Public Statements & Remarks

Illicit Finance and Other Key Risks of Digital Assets: Keynote at City Week 2023

CFTC Commissioner Christy Goldsmith Romero in London

April 25, 2023

Remarks as Prepared for Delivery

Standard Disclaimer

Thank you to the Organising Partners and Patrons for the invitation to speak here at City Week on key risks of digital assets.

Tomorrow is reportedly the 12th anniversary of the day that Satoshi Nakamoto, the creator of Bitcoin and blockchain, sent his final message to developers.[1] It has long been speculated that he left disillusioned after *PC-World* published that Bitcoin could be used for payments to WikiLeaks after it was blacklisted by banks. He walked away the day after messaging, "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."[2]

I wonder what Satoshi thinks of the entire industry that has grown from his vision, about this past tumultuous year for that industry, and the use of Bitcoin for illicit finance. A hornet's nest has been kicked indeed.

Satoshi's vision for a peer-to-peer network without a trusted third party inspired a global financial services ecosystem of intermediaries, platforms, projects, and markets. However, most digital assets today are transacted on centralized "exchanges," that act as "trusted" third parties, differing from Satoshi's vision. Retail and institutional participation in digital asset markets exploded in recent years to a $3 trillion valuation, in part because investors trusted in those exchanges. Trust was eroded with high-profile meltdowns and contagion, leaving investors with nearly $2 trillion in losses,[3] and the industry in a crisis of trust.[4]

As a U.S. regulator in law enforcement for 21 years combatting money laundering, fraud and other crime, I will talk first about the most serious risk in digital asset markets—the use of crypto for illicit finance. I will also talk about the risk of cyber hacks, fraud, and financial stability. I will share my views about how to manage these risks, while promoting market integrity and protecting customers.

The crypto markets are used to facilitate illicit financing of drugs, human trafficking, ransomware, terrorism, and malicious state sponsored activity posing national security risks.

The use of digital assets for illicit finance poses national security and other risks. Attracted by the allure of anonymity, crypto's darkest corner facilitates the financing of terrorism, the drug trade, darknet markets, cyber gangs, money launderers, and malicious state sponsored activity.[5]

In 2020, the U.S. Department of Justice ("DOJ") dismantled three terrorist financing campaigns of Hamas, al-Qaeda, and ISIS, seizing 300 cryptocurrency accounts. One of these terrorist groups boasted that Bitcoin donations were untraceable and would be

used for violent causes. DOJ has shut down darknet marketplaces, like Silk Road and Hydra. DOJ also shut down Hydra's largest counterparty, the crypto exchange Bitzlato, which Treasury has identified as a primary money laundering concern in connection with Russian illicit financing.[6]

Cryptocurrency is used to finance cybercrime and is demanded for ransomware payments. The victims of cyber attacks can be individuals, companies, hospitals, schools, governments, the financial sector, transportation, critical infrastructure like the Colonial Pipeline, and supply chains like JBS, the world's largest meat supplier. There have been significant cyber hacks sponsored by Russia, including related to the U.S. 2016 election, French elections in 2017, the 2018 Olympic games, and Ukraine.

U.S. authorities worked with authorities from many nations to take down Hydra and Genesis Market, who sold account access credentials stolen from 1.5 million compromised computers.[7] And in January, DOJ shut down Hive, one of the largest ransomware groups.

The U.S. Department of Treasury ("Treasury") recently found that "the most current illicit finance risk in this domain is from [decentralized finance] DeFi services that are not compliant with existing anti-money laundering ("AML")/countering the financing of terrorism ("CFT") obligations.[8] Treasury found that illicit actors, including ransomware gangs, thieves, scammers, and Democratic People's Republic of Korea cyber actors, are using DeFi services to transfer and launder illicit proceeds, exploiting vulnerabilities in the law enforcement regime as well as the DeFi technology.[9]

Digital asset technologies pose a significant risk of customer loss through cybercrime.

Last year was a record-setting year for crypto cybercrime with more than $3.8 billion stolen. The criminals are sophisticated, relentless, and often state actors. DeFi's open source code and public blockchain make it vulnerable to cyber hacks, as seen by the fact that 82% of the hacks involved DeFi.[10]

Exchanges also face cyber risks. FTX CEO John Ray recently reported that FTX "grossly deprioritized and ignored cybersecurity controls" and "lacked a reasonable ability to prevent, detect, respond to, or recover from a significant cybersecurity incident, including" a $432 million breach in November.[11]

Private key management is essential. In the Ronin Bridge hack, the largest hack ever, the hackers were able to access the private keys to steal $600 million in crypto.

Fortifying cross-chain bridges that permit users to migrate crypto assets across different blockchains is critical. Almost two-thirds of hacks affecting DeFi protocols came via breaches on cross-chain bridges.[12] Binance was hacked over a cross-chain bridge in October.[13]

It's also important to secure third party services, such as customer interfaces. Man-in-the-middle hacks exploit third party vulnerabilities, as seen in the $120 million Badger DAO hack.

Fraud has become a hallmark of digital asset markets, the human toll of which may be overlooked.

The hype and buzz around digital assets have attracted opportunists and criminals. The CFTC will aggressively police fraud in digital asset markets. We have filed 73 digital assets civil prosecutions for fraud and other illegal acts, about one-third of them during my tenure.[14] This, combined with my two decades of combatting fraud, give me

insight into the human toll of crypto fraud—the victims. Frauds involving ponzi schemes, rug pulls, fictitious projects, empty promises, and lies about track records of success, devastate victims financially and emotionally.

Perhaps the worst victimization comes from scammers who prey on loneliness in romance scams and the newly emerged "pig-butchering" scam, where scammers "fatten up" victims by tricking them into believing they are in a romantic relationship, and then "butcher" them into investing in a fraudulent crypto scheme on a fake website that looks like a legitimate crypto offering or trading platform.[15]

In 2022, frauds reported to the FBI involving cryptocurrency, including pig butchering, represented the highest of any category of investment scams. Losses from these scams have increased 183% since 2021, with $2.57 billion in losses in 2022.[16]

Digital assets pose non-bank financial stability risk.

Satoshi's vision for a peer-to-peer network to transfer value without a trusted third party and outside of the traditional financial system ("Trad Fi") is by design a shadow banking system. Much like other non-bank activity, regulators do not have visibility into risks of digital asset activity. I came to the CFTC from Treasury where for the last decade I served as the Special Inspector General over the Troubled Asset Relief Program ("SIGTARP"), in law enforcement and other work to strengthen financial stability after the 2008 financial crisis.

Within three months of joining the CFTC, starting in June 2022, I began warning of financial stability risks in crypto markets that echoed the 2008 crisis.[17] This included run risk, contagion risk, hidden exposures in opaque, complex products, and underlying assets that were not the high quality represented. I also said that because the Bitcoin (and other non-securities) markets were not regulated, regulators could not see the extent of the risk. Additionally, I warned of risks novel to crypto, such as conflicts of interests as many companies use multiple affiliates to serve as exchanges, brokers, clearing agencies, and other functions (known as vertical integration). And I warned that customer assets were commingled with company assets, and of heightened cyber risk. All of these risks were then publicly exposed. Digital assets have seen serious disruptions and market stresses, losing two-thirds of value in high profile meltdowns and a loss of market confidence evidenced by extremely fast runs often triggered by social media. Many retail customers have either lost their funds or seen them tied up in bankruptcies, particularly when customer assets were commingled with company assets.

Today I want to highlight two specific areas that contribute to financial stability risk: first, the fact that customers of crypto exchanges often do not have control of their assets or bankruptcy priority, and second, conflicts of interest including vertical integration.

Customers of Crypto Exchanges Often Do Not Have Control of their Assets or Bankruptcy Priority

Because crypto exchanges are often structured similar to traditional exchanges and perform similar functions, they present similar financial stability risks, but they are often outside of the regulatory perimeter or unwilling to step into it. Exchanges operate "off chain" maintaining customer trades in an internal, centralized account ledger, like traditional exchanges. The exchange also maintains possession and control of the customers' funds and crypto.

Customers may not realize that their transaction is not on the blockchain and that they do not have keys or other control over what they would consider to be *their* assets. Disclosures are inadequate in both content and delivery to be effective in informing customers of their rights and risks. Customers have been held to contractual language that most have never read, much less negotiated. They often scroll through electronic disclosures without reading them and click to accept. Courts are upholding these "click-wrap agreements" as seen in the Celsius bankruptcy, where the court found that customer deposits were owned by the exchange, not the customers.[18] This is further complicated when, as seen with FTX, customer assets are commingled with exchange assets.[19]

Conflicts of Interest Including Vertical Integration

FTX's actions with its affiliates laid bare the risk of undisclosed and unmitigated conflicts of interest—a risk that I warned about in October, a few weeks before FTX's collapse saying:[20]

> Crypto-related companies may serve multiple functions that are separated into different entities in traditional finance. An exchange may also be a market maker, clearinghouse, lender, and/or custodian. These conflicts present significant risk that in a regulated environment would be disclosed and resolved. In an unregulated environment, the full extent of these conflicts may not be disclosed or resolved, which could lead to cascading losses and contagion risk.[21]

Treasury Secretary Janet Yellen recently said that Treasury is "working to address risks associated with vertical integration of crypto-trading platforms and lack of visibility into the operations of subsidiaries and other entities across these businesses."[22] Vertical integration poses significant contagion risk. The extent of contagion risk is unknown when a regulator like the CFTC regulates one company, but has no visibility into, or oversight over, affiliates.

Managing digital asset risk

Given that digital assets are already of significant size in the global financial system, it is imperative that these serious risks are managed. The stakes are too high. Market integrity, national security, and financial stability are non-negotiable. The private sector and governments both have a role to play in reducing these risks and in protecting customers.

Managing National Security Risk and Illicit Finance Risk:

To reduce the risk of illicit finance, identity is a foundational challenge. It is essential for governments and the industry to address that which makes crypto so attractive to illicit finance—the allure of anonymity. While the public blockchain can provide some traceability and transparency, the use of mixers and technology designed to enhance anonymity presents substantial risk. Treasury recently sanctioned two mixers, Blender and Tornado Cash. Treasury said that Tornado Cash was used to launder $7 billion, including millions stolen by the Lazarus Group, a North Korea state-sponsored hacking group that engaged in cyber hacks to support illegal nuclear and ballistic missile programs.[23]

Law abiding customers do not want their funds mixed with North Korea cybergangs or terrorist organizations. Legally compliant crypto companies should not use these mixers.

It is possible for all crypto companies to distance themselves from mixers and anonymity-enhanced technology, while still appropriately providing financial privacy for customers. Financial privacy is different from anonymity. TradFi provides financial privacy while verifying identity, as part of KYC (know your customer), AML, and CFT controls. The digital asset industry should verify digital identity. There are existing technologies to provide digital identity, and more being developed, which was the subject of a recent meeting of the CFTC's Technology Advisory Committee that I sponsor.[24] Exchanges as well as those offering DeFi services should verify digital identity. More often than not, DeFi services are not fully decentralized but instead maintain central parties who could verify identity, and may be held accountable to do so. Congress is also considering new laws on addressing anonymity and digital identity.[25]

The U.S. government will continue to prioritize preventing crypto's use for illicit finance. DOJ continues to shut down crypto's path of illicit finance. The CFTC will continue to be aggressive in enforcing the law. The CFTC brought two enforcement actions against crypto exchanges, BitMEX and Binance, alleging that they undertook activities with customers in the U.S. that required CFTC registration and that they did not follow AML controls. For example, BitMEX took no steps to verify its customers' identities, allowing individual customers to trade simply by providing an email address.[26] The CFTC brought its action in parallel with the criminal indictment of four BitMEX executives.[27] Treasury has shown its willingness to sanction mixers. A couple of weeks ago, Treasury issued a report on the use of DeFi for illicit finance recommending strengthening U.S. AML/CFT supervision and, when relevant, enforcement of crypto activities, including DeFi services.[28]

Managing Financial Stability Risks: Governments have a responsibility to reduce the risks that digital assets pose to financial stability. This is still a sizeable market of around $1 trillion,[29] with a lot of participating retail investors. I advocate for a same risk, same regulatory outcome approach, with the same market guardrails and customers protections (including banning commingling of customer assets and customer priority in bankruptcy) that have proven to promote financial stability. In the U.S., Congress should consider closing the regulatory gap in the Bitcoin and other non-securities spot markets.[30] Congress should also consider reducing the risks of conflicts of interest, including those raised by vertical integration. This could include requiring firms to disclose and resolve conflicts of interest, and providing regulators greater visibility and oversight tools related to affiliates.

Eliminating Cyber Vulnerabilities: Cyber experts on the Committee that I sponsor agree that it will not be sufficient to manage cyber vulnerabilities; instead, the industry must eliminate those vulnerabilities. The stakes are too high, with hacks used to fund weapons and other illegal activity, and customers without recourse when their assets are stolen in a hack. It will not be sufficient to assume that smart contracts work without fail or that there are no vulnerabilities. The industry should strengthen cybersecurity, including through code audits, fortifying cross-chain bridges, strengthening private key management, and shoring up vulnerabilities of third party services.

Conclusion

These are global risks with implications far more dire than Satoshi could have conceived when he talked about the hornet's nest. Because digital assets cross

borders, countering these global risks will require both private sector commitment and international government cooperation and coordination. We are stronger working together. We can leave no safe passage for illicit finance, cyber criminals, fraudsters or those who risk the stability of our global financial system.

Appendix A:

The CFTC's Robust Enforcement Program in the Crypto Space

Fiscal Year	Total Number of Digital Asset Cases	Number of Digital Asset Cases Alleging Fraud or Manipulation
2023	7	7
2022	19	9
2021	23	8
2020	10	8
2019	4	3
2018	6	5
2017	1	1
2016	1	0
2015	2	0
Total	**73**	**41**

FY2023 Digital Asset Cases

1. CFTC v. Jeremy Rounsville, CFTC Docket No. 23-02 (Nov. 3, 2022)
2. CFTC v. Samuel Bankman-Fried, FTX Trading Ltd. d/b/a FTX.com (FTX), and Alameda Research LLC (Alameda), Caroline Ellison, and Gary Wang, No. 22-cv-10503 (S.D.N.Y. Dec. 13, 2022)
3. CFTC v. Avraham Eisenberg, No. 23-cv-173 (S.D.N.Y. Jan. 9, 2023)
4. CFTC v. Vista Network Technologies and Armen Temurian, No. 23-cv-01235 (E.D.N.Y. Feb. 15, 2023)
5. CFTC v. Nishad Singh, No. 23-cv-01684 (S.D.N.Y. Feb. 28, 2023)
6. CFTC v. Changpeng Zhao, Binance Holdings Limited, Binance Holdings (IE) Limited, and Binance (Services) Holdings Limited, No. 23-cv-01887 (N.D. Ill. Feb. 27, 2023)
7. CFTC v. Rashawn Russel, No. 23-cv-02691 (E.D.N.Y. April 11, 2023)

Y2022 Digital Asset Cases

1. CFTC v. Tether Holdings Limited, et al., CFTC Docket No. 22-04 (Oct. 15, 2021)
2. CFTC v. iFinex Inc., BFXNA Inc., and BFXWW, CFTC Docket No. 22-05 (Oct. 15, 2021)
3. CFTC v. Blockratize, Inc. d/b/a Polymarket.com, CFTC Docket No. 22-09 (Jan. 03, 2022)
4. CFTC v. Dwayne Golden, et. al., No. 22-cv-1252 (E.D.N.Y. filed March 8, 2022)
5. CFTC v. James Ward, CFTC Docket No. 22-12 (Mar. 8, 2022)
6. CFTC v. Eddy Alexandre and Eminifx, Inc., No. 22-cv-03822 (S.D.N.Y. filed May 5, 2022)
7. CFTC v. Sam Ikkurty a/k/a Sreenivas I Rao, Ravishankar Avadhanam, and Jafia LLC, No. 22-cv-2465 (N.D. Ill. Filed May 10, 2022)
8. CFTC v. Gemini Trust Co., LLC, No. 22-cv-04563 (S.D.N.Y. filed June 2, 2022)

9. CFTC v. Mirror Trading International Proprietary Limited and Cornelius Johannes Steynberg, No. 22-cv-00635 (W.D. Tex. filed June 30, 2022)
10. CFTC v. Emerson Pires, Flavio Goncalves, Joshua Nicholas and Empires Consulting Corp., No. 22-cv-21997 (S.D. Fla. filed June 30, 2022)
11. CFTC v. Rathnakishore Giri, NBD Eidetic Capital, LLC, and SR Private Equity, LLC, No. 22-cv-3091 (D. Ohio Aug. 12, 2022)
12. CFTC v. bZeroX, Tom Bean, and Kyle Kistner, CFTC Docket No. 22-31 (Sept. 22, 2022)
13. CFTC v. Ooki DAO, No. 22-cv-5416 (N.D. Cal. Sept. 22, 2022)
14. CFTC v. Cryptostockoptionstrade Ltd., CFTC Docket No. 22-26 (Sept. 22, 2022)
15. CFTC v. Global Smart Option Broker Ltd., CFTC Docket No. 22-27 (Sept. 22, 2022)
16. CFTC v. Hypertradingoption Ltd., CFTC Docket No. 22-28 (Sept. 22, 2022)
17. CFTC v. Stockbrokertechniques Ltd., CFTC Docket No. 22-29 (Sept. 22, 2022)
18. CFTC v. SprintTrade, CFTC Docket No. 22-26 (Sept. 25, 2022)
19. CFTC v. Adam Todd, Digitex LLC, Digitex Limited, Digitex Software Limited, and Blockster Holdings Limited Corporation, No. 22-cv-23174 (S.D. Fla. Sept. 30, 2022)

FY 2021 Digital Asset Cases

1. CFTC v. HDR Global Trading Limited, 100x Holdings Limited, ABS Global Trading Limited, Shine Effort Inc Limited, HDR Global Services(Bermuda) Limited, Arthur Hayes, Benjamin Delo, and Samuel Reed, No. 1:20-cv-08132 (S.D.N.Y. filed Oct. 1, 2020)
2. CFTC v. Jeremy Spence, No. 1:21-cv-00699 (S.D.N.Y. filed Jan. 26, 2021)
3. CFTC v. John David McAfee; Jimmy Gale Watson, No. 1:21-cv-01919 (S.D.N.Y. filed Mar. 5, 2021)
4. CFTC v. Coinbase Inc., CFTC Docket No. 21-03 (Mar. 19, 2021)
5. CFTC v. Glenn Olson, CFTC Docket No. 21-05 (Apr. 6, 2021)
6. CFTC v. Josef Gherman and J Squared LLC, CFTC Docket No. 21-06 (Apr. 20, 2021)
7. CFTC v. Abner Alejandro Tinoco and Kikit & Mess Investments, No. 3:21-cv-00237-DCG (W.D. Tex. Sept. 28, 2021)
8. CFTC v. Payward Ventures, Inc. d/b/a Kraken, CFTC Docket No. 21-20 (Sept. 29, 2021)
9. CFTC v. Tradingforexpay, CFTC Docket No. 21-32 (Sept. 30, 2021)
10. CFTC v. Cryptofxtrader, CFTC Docket No. 21-23 (Sept. 30, 2021)
11. CFTC v. Bitfxprofit, CFTC Docket No. 21-22 (Sept. 30, 2021)
12. CFTC v. Globalnationfx, CFTC Docket No. 21-25 (Sept. 30, 2021)
13. CFTC v. BinanceFxTrade, CFTC Docket No. 21-21 (Sept. 30, 2021)
14. CFTC v. MaxForexOption, CFTC Docket No. 21-26 (Sept. 30, 2021)
15. CFTC v. ProCryptoMinners, CFTC Docket No. 21-28 (Sept. 30, 2021)
16. CFTC v. ProFX-Capitals, CFTC Docket No. 21-29 (Sept. 30, 2021)
17. CFTC v. Smarter Signals, CFTC Docket No. 21-30 (Sept. 30, 2021)
18. CFTC v. Prime Expert Trade, CFTC Docket No. 21-27 (Sept. 30, 2021)

19. CFTC v. Star Fx Pro, CFTC Docket No. 21-31 (Sept. 30, 2021)
20. CFTC v. Excotradeoptions, CFTC Docket No. 21-24 (Sept. 30, 2021)
21. CFTC v. Climax Capital FX, CFTC Docket No. 21-33 (Sept. 30, 2021)
22. CFTC v. Digitalexchange24.com, CFTC Docket No. 21-34 (Sept. 30, 2021)
23. CFTC v. Uduakobong Udo Inyangudo, No. 1:21-cv-11615 (Sept. 30, 2021)

FY 2020 Digital Asset Cases *(exclusive of administrative matters)*

1. CFTC v. XBT Corp. SARL d/b/a First Global Credit, CFTC Docket No. 20-04 (Oct. 31, 2019)
2. CFTC v. Q3 Holdings, LLC, Q3 I, LP, and Ackerman, No. 1:20-CV-01183 (S.D.N.Y. Feb. 11, 2020)
3. CFTC v. Joshua Christian McDonald and Perfection PR Firm LLC, No. 20-cv-00261 (E.D. Mo. filed February 14, 2020)
4. CFTC v. Clark, and Venture Capital Investments Ltd., No. 1:20-cv-00382 (D. Colo. Feb. 14, 2020)
5. CFTC v. Alan Friedland, Fintech Investment Group, Inc. and Compcoin LLC, No. 6:20-cv-00652 (M.D. Fla. filed Apr. 16, 2020)
6. CFTC v. Daniel Fingerhut, Digital Platinum, Inc., Digital Platinum, Ltd., Huf Mediya Ltd., Tal Valariola and Itay Barak, No. 1:20-cv-21887-DPG (S.D. Fla. filed May 5, 2020)
7. In re Plutus Financial, Inc. d/b/a Abra, and Plutus Technologies Philippines Corp. d/b/a Abra International, CFTC Docket No. 20-23 (Jul. 13, 2020)
8. CFTC v. Dennis Jali, Arley Ray Johnson, and John Frimpong, 1st Million LLC, Smart Partners LLC, and Access to Assets LLC, No. 8:20-cv-02492-GJH (D. Md. filed Aug. 28, 2020)
9. CFTC v. Mayco Alexis Maldonado Garcia, Cesar Castaneda, Joel Castaneda Garcia, and Rodrigo Jose Castro Molina, jointly d/b/a Global Trading Club, No. 4:20-cv-03185 (S.D. Tex. filed Sep. 11, 2020)
10. CFTC v. Laino Group Limited d/b/a PaxForex, No. 20-cv-03317 (S.D. Tex. Filed Sept. 28, 2020)

FY 2019 Digital Asset Cases

1. In re Joseph Kim, CFTC Docket No. 19-02 (CFTC filed October 29, 2018)
2. CFTC v. Control-Finance Limited, and Reynolds, No. 1:19-cv-05631 (S.D.N.Y. filed Jun. 17, 2019)
3. CFTC v. Jon Barry Thompson, No. 1:19-cv-09052 (S.D.N.Y. filed Sep. 30, 2019)
4. CFTC v. Circle Society Corp. and David Saffron, No 19-cv-01697 (D. Nev. Filed Sept. 30, 2019)

FY 2018 Digital Assets Cases

1. CFTC v. Patrick K. McDonnell and CabbageTech, Corp. d/b/a Coin Drop Markets, No. 1:18-cv-00361 (E.D.N.Y. filed Jan. 18, 2018)
2. CFTC v. Dillon Michael Dean and The Entrepreneurs Headquarters Limited, No. 18-cv-345 (E.D.N.Y. filed Jan. 18, 2018)
3. CFTC v. Blake Harrison Kantor, Nathan Mullins, Blue Bit Banc, Blue Bit Analytics (E.D.N.Y. filed April 16, 2018)

4. CFTC v. Randall Crater, Mark Gillespie and My Big Coin Pay, Inc., No. 1:18-cv-10077-RWZ (D. Ma. filed Jan. 16, 2018, amended Apr. 20, 2018)
5. CFTC v. 1pool Ltd, No. 18-cv-2243 (D.D.C. filed Sept. 27, 2018)
6. CFTC v. Diamonds Trading Investment House and First Options Trading, No. 18-cv-00807-O (N.D. Tex. Filed Sept. 28, 2018)

FY 2017 Digital Asset Cases

1. CFTC vs. Gelfman Blueprint, Inc., et al., Case 1:17-cv-07181 (S.D.N.Y. filed Sept. 21, 2017)

FY 2016 Digital Asset Cases

1. In re BFXNA Inc. d/b/a BITFINIX, CFTC Docket No. 16-19 (Filed 6/2/2016)

FY 2015 Digital Asset Cases

1. In re Coinflip, Inc. d/b/a Derivabit and Francisco Riordan, CFTC Docket No. 15-29 (CFTC filed Sep. 17, 2015)
2. In re TeraExchange LLC, CFTC Docket No. 15-33 (CFTC filed Sep. 24, 2015)

---

[1] *See* Pete Rizzo, *10 Years Ago Today, Bitcoin Together Satoshi Nakamoto Sent His Final Message*, Forbes (Apr. 26, 2021), 10 Years Ago Today, Bitcoin Creator Satoshi Nakamoto Sent His Final Message (forbes.com).
[2] *See* Pete Rizzo, *The Last Days of Satoshi: What Happened When Bitcoin's Creator Disappeared*, (Apr. 26, 2021), What Happened When Bitcoin Creator Satoshi Nakamoto Disappeared - Bitcoin Magazine - Bitcoin News, Articles and Expert Insights.
[3] *See* The White House, Council of Economic Advisors, *Economic Report of the President*, *Together with the Annual Report of the Council of Economic Advisors, "Digital Assets Relearning Economic Principles,"* (Mar. 2023), *https://www.whitehouse.gov/wp-content/uploads/2023/03/ERP-2023.pdf*.
[4] *See* CFTC Commissioner Christy Goldsmith Romero, *Crypto's Crisis of Trust: Lessons Learned from FTX's Collapse*, (Jan. 18, 2023) https://www.cftc.gov/PressRoom/SpeechesTestimony/oparomero5.
[5] *See* Attorney General, U.S. Department of Justice, *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*, (Sept. 6, 2022), https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf.
[6] *See* Deputy Secretary Wally Adeyemo, *Remarks by Deputy Secretary of Treasury Wally Adeyemo on Action Against Russian Illicit Finance*, (Jan. 18, 2023), Remarks by Deputy Secretary of the Treasury Wally Adeyemo on Action Against Russian Illicit Finance | U.S. Department of the Treasury.
[7] *See* U.S. Department of Justice, *Criminal Marketplace Disrupted in International Cyber Operation*, (Apr. 5, 2023), https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation.
[8] *See* Treasury, *Illicit Finance Risk Assessment of Decentralized Finance*, (April 2023), Treasury Releases 2023 DeFi Illicit Finance Risk Assessment | U.S. Department of the Treasury.
[9] *See Id.*
[10] *See* Chainalysis, *The 2023 Crypto Crime Report,*(Feb. 2023), https://go.chainalysis.com/2023-crypto-crime-report.html. See *also* Chainalysis, *2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers* (Feb. 1, 2023), https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/. *See also* TRM Labs, *DeFi, Cross-Chain Bridge Attacks Drive Record Haul from Cryptocurrency Hacks and Exploits*, (Dec. 16, 2022) https://www.trmlabs.com/post/defi-cross-chain-bridge-attacks-drive-record-haul-from-cryptocurrency-hacks-and-exploits.

[11] *See First Interim Report of John J. Ray III*, In re FTX Trading Ltd. et al., (Del. Bankr. Ct. Apr. 9, 2023).
[12] *See* Chainalysis, *2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers*, (Feb. 1, 2023), https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/.
[13] *See Binance CEO Changpeng Zhao breaks down $570 million crypto hack*, CNBC (Oct. 7, 2022), https://www.cnbc.com/video/2022/10/07/binance-ceo-changpeng-zhao-breaks-down-570-million-crypto-hack.html.
[14] *See* U.S. Commodity Futures Trading Commission, *Annual Enforcement Results, Appendix A: FY 2022 Enforcement Actions,* "Listing of Those CFTC FY 2022 Enforcement Actions That Involved Conduct Related to Digital Assets," (Oct. 20, 2022), https://www.cftc.gov/media/7861/DOE_ResultsFY22_AddendumA100722/download. Appendix A to this speech includes CFTC enforcement cases so the public can see our efforts to reduce risk through law enforcement, available at https://www.cftc.gov/media/8491/AppendixA_TheCFTCs_Robust_Enforcement_Program_in_the_Crypto_Space042523/download.
[15] *See* U.S. Department of Justice, *Justice Department Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case* (Apr. 3, 2023), https://www.justice.gov/usao-cdca/pr/justice-dept-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes-over-half.
[16] *See Id.*
[17] Axios (full video available), *CFTC Commissioner Calls for More Crypto Regulation* (June 14, 2022), CFTC commissioner calls for crypto regulation (axios.com) ("Goldsmith Romero, who spent time at the Treasury Department overseeing the TARP program, noted two similarities between the state of crypto today and what took place in the 2008 financial crisis."); *see also* CFTC Commissioner Christy Goldsmith Romero, Financial Stability Risks of Crypto Assets: Remarks before the International Swaps and Derivatives Association's Crypto Forum 2022, New York (Oct. 26, 2022) ("Crypto markets face similar financial stability risks as the traditional financial system, with parallel themes to 2008."); *see also* Coin Desk, *CFTC Commissioner Romero on Why Crypto Echoes Risk of 2008 Financial Crisis* (Oct. 27, 2022), CFTC Commissioner Romero on Why Crypto Echoes Risks of 2008 Financial Crisis | Watch (msn.com); *see also* CFTC Commissioner Christy Goldsmith Romero, *Protecting Against Emerging Global Fintech Threats in Cyberspace and Cryptocurrencies* (Nov. 30, 2022), Keynote Remarks of Commissioner Christy Goldsmith Romero at the Futures Industry Association, Asia Derivatives Conference, Singapore | CFTC.
[18] *Memorandum Opinion and Order Regarding Ownership of Earn Account Assets,* In re Celsius Network, LLC, et al. (S.D.N.Y. Bankr. Ct. Jan. 4, 2023), IN RE CELSIUS NETWORK LLC | Case No. 22-10964... | 20230105500| Leagle.com (Chief Bankruptcy Judge Martin Glenn ruled that Celsius owned $4.2 billion in customer stablecoin and other deposits made in connection with its "Earn" program, not the customers who deposited crypto into their accounts. This left approximately 600,000 Celsius customers holding only general unsecured claims, without bankruptcy priority.)
[19] *See First Interim Report of John J. Ray III*, In re FTX Trading Ltd. et al., (Del. Bankr. Ct. Apr. 9, 2023) ("FTX was controlled by a small group of individuals who commingled and misused corporate and customer funds, lied to third parties about their business, joked internally about their tendency to lose track of millions of dollars in assets, and thereby caused the FTX Group to collapse as swiftly as it had grown.")
[20] *See Id.* (In FTX's bankruptcy, it was reported that affiliate Alameda Research had special privileges on FTX exchanges "to trade and withdraw virtually unlimited" amounts of customer assets and avoid liquidation.)
[21] CFTC Commissioner Christy Goldsmith Romero, *Financial Stability Risks of Crypto Assets: Remarks before the International Swaps and Derivatives Association's Crypto Forum 2022, New York* (Oct. 26, 2022).
[22] *See Remarks by Secretary of the Treasury Janet L. Yellen at the National Association for Business Economics 39th Annual Economic Policy Conference*, (Mar. 30, 2023), Remarks by Secretary of the Treasury Janet L. Yellen at the National Association for Business Economics 39th Annual Economic Policy Conference | U.S. Department of the Treasury.

[23] *See* Office of Foreign Assets Control, U.S. Department of the Treasury, *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups* (Sept. 13, 2019), https://home.treasury.gov/news/press-releases/sm774; *see also* Office of Foreign Assets Control ("OFAC"), U.S. Department of the Treasury, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash* (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

[24] *See* U.S. Commodity Futures Trading Commission's Technology Advisory Committee, *Inaugural Meeting of the Newly Constituted Technology Advisory Committee Covering DeFi, Cyber Resilience, and Responsible AI* (Mar. 22, 2023), https://www.youtube.com/watch?v=a7xcSGxesRE.

[25] *See* Digital Asset Anti-Money Laundering Act of 2022, DAAML Act of 2022.pdf.

[26] *See* Attorney General, U.S. Department of Justice, *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*, (Sept. 6, 2022), https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf ("BitMEX falsely claimed that it did not serve U.S. customers, but in fact it had extensive U.S.-based operations and served thousands of U.S. customers. As a result of its willful failure to implement AML and KYC programs, BitMEX was in effect a money laundering platform. For example, in May 2018, Arthur Hayes, BitMEX's founder and CEO, was notified of allegations that BitMEX was being used to launder the proceeds of a cryptocurrency hack. However, the company took no steps to file a suspicious activity report, as required by law, and filed no suspicious activity reports from September 2015 through September 2020, the charged time period. An analysis by FinCEN concluded that BitMEX conducted at least $209 million worth of transactions with known darknet markets or unregistered MSBs providing mixing services…. In August 2021, the company settled with the CFTC and also settled a regulatory action brought by FinCEN, agreeing to pay a total of a $100 million fine. Additionally, all four defendants in the criminal case entered guilty pleas in 2022, and each of the three founders agreed to pay a $10 million fine.")

[27] *See Id.*

[28] *See* Treasury, *Illicit Finance Risk Assessment of Decentralized Finance*, (April 2023), Treasury Releases 2023 DeFi Illicit Finance Risk Assessment | U.S. Department of the Treasury.

[29] *See Cryptocurrency Prices by Market Cap*, CoinMarketCap (last accessed Apr. 3, 2023), Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap. Bitcoin, which is often viewed as a proxy for crypto-market sentiment, comprises half of that total market cap and in 2023, soared more than 70%.

[30] Congress is considering legislation in this area as seen with two bills introduced in the last Congress.