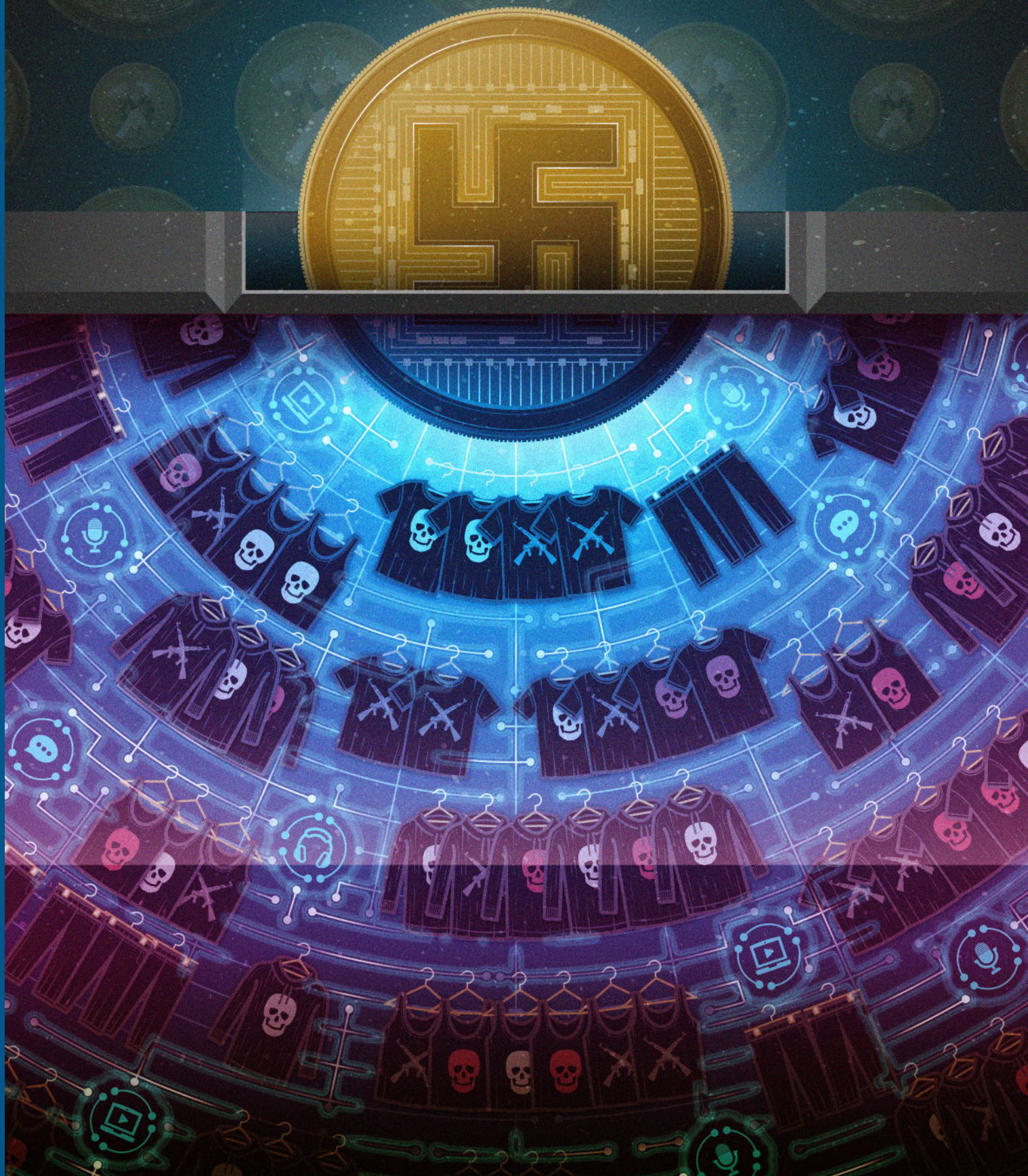
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Crypto-Fascists

Cryptocurrency Usage by Domestic Extremists

Daveed Gartenstein-Ross, Varsha Koduvayur, and Samuel Hodgson

March 2022



Crypto-Fascists

Cryptocurrency Usage by Domestic Extremists

Daveed Gartenstein-Ross

Varsha Koduvayur

Samuel Hodgson

March 2022

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

Introduction

According to data from the analytics firm Chainalysis, "domestic extremists have been receiving a steady stream of cryptocurrency donations since 2016."[1] However, since the notorious "Unite the Right" rally in Charlottesville, Virginia, in 2017, their use of cryptocurrency has spiked. That event spurred many financial services providers to "deplatform" certain extremist groups. Many of these providers, including credit card processors, banks, and payment providers such as PayPal and Venmo, have increasingly refused to serve white supremacist groups, particularly in the United States. Thus, Bitcoin and other cryptocurrencies present attractive digital alternatives. (Older technologies have also proven attractive; some white supremacist groups have resorted to asking for donations through the mail.)[2]

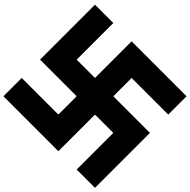
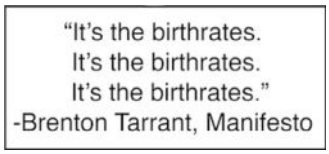
Some white supremacist groups accept cryptocurrency donations to support content they produce, such as video streams, podcasts, and radio shows. In these cases, cryptocurrency can help protect the identities of both the content producers and the viewers. In other cases, groups take cryptocurrency as payment for merchandise they produce and sell, such as apparel, books, and various accessories. In these cases, cryptocurrency usage often exists alongside traditional payment methods, supplementing rather than supplanting debit cards, credit cards, and other forms of payment.

Cryptocurrency can also be used to pay for legal defense, purchase supplies (including VPNs), or provide general support to a group or to particular individuals. In addition to protecting the privacy of donors, cryptocurrency frequently lies beyond the grasp of courts that have imposed financial penalties on extremists. For example, the neo-Nazi publication *The Daily Stormer* accepts cryptocurrency donations allegedly in part to avoid paying off millions of dollars in civil judgments against publisher Andrew Anglin.[3]

As Anglin's case shows, domestic extremists may benefit from the lack of an adequate regulatory and compliance framework around cryptocurrency. Moreover, ongoing enhancements of user privacy in certain cryptocurrencies, notably the emergence of "privacy coins" such as Monero, can further insulate these groups from law enforcement and compliance professionals. Domestic extremists may also use techniques known as "mixing" and "coinjoining" to camouflage their transactions within larger flows of cryptocurrency trading activity.

To address the challenges posed by domestic extremists' use of cryptocurrency, policymakers, private-sector firms, and civil society actors should become more vigilant. The U.S. government should designate more violent white supremacist groups as terrorist organizations, as today only one such organization (the Russian Imperial Movement) has been designated. Designating others would help to cut off their funding flows and other means of support. Policymakers should also enhance the regulation of the cryptocurrency industry. This should include establishing uniform standards for cryptocurrency exchanges and virtual asset service providers; bringing "stablecoins" and privacy coins, as well as decentralized finance, within the regulatory perimeter; and supporting global standards for virtual assets, among other measures. Blockchain analysis firms and nonpartisan watchdog groups should monitor extremists' use of cryptocurrency and assess the risks associated with different exchanges. Extremists will continue exploiting cryptocurrency to support their illicit activities unless policymakers fill today's regulatory gaps while the private sector and civil society amplify their efforts to expose the profits of hate.

1. "Alt-Right Groups and Personalities Involved in the January 2021 Capitol Riot Received Over $500k in Bitcoin from French Donor One Month Prior," *Chainalysis*, January 14, 2021. (https://blog.chainalysis.com/reports/capitol-riot-bitcoin-donation-alt-right-domestic-extremism)
2. Alex Newhouse, "From Classifieds to Crypto: How White Supremacist Groups Have Embraced Crowdfunding," *Middlebury Institute of International Studies*, 2019, page 3. (https://www.middlebury.edu/institute/sites/www.middlebury.edu.institute/files/2019-06/Alex%20Newhouse%20CTEC%20Paper.pdf)
3. Michael Kunzelman, "Neo-Nazi website founder accused of ignoring $14M judgment," *Associated Press*, December 11, 2020. (https://apnews.com/article/technology-race-and-ethnicity-montana-courts-1554c9a9254449b75018cee56317c557)

Name(s) and Symbol(s)	Key Tenets	Notable Proponents
Neo-Nazism/National Socialism 	» Establishment of a fascist political organization based on the German Third Reich. » Extermination, removal, or domination of non-white ethnic groups. » Elimination of a purported Jewish conspiracy.	» National Action » National Socialist Movement
Great Replacement/White Genocide 	» Non-white ethnic groups are replacing whites as the dominant ethnic group through immigration, higher birthrates, race mixing, and cultural destruction.	» Brenton Tarrant » Dylann Roof
Accelerationism 	» A revolutionary overthrow of the current political system is necessary to bring about white power. » Violent, high-visibility actions by lone wolves and small cells can accelerate the inevitable race war, often called the "boogaloo."	» Atomwaffen Division and offshoots » The Base
White Power Skinheads  	» Adoption of Nazi aesthetics, symbology, and racism. » Emphasis on "warrior culture" and physical violence, including street violence, assault, and murder.	» Hammerskin crews » Rise Above Movement
White Nationalism/White Separatism  	» Primary goal is the establishment of white power in a particular geographic region through creation of a new state or the takeover of an existing one.	» Nordic Resistance Movement » Azov Battalion, National Corp, and National Militia

The Basics of Cryptocurrency and Blockchain Technology

While there is no consensus definition of cryptocurrency, the law firm Latham & Watkins provides a useful description. It defines cryptocurrency as:

> a medium of exchange that functions like money (in that it can be exchanged for goods and services) but, unlike traditional currency, is untethered to, and independent from, national borders, central banks, sovereigns, or fiats. In other words, it exists completely in the virtual world, traded on multiple global platforms. These currencies are designed to incorporate and exchange digital information through a process made possible by principles of cryptography, which makes transactions secure and verifiable.[4]

Similarly, the Financial Action Task Force, an intergovernmental organization that focuses on countering money laundering and terrorist financing, defines cryptocurrency as "a math-based, decentralised convertible virtual currency that is protected by cryptography—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy."[5]

In January 2009, the world's first viable cryptocurrency, Bitcoin, emerged. The technological cornerstone of Bitcoin and all other current cryptocurrencies is a public ledger known as a blockchain. The blockchain records information about each transaction using public and private keys composed of a string of numbers and letters unique to each account. The public keys are used to receive funds, while the private keys are used to send them. Together, they form the wallet, which is a tool to access a user's bitcoins. This system prevents users from spending the same unit of currency twice or creating new units, thus enabling secure peer-to-peer exchanges of cryptocurrency without the need for a bank or other intermediary.

For average users of Bitcoin (which remains the most popular cryptocurrency), buying bitcoins is as easy as downloading an app, logging onto a Bitcoin exchange website, and creating a wallet. The use of Bitcoin is also becoming even simpler thanks to Bitcoin ATMs and point-of-sale machines that allow businesses to receive bitcoin payments in person instead of strictly over the internet. Following Bitcoin's initial success, developers began releasing other cryptocurrencies. As of February 2022, there were over 10,000 active cryptocurrencies. Bitcoin comprises 43 percent of the total market capitalization, with a value of roughly $818 billion in a $1.9 trillion market.[6]

The logos and branding for Bitcoin, Monero, and Ethereum.

One cryptocurrency, Monero, incorporates several advanced privacy features that are not native to Bitcoin. Monero wallet addresses are designed to be difficult to link to their owners. Monero groups together multiple transactions to hide the movement of money, and it obscures transaction amounts.[7] *Wired* has described Monero as "fully anonymous and virtually untraceable," although there appear

4. "Cryptocurrency: A Primer," *Latham & Watkins*, 2015. (https://www.lw.com/thoughtLeadership/LW-cryptocurrency-a-primer)
5. Financial Action Task Force, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," June 2014. (https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf)
6. "Cryptocurrency Market Capitalization," *Coinmarketcap.com*, accessed February 17, 2022. (https://coinmarketcap.com)
7. Ibid.

to be exceptions to this rule, and a U.S.-based company, CipherTrace, says it has found a way to conduct "enhanced Monero tracing."[8] Other major privacy-oriented cryptocurrencies include Zcash and Dash, which together had a market capitalization of around $2.3 billion in February 2022, compared to Bitcoin's $818 billion.[9] Privacy coins are ideal for use by extremist groups, since these coins obscure the parties involved in financial transactions, including illicit ones.

Blockchain technology holds the potential to restructure a number of industries that rely on shared information, such as finance, healthcare, international shipping, voting, and more. Blockchain-based technologies have also powered the emergence of decentralized finance (DeFi). DeFi is a movement to replace traditional financial services with decentralized alternatives based on blockchain technology and smart contracts. Current DeFi applications include stablecoins, which are pegged to a traditional currency or to a commodity (such as gold) and thus "maintain a stable value relative to a national currency or other reference assets," and advanced financial instruments, such as cryptocurrency futures.[10]

More recently, blockchains have been used to create non-fungible tokens (NFTs). NFTs are unique digital assets recorded on blockchains. While often produced in the form of digital art, they can also appear in a broad range of collectibles. Each time a NFT is bought or sold, the transaction is recorded on the blockchain, creating a permanent and public record of ownership in a "chain of custody" dating to the NFT's creation. This record means that like cryptocurrencies, the ownership of an NFT is verifiable, and NFT records cannot easily be destroyed, as their existence is tied to a distributed blockchain verifying their authenticity and uniqueness. A large and growing number of NFT platforms exist. The majority use the Ethereum blockchain to store NFTs and track transactions.[11] For some violent non-state actors, NFTs may represent an alternative to cryptocurrencies for storing and laundering value.

Cryptocurrency Usage

Domestic extremists have consistently used cryptocurrency for three publicly observable purposes. The first is to make donations to support digital content, such as video streaming, podcasts, and radio shows. The second is to pay for extremism-related merchandise. The third is to make general donations to extremist organizations or individuals.

Donations for Digital Content

Domestic extremists have raised significant sums of money in cryptocurrency from their content streams, aided by the rise of internet platforms such as the video streaming service DLive, the social networking site Minds, and the video hosting service BitChute. The primary forms of content these extremists produce are web publications, online forums, radio shows, videos, and podcasts. Donations to support such content are examples of "monetized propaganda," allowing extremists to monetize hate speech while broadcasting

8. CipherTrace, Press Release, "CipherTrace Announces Enhanced Monero Tracing Capabilities for Government Agencies and Financial Institutions," August 4, 2021. (https://ciphertrace.com/enhanced-monero-tracing); Andy Greenberg, "Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire," *Wired*, January 25, 2017. (https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire)
9. "Cryptocurrency Market Capitalization," *Coinmarketcap.com*, accessed February 17, 2022. (https://coinmarketcap.com)
10. U.S. President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, "Report on Stablecoins," November 2021, page 1. (https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf); Sid Coelho-Prabhu, "A Beginner's Guide to Decentralized Finance (DeFi)," *Coinbase*, January 6, 2020. (https://blog.coinbase.com/a-beginners-guide-to-decentralized-finance-defi-574c68ff43c4)
11. Ollie Leech, "What Are NFTs and How Do They Work?" *CoinDesk*, March 23, 2021. (https://www.coindesk.com/what-are-nfts)

to a large and geographically diverse audience.[12] There are several prominent examples of domestic extremist groups and individuals who receive cryptocurrency donations in return for their content.

During the assault on the Capitol on January 6, 2021, some of the rioters used DLive to livestream their actions. For example, Anthime "Tim" Gionet, also known as "Baked Alaska," raised over $2,000 from his livestream of the riot.[13] DLive is popular among extremists because of its minimal moderation. The platform allows cryptocurrency-based donations via "lemons," the site's currency. Viewers buy lemons — DLive offers Bitcoin, Bitcoin Cash, Litecoin, Ethereum, and USD Coin as alternative payment options — and can send the lemons to streamers as tips, which the streamers can cash out of their DLive accounts as currency. Each lemon is worth $0.012.[14]

Even prior to the Capitol riot, Megan Squire, a computer science professor at Elon University, found that several known extremist figures were making five to six figures annually from their DLive streams. Her work found that "these leaders include pro-Trump pundit Nick Fuentes, Patrick Casey of American Identity Movement (formerly Identity Evropa), British neo-Nazi Mark Collett and Austria's Martin Sellner of Generation Identity, who became infamous for corresponding with the man who murdered 51 Muslims in a 2019 terror attack in Christchurch, New Zealand."[15] The Christchurch attacker's video and manifesto were posted on the online message board *Kiwi Farms*, which is also supported by donations denominated in cryptocurrencies, such as Bitcoin, Litecoin, Ethereum, Monero, and Cardano.[16]

Nick Fuentes is the host of *America First*, an influential podcast that spreads core tenets of the modern white nationalist movement. Fuentes is also a leader of the white nationalist and antisemitic group Groyper Army. He raised nearly $94,000 on DLive between April 2020 and January 2021.[17] He also received a bitcoin donation worth approximately $250,000 in December 2020 from a far-right French donor who was eventually identified as Laurent Bachelier.[18] DLive banned Fuentes from the platform after January 6.

Other groups in the white supremacist ecosystem who solicit cryptocurrency donations include The Right Stuff (TRS), a neo-Nazi media network founded and run by Michael "Enoch" Peinovich, who rose to prominence for creating the antisemitic "(((echo)))"

12. Lecia Brooks, "Dollars Against Democracy: Domestic Terrorist Financing in the Aftermath of Insurrection," *Testimony Before the United States House Committee on Financial Services Subcommittee on National Security, International Development, and Monetary Policy*, February 25, 2021. (https://www.splcenter.org/sites/default/files/splc_statement_for_house_financial_services_subcommittee_hearings_on_domestic_terrorism_financing.pdf)
13. Makena Kelly, "DLive is under congressional scrutiny over Capitol attack," *The Verge*, February 9, 2021. (https://www.theverge.com/2021/2/9/22274169/dlive-capitol-riot-attack-extremism-video-baked-alaska)
14. "Purchasing Lemon," *DLive*, accessed February 14, 2022. (https://help.dlive.tv/hc/en-us/articles/360039326011-Purchasing-Lemon); Hannah Gais and Michael Edison Hayden, "Extremists Are Cashing in on a Youth-Targeted Gaming Website," *Southern Poverty Law Center*, November 17, 2020. (https://www.splcenter.org/hatewatch/2020/11/17/extremists-are-cashing-youth-targeted-gaming-website)
15. Hannah Gais and Michael Edison Hayden, "Extremists Are Cashing in on a Youth-Targeted Gaming Website," *Southern Poverty Law Center*, November 17, 2020. (https://www.splcenter.org/hatewatch/2020/11/17/extremists-are-cashing-youth-targeted-gaming-website)
16. Marnie O'Neill, "Website Kiwi Farms refuses to surrender data linked to accused Christchurch terrorist Brendan Tarrant," *News.com.au* (Australia), March 19, 2019. (https://www.news.com.au/technology/online/website-kiwi-farms-refuses-to-surrender-data-linked-to-accused-christchurch-terrorist-brendan-tarrant/news-story/46d3c925ef84b24dde6194c42b3c2241); "Christchurch Mosque Shootings: Website Kiwi Farms Refuses to Surrender Data Linked to Accused," *New Zealand Herald* (New Zealand), March 18, 2019. (https://www.nzherald.co.nz/nz/christchurch-mosque-shootings-website-kiwi-farms-refuses-to-surrender-data-linked-to-accused/YYMW2OF5GE3C7EYAMJAPSDANKI)
17. Peter Stone, "US far-right extremists making millions via social media and cryptocurrency," *The Guardian* (UK), March 10, 2021. (https://www.theguardian.com/world/2021/mar/10/us-far-right-extremists-millions-social-cryptocurrency)
18. Ibid.

meme, which other far-right figures began to use on social media platforms to denote Jewish names.[19] TRS hosts the shows *Fash the Nation* and *The Daily Shoah*, which promote Holocaust denialism and white supremacy. TRS' website allows listeners to donate cryptocurrency and accepts Bitcoin, Dogecoin, Bitcoin Cash, Monero, and Ethereum.

The Daily Stormer is a neo-Nazi message board and propaganda site run by Andrew Anglin with assistance from webmaster Andrew "weev" Auernheimer. Anglin was an early adopter of cryptocurrency.[20] He is known to possess at least 200 Bitcoin wallet addresses and in 2019 claimed to be netting $15,000 a week in cryptocurrency.[21] *The Daily Stormer*'s name is a nod to the Nazi-era propaganda sheet *Der Stürmer*. Though the website publicly purports to reject violence, its content promotes neo-Nazism, white supremacy, racism, and antisemitism. The site's writers and users post content implicitly threatening violence against racial and ethnic minorities, including black people and Jews. *The Daily Stormer* used to accept donations in Bitcoin and Monero, though it recently switched to accepting Monero exclusively.[22]

Notably, in the wake of the Charlottesville rally, *The Daily Stormer* received a donation of 14.88 bitcoins, worth more than $60,000 at the time, to keep the site afloat as web service providers began to cut the site off.[23] The amount of the donation is itself an explicit reference to core white supremacist ideas. The "14" is a reference to the late white supremacist David Lane's "*14 Words*": "We must secure the existence of our people and a future for white children." The "88" stands for "*Heil Hitler*." (*H* is the eighth letter of the alphabet, so "88" in this context denotes "HH"). A forensic analysis of the donation found that it came from someone who possessed $25 million in Bitcoin.

Stormfront, a prominent messaging board for white supremacists, accepts donations in Bitcoin, Ethereum, and Litecoin. Don Black, *Stormfront*'s creator, was an early adopter of cryptocurrency. Black is a former national leader of the Ku Klux Klan who was convicted in the United States for plotting to overthrow the government of the Caribbean island nation of Dominica.[24] Several individuals who have perpetrated white supremacist violence have also posted on *Stormfront*. The most infamous is Anders Breivik, whose attacks in Norway claimed 77 lives in July 2011.[25]

Counter-Currents is a media outlet run by Greg Johnson that advocates for the creation of a white ethno-state.[26] The outlet attempts to drape its ideas in academic language and is a prolific publisher of articles, podcasts, and books. *Counter-Currents* accepts donations in over 10 kinds of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, and Monero, to name a few.[27]

19. See Anthony Smith and Cooper Fleishman, "(((Echoes))), Exposed: The Secret Symbol Neo-Nazis Use to Target Jews Online," *Mic*, June 1, 2016. (https://www.mic.com/articles/144228/echoes-exposed-the-secret-symbol-neo-nazis-use-to-target-jews-online#.bCO0mb4CJ)
20. Michael Edison Hayden and Megan Squire, "Neo-Nazi's Bitcoin History Suggests Russian Darknet Link," *Southern Poverty Law Center*, July 15, 2021. (https://www.splcenter.org/hatewatch/2021/07/15/neo-nazis-bitcoin-history-suggests-russian-darknet-link)
21. Luke O'Brien, "Who Gave Neo-Nazi Publisher Andrew Anglin A Large Bitcoin Donation After Charlottesville?" *HuffPost*, June 12, 2019. (https://www.huffpost.com/entry/andrew-anglin-bitcoin-mysterious-donor_n_5d011cc6e4b0304a12087e0c)
22. Andrew Anglin, "Support the Daily Stormer: How to Buy and Send Monero," *The Daily Stormer*, February 21, 2021. (https://web.archive.org/web/20220129111309/https://dailystormer.su/support-the-daily-stormer-how-to-buy-and-send-monero/)
23. Luke O'Brien, "Who Gave Neo-Nazi Publisher Andrew Anglin A Large Bitcoin Donation After Charlottesville?" *HuffPost*, June 12, 2019. (https://www.huffpost.com/entry/andrew-anglin-bitcoin-mysterious-donor_n_5d011cc6e4b0304a12087e0c)
24. "Don Black / Stormfront," *Anti-Defamation League*, June 24, 2013, page 6. (https://www.adl.org/sites/default/files/documents/assets/pdf/combating-hate/Don-Black.pdf)
25. Alyssa Newcomb, "Stormfront Website Posters Have Murdered Almost 100 People, Watchdog Group Says," *ABC News*, April 17, 2014. (https://abcnews.go.com/US/stormfront-website-posters-murdered-100-people-watchdog-group/story?id=23365815)
26. Greg Johnson, "Notes on the Ethnostate," *Counter-Currents*, September 15, 2017. (https://counter-currents.com/2017/09/the-ethnostate)
27. "Donate With Cryptocurrency," *Counter-Currents*, accessed March 2, 2022. (https://countercurrents.com/donate-with-cryptocurrency/)

White Rabbit Radio is a white nationalist media platform hosted by Timothy Gallagher Murdock, who goes by the pseudonym "Horus the Avenger." Murdock is an advocate of the "white replacement" conspiracy theory, which posits that non-white immigration and race mixing are intentionally destroying the white race as part of a Jewish-led plot.[28] The website accepts donations in Bitcoin, Monero, Cardano, Ethereum, Litecoin, and several other cryptocurrencies.

Payments for Merchandise

Extremist merchandise is widely available on the internet. Selling merchandise can help both to sustain a group financially and to spread its message to a broader audience. Merchandise also functions as a membership-identifying and membership-promoting device for extremist groups. Daniel J. Rogers, co-founder and chief technology officer of the Global Disinformation Index, notes:

> One only needs to search Amazon or Etsy for the term "QAnon" to uncover shirts, hats, mugs, books, and other paraphernalia that both monetize and further popularize the domestic violent extremist threat. Images from [January 6, 2021] are rife with sweatshirts that say "Camp Auschwitz" or "6 Million Was Not Enough" that until very recently were for sale on websites like TeeSpring 2 and CafePress… Yes, the merchandise sold through these platforms supplies funds to those who would peddle or exploit this ideology, but this merchandise also acts like a team jersey for the hate groups, bolstering the narrative itself and helping the groups recruit new members and foment further hatred toward their targets.[29]

The success of the Rise Above Movement (RAM), an independent white supremacist group, exemplifies the potential of white supremacist merchandising.[30] RAM is notable for combining skinheads' emphasis on street fighting with a veneer of respectability and slick marketing, perhaps best evidenced by the group's merchandise and media arm, Will2Rise (W2R). W2R sells T-shirts, accessories, stickers, bottoms, and outerwear. Its website advertises "Brother Brands," presumably to promote other white supremacist merchandise (though clicking on the link produces a "404 error" message as of February 2022). W2R openly advertises what it calls an "ethical supply chain," noting that all its products are manufactured in Eastern Europe, "so not a single hand touches the production that is not of like mind."[31] W2R accepts payments in Bitcoin, Cardano, Ethereum, Polkadot, and Litecoin.

Nick Fuentes, the host of the abovementioned podcast *America First*, also sells merchandise that can be purchased with the cryptocurrency Litecoin. The website features shirts, sweatshirts, flags, hats, and mugs along with a seasonal collection titled "White Boy Summer." Individuals wearing *America First* merchandise were among those who stormed the Capitol on January 6, 2021.[32]

Donations for General Support

Cryptocurrency donations will likely grow as extremist groups find themselves denied service by traditional payment processors.[33] At times, white supremacist groups and individuals request cryptocurrency for specific uses, such as legal defense funds, but most solicitations for cryptocurrency tend not to include earmarks.

28. "White Genocide," *White Rabbit Radio*, accessed October 5, 2021. (https://whiterabbitradio.net/category/white-genocide-2)
29. Daniel J. Rogers, "Dollars Against Democracy: Domestic Terrorist Financing in the Aftermath of Insurrection," *Testimony Before the United States House Committee on Financial Services Subcommittee on National Security, International Development, and Monetary Policy*, February 25, 2021. (https://financialservices.house.gov/uploadedfiles/hhrg-117-ba10-wstate-rogersd-20210225.pdf)
30. RAM recently rebranded itself as Revolt Through Tradition. Given extremist groups' tendency to rebrand frequently, this report continues to refer to this group as RAM, the name by which it is best known.
31. "Our Mission," *Will2Rise*, accessed September 18, 2021. (https://will2rise.com/elements/pages/about)
32. "Nicholas J. Fuentes: Five Things to Know," *Anti-Defamation League*, July 8, 2021. (https://www.adl.org/blog/nicholas-j-fuentes-five-things-to-know)
33. "Funding Hate: How White Supremacists Raise Their Money," *Anti-Defamation League*, 2017, page 13. (https://www.adl.org/sites/default/files/documents/adl-report-funding-hate-how-white-supremacists-raise-their-money.pdf)

Jason Kessler, the organizer of the "Unite the Right" rally, is soliciting cryptocurrency donations for the Charlottesville legal defense fund. His website lists Bitcoin as one way to donate to the fund. One campaign for Kessler's legal defense fund on the Christian crowdfunding site *GiveSendGo* — which has hosted fundraisers for people involved in the January 6 riot — lists Bitcoin and Monero as ways to support the fund, though Kessler's website mentions only Bitcoin.[34]

Douglass Mackey, a white nationalist and far-right internet personality, has also received cryptocurrency donations for his legal defense fund. U.S. authorities arrested Mackey in January 2021 on charges of disseminating disinformation designed to prevent people from exercising their constitutional right to vote. A press release detailing the charges against Mackey, issued by the U.S. Attorney's Office for the Eastern District of New York, explains that in 2016 he sought to trick thousands of African Americans into casting invalid votes. Specifically, Mackey used social media to spread false claims that voters could avoid lines at their polling place by texting their choice of presidential candidate to a number he provided. As a result, "4,900 unique telephone numbers" sent messages to that number, indicating their support for Hillary Clinton, whom Mackey opposed.[35]

Mackey, who posted on social media under the name "Ricky Vaughn," also shared antisemitic content, including a Nazi-era cartoon that depicted Jews as an octopus whose tentacles encircle the globe.[36] Shortly after his arrest, a legal defense fund for Mackey emerged, describing itself as having been established by his "friends and supporters." On March 11, 2021, one donor gave $58,662.50 in Bitcoin to the fund, making up the majority of its balance.[37] The fund's website also features wallet addresses for Ethereum, Monero, Dogecoin, and ZCash.[38] One donor also gave to Bitcoin wallets owned by *The Daily Stormer*'s Andrew Anglin and the National Alliance, a neo-Nazi group, before making cryptocurrency donations to Mackey.[39]

The National Socialist Movement calls itself "America's Premier White Civil Rights Organization" and advocates for national socialism in the United States.[40] Though the group purportedly disavows violence, it has in the past called for the forceful removal of all non-whites from the United States, and an individual affiliated with the group tried to attack black passengers aboard an Amtrak train in 2017.[41] The organization's website says it accepts Bitcoin donations.[42]

34. "Charlottesville Legal Defense Fund," *GiveSendGo*, accessed September 21, 2021. (https://givesendgo.com/utr); "Donate," *JasonKessler.us*, accessed September 21, 2021. (https://jasonkessler.us/donate)
35. U.S. Attorney's Office for the Eastern District of New York, Press Release, "Social Media Influencer Charged with Election Interference Stemming from Voter Disinformation Campaign," January 27, 2021. (https://www.justice.gov/usao-edny/pr/social-media-influencer-charged-election-interference-stemming-voter-disinformation)
36. Luke O'Brien, "Trump's Most Influential White Nationalist Troll Is A Middlebury Grad Who Lives In Manhattan," *HuffPost*, April 5, 2018. (https://www.huffpost.com/entry/trump-white-nationalist-troll-ricky-vaughn_n_5ac53167e4b09ef3b2432627)
37. Hannah Gais and Megan Squire, "Mystery Donor Backing Pro-Trump Disinfo Troll With Bitcoin," *Southern Poverty Law Center*, September 14, 2021. (https://www.splcenter.org/hatewatch/2021/09/14/mystery-donor-backing-pro-trump-disinfo-troll-bitcoin)
38. "How to Donate to Douglass Mackey's Legal Defense Fund," accessed September 21, 2021. (https://www.douglassmackey.com/updates/douglass-mackey-legal-defense-fund)
39. Hannah Gais and Megan Squire, "Mystery Donor Backing Pro-Trump Disinfo Troll With Bitcoin," *Southern Poverty Law Center*, September 14, 2021. (https://www.splcenter.org/hatewatch/2021/09/14/mystery-donor-backing-pro-trump-disinfo-troll-bitcoin)
40. "The NSM: America's Nazi Party" *National Socialist Movement*, accessed September 21, 2021. (https://www.nsm88.org/about)
41. Plea Agreement, *United States v. Wilson*, 4:18-cr-03005-JMG-CRZ (D. Neb., filed July 12, 2018). (https://www.courtlistener.com/recap/gov.uscourts.ned.78514/gov.uscourts.ned.78514.27.0_1.pdf)
42. "Help Fund the NSM!" *National Socialist Movement*, accessed September 21, 2021. (https://www.nsm88.org/donate)

Atomwaffen Division (AWD) ostensibly disbanded in March 2020, though many informed observers believe that AWD rebranded itself as the National Socialist Order. Thus, this report continues to refer to AWD in the present tense. It is an accelerationist white supremacist group with an international membership.[43] The organization seeks to instigate a race war that would lead to the destruction of the current U.S. political system.[44] AWD has hosted paramilitary training camps throughout the United States that feature weapons training, physical fitness exercises, and hand-to-hand combat training. A website affiliated with AWD accepted donations through Monero.[45]

Tactics Used to Obfuscate Identity

As law enforcement has investigated domestic extremist groups more vigorously, extremists have increasingly sought to obfuscate their identities to make tracing cryptocurrency payments more challenging.

Fiat entry and exit points — the points on a given cryptocurrency exchange where fiat money is converted into or back from cryptocurrency — present the most challenging hurdles for extremists in their attempts to obfuscate identities. Governments have become increasingly vigilant in applying anti-money-laundering (AML) and know-your-customer (KYC) regulations to cryptocurrency exchanges.[46]

However, new opportunities to use and transfer cryptocurrency without converting the funds into fiat currency are eroding this barrier. Increasing acceptance of cryptocurrency by merchants removes the need to convert funds into fiat money to procure goods and services. Decentralized cryptocurrency exchanges appear to be beyond the reach of regulation.[47] These exchanges are used for trading between cryptocurrencies, a practice that can obfuscate one's transaction history.

Wasabi Wallet and Samourai are two platforms that enable coinjoining.

Domestic extremists have also used a tactic known as "mixing" to further mask ownership of the funds. As the prominent cryptocurrency-focused site *CoinDesk* notes, a mixer is a "service where you could send your bitcoin, pay a small fee, and then receive different bitcoin than the ones that were sent."[48] The individuals exchanging cryptocurrency do not know each other's identity, nor does the service provider know who they are.

43. "Odin," *IronMarch*, October 12, 2015. (Archived version available at: https://web.archive.org/web/20170615224829/http://ironmarch.org/index.php?/topic/5647-atomwaffen-division-central-topic); Alexander Reid Ross, Emmi Bevensee, and ZC, "Transnational White Terror: Exposing Atomwaffen And The Iron March Networks," *Bellingcat*, December 19, 2019. (https://www.bellingcat.com/news/2019/12/19/transnational-white-terror-exposing-atomwaffen-and-the-iron-march-networks)

44. A defunct iteration of AWD's website provided a list of texts explaining the group's ideology. These works included James Mason's *Siege* and Adolf Hitler's *Mein Kampf*. See: "Reading List," *Atomwaffen Division*, archived February 12, 2018. (Archived version available at: https://web.archive.org/web/20180212212616/https://atomwaffendivision.org/join-us); Max Macro, "Violence," *Rope Culture,* March 6, 2017. (Archived version available at: https://web.archive.org/web/20170622024251/http://ropeculture.org/2017/03/06/violence)

45. "Donate," *Siege Culture*, November 7, 2019. (Archived version available at: https://web.archive.org/web/20191107025715/https://siegekultur.biz/donate)

46. For further discussion of the state of AML and KYC protocols globally, see: Financial Action Task Force, "12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers," June 2020. (https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf)

47. Authors' conversation with Yaya Fanusie (adjunct senior fellow, Center for a New American Security, and chief strategist, Cryptocurrency AML Strategies), April 2021; Yaya Fanusie, "Merchant Crypto Payments: A New National Security Frontier," *Lawfare*, March 24, 2021. (https://www.lawfareblog.com/merchant-crypto-payments-new-national-security-frontier)

48. Jon Matonis, "A Taxonomy of Bitcoin Mixing Services for Policymakers," *CoinDesk*, August 8, 2014. (https://www.coindesk.com/markets/2014/03/17/a-taxonomy-of-bitcoin-mixing-services-for-policymakers)

"Coinjoining" is similar to mixing, except it bundles together multiple transactions to add an additional layer of anonymity. Through a protocol called CoinJoin, privacy-focused cryptocurrency wallets, such as Wasabi, enable a process whereby multiple users engage in "one large transaction with multiple inputs and multiple outputs… The purpose of a CoinJoin transaction composed by multiple inputs and outputs is to break blockchain surveillance heuristics," which examine patterns in publicly available blockchain data that may point to the identity of users.[49] Samourai is another platform that enables coinjoining.

An assessment from Europol, the European Union's law enforcement agency, describes such mixing protocols as a "top threat" enabling the use of cryptocurrency on the dark web, a corner of the internet that is difficult to access and hosts numerous illicit activities.[50]

Other Potential Uses of Cryptocurrency by Domestic Extremists

There are at least two potential ways that domestic extremists may leverage the enhanced privacy features that are increasingly incorporated into certain cryptocurrencies. The first is to access markets on the dark web to purchase illicit goods and services. The second is to employ self-executing "smart contracts" to outsource criminal activities, potentially including attacks.

Procurement Through Online Black Markets and Payment for Other Illicit Services

Some early cryptocurrency users in the white supremacist community were drawn to the dark web.[51] It is commonly accessed via Tor, "a special network of computers on the Internet, distributed around the world, designed to conceal true IP addresses and therefore the identities of the networks' users. The Tor network is designed to make it practically impossible to physically locate the computers hosting or accessing the websites on the network."[52] The added protection afforded by privacy coins, as well as by mixing and coinjoining, helps extremists reduce the risk of exposure while accessing black markets on the dark web.

Many notable and easily accessible marketplaces on the dark web sell drugs, guns, ammunition, fake passports, and stolen personal information. Silk Road, a pioneering platform for illicit activities, used Bitcoin as its sole medium of exchange for conducting business before an operation by the FBI and Europol shut the site down in 2013. Law enforcement took down another dark web market, AlphaBay, in 2017. At the time, *The New York Times* noted that AlphaBay had grown "into a business with 200,000 users and 40,000 vendors — or 10 times the size of Silk Road."[53]

Despite these law enforcement successes, other dark web marketplaces have continually emerged to meet the demand for illicit goods and services. Elsewhere on the dark web, one can find assassins and hackers for hire, weapons, deadly toxins, kidnappers, mercenaries who will torture a chosen victim, and similar goods

49. Riccardo Masutti, "What is CoinJoin?" *Wasabi Wallet*, September 23, 2020. (https://blog.wasabiwallet.io/what-is-a-coinjoin)
50. Europol, "Internet Organized Crime Threat Assessment 2020," October 2020, page 58. (https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020)
51. Michael Edison Hayden and Megan Squire, "Neo-Nazi's Bitcoin History Suggests Russian Darknet Link," *Southern Poverty Law Center*, July 15, 2021. (https://www.splcenter.org/hatewatch/2021/07/15/neo-nazis-bitcoin-history-suggests-russian-darknet-link)
52. Alan Brill and Lonnie Keen, "Cryptocurrencies: The Next Generation of Terrorist Funding?" *Defence Against Terrorism Review*, Volume 6, Number 1, Spring & Fall 2014, page 20. (https://securitypolicylaw.syr.edu/wp-content/uploads/2015/05/Brill_Cryptocurrencies.pdf)
53. Nathaniel Popper and Rebecca R. Ruiz, "2 Leading Online Black Markets Are Shut Down by Authorities," *The New York Times*, July 20, 2017. (https://www.nytimes.com/2017/07/20/business/dealbook/alphabay-dark-web-opioids.html)

and services.[54] Whether these services will deliver as advertised is an open question. In some cases, the individuals advertising on the dark web may be scammers or government informants.[55]

Smart Contracts

Ethereum developed the idea of "smart contracts," which eliminate the need for a middleman in contractual transactions. According to the International Monetary Fund (IMF), a smart contract is "a computerized protocol that executes the terms of a contract." A smart contract

> thus encodes the terms of a traditional contract into a computer program and executes them automatically. With blockchain technology, smart contracts can in principle be self-executing and self-enforcing, without the need for intermediaries. They could encapsulate complex terms and conditions such as those found in many financial derivatives, which are often contingent on external events such as the prices of financial instruments or their volatility.[56]

Strikingly, external events such as an election or assassination can trigger the execution of a smart contract. Domestic extremist groups could potentially use such contracts to sponsor terrorist attackers with little direct oversight or planning. For example, a contract could ensure payment to a given person or to the person's family, contingent upon news indicating the completion of a certain attack. In essence, extremists could wield smart contracts as "classified ads" for attacks.

To avoid law enforcement detection, extremist groups could use a new wallet with every contract, similar to trying to dodge a wiretap by using a disposable, or "burner," phone. Though there are not yet any known cases in which extremists have employed smart contracts, it is a threat worth monitoring.

Policy Recommendations

Domestic extremists have migrated to cryptocurrencies for various reasons, including attempts to avoid paying legal judgments, the need to circumvent a denial of service by more traditional financial institutions (such as PayPal), and general privacy concerns. Domestic extremists have been able to raise millions of dollars through these platforms. To mitigate the continued threat posed by white supremacist extremists and their supporters, the U.S. government and the private sector should institute policies that target extremists' use of cryptocurrency.

Designate Violent White Supremacist Groups as Terrorist Organizations

Designations are one of the most powerful tools that the U.S. government can use to reduce violent white supremacists' fundraising capabilities. To date, the U.S. government has designated only one white supremacist group, the Russian Imperial Movement, as a Specially Designated Global Terrorist.[57] **While U.S. law does not allow the designation of solely domestic groups, the government can and should increase the number of designations of violent white supremacist groups with a sufficient foreign nexus**. Designations of violent white supremacist groups that satisfy relevant criteria can help disrupt fundraising activities while also giving the U.S. government a better understanding of extremists' financial networks and key backers.

54. See: Assistant Attorney General Leslie R. Caldwell, U.S. Department of Justice, *Remarks at the ABA's National Institute on Bitcoin and Other Digital Currencies*, June 26, 2015. (https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-aba-s-national-institute)
55. See: Thomas Brewster, "A Dark Web Murder-For-Hire Scammer Became an FBI Informant," *Forbes*, August 27, 2021. (https://www.forbes.com/sites/thomasbrewster/2021/08/27/dark-web-hitman-scammer-became-an-fbi-informant)
56. Dong He et al., International Monetary Fund, "Virtual Currencies and Beyond: Initial Considerations," 2016, page 23. (https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf)
57. Coordinator for Counterterrorism Nathan A. Sales, U.S. Department of State, "Designation of the Russian Imperial Movement," April 6, 2020. (https://2017-2021.state.gov/designation-of-the-russian-imperial-movement/index.html)

Through existing federal enforcement mechanisms, designations would also encourage cryptocurrency companies to disengage from designated entities.

Support Global Standards Regarding Virtual Assets

U.S. policymakers should support global standards on virtual assets that the Financial Action Task Force (FATF) has set. FATF recently updated its guidance to include standards pertaining to virtual assets and virtual asset service providers.[58] According to a recent report by the President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, worldwide adoption of international standards that regulate service providers associated with stablecoins is a "critical factor for illicit finance risk mitigation." The report notes that illicit actors could exploit international gaps in standards enforcement by "using services in countries with weak regulatory and supervisory regimes."[59] The adoption of global standards would provide a more unified, holistic approach to risk in the cryptocurrency sphere.

The white supremacist extremist movement is transnational. Global norms will be necessary to address these groups' cryptocurrency-based fundraising capabilities. More uniform enforcement of FATF's guidance would help the cryptocurrency industry apply the right type of scrutiny to illicit transactions or suspicious tools. It is worth noting that the Treasury Department has already been active in promoting global standards.[60] The U.S. government should build upon the department's efforts.

Establish Standards for Transactions Involving Central Bank Digital Currencies

The financial website *Investopedia* defines central bank digital currencies (CBDCs) as

> the virtual form of a fiat currency. A CBDC is an electronic record or digital token of a country's official currency. As such, it is issued and regulated by the nation's monetary authority or central bank. As such, they are backed by the full faith and credit of the issuing government. CBDCs can simplify the implementation of monetary and fiscal policy and promote financial inclusion in an economy by bringing the unbanked into the financial system. Because they are a centralized form of currency, they may erode the privacy of citizens. CBDCs are in various stages of development around the world.[61]

Western governments have been slow to embrace CBDCs. By contrast, China has already introduced a trial version of its digital yuan, becoming the first major power to release a CBDC wallet.[62] **Policymakers should establish appropriate regulatory standards for transacting with and using CBDCs**. Admittedly, the introduction of CBDCs raises several concerns. For example, will regular exchanges that offer cryptocurrencies such as Bitcoin and Monero be authorized to offer CBDCs alongside their current offerings, or will governments establish separate, government-run cryptocurrency exchanges solely for CBDCs? If the former, then regular exchanges could potentially offer extremists the ability to transact in CBDCs. A second concern is that some CBDCs may

58. See: Financial Action Task Force, "Virtual Assets and Virtual Asset Service Providers," 2021. (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf)
59. U.S. President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, "Report on Stablecoins," November 2021, page 19. (https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf)
60. Ibid., page 20.
61. Shobhit Seth, "Central Bank Digital Currency (CBDC)," *Investopedia*, August 25, 2021. (https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp)
62. Ana Grabundzija, "China Enters 2022 With a First-Mover Advantage on the CBDC Front," *CryptoSlate*, January 5, 2022. (https://cryptoslate.com/china-enters-2022-with-a-first-mover-advantage-on-the-cbdc-front-releases-pilot-versions-of-digital-yuan-wallet-apps-for-android-ios)

make it easier for certain governments to transact directly with illicit actors. In its discussion of Russia's plan to create a digital ruble, *Investopedia* notes that observers suggest "that one of the main reasons for Putin's interest in blockchain is that transactions are encrypted, making it easier to discreetly send money without worrying about sanctions."[63]

Policymakers should consider how to prevent illicit groups, including designated white supremacist extremist organizations, from exploiting CBDCs. Policymakers should thus consider establishing standards for who deals with CBDCs and which institutions facilitate CBDC payments. By working to mitigate money laundering and other illicit finance risks stemming from CBDCs, policymakers can help prevent extremists' abuse and exploitation of these government-backed digital assets.

Forge Partnerships Between Blockchain Analysis Firms and Non-Partisan Watchdogs

Blockchain analysis firms should collaborate with credible non-partisan watchdog groups to address the challenges posed by extremist use of cryptocurrencies. Partnerships between blockchain analysis firms and watchdog groups would leverage both actors' tools and intelligence, increasing overall awareness of extremists' use of cryptocurrencies and allowing relevant companies in the cryptocurrency sphere to better understand extremists' use of cryptocurrency and where the greatest risks exist. The resulting intelligence (such as mapping of extremist activity in the cryptocurrency space) would need to be private and closely held. Publicizing intelligence successes would spur domestic extremists to seek ways to further obfuscate their cryptocurrency usage or to migrate to privacy coins that are more difficult to track.

Collaboration between blockchain analysis firms and watchdog groups could also result in an assessment of cryptocurrency exchanges that would be most effective if made public. An assessment of cryptocurrency exchanges — examining how risky they are and how much illicit activity occurs on them — is another product that could arise from this partnership between blockchain analysis firms and watchdog groups. Some blockchain analysis firms have already begun rating the compliance processes of cryptocurrency exchanges and virtual asset service providers. These firms assess the extent to which exchanges are associated with illicit activities, or, in the case of virtual asset service providers, the extent of the provider's compliance controls, such as KYC and due diligence. Deepening partnerships could result in a mechanism to assess or rate the reputations of various exchanges more robustly, which would help identify where domestic extremists are most active. Such an assessment of exchanges could also have a reputational impact within the cryptocurrency industry, influencing banks' willingness to transact with different exchanges — and ideally spurring problematic exchanges to clean up their platforms. Lastly, this partnership could provide virtual asset service providers with early notice of illicit activity on their platforms, empowering them to take remedial action.

Consider Bringing DeFi Within the Regulatory Perimeter

Decentralized finance poses a significant risk of "money laundering and terrorist financing," according to a White House report.[64] Domestic extremists are sure to leverage this technology further. Policymakers should therefore consider identifying and appointing a regulator for DeFi.

63. Jake Frankenfield, "CryptoRuble," *Investopedia*, July 25, 2021. (https://www.investopedia.com/terms/c/cryptoruble.asp)
64. U.S. President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, "Report on Stablecoins," November 2021, page 10. (https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf)

Regulating DeFi can help curb white supremacists' exploitation of DeFi and decentralized exchanges. Decentralized exchanges, unhosted wallets, and other similar protocols should not be banned. But through regulation and oversight, policymakers could help the cryptocurrency industry and financial institutions better monitor illicit or suspicious transactions.

Consider Regulation of Stablecoins

The White House is exploring the idea of bringing stablecoins under a regulatory umbrella. The White House recently chaired a working group and produced a series of recommendations regarding how stablecoins should be regulated, calling on Congress to legislate federal supervision and oversight of stablecoin issuers, custodial wallet providers, and other relevant entities.[65] **Policymakers should consider enacting comprehensive legislation to establish regulation and oversight of stablecoins and their usage**. This would further curb white supremacists' ability to exploit stablecoins, while providing the cryptocurrency industry with a clear and uniform set of regulations regarding how to treat illicit activity.

Enhance Regulation of Privacy Coins

Policymakers should strengthen the reporting standards for exchanges working with privacy coins. An example of enhanced regulation is requiring exchanges to file customer transaction reports for privacy-coin transactions worth over $250. Stronger regulation of privacy coins would provide necessary oversight and could possibly lead to a reduction in their usage.

Consider Discouraging Privacy Coins Worldwide

While banning cryptocurrency or affiliated protocols is not a prudent recommendation, it is not feasible, either. Still, governments can consider discouraging cryptocurrency exchanges from accepting privacy coins such as Monero or Zcash. Privacy coins allow users to obfuscate their identities and incorporate advanced features to help make them virtually untraceable (at least for now). Precedents for discouraging exchanges from accepting privacy coins exist. In November 2021, Kraken, a cryptocurrency exchange, announced that it would delist Monero in the United Kingdom, in compliance with UK regulations. In January 2021, Bittrex, another exchange, delisted Monero, Zcash, and the privacy coin Dash.[66] In 2019, the South Korean unit of the OkEx cryptocurrency exchange delisted five privacy coins, including Monero and Dash, in compliance with FATF's anti-money laundering rules. **Policymakers should consider encouraging other exchanges worldwide to delist privacy coins on the basis of the risks they pose**.

Domestic extremists' use of cryptocurrencies will likely only grow. As law enforcement continues its efforts to thwart domestic terrorist activity, these groups and individuals will further attempt to shroud their funding streams — their lifelines — in secrecy. Halting extremists' funding flows will be key to countering their violent actions and mitigating the threat they pose. Policymakers should act now.

65. Ibid.

66. Zhiyuan Sun, "Kraken to delist Monero for UK customers by the end of November," *Coin Telegraph*, November 19, 2021. (https://cointelegraph.com/news/kraken-to-delist-monero-for-uk-customers-by-the-end-of-november); Andrew Singer, "Regulators dial up the heat: Dash, ZEC and Monero reach boiling point?" *Coin Telegraph*, January 10, 2021. (https://cointelegraph.com/news/regulators-dial-up-the-heat-dash-zec-and-monero-reach-boiling-point)

Acknowledgments

The authors sincerely thank Yaya J. Fanusie, Collin Almquist, and Mario Cosby for providing crucial feedback and for taking the time out of their busy schedules to serve as external readers. We also wish to thank FDD's Jonathan Schanzer, David Adesnik, and John Hardie for their edits and feedback, both substantive and stylistic. We are grateful for the assistance of Allie Shisgal, who kept the process organized and running like clockwork, and Erin Blumenthal, who managed the production of this report. We are so thankful to Daniel Ackerman for his brilliant cover design.

Cover Illustration by Daniel Ackerman

About the Authors

Dr. Daveed Gartenstein-Ross is a scholar, practitioner, author, and entrepreneur who is the founder and chief executive officer of Valens Global, a private firm focused on fashioning creative solutions to complex 21st-century challenges in the national security domain and beyond. Dr. Gartenstein-Ross is a senior advisor on asymmetric warfare at the Foundation for Defense of Democracies, where he previously served as a senior fellow. He also previously held positions at the U.S. Department of Homeland Security, at Google's tech incubator Jigsaw, and at Georgetown University. He is the author or volume editor of over 25 books and monographs, with a book on jihadist groups' organizational learning processes forthcoming from Columbia University Press. Dr. Gartenstein-Ross holds a Ph.D. in world politics from the Catholic University of America and a J.D. from the New York University School of Law.

Varsha Koduvayur is an analyst at Valens Global, where she focuses on domestic violent extremism and geopolitics. In this role, she works on public-facing research on the domestic violent extremist space, with a particular emphasis on white supremacy and racially motivated violent extremism, along with geopolitical research products for private-sector clients. Prior to joining Valens, Ms. Koduvayur was a senior research analyst at FDD, where she covered the Gulf Arab states. Her work has appeared in *Foreign Policy*, *Foreign Affairs*, and *CNN Business*, among other outlets. She holds a B.A. in international relations and Arabic from Michigan State University.

Samuel Hodgson is an analyst at Valens Global, where he focuses on white supremacist extremist organizations. In this role, he works on a series of projects for a U.S. government client that involve granular, forward-looking analysis about a variety of violent non-state actors. In addition, Mr. Hodgson has worked on several other projects at Valens, including co-authoring an article addressing the causes of insurgent group fragmentation, published in *Studies in Conflict & Terrorism*. Before joining Valens, Mr. Hodgson was a senior analyst with the project management office at Jenner & Block LLP. He holds a B.A. in political science from the University of Chicago.

About the Foundation for Defense of Democracies

FDD is a Washington, DC-based, nonpartisan policy institute focusing on foreign policy and national security. For more information, please visit www.fdd.org.

About FDD's Center on Economic and Financial Power

FDD's Center on Economic and Financial Power (CEFP) studies national economic security, with a focus on how the United States can leverage its economic and financial power to achieve its national security objectives. CEFP promotes greater understanding of how the U.S. government can best employ its economic and financial authorities to counter its adversaries.

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.fdd.org