Volume 5, No. 1 | January–February 2022

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Editor's Note: Transparency
Steven A. Meyerowitz

Archimedes' Lever and Audience Participation—or—Multifactor Soft-Law Transparency for AI System Process Development
James A. Sherer

National Artificial Intelligence Advisory Committee Established by Department of Commerce
Lamar Smith, Natasha G. Kohne, Ed Pagano, Hans Christopher Rickhoff, and Christina Barone

AI as a Patent Inventor—An Update from South Africa and Australia
Anna Yuan, Georgia Wright, and Alistair Maughan

New U.S. Digital Assets Bill Casts Wide Net
Yvette D. Valdez, Stephen P. Wink, Adam Bruce Fovent, Adam Zuckerman, and Deric Behar

Six Things Employers Need to Know Before Offering Cryptocurrency in 401(k)s
Caroline S. Scala, Raymond W. Perez, Tyler Woods, and Erica G. Wilson

Federal Court Says Voice Service Providers "Mey" Face TCPA Liability for Facilitating Spoofed Robocalls
John C. Nelson Jr., Ken Payson, David M. Gossett, and John D. Seiver

International Coalition Publishes Report and Recommendations on AI and Medicinal Products
Grant Castle, Daniel Pavin, Ellie Handy, and Sam Jungyun Choi

Decentralized Finance—Risks, Regulation, and the Road Ahead
Katherine Kirkpatrick, Matthew B. Hanson, Ana B. Daily, and Thomas Spiegler

Everything Is Not *Terminator*: AI-Generated Content Under the First Amendment
John Frank Weaver

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 5, No. 1 | January–February 2022

5 **Editor's Note: Transparency**
Steven A. Meyerowitz

9 **Archimedes' Lever and Audience Participation—or—Multifactor Soft-Law Transparency for AI System Process Development**
James A. Sherer

35 **National Artificial Intelligence Advisory Committee Established by Department of Commerce**
Lamar Smith, Natasha G. Kohne, Ed Pagano, Hans Christopher Rickhoff, and Christina Barone

37 **AI as a Patent Inventor—An Update from South Africa and Australia**
Anna Yuan, Georgia Wright, and Alistair Maughan

41 **New U.S. Digital Assets Bill Casts Wide Net**
Yvette D. Valdez, Stephen P. Wink, Adam Bruce Fovent, Adam Zuckerman, and Deric Behar

51 **Six Things Employers Need to Know Before Offering Cryptocurrency in 401(k)s**
Caroline S. Scala, Raymond W. Perez, Tyler Woods, and Erica G. Wilson

57 **Federal Court Says Voice Service Providers "Mey" Face TCPA Liability for Facilitating Spoofed Robocalls**
John C. Nelson Jr., Ken Payson, David M. Gossett, and John D. Seiver

61 **International Coalition Publishes Report and Recommendations on AI and Medicinal Products**
Grant Castle, Daniel Pavin, Ellie Handy, and Sam Jungyun Choi

67 **Decentralized Finance—Risks, Regulation, and the Road Ahead**
Katherine Kirkpatrick, Matthew B. Hanson, Ana B. Daily, and Thomas Spiegler

81 **Everything Is Not *Terminator*: AI-Generated Content Under the First Amendment**
John Frank Weaver

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Decentralized Finance—Risks, Regulation, and the Road Ahead

Katherine Kirkpatrick, Matthew B. Hanson, Ana B. Daily, and Thomas Spiegler*

In this article, the authors explore the risks of decentralized finance as it grows and, in turn, draws increasing scrutiny from regulators.

Even those who are most suspicious of the rise of cryptocurrency will likely admit that the underlying blockchain technology and its potential uses are exciting. One use of this technology, decentralized finance, or DeFi, is on the cusp of major growth. Regulators are aware of this growth and are moving to act accordingly. As a possible preview of the coming regulatory efforts, in the spring of 2021 Treasury Secretary Janet Yellen urged regulators to accelerate their establishment of a regulatory framework for stablecoins, a rapidly growing class of digital currencies that, among other things, can be used on DeFi platforms to temper pricing volatility.[1]

Since Secretary Yellen's comments, Securities and Exchange Commission ("SEC") Chair Gary Gensler has made it clear that the regulation of DeFi platforms and stablecoins is on the SEC's agenda.[2] Chair Gensler wrote to Senator Elizabeth Warren that both should be among Congress' legislative priorities, adding that "[r]egulators would benefit from additional plenary authority to write rules for and attach guardrails to crypto trading and lending."[3] The SEC also brought its first enforcement case against a DeFi platform in August 2021.[4] In this article, we explore the risks of DeFi as it grows and, in turn, draws increasing scrutiny from regulators.

DeFi Basics

DeFi describes blockchain-based alternative finance systems. DeFi platforms enable users to engage in traditional financial transactions like lending and borrowing through direct peer-to-peer exchanges, eliminating the role of traditional financial intermediaries by directly mediating the transfer of value. Transactions

Robotics, Artificial Intelligence & Law / January–February 2022, Vol. 5, No. 1, pp. 67–80.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

are settled on a public blockchain, rather than through a bank or other central institution. DeFi services use a non-custodial design, meaning assets issued or managed on DeFi platforms theoretically cannot be moved or expropriated unilaterally by parties other than the account owners.[5] The use of open source code—meaning code designed to be publicly accessible—allows participants to view and verify protocols directly as well as create derivative or competitive services.[6] The composability[7] of DeFi's programmatic components allows financial instruments and services to incorporate multiple DeFi services and protocols, which distinguishes DeFi from private services or standalone digital assets.[8] To effectuate transactions, DeFi uses open protocols[9] and decentralized applications, or DApps.[10]

These protocols and DApps are powered by smart contracts—programs that automatically run when certain conditions are met, which are generally built on existing blockchains such as Ethereum.[11] Smart contracts replace the intermediary role of centralized financial institutions with self-executing lines of code built into a blockchain.[12]

DeFi has experienced fast-paced growth since mid-2020. As of August 2021, the "total value locked" in DeFi sits around $75 billion.[13] This value represents the amount of assets that are currently being staked across all DeFi protocols (i.e., pledged, loaned, or otherwise provided to the network to fund DeFi transactions). And even that figure may only be a fraction of its future potential.[14]

DeFi Risks

Despite DeFi's rapid growth, its open source ecosystem with the potential to democratize banking and finance, and its potential efficiencies, there are significant risks for industry participants to consider. These can be categorized into three buckets: technological risk, asset risk, and compliance/legal risk.

Technological Risk

The technological risks implicated by DeFi are rooted in the current limitations of blockchain technology. Many DeFi protocols are powered by Ethereum, including nine of the largest DeFi projects.[15] The Ethereum public blockchain infrastructure is far

from infallible: increased customer adoptions of DeFi has led to a corresponding increase in attacks, bugs, and network congestion. These can lead to high network transaction fees, failed transactions, and liquidation issues. In some cases, extreme network congestion has led DeFi apps to stop functioning altogether. In March 2020, for example, network congestion caused a major DeFi app to malfunction, leading to over $8.32 million worth of cryptocurrency being auctioned off for nothing.[16]

In addition to scalability challenges, DeFi platforms—like other forms of financial services operations—also face major cybersecurity threats. Smart contract security has improved since the notorious decentralized autonomous organization ("DAO") hack of 2016, in which $50 million in Ether was stolen.[17] Nonetheless, several major players have recently experienced cybersecurity attacks, resulting in significant losses. Hackers stole about $120 million from DeFi protocols in 2020 in 15 separate attacks—less than half was later recovered.[18] By the midpoint of this year, there had been at least 23 attacks, netting hackers more than $400 million in value.[19] And that was before one major DeFi platform disclosed on August 10 that hackers had stolen digital assets worth more than $600 million from its platform.[20] Many of the major DeFi "hacks" have been so-called "flash loan attacks"[21] that sometimes take advantage of temporary defects in price feeds.[22] Other examples have seen attackers exploit bugs or flaws within a protocol code.[23]

Further, even if the smart contracts are technologically sound, hackers can target other vulnerabilities. For example, in April 2021, hackers targeted one DeFi protocol by stealing access to the code from the founder's computer. The situation resulted in losses of around $80 million.[24]

And beyond hackers, investors risk being targeted by exit scams, such as "rug pulls." Exit scams are typically understood in the context of an initial coin offering ("ICO"), where promoters take off with investors' money during or after the ICO. DeFi rug pulls are a new form of exit scam where a developer abandons a project and leaves with the funds.[25] Harkening back to more traditional forms of offering fraud, anonymous team members on social media promise a large annual percentage yield ("APY") to retail liquidity providers, and, as soon as enough funds have been locked into a smart contract, the developer withdraws all the funds from the liquidity pool and disappears, causing the token's price to crash to zero.[26]

Given the ever-growing scale of financial transactions in this space, even minor instability or hiccups in data security could result in significant losses for individual investors. As a result, insurance brokers are also beginning to get involved, providing users with insurance against losses due to hacks or malfunctioning software.[27]

Asset Risk

DeFi applications are often built on the Ethereum blockchain, and the collateral pledged in DeFi transactions is typically cryptocurrency. Given the volatility of digital assets, it is possible for the value of that collateral to decline sharply, causing associated liquidity risks. This, in turn, can fuel a broader sell-off, and this uncertainty and instability can lead to catastrophic "bank runs" that send token values plummeting.

The volatility of the crypto market is well known. In 2018, for instance, Bitcoin dropped more than 80 percent, nearing its worst ever bear market before rebounding.[28] And the market can be heavily influenced by unexpected outside factors like social media. For example, after Tesla CEO and crypto enthusiast Elon Musk tweeted a meme interpreted by many to mean Tesla might scale back its Bitcoin holdings, Bitcoin dropped significantly.[29] As one investor put it, "the market movement post-Musk's tweets continues to show how nascent this asset class is."[30]

While panic buying results in major spikes, driving up value beyond the true underlying value, panic selling of DeFi tokens can likewise result in major crashes that would be highly unusual with fiat currency. For example, in June 2021, tokens including Galaxium and Crypto Village Accelerator each lost more than 60 percent over the course of 24 hours.[31] Even more established tokens such as Uniswap lost seven percent in the same 24-hour period, which although not as extreme as the headline-grabbing 60 percent loss for less established tokens, still points to significant volatility of the kind that would be highly unusual with fiat currencies like the U.S. dollar.[32] Sophisticated investors are not immune from this volatility and associated risks. For example, entrepreneur Mark Cuban called for regulation of DeFi after a DeFi token he held crashed to zero in one day as a result of a "bank run" on the token.[33]

Some individuals have sought to use stablecoins, which are backed by an asset (often fiat currency), to minimize this risk.

Early on, DeFi apps would attract new users and deposits by offering high yields that were typically paid out in the native token of the protocol, which were typically very volatile. Stablecoins, as the name would suggest, are designed to be more stable, in some cases thanks to being collateralized by the value of an underlying asset like U.S. dollar cash and cash equivalents. Basing transactions on these familiar units is appealing to some investors more comfortable with traditional financial services. But with great risk comes potentially great reward. Although using stablecoins theoretically dampens volatility as compared to other tokens, their use is often associated with lower returns because of lower risk, due at least in part to their tie to fiat currencies.[34]

Compliance Risk

DeFi is still in its infancy. Many DeFi services are offered by unincorporated entities that operate outside of regulatory structures that exist around more traditional financial products. Most of the services in the space are software programs that automate financial transactions and replace the traditional role of the bank as an intermediary. This creates several risks and results in an uncertain regulatory environment. The lack of intermediaries, the anonymity of peer-to-peer transactions, and the global reach of DeFi present potentially amplified compliance risks for participants in the space. In the absence of clear, direct guidance from regulatory agencies, DeFi platforms face potentially vast and confusing compliance and legal obligations. Their operations can implicate a host of considerations, ranging from anti-money laundering to consumer protection.

To address these issues, investors, experts, and regulators alike have called for greater regulatory clarity in the realm of DeFi. All eyes are on the federal financial regulators and Congress as those groups of policymakers attempt to navigate a novel and highly complex arena and to construct a workable regulatory regime. To date, much of the guidance provided so far on digital assets has focused on areas such as initial coin offerings, and not necessarily on DeFi. Although, if the recent public comments, enforcement interest, and stablecoin conversations among financial regulators are signs, that may change in the near-to-medium term.

Regulatory Environment

Several regulators have weighed in with guidance relevant to DeFi developers and users. But the decentralized nature of DeFi makes it uniquely hard to regulate as rule makers are faced with the question of who, what, where, and how to regulate a rapidly changing space.

SEC Guidance

Given the wide range of regulators that oversee various corners of traditional financial services products, creating a robust DeFi regulatory framework will likely involve a significant amount of coordination among regulators.

In May, SEC Chair Gensler highlighted the number of challenges for investors and SEC staff posed by "[c]rypto lending platforms and so-called decentralized finance ('DeFi') platforms."[35] Chair Gensler also signaled that the SEC under his watch would "be ready to bring cases involving issues such as crypto, cyber and fintech," in a speech to FINRA conference attendees.[36] Although much of the activity in DeFi is more akin to banking in nature (i.e., a significant amount of activity to date centers around borrowing, lending, and to a lesser extent, insurance), they involve a number of aspects that could bring them within SEC jurisdiction.[37] Chair Gensler stated as much in his August 3 speech and August 5 letter to Senator Warren, which directly asked for lawmakers to give the SEC more power to oversee crypto lending and DeFi platforms.[38]

Aside from Chair Gensler, SEC Commissioner Hester Peirce has stood out among the commissioners in expressing views publicly about DeFi. Peirce, in comments pre-dating but similar to Gensler's recent remarks, has stated that if a protocol intends to mimic securities or relate to asset management, it could be within the SEC's purview. In March 2021, for example, Peirce stated, "if you set up some sort of decentralized exchange (DEX) or automated market maker (AMM) that is trading securities among other things, then you have to think about what the implications are there."[39] (Commissioner Peirce has also proposed a three-year safe harbor proposal for token sales, although this proposal has not yet taken hold.[40])

The SEC's enforcement activity also sheds light on the SEC's thinking about Fintech, digital assets, and DeFi. In 2017, the SEC's "DAO Report," which stemmed from an investigation conducted by the SEC's Enforcement Division, stated that offers and sales of digital assets could be subject to federal securities laws.[41] What followed was a significant uptick in enforcement activity around the initial coin offering ("ICO") boom. Between 2017 and 2021, the SEC brought close to 80 crypto-related enforcement actions, over half of which related to ICOs.[42]

The SEC has so far only announced one enforcement action against a DeFi platform, and that case was really focused on the platform misrepresenting to investors how the platform was operating.[43] But the SEC also alleged unregistered sales of securities—violations of Sections 5(a) and 5(c) of the Securities Act of 1933—common allegations in the many enforcement actions brought against other digital asset businesses in recent years. Commentators in the space have noted that the SEC is looking very carefully at a number of DeFi projects, and as such, DeFi app developers should be mindful of the SEC's understanding of, and approach to decentralization to avoid SEC scrutiny.[44]

CFTC Guidance

The Commodity Futures Trading Commission ("CFTC") has also taken an interest in DeFi projects, some of which are within the CFTC's regulatory purview. The CFTC first announced jurisdiction over digital assets in its 2015 *CoinFlip* order, in which it stated that it considered virtual currencies to be "commodities" as defined by the Commodity Exchange Act ("CEA").[45] The CFTC's jurisdiction over digital assets deemed commodities is not as far reaching as the SEC's jurisdiction over securities. For example, the CFTC has exercised anti-fraud and anti-manipulation authority over virtual currencies that are traded as a commodity in interstate commerce or that are traded for future delivery, rather than immediate delivery. It also has more limited regulatory oversight over virtual currency spot markets that use margin, leverage, or financing.[46]

In October 2020, the CFTC brought an enforcement action against BitMEX, one of the world's largest crypto-based derivatives exchanges.[47] BitMEX was accused of allowing U.S. residents to transact without registering with the CFTC and failing to

implement key safeguards required by the CEA and CFTC's regulations. While BitMEX was not a DeFi project per se, charges against BitMEX for weak anti-money laundering and know-your-customer policies were warning signs for the world of decentralized finance.[48] Shortly thereafter, now-former CFTC chairman Heath Tarbert said during a CoinDesk event that the agency might be looking at other noncompliant cryptocurrency exchanges and DeFi projects.[49] On August 10, a federal court entered a consent order in the case that required five BitMEX entities to pay a $100 million civil monetary penalty.[50]

This past summer, Commissioner Dan Berkovitz also said in a public speech that unlicensed DeFi markets may be operating illegally in the United States.[51] Berkovitz noted that the "CEA requires futures contracts to be traded on a designated contract market (DCM) licensed and regulated by the CFTC." Berkovitz noted that there were no DeFi platforms registered as DCMs at that point. In July, Berkovitz noted that the DeFi space is getting a CFTC-wide review and that companies seeking to participate in the DeFi ecosystem should be consulting with regulators.

Conclusion

Participants in the Fintech space have long had to adapt to the fast-changing nature of new developments (and accompanying confusion regarding rules), and DeFi compliance is no exception. Because decentralized tools developed as an alternative to the traditional financial system established on trust, where intermediaries are needed to hold client assets and carry out transactions, the current framework of regulation based on this traditional model will undoubtedly encounter ways it fits only awkwardly onto a new system predicated on the absence of intermediaries.

Investors should take stock of technological, asset-specific, and compliance risks when considering whether to invest in a project and/or use DeFi networks for their use cases.

DeFi application developers and other project participants should consider implementing certain steps to ensure they have the processes in place to identify and deal with risks.

- First, market participants should set up a compliance department and designate responsible parties in the event

something goes wrong. Developers should consider who will deal with regulators in the event they ask questions, as well as how to anticipate possible scenarios that might cause compliance issues (and avoid them).

- Second, compliance departments should stay up-to-date on all recent guidance related to DeFi and digital asset regulation more broadly, which could provide insight into operational risks and solutions. DeFi project developers may consider setting up proactive meetings with regulatory stakeholders to gain insight into the current landscape and regulation slated to come down the pike.
- Third, participants should prioritize transparency in recording and publishing holdings, expenses, and transactions, so regulators can have access to relevant information easily, if necessary.
- Finally, DeFi stakeholders should take to heart the limited but concrete recent developments that might apply to their products. The SEC's recent enforcement actions make clear that DeFi projects might be subject to federal securities laws if the SEC views the related tokens as investment contracts. Therefore, industry participants should consider the legal implications of the *Howey* test, and consult experienced securities law counsel, when structuring their projects.

These risks will persist, even as the industry matures. And regulatory scrutiny will only increase along with the growth of the overall industry, as we may now see accelerated in the stablecoin space. Industry participants should take stock of the existing risks and requirements, ensure they have appropriate risk-based structures in place, and then demonstrate (through documentation on particularly important points) that they are abiding by those structures.

Notes

* Katherine Kirkpatrick (kkirkpatrick@kslaw.com), a partner in the Special Matters and Government Investigations practice and co-chair of King & Spalding LLP's Financial Services Industry group, focuses her practice on white-collar criminal defense, government and internal investigations, corporate compliance, and regulatory matters. Matthew B. Hanson (mhanson@kslaw.com) is a partner at the firm, representing companies and individuals in

government investigations by the Securities and Exchange Commission, the Department of Justice, Congress, and other federal and state regulators. Ana B. Daily (adaily@kslaw.com) is a Special Matters and Government Investigations associate at the firm. Thomas (Tom) Spiegler (tspiegler@kslaw.com) is an associate in the firm's Trial and Global Disputes practice.

1. Kevin Werbach, DeFi Is the Next Frontier for Fintech Regulation, The Regulatory Review (Apr. 28, 2021), *available at* https://www.theregreview.org/2021/04/28/werbach-defi-next-frontier-fintech-regulation/.

2. U.S. Sec. & Exch. Comm'n, Chair Gary Gensler, Remarks Before the Aspen Security Forum (Aug. 3, 2021), *available at* https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03. On DeFi platforms: "Make no mistake: To the extent that there are securities on these trading platforms, under our laws they have to register with the Commission unless they meet an exemption. Make no mistake: If a lending platform is offering securities, it also falls into SEC jurisdiction." And on stablecoins: "[T]he use of stablecoins on these platforms may facilitate those seeking to sidestep a host of public policy goals connected to our traditional banking and financial system: anti-money laundering, tax compliance, sanctions, and the like. This affects our national security, too. Further, these stablecoins also may be securities and investment companies. To the extent they are, we will apply the full investor protections of the Investment Company Act and the other federal securities laws to these products."

3. U.S. Sec. & Exch. Comm'n, Chair Gary Gensler Letter to Sen. Warren (Aug. 5, 2021), *available at* https://www.warren.senate.gov/imo/media/doc/gensler_response_to_warren_-_cryptocurrency_exchanges.pdf.

4. U.S. Sec. & Exch. Comm'n, SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings (Aug. 6, 2021), *available at* https://www.sec.gov/news/press-release/2021-145.

5. Decentralized Finance (DeFi) Policy-Maker Toolkit, World Economic Forum (June 8, 2021), *available at* http://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf.

6. *Id.*

7. *Id.* Composability refers to the concept that multiple components can be chosen and assembled in different ways to satisfy different users.

8. *Id.*

9. Open protocols, like open source software, are not owned by any particular entity.

10. Fabian Schar, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Economic Research Division of the Federal Reserve Bank of St. Louis (Feb. 5, 2021), *available at* https://files.stlouisfed.org/files/htdocs/publications/review/2021/04/15/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets.pdf.

11. Alan Cohn & Evan Abrams, Decentralized Finance (DeFi): Overview, Practical Law Finance (Dec. 2020).

12. How Do Ethereum Smart Contracts Work, CoinDesk (Dec. 30, 2020, 6:48 AM), *available at* https://www.coindesk.com/learn/how-do-ethereum-smart-contracts-work/.

13. Homepage, DeFi Pulse, *available at* https://defipulse.com/ (last accessed on June 23, 2021).

14. Financial Services Global Market Report 2021—By Type (Lending And Payments, Insurance, Reinsurance And Insurance Brokerage, Investments, Foreign Exchange Services), Business Research Company (Dec. 2020), *available at* https://www.thebusinessresearchcompany.com/report/financial-services-global-market-report-2020-30-covid-19-impact-and-recovery.

15. Gareth Jenkinson, As DeFi booms, Ethereum's blockchain competitors are catching up, Cointelegraph (Jan. 21, 2021), *available at* https://cointelegraph.com/news/as-defi-booms-ethereum-s-blockchain-competitors-are-catching-up.

16. Brady Dale, Mempool Manipulation Enabled Theft of $8M in MakerDAO Collateral on Black Thursday: Report, Nasdaq (Jul. 22, 2020, 2:41 PM), *available at* https://www.nasdaq.com/articles/mempool-manipulation-enabled-theft-of-%248m-in-makerdaocollateral-on-black-thursday%3A-report.

17. Klint Finley, A $50 Million Hack Just Showed That the DAO Was All Too Human, Wired (June 18, 2016, 04:38 AM), *available at* https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/.

18. Paul Vigna, DeFi Is Helping to Fuel the Crypto Market Boom—and Its Recent Volatility, Wall Street Journal (June 3, 2021, 5:30 AM), *available at* https://www.wsj.com/articles/defi-is-helping-to-fuel-the-crypto-market-boomand-its-recent-volatility-11622712602.

19. *Id.*

20. Anna Hirtenstein, Crypto Hackers Stole More Than $600 Million From DeFi Network, Then Gave Some of It Back, Wall Street Journal (Aug. 11, 2021 4:50 PM), *available at* https://www.wsj.com/articles/poly-network-hackers-steal-more-than-600-million-in-cryptocurrency-11628691400.

21. A flash loan is a form of instantaneous, smart contract-powered uncollateralized lending where a borrower must repay the loan before the transaction ends.

22. Osato Avan-Nomayo, DeFi hacks and exploits total $285M since 2019, Messari reports, Cointelegraph (Apr. 29, 2021), *available at* https://cointelegraph.com/news/defi-hacks-and-exploits-total-285m-since-2019-messari-reports; William Foxley, Everything You Ever Wanted to Know About the DeFi "Flash Loan" Attack, CoinDesk (Feb. 19, 2020), *available at* https://www.coindesk.com/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack.

23. Paddy Baker, DeFi Lender bZx Reclaims $8M Stolen in Sunday's Attack, CoinDesk (Sept. 14, 2020, 9:26 AM), *available at* https://www.coindesk.com/bzx-reclaims-8m-hack.

24. Jamie Crawley, DeFi Protocol EasyFi Reports Hack, Loss of Over $80M in Funds, CoinDesk (Apr. 20, 2021, 9:10 AM), *available at* https://www.coindesk.com/defi-protocol-easyfi-reports-hack.

25. Vildana Hajric, Katherine Greifeld, WhaleFarm Crash Is Latest Too-Good-To-Be True DeFi Collapse, Bloomberg (June 30, 2021, 10:34 AM), *available at* https://www.bloomberg.com/news/articles/2021-06-30/whalefarm-crash-is-latest-too-good-to-be-true-defi-collapse.

26. *Id.*

27. Ian Allison, Insurance Giant Aon Is Testing the Waters of DeFi, CoinDesk (Mar. 3, 2021), *available at* https://www.coindesk.com/insurance-giant-aon-is-testing-the-waters-of-defi.

28. Kate Rooney, Bitcoin is down more than 80% from last year's high, nearing its worst-ever bear market, CNBC (Nov. 26, 2018), *available at* https://www.cnbc.com/2018/11/26/bitcoin-nears-its-worst-ever-bear-market-down-more-than-80percent-from-the-high.html.

29. Elon Musk (@elonmusk), Twitter (Jun 3, 2021, 9:07 PM), https://twitter.com/elonmusk/status/1400620080090730501.

30. Daniel Cawrey, Market Wrap: Musk-Induced Sell-Off Spurs Crypto Price Drop Before a Slight Recovery, CoinDesk (Jun. 4, 2021), *available at* https://www.coindesk.com/market-wrap-musk-dump-most-of-crypto-fall-before-recovery.

31. Vildana Hajric, DeFi Crash Accelerates With Some Once-Hot Investments Losing 50%, Bloomberg (June 18, 2021, 8:37 PM), *available at* https://www.bloombergquint.com/onweb/defi-crash-accelerates-with-some-once-hot-investments-losing-50.

32. *Id.*

33. Joe Weisenthal, Mark Cuban Calls for Stablecoin Regulation After Trading Token That Crashed to Zero, BLOOMBERG (June 17, 2021), *available at* https://www.bloomberg.com/news/articles/2021-06-17/mark-cuban-defi-iron-finance-crashed-100.

34. Jordan Finneseth, Altcoin Roundup: Stablecoin pools could be the next frontier for DeFi, Cointelegraph (Jun 25, 2021), *available at* https://cointelegraph.com/news/altcoin-roundup-stablecoin-pools-could-be-the-next-frontier-for-defi.

35. U.S. Sec. & Exch. Comm'n, Chair Gary Gensler, Testimony Before the Subcommittee on Financial Services and General Government, U.S. House Appropriations Committee (May 26, 2021), *available at* https://www.sec.gov/news/testimony/gensler-2021-05-26.

36. U.S. Sec. & Exch. Comm'n, Chair Gary Gensler, Remarks at 2021 FINRA Annual Conference (May 20, 2021), *available at* https://www.sec.gov/news/speech/gensler-finra-conference.

37. U.S. Sec. & Exch. Comm'n, Chair Gary Gensler, Remarks Before the Aspen Security Forum (Aug. 3, 2021), *available at* https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03.

38. *See id.*; U.S. Sec. & Exch. Comm'n, Chair Gary Gensler Letter to Sen. Warren (Aug. 5, 2021), *available at* https://www.warren.senate.gov/imo/media/doc/gensler_response_to_warren_-_cryptocurrency_exchanges.pdf.

39. Ledger Insights, SEC's Hester Peirce Outlines DeFi Regulatory Issues (Mar. 24, 2021), *available at* https://www.ledgerinsights.com/sec-hester-peirce-outlines-defi-regulatory-issues/.

40. U.S. Sec. & Exch. Comm'n, Commissioner Hester M. Peirce, Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization (Feb. 6, 2020), *available at* https://www.sec.gov/news/speech/peirce-remarks-blockress-2020-02-06. The proposed safe harbor, which she said she intends to raise to SEC Chairman Gensler and her fellow commissioners, would create a sandbox that would allow for token sales to occur without fear of direct regulation. Commissioner Peirce first proposed the three-year grace period for developers and companies in the DeFi space to build and launch their networks last year, but this proposal failed to be adopted by the other commissioners. Undeterred, in April of this year, Peirce reintroduced an updated 2.0 version of her safe harbor proposal, posting the entire proposal on popular software hosting platform GitHub.

41. U.S. Sec. & Exch. Comm'n, U.S. Securities Laws May Apply to Offers, Sales, and Trading of Interests in Virtual Organizations (July 25, 2017), *available at* https://www.sec.gov/news/press-release/2017-131.

42. U.S. Sec. & Exch. Comm'n, Cyber Enforcement Actions, *available at* https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

43. U.S. Sec. & Exch. Comm'n, SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings (Aug. 6, 2021), *available at* https://www.sec.gov/news/press-release/2021-145.

44. Lachlan Keller, As SEC goes after Ripple and Bitcoiin2Gen, is DeFi next in its line of fire? Forkast (Feb. 1, 2021), *available at* https://forkast.news/defi-future-crypto-sec-decentralized-finance/.

45. *In re Coinflip, Inc.*, Dkt. No. 15-29 (C.F.T.C. Sept. 17, 2015).

46. American Bar Assoc., Digital and Digitized Assets: Federal and State Jurisdictional (Dec. 2020), *available at* https://www.americanbar.org/content/dam/aba/administrative/business_law/buslaw/committees/CL620000pub/digital_assets.pdf.

47. CFTC, Release Number 8270-20, CFTC Charges BitMEX Owners with Illegally Operating a Cryptocurrency Derivatives Trading Platform and Anti-Money Laundering Violations (Oct. 1, 2020), *available at* https://www.cftc.gov/PressRoom/PressReleases/8270-20.

48. Joshua Mapperson, Why the BitMEX charges could be bad news for DeFi, Cointelegraph (Oct. 2, 2020), *available at* https://cointelegraph.com/news/why-the-bitmex-charges-could-be-bad-news-for-defi.

49. Nikhilesh De, CFTC Chairman Heath Tarbert Talks Ethereum, DeFi and the Next BitMEX, CoinDesk (Oct. 14, 2020), *available at* https://www.coindesk.com/heath-tarbert-invest-eth-fireside.

50. CFTC, Release Number 8412-21, Federal Court Orders BitMEX to Pay $100 Million for Illegally Operating a Cryptocurrency Trading Platform and Anti-Money Laundering Violations (Aug. 10, 2021), *available at* https://www.cftc.gov/PressRoom/PressReleases/8412-21.

51. CFTC, Climate Change and Decentralized Finance: New Challenges for the CFTC (June 8, 2021), *available at* https://www.cftc.gov/PressRoom/SpeechesTestimony/opaberkovitz7.