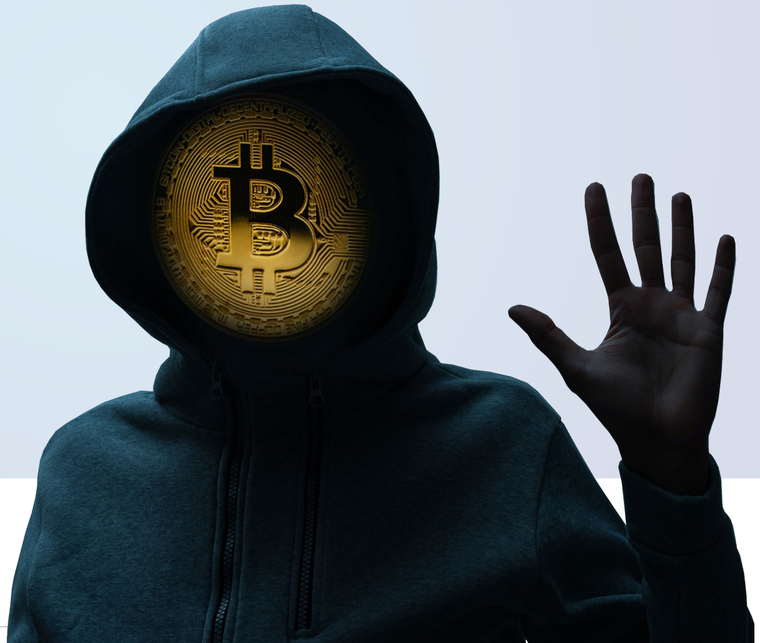
BETTER MARKETS

A Criminal's Guide to Crypto

The crypto industry hasn't made a credible "use" case for cryptocurrencies, but cryptocurrencies have certainly proven their value to criminals.

Ever wonder how a criminal's guide to crypto might read?

Consider this brochure on the advantages of crypto for criminals!



We think the criminal mind can readily appreciate the benefits of cryptocurrencies.

Consider the unique features that cryptocurrencies possess that make them appealing for conducting illegal activities:

1. They are decentralized and unsupervised by any government or central bank.
2. They are virtual and therefore generally unbounded by geographic borders.
3. They do not require that transactions be conducted in person.[1]

If you think that this is the innovation that a criminal mastermind has been waiting for, then we think you are right!

Here are some of the most nefarious ways in which you can use cryptocurrencies.

Money Laundering

Are you constantly worrying about what to do with illicit funds?

Do you struggle with cleaning dirty money?

Cryptocurrencies offer the solution to your money laundering problems!

If you're like most criminals, you need to make your dirty money usable. But the traditional financial system can make that very difficult. Yet your criminal enterprise will never be successful if it can't launder the proceeds of your ill-gotten gains.

Let's say that you are a drug trafficking organization. Your organization needs to move the proceeds of its operations from the location of distribution to the location of manufacturing. One option is to have your lower-level distributors deposit cash at bank branches in one region and then withdraw the cash at bank branches in another region. But this process is time-consuming and risky. The distributors may be unreliable, the tellers may ask a lot of questions, or the banks may close the accounts due to suspicious activity.

Fortunately, cryptocurrencies eliminate these money laundering obstacles! By having your customers pay in cryptocurrency, or by having your lower-level distributors convert their cash into cryptocurrency, you can keep the proceeds of your operations in a digital wallet. Since these wallets can be established with little or no ID verification, your associates can put funds into these wallets without any oversight or fear of detection. The funds may then be immediately transferred from one region to another, without ever touching a regulated institution.[2]

The cryptocurrency ecosystem also offers a variety of enhanced money laundering options. Once you convert your illicit funds to a cryptocurrency, you can exchange your virtual assets for other virtual assets that are easier to use or are less traceable; you can use mixers to functionally obfuscate the source, destination, or amount involved in a transaction; or you can place your virtual assets in a liquidity pool where they may generate returns from trading fees. And when you want to convert your virtual assets back into cash, there are several digital asset service providers that have weak or non-existent anti-money laundering controls and that operate in jurisdictions without anti-money laundering standards for digital assets![3]

So, how can cryptocurrencies improve your ability to launder money? Let's review:

Tired of trying to haul bags of cash around the world?

Cryptocurrency transactions have no borders, so it is easy and practical to move your illicit funds.

Worried that large cash transactions are easily monitored?

Many cryptocurrency intermediaries don't comply with anti-money laundering laws, so your large cryptocurrency transfers are unlikely to be detected by meddlesome regulators.[4]

Fearful that the illicit funds will be traced back to you?

Cryptocurrency mixers allow users to commingle their funds in order to obfuscate ownership.[5]

The use of cryptocurrencies could be the difference between continuing to successfully exploit the communities in which you operate and having law enforcement put an end to your reign of terror, so modernize your money laundering operations with cryptocurrencies today!

Ransomware

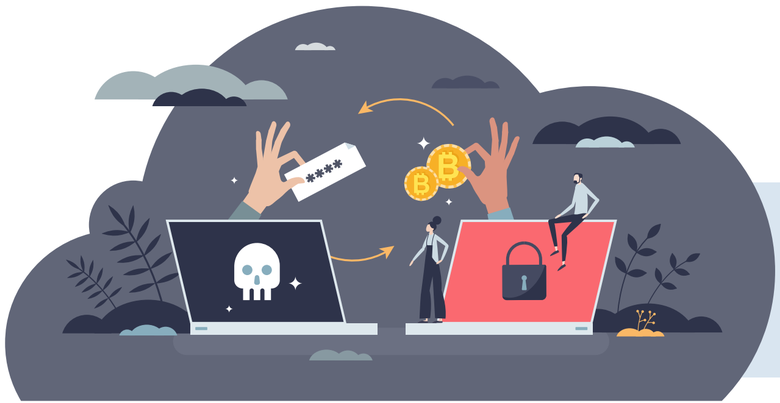
Perhaps you don't have illicit funds to launder?

Instead, maybe you need to obtain some illicit funds in the first place?

Fortunately, cryptocurrencies are also perfect for ransomware!

In case you are unfamiliar with ransomware, ransomware usually involves seizing an organization's data or hijacking computer systems and only unlocking access for a ransom. As the practice has proliferated, hackers have recognized the advantages of cryptocurrencies for the cybercriminal community and have taken to demanding ransom payments in cryptocurrencies.[6] In 2020, for example, hacker groups received at least $350 million in crypto ransoms.[7] Ransomware is also a growing sector of the cybercrime community. The average ransomware payment in the fourth quarter of 2022 was $408,644, up 58% from the third quarter of 2022![8]

Why use cryptocurrencies for your ransomware needs? You can receive your ransom payment in a cryptocurrency anonymously, in a transaction that will be hard to trace, and in a private digital wallet that is not held at a regulated institution. And as noted in our money laundering feature, receiving your ransom payment in a cryptocurrency makes it easy to launder. These features make cryptocurrencies ideal for a ransom payment from those you are extorting.



Here are some of our notable success stories involving cryptocurrencies and ransomware:

$40M in Bitcoin

In March 2021, a cybercriminal group called Phoenix **locked CNA Financial Corp. out of its network**. Phoenix carried out the attack on **CNA Financial, one of America's largest insurance companies**, using a variant of ransomware created by the Russian cybercrime syndicate known as Evil Corp. In order to regain control of its network, CNA Financial paid Phoenix $40 million in bitcoin.[9]

$5M in Bitcoin

In May 2021, the criminal cybergroup known as DarkSide forced **Colonial Pipeline to shut down approximately 5,500 miles of its East Coast pipeline**. The hack of the pipeline, which carried nearly half of the fuel supply to the East Coast**, led to a spike in gas prices, panic buying, and localized fuel shortages**. DarkSide demanded a ransom of $5 million, which Colonial paid in bitcoin.[10]

$11M in Bitcoin

In June 2021, the Russian-linked cyber gang named REvil caused **JBS USA to halt its meatpacking operations for a day**. The attack on JBS, which was the world's largest meat producer and which produced nearly a quarter of America's beef, **threatened to disrupt food supply chains and further inflate food prices.** JBS paid REvil a ransom payment of about $11 million in bitcoin[11]

Please don't hesitate to reach out if you have any questions regarding how cryptocurrencies can help you execute your next ransomware plot!

Evading Sanctions

Maybe you're thinking that money laundering and ransomware attacks are fine for smaller criminal enterprises, but what if you're a nation-state intent on bringing the world to its knees?

We all know that it can be hard to carry out your plans for world domination if you've been tagged as a "rogue nation" or part of a so-called "axis of evil." Well, one of the best features of cryptocurrencies is that they are perfect for evading international sanctions!

Cryptocurrencies are a powerful tool for sanctions evasion for two main reasons. First, commercial banks are often key to sanctions enforcement because they track the source of money and check whether individuals or companies appear on entity lists. But cryptocurrencies are exchanged without the involvement of a commercial bank. Second, blockchains are vulnerable to cyberattacks. By masking or altering the details of a transaction from the blockchain, cyberattacks allow for illegal money transfers without the risk of detection[12]

Here are some examples of sanction evasions from some of our favorite countries:

RUSSIA $5 MILLION

Over a year after Russia launched its full-scale invasion of Ukraine, **crypto exchanges allow Russians to move their holdings in and out of the country using P2P platforms**, despite escalating sanctions. For example, Huobi and KuCoin, two of the world's largest crypto exchanges based in the Seychelles, still allow traders to transact with debit cards issued by sanctioned Russian banks. Singapore-based exchange ByBit allows users to convert Russian rubles into crypto, and Russians may also purchase crypto on the exchange after depositing fiat currency. Cryptocurrencies also aid Russia's invasion of Ukraine, despite the presence of sanctions, though their use in donations. Over the last year, about $5 million in donations have been funneled to approximately 100 different pro-Russia groups.[13]

IRAN $1 BILLION

Iran, the most sanctioned country before Russia's invasion of Ukraine, has been under a U.S. sanctions regime for nearly 40 years, and a foreign company trading with Iran will likely face penalties if the transfers involve dollars or if a U.S. citizen works at that company. Against this backdrop, **Iran permitted the use of cryptocurrencies and smart contracts to pay for imported goods to avoid using the dollar and to circumvent sanctions**. In August 2022, Iran made its first official cryptocurrency imports order worth $10 million. Iran has made further use of cryptocurrencies to evade sanctions through bitcoin mining to make up for lost revenue. As U.S. sanctions have hampered Iran's oil exports, it now utilizes its oil surplus to supply electricity for bitcoin mining hubs and gain revenues from it. In 2020, Iran hosted around 4.5% of global bitcoin mining, worth $1 billion.[14]

NORTH KOREA $1.7 BILLION

North Korea has used cryptocurrencies to make up for lost revenue through cyberattacks. Since 2006, U.S. and U.N. sanctions have targeted North Korean exports. These sanctions have crippled North Korea's ability to export goods. For example, in 2020, North Korea earned only $89 million in official exports. But fortunately, **North Korea has been able to recover its lost revenues by hacking cryptocurrency wallets and laundering the stolen funds through crypto platforms**. In 2022 alone, North Korea stole $1.7 billion of cryptocurrency. make up for lost revenue. As U.S. sanctions have hampered Iran's oil exports, it now utilizes its oil surplus to supply electricity for bitcoin mining hubs and gain revenues from it. In 2020, Iran hosted around 4.5% of global bitcoin mining, worth $1 billion[15]

If these high-profile nations can use cryptocurrencies to stymie efforts to bring them to heel, imagine what cryptocurrencies can do for your fledgling autocracy!

Terrorist Financing

Although we encourage all oppressive regimes to explore the benefits of cryptocurrencies, we recognize that not everyone intent on subjugating humanity will be part of a dictatorial government.

Fortunately, cryptocurrencies are just as valuable for terrorist groups. Your terrorist organization needs to look no further than cryptocurrencies for its funding needs.

You've probably noticed that anti-terrorism measures passed after 9/11 have made terrorist financing more difficult. That's because counterterrorism financing measures focus on tracking the flow of money through bank accounts and preventing transactions that might be used to support attacks and other terrorist activities.[16] But since transactions in cryptocurrencies are hard to track and are made without the involvement of a regulated bank, cryptocurrencies subvert almost all of the rules preventing financial support for terrorist organizations, and will make most of the financial tracking work done by the United States after 9/11 obsolete.[17] As a result, cryptocurrencies allow terrorists to fund attacks more easily than fiat currencies![18]

Here are some of the ways to fundraise for terrorist activities using cryptocurrencies:

This is absolutely a fake tweet for satirical purposes only.

USE TWITTER!

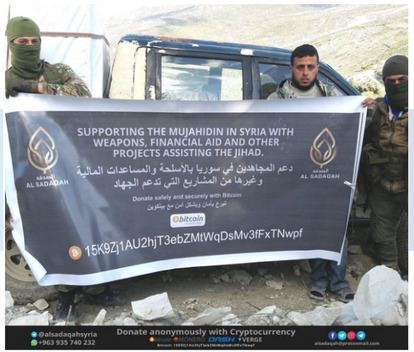
You can use social media to provide instructions for using cryptocurrencies to donate funds to a terrorist organization. In 2015, a teenager used Twitter to provide instructions for how to use bitcoin to mask the provision of funds to ISIL. The teenager used his twitter account to conduct twitter-based conversations on ways to develop financial support for ISIL using cryptocurrencies and tweeted a link to an article he wrote entitled "Bitcoin and the Charity of Jihad." The article included statements on how to set up an anonymous donation system to send money, using bitcoin, to the mujahedeen. So cryptocurrencies are so easy to use to support terrorism that even a teenager can do it![19]

ON THE WEB

You can publish your terrorist organization's public cryptocurrency key on a website to raise funds through cryptocurrency donations from anyone anywhere in the world, while avoiding any reliance on third-party intermediaries. For example, the Islamic State has solicited donations by posting a bitcoin address. You can use the dark web to help facilitate these types of fundraising appeals.[20]

OTHER SOCIAL MEDIA CHANNELS

You can post a call on your social media pages and official websites for cryptocurrency donations to fund your campaign of terror. Or **you can purport to act as a charity and then use social media to solicit cryptocurrency donations** in order to further your terrorist organization's goals.[21] In this regard, it always helps to include a giant poster touting the benefits of cryptocurrencies:



— Notes —

1. Sholmit Wagman, *Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing*, 14 Harvard National Security Journal 87, 88 (2022), https://ssrn.com/abstract=4311926.

2. Alexandra D. Comolli and Michele R. Korver, *Surfing the First Wave of Cryptocurrency Money Laundering*, 69 DOJ J. Fed. L. & Prac. 183, 190-93 (2021).

3. U.S. Dep't of the Treasury, Illicit Finance Risk Assessment of Decentrallized Finance, at 16-18 (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

4. Nick Oberheiden, *Crypto Laundering: Bitcoin + Money Laundering*, The National Law Review (Oct. 14, 2021), https://www.natlawreview.com/article/crypto-laundering-bitcoin-money-laundering.

5. Menqui Sun, *Treasury Warns Crypto Industry of Money-Laundering Risks in "Mixers,"* The Wall Street Journal (Nov. 21, 2022), https://www.wsj.com/articles/treasury-warns-crypto-industry-of-money-laundering-risks-in-mixers-11669066067.

6. Financial Crimes Enforcement Network, Financial Trends Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2022, at 2, https://www.fincen.gov/sites/default/files/shared/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf.

7. Hannah Murphy, *How do criminals exploit cryptocurrencies?*, Financial Times (Nov., 29, 2021), https://www.ft.com/content/85c8d520-b2d9-4a35-abdb-2f56cdd48792.

8. Institute For Security And Technology, Ransomware Task Force May 2023 Progress Report, at 3-4, https://securityandtechnology.org/wp-content/uploads/2023/05/Ransomware-Task-Force-Gaining-Ground-May-2023-Progress-Report.pdf.

9. Kartikay Mehrotra and William Turton, CNA Financial Paid $40 Million in Ransom After March Cyberattack, Bloomberg (May 20, 2021), https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack?sref=mQvUqJZj; https://www.congress.gov/117/meeting/house/114235/documents/HHRG-117-GO00-20211116-SD005.pdf.

10. *Meatpacker JBS says it paid equivalent of $11 mln in ransomware attack*, Reuters (June 10, 2021), https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/; Jacob Bunge, *JBS Paid $11 Million to Resolve Ransomware Attack*, The Wall Street Journal (June 9, 2021), https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.

11. Christopher Bing et al., *U.S. Seizes $2.3 mln in bitcoin paid to Colonial Pipeline Hackers*, Reuters (June 7, 2021), https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/; Emma Newburger, *Colonial Pipeline resumes normal operations after hack, but many gas stations still face shortages*, CNBC (May 15, 2021), https://www.cnbc.com/2021/05/15/colonial-pipeline-resumes-normal-operations-after-hack.html; Eamon Javers and Amanda Macias, *Colonial Pipeline Paid $5 Million Ransom to Hackers*, CNBC (May 13, 2021), https://www.cnbc.com/2021/05/13/colonial-pipeline-paid-ransom-to-hackers-source-says.html.

— Notes —

12. William Alan Reinsch and Andera L. Palazzi, *Cryptocurrencies and U.S. Sanctions Evasion: Implications for Russia, Center for Strategic and International Studies* (Dec. 20, 2022), https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia#:~:text=Q1%3A%20What%20features%20of%20cryptocurrencies,(2)%20vulnerable%20to%20cyberattacks; *Russian Sanctions and Cryptocurrency*, Congressional Research Service (May 4, 2022), https://crsreports.congress.gov/product/pdf/IN/IN11920.

13. Sam Sutton and Lara Seligman, *Two major crypto exchanges failed to block sanctioned Russians*, Politico (Feb. 24, 2023), https://www.politico.com/news/2023/02/24/two-major-crypto-exchanges-failed-to-block-sanctioned-russians-00084391; Allyson Versprille, *IRS Working With Ukraine to Track Russian Crypto Sanctions Evaders*, Bloomberg (May 11, 2023), https://www.bloomberg.com/news/articles/2023-05-11/irs-chainalysis-working-with-ukraine-to-track-russian-crypto-sanctions-evaders?sref=mQvUqJZj.

14. Reinsch and Palazzi, *supra* note 12.

15. *Id.*; Glenn Thrush, *U.S. Indicts Four Men in Scheme to Launder Cryptocurrency for North Korea*, N.Y. Times (Apr. 24, 2023), https://www.nytimes.com/2023/04/24/us/politics/justice-dept-cryptocurrency-north-korea.html; Choe Sang-Hun and David Yaffe-Bellany, *How North Korea Used Crypto to Hack its Way Through the Pandemic*, N.Y. Times (June 30, 2022), https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html.

16. Hadar Y. Jabotinsky and Michal Lavi, *Speak Out: Verifying and Unmasking Cryptocurrency User Identity*, 32 Fordham Intell. Prop. Media & Ent. L.J. 518, 527 (2022).

17. Abigail (Abby) Smith, *Funding Tomorrow's Terrorists and Criminals: Cryptocurrency's Impact on the World Stage*, Georgetown Security Studies Review (Mar. 23, 2023), https://georgetownsecuritystudiesreview.org/2023/03/23/funding-tomorrows-terrorists-and-criminals-cryptocurrencys-impact-on-the-world-stage/.

18. Jabotinsky and Lavi, *supra* note 16, at 526.

19. Financial Action Task Force, Emerging Terrorist Financing Risks, at 36 (Oct. 2015), https://www.fatf-gafi.org/en/publications/Methodsandtrends/Emerging-terrorist-financing-risks.html.

20. Jabotinsky and Lavi, supra note 16, at 557; Armin Krishnan, *Blockchain Empowers Social Resistance and Terrorism through Decentralized Autonomous Organizations*, 13 Journal of Security Studies 41, 45 (2020), https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1743&context=jss; Joshua Baron *et al.*, *National Security Implications of Virtual Currency: Examining the Potential for Non-state Actor Deployment*, at 19-20, Rand Corporation (2015), https://www.rand.org/pubs/research_reports/RR1231.html; Adam Taylor, *The Islamic State (or someone pretending to be it) is trying to raise funds using Bitcoin*, Washington Post (June 9, 2015), https://www.washingtonpost.com/news/worldviews/wp/2015/06/09/the-islamic-state-or-someone-pretending-to-be-it-is-trying-to-raise-funds-using-bitcoin/.

21. U.S. Dep't of Justice, *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns* (Aug. 13, 2020), https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

BETTER MARKETS

Better Banks

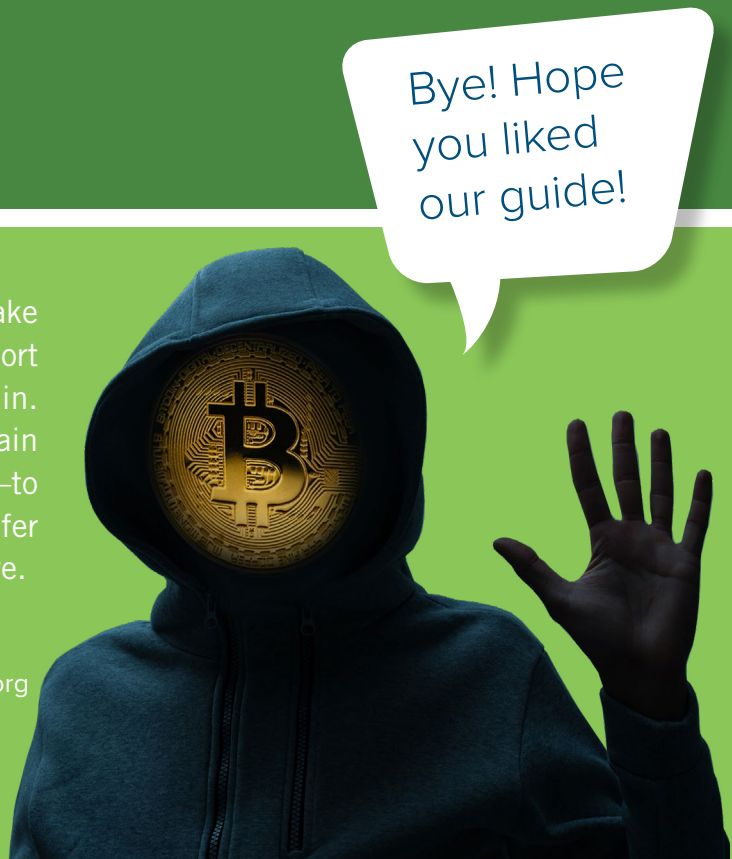
Better Businesses

Better Economic Growth

Better Jobs

Better Lives

Better Communities



Better Markets is a non-profit, non-partisan, and independent organization founded in the wake of the 2008 financial crisis to promote the public interest in the financial markets, support the financial reform of Wall Street and make our financial system work for all Americans again. Better Markets works to restore layers of protection between hardworking Americans on Main Street and Wall Street's riskiest activities. We work with allies–including many in finance–to promote pro-market, pro-business and pro-growth policies that help build a stronger, safer financial system that protects and promotes Americans' jobs, savings, retirements and more.

2000 Pennsylvania Ave. NW, STE 4008 | Washington, DC 20006 | (202) 618-6464 | www.BetterMarkets.org