Managing Cryptocurrency's Impact in Darknet Marketplaces

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Eric Kharitonashvili

Fall 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction: Cryptocurrency's Role in Darknet Markets

a. **Common Ground:** Cryptocurrency and decentralized applications are the primary vehicle for dark web drug markets and cybercrime boards to illegally profit and launder hundreds of millions of untaxed dollars at an ever-growing rate. As Campbell puts it, Crypto can "sidestep the plethora of anti-money laundering regulations developed over the past 25 years." Governments around the world are taking legal action to rectify this problem. (Cambell, 2018, p. 4)

b. **Destabilizing Condition:** Crypto laws that track users and exchanges to prevent illegal activity have skyrocketed (Hacker, 2018, p. 1). However, blockchain technology development makes it near impossible for governments to track online transactions from criminals. Darknet market profits and untraceable transaction volume continues to grow. We have not implemented systems capable of dealing with this problem.

c. **Cost and Consequences:** As crypto laws tighten, citizens who follow the law - most cryptocurrency users - lose their right to privacy-protected transactions. However, with the development of technology such as privacy coins and decentralized crypto-mixers, law-breaking drug sites and nefarious users cannot be traced and are ever-increasing in untaxed sales of guns, drugs, hacked passwords, illegal pornography, and more.

d. **Approach to Resolution:**

i. I will attempt to understand cryptocurrency's role as a *reverse salient* in an early 2010's darknet ecosystem through the lens of Actor-Network Theory.

ii. Using this understanding, analyzing other technology heavily moderated by the government makes for reliable precedent regarding hard-to-govern systems. Research on ways to stop these systems is paramount. Some specific examples of similar systems include cheating, illegal hunting, money laundering, crime organizations, and existing peer-to-peer technology laws involving copyright infringement. Analyzing systems like these guides the way to minimize illicit dark web activities while ensuring the value of blockchain technology is maintained.

Section 1: Context and Definitions for the Darknet and Legal Space

The rise of decentralized blockchain technology has been unprecedented. Blockchain technology has reached a trillion-dollar market cap in only 13 years. This technology can change the landscape of many industries by eliminating profit-incentivized middlemen with technological systems. This is only possible because technical systems, not people, govern blockchain.

In a fully fleshed-out blockchain society, institutions requiring profit, employees, tax requirements, and buildings could be replaced with code. Take banks, for example. Banks loan money according to specific rules and require substantial profits to afford their employees, facilities, and more. A piece of code sophisticated enough to run on the blockchain can guarantee similar loans without all the overhead. This significantly cuts out the profit-taking middleman leaving more money for the lender and, thus, the economy as a whole.

Another way blockchain can cut out needless middlemen is with online transaction fees. Companies worth tens of billions of dollars, like Stripe, Paypal, Mastercard, and Venmo, require a cut of profits that average around 3% of the total transaction (Stripe, 2022). As blockchain technology and methodology progresses, online purchase price fees could be drastically reduced as cryptocurrency can cut out the middleman.

The only reason this upside is possible is that systems and not people govern blockchain technology. *Plans* do not require profit. *People* do. If these systems develop, they could cut many inefficiencies out of the economy.

With all of the benefits of having financial ordeals governed by systems rather than people, there are also significant drawbacks. Some cryptocurrencies, like Monero, are entirely anonymous. Current mathematical cryptographic understanding says it is impossible to track who and where these coins go to and come from. These coins are essential to darknet market operations where cartels, illegal drug operations, identity theft, and illegal and unregistered gun sales earn billions of untaxed dollars annually. (Cambell, 2018, p. 17)

Some technologies allow for *the anonymous sending of non-anonymous* or pseudo-anonymous coins. Crypto-mixers are a famous example of this. They are illegal but cannot be taken down by the government. They run on the blockchain. The creators of these mixers can remain completely anonymous due to the nature of cryptocurrency. Government regulation is hard to enforce when no one can determine to whom the unknown group should be liable.

A specific example of this is the open-source project Tornado. The use of this mixer's website, and any receiving or sending transactions using this technology, was made illegal by the U.S. treasury department and was banned from the internet. However, using blockchain protocols, this mixer is still available on a decentralized version of the internet and *cannot be taken down*. After it was banned, thousands of illegal coins were sent to popular wallets (U.S. Dept Treasury,

2022). This was a case of people demonstrating that blockchain technology cannot be governed. Even if the government were to arrest the developers of this technology, Tornado would still run. Even if the creators of Tornado decide to take it down, Tornado's code was open-sourced. More people could remake this mixer. Effectively, no one can ever take this mixer down.

So, all of cryptocurrency's potential and flaws stem from the fact that it is a decentralized system. It does not need profit, and it also does not need to follow laws. Legally, what should be done here? Banning cryptocurrency, as China did, does not solve the problem. They are still consistently shipping and receiving drugs on darknet marketplaces (Scourfield, 2019, p. 9). Not doing anything will result in billions of dollars funneled toward crime organizations and tax evasion. A nuanced implementation of the law - law specific to ungovernable systems - needs to be created for cryptocurrency to maximize the benefit and minimize the harm this technology can cause.

Other "ungovernable" systems exist. Peer-to-peer copyright law and torrenting sites, international and state-sponsored cybercrime, illegal hunting, and even video game cheating are all examples of situations comparable to cryptocurrency. Catching nefarious actors is nearly impossible. Thus, enforcement of these laws is difficult. In writing about international cybercrime, Reassu claims that "regulation will be achieved not through centralized authority but the spread of norms, informal rules, and regimes." (Reassure, 2007, p. 1).

This problem boils down to making cheating the system far more undesirable than playing fairly within the system. Cybercrime as a domain has handled this exceptionally well. The vast majority of individuals who have the skills to hack into systems are compensated very well and tend not to be the ones breaking into systems; instead, they are the ones protecting the systems (Silic, 2021, p. 10). This is because of the harsh and consistent punishments that hacking has. On the other hand, Crypto is more relaxed and consistent with the law. In terms of regulation, Kethineni emphasizes that Bitcoin and cryptocurrency have dangerous legal precedence and consistency by stating, "bitcoin currently operates in a gray area" (Kethineni, 2020, p. 145). Ross Albright, the creator and maintainer of the first multimillion-dollar darknet drug market, "Silk Road," was sentenced to two life sentences in prison. Then, a darknet marketplace with even more users and drugs sold called "Silk Road 2.0" was taken down, and the admitted co-founder of this site, Blake Bentall, was charged with only eight years in prison (U.S. DOJ, 2016). There is little precedent and consistency in handling cases like these.

Another way to approach this problem is from a buyer's point of view. Reducing demand could be an effective strategy in combating darknet markets. Weed vendors and weed-related profits mainly sustain these drug markets. However, with weed becoming legalized in more and more states in the USA, one would expect the weed numbers in darknet USA sales to be going down. The opposite is true. Legalized weed shops are penalized by the government to degrees that make it very hard to compete with illegal vendors who do not abide by the same regulations, taxes, and penalties that legal shops have to deal with, leading to an increased percentage of drug buyers on the dark web. As Bancroft states, "Cryptomarkets [also] expose pricing, allowing buyers to compare offers," thus allowing for even lower illegal drug prices on the darknet

(Bancroft, 2022, p. 3). Analyzing the buyers' side of darknet marketplaces may reveal answers as to how the regulation of cryptocurrency should be handled.

Synthesizing this information and contextualizing it regarding cryptocurrency regulation requires a thinking framework. Actor-Network theory will play a pivotal role in determining the efficacy of any rule proposed. Crypto has acted as a reverse salient in this sociotechnical ecosystem of darknet developers, drug users, and technical systems already in place to allow for anonymous internet-to-real-life transactions. Cryptocurrency as an actor must be understood thoroughly as the gateway payment system of the darknet. That critical component enables these websites to turn a profit reliably.

Section 2: Context and Definitions for the Darknet and Legal Space

A framework helps contextualize and process how to approach the problem of managing and designing ungovernable systems in cryptocurrency. Breaking sociotechnical systems like darknet markets down into understandable and thoroughly thought-through actors and bringing all of the understood pieces back together is a more manageable way to understand how these actors work and the resulting conclusions.

Actor-Network Theory is a well-known and appropriate framework for contextualizing and interpreting the problems of the cryptocurrency and the Darknet sociotechnical system. Essentially, this framework deconstructs all living and technical systems into individual actors. These actors all have roles and incentives regarding the procedure. When these actors interact, they form the network that comprises the sociotechnical system. Each of these actors is assumed to have its mission, each affecting the network. In the context of cryptocurrency and Darknet markets, the main actors involved are the drug or illegal substance dealers who provide the website with the supply, the market buyers who go to the website to purchase drugs, and the website that brings the two together. Underlying this is the technology making these transactions possible - cryptocurrency and the Tor protocol, which makes it impossible to trace who is connecting to which website allowing for anonymity on both the client and server sides. (Lacson, et. Al, 2016, p. 44) These actors participate in anonymous online transactions where taxes are not accounted for, drugs are sold, and scams take place, as shown in Figure 1.

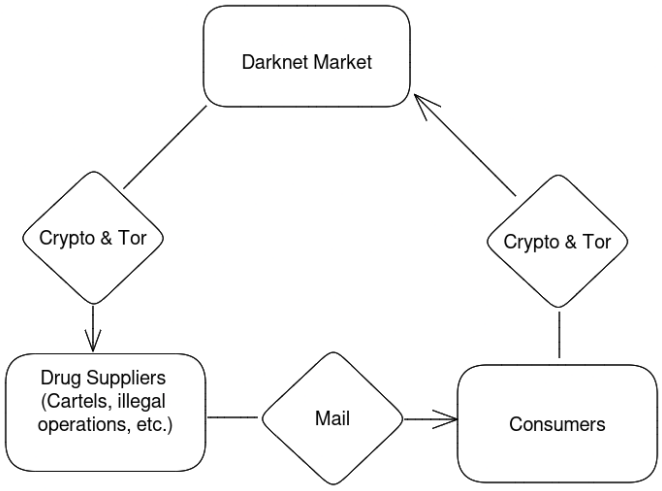

Figure 1: Darkweb Actor Network Relations (Created by Author)

Trust is pivotal in all criminal markets, online and offline, compared to legal ones. From the consumer's point of view, there is no protection against illegal transactions by the government and no authority to report when stolen or scammed. Doing so would lead to admitted criminal acts. From the provider's point of view, the market could be a hidden honeypot that acts as an illegal organization run by the government to catch these dealers red-handed (Zeid, 2018, p.11). This is why cryptocurrency and the Tor networking protocol are essential in Darknet exchanges. Cryptocurrency and Tor allow all nontechnical actors to purchase and exchange information anonymously.

Through Actor-Network Theory, the role of cryptocurrency in these Darknet transactions is clear - it is an actor that *anonymously* transacts money from consumer to drug supplier. This anonymity is the core of online trust. This also explains why privacy coins like Monero are

becoming more popular in these drug markets than other pseudo-anonymous coins like Bitcoin. Monero's transactions and transaction history are entirely untraceable. Bitcoin's transactions are theoretically fully traceable. However, connecting a person's real-life identity to their computer wallet is more complicated. Technologies building on this anonymity, like Bitcoin Tumblers or Tornado, use encryption and other cryptographic techniques to hide transactions of pseudo-anonymous coins like Bitcoin or Ethereum. As Thomale puts it, the laws on cryptocurrency regulation are “inconsistent at best, … and unenforceable at worst.” (Thomale, 2018, 683) Tornado is illegal in the USA because of its role in money laundering in North Korea, but other mixers that do the same things are legal for some reason. Rules and regulations as they currently stand seem inconsistent.

The website and vendor relationships are worth discussing as well. The marketplace acts as the primary credible source of trust for consumers. Therefore, well-trusted marketplaces are highly sought out by drug dealers who want to sell many products at a high price. More "exclusive" marketplaces that have built trust with consumers tend to charge more fees and be higher in price than new up-and-coming websites. Dealers strive for rating points to climb up on the website, leading to higher search placement and more orders. A specific example of an up-and-coming marketplace is the *Nemesis Market*. This marketplace sells everything from fake social security cards to drugs to malware. They have a referral program where the referee gets a 50% commission on fees for dealers who sign up for the site. The general trend on these sites is only a 25% commission. Gaining user and vendor trust is the biggest aim for those who run these sites. (Kethineni, 2018, 153) If there was a way to limit how much confidence they could achieve, that

could slow the growth of these sites. A demonstration of how these sites look can be found below in figure 2.

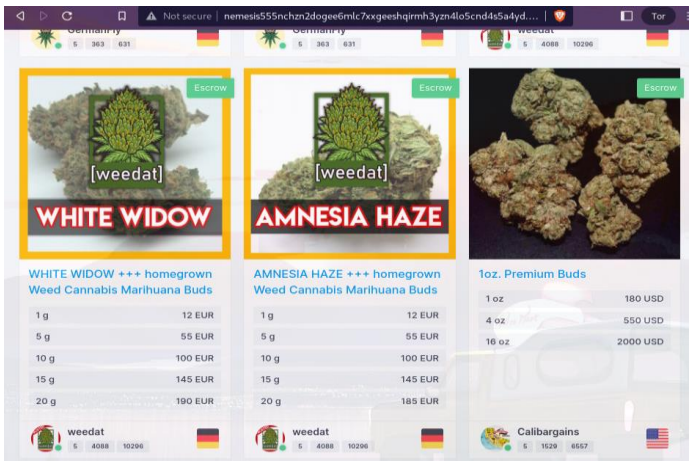

Figure 2: Darknet Marketplace Website (Created by Author) *Note visiting these sites is legal, purchases are not

Section 3: A Middle Ground for Government Intervention and Privacy

Optimal solutions to managing the legality of cryptocurrency can be derived from social thought experiments and frameworks like Actor-Network Theory, as explained above. Cryptocurrency and blockchain networks allow for peer-to-peer spending in *three* primary forms.

1. Pseudo-anonymous coins like Bitcoin allow for a history of transactions to be seen and knowledge of where people are spending because transactions are made public. The wallet information, however, is not tied to any real identity or social security number.
2. Private coins like Monero provide peer-to-peer transactions that are cryptographically impossible to calculate and trace. Spending and receiving money is hidden from everyone. (Alonso, 2018, p.53).
3. The government-enforced currencies are tied to the government and generally tend to have all transactions and wallets tied to real people's identities. Transactions may or may not be private to companies, but everything is accessible by the government.

The optimal solution this paper argues for would be a mix of pseudo-anonymous and government-backed public coins, as shown in figure 3. This would give individual citizens the same amount of privacy as they do with the current fiat currency system. Compromising user privacy and the ability of the government to track illegal activities is what this paper argues would be optimal.

In regards to allowing the government to peer in on cryptocurrency transactions, many cryptocurrency enthusiasts believe this is antithetical to the decentralized and blockchain movement. Bitcoin, the first cryptocurrency and first-ever use of blockchain technology, was made in response to the 2008 U.S. economic crash. Satoshi Nakamoto, the anonymous inventor of Bitcoin, did not like the "inherent weakness of the trust-based model" in our current financial

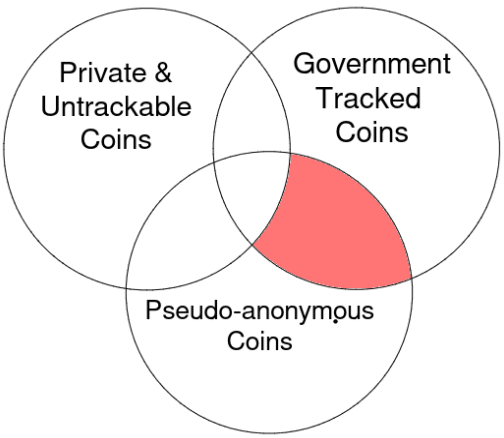

Figure 3: Optimal Coin's Governance Region (Created by Author)

system (Nakamoto, 2009, p.1). In other words, Satoshi was not a fan of the government's ability to create or destroy money on a whim. Satoshi did not like that if the people of a currency lost faith in the institution, the currency lost value.

Satoshi wanted a trustless system for money - one ruled by programmatic rules and technology, not emotional and, at times, illogical people. Therefore, it is logical that many cryptocurrency adopters believe this same thing. They do not want the government involved with Crypto - even regarding taxes and darknet spending. However, Satoshi hated the fact that Bitcoin was used for the darknet. One of his last messages in regards to Wikileaks and criminal activity in Bitcoin was, "It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us." (Nakamoto, 2010, p.1) A popular interpretation is that Satoshi did not want his cryptocurrency to be used for criminal activity. Satoshi's vision was not a society of people avoiding taxes and buying drugs; instead, he wanted a currency that the government could not manipulate.

A society with strictly private coins that cannot be tracked would be a net harm to everyone. The government could not enforce tax laws or track harmful drugs, guns, pornography, fraud vendors, or consumers. There are positives to having privacy coins. Markets would equalize in many ways. Companies would not be able to discriminate concerning race, location, gender, or price. People living under authoritarian regimes could spend freely without their governments enacting social credit system repercussions. Even legal data involving online transactions would belong to the consumer, not the hands of Stripe, Google, Facebook, and Amazon. Companies are already taking people's money; privatized coins would allow them not to take their data.

Legally, user privacy and crypto coins are tricky. Even the slightest bit of leeway allows actors to take advantage of the system massively because it is nearly impossible to catch them. The moral

and legal argument of these coins stands with whether people should be able to spend without trial. This is a more nuanced question than it seems at first glance. Cash is made by the government or given out from a bank. The government can reasonably track what it produces and distributes - especially online. Crypto appears from thin air once mined. Crypto begins as untracked and can stay untracked, allowing darknet markets to exist.

An optimal solution derived from the previous Actor-Network theory analysis would keep most benefits from the privatized coins and the safety of government-enabled cash. The way to do this is with incentives, social pressure, and cheating psychology integrated into the law.

Many crime systems in which most people cannot and are never caught operate similarly to this proposition. Punishments are harsh and consistent because many actors will never be seen. This makes people too scared to cheat. In video games and hunting, in particular, this is effective. When the Silk Road was taken down initially, and Ross Ulbright was sentenced to life in jail, many drug markets closed. Strict policies steer people away from this kind of behavior (Lacson, et. Al, 2016, p. 49).

Another way to make people stop cheating is to incentivize playing the game fair. When cheaters go through too many hoops to cash out their rewards, they do not cheat in the first place. Illegalizing ways to anonymously turn cryptocurrency into cash, such as decentralized exchanges for privacy coins, could be a step. Cryptocurrency by many can be seen as a modality of

investment, but it is also seen as a type of currency. Treating Crypto as an asset like a stock makes it a tax burden when people want to exchange their money. A separate asset class with lower taxes than most assets and higher taxes than foreign exchange markets is worth considering.

Creating a centralized currency can also incentivize people to avoid anonymously buying cryptocurrency. For example, the USA can release a coin that would be tied to one's identity but provides many benefits. Automated and optimized taxation reports, better financial tracking, and government incentive programs. Even if users were to trade this for pseudo-anonymous coins like Bitcoin, those wallets could be noted and tracked by government authorities if need be.

Conclusion

Cryptocurrency is a system that operates on programmatic rules and technology. It does not need employees, buildings, or anything except the internet and people willing to run nodes on the network. For this reason, cryptocurrency has the potential to revolutionize many sectors of the economy and how people live their lives. However, operating as a system does come with downsides. The government can shut down companies and crime organizations that do not follow the law. Shutting down a cryptocurrency, though, is a much more complex and realistically impossible endeavor. Illegal transactions and drug markets utilizing this decentralized power have emerged as billion-dollar industries. Moderating the use of cryptocurrency through the law to minimize the number of illicit activities and maximize this technology's legal and cost-saving potentials is paramount if cryptocurrency is to live up to its full potential and change how society interacts with virtually all online markets.

Actor-Network Theory can derive that the actors involved with illegal darknet transactions utilize cryptocurrency because they trust the system. The vendors can receive untaxed anonymous Crypto and launder it easily compared to other payment systems. Consumers can secretly purchase items without their identities revealed. Remove the anonymity from Crypto, and the trust is no more.

Removing this anonymity is more involved than just making anonymous coins illegal. Catching and punishing unknown transactors is nearly impossible. Proper incentive structures are needed. Analyzing how to prevent cheating in all domains that are almost impossible to be seen provides evidence that harsh and consistent punishment and difficulty of cheating are the most impactful features that prevent bad actors. Designing laws following these philosophies may minimize the amount of Crypto used for drugs, scams, and other illegal activities while still allowing the door open to innovation and future development of the technology.

References

Alanzo, K., KOE, 2018. *Zero to Monero: First Edition A technical Guide to a Private Digital Currency; for Beginners, Amateurs, and Experts* https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf

Andrew Scourfield, Catherine Flick, Jack Ross, David M. Wood, Natalie Thurtle, Darryl Stellmach & Paul I. Dargan (2019) Synthetic cannabinoid availability on darknet drug markets—changes during 2016–2017, Toxicology Communications, 3:1, 7-15, DOI: 10.1080/24734306.2018.1563739

Bancroft, A. Potential Influences of the Darknet on Illicit Drug Diffusion. Curr Addict Rep (2022). https://doi.org/10.1007/s40429-022-00439-2

Campbell-Verduyn, M. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime Law Soc Change* 69, 283–305 (2018). https://doi.org/10.1007/s10611-017-9756-5

Duxbury, S.W., Haynie, D.L. The Network Structure of Opioid Distribution on a Darknet Cryptomarket. J Quant Criminol 34, 921–941 (2018). https://doi.org/10.1007/s10940-017-9359-4

Harrison, R.D., Sreekar, R., Brodie, J.F., Brook, S., Luskin, M., O'Kelly, H., Rao, M., Scheffers, B. and Velho, N. (2016), Impacts of hunting on tropical forests in Southeast Asia. Conservation Biology, 30: 972-981. https://doi.org/10.1111/cobi.12785

Hacker, P. & Thomale, C. (2018). Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law. *European Company and Financial Law Review, 15*(4), 645-696. https://doi.org/10.1515/ecfr-2018-0021

Kethineni, S., Cao, Y. & Dodge, C. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. Am J Crim Just 43, 141–157 (2018). https://doi.org/10.1007/s12103-017-9394-6

Key player in 'silk road 2.0' sentenced to eight years in prison. The United States Department of Justice. (2016, June 6). Retrieved October 27, 2022, from https://www.justice.gov/usao-wdwa/pr/key-player-silk-road-20-sentenced-eight-years-prison

Lacson, Wesley, and Beata Jones. "The 21st Century DarkNet Market: Lessons from the Fall of Silk Road ." *International Journal of Cyber Criminology*, vol. 10, 2016, pp. 60–61., https://doi.org/10.5281/zenodo.58521 . Accessed 2 Dec. 2022.

Li Wang, Liu Fan, SungMin Bae, How to persuade an online gamer to give up cheating? Uniting elaboration likelihood model and signaling theory, Computers in Human Behavior, Volume 96, 2019, Pages 149-162, ISSN

Miron, J. & Soares, P., 2021. Regulation and Taxes Are Stifling California's Weed Industry, Cato Institute. Retrieved from https://policycommons.net/artifacts/1897980/regulation-and-taxes-are-stifling-californias-weed-industry/2649107/ on 28 Sep 2022. CID: 20.500.12592/xmfrsh.

Nakamoto, S., 2009. *Bitcoin open source implementation of P2P currency* http://bitcoin.org/bitcoin.pdf

Nakamoto, S., 2010 *Added some Dos Limits*. An error has occurred! (n.d.). Retrieved October 27, 2022, from https://bitcointalk.org/index.php?action=profile%3Bu

Nicola Dalla Guarda (2015) Governing the ungovernable: international relations, transnational cybercrime law, and the post-Westphalian regulatory state, Transnational Legal Theory, 6:1, 211-249, DOI: 10.1080/20414005.2015.1042226

Pricing & fees | stripe official site. (n.d.). Retrieved October 27, 2022, from https://stripe.com/pricing

R. B. Zeid, J. Moubarak and C. Bassil, "Investigating The Darknet," 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 727-732, doi: 10.1109/IWCMC48107.2020.9148422.

Rosenau, J.N. (2007), Governing the ungovernable: The challenge of a global disaggregation of authority. Regulation & Governance, 1: 88-97. https://doi.org/10.1111/j.1748-5991.2007.00001.x

Silic, M., Lowry, P.B. Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes. *Inf Syst Front* 23, 329–341 (2021). https://doi.org/10.1007/s10796-019-09949-3

U.S. Treasury sanctions notorious virtual currency mixer Tornado cash. U.S. Department of the Treasury. (2022, August 8). Retrieved October 27, 2022, from https://home.treasury.gov/news/press-releases/jy0916