemnation. An immediate declaration would ensure that the prize cause was commenced while the relevant evidence was still fresh and would provide any aggrieved party a quick opportunity to rebut the seizure. A prize court system would render important checks on the actions of cyber privateers, as these courts would evaluate whether the evidence of attribution is believable and would ultimately determine whether the capture was made within the bounds of the privateer's letter of marque. Luckily, Congress has already created a framework for naval privateering that could be modified for cyber privateering.

2. A Theoretical Framework for Cyber Prize Courts

Congress can refashion the existing legislation for naval prize courts to administer the prize causes generated in cyberspace. Prize courts are judicial tribunals that operate to "allow[ ] privateers, or private individuals acting pursuant to governmental commissions, to seize the assets of enemy ships and retain the assets as their legitimate capture."[168] The body of law generated by prize courts is applicable to modern piracy in cyberspace because it shares many characteristics with the piracy that once troubled the high seas. Before the development of maritime law, the ocean was a relatively lawless place. During a long journey, ships could "be miles away from nearby witnesses, police, or courts."[169] The ocean was (and still is) critical to commerce and, even today, there are troubles with piracy in certain parts of the world.[170] The internet too has developed into an important part of global trade. Like the ocean during the Age of Exploration, it is difficult for governments to impose the rule of law on the vast reaches of cyberspace as technological constraints, jurisdictional challenges, and the dispersed nature of the internet's users

> 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.

Id.

167. 1812 Privateering Act, ch. 107, § 6, 2 Stat. 759, 761 (1812).
168. Garrett, *supra* note 7, at 688.
169. *Id.* at 687.
170. *Id.*

"have forestalled the ability of governments to effectively regulate it."[171]

Although Congress has not authorized the issuance of any new letters of marque and reprisal for over two centuries, during the 1950s, it preemptively passed reworked procedures for new prize court proceedings should U.S. privateers ever again capture enemy vessels during a time of war.[172] This legislation "applies to all captures of vessels as prize during war by authority of the United States" but does not cover "[p]roperty seized or taken upon the inland waters of the United States by its naval forces."[173] Congress could amend the legislation to cover all captures of cryptocurrency made under the authority of a letter of marque, whether seized from American or foreign criminals.

The procedures of a prize cause are relatively simple. Congress granted the federal district courts "original jurisdiction, exclusive of the courts of the States, of each prize and each proceeding for the condemnation of property taken as prize."[174] "[P]roceedings for the adjudication of the prize cause" can be brought either in the district court closest to the port where the prize was turned over to the government or in a venue chosen by the Attorney General if the capture was made in territorial waters of a consenting cobelligerent.[175] The proceedings must commence within a reasonable time, or "any party claiming the captured property may . . . bring an original suit for restitution."[176] These procedures could easily be adapted for a prize cause pertaining to digital assets that have been seized by cyber privateers. The district court where a cyber privateer operates would have jurisdiction over prize causes relating to any captures made by that privateer, and the requirement that proceedings be started within a "reasonable time" would provide a safeguard against an innocent party's assets being seized and held without a reasonably speedy hearing.

Once a captured vessel has been brought into U.S. jurisdiction, government officials and the privateer have several different roles and responsibilities to fulfill. U.S. attorneys are responsible for representing the United States in any prize cause brought within their judicial district.[177] They are charged with "protect[ing] the interests of the United States and . . . examin[ing] all fees, costs, and expenses sought to be charged against the prize fund."[178] The commanding officer of the vessel that effectuates the capture must supply any relevant documents and the wit-

171. *Id.* at 690.
172. 10 U.S.C. §§ 8851–8881 (1956).
173. *Id.* § 8851(a)–(c).
174. *Id.* § 8852(a). This jurisdiction only applies to prizes that are brought into "(1) the United States, or the Commonwealths or possessions; (2) . . . the territorial waters of a cobelligerent; (3) . . . a locality in the temporary or permanent possession of, or occupied by, the armed forces of the United States; or (4) appropriated for the use of the United States." *Id.* § 8852(a)(1)–(4). This jurisdiction can only be exercised over prizes captured or brought into the waters of a cobelligerent if that nation consents to the proceedings. *Id.* § 8852(c).
175. *Id.* § 8853(a)–(b).
176. *Id.* § 8854(2).
177. *Id.* § 8856(a).
178. *Id.*

nesses of the capture to the prize commissioner for investigation.[179] Prize commissioners are appointed to serve in each judicial district,[180] and they are responsible for taking possession of the proof of lawful capture, creating interrogatories for the privateer, interviewing any witnesses, and reporting all of their findings to the prize court.[181] Once the prize commissioner has gathered all of the necessary evidence, the U.S. attorney "shall promptly—(1) file a libel against the prize property; (2) obtain a warrant from the court directing the marshal to take custody of the prize property; and (3) proceed to obtain a condemnation of the property."[182] In a cyber privateering prize cause, these duties could remain relatively unchanged. The U.S. attorney would still represent the U.S. government, and the prize commissioner would still be charged with collecting evidence to present before the prize court. Only the role of the "commanding officer" would be altered. The privateer would be required to produce all of their online history logs, detailed information of exactly how the seizure was made, and the information for the new account where the seized Bitcoins were being held.

Finally, assuming that the prize court determined that the seizure was made lawfully within the restrictions of the privateer's letter of marque, the shares of the prize would be divided. Normally the prize court would order the sale of the condemned prize,[183] which would then be performed by an auctioneer after notice had been posted for several days.[184] However, when a privateer recovers private property that was captured by the enemy, "the court shall restore the property to its owner upon his claim and on payment of such sum as the court may award as salvage, costs, and expenses."[185] In the case of stolen Bitcoins, this section would not need to be changed at all. An individual robbed of their Bitcoins would only need to file a report with the cyber privateering oversight agency, which would then alert the privateers of the theft. Once a privateer located and recovered the cryptocurrency, the prize courts would merely turn the Bitcoins back over to the rightful owner, while allowing the privateer to take a percentage of the Bitcoin as payment for their services. In this way, changes can be made to the preexisting legal framework to provide for workable and efficient procedures to affirm the legality of captures and return Bitcoins to their owners.

3. Bitcoin as a Profit Motive

Bitcoins play an exceedingly important role in this proposed cyber privateering framework, as they would serve as the profit motive necessary to incentivize those with the skills to act as cyber privateers to perform

179. *Id.* § 8857.
180. *Id.* § 8855(a).
181. *Id.* § 8860.
182. *Id.* § 8859(a).
183. *Id.* § 8865(a)(1).
184. *Id.* § 8866.
185. *Id.* § 8872(c).

this work. During the American Revolution, the privateers did not attack British merchant shipping for private redress.[186] They "sailed for the profits they would receive by capturing and selling goods[,] . . . [which] were potentially enormous."[187] One of the greatest problems that other proposals for cyber privateering have faced is the lack of a reasonable incentive for skilled computer technicians to dedicate their time and energy to working within the strict legal framework of privateering.[188] In an information security context, this problem is especially troubling as the information that cyber privateers would be protecting or recovering could hypothetically be sold to provide the privateer with some share of the value, and that would defeat the entire purpose of creating cyber privateers in the first place.[189] Another issue with information is that it has no set value; any sale designed to get the highest price would almost certainly require some sort of auction, which again contravenes the intention of authorizing privateers at all.[190] Some scholars have suggested that Congress could circumvent this problem by paying privateers a flat fee for their services.[191] This solution would require that the taxpayers fund the program, which is not desirable. The situation before the introduction of cryptocurrency seemed to leave scholars between a rock and a hard place, as cyber privateers would either need to be repaid out of public funds or through the creation of unsavory secondary markets that would essentially undermine the purpose of a cyber privateering program.

However, a regime aimed at the recovery of stolen Bitcoins proffers a way to build cyber privateering around a marketable asset that could be easily valued and sold without revealing sensitive information or placing the privateers on the taxpayer's dime. Bitcoin is different from information because cryptocurrencies have defined values set by exchanges.[192] The availability of an exchange rate determined by the market from thousands of transactions per day eliminates the need for an auction to dispose of the seized Bitcoins. The court could simply refer to the prevailing exchange rate between BTC and USD at the time of condemnation and then take a predetermined percentage of that value to pay the cyber privateer, as well as the court costs associated with the prize cause. The remainder of the Bitcoins could then be returned to their original owner(s). In this way, the private party would receive the benefits from recovery of their Bitcoins for a reasonable commission, and justice would be done without any subsidy from taxpayers. Additionally, Bitcoins are not like sensitive information in that they can be sold without completely subverting the purpose of authorizing cyber privateers. Ultimately, this

186. Young, *supra* note 25, at 903.
187. *Id.*
188. *See* Garrett, *supra* note 7, at 705 (noting that, in a national defense context, Congress would have to determine "what economic incentives . . . hackers [would] receive for preventing cyber attacks").
189. *See id.*
190. *See id.*
191. *See id.*
192. Grinberg, *supra* note 13, at 167.

would allow for victims of Bitcoin theft to recover their stolen assets with very little bureaucracy or cost.

B. Precedents for Non-Traditional Redress by Private Actors

Several different scholars and politicians have actually suggested the use of privateers as a remedy for modern problems in just the last two decades.[193] One of the most notable examples occurred in 2007, when Representative Ron Paul proposed a bill to the House of Representatives designed "[t]o authorize the President to issue letters of marque and reprisal with respect to certain acts of air piracy upon the United States on September 11, 2001."[194] The bill was meant to further the U.S. effort in the War on Terror.[195] The bill would have allowed privateers "to employ all means reasonably necessary to seize outside the geographic boundaries of the United States and its territories the person and property of Osama bin Laden, [and] of any al Qaeda co-conspirator."[196] While the bill ultimately failed to pass, it illustrated the willingness of American lawmakers to return to privateers as a viable solution to problems where traditional measures are unlikely to reach the desired result.

Both the federal and state governments have already approved of other nontraditional methods to provide aggrieved parties with private redress, including the use of bounty hunters. In 1872, the Supreme Court declared that bounty hunting was a legal practice that should be endorsed as a sometimes more effective alternative to law enforcement action.[197] This endorsement continues to this day, as the Federal Bureau of Investigation and the U.S. Marshals Service each offer bounties ranging from $25,000 to $1,000,000 on fugitives listed on their respective "Most Wanted" lists.[198] States have also authorized private citizens to act as bounty hunters, and "[m]ost states have statutes that detail their licensing requirements, the bounty hunter's arrest authority, and insurance requirements."[199] Similar to the proposed privateering framework, certain states also require that each bounty hunter be registered and put up a bond with the state.[200] Unlike bounty hunting, cyber privateering would involve no physical conflict and would not risk the life of either the privateer or the target cybercriminal.

Perhaps a closer analogy to cyber privateering is the remedy of repossession. Repossession occurs when a secured creditor seeks to regain possession of chattel pledged as collateral on a debt from the debtor without

193. *See* H.R. 3216, 110th Cong. (2007); Hutchins, *supra* note 98, at 861–62.
194. H.R. 3216, 110th Cong. (2007).
195. *See id.*
196. *Id.*
197. Kessinger, *supra* note 2, at 13.
198. *Id.* at 13 n.159.
199. *Id.* at 14.
200. *See* Fla. Stat. Ann. § 648.30(1)–(3) (West 2011).

judicial process.[201] Creditors embrace this remedy because "it is a quick, secure, and inexpensive method for the creditor" to recover the collateral.[202] While the Supreme Court has ruled against state seizures of personal property without the opportunity for the aggrieved party to have notice and a hearing,[203] challenges against repossession have largely been unsuccessful, and the practice is still generally accepted throughout the United States.[204] Repossession is tolerated even though some of its uses may result in physical confrontations, as popularized by many reality television programs. Like repossession, cyber privateers would be acting to return property to its rightful owner in the cheapest and fastest manner. But again, it is important to note that cyber privateering would not risk physical injury to any party involved and would also be subject to oversight by a supervisory agency, as well as the modified prize court system. Overall, these precedents show that the American public is generally in favor of allowing victims to embrace self-help mechanisms and that a political appetite for privateering in modern America still exists despite the practice's disuse on the high seas for over a century. These precedents also illustrate that the right framework is likely to be accepted by the judicial system, as the judiciary already endorses practices that involve far more danger of error or physical harm than would be at play in cyber privateering.

V. ADDRESSING MAJOR CONCERNS AND FEARS OF REPRISAL

A. Legal Challenges

While resurrecting letters of marque and reprisal in a cyber context is clearly constitutionally permissible, there are several issues raised by existing domestic and international law that may call the legality of cyber privateers into question. Domestically, the Computer Fraud and Abuse Act (CFAA) stands as a substantial obstacle that would have to be amended before cyber privateers could operate without fear of criminal or civil liability. The CFAA was originally designed to protect government computers from external, unauthorized intrusions.[205] The statute eventually evolved to impose civil liability on anyone who accesses and causes damage to a computer "used in a manner that affects interstate or foreign commerce," which could theoretically apply to any computer in the world.[206] While some case law seems to suggest that courts will refuse

201. *See* Jay M. Zitter, Annotation, *Secured Transactions: Right of Secured Party to Take Possession of Collateral on Default Under UCC § 9-503*, 25 A.L.R.5th 696, § 2a (1994).

202. *Id.*

203. *See generally* N. Ga. Finishing, Inc. v. Di-Chem, Inc., 419 U.S. 601, 606 (1975); Sniadach v. Fam. Fin. Corp., 395 U.S. 337, 342 (1969).

204. *See* Gary D. Spivey, Annotation, *Validity, Under State Law, of Self-Help Repossession of Goods Pursuant to UCC § 9-503*, 75 A.L.R.3d 1061, § 2 (1977).

205. Kessinger, *supra* note 2, at 15.

206. 18 U.S.C. § 1030(e)(2)(B) (2012); *see id.* § 1030(g).

to impose liability without "damage,"[207] scholars have concluded that private parties would almost certainly not be able to seize digital assets without government authorization.[208] If Congress were to authorize the issuance of cyber letters of marque, it would need to amend the CFAA to allow the cyber privateers to complete their functions without exposure to civil liability. This change could be modeled after the existing exception for law enforcement and intelligence agencies[209] and would be in accord with requests from other critics who have recommended that Congress remove the potential liability for U.S. servicemembers who perform operations in cyberspace.[210]

On the international stage, there are no definite legal constraints that would prevent the United States from issuing new letters of marque, but the proposed framework does raise some possibility of criminal or civil liability in foreign jurisdictions. As previously discussed, the United States is not bound by the Paris Declaration of 1856, due to its refusal to become a signatory party and its longstanding opposition to the treaty's provisions.[211] More recently, the United States and several major European states came together in 2001 to create the Budapest Convention with the aim of curbing international cybercrime.[212] These accords essentially ask each signatory to identify and outlaw certain cybercrime activities but leave the signatories "free, if they wish, to permit such conduct when it occurs pursuant to established legal defenses, excuses, or justification."[213] Scholars have opined that the document is rife with opportunities for signatory nations to refuse to comply and that it completely lacks the necessary enforcement mechanism to render it effective.[214] Ultimately, because the treaty only asks signatories to outlaw and prosecute "'*illegal* access,' '*illegal* interception,' [and] criminal 'misuse of devices,'" the United States would not violate it by issuing new letters of marque, as this action is entirely permissible under existing U.S. constitutional law.[215]

The most pressing legal concern for the United States in authorizing cyber privateers would be the possibility of civil liability, criminal liability, or requests for extradition under foreign laws. It is unlikely that anyone would apply for a cyber letter of marque if the risk of foreign prosecution was not addressed preemptively. Germany, for example, has criminalized cyber self-defense and could choose to prosecute cyber privateers for

207. *See generally* United States v. Czubinski, 106 F.3d 1069, 1078–79 (1st Cir. 1997); Moulton v. VC3, No. 1:00CV434-TWT, 2000 WL 33310901, at *6 (N.D. Ga. Nov. 7, 2000).

208. Kessinger, *supra* note 2, at 15–16.

209. *See* 18 U.S.C. § 1030(f).

210. Picard, *supra* note 8, at 129.

211. *See supra* Part II.D.

212. Rosenzweig, *supra* note 27, at 108–09.

213. *Id.* at 109.

214. *See* Kessinger, *supra* note 2, at 18–19; Rosenzweig, *supra* note 27, at 109.

215. Kessinger, *supra* note 2, at 19 (quoting Council of Europe, Convention on Cybercrime, 6 Nov. 23, 2001, S. TREATY DOC. NO. 108-11, E.T.S. No. 185).

their activities under this law.[216] There are several possible solutions to this problem, the first being to ignore foreign laws entirely. While this is certainly the option that carries the most risk, it may be feasible as some countries, like Germany, that have criminalized cyber self-defense have been rather lax in actually enforcing these laws against violators in their own jurisdictions.[217]

Alternatively, the United States could seek the assent of foreign nations for American cyber privateers to seize assets belonging to cyber pirates residing in those jurisdictions. The existing U.S. laws for naval prize courts include a section specifically dealing with the necessity of consent from "cobelligerents" and the effects of such consent.[218] While some nations may be initially reluctant, it is quite likely that they would agree to these recovery measures, if the accuracy of any seizure could be reasonably established and the actions do not affect the property of uninvolved third parties.[219] After all, privateers are fundamentally different from pirates, as they act with legal authorization from their sponsoring government and are bound by the provisions of their letter of marque. Like the efforts of major powers to keep their citizens and commerce safe on the seas, efforts to reduce the impact of cyber piracy are also likely to be met with sympathy from foreign nations.[220] Overall, the only major legal challenge to the establishment of a cyber privateering regime is the CFAA; it is highly likely that the United States would be able to negotiate with the international community for the privateers' immunity from civil or criminal liability because of the inherently defensive nature of the privateers' actions.

B. Practical Concerns

Critics of the revival of privateering have raised the alarm over several different practical difficulties that may arise in a cyber-privateering framework, but these worries are largely overblown. Concerns for the safety of privateers are largely only applicable in a physical—rather than cyber—context, such as the use of letters of marque to combat the piracy problem off the coast of Somalia.[221] Cyber privateers would operate from the safety of the United States, without exposure to physical danger and out of the reach of foreign powers that may oppose the seizure of Bitcoins from their jurisdictions.[222] Some critics have argued that the danger of a cyber privateer going "rogue" is much too great and that any

216. *See* Rosenzweig, *supra* note 27, at 114.
217. *See id.* at 114–15.
218. 10 U.S.C. § 8881 (2012).
219. *See* Rabkin, *supra* note 28, at 220.
220. *Id.* at 216.
221. *See* Hutchins, *supra* note 98, at 843–44; Kessinger, *supra* note 2, at 14.
222. *Cf.* Young, *supra* note 25, at 929–30 (noting that if privateers were authorized to conduct physical operations in the jurisdiction of a foreign nation, the United States would need to consider the risk of their capture and possible war).

supervisory authority would be unable to effectively monitor their activities at all times.

It is true that in the past some privateers did exceed the bounds of their letters of marque, such as the famous example of Captain William Kidd. In 1696, Kidd received a letter of marque from King William III of England to combat the growing threat of piracy in the Caribbean, but Kidd turned to piracy within months of the start of his voyage.[223] In modern times, similar abuses by private contractors hired by the U.S. Army in the Middle East have called into question the ability of private companies to operate legally.[224] But Congress has several tools at its disposal to curb any piratical behavior in cyber privateers. First, as discussed above, Congress could impose stringent training and monitoring requirements on applicants for letters of marque.[225] Additionally, the threat of forfeiture of a privateer's bond would likely act as a strong deterrent to any temptation to skirt the law.[226] If Congress desired to prepare further safeguards, it could legislate the creation of cyber courts-martial with procedures similar to those instituted by the United States for naval privateers long ago.[227]

Some opponents of cyber privateering might argue that the recovery of stolen Bitcoin is best left to law enforcement agencies who are already empowered to pursue these assets and detain the thieves. However, "law enforcement personnel are questionably competent when it comes to cyber attacks and cybercrime."[228] Private firms have many advantages that law enforcement agencies do not, as they "can offer much larger salaries to researchers and more desirable working conditions."[229] Private firms also have the capability to exchange information about cyberattacks and new cyber-tracing techniques amongst themselves, as they are not encumbered by security regulations that apply to governmental agencies and employees.[230] Law enforcement agencies are particularly at a disadvantage in tracking the perpetrators of Bitcoin theft, as the necessary electronic tracing is beyond the skills demanded by traditional law enforcement roles.[231] Ultimately, "limit[ing] the potential for private involvement in [the recovery of stolen Bitcoin] is to forgo a vast amount of potential reinforcement" that is desperately needed in the effort to return stolen assets to their rightful owners.[232]

Finally, there is the worry that cyber privateers might seize Bitcoins that were not actually stolen. Both the proposed solutions to the attribution problem and the use of a modified prize court system discussed

223. *See* Garrett, *supra* note 7, at 700.
224. *See* Young, *supra* note 25, at 919–20.
225. *See supra* Part IV.A.1.
226. *See id*.
227. Young, *supra* note 25, at 920.
228. Kessinger, *supra* note 2, at 16.
229. Rabkin, *supra* note 28, at 245.
230. *See id.*
231. Rho, *supra* note 29, at 713–14.
232. Rabkin, *supra* note 28, at 245.

above would act as safeguards against an erroneous seizure, as the privateer would be required to present evidence that the seized Bitcoins were those taken from the victim and that evidence would be evaluated by an impartial judge.[233] Besides this, Congress could include an opportunity for any aggrieved party to appeal from a condemnation decision. The existing legislation for naval prize causes already allows "an appeal in a prize cause if it appears that a notice of appeal was filed . . . within thirty days after the final decree in that cause."[234] This provision could be carried over to the modified cyber prize cause framework and would ensure that a cyber privateer is only paid once their seizure has cleared the entire prize court system with ample opportunities for any opposition to be heard. It is quite clear that any practical obstacles to a cyber-privateering regime are either overstated or can be easily addressed through additional legislation from Congress or rulemaking by the new oversight agency.

VI. CONCLUSION

In conclusion, letters of marque provide Congress with a cheap and effective method to address the growing threat of cyber piracy in relation to Bitcoin. The United States currently fails to offer its citizens a means to recover their stolen cryptocurrency in a timely fashion, and cyber privateers could fill that need with only minimal expense to the taxpayer. The government faces a situation similar to that of the Navy during the Revolutionary War and the War of 1812, as law enforcement is woefully underprepared to address the challenges presented by cryptocurrency, but private enterprise could step in to stem the tide of cyber piracy.

The idea of using privateers to solve a tough issue is not new. There is ample precedent for the government to authorize private redress, from the historical examples of letters of marque to the modern practices of bounty hunting and repossession. Recently proposed bills suggest that politicians have not dismissed the possibility of using privateers to solve difficult problems that are otherwise challenging or costly. The resuscitation of this constitutional power has academic backing, as one scholar has stated, "[A]s a means to commission private actors to augment national forces in international crises, the Letter of Marque and Reprisal could yet have modern applications. It remains for innovative executive and legislative experiment to revive the ancient practice in a form befitting modern international problems."[235]

There are risks inherent in this course of action, but they are manageable because cyber privateering is highly unlikely to result in the physical harm of American citizens or foreign nationals. The threat of cyber piracy is not just an American problem, so the United States must work with the

233. *See supra* Part IV.A.1–2.
234. 10 U.S.C. § 8880 (2012).
235. Theodore M. Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 221 (2009).

international community to fight back against the worrying trend of attacks on Bitcoin and other cryptocurrencies. As it seems more and more likely that Bitcoin and its cousins will fundamentally alter the way that consumers and businesses interact online, the government must take a more proactive role in protecting the owners of these assets from those who would enrich themselves unjustly. The issuance of cyber letters of marque would be a strong first step towards countering these criminals. With international cooperation and the right institutional safeguards in place, cyber privateers may be able to severely cripple the piratical activities of the scourges of the new oceans.