DECENTRALIZED FINANCE: IDENTITY PROTECTION AND ECONOMIC OPPORTUNITY FOR BOTH GOOD AND BAD ACTORS

Alyssa Rose Domino*

INTRODUCTION

Imagine a world in which a person could take out and then pay off millions of dollars of loans without providing their personal identification. This world exists for anyone who has an internet connection.[1] Anyone with internet access can reach the decentralized finance (DeFi) ecosystem, an online network of financial products and services that allows people to lend, borrow, buy, and sell directly with others.[2] The network of transactions on a DeFi platform are visible in real time, but each user transacts under a pseudonym.[3] As such, two key features of the DeFi ecosystem are that 1) it promises user pseudonymity and 2) there are no central authorities or institutions that

* Alyssa Rose Domino is a juris doctor candidate at the Georgetown University Law Center, with expected graduation in 2023. She is a Featured Online Contributor for Volume 59 of the *American Criminal Law Review*.

1. *Decentralized Finance (DeFi)*, ETHEREUM, https://ethereum.org/en/defi/#what-is-defi (last visited Nov. 26, 2021) [hereinafter *What is DeFi?*] ("Some folks have even taken out and paid off loans with millions of dollars without the need for any personal identification").

2. *Id.* ("DeFi is a collective term for financial products and services that are accessible to anyone who can use Ethereum – anyone with an internet connection.")

3. Even when a user can anonymously create an account to transact on a DeFi network, the blockchain network itself can be viewed publicly, so it is technically pseudonymous not anonymous. DYLAN YAGA, PETER MELL, NIK ROBY & KAREN SCARFONE, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., BLOCKCHAIN TECHNOLOGY OVERVIEW (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf ("[T]he blockchain enabled users to be pseudonymous. This means that users are anonymous, but their account identifiers are not; additionally, all transactions are publicly visible."). There are ways for users to achieve heightened privacy on a DeFi platform. For example, privacy coins, which are a certain type of token that users can trade on a DeFi platform, provide heightened anonymity because they mix up pools of transactions, making them difficult to trace. *See generally* Werner Vermaak, *What Are Privacy Coins*, COINMARKETCAP, https://coinmarketcap.com/alexandria/article/what-are-privacy-coins (last visited Nov. 29, 2021).

can deny exchanges or user access to a transaction.[4] DeFi removes the middlemen from transactions, allowing any individual to exchange with any other individual anywhere in the world.[5]

DeFi countervails widespread trends toward a data-centric economy. In traditional finance where banks are the intermediaries, customers must provide personal data before opening an account or applying for a loan.[6] Even beyond the banks, personal information is widely available.[7] That information may dictate other aspects of a person's economic reality, such as their performance on an employment screening test,[8] how much they pay for a seat on an airplane,[9] and the types of products advertised to them on their social media platform of choice.[10] While our data drives an increasingly large amount of our

4. *What is DeFi?*, *supra* note 1.

5. *DeFi: A Comprehensive Guide to Decentralized Finance*, COIN TELEGRAPH, https://cointelegraph.com/defi-101/defi-a-comprehensive-guide-to-decentralized-finance (last visited Nov. 27, 2021) [hereinafter *Guide to DeFi*].

6. Banks typically require two forms of government-issued identification, proof of address, and an opening deposit. Richie Bernardo, *How to Open a Checking Account: Step-by-Step Guide, Tips & More*, WALLETHUB (Feb. 15, 2015), https://wallethub.com/edu/ca/how-to-open-a-checking-account/10299.

7. FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (stating that most companies keep user personal information such as names, social security numbers, credit card numbers and other account data on file in order to meet payroll and engage in other business needs).

8. Employment screening companies extend this information by collecting, monetizing, and providing personal information such as credit history, public records from civil court proceedings, employment history, and former arrests to fuel employer background checks. CONSUMER FIN. PROT. BUREAU, MARKET SNAPSHOT: BACKGROUND SCREENING REPORTS 2 (2019), https://files.consumerfinance.gov/f/documents/201909_cfpb_market-snapshot-background-screening_report.pdf. To do this, screening companies use web-scraping technology or purchase datasets complete with consumer information—often including name and date of birth—from sources such as law enforcement agencies, courts, or corrections offices. Brief for Nat'l Consumer L. Ctr. et al. as Amici Curiae Supporting Petitioner-Appellant at 11, Henderson v. Source for Pub. Data, No. 21-1678 (4th Cir. Oct. 15, 2021).

9. Alexander Luttman, *Evidence of Directional Price Discrimination in the U.S. Airline Industry*, 62 INT'L J. OF INDUST. ORG. 291, 291 (2019).

10. Advertisers paid approximately $84 billion in 2020 to display their ads to specific sets of Facebook and Instagram users that Facebook had grouped together by mining the personal data of its users. First Amended Complaint at 15, Fed. Trade Comm'n v. Facebook, Inc., No. 1:20-cv-03590-JEB (D.D.C. Aug. 19, 2021).

personal and collective economic activity—contributing to discrimination[11] and information silos[12]—pseudonymous DeFi transactions make it harder to discriminate against certain users on DeFi platforms. But this comes at a potentially high cost. When anyone in the world can invest and exchange on DeFi platforms, the networks become vulnerable to malicious actors ranging from attackers who short currency[13] to terrorist groups that use DeFi for crowdfunding and idea proliferation.[14] This demands tighter regulation of DeFi and strategies for patrol and prosecution of national security threats enabled through these networks.

This Essay argues that while there are many advantages to the extensive adoption of the DeFi ecosystem, it is necessary to consider national security threats that arise as people around the world increasingly transact on this market. The existence of DeFi threatens national security because bad actors can illicitly finance weapon sales and use the identity-free globalized network to expand their influence. While certain elements of DeFi improve law enforcement's ability to track, predict and prepare for attacks, other elements of the digitized financial system help bad actors evade detection by law enforcement domestically and internationally. Part I of this essay will provide a brief introduction to decentralized finance. Part II will demonstrate the relationship between DeFi and U.S. national security interests. Part III will discuss the strategies to mitigate national security risks that accompany DeFi, with an emphasis on how access to, and accountability over, personally identifiable information shapes threats

11. *See* Valeria Schneider, *Locked Out By Big Data: How Big Data, Algorithms and Machine Learning May Undermine Housing Justice*, 52 COLUM. HUM. RTS. L. REV. 251 (2021); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* 81 PROC. OF MACH. LEARNING RSCH. 1 (2018).

12. *See* Muhammad Ali, Piotr Sapiezynski, Aleksandra Korolova, Alan Mislove & Aaron Rieke, Ad Delivery Algorithms: The Hidden Arbitrators of Political Messaging 1 (Dec. 17, 2019) (unpublished manuscript), https://arxiv.org/abs/1912.04255.

13. William M. Peaster, *Inside This Weekend's DeFi Attack: How a Bad Actor Launched a Money Lego Assault*, BLOCKONOMI (Feb. 18, 2020), https://blockonomi.com/inside-this-weekends-defi-attack/.

14. Arun Iyer, *Preparing for Future Acts of Terrorism: Non-kinetic Acts and Decentralization*, THE ATL. COUNCIL (Sept. 7, 2021), https://www.atlanticcouncil.org/commentary/article/preparing-for-future-concepts-in-terrorism-non-kinetic-acts-and-decentralization/.

of criminal activity.

PART I: AN INTRODUCTION TO DECENTRALIZED FINANCE

A. How Does DeFi Work?

Users of a DeFi system begin by purchasing digital currency that grows in value (like a stock) as other investors buy it. Users can then 1) step back and let their digital currency grow, 2) cash out, 3) move their investment to a different currency, or 4) use their growing money as collateral against a loan on another investment. These are all activities that traditionally require mediation through a bank. However, on a decentralized platform there is no bank—no middleman—in any financial transaction.[15] In fact, "decentralization" in the context of DeFi means exactly this: there is no centralized institution that facilitates investments a person makes in a digital token or trades a person makes with another individual. Instead, these trades are automated.[16]

A DeFi system has several components: 1) a decentralized infrastructure; 2) money; and 3) decentralized applications (DApps).[17] The decentralized infrastructure operates like a marketplace; the digital

15. *Guide to DeFi*, *supra* note 5 ("Instead of using an intermediary such as a bank to borrow capital, you would send amounts of a specific cryptocurrency to a secure digital location—a smart contract—as collateral for your loan, receiving a different asset in return. Your collateral assets would then sit locked up until you send back the loan amount.").

16. *Id.* While this definition of "decentralized" is generally agreed upon, there is debate about how to measure the degree of decentralization of any given DeFi market. One generally accepted metric used to measure the degree of decentralization of a DeFi market is the Nakamoto coefficient. Packy McCormick, *Solana Summer*, NOT BORING (Aug. 23, 2021), https://www.notboring.co/p/solana-summer. Coined by Balaji Srinivasan, the Nakamoto coefficient is a quantitative measure of a system's decentralization that determines how many entities of a decentralized system one would need to compromise to control each essential subsystem of a decentralized system, thereby controlling the system. According to this theory, the higher the minimum Nakamoto coefficient is, the more mathematically decentralized the system. Balaji S. Srinivasan, *Quantifying Decentralization*, EARN.COM (July 27, 2017), https://news.earn.com/quantifying-decentralization-e39db233c28e. Other metrics for decentralization factor in variables like barriers to entry for new users to reach different conclusions regarding the degree of decentralization of a DeFi marketplace. McCormick, *supra*.

17. *Guide to DeFi*, *supra* note 5.

currency that moves through that marketplace is like the money that changes hands in a real-world marketplace; and the DApps are like produce, cheese, and pickle stands at the marketplace where buyers and sellers interact.

1. Decentralized Infrastructure

A DeFi infrastructure (the marketplace) eliminates institutions using smart contracts: automatically executing contracts that allow a transaction to remain exclusively between the buyer and seller.[18] Smart contracts are executable "if-then" statements that automatically go live once the agreed-upon conditions are met.[19] For example, if Party A agrees to sell 100 digital tokens of Bitcoin[20] to Party B once one Bitcoin token is worth 10 digital Ether tokens[21], then the exchange will automatically occur once this condition is met. In other words, the exchange will occur when one Bitcoin is worth 10 Ether.

All exchanges on a DeFi infrastructure platform occur through smart contracts.[22] The primary and currently most well-known DeFi infrastructure platform is Ethereum.[23] The purported chief competitor of Ethereum is Solana.[24] Referring back to the "marketplace" analogy,

---

18. Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia 10–11 (Mar. 20, 2015) (unpublished manuscript), https://ssrn.com/abstract=2580664 (defining smart contracts as "digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention"). For a history of smart contracts, *see* Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 320–24 (2017).

19. Wright & De Filippi, *supra* note 18, at 11.

20. Bitcoin is a digital currency described *infra* Section I.A.2; *see also* Kate Ashford & Benjamin Curry, *What is Bitcoin and How Does it Work?* FORBES ADVISOR (Oct. 26, 2021), https://www.forbes.com/advisor/investing/what-is-bitcoin/.

21. Ether, like Bitcoin, is a digital currency as described *infra* Section I.A.2; *see also* Jake Frankenfield, *What is Ether (ETH)?*, INVESTOPEDIA (Aug. 24, 2021), https://www.investopedia.com/terms/e/ether-cryptocurrency.asp.

22. *Guide to DeFi*, *supra* note 5.

23. *Id.* ("The smart contract platform Ethereum is the top blockchain facilitating decentralized marketplaces, but many others exist that allow users to trade or exchange specific assets, such as nonfungible tokens.")

24. Joanna Ossinger, *Ethereum Rival Solana Climbs to Seventh in Crypto Top 10*, BLOOMBERG (Sept. 6, 2021), https://www.bloomberg.com/news/articles/2021-09-06/token-of-ethereum-rival-solana-jumps-to-seventh-in-crypto-top-10.

Ethereum and Solana operate as digital marketplaces.[25]

2. Decentralized Currency

The second element of the DeFi ecosystem is the money that moves through it. There are many forms of DeFi currency on the market today, but two particularly well-known digital currencies are Bitcoin and Ether.[26] Decentralized currency is generally divisible into two categories: Stablecoins, which are pegged to government-issued currencies such as the U.S. dollar, and cryptocurrencies, which are not pegged to government-issued currencies but are used as collateral in DeFi transactions.[27] In other words, the value of a Stablecoin currency is fixed to the value of a paper currency like the U.S. dollar. [28] The value of a cryptocurrency depends upon the value of other cryptocurrencies in the digital marketplace.[29]

3. Decentralized Applications (DApps)

The final component of a DeFi ecosystem is the DApp, the proverbial produce stands that populate an analogical DeFi marketplace. In traditional finance, when a user invests money, withdraws money, or makes a trade, they must interface with a bank, a broker, or some other centralized institution. In a DeFi system, DApps replace these institutions, but they are built and operate differently from traditional exchange infrastructure. DApps often include no exchange operators, identity verification, or transaction fee.[30] DApps are created

25. *Id.* (comparing Bitcoin, the digital currency, to DeFi, the digital marketplace: "At its core, Bitcoin carries qualities touted as pillars of decentralization. DeFi, however, expands on those qualities, adding additional capabilities.").
26. *See* Top DeFi Tokens by Market Capitalization, COIN MARKET CAP (last visited Nov. 1, 2021), https://coinmarketcap.com/view/defi/.
27. *Guide to DeFi*, *supra* note 5.
28. *Id.* Notably, Stablecoins are *fixed to* but not *backed by* USD reserves. Instead, they are backed by crypto collaterals that can be viewed publicly on the Ethereum blockchain. These currencies are overcollateralized so that, even if they are backed by a more volatile cryptocurrency, they will likely stay at 100% value or more if the price of the cryptocurrency plummets.
29. *Guide to DeFi*, *supra* note 5.
30. David Johnston (DavidJohnstonCEO), Sam Onat Yilmaz, Jeremy Kandah, Nikos Bentenitis, Farzad Hashemi, Ron Gross, Shawn Wilkinson & Steven Mason, *The*

by users of a DeFi marketplace and are usually open-source, which means they are open to being edited by other users of the marketplace.[31] The data and records that detail how the DApp works are stored on a public, decentralized blockchain.[32] A blockchain is the database of every transaction that occurs in a cryptocurrency system, and a public blockchain is when one of these databases is available for anyone to see.[33] A DApp enables users to exchange digital currency, and it must generate currency according to an algorithm that proves its value.[34] Using a DApp, you can lend cryptocurrency out and earn interest without a housed institution.[35] The service automatically links buyers to sellers. A similar structure exists for insurance: the services connect people who are willing to pay for insurance with those who offer it.

B. Notable Elements and Implications of DeFi

Two features of DeFi are worth underscoring. First, users are pseudonymous, which means that transactions occur under pseudonyms[36] and often, users do not have to submit any personally identifiable information to begin transacting on a DeFi marketplace.[37] Second, the blockchain is public, which means anyone can view transactions occurring between parties on the network at any time.[38]

This decentralized environment for high-speed, global, pseudonymous transactions presents a challenge for the government on both a prosecutorial and regulatory level. If a user participates in an illegal transaction on a DeFi system, is that individual implicitly

---

General Theory of Decentralized Applications, Dapps, GITHUB, (Nov. 12, 2020), https://github.com/DavidJohnstonCEO/DecentralizedApplications [hereinafter *Theory of Dapps*].

31. *Id.*

32. *Id.*

33. Luke Conway, *Blockchain Explained*, INVESTOPEDIA, (Nov. 4, 2021), https://www.investopedia.com/terms/b/blockchain.asp.

34. *Theory of Dapps*, *supra* note 30.

35. *What is DeFi?*, *supra* note 1.

36. *Id.*

37. *Id.*

38. Anna Daily, Matthew Hanson, Katherine Kirkpatrick & Thomas Spiegler, *Decentralized Finance—Risks, Regulation, and the Road Ahead*, JD SUPRA, (Sept. 1, 2021), https://www.jdsupra.com/legalnews/decentralized-finance-risks-regulation-9351911/.

protected from records and monitoring?[39] How will regulatory inconsistencies on a global scale affect traceability of malicious activity?[40] Are the hosts of either the platform interface or the DApps built on top of it liable for the activity occurring on the interface?[41] If so, how do regulators or prosecutors identify those hosts, especially hosts of the DApps? These questions are pressing when it comes to matters of national security. A pseudonymous, decentralized environment like DeFi could provide a place for proliferation of funds and ideas by and for terrorist and hate groups that would be sanctioned in a more centralized setting.

PART II: DECENTRALIZED FINANCE AS A PLATFORM FOR CRIMINAL ACTIVITY AND A THREAT TO NATIONAL SECURITY

In 2019, criminal activity represented 2.1% of all cryptocurrency transactions, amounting to about $21.4 billion of transfers.[42] In 2020, this number fell to $10 billion—0.34%—of transaction volume as overall economic activity nearly tripled.[43] While criminal activity is shrinking as the platforms become more mainstream, crypto and more specifically DeFi has served as a platform for criminal activity and could potential be a threat to national security. DeFi markets are new, so national security concerns arising from these platforms have not yet come to light. However, given the identity-free, decentralized nature of the global marketplace, it could serve as a

39. Fabian Schar, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, ECON. RSCH. DIV. OF THE FED. RSRV. BANK OF ST. LOUIS, (Feb. 5, 2021), https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets.

40. Iyer, *supra* note 14.

41. Schar, *supra* note 39 ("If the keyholders do not create or store their keys securely, malicious third parties could get their hands on these keys and compromise the smart contract. Alternatively, the core team members themselves may be malicious or corrupted by significant monetary incentives.").

42. Tanzeel Akhtar, *Criminal Activity in Crypto Transactions Fell Sharply in 2020, Says Chainalysis*, COINDESK, (Sept. 14, 2021), https://www.coindesk.com/markets/2021/01/19/criminal-activity-in-crypto-transactions-fell-sharply-in-2020-says-chainalysis/ [hereinafter *Criminal Activity in Crypto*].

43. *Id.*

breeding ground for fraud, crowdfunding, and idea-spreading for non-state illicit actors, and a marketplace for the purchase and sale of illegal weapons where the transactors remain nameless.

A recent SEC enforcement action illustrates how DeFi is a platform where criminal activity that was common in traditional finance can also proliferate. In August 2021, the SEC charged cofounders of Blockchain Credit Partners for unregistered sales of securities in excess of $30 million.[44] The partners lied to investors about the status of their digital currency investments and used smart contracts to sell digital tokens and misrepresent company operations to their clients, falsely claiming successful business dealings and profits.[45] This was an instance of individuals acting as custodians to investor clients in the way that a stock broker acts as a custodian to an individual investing in the market. This shows that opportunities for fraud that were more common in traditional finance are possible on the DeFi network as well. However, as was seen in this case, criminal activity will likely be quickly prosecuted in DeFi and will occur where that traditional model is transposed.[46]

Ransomware attacks using crypto-currency were up 344% from 2019 to 2020.[47] The recent ransomware attack on Georgia-based petroleum pipeline, Colonial Pipeline, shows how bad actors could use non-traditional finance to demand ransom in remote infrastructure

---

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

45. *Id.*

46. An early major attack on DeFi was a 2016 $50 million hack of a fund called the DAO, or Decentralized Autonomous Organization, that ran on Ethereum. Klint Finley, *A $50 Million Hack Just Showed That the DAO Was All Too Human*, WIRED, (June 18, 2016), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/. Partially in response to the hack, the SEC released the DAO Report a year later, which provided that the DAO was made up of securities that were subject to the federal securities laws. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81,207, 2017 WL 7184670 (July 25, 2017). The hack illustrates early risks and growing pains associated with DeFi, and the DAO Report provides an example of early guidance that became a basis for enforcement action in this space.

47. *Schemes and Subversion: How Bad Actors and Foreign Governments Undermine and Evade Sanctions Regimes: Virtual Hearing Before the Subcomm. on Nat'l Sec., Int'l Dev. and Monetary Pol'y of the Comm. on Fin. Servs.*, 117th Cong. 103 (2021) [hereinafter *Schemes and Subversion*].

attacks that threaten national security. Colonial Pipeline, which is a major fuel supplier to the East Coast of the United States, withstood a ransomware attack that the Department of Justice has since attributed to the criminal hacker group, DarkSide.[48] DarkSide used malware to lock Colonial out of its systems until the ransom of 75 Bitcoins, worth about $4.4 million, was paid.[49] The disruption created gas shortages and a spike in gas prices across the United States.[50] The FBI was able to trace the money and retrieve about half the funds Colonial paid, but because DarkSide supplies its ransomware services to its partners, it has been difficult to identify "the real threat actor behind the attack on Colonial, who can be any one of the partners of DarkSide."[51]

Though it was a crypto-based—not DeFi based—attack, this situation illustrates how cybercriminals could use DeFi to rapidly hamstring U.S. infrastructure and limit the government's ability to retrieve ransom funds or prosecute the offenders. Institutions that are central to the U.S. economy, such as the Federal Reserve, are not immune to such an attack, especially in light of the Fedwire system briefly shutting down in early 2021.[52] The Colonial Pipeline hack simultaneously illustrates both risks associated with centralized data and information as a target for bad actors[53] as well as risks associated with a decentralized network that enables the attack to be entirely remote, provides for extraordinarily rapid movement of money, and can make the routing of funds especially hard to trace to an end user.

DeFi also presents new avenue for terrorist organizations to evade sanctions.[54] Fifteen percent of all ransomware payments made in 2020 carried a risk of sanctions violations.[55] While many cryptocurrency transactions are intermediated by an exchange with

48. Sara Morrison, *How a Major Oil Pipeline Got Held for Ransom*, RECODE (June 8, 2021), https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.
49. *Id.*
50. *Id.*
51. *Id.*
52. *Digitizing the Dollar: Investigating the Technological Infrastructure, Privacy, and Financial Inclusion Implications of Central Bank Digital Currencies: Virtual Hearing Before the Task Force on Fin. Tech. of the Comm. on Fin. Servs.*, 117th Cong. 20 (2021).
53. *Id.*
54. *Schemes and Subversion*, *supra* note 47, at 12.
55. *Id.* at 103.

compliance obligations that often include ensuring that the transacting parties are not sanctioned persons, decentralized finance does not rely on these intermediaries.[56] This can make it challenging for both law enforcement and other users on a DeFi network to determine whether a party to a one-to-one transaction is a sanctioned individual.[57]

The pseudonymous and decentralized nature of the global DeFi marketplace make it susceptible to abuse by fraudsters and terrorist groups that seek avenues for crowdfunding, weapons sales, and the spread of ideas. Regulation of this space must target accountability and security of the DeFi system without stifling the innovation that makes the space attractive to investors in the first place.[58]

PART III. STRATEGIES TO MITIGATE RISKS THROUGH REGULATION AND LITIGATION

In order to mitigate national security threats that arise in a DeFi setting, it is necessary to identify avenues for accessing user and host information. This Essay identifies two. One avenue is through user-centric data collection using anti-money laundering[59] and "know your customer" (KYC) protocols.[60] The second is through network-centric data analysis on the public blockchain.[61] Anti-money laundering regulations help provide access to user information on an as-needed basis, and the public nature of the blockchain enables access to network

56. *Id.* at 66.
57. *Id.*
58. *Id.* at 107.
59. Peter Cramer & Seetha Ramachandran, *Treasury Department Steps Up Its Counter-Ransomware Efforts and Simultaneously Issues New Sanctions Compliance Guidance for Virtual Currency Industry*, JD SUPRA, (Oct. 28, 2021), https://www.jdsupra.com/legalnews/treasury-department-steps-up-its-6052008/ ("In the new Guidance, OFAC noted that the virtual currency industry, which includes technology companies, exchanges, miners, wallet providers, service providers and users, plays an increasingly critical role in preventing sanctioned persons from using virtual currencies to evade sanctions and harm national security, and that OFAC sanctions apply equally to entities in the virtual currency industry and traditional financial institutions.").
60. For introductory information on "know your customer" compliance requirements, *see* James Chen, *Know Your Client (KYC)*, INVESTOPEDIA, (Apr. 17, 2021), https://www.investopedia.com/terms/k/knowyourclient.asp.
61. Daily et al., *supra* note 38.

data. When analyzed together, the network remains decentralized, but it becomes less anonymous, and both the hosts and the users can be held to a greater degree of accountability.

A. Anti-money Laundering Regulations

On May 11, 2016, the Financial Crimes Enforcement Network ("FinCEN"), a bureau of the U.S. Department of Treasury, issued a rule called Customer Due Diligence Requirements for Financial Institutions.[62] The rule "aims to improve financial transparency and prevent criminals and terrorists from misusing companies to disguise their illicit activities and launder their ill-gotten gains."[63] This rule outlines what is colloquially known in banking and legal compliance communities as "know your customer" or "KYC" requirements for banks and like institutions.[64] The institutions periodically request and verify personally identifiable information (PII) from their customers to ensure that they—as the name would have it—know their customers. By keeping this file of information, the institutions can cut criminal actors out of banking networks or, at the very least, speed up the process of tracking illicit activity a customer engages in.[65]

On August 10, 2021, the Senate passed an infrastructure bill that included a provision imposing reporting requirements on cryptocurrency "brokers."[66] According to this legislation, a broker includes "any person who (for consideration) is responsible for regularly providing any service effectuating transfers of digital assets on behalf of another person."[67] This legislation means that anyone who launches a DApp is a "broker" subject to reporting requirements regarding the movement digital currency that passes through the digital application. However, because currency and data on the blockchain is aggregated at each block,[68] this information is difficult to collect in

62. Treas. Reg. § 29397 (2016).
63 *Information on Complying with the Customer Due Diligence (CDD) Final Rule*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule (last visited October 8, 2021).
64. *Id.*
65. *Id.*
66. H.R. 3684, 117th Cong. § 80603 (2021).
67. *Id.*
68. Conway, *supra* note 33.

some cases and impossible in others. Low-level "brokers" who are unable to identify their users are left with a choice of not complying with the requirement or exiting the market.[69]

This legislation did not arise in a vacuum. In October 2021, the Financial Action Task Force (FATF), an intergovernmental organization developed by the G7 to combat money laundering and terrorism financing, published compliance standards for virtual assets and virtual asset service providers (VASPs).[70] FATF recently released updated guidance for virtual asset compliance to ensure that DeFi "owners and operators" are subject to KYC requirements under anti-money laundering and terrorism financing regulatory regimes.[71] FATF members including the United States are expected to implement policies consistent with the new regulations.[72] As illustrated by the infrastructure bill, however, overly broad definitions of the terms "owners and operators" can make these regulatory schemes inoperable.

Perhaps a superior method for routinizing KYC in the DeFi space is to make DeFi platforms subject to the Bank Secrecy Act,[73] which "requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities."[74] This would ensure that fewer low-level brokers are subject to providing information on users that they do not have access to. It would also provide guideline KYC requirements for public companies and regulated institutions that want to enter the market but do not want to subject themselves to retroactive regulatory blowback. [75] In addition

---

69. David Z. Morris, *DeFi Feels Like Nothing Regulators Have Seen Before. How Should They Tackle It?*, COINDESK, (Oct. 19, 2021), https://www.coindesk.com/policy/2021/10/19/defi-is-like-nothing-regulators-have-seen-before-how-should-they-tackle-it/ (stating that regulation of DeFi would make the technology more accessible to many more participants).

70. FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH: VIRTUAL ASSETS AND VIRTUAL ASSET SERVICES PROVIDERS (2019), https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

71. *Schemes and Subversion*, *supra* note 47, at 107.

72. *Id.*

73. *Id.*

74. *FinCEN's Mandate from Congress*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-regulations (last visited Nov. 25, 2021).

75. Morris, *supra* note 69.

to DApps, DeFi platforms want clearer regulations. DeFi platform Swarm Markets left the ambiguously regulated U.S. market in 2019 and relocated to the German market, where the firm regulations give the platform firm grounds for growth with guarantees for self-custody, decentralized liquidity provisions and transparency.[76] Subjecting DeFi platforms to the Bank Secrecy Act could provide guidance to large-scale brokers without subjecting small-scale brokers to requirements that they lack the resources to comply with.

One challenge with trying to superimpose traditional KYC mechanisms onto DeFi is that, in traditional KYC, the institution is the link between the regulatory agency and the end user.[77] When there is no institution regulating the space, which party is best suited to keep KYC and have the responsibility to report suspicious activity? Companies are cropping up to encrypt and handle this data for the users and hosts, reintroducing additional parties to transactions.[78] Innovations in KYC processes, such as zero-knowledge proofs[79] and portable KYC[80] provide avenues through which traders could remain unidentifiable until law enforcement subpoenaed their identity records.[81] There are many regulatory wrinkles to iron out, but enhanced KYC in the DeFi space can be a positive force for both mitigating the risks of national security threats and promoting industry while maintaining the privacy and speed of transaction that makes this space so attractive to investors to begin with.

---

76. *Id.*
77. *Guide to DeFi*, *supra* note 5.
78. *See e.g.,* KYC-CHAIN, *https://KYC-Chain.com* (last visited October 8, 2021).
79. Zero-knowledge proofs enable the verification of facts that are derived from a secret the verifier cannot access, offering the prospect of people transacting in confidence without accessing potentially compromising information about each other. Michael J. Casey, *Zcash's Halo Breakthrough Is a Big Deal – Not Just For Cryptocurrencies,* COINDESK, (Sept. 13, 2021), https://www.coindesk.com/markets/2019/10/14/zcashs-halo-breakthrough-is-a-big-deal-not-just-for-cryptocurrencies/.
80. Morris, *supra* note 69 ("'[P]ortable' KYC . . . could allow a clearance from one trading venue to be used on another; that could include getting cleared by a centralized exchange . . . and then using that credential elsewhere.").
81. *Id.*

B. Public Blockchain

In the DeFi system, both smart contracts and the blockchain—the network of smart contract transactions—are public.[82] This means that anyone can audit the network at any time. As a result, contracts that have been infected by a bug or are hacked by a third party quickly come under scrutiny.[83] While the public blockchain reveals information about the health of the contract, it does not reveal information about the parties to the contract or what the funds are supporting, for example crowd funding or arms exchanges. It provides access to information in the aggregate and on a pseudonymous basis only. While this structure helps users maintain privacy in direct transactions, it also provides a shield for illicit actors to raise money and transact.[84]

Together with KYC protocols, however, public blockchain can increase the security of a financial transaction. If the public can analyze the contract and network, and the host collects and verifies user PII, suspicious activity can be spotted on a network level and verified and prosecuted using the KYC. There are gaps in this system. Certain types of criminal activity will not raise a flag on the public blockchain because, from node to node, nothing looks amiss.[85] There are also ethical questions about trusting interface hosts with user data and further issues about allowing them to share this information upon request with the U.S. government and other state actors. There are also advantages to it. The public network allows users, hosts, and watchdogs alike to reduce fraud in this space at an unparalleled rate. The same is true of

82. *Guide to DeFi*, *supra* note 5.
83. Wright & De Filippi, *supra* note 18, at 2. ("The blockchain is a distributed, shared, encrypted-database that serves as an irreversible and incorruptible public repository of information.")
84. *Id.* at 23. ("[Block-chain based] anonymous communication channels—combined with decentralized (autonomous) organizations—could increase the ability of bad actors to effectuate harm. With communication networks that are harder to crack and the possibility of coordinating through the use of decentralized organizations, crime may be easier to plan and execute and an entirely new chapter of cyberwarfare and cybercrime may emerge.")
85. *Schemes and Subversion*, *supra* note 47, at 66. ("DeFi may pose risks that sanctioned parties are able to transact and receive items of value without their counterparties knowing that they are sanctioned or even being aware that they may be prohibited from transacting with such persons.")

hacks. DeFi is unique in that it enables preservation of privacy even in the process of rooting out fraudulent activity, reframing the concept of "fraud" altogether.

Notably, KYC does not operate perfectly in traditional finance.[86] But when combined with the efficiencies and automation of crypto, KYC and the public blockchain provide greater access to user and network information and can go further than even traditional KYC too help protect against fraud and illicit movement of money.

CONCLUSION

An intentional increase of data collected from individuals who use DeFi and increased analysis of the blockchain has a strong potential to support U.S. national security interests. In August 2021, SEC Chair Gary Gensler spoke to the Aspen Security Forum about cryptocurrency, underscoring that, if DeFi platforms offer securities, they must register with the SEC unless they meet an exemption.[87]

---

86. *Id.* at 141 ("Despite the banks' sweeping powers to investigate account holders, the FinCEN Files investigation reveals that major financial institutions often fail to perform the most basic checks on their customers, such as verifying where a business is located when someone opens a new account. The lapses allow criminal groups to hide behind shell corporations, registered with no identifying details about their ownership, and slide the proceeds of their crimes into the global financial system.").

87. *The Distributed Ledger: Blockchain, Digital Assets and Smart Contracts: SEC Chairman Makes Remarks Before the Aspen Security Forum and to the Wall Street Journal*, SKADDEN ARPS, SLATE, MEAGHER & FLOM LLP (Aug. 2021), https://www.skadden.com/en/insights/publications/2021/08/the-distributed-ledger. Three cases have generally been used to inform SEC decisions regarding when an investment is a security or exchange: *SEC v. W.J. Howey Co., Landreth Timber Co. v. Landreth,* and *Reves v. Ernst & Young.* In 1946, *SEC v. Howey* addressed the question of whether, under the Securities Act of 1933, a contract is a security when it involves the investment of collective money for a profit based on the acts of others. *SEC v. Howey,* 328 U.S. 293 (1946). The opinion defined an investment contract as any "contract, transaction, or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party . . . ." *Id.* It held that the purchase contract that Howey offered was a security because the purchasers of Howey's product were only interested in obtaining profits solely from the efforts of Howey company. Applying *Howey* to DeFi means applying the following test to actors on the chain: is there 1) an investment of money; 2) in a common enterprise; 3) with an expectation of profits; 4) which are derived solely from the efforts of the promoters or third parties? Nathan Reiff, *Howey Test*, INVESTOPEDIA, (July 05, 2021), Investopedia.com/terms/h/howey-test.asp. In *Landreth Timber Co. v.*

Chair Gensler's remarks illustrate several trends occurring in regulation of DeFi. One is that many agencies are weighing in on how this space should be regulated to mitigate criminal activity on DeFi platforms, particularly activity that threatens national security.[88] Another is that the more decentralized the network, the more difficulty the government faces regulating of that network.[89] This reality increases the risk that innocent actors will be regulated while bad actors, including those plotting ransomware schemes and evading sanctions, will move to more decentralized DeFi platforms to avoid detection. Widespread KYC requirements and blockchain analysis can help mitigate this risk, ensuring that there is a floor for user data collection that can be retrieved on an as-needed basis. With purposeful regulation, DeFi could be a place for privacy, security, and innovation. Until that purposeful regulation is developed and adopted, however, users and private companies must remain alert to possible criminal activity—and law enforcement must remain alert to national security threats—on DeFi platforms.

Landreth, the Court distinguished Landreth from Howey, finding that a stock is always a security, and the *Howey* test need not to be applied to evaluate a stock. *Landreth Timber Co. v. Landreth*, 471 U.S. 681 (1985). Therefore, when a business is sold by the sale of equity in that business, it is a security, and therefore the exchange must comply with registration requirements under the Exchange Act and Securities Act. Finally, in *Reves v. Ernst & Young,* the Court held that the co-op note at issue was a security, and that a note will be considered a security if investors in the note seek a profit from it, the note can be used to trade for investment, the public expects the note to be a security and the Securities Acts will meaningfully reduce the risk associated with the note. *Reves v. Ernst & Young*, 494 U.S. 56 (1990).

88. For an illustration of historical fragmentation of financial regulation by the federal government, *see* U.S. GOV'T ACCOUNTABILITY OFF., GAO-08-751, FINANCIAL REGULATION: COMPLEX AND FRAGMENTED STRUCTURE COULD BE STREAMLINED TO IMPROVE EFFECTIVENESS (2016).

89. *What is DeFi?*, *supra* note 1.