Crypto
Council for
Innovation

Key Elements of an Effective DeFi Framework

OCTOBER 5, 2023

About CCI

The Crypto Council for Innovation (CCI) is the premier global alliance advancing crypto innovation. We believe in leading with a global world view, advocating for inclusive regulation, developing actionable and evidence-based insights, working in trusted partnership with government and business stakeholders and unlocking the promise of Web3.

Table of contents

Executive Summary

Source: @Tom Chrostek/unsplash

Decentralized Finance (DeFi) is a rapidly growing but nascent industry. It utilizes blockchain technology to add functionality to the next iteration of the Internet–Web3, that empowers consumers and businesses to use financial services in a cost efficient and independent manner, and provides them with an opportunity to participate in a new financial system. If properly developed and deployed, the proliferation of DeFi will lead to greater financial inclusion, consumer participation, and market efficiencies than the legacy financial system.

At the time of writing, the total market capitalization of DeFi projects is approximately $42 billion (with an all-time high of approximately $173 billion) while total value locked (TVL) in such projects sits at approximately $38 billion (with an all-time high of approximately $178 billion). While these nominal amounts are not large when compared to total amounts in the global financial system, DeFi's exponential growth, along with its novel approach to financial services, have caught the eyes and concerns of policymakers around the globe.

The G20, the Financial Stability Board, and other international standards setters, along with central banks, regulators, and finance ministries worldwide are currently studying how DeFi works and its benefits and risks. However, DeFi is often misunderstood both as a concept and as a sector. We at the Crypto Council for Innovation (CCI) prepared this white paper to contribute to the public discourse on DeFi.

As policymakers consider regulatory approaches to DeFi and the challenges to regulating decentralized financial services that have no obvious entities in control, we put forward a regulatory approach to DeFi that mitigates financial safety and soundness concerns, and financial stability risks, while also protecting consumer end-users and fostering innovation. We outline critical elements for an effective DeFi regulatory framework that are feasible, suitable, and proportionate for regulators and DeFi innovators.

CCI's Key Elements of an Effective DeFi Framework

- **A DeFi regulatory approach should adhere to the principle: 'Same Activity, Different Risks, Different Regulation BUT Same Regulatory Outcome' (NOT 'Same Activity, Same Regulatory Outcome').** DeFi may provide services similar to those provided by traditional finance (TradFi), but the risks can be fundamentally different For example, traditional lending activities have credit and liquidity risks, while DeFi lending has novel operational and market risks. Therefore, the longstanding regulatory principle 'Same activity, Same risk, Same regulation' does not apply well where the risks are very different. A viable regulatory framework for DeFi should take these differences into account. But both TradFi and DeFi regulatory frameworks should achieve the *same regulatory outcomes*: safety and soundness of participants, financial stability, and consumer and investor protections.

- **Defining DeFi: the term 'DeFi' refers to the ecosystem of applications and protocols enabled by blockchain technology that provides digital and open access to financial services without a single intermediary or small group of intermediaries controlling the system offering the financial service.** DeFi is a subgroup of a broader category of decentralized services and products. By removing the traditional financial intermediary 'middlemen,' DeFi holds the promise of lowering access barriers to financial services, reducing bias and fees that had inhibited participation in traditional financial activities, and enhancing overall individual financial sovereignty and opportunity.

- **DeFi digital tech stacks:** at the top of the DeFi ecosystem are the end-users who use financial services applications (or 'apps') that access DeFi protocols, which in turn are built on top of base layer blockchains—all of which essentially form digital technology stacks.

- **DeFi protocols are public goods that should remain accessible to any business building financial services apps and be exempt from regulatory requirements and obligations if they possess certain features.** The base layer blockchain is a public good akin to the Internet, while DeFi protocols are reminiscent of Web1 protocols like HTTP, SMTP, and FTP. These served as public goods, enabling innovators to develop applications and businesses during the early days of the Internet (like AOL, Gmail, and MS Outlook). DeFi protocols should continue to act as public goods, and any regulatory model should acknowledge and encourage this categorization.

- **To be exempt from regulatory requirements, DeFi protocols must exhibit five features, namely: (1) decentralized, (2) open source, (3) autonomous, (4) standardized, and (5) non-discriminatory access and use, to be 'Public Good Protocols'.** DeFi protocols should be encouraged to act as public goods for the global financial ecosystem and meet certain baseline criteria to ensure they are sufficiently safe to act as digital public infrastructure that adds new functionality to the Internet.

  To foster Public Good Protocols, DeFi protocols should be encouraged to possess these critical characteristics, which would therefore exempt them from financial regulation:

  1. **Decentralized**: This paper puts forth **two critical tests** to determine a protocol's decentralized status. First, no single person or the managerial efforts of a specific or limited group of persons can (i) control or fundamentally alter a protocol's purpose or code; (ii) control user funds or assets; (iii) reverse transactions; or (iv) restrict access to the protocol. Second, a decentralized protocol must be built on a public and permissionless blockchain to help ensure the protocol's decentralized and non-discriminatory nature. For the purposes of this paper, base layer blockchains are assumed to be public and permissionless.

  2. **Open source**: The protocol's software should be open source, enabling the public to view, contribute to and learn from the protocol's technology. This avoids vendor lock-in, helps to quickly identify and fix errors, and fosters network effects through community engagement.

  3. **Autonomous**: The protocol's smart contracts should be self-executing, meaning the rules and actions are predetermined. The autonomous nature of the protocol's smart contracts ensures the protocol's credible neutrality (i.e., that the protocol will not discriminate against individuals or types of transactions).

  4. **Standardized**: Protocols should use existing technical standards and/or take steps to maximize their potential composability and interoperability.

  5. **Non-discriminatory access and use**: Protocols should allow users to freely access and use the system as a form of public good. As mentioned under the 'decentralized' characteristic above, protocols should be built on public, unbiased and non-discriminatory blockchains (i.e., permissionless).

Benefits of Public Good Protocols

- **Financial applications built on Public Good Protocols can leverage the open, neutral, and decentralized nature of the protocol technology to offer new and low-cost financial services that will form a critical part of the next iteration of the Internet (i.e., Web3)**—one that mitigates many of the risks in the TradFi system through increased transparency, innovative forms of governance, and enhanced security.

  We outline some of DeFi's benefits in this paper, including:

  1. **Reducing counterparty risks.** The intra-transaction composability of smart contracts allows multiple actions to be executed within a single transaction. This feature reduces the reliance and trust needed for numerous parties to effectively facilitate custody, escrow, clearing, and settlement. In addition, the self-custodial nature of Public Good Protocols empowers the end-user to utilize a broader set of customizable services through programmable smart contracts.

  2. **Improving financial inclusion and access.** Historically, marginalized communities have faced various forms of exclusion from the traditional financial system, limiting their access to basic financial services and opportunities to grow wealth. DeFi's inherent qualities, such as unbiased permissionlessness, composability, and self-custody, also support greater access to financial services while reducing rent-seeking intermediaries. DeFi can also help promote growth and efficiencies in emerging markets and mitigate access challenges in disruptive regimes.

3 **Increased transparency.** The visibility of on-chain transactions also provides a rich data source for real-time risk management while reducing information asymmetries. As a consequence of this transparency and decentralization, public blockchains act as a public good in the form of financial infrastructure by providing neutral, independent, and immutable transaction records, while DeFi protocols act as another public good in the financial infrastructure by providing accessible and unbiased operations.

4 **Improving security and resilience.** DeFi has fewer points of failure relative to Centralized Finance (CeFi)/TradFi alternatives. Distribution of information reduces the likelihood of unilateral changes to the ledger by a single entity. It also reduces the likelihood of a systemic failure of the blockchain. Furthermore, self-custody eliminates counterparty risk exposure to third-party custodians.

5 **Provide participatory stakeholder governance.** DeFi protocols can allow participants to participate in the protocol's governance. For example, many decentralized protocols utilize Decentralized Autonomous Organizations (DAOs) to assist with operations and protocol improvements. They allow members to participate directly in the governance of the blockchain. Persons or parties can become members of DAOs by acquiring governance tokens of the protocol or blockchain. This vehicle provides end-users access to participate in the governance process. DAOs are also subject to the decentralization test and should not be controlled by any single member or through the managerial efforts of a small group of members.

Risks in Public Good Protocols

- DeFi activities may be similar to those in TradFi, but the risks associated with them can be fundamentally different. The decentralized design of Public Good Protocols may eliminate or significantly reduce traditional financial risks, such as counterparty, credit, and custodial risks, as well as human error, bias, and even corruption/embezzlement, while introducing other risks. Key DeFi risks are often operational, relating to flaws in the design, governance, or interconnections in the decentralized system. Some of these key risks fall into the following categories:

1 **Illicit finance/anti-money laundering (AML) risks.** Illicit actors have been found to use DeFi services for purposes of money laundering and transferring illicit proceeds. However, the visibility of DeFi transactions enables public tracking of on-chain activity, helping financial authorities to investigate and mitigate laundering. *Note: this paper does not explore in-depth how illicit finance regulation should be applied to DeFi. CCI plans to explore illicit finance regulation of DeFi in a companion paper in coming months.*

2 **Flawed DAO governance risks.** Many DAOs suffer from a lack of active participation by all of their members, leading to an uneven distribution of participation. This concentration of voting participation in active but smaller groups of token holders could lead to protocol governance being concentrated in the hands of a few parties. In turn, these few parties could attempt to benefit at the expense of other DAO members. Much of this uncertainty and risk could potentially be mitigated through regulatory standards regarding decentralized governance.

3 **Cybersecurity risks, including smart contracts and oracle vulnerabilities.** While discussion of DeFi cybersecurity risks typically focuses on the resiliency of the underlying blockchain, cybercriminals are more likely to exploit the protocol's smart contract vulnerabilities. However, the majority of smart contract hacks have been hacks of cross-chain bridges, which are often controlled by a single or small group of parties.

For DeFi protocols, there are three main types of smart contract vulnerabilities: (i) initiating a flash loan to exploit a smart contract vulnerability, allowing them to drain funds within the bounds of the smart contract; (ii) exploiting token bridge signature requirements to steal investment funds, and (iii) taking advantage of a platform's reliance on a single oracle by conducting leveraged trading to manipulate pricing and exploit pricing errors. Code audits, bounty programs, and decentralized oracles can help mitigate these risks. We also recommend public-private information sharing and analysis centers.

4. **Underlying base layer blockchains risks.** DeFi protocols are exposed to risks posed by their underlying blockchains, including validator-related risks. For instance, due to the high transparency of Ethereum, validators through the Proof of Stake (PoS) consensus mechanism can front-run blockchain transactions and selectively order them to their benefit (i.e., maximum extractable value (MEV)). Concentrations of power in the validation process could lead to 51% attacks or validator cartels, leading to blockchain alterations to the benefit of those in control. Depending on specific objectives, alternative consensus mechanisms to PoS, such as Delegated Proof of Stake (DPoS) and Proof of History (PoH), may alleviate the outlined risks by increasing decentralization of the consensus mechanism or bolstering the objectivity of transaction ordering.

5. **Interconnections with the traditional financial system.** As more TradFi institutions and users engage with DeFi, the interconnectedness between the two sectors will grow. Risks stemming from failures in TradFi can spill over into DeFi and vice versa. For example, stablecoins are crucial in DeFi as they provide the main form of value transfer (i.e., payment) in DeFi systems. But when Silicon Valley Bank failed earlier this year, Circle (the issuer of fiat-backed stablecoin USDC) lost access to $3.3 billion in cash reserves held at the bank, leading to a temporary dollar de-peg for one of the most important payments stablecoins used in DeFi.

DeFi Policy Recommendations

In adherence to the principle of *'Same Activity, Different Risk, Different Regulation but Same Regulatory Outcome,'* this paper proposes a specific regulatory approach: *'Regulate Businesses, Not Public Good Protocols,'*—which places regulatory obligations on the app-operating businesses.

Following this approach, we propose three policy recommendations:

1. **Mandatory Disclosure**: A standardized disclosure regime for app-operating businesses that includes information about the underlying DeFi protocol.

2. **Independent Certification**: The establishment of an Independent Certification Regime Organization (ICRO), which certifies DeFi protocols that meet the ICRO's criteria, including security code audits.

3. **Regulatory Safe Harbor**: A safe harbor regime for nascent protocols that aim to decentralize.

We believe this *'Regulate Businesses, Not Public Good Protocols'* approach prioritizes consumer and investor protection and mitigates financial risks without stifling the benefits of these innovative technologies. It provides many of the necessary economic and regulatory incentives to encourage businesses operating DeFi applications to be in compliance with the applicable laws in the jurisdictions where they are providing services and a pathway for Public Good Protocols to develop safely and decentralize through the regulatory safe harbor program. Mandatory disclosure obligations would be the responsibility of the app-operating businesses, and this disclosure regime would be enhanced by a certification regime through which the ICRO independently certifies Public Good Protocols. Importantly, this overall framework will help foster the growth, security, and resilience of Public Good Protocols to serve as the public goods infrastructure for the Web3 ecosystem of the future.

1 Introduction

Source: @maximalfocus/unsplash

Decentralized Finance (DeFi) is a rapidly growing but nascent industry. It utilizes blockchain technology to add functionality to the next iteration of the Internet–Web3, that empowers consumers and businesses to use financial services in a cost efficient and independent manner, and provides them with an opportunity to participate in a new financial system. If properly developed and deployed, the proliferation of DeFi will lead to greater financial inclusion, consumer participation, and market efficiencies than the legacy financial system. The economic principles of decentralization were popularized by the economist-philosopher Friedrich Hayek in the 20th century,[1] but have recently been introduced in the real world through 'trustless platforms' enabled by blockchain technology when Satoshi Nakamoto published the Bitcoin white paper in 2008.[2]

However, DeFi can be deeply misunderstood both as a concept and as a sector. Many so-called DeFi applications (or apps) and protocols that have failed or suffered detrimental security hacks were in fact controlled by a single party or through the managerial efforts of a small group and, therefore, were not actually decentralized.

The DeFi sector has experienced exponential growth in several metrics since its initial ascent in 2019, where its total market capitalization grew more than tenfold year-over-year.[3] Over a similar period, the total value locked (TVL)[4] in DeFi protocols increased by several multiples and reached approximately $9.4 billion by February 2020.[5] At the time of writing, the total market capitalization of DeFi projects is approximately $42 billion (with an all-time high of approximately $173 billion) while TVL in such projects sits at approximately $38 billion (with an all-time high of approximately $178 billion).[6] These dramatic increases signify not only the developmental stride of the DeFi sector, but also the substantial expansion of on-chain liquidity over time.[7] While these nominal amounts are not large compared to the global financial system, this exponential growth, along with the novel approach to financial services, have caught the eye and concern of policymakers around the globe.

Although DeFi is still in its infancy, the G20 has announced its intention to monitor DeFi in its Finance Ministers & Governors Communique from February.[8] The Financial Stability Board (FSB) issued an analytical report in February 2023,[9] and policy recommendations are expected to follow suit. After releasing its proposed recommendations

[1] Friedrich A. Hayek, *The Use of Knowledge in Society*, 35 Am. Econ. Rev. 519, 519-521 (1945) (discussing decentralized planning as the foundation of economic competition. *See also* Friedrich A. Hayek, The Road to Serfdom 43-51, 149 (Routledge 2001) (1944) (discussing the imperative of decentralization where economic factors become increasingly numerous and impossible for a single board to gain a synoptic view of).

[2] *Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), https://bitcoin.org/bitcoin.pdf.

[3] *Top 100 DeFi Coins by Market Capitalization*, Coingecko, https://www.coingecko.com/en/categories/decentralized-finance-defi (last visited Sept. 14, 2023) (demonstrating an increase in the total DeFi market capitalization from approximately $1.6 billion on September 1, 2019 to approximately $20.7 billion on September 1, 2020 for the top 100 DeFi tokens).

[4] Total value locked (TVL) is a metric that measures the aggregate value of all crypto assets locked in DeFi protocols via smart contracts. TVL may also refer to the value of assets locked on a specific protocol. To calculate TVL, one determines the value of all crypto assets currently locked into DeFi protocols including assets put up for collateral, staked assets, and assets placed into protocol liquidity pools. One then converts the value of those assets to a standard unit (such as USD) and adds the total value of all those assets to determine the TVL. This can be done for a single DeFi protocol, for a specific subset of DeFi protocols (i.e., TVL of lending protocols or TVL of Decentralized Exchanges), or for all DeFi protocols in aggregate. Here, we use the aggregate TVL of all 2,706 protocols listed on DeFi Llama. Note also that TVL denominated in USD is volatile as it changes depending on prices of crypto assets.

Cryptopedia: Total Value Locked, Gemini, https://www.gemini.com/cryptopedia/glossary#totalvaluelocked (last visited June 21, 2023). Emi Lacapra, *What Is Total Value Locked (TVL) in Crypto and Why Does It Matter?*, Cointelegraph (May 22, 2022), https://cointelegraph.com/explained/what-is-total-value-locked-tvl-in-crypto-and-why-does-it-matter.

[5] *DeFi: Overview*, Defi Lalama, https://defillama.com/ (last visited Sept. 14, 2023) (presenting both the current and historical TVL across all DeFi protocols and showing an increase in TVL from $448 million on October 1, 2019 to $9.46 billion on October 1, 2020).

[6] CoinGecko, *supra* note 3 (showing the December 2021 high in total market capitalization through to the current figure); DeFi Llama *supra* note 5 (noting the December 2021 high in TVL through to the current figure).

[7] *Id.*

[8] *Chair's Summary and Outcome Document: G20 Finance Ministers and Central Bank Governors Meeting*, Ministry of Fin. Japan 7 (Feb. 25, 2023), https://www.mof.go.jp/english/policy/international_policy/convention/g20/g20_20230225.pdf.

[9] *The Financial Stability Risks of Decentralized Finance*, Fin. Stability Bd. (Feb. 16, 2023), https://www.fsb.org/wp-content/uploads/P160223.pdf.

for crypto exchanges (i.e., CeFi) in May 2023,[10] the International Organization of Securities Commissions (IOSCO) proposed recommendations for DeFi in September 2023 and is expected to finalize them by the end of this year. Likewise, the FSB plans to conduct policy work on DeFi by the end of 2024.[11]

Regionally, the European Union, in its deliberation of crypto assets regulation (the Markets in Crypto Assets Regulation (MiCA)), decided to postpone regulating DeFi until after it first conducts a study.[12] In the US, bills have been introduced trying to carve out DeFi,[13] and regulatory proposals have been made to provide safe harbor for protocols in the process of becoming decentralized.[14] Needless to say, most major jurisdictions are examining how best to regulate DeFi or, in some cases, even to contain it.

Against this backdrop of policymaker activities from multilateral to national developments, many aspects of the DeFi ecosystem are quickly evolving and maturing. The ecosystem is dynamic, and far from monolithic. Any regulatory model will need to be forward looking and as flexible as possible to accommodate this global reality.

Traditional financial regulation has historically utilized an entities-based approach. Regulation is generally applied through licenses, charters, or registrations obtained from the relevant regulator(s). For example, parties who wish to form a new bank must obtain a bank charter from a bank supervisor. Once the charter is granted, the bank regulator has the legal authority to examine the newly formed bank and subject it to prudential regulatory requirements. This legal entities-based approach is challenging to apply in the DeFi sector, where no single party or small group of parties have control over the provision of the financial service.

We have attempted in this paper to tackle this regulatory challenge. Our objective is to help foster a healthy, sustainable DeFi ecosystem that is inclusive and open. We have carefully considered the policy and regulatory challenges and outlined an approach that we believe is viable and feasible for both regulators and the industry.

This paper is divided into four main sections. In **Section II**, we discuss the definition of DeFi and introduce the concept of DeFi protocols as public goods digital infrastructure like the Internet (‘Public Good Protocols’). This section is then followed by an outline of benefits (**Section III**) and risks (**Section IV**) of DeFi protocols. We then put forward a regulatory approach and policy recommendations in **Section V**. This paper aims to assist policymakers as they consider the very challenging question of how best to regulate DeFi as an emerging and vital part of our financial system.

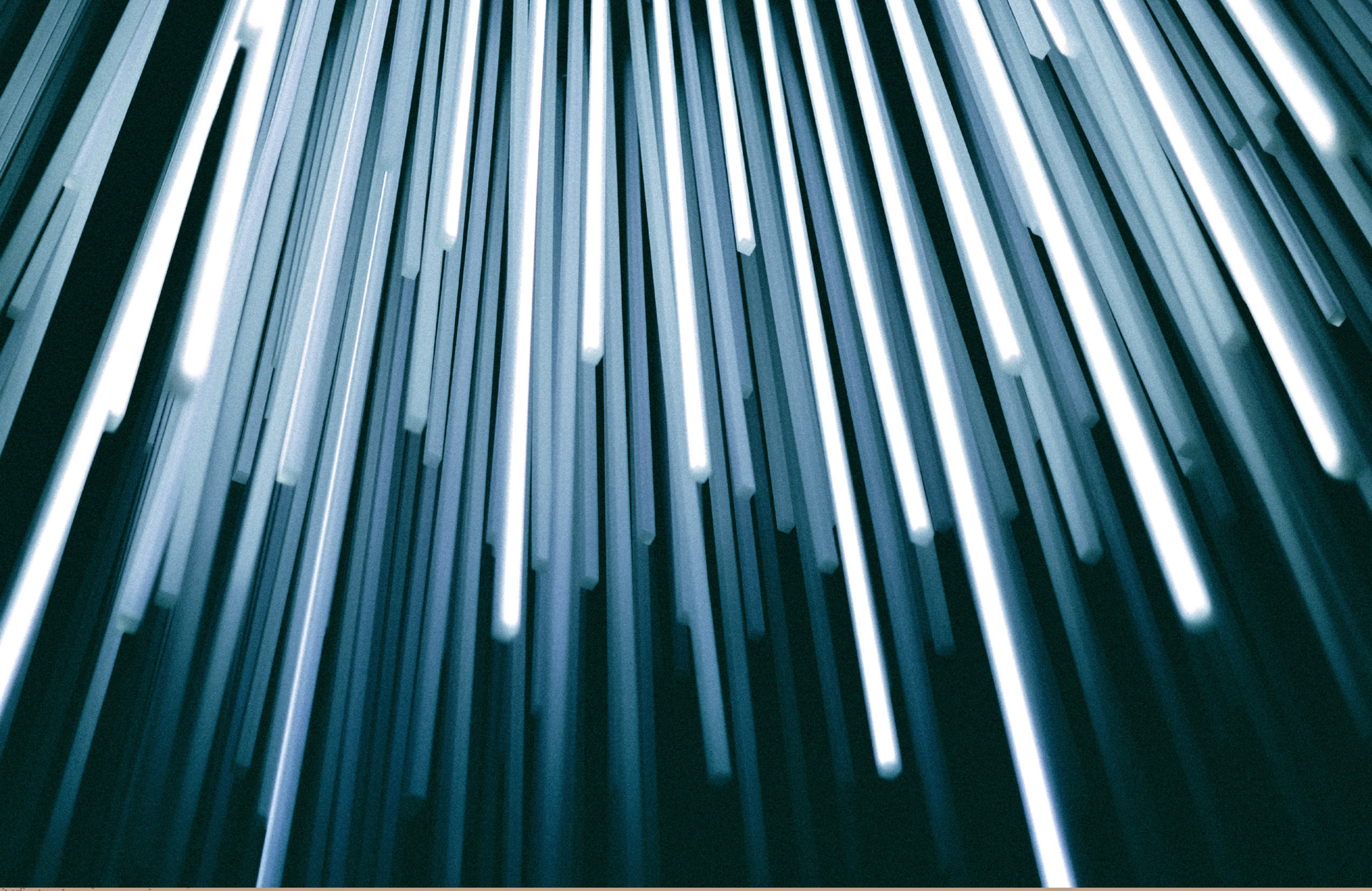
[10] Policy Recommendations for Crypto and Digital Asset Markets (Int'l Org. Sec. Comm'n, Consultation Report 2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf; Policy Recommendations for Decentralized Finance (DeFi) (Int'l Org. Sec. Comm'n, Consultation Report 2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf.

[11] *The Global Regulatory Framework for Crypto-Asset Activities Umbrella Public Note to Accompany Final Framework*, Fin. Stability Bd. (July 17, 2023), https://www.fsb.org/wp-content/uploads/P170723-1.pdf.

[12] Parliament and Council Regulation 2023/1114 of May 3, 2023, on Markets in Crypto Assets (MiCA) and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, May 3, 2023, at 18 (clarifying DeFi as outside the scope of this regulation) and 452-459 (clarifying a forthcoming report that will include an assessment of DeFi and of the appropriate regulatory treatment of DeFi systems), available at: https://data.consilium.europa.eu/doc/document/PE-54-2022-INIT/en/pdf.

[13] *E.g.*, Discussion Draft for Digital Asset Market Structure Act of 2023, H.R. [unassigned], 118th Cong. 157-61 (2023), available at: https://financialservices.house.gov/uploadedfiles/digital_002_xml.pdf.

[14] *E.g.*, Comm'r Hester Peirce, *Safe Harbor 2.0: Proposed Safe Harbor–Time-limited Exemption for Tokens, GitHub* (Apr. 13, 2021), https://github.com/CommissionerPeirce/SafeHarbor2.0. The Bank for International Settlements has also been conducting research on DeFi. *See* Aramonte et. al., *DeFi Risks and the Decentralisation Illusion*, Bank For Int'l Settlements, (Dec. 6, 2023), https://www.bis.org/publ/qtrpdf/r_qt2112b.htm. *See also* Aquilina et. al., *DP17810 Decentralised Finance (DeFi): a Functional Approach*, (Ctr. for Econ. Pol'y Res. Discussion Paper, Paper No. 17810, Jan. 16, 2023), https://cepr.org/publications/dp17810.



2 Defining Decentralized Finance (DeFi), Best Practices and Benefits

Source: @cristopher burns/unsplash

A. What is DeFi?

Since its inception, the Internet has introduced forces of decentralization into the global economy, dramatically transforming economic and social systems and behavior. For example, decentralizing forces of the Internet have led to the platformization of services, such as e-commerce platforms, which have replaced many brick and mortar retailers. These forces have also led to the platformization of financial services leveraging customer-permissioned data that banks share with fintech firms to provide fintech services and products (i.e., open banking).

However, these decentralizing forces were accompanied by centralizing elements as the Internet developed from decentralized digital services of Web1 (e.g., read-only, self-hosted websites and email, etc.) and transitioned to the centralized platforms of Web2 (e.g., read-and-write platforms managed by corporate intermediaries, such as Facebook, Twitter, Amazon, etc.). These platforms consolidated Internet ownership and economic value, resulting in monopolistic practices at the expense of users. Likewise, the existing financial system heavily relies on intermediaries. This current intermediary-based system excludes a significant portion of the global population from accessing financial services.[15]

The next evolution of the Internet, often called Web3, will be a read-write-own network. This read-write-own Internet aims to create systems that incentivize distributed ownership, user empowerment, and participant cooperation without the need to trust or rely on centralized intermediaries.[16] DeFi is one example of this new paradigm. It allows users to retain complete control over their assets while avoiding the need to rely on intermediaries. DeFi is, therefore, a crucial component of the Web3 economy that supports fair access to financial services, ownership or participation interests in these services, and improved market efficiencies.

DeFi is a subset of a broader category of decentralized services (including social media, messaging, digital commerce, digital identity, etc.) that focuses on offering financial services. The term 'DeFi' refers to the ecosystem of applications and protocols enabled by blockchain technology to provide digital and open access to financial services without a single intermediary or small group of intermediaries controlling the system offering the financial service. By removing the 'middlemen,' DeFi holds the promise of lowering access barriers to a multitude of financial services, reducing fees that had inhibited participation in traditional financial activities, and enhancing overall individual financial sovereignty and opportunity.[17]

Digital tech stacks

DeFi comprises a number of components that build on top of each other. These components include, but are not limited to, base layer blockchains, autonomous protocols, smart contracts, applications,[18] self-hosted wallets or accounts, identity systems, Decentralized Autonomous Organizations (DAOs),[19] stablecoins, and other digital assets. Building on base layer blockchains, DeFi protocols serve as the software infrastructure for applications, which provide the user interface. Users generally connect to the DeFi protocols via applications (or apps) built on top of these protocols. As illustrated in Figure 1, these specific components form the digital tech 'stacks' of the DeFi ecosystem.

These DeFi protocols are reminiscent of how Web1 protocols like HTTP, SMTP, and FTP served as public goods, enabling innovators to develop applications and businesses during the early days of the Internet (like AOL, Gmail,

[15] Anju Patwardhan, Ken Singleton, Kai Schmitz, *Financial Inclusion in the Digital Age,* INT'L FIN. CORP. 11-15 (Mar. 2018), https://mfc.org.pl/wp-content/uploads/2019/02/Financial_Inclusion_in_the_Digital_Age.pdf.

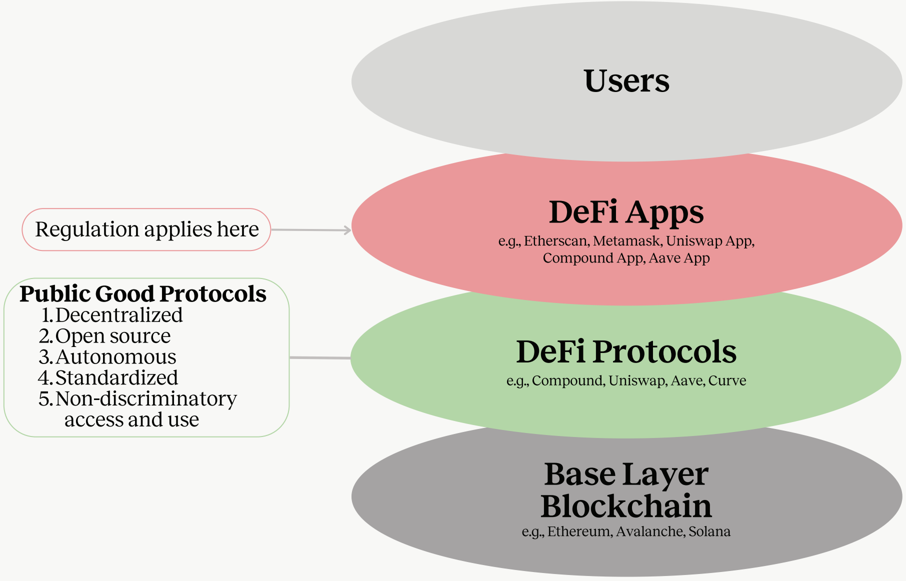
[16] Chris Dixon, *Why Web3 Matters,* A16Z CRYPTO (Sept. 26, 2021), https://a16zcrypto.com/posts/article/why-web3-matters/.

[17] *See* Marvin Ammori, *Decentralized Finance: What It Is, Why It Matters,* A16Z CRYPTO (June 15, 2021), https://a16zcrypto.com/posts/article/what-is-decentralized-finance/#section--1 (explaining that DeFi can provide access to services such as insurance, dollar-denominated savings, and credit at costs significantly lower than what would otherwise be needed in traditional financial infrastructure).

[18] Decentralized applications or DApps are usually applications controlled by a business. They are not decentralized, but they are built on decentralized protocols. For the purposes of the paper, we use the more general term 'app'.

[19] We articulate DAO's more in depth later in this paper. *See* discussion 'Benefit: Participatory Stakeholder Governance'.

FIGURE 1
DeFi Technology Stack


Users
Regulation applies here
DeFi Apps
e.g., Etherscan, Metamask, Uniswap App, Compound App, Aave App
Public Good Protocols
1. Decentralized
2. Open source
3. Autonomous
4. Standardized
5. Non-discriminatory access and use
DeFi Protocols
e.g., Compound, Uniswap, Aave, Curve
Base Layer Blockchain
e.g., Ethereum, Avalanche, Solana

and MS Outlook). Similarly, Web3 applications and businesses leverage DeFi protocols to enhance user experience, broaden access to financial services, and foster market efficiencies, such as improved price discovery. Accordingly, DeFi protocols function as the necessary and critical plumbing for a Web3 financial system. For example, the Uniswap Protocol provides the plumbing that supports a multitude of applications that are built on top of it, including the Uniswap interface—the application run by the team that initially developed the Uniswap protocol—and all the applications that were developed independently that utilize the Uniswap protocol, such as Oku Trade, 1inch, Metamask swap, Coinbase wallet swap, Instadapp, and others.[20]

Harnessing autonomous software protocols and smart contracts to replace the requisite trust needed in centralized operations and intermediaries,[21] DeFi allows users to engage in peer-to-peer transactions and with new innovations in a system where information and decisions are publicly accessible, immutable, and available in real time. It is also important to note that innovations from DeFi can be beneficial for uses beyond DeFi. For instance, DeFi is currently a valuable technology testing ground for digital identity solutions.[22] Therefore, regulating DeFi could have second or third order effects on non-DeFi related innovation.[23]

[20] Uniswap, https://app.uniswap.org/ (last visited Feb. 1, 2020). Note that the Uniswap protocol is distinct from the Uniswap application. The Uniswap protocol is autonomous code that functions independent of human intervention once deployed on a blockchain network. This protocol is the core engine that powers the entire Uniswap system and enables on-chain token swaps and liquidity provision. Unlike the protocol, the Uniswap application is not autonomous and is maintained by the Uniswap Foundation, which regularly updates and adds new features to it. The application serves as the user-friendly interface that translates the user's intent (i.e., swap 1 ETH for 2,000 DAI) into a transaction that conforms to the Uniswap protocol, sends the transaction to the Ethereum network, then translates the results back into a form that the user can easily understand (i.e. 'swap complete,' etc). *See* Resources: FAQ, Uniswap Found., (explaining the function of the Uniswap foundation in relation to the Uniswap App and Protocol) https://www.uniswapfoundation.org/faqs (last visited July 24, 2023). *See also* Hayden Adams et al., *Uniswap v4 Core [Draft]*, Uniswap (June 2023), https://github.com/Uniswap/v4-core/blob/main/whitepaper-v4-draft.pdf (providing background information on the Uniswap protocol upgrade).

[21] *See* Raphael Auer et. al., *The Technology of Decentralized Finance (DeFi)* (Bank for Int'l Settlements Working Paper, Paper No. 1066, Jan. 17, 2023), https://www.bis.org/publ/work1066.pdf (discussing how algorithmic automation of financial activity, composition of various DeFi applications, and openness facilitated by DeFi are key characteristics that can shape the future financial ecosystem).

[22] Technology focused on self-managed identity (i.e., decentralized identity) can be one of many solutions regulators can help support. Companies such as Block (through TBD), SpruceID, Centre, Circle, Coinbase, and others (through the Verite standard), as well as Aleo, Transmute Industries and Disco, are working on such self-managed identity solutions that enable people to control their finances, data and identity.

[23] For example, some of the core principles and building blocks in DeFi could theoretically be utilized towards building critical digital infrastructure, like Zero Trust identity and access management system architectures, or Software Bill of Materials (SBOMs), which the U.S. federal government is currently prioritizing. *E.g., NSTAC Report to the President: Zero Trust & Identity Management*, President's Nat'l Sec. Telecomm. Advisory Comm. at ES-1 (Feb. 23, 2022) (discussing President Biden's Executive Order 14028, calling for advancing toward Zero Trust Architectures), https://www.cisa.gov/sites/default/files/publications/NSTAC_Report_to_the_President_on_Zero_Trust_and_Trusted_Identity_Management.pdf; Press Release, Dep't of Homeland Sec., DHS S&T Forms New Startup Cohort to Strengthen Software Supply Chain Visibility Tools (Apr. 27, 2023) (discussing SBOMS), https://www.dhs.gov/science-and-technology/news/2023/04/27/st-forms-new-startup-cohort-strengthen-software-supply-chain-visibility-tools.

B. DeFi Protocols: Best Practice and Standards

Same Activity, Different Risks, Different Regulation but Same Regulatory Outcome

Financial regulators often rely on the general principle of '*Same Activity, Same Risks, Same Regulation*.'[24] Following this principle, if DeFi offers financial services resembling those of traditional financial (TradFi) institutions,[25] then DeFi and TradFi should be subject to the same regulation. However, the risks posed by DeFi can be fundamentally different, given DeFi's significantly different governing and operational structures, high transparency, and underlying technologies.[26] For instance, DeFi lending protocols may provide loans like TradFi firms.[27] However, unlike TradFi lenders, DeFi lending protocols require overcollateralization.[28] Therefore, DeFi lending protocols have less credit, maturity mismatch, and counterparty risks than TradFi lenders.[29] To this end, these reduced risks contribute to the 'same regulatory outcome' that all regulators strive for: financial safety and soundness, consumer and investor protection, and financial stability.

We acknowledge that the risks of a DeFi service and its corresponding TradFi service can indeed overlap, but it is imperative for regulators to carefully examine the risks of each category of DeFi services before adopting the appropriate regulatory treatment. DeFi services may offer the same activity as TradFi but pose inherently different risks. Accordingly, these different risks should be subject to different—and more appropriate—regulation. This

[24] For instance, when the FSB and IOSCO proposed rules for stablecoins, they relied on this premise to argue that stablecoin issuers should be treated like other payment providers. *See Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations,* Fin. Stability Bd. 2 (Oct. 13, 2023), https://www.fsb.org/wp-content/uploads/P131020-3.pdf; *See also* U.S. Federal Reserve Vice-Chair Michael S. Barr, *Supporting Innovation with Guardrails: The Federal Reserve's Approach to Supervision and Regulation of Banks' Crypto-related Activities,* U.S. Fed. Reserve (Mar. 9, 2023), https://www.federalreserve.gov/newsevents/speech/barr20230309a.htm.

[25] For the purposes of this paper, TradFi institutions include banks, insurance companies, broker-dealers, exchanges, custodians, asset managers, and others.

[26] *See, e.g.,* Nic Carter & Linda Jeng, DeFi Protocol Risks: The Paradox of DeFi, in Regtech, Suptech and Beyond: Innovation and Technology in Financial Services 5-6 (2021) (articulating how transparency provides an opportunity to efficiently disintermediate traditional financial services, but such transparency leaves smart contracts' potential exploits visible to a wider range of actors).

[27] *E.g.,* Compound, https://compound.finance/ (Last visited Jul. 22, 2023).

[28] A recent example involved the Curve Finance exploit, which led to a drop in the price of the CRV token. Curve Finance Founder Michael Egorov had taken out large DeFi loans using his CRV tokens as collateral. The Curve Finance exploit led to a 20% drop in the price of CRV tokens, which meant the value of Egorov's CRV collateral was no longer sufficient to serve as collateral for his large loans, which led Egorov to scramble for additional funds before DeFi lenders like Aave liquidated his CRV tokens. Eventually, Egorov was rescued by Justin Son, another prominent crypto participant. *See* Sage D. Young & Sam Reynolds, *Curve Founder Raises $42.4M to Pay Off $80M On-Chain Debt,* Coindesk (Aug. 4, 2023), https://www.coindesk.com/business/2023/08/03/curve-founder-still-owes-80m-despite-raising-nearly-30m-in-past-two-days/#:~:text=Curve%20Founder%20Michael%20Egorov%20is,%2480M%20On%2DChain%20Debt.
This example demonstrates how DeFi loan risk rests on the borrower—not on the lender—because the lenders in this case required overcollateralization. Hypothetically speaking, if Aave had liquidated Egorov's collateral of CRV tokens, the Curve Finance protocol would have continued to operate. The main risk for Curve Finance would have been that other parties could have then purchased these Curve tokens at a very low price and, more importantly, acquired significant governance power of Curve Finance. *See also* Robert Leshner & Geoffrey Hayes, Compound: The Money Market Protocol, Compound Fin. (Feb. 2019), https://compound.finance/documents/Compound.Whitepaper.pdf. (explaining the functionality of Compound's overcollateralized protocol); *see* discussion *infra* 'Benefit: Participatory stakeholder governance'.

[29] In the context of the Compound protocol, the protocol's autonomous utilization of user-supplied liquidity and overcollateralization are designed to minimize counterparty risks and credit risks found in non-DeFi systems. *See id;* cf. Carter & Jeng, *supra* note 26, at fn. 62 (articulating how operational and legal frictions arise in traditional finance in the settlement process as a result of utilizing intermediaries whereas these intermediaries are not existent in DeFi). Other research on DeFi claims that in mimicking the functions of TradFi, DeFi suffers from similar and potentially amplified vulnerabilities as TradFi. *See* Aramonte et. al., DeFi Risks and the Decentralisation Illusion, Bank For Int'l Settlements, (Dec. 6, 2023), https://www.bis.org/publ/qtrpdf/r_qt2112b.htm. *See also* Aquilina et. al., DP17810 Decentralised Finance (DeFi): a Functional Approach, (Ctr. for Econ. Pol'y Res. Discussion Paper, Paper No. 17810, Jan. 16, 2023), https://cepr.org/publications/dp17810.

'*Same Activity, Different Risk, Different Regulation but Same Regulatory Outcome*' approach should mitigate DeFi risks in the financial system without stifling innovation.

To address this objective, we build upon the 'Regulate Apps Not Protocols' framework put forth by Andreessen Horowitz, which we further articulate as '*Regulate Businesses, Not Public Good Protocols*.'[30] Through this framework, we identify both (1) businesses that operate apps and (2) businesses that operate Non-Public Good Protocols, as suitable access points that can be regulated while preserving the tech neutrality of the underlying infrastructure of DeFi protocols and base layer blockchains. In contrast, DeFi protocols with characteristics we enumerate below ('Public Good Protocols') should not be subject to explicit regulation.[31] We elaborate on this regulatory approach in the section on 'Features of 'Public Goods Protocols."

Framework for Public Good Protocols

Before discussing the features of Public Good Protocols, we need to first discuss what are protocols and, more specifically, identify what DeFi protocols are.

What are Protocols and DeFi Protocols?

First, protocols are a set of rules defining how computers communicate with one another.[32] Examples of commonly used protocols underlying the current Internet infrastructure include HTTP (data exchange for websites), SMTP (email), FTP (file transfer), as well as the SMS and MMS protocols that allow text message communication.

In the context of crypto assets and DeFi, protocols establish the programmable logic relating to crypto asset issuance, use, transfer, and exchange, for specific use cases such as decentralized exchanges, markets, and on-chain asset management.[33] DeFi protocols have been built on various base layer blockchains. Any user or user facing application can access these protocols. While base layer blockchains may also be considered protocols in the sense that they set operational standards for data transfer and communication across computer nodes, for the purposes of this paper we use the term 'protocol' to refer to the digital software stack built on top of the base layer blockchain.

Given its namesake, it should be unsurprising that decentralization is a critical component of DeFi protocols. As we articulate later in the paper, actual decentralization in practice—not just in the name—is essential to cultivating DeFi's potential benefits for users.[34] Discourse on decentralization is often muddied by authors imprecisely using it as a blanket term when referring to different portions of the blockchain ecosystem, including validators, developers, and apps.[35]

[30] *See* Miles Jennings, *Regulate Web3 Apps, Not Protocols,* A16Z CRYPTO (Sept. 29, 2022), https://a16zcrypto.com/posts/article/web3-regulation-apps-not-protocols/ [hereinafter RANPs Pt. 1].

[31] *See* discussion *infra* 'DeFi Protocols - Best Practices and Standards'.

[32] *What Is a Protocol?*, CLOUDFARE, https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/ (Last visited May 30, 2023).

[33] Fabian Schär, *Decentralized Finance: On Blockchain-and-Smart Contract-Based Financial Markets,* 103 FED. RES. BANK OF ST. LOUIS REV. 153, 155-68 (2021) (discussing DeFi architecture).

[34] *See* discussion *infra* 'Benefits of Decentralized Finance'.

[35] ANGELA WALCH, *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, in CRYPTO ASSETS: LEGAL AND MONETARY PERSPECTIVES (Chris Brummer ed., 2019).

Features of Public Good Protocols

Regulators should have the tools to monitor and effectively oversee consumers' safety in this nascent ecosystem. Consequently, it is paramount to have clarity over *which types* of DeFi protocols should be exempt from regulation.[36] If the statutory definition of a protocol is too expansive or permissive, a centralized business could circumvent regulation using smart contracts deployed to a blockchain instead of off-chain proprietary software.[37] If it is too limiting, no protocol will qualify for the exclusion and innovation could come to a halt.[38]

From analyzing the protocols developed over the past half decade in the crypto assets sector, we've identified five baseline criteria that protocols should meet to ensure they are sufficiently safe to act as digital public infrastructure and to best facilitate the next evolution of an inclusive Internet.[39] We refer to DeFi protocols that meet these five features as 'Public Good Protocols.' We articulate below why each of these features is crucial, and many benefits expressed in the 'Benefits of DeFi' section rely on one or a combination of these features.

Public Good Protocols must have the following five features:

1. Decentralized
2. Open source
3. Autonomous
4. Standardized
5. Non-discriminatory access and use

Any potential statutory definition outlining which DeFi Protocols should be exempt from regulation should utilize a principles-based approach that draws upon the five features we've identified in Public Good Protocols. These features establish a baseline level of risk mitigation to ensure that Public Good Protocols are sufficiently safe to act as digital public infrastructure. Establishing these features as a threshold would facilitate a positive feedback loop. By excluding protocols with some or all of these aforementioned characteristics, protocol developers will subsequently be incentivized to build Public Good Protocols with these beneficial traits. Additionally, under this framework, regulators will be afforded pathways to sufficiently protect consumers. Both businesses built on top of Public Good Protocols and Non-Public Good Protocols could be subject to regulation crafted by policymakers and relevant agencies.

[36] Miles Jennings & Brian Quintenz, *Regulate Web3 Apps, Not Protocols Part IV: Practical Application,* a16z crypto (Sept. 29, 2022), https://a16zcrypto.com/posts/article/regulate-web3-apps-not-protocols-practical-application/ [hereinafter RANPs Pt. 4].

[37] *Id.*

[38] *Id.*

[39] *See* discussion *infra* 'Benefits of Decentralized Finance'.

1 Feature: 'Decentralized' status

The term 'decentralized' refers to control over various components within and related to the crypto ecosystem that is not residing with a single party or via the managerial efforts of a specific or limited group of parties.[40] The term 'decentralized' is often inaccurately used, so we propose two threshold tests that Public Good Protocols must meet to be deemed decentralized:

Two Primary Tests for Decentralized Status

A first critical test to determine if a protocol is decentralized is:

- Can any single person[41] or the managerial efforts of a specific or limited group of persons:
  - i. control or fundamentally alter a protocol's purpose or code;
  - ii. control user funds or assets;
  - iii. reverse transactions; or
  - iv. restrict access to the protocol?[42]

If the answer is 'no,' then the protocol is deemed to be decentralized. Otherwise, the protocol does not have the status of being decentralized and would fall on a spectrum of being more or less *centralized*.[43] DAOs should be subject to this test if they contribute to the development or governance of a protocol. They should engage in governance minimization to reduce the risk of information asymmetries that could restrict access, unexpectedly reverse transactions, or alter the protocol's purpose. See section 4(B) for a discussion on protocol governance risks.

[40] Letter from Andreessen Horowitz to HM Treasury (Apr. 29, 2023), https://api.a16zcrypto.com/wp-content/uploads/2023/04/a16z_HMT-crypto-consultation-response-29-April.pdf. ("[D]ecentralised cryptoassets primarily derive their value from decentralised sources, such as market forces, user demand for the underlying protocol and the number of developers building on top of the protocol, rather than the managerial efforts of a single development team. . .[T]hey are inherently trustless (in the sense that no single group of individuals possesses classic "insider information" that could have a material effect on asset prices) . . .Conversely, centralised cryptoassets primarily derive their value from centralised sources, such as the managerial efforts of a development team"). We recognize that decentralization is often used imprecisely and can refer broadly to "the network of computers that comprise a permissionless blockchain" as well as "how power or agency works within permissionless blockchain systems." *See* Walch, *supra* note 35, at 4-12. For the purposes of this piece, we recognize this ambiguity, which is why we use the two primary tests described later in this section.

[41] A 'person' can refer to a human or non-human entity including corporations, partnerships, limited liability companies, etc. *Persons*, Cornell Legal Info. Inst., https://www.law.cornell.edu/wex/legal_person (last visited May 30, 2023).

[42] We recognize that 'small group' is a relatively ambiguous sub-test. We note that the focus should not be on the particular *number* of individuals but rather the information asymmetries that arise when a protocol's development, purpose, and access can be controlled or altered by a select group of individuals without appropriate disclosure or transparency to the broader group of users. DAOs should be subject to this test if they contribute towards the development of a protocol. They should engage in governance minimization to reduce the risk of information asymmetries propping up that could restrict access, unexpectedly reverse transactions, or alter the protocol's purpose. *See* discussion *infra* 'Policy Recommendations: Solving the DAO Dilemma'. *See also Decentralization Factors for Tokenized Consensus Protocols (Layer 1s and Layer 2s)*, Latham & Watkins LLP & a16z Crypto, https://api.a16zcrypto.com/wp-content/uploads/2023/05/Decentralization-Factors-for-Token-Consensus-Protocols-Rev6.pdf (last visited June 13, 2023); *Decentralization Factors for Tokenized Smart Contract Protocols,* a16z Latham & Watkins LLP & a16z Crypto, https://api.a16zcrypto.com/wp-content/uploads/2023/05/Decentralization-Factors-for-Token-Smart-Contract-Protocols-Rev6.pdf (last visited June 13, 2023) (providing various factors to consider when making determinations of decentralization).

[43] Gabriel Shapiro provides a slightly different formulation of the test for a 'sufficiently decentralized' DeFi protocol, whereby 1) validation power, 2) consensus power, 3) protocol/client power, 4) economic power, and 5) user power, should all be decentralized. @Lex_Node, Twitter (Sept. 7, 2020, 11:47 AM), https://twitter.com/lex_node/status/1302679831419600897?s=20.

An important second test asks:

- Is the protocol built on top of a public and permissionless blockchain?

If the answer is 'no,' then the private and permissioned features of the underlying blockchain could negatively impact the decentralized nature of the protocol. For the purposes of this paper, base layer blockchains are assumed to be public and permissionless. Such base layer blockchains are also presumed to be digital infrastructure, like the Internet, and outside the scope of regulation.

Protocols commonly referred to as 'Decentralized in Name Only' (DINOs), are an example of insufficiently decentralized protocols.[44] Applying the Decentralized Status Test reduces the risk of protocols being incorrectly labeled as decentralized when, in reality, they can be controlled or altered by a person or small group of parties.

It is imperative to note that developers and businesses building protocols, in many cases, may start with a centralized model, but eventually move towards a decentralized one. The process of transitioning to greater decentralization and the corresponding suggested regulatory approaches that could facilitate this process is discussed in greater detail in the Policy Recommendations in section (V), particularly sub-section 3, on establishing a Regulatory Safe Harbor for nascent DeFi innovations.

2 Feature: Open source

The open source model for DeFi protocols follows the model set by Linux, an open source software publicly developed by more than 15,600 unaffiliated individuals. These individuals collaborated and built an operating system that now powers everything from digital platforms, such as Google, Facebook, and Wikipedia, to televisions, thermostats, and airline entertainment consoles, as well as technologies that underpin core banking platforms used by financial institutions.[45] Linux's open source software is free, and its source code is available to the public to view, edit and contribute to.[46]

Open source software differs from proprietary or 'closed source' software, for which only the original developer or developer team can control or modify. Closed source software is often licensed and cannot be modified without permission. Open source software is software that is available to the public to view, contribute to and learn from.[47]

There are many reasons for using the open source approach rather than closed source. The developer community has the control and ability to quickly examine the code for issues and flaws, which in turn contributes to the security of the software. Open source software provides an opportunity for anyone to audit the code and swiftly implement code fixes, which ultimately facilitates more secure software over time than closed source versions.[48]

Open source code also fosters user and developer communities, which in turn support sustainable ecosystems where users can experiment with, learn from, and promote the open source code. In addition, users do not have to fear vendor lock-in or losing access to the code and tools they use for long-term projects.[49] The network effects facilitated by open source software also increase market competitiveness and other benefits to the open source software's users rather than only to the intellectual property owners, as happens with a closed source protocol.[50]

[44] Paul Arssov, *DINO (Decentralized In Name Only) Vs. True Decentralization*, HackerNoon (Apr. 20, 2021), https://hackernoon.com/dino-decentralized-in-name-only-vs-true-decentralization-x3r339g.

[45] Peter Van Valkenburgh, What is *"Open Source" and Why is it Important?*, Coin Center (Oct. 17, 2017), https://www.coincenter.org/education/advanced-topics/open-source/; Linux Found., Linux Kernel History Report 21 (2020).

[46] *What is Linux?*, OpenSource, https://opensource.com/resources/linux (last visited June 16, 2023).

[47] *What is Open Source?*, OpenSource, https://opensource.com/resources/what-open-source (last visited June 16, 2023).

[48] David A. Wheeler, *Secure Programming HOWTO: Is Open Source Good for Security?*, https://dwheeler.com/secure-programs/Secure-Programs-HOWTO/open-source-security.html (last visited May 23, 2023).

[49] *What is Open Source?*, *supra* note 47.

[50] RANPs Pt. 1, *supra* note 30.

3 Feature: Autonomous

Public Good Protocols should primarily function autonomously. This means that the protocol's smart contracts are self-executing, and the same input to interact with the code should generate the same expected output. Because the protocol's functionality is predefined by the set of rules embedded in its smart contracts, the protocol operates predictably, transparently, and consistently. Autonomous functionality thus helps to maintain the protocol's credible neutrality.[51] 'Credible neutrality' is defined by Ethereum co-founder, Vitalik Buterin, as being essentially non-discriminatory and fair (see also Feature 5: Non-discriminatory access and use).[52] Adding human intermediaries to the functioning of software protocols also risks undermining the protocol's credible neutrality because intermediaries could co-opt the protocol for their own interests.[53]

Moreover, when Public Good Protocols rely on code instead of intermediaries, anyone can inspect and audit the public ledgers of the blockchains upon which they are built.[54] The combined transparency of the public ledger (which records the price and quantity of each transaction) and of the protocol's smart contracts that govern the protocol's operations[55] would also assist regulators and users in monitoring the protocol's security in ways not available in more opaque TradFi activities.[56]

4 Feature: Standardized

Public Good Protocols should use existing technical standards or contribute to establishing standards to the extent possible to maximize their potential composability and interoperability.[57] Composability refers to the ability of a protocol's smart contracts to interact with those in other protocols frictionlessly. This allows participants in the network to leverage the work of others, which in turn fuels further activities.[58] Composability, in turn, facilitates interoperability across protocols, enabling users to seamlessly move their digital property from one system to another, unlocking value that would otherwise be trapped in a single system.[59]

[51] *Id.*

[52] Vitalik Buterin names four primary rules to building a 'credibly neutral' mechanism: "1) Don't write specific people or specific outcomes into the mechanism, 2) Open source and publicly verifiable execution, 3) Keep it simple, 4) Don't change it too often." Vitalik Buterin, *Credible Neutrality As A Guiding Principle,* Nakamoto (Jan. 30, 2020), https://nakamoto.com/credible-neutrality/.

[53] We elaborate further on this topic later. *See* discussion *infra* 'Benefits of Decentralized Finance: Reducing Counterparty Risk'.

[54] Letter from Andreessen Horowitz to HM Treasury, *supra* note 40, at 11.

[55] *Id.*

[56] *See* discussion *infra* 'Benefits of Decentralized Finance'.

[57] One example is the Ethereum Request for Comment (ERC) standards, which are used to create a streamlined, standard approach for various smart contract transactions. *The Ultimate List of ERC Standards You Need to Know,* 101 Blockchains (July 10, 2021), https://101blockchains.com/erc-standards/.

[58] Linda Xie, *Composability is Innovation,* a16z crypto (June 15, 2021), https://a16zcrypto.com/posts/article/how-composability-unlocks-crypto-and-everything-else/ (tracing this flywheel effect of innovation through an analysis of Ethereum's development and the apps that subsequently built on top of it).

[59] One of the most impactful forms of DeFi composability is the widespread use of ERC-20 token standard, which outlines the ways in which Ethereum tokens should operate on the blockchain. The formalization and adoption of this standard allowed Ethereum smart contracts to act as 'legos' wherein developers could build off one another's work, expediting innovation. *Id.*

5 Feature: Non-discriminatory access and use

Public Good Protocols should allow users to freely access and use the system as a form of public goods. Protocols that discriminate against open access or require permission to be accessed could be co-opted for malicious purposes by those who seek to block their competitors from using the system. Similarly, non-discriminatory usage means that Public Good Protocols should not have the ability to alter or censor transactions that specific individuals have made.[60]

Another important consideration is if the decentralized protocol is built on top of a public and permissionless blockchain. If the protocol is built on a private, permissioned blockchain, then there could be implications for the non-discriminatory nature of the protocol. For the purposes of this paper, base layer blockchains are assumed to be public and permissionless.

Permissionless, non-discriminatory access is also important for accelerating innovation, as it creates a layered infrastructure wherein other protocols and applications can be built to enhance or provide additional features to the underlying system. TCP/IP, the underlying protocol that powers the internet today, is a permissionless technical specification. When developers created innovative protocols for developing websites with images and interactive links and abandoned pure text-based interfaces, they did not need approval from a central party.[61] If the internet's base layer were originally permissioned, it would have imposed costs to public participation, limiting the diversity of the many beneficial protocols built atop TCP/IP that we use today.[62]

In line with the philosophy that underpinned the Internet's history, which has yielded benefits for users, Public Good Protocols should also provide open access to users. Permissionless access means that the costs of building upon these protocols are low, facilitating greater competition and participation by businesses designing user-facing applications on these foundational software layers.[63] For the DeFi ecosystem to provide financial services to those who have been underserved or are in economically precarious environments, Public Good Protocols cannot be permissioned, or else they risk replicating the forms of exclusion found today in TradFi. Rather, they must act and function as public goods.[64]

[60] RANPs Pt. 4, *supra* note 36.

[61] Peter Van Valkenburgh, *What Does "Permissionless" Mean?*, Coin Center (Jan. 31, 2017), https://www.coincenter.org/education/advanced-topics/what-does-permissionless-mean/.

[62] *Id.*

[63] *Id.*

[64] *See* discussion *infra* 'Benefits of Decentralized Finance'.

3 DeFi: An Alternative Form of Financial Services

Source: @mcdobbie hu//unsplash

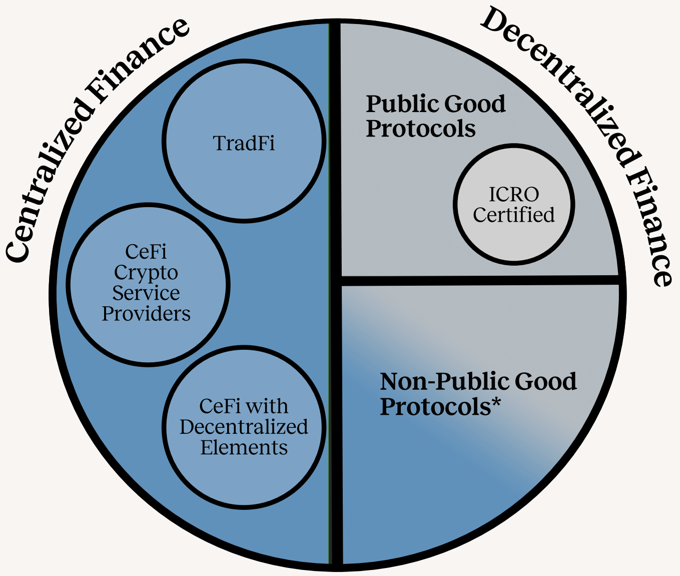
DeFi uses programmable blockchain technology to develop decentralized protocols capable of providing disintermediated financial services, generating greater optionality, increased efficiency, and reduced costs and participation interests for end users. It leverages the Web3 Internet's read/write/own features and augments user control, autonomy, and participation in financial services. DeFi's enhanced flexibility and programmability support innovation and new opportunities for users, but with a much different risk profile from TradFi.

In contrast, centralized finance (or "CeFi") is the provision of financial services that are controlled by a single party or managerial efforts of a small group of parties. It includes crypto service providers, such as centralized crypto exchanges and custodians, as well as centralized issuers of stablecoins and digital assets, and others. These centralized participants provide important services in the digital assets ecosystem while providing ideal experiences for users. Although many refer to CeFi as crypto sector-specific, the TradFi sector also comprises centralized intermediaries (e.g., banks, broker-dealers, exchanges, asset managers and custodians, etc.) and as such, is also an example of CeFi. See Figure 2 below.

Our financial system is currently evolving to encompass both DeFi and CeFi elements. We also anticipate that DeFi and CeFi will coexist and interact. For instance, the future financial system could entail a CeFi business providing easily accessible and user-friendly interfaces while leveraging the programmability, security, and functionalities of the underlying DeFi infrastructure. Other users—retail and institutional—may want the optionality to access DeFi services directly. Many users will use both options.

FIGURE 2

Financial Ecosystem: CeFi & DeFi


Centralized Finance
Decentralized Finance
TradFi
CeFi Crypto Service Providers
CeFi with Decentralized Elements
Public Good Protocols
ICRO Certified
Non-Public Good Protocols*

* Although these protocols may be used by DeFi apps, they also possess centralization characteristics found in CeFi

** Darker color indicates greater level of regulation

Before articulating our proposed regulatory approach in-depth, we outline the benefits of DeFi to establish why a regulatory framework for this nascent sector should be designed to take into account the significantly different characteristics of DeFi. Many of DeFi's benefits arise from the features elaborated for Public Good Protocols: decentralized, open source, autonomous, standardized, and non-discriminatory. The gains that consumers, businesses, and investors can capture from DeFi are varied and nuanced, and regulating with a sledgehammer instead of a scalpel may inadvertently foreclose future innovations that take full advantage of the potential of DeFi while failing to target the appropriate and critical sites of risk.

A. Benefits of DeFi

While innovative uses of DeFi continue to grow, prominently used DeFi services and products currently include borrowing and lending services, insurance, and asset management. Financial applications that sit on top of decentralized protocols can leverage the open, neutral, and decentralized nature of the blockchain technology to establish new economic structures that mitigate many of the risks in the TradFi system through increased transparency, innovative forms of governance, and enhanced security. As we outline the benefits offered by DeFi below, we note that these benefits are based on features required for Public Good Protocols.

1 Benefit: Reducing counterparty risks

Public Good Protocols can mitigate various counterparty risks that arise in TradFi services due to the use of various intermediaries. The intra-transaction composability of smart contracts allows multiple actions to be executed within a single transaction, reducing the reliance and trust needed for numerous parties to effectively facilitate custody, escrow, clearing, and settlement.[65] Additionally, the use of autonomous and composable smart contracts decreases the costs traditionally associated with executing a transaction, such as finding and selecting a counterparty, concluding a contract, and enforcing a claim.[66]

Moreover, unlike in CeFi, where a centralized entity typically holds onto the users' assets and executes transactions on their behalf, DeFi users only temporarily grant smart contracts access to their assets to complete a transaction on the blockchain.[67] This self-custodial nature of Public Good Protocols places the financial focus on individual asset owners, empowering them to make decisions based on a broader set of customizable services through programmable smart contracts. There are numerous examples where consumers have placed trust in CeFi–including TradFi—businesses, for these businesses to fail in meeting their promises to their customers.[68] The popular warning "not your keys, not your coins" is fully baked into the self-custodial nature of Public Good Protocols. An individual maintains complete control over their keys, eliminating forms of counterparty risk or other execution risks, such as the uncertainties associated with how a centralized entity may be managing or commingling a user's funds.[69]

[65] Tamás Katona, *Decentralized Finance – The Possibilities of a Blockchain 'Money Lego' System,* 20 Fin. and Econ. Rev. 74, 86-89 (2021) (discussing replacement of central counterparties using DeFi); Fabian Schär, *Decentralized Finance Could Support a New Financial Infrastructure if Challenges are Overcome*, IMF: Finance & Development (Sept. 2022), https://www.imf.org/en/Publications/fandd/issues/2022/09/Defi-promise-and-pitfalls-Fabian-Schar (noting the elimination of certain risks since assets can only be transferred upon predefined smart contract conditions being fulfilled).

[66] Katona, *supra* note 65, at 75-76.

[67] Turan Sert, *Key DeFi Attributes: Non-Custodial*, Medium: BCIST Center (Nov. 27, 2021), https://medium.com/bcistcenter/key-defi-attributes-non-custodial-e927f761609f (discussing the technical features of smart contracts that facilitate the non-custodial nature of DeFi services).

[68] Notable TradFi examples include the Bernie Madoff Ponzi scheme and the Cyprus bank account levy. Kade Garnett, *What Are the Pros and Cons of DeFi?*, Decrypt (Feb. 13, 2023), https://decrypt.co/resources/what-are-the-pros-and-cons-of-defi-learn. Notable CeFi failures include FTX and BlockFi. *Id.*

[69] The phrase "not your (private) keys, not your coins" and the phrase "if you have your keys, you have your coins" are frequently stated in the DeFi community. Both phrases underscore the importance of users owning their own keys to mitigate the risk of a third-party commingling user funds or using them in ways they did not or would not consent to. *See Id.* Note that as institutional investors have sought out means to invest in DeFi products or services, products have been designed that allow institutional investors to do so while simultaneously eliminating the risk nefarious fund managers can commingle client assets with unverified sources. Yoshiki Takeuchi, Why Decentralised Finance Matters and the Policy Implications 54, Off. for Econ. Cooperation & Dev. (2022).

2 Benefit: Increased financial access

The permissionless nature of DeFi enables users to have greater access to financial services while reducing the existence of rent-seeking intermediaries.[70] Like other fintech innovations, DeFi provides faster and cheaper settlement than traditional payment services. Real time payment and settlement are especially important for individuals who live paycheck to paycheck, and businesses with sensitive cash flow management.[71] Furthermore, the inherent qualities of DeFi, such as permissionlessness, composability, and self-custody, could support critical use cases within and outside the US, particularly among communities that have met with obstacles in accessing traditional financial services for historical, political, or economic reasons.[72]

A Fostering Trust for Communities Historically Excluded from Traditional Financial Services

Historically, marginalized communities have faced various forms of exclusion from the traditional financial system, limiting their access to basic financial services and opportunities to grow wealth. Discriminatory lending practices, the inaccessibility of physical banking branches, and cost barriers are among some of the obstacles to increasing financial inclusion.[73] According to the FDIC Survey of Household Use of Banking and Financial Services, 6% of adults (nearly 20 million Americans) do not have a bank account, with the statistic being disproportionately greater among African American (13%) and Hispanic (11%) communities.[74] Furthermore, one of the most commonly cited reasons for not having a bank account was a lack of trust in banks.[75] Likewise, a survey conducted by Ariel-Schwab indicates that African American investors are more likely than white investors to have (i) never invested or stopped investing due to lack of trust in the stock market (36% versus 25%) or due to lack of trust in financial institutions (25% versus 19%).[76]

Against this backdrop, historically-excluded communities have found the decentralized nature of crypto particularly appealing.[77] The self-custodial and transparent qualities of DeFi have the potential to empower individuals with independence in financial decision-making while retaining control of their assets. Additionally, rules-based smart contracts discourage human discrepancies and discriminatory behavior in lending and financing. As a trustless[78] financial system, which does not require trusting an intermediary, DeFi is an important alternative to financial services for those who distrust traditional financial intermediaries.[79]

[70] *See* Takeuchi, *supra* note 69, at 49-53.

[71] Sheila Warren, *Hearing to Review S.4760 the Digital Commodities Consumer Protection Act*, Before the Comm. on Agric., Nutrition, and Forestry, 117th Cong. 5-6 (2022) (testimony of Sheila Warren, CEO, Crypto Council for Innovation), https://cryptoforinnovation.org/wp-content/uploads/2022/09/Crypto-Council-Written-Testimony-Sheila-Warren.pdf. Individuals harmed by natural disasters or in the midst of war or other forms of turmoil in particular benefit from real-time crypto payment and settlements. *See, e.g.*, Liz Mills, Post-Earthquake Crypto Donations Flood into Turkey, Crypto Council for Innovation (Mar. 1, 2023), https://cryptoforinnovation.org/update-post-earthquake-crypto-donations-flood-into-turkey/; Ananya Kumar and Nikhil Raghuveera, *Can Crypto Deliver Aid Amid War? Ukraine Holds the Answer,* Atlanta Council (Apr. 4, 2022), https://www.atlanticcouncil.org/blogs/new-atlanticist/can-crypto-deliver-aid-amid-war-ukraine-holds-the-answer/.

[72] *See* Renée Barton et. al., *Income and Wealth Creation in Web3 Case Studies Demonstrating Economic Outcomes,* Cradl at 68-71 (Jan. 2023), https://www.cradl.org/new-income-wealth-web3#report-form. *See also* Saif Ahmed Abdulhakeem & Qiuling Hu, *Powered by Blockchain Technology, DeFi (Decentralized Finance) Strives to Increase Financial Inclusion of the Unbanked by Reshaping the World Financial System*, 12 Modern Econ. 1, 12-13 (2021) (discussing the aim of DeFi to lessen the power and control of intermediaries and create transparent, permissionless, and open source financial ecosystem that is accessible to anyone).

[73] *See* Warren, *supra* note 71, at 18.

[74] Ed. Mark Kutzbach et. al., FDIC National Survey of Unbanked and Underbanked Households 13-15 (Karyen Chu ed., Fed. Deposit Insurance Corp, 2021).

[75] *Id.* at 19 (Noting "don't trust banks" was the second-most cited main reason for not having an account in 2021 by survey participants).

[76] *Ariel-Schwab Black Investor Survey,* Charles Schwab (2022), https://www.schwabmoneywise.com/tools-resources/ariel-schwab-survey-2022.

[77] Valerie Viard et al., *Black Experiences in Web3,* Cradl (Dec. 2022), https://www.cradl.org/black-experiences-crypto.

[78] 'Trustlessness' refers to the ability of a network to mediate transactions without any of the involved parties needing to trust a third party. *Trustlessness,* Ethereum Found., https://ethereum.org/en/glossary/#trustlessness (last visited June 20, 2023).

[79] *See* Warren, *supra* note 71, at 2-4.

B Protection from Inflation and Disruptive Regimes

The self-custody feature of Public Good Protocols embodied by self-hosted wallets or accounts is critical in regimes where inflation severely hampers wealth preservation or in environments where third parties can unilaterally disrupt traditional financial services. In Afghanistan, where financial services have become unreliable, civilians have been using crypto in part to hedge against the Taliban's seizure of assets.[80] Likewise, when the Feminist Coalition's bank account was shut down in Nigeria, Bitcoin became critical for raising donations for the coalition's #EndSARS campaign against police brutality.[81] In the face of crackdowns on speech, dissidents and independent media organizations in Belarus, Hong Kong, and Russia have resorted to crypto for funding and donations.[82]

C Promoting Growth and Efficiency in Emerging Markets

DeFi can also play a significant role in emerging markets where consumers and businesses have challenges in accessing TradFi services. Small medium enterprises (SMEs) can tap liquidity and access alternative financing opportunities through DeFi lending and borrowing protocols, which often provide more competitive rates than TradFi.[83] For instance, in the previous year, leading DeFi protocols provided loans at a mean interest rate of 1.8%,[84] in contrast to the TradFi prime rate, which escalated from 4.5% to 8.5% over the same period.[85] SMEs may also use major DeFi exchanges to convert payments in different currencies for faster, cheaper, and less complicated settlement. According to a 2022 survey by Visa of nine economies around the world, almost one-quarter of small businesses in these markets plan to accept digital currencies as a form of payment.[86] Chargebacks and payment reversals can be exceptionally costly for smaller merchants, making the final settlement nature of crypto asset transactions particularly appealing.[87]

Informal, short-term, cross-border businesses in Sub-Saharan Africa and Latin America have also found a use for crypto, especially when they are prevented from opening a local bank account in the client country.[88] Moreover, DeFi products have a wider range of customizability for the amount, duration, and cost of the loan or other financial service, while the predetermined rules of smart contracts ensure that financing decisions are made with fewer inconsistencies and biases.[89]

[80] Michael Pisa, Responding to Afghanistan's Humanitarian Crisis: The Potential Role of Digital Payments, Ctr. Glob. Dev. (May 3, 2022), https://www.cgdev.org/publication/responding-afghanistans-humanitarian-crisis-potential-role-digital-payments; Eltaf Najafizada, Afghan Crypto Buyers Aren't Trying to Strike it Rich. *They're Just Trying to Keep What They Have Out of The Taliban's Reach,* FORTUNE (Apr. 24, 2022, 2:44 PM), https://fortune.com/2022/04/24/afghan-crypto-buyers-keep-money-out-of-taliban-reach-stablecoin-herat/.

[81] Colin Harper, *Nigerian Banks Shut Them Out So These Activists Are Using Bitcoin to Battle Police Brutality,* COINDESK (Oct. 16, 2020), https://www.coindesk.com/tech/2020/10/16/nigerian-banks-shut-them-out-so-these-activists-are-using-bitcoin-to-battle-police-brutality/.

[82] Roger Huang, *Dissidents Are Turning To Cryptocurrency As Protests Mount Around The World,* FORBES (Oct. 19, 2020, 11:26 AM), https://www.forbes.com/sites/rogerhuang/2020/10/19/dissidents-are-turning-to-cryptocurrency-as-protests-mount-around-the-world/?sh=1a88eac7584c; Jillian Deutsch & Aaron Eglitis, Putin's Crackdown Pushes Independent Russia Media Into Crypto, Bloomberg (May 9, 2022, 11:00 PM), https://www.bloomberg.com/news/articles/2022-05-10/putin-s-crackdown-pushes-independent-russian-media-into-crypto.

[83] *See* discussion *supra* 'Benefit: Reducing Counterparty Risk'. Note, however, that the comparison of DeFi and TradFi lending is made complex by the fact that DeFi loans are typically overcollateralized whereas TradFi lending is uncollateralized, meaning it's often not an apples-to-apples comparison.

[84] Ally Zach, *Maker's Money Market,* Messari (Feb. 22, 2023) https://messari.io/report/maker-s-money-market.

[85] *Bank Prime Loan Rate (DPRIME)*, FED. RES. BANK OF ST. LOUIS (Last visited May 31, 2023), https://fred.stlouisfed.org/series/DPRIME.

[86] Hannah Lang, *A Quarter of Small Businesses Across Nine Countries Plan to Offer Crypto Payments: Visa Survey,* REUTERS (Jan. 12, 2022, 5:02 AM), https://www.reuters.com/technology/quarter-small-businesses-across-nine-countries-plan-offer-crypto-payments-visa-2022-01-12/.

[87] Amy Nichol Smith & Rob Watts, 33% of *Small Businesses Have Been Severely Impacted By Credit Card Fraud – Are Payment Processing Services Truly Secure?*, FORBES (Mar. 2, 2023), https://www.forbes.com/advisor/business/software/payment-processing-users-safety/.

[88] Kristy Lam, *Non-Dollar Stablecoins Gain Momentum, Risks to USD Rise*, *Crypto Council for Innovation* (Apr. 4, 2023), https://cryptoforinnovation.org/non-dollar-stablecoins-gain-momentum-risks-to-usd-rise/.

[89] Simon Chandler, *DeFi and Credit on the Blockchain: Why Loans Are Better When They're Decentralized*, COINTELEGRAPH (May 25, 2019), https://cointelegraph.com/news/defi-and-credit-on-the-blockchain-why-loans-are-better-when-theyre-decentralized.

3 Benefit: Increased transparency

Transparency is a core feature of Public Good Protocols and forms the basis of trust within a decentralized system. Because the public can view transactions recorded on the blockchain ledger and ascertain the predetermined rules and functions of smart contracts, users can observe transactions in real time, verify information on the ledger independently, and transact efficiently without needing to know the identity and personal details of other participants within the system. Because of this transparency and decentralization, public blockchains act as a public good in the form of financial infrastructure by providing neutral, independent, and immutable transaction records, while DeFi protocols act as another public good in the financial infrastructure by providing accessible and unbiased operations.[90]

The visibility of on-chain transactions also provides a rich data source for real-time risk management while reducing information asymmetries. Analyzing on-chain transactions can uncover rehypothecated assets, conflicts of interest, and risks associated with credit, liquidity, and concentration.[91] Likewise, lenders and borrowers can be held to a higher degree of accountability because anyone can see the relevant parties' transaction history.[92] Notably, harmful actions and opaque risk taking that centralized financial platforms, such as FTX, undertook become nearly impossible in DeFi since activities and engagement with user funds are on open, immutable blockchains.[93]

Beyond risk mitigation, DeFi applications—such as the 1inch Wallet—built on top of Public Good Protocols, have enabled donors to transfer, track, and account for their contributions to charitable organizations, such as The Humane Society of the United States, Amref Health Africa, and the National Wildlife Foundation, reassuring donors that their funds are used as intended.[94] This is crucial at a time when organizations and political factions are frequently blamed for exploiting donations, and individual giving is decreasing due to a lack of trust in the charity collection process.[95] Researchers have additionally proposed blockchain-based frameworks to collect and spend charity donations in a publicly auditable manner.[96] For example, the U.S. experiences challenges in sending aid and investments to the right recipients.[97] Sending USD-backed stablecoins to, for instance, an identified, foreign government-controlled wallet address could help solve the delivery problem and allow the US to monitor the receiving governments' use of funds.[98]

[90] Schär, *supra* note 65, at 168-69.

[91] *See* discussion *supra* 'Benefits of Decentralized Finance: Reducing Counterparty Risk'.

[92] Chandler, *supra* note 89.

[93] Index Coop DAO, DeFi is the Answer to the *FTX Crisis—but We Must Get Better at Communicating It,* Decrypt (Nov. 20, 2022), https://decrypt.co/115149/defi-is-the-answer-to-the-ftx-crisis-but-we-must-get-better-at-communicating-it.

[94] *What is 1inch (1INCH)?,* The Giving Block (last visited May 30, 2023), https://thegivingblock.com/resources/cryptocurrency/1inch/; *see generally, e.g., Paul Sullivan, Nonprofits Get a New Type of Donation: Cryptocurrency,* N.Y. Times (July 30, 2021), https://www.nytimes.com/2021/07/30/your-money/cryptocurrency-donation-nonprofit.html (elaborating on the tax and accounting benefits of crypto donations).

[95] *See, e.g.,* Tessa Fox, Assad Regime *'Siphons Millions in Aid' by Manipulating Syria's Currency,* The Guardian (Oct. 21, 2021), https://www.theguardian.com/global-development/2021/oct/21/assad-regime-siphons-millions-in-aid-by-manipulating-syrias-currency.

[96] Muhammad S. Farooq, *A Framework to Make Charity Collection Transparent and Auditable Using Blockchain Technology,* 83 Comput. & Elec. Eng'g (2020) (discussing blockchain solutions for transparency in donation systems); Michael Bodley, *Can Stablecoins Revolutionize Foreign Aid? The UN Thinks So.,* Blockworks (Dec. 16, 2022) (highlighting billions of dollars' worth of embezzlement in foreign aid distributed via fiat currency, and noting the solution provided by stablecoins), https://blockworks.co/news/un-stablecoins-revolutionize-foreign-aid.

[97] *See, e.g.,* Curt Tarnoff, Iraq: Reconstruction Assistance, Cong. Rsch. Serv. (Aug. 7, 2009) (discussing "less than adequate controls" related to $8.8 billion of development bank resources moved through Iraqi ministries, and the failure to track 15%-20% of the Iraq Relief and Reconstruction Fund after remittance); David Francis, *How the US Lost Billions over Nine Years in Iraq*, CNBC (June 19, 2014), https://www.cnbc.com/2014/06/19/how-the-us-lost-billions-over-nine-years-in-iraq.html (discussing $8 billion of $61 billion allocated for Iraq's reconstruction going to waste, and a SIGIR audit revealing that $12.5 billion of the Department of Defense's $19.6 billion total obligation was left untraceable).

[98] Remitting aid via stablecoins has proven not just theoretically useful, but also effective in practice. *See, e.g.,* UNHCR *Wins Award for Innovative Use of Blockchain Solutions to Provide Cash to Forcibly Displaced in Ukraine,* U.N. High Comm'r for Refugees (Mar. 23, 2023), https://www.unhcr.org/news/unhcr-wins-award-innovative-use-blockchain-solutions-provide-cash-forcibly-displaced-ukraine.

4 Benefit: Security and resilience

By building on the security of decentralized blockchains, DeFi has fewer points of failure relative to CeFi/TradFi alternatives. For instance, validators of blockchains must cryptographically verify a transaction's legitimacy for the transaction to be added to the blockchain's public ledger, and each node operator has a copy of the ledger. This distribution of information reduces the likelihood of unilateral changes to the ledger by a single entity. It also reduces the likelihood of a systemic failure of the blockchain. If a node were to fail, the other nodes have the distributed ledger to continue operating the blockchain.[99] Whereas in TradFi, all data and records can be lost if a TradFi institution fails or experiences a detrimental cybersecurity attack, forcing operations to stop.[100] In this sense, decentralized systems are more resilient to cybersecurity risks than more centralized systems.[101]

DeFi's self-custodial nature further protects personal funds. Self-custody eliminates counterparty risk exposure to third-party custodians.[102] Compared to CeFi/TradFi, DeFi can transform central honeypots of data and customer funds from single points of failure into resilient, distributed, immutable ledgers that safeguard user funds and data transparently.[103] Additionally, this tamper-proof nature of underlying blockchains means that no completed transaction can be modified without detection, thereby promoting trust and security in the network.[104]

5 Benefit: Participatory stakeholder governance

DeFi protocols can allow participants to participate in the protocol's governance. For example, some decentralized protocols utilize DAOs, to assist with operations and protocol improvements.[105] A DAO is generally an organized group of persons or parties that coordinates the governance of a protocol or blockchain through a shared set of rules.[106] DAOs allow members to participate directly in the governance of the blockchain, but they are not controlled by a single member or through the managerial efforts of a small group of members. Individuals or parties can become members of DAOs by acquiring governance tokens of the protocol or blockchain.[107]

[99] Javad Zarrin, Hao W. Phang, Lakshimi B. Saheer & Bahram Zarrin, *Blockchain for Decentralization of Internet: Prospects, Trends, and Challenges,* 24 Cluster Comput. 2841, 2842-43, 2846 (2021) (discussing the security advantage and reliability of decentralized blockchains in preventing network attacks).

[100] *See* Sky Jung, *Privacy in Decentralized Finance: Should We Be Concerned?*, Harvard Tech. Rev. (Aug. 22, 2021), https://harvardtechnologyreview.com/2021/08/22/privacy-in-decentralized-finance-should-we-be-concerned/.

[101] *See* Takeuchi, *supra* note 69, at 40-41.

[102] *See* discussion *supra* 'Benefits of Decentralized Finance: Reducing Counterparty Risk'.

[103] *See* Hendrik Amler et. al., *DeFi-ning DeFi: Challenges & Pathway*, Cornell arXiv (Jan. 14, 2021) (discussing the trustless, transparent, interconnected, decentrally governed, and self-sovereign advantages of DeFi when compared to CeFi and emphasizing the lack of central authority controlling and organizes access to data and funds in DeFi). *See also Liyi Zhou, et al., SoK: Decentralized Finance Attacks,* Cornell arXiv (Apr. 7, 2023) (discussing the benefits of atomic composability used in DeFi platforms relative to CeFi); Kaihua Qin et. al., *CeFi vs. DeFi—Comparing Centralized to Decentralized Finance,* Cornell arXiv (June 16, 2021) (noting the relative simplicity of tracing DeFi funds when compared with tracing CeFi assets due to the transparency of DeFi; emphasizing user-control, and accessibility as the unique advantages of DeFi, and elaborating the risks related to intermediaries and single points of failure in CeFi).

[104] *See What is Blockchain Security?*, IBM, https://www.ibm.com/topics/blockchain-security (last visited May 24, 2023).

[105] Note that some individuals conceptualize the 'A' in DAOs as 'autonomous' in the sense that they have autonomy, not because they are automated. *See, e.g.,* Gabriel Shapiro, Autonomy v. Decentralization, Medium (Mar. 3, 2023), https://lex-node.medium.com/autonomy-vs-decentralization-ceb2645f9cd5.

[106] *What are DAOs?*, Ethereum Found., https://ethereum.org/en/dao/#what-are-daos (last visited June 20, 2023); *see also* Louis Lehot & Patrick D. Daugherty, DeFi and the DAO: *How the Law Needs to Change to Accommodate Decentralized Autonomous Organizations*, Foley Ignite (Dec. 14, 2021), https://www.foley.com/en/insights/publications/2021/12/louis-lehot-defi-dao-how-law-needs-to-change.

[107] *See* DAO Membership, Ethereum Found., https://ethereum.org/en/dao/#dao-membership (last visited June 20, 2023).

DAOs are often used to oversee the development of DeFi protocols, as they provide an efficient and auditable form of governance.[108] While the exact governance arrangements are DAO-specific and designed through continued experimentation, these organizations are essential for facilitating the evolution and growth of decentralized protocols to accommodate technological improvements or changes in market conditions, and to resolve potential disputes.[109]

The evolution of the Compound protocol illuminates these benefits. Launched by Compound Labs in 2017, its founders developed a protocol to facilitate permissionless, overcollateralized crypto lending through the use of algorithmically-determined interest rates.[110] On the lending side, users earn interest by supplying assets to one of the protocol's liquidity pools.[111] On the borrowing side, users are able to borrow crypto assets from the protocol's liquidity pools as long as the amount borrowed is worth less than the value of the crypto asset collateral provided.[112] As one of the first DeFi protocols, Compound illustrated the feasibility and demand of a robust lending protocol[113]—stress testing has demonstrated its ability to scale without sacrificing user safety offered by its overcollateralized model.[114]

While Compound Labs steered the protocol's development and funding in its early stages, it experimented with using community governance to make modifications to the protocol, such as determining what additional crypto assets should be accepted as collateral.[115] Eventually, Compound Labs transitioned to a purely decentralized model and distributed COMP tokens to the protocol's contributors and stakeholders.[116] COMP token owners consequently constitute the Compound DAO and can put forth proposals to update the protocol and vote to approve or deny proposals of other DAO members.[117] Since its launch, Compound DAO members have submitted 168 proposals, and 130 have been executed.[118]

The legal nature of DAOs is still evolving. DAOs are such a recent phenomenon that there are few, if any, laws in major jurisdictions around the globe that define their legal status, but some lawmakers are beginning to examine this gap.119 Similar to the articles of incorporation found in corporations, a set of rules and principles determining

[108] *See* Letter from Andreessen Horowitz to HM Treasury, *supra* note 40, at 7 (explaining that DAO decision-making can fund projects crucial to the development of its corresponding protocol). *See generally Linda Xie, A Beginner's Guide to DAOs,* Mirror.XYZ (Mar. 12 , 2021), https://linda.mirror.xyz/Vh8K4leCGEO06_qSGx-vS5lvgUqhqkCz9ut81WwCP2o (elaborating on the various use-cases of DAOs, which include art collectives, meta-governance of other DAOs, and prediction markets).

[109] *See, e.g., Maker DAO*, Messari, https://messari.io/asset/maker/profile (last visited May 31, 2023) (developing a money market and stablecoin protocol); *see also* GNOSIS, Messari, https://messari.io/asset/gnosis/profile (last visited July 21, 2023).

[110] Robert Leshner, *Introducing Compound, the Money Market Protocol,* Medium (Jan. 30, 2018), https://medium.com/compound-finance/introducing-compound-the-money-market-protocol-4b9546bac87.

[111] Leshner & Hayes, *supra* note 28.

[112] *Id.* For example, if a user were to provide 1,000 Crypto Token X worth $100, they could then borrow $50 worth of any other crypto asset available on the protocol. To retrieve their collateral, the user would then pay back the amount borrowed plus the interest rate algorithmically determined by the protocol. *See What is Compound in 5 Minutes,* Cryptopedia (June 28, 2022), https://www.gemini.com/cryptopedia/what-is-compound-and-how-does-it-work#section-compound-crypto-borrowing.

[113] By 2020, the platform had gained immense popularity and had received more than $1.7 billion in total deposits. Brady Dale, *Compound Tops $1B in Crypto Loans as DeFi Farmers Keep Digging for Yield,* Coindesk (July 13, 2020), https://www.coindesk.com/tech/2020/07/13/compound-tops-1b-in-crypto-loans-as-defi-farmers-keep-digging-for-yield/.

[114] Coindesk Hsien-Tang Kao et. al., An Analysis of the Market Risk to Participants in the Compound Protocol 6-8 (2020) (demonstrating that Compound contracts could withstand agent-based simulations and stress-testing even after scaling up at 10x the current borrow size at the time).

[115] Robert Leshner, *Select the Next Compound Asset,* Medium (Aug. 14, 2019), https://medium.com/compound-finance/select-the-next-compound-asset-9e5e98f26822.

[116] Jake Chervinsky, *The Compound Protocol Belongs to the Community,* Medium (June 16, 2020), https://medium.com/compound-finance/compound-community-ownership-ee0ed1252cc3.

[117] Communications related to DAO votes takes place primarily via their governance forum, which provides background information on how to vote, put forth proposals, and other ways to get involved in the Compound community. *See generally* Compound, https://www.comp.xyz/ (last visited July 21, 2023).

[118] Comp.Vote, https://comp.vote/ (last visited July 21, 2023) (listing all the voting results of previous proposals).

[119] For example, California legislators have introduced a bill on the legal status of DAOs. *Jason Nelson, DAOs Could Get Official Standing Under Proposed California Law,* Decrypt (Apr. 24, 2023), https://decrypt.co/137767/daos-could-get-official-standing-under-california-law.

governance structure and processes are embedded in the DAO when it is established.120 But, DAOs execute operations autonomously through the use of smart contracts, reducing the need for human intermediaries to conduct operations.[121] In turn, this allows the benefits related to transparency, inclusion, and security mentioned above to positively impact community governance.[122]

Increasingly, Web3 ecosystems will leverage DAOs, as their novel organizational structure allows users and builders to own their contributions to networks, intellectual property, and digital identities.[123] This direct participation along with self-custody features mark a stark shift from the status quo of Web2. When DAOs distribute governance tokens to DAO members in a manner that promotes protocol participation and use, user-stakeholders are incentivized and rewarded for contributions in a more equitable manner than in traditional companies.[124] As DAOs, foundations, and businesses continue to experiment with community governance and progressive decentralization, the results found in protocols like Compound will continue to replicate.[125]

[120] Theodor Marcu, *The ABCs of DAOs: How Decentralized Autonomous Organizations are Automating the Corporation*, The Network State (June 20, 2021), https://thenetworkstate.com/daos.

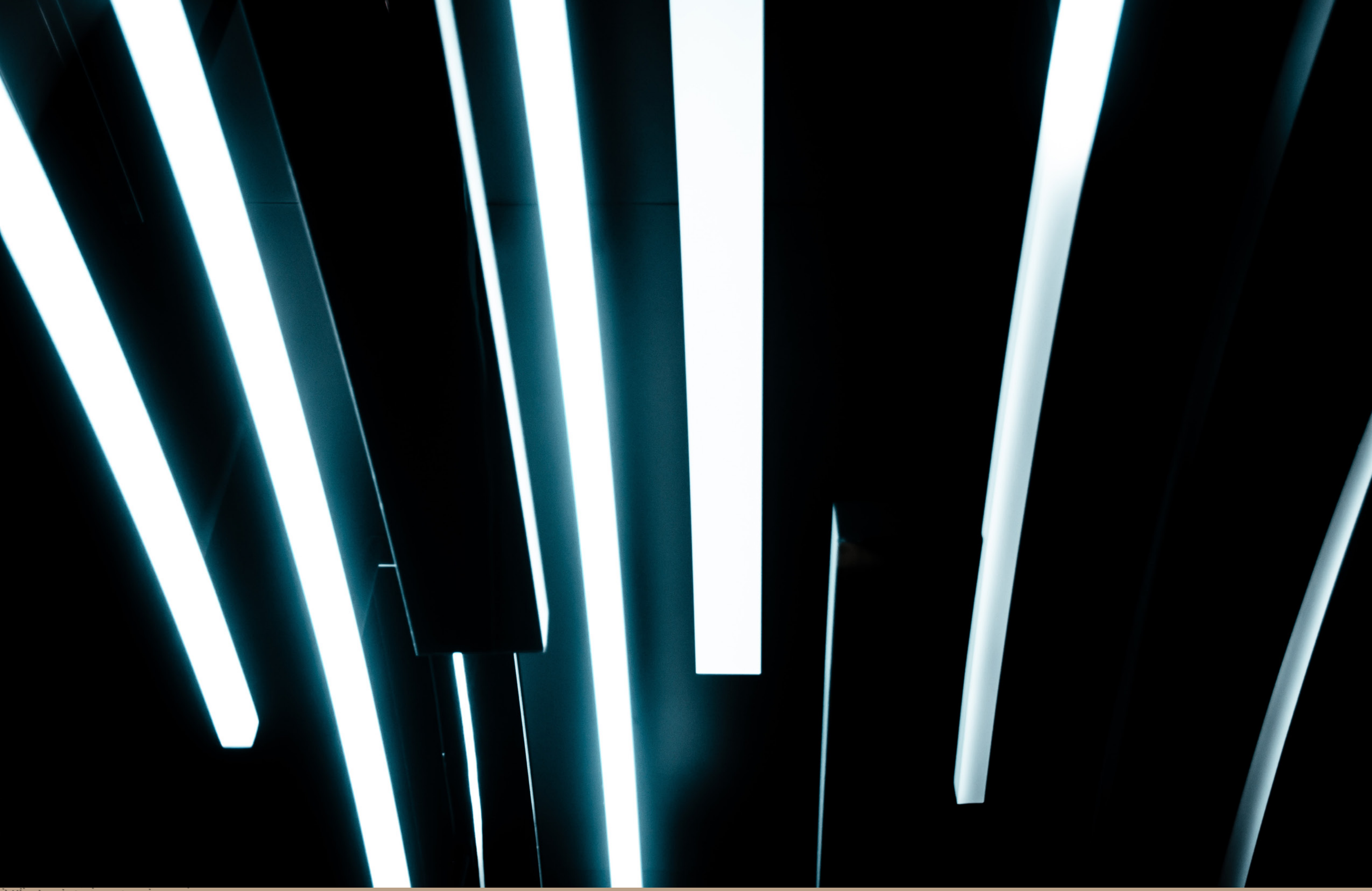
[121] *Id.*

[122] DAOs sharing similar missions may need to compete for top member contributors and are therefore incentivized to be as transparent as possible and not engage in exploitative rent extraction from the group. Because proposals to improve the protocol are shared publicly to be voted on by all network participants, the transparent nature of governance decisions also provides a channel for risk mitigation via public participation. *See* Xie, *supra* note 108.

[123] *See* Letter from Andreessen Horowitz to HM Treasury, *supra* note 40, at 3.

[124] *Id.*

[125] *See*, e.g., *Introducing UNI*, Uniswap Labs (Sept. 15, 2020), https://blog.uniswap.org/uni.



4 Risks of DeFi

Source: @maximalfocus/unsplash

A. Current risks

As mentioned above, DeFi activities may be similar to those in TradFi, but the risks can be fundamentally different. For example, the decentralized design of DeFi protocols may eliminate or significantly reduce traditional financial risks, such as counterparty, credit, and custodial risks, while introducing other kinds of risks. Key DeFi risks are often operational, relating to flaws in the design, governance, or interconnections in the decentralized system.

This section briefly surveys some of the significant risks present in DeFi. First, illicit actors may use DeFi protocols to conduct money laundering operations. Second, the concentration of control in some cases of DAO governance may facilitate unilateral decision-making to the detriment of the majority of token holders. Third, layers of the technology stack, such as the protocol or the underlying blockchain, may not function as intended or be co-opted for malicious purposes. Finally, greater interconnectedness between TradFi and DeFi may introduce spillover risks from one financial system to another. Note that many of these mentioned risks stem from centralization-driven vulnerabilities.

DeFi-related technology solutions are emerging that can help mitigate some of these issues. These solutions help address these risks by ensuring or reinforcing the decentralized nature of the DeFi system. For example, as articulated below, newly-designed voting mechanics like quadratic voting aim to address DAO governance issues (discussed below) by reducing concentration in governance.[126]

Moreover, while Public Good Protocols may not eliminate these risks altogether, the inherent qualities of Public Good Protocols can help address them and may even make some risks comparatively *less* risky than their TradFi counterparts. Public Good Protocols do not mitigate risk entirely, but we argue they are a material improvement of the status quo.

Lastly, we recognize that while DeFi native technological improvements and the use of Public Good Protocols can reduce the risk for users significantly, regulators may still find that there is unacceptable risk remaining. Following the DeFi Protocol Risks section below, we propose a regulatory approach that follows the updated principle of '*Same Activity, Different Risk, Different Regulation but Same Regulatory Outcome*.' This regulatory approach targets DeFi applications and businesses, not the underlying Public Good Protocols.

[126] *See* discussion *supr*a 'Benefits of DeFi: Participatory Stakeholder Governance'; discussion infra 'Flawed DAO Governance: Solving the DAO Dilemma'.

B. DeFi protocol risks

Protocols can have several risk factors that stem from their design, data they rely on (i.e., oracles127), the blockchain on which they were built, and their governance. These risks generally fall into five main categories:

1. illicit finance/AML risks;[128]
2. flawed protocol governance;
3. cybersecurity vulnerabilities;
4. underlying blockchain risks; and
5. interconnections with the traditional financial system[129]

Some of the risks that fall into these categories have analogs in TradFi, such as credit, market and liquidity risks. For example, during times of extreme price volatility that trigger liquidation of lenders' positions, DeFi lending protocols may not have the sufficient reserves necessary to return assets to lenders.

However, technical developments, alongside the benefits inherent in the features of Public Good Protocol, are addressing these challenges.[130] For example, the lending protocol Aave is permissionless, meaning anyone can use it to borrow digital assets regardless of their credit status or identity profile. To ensure that lenders are paid back, the Aave protocol requires borrowers to provide collateral in digital assets with value greater than the amount of digital assets borrowed.[131] This overcollateralization requirement minimizes the credit risk exposure for lenders. Moreover, the Aave protocol utilizes autonomous smart contracts that automatically liquidate borrowers' positions when they fail to maintain their collateral ratios during negative price swings.[132] These automatic liquidation mechanisms could present a risk of amplifying volatility in the event of widespread liquidations. However, enhanced protocol reserves, conservative collateralization ratios, insurance pools (often referred to as 'safety modules') and other measures can mitigate much of this risk. Additionally, systemic impacts will likely be reduced in a more mature crypto asset ecosystem where greater asset diversity can provide a more diversified collateral pool that can help reduce price volatility and correlations across these assets.

However, many of the risk categories contain operational risks without analogs in the traditional financial system. They are usually related to the protocol's design, technologies used, and governance arrangements that do not ensure decentralization. For instance, some DeFi protocols offer so-called 'flash loans.' Flash loans are typically repaid in the same blockchain transaction, so there is minimal liquidity and credit risk. But they do give potential hackers or manipulators access to unlimited leverage, which they can use for a 51% attack.[133]

[127] Blockchain oracles are third-party services that connect blockchains to external systems for information, such as off-chain prices, temperature, or other real-world inputs. *See What is the Blockchain Oracle Problem?*, Chainlink (May 24, 2023), https://chain.link/education-hub/oracle-problem.

[128] CCI will be issuing a paper on DeFi and Illicit Finance/AML regulation later this year.

[129] Carter & Jeng, *supra* note 26, at 7-9.

[130] Examples of private sector solutions to the reliability of oracle information include decentralized oracle networks, which aid in preventing oracle attacks. *See, e.g., What is the Blockchain Oracle Problem?*, *supra* note 127.

[131] Roberto de Isidro, *Aave: The Basics,* GlobalX (Mar. 14, 2023), https://www.globalxetfs.com/aave-the-basics/.

[132] *Risk Parameters*, Aave (Last visited May 31, 2023), https://docs.aave.com/risk/asset-risk/risk-parameters.

[133] *See* Carter & Jeng, *supra* note 26 at 16.

① Protocol Risk: Illicit finance/AML risks

According to the U.S. Department of the Treasury's Illicit Finance Risk Assessment of Decentralized Finance, illicit actors, including "ransomware cybercriminals, thieves, scammers, and Democratic People's Republic of Korea (DPRK) cyber actors," have been found to use DeFi services for purposes of money laundering and transferring illicit proceeds.[134] DeFi's use by illicit actors is a legitimate threat that needs to be addressed and mitigated.

Overall, blockchain analysis has assessed that in 2022, a very small percentage of crypto asset transactions, including both CeFi and DeFi activity, came from known illicit sources.[135] Interestingly, the majority of funds leaving ransomware wallets[136] end up at centralized exchanges,[137] presumably to cash out to fiat, with only a small proportion going to DeFi.[138] This demonstrates that the issue may largely lie with insufficient centralized exchange supervision and compliance, rather than with DeFi. In general, the visibility of crypto asset transactions allows the public to track on-chain activity, helping financial authorities to investigate launderers and potentially recover illicit proceeds.[139] Nonetheless, increased monitoring, continued private sector innovations (including tools to enhance centralized exchange supervision and compliance), and industry collaboration with the public sector are necessary to advance the efforts to deter illicit activity. This is far from a comprehensive discussion of illicit finance regulatory challenges with DeFi, and CCI plans to release a more detailed paper to discuss the illicit finance and AML risks in DeFi and to discuss potential regulatory approaches.

② Protocol Risk: Flawed protocol governance

A commonly discussed issue with protocol governance is the lack of distribution in overall governance participation, whether through a DAO or other arrangement. DAOs have become an important mechanism for many protocols. Some DAO members tend to be more active in voting on DAO governance proposals than others—a common problem with many voting systems in general (including U.S. elections). This concentration of voting participation in a smaller group of token holders could lead to protocol governance being concentrated in the hands of a few parties. In turn, these few parties could attempt to benefit at the expense of other DAO members.[140]

[134] Illicit *Finance Risk Assessment of Decentralized Finance*, U.S. Dep't of the Treasury at 1 (Apr. 2023) https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[135] *See The 2023 Crypto Crime Report,* Chainalysis at 7 (2023), https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf. ("[I]llicit activity in cryptocurrency remains a small share of total volume at less than 1%."). *See also* Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity, Chainalysis (Jan. 6, 2022).

[136] Ransomware is a type of malicious software that blocks access to a user's computer system or threatens to leak sensitive or personal data. The goal of most ransomware attacks is to extort a ransom payment in exchange for restoring access to sensitive encrypted data. Ransomware has become a powerful tool for bad actors targeting users that could potentially lose their all-important data. *See generally Cryptopedia: Ransomware*, Gemini, https://www.gemini.com/cryptopedia/glossary#ransomware (last visited June 23, 2023).

[137] CeFi Exchanges have monitoring tools in place for this that track funds coming from and going to known illicit wallet addresses, file SARs, and work closely with law enforcement if subpoenaed to turn over customer data in the course of illicit finance investigations. *See, e.g., Paul Grewal, Transparency Report 2022*, Coinbase (Dec. 12, 2022), https://www.coinbase.com/blog/transparency-report-2022. Some Decentralized Exchanges like Uniswap also use these monitoring tools and report suspicion of illicit usage to law enforcement. *See e.g.,* Terms of Service: 3.4 Additional Rights, Uniswap, https://uniswap.org/terms-of-service (last visited June 13, 2023); Alison Jimenez, 2021 Cryptocurrency Exchange Suspicious Activity Reports, Sec. Analytics (Feb. 2, 2022), https://securitiesanalytics.com/2021-cryptocurrency-exchanges-suspicious-activity-reports/; Crypto Incident Response, Chainalysis, https://www.chainalysis.com/crypto-incident-response/ (last visited June 13, 2023).

[138] The 2023 Crypto Crime Report, *supra* note 135, at 30 (noting that 48.3% of ransomware funds went to mainstream CeFi exchanges in 2022).

[139] *See e.g., id.* at 54 (noting seizures made by governments enabled to track down funds using blockchain: $3.6 billion from two individuals accused of laundering funds stolen from a 2016 hack, an additional $3.6 billion seized from defunct dark web market 'Silk Road', and $30M from North Korean hacking syndicate 'Lazarus Group').

[140] *See, e.g., The Financial Stability Risks of Decentralized Finance, supra* note 9, at 12-13 (showing features of particular DeFi governance tokens and the high concentrations of those tokens among the top 100 largest wallets).

DAOs are a new construct and continue to evolve and develop more nuanced and sophisticated models that can mitigate this concentration risk—which is, in itself, a risk of centralization. DAOs should be incentivized to progressively decentralize. It is also in a DAO's interest to encourage greater user participation to increase use of the protocol. In turn, users, by holding governance tokens, benefit as owner participants of the protocol. For instance, DAOs may use token rewards to incentivize participants to use or contribute to the protocol. This shared ownership model can generate positive network effects for the usage and utility of the protocol, which in turn attracts more participant engagement.[141] At a minimum, the incentives for DAOs are such that decisions are likely to be made in a less concentrated manner than traditional corporations.

Furthermore, progressive decentralization of a protocol—a process in which founding teams relinquish control of a protocol to the community by degrees over time—is becoming more common as founding teams are developing better practices. For example, when a founding team is in the early stages of establishing product-market fit, the team may find operating as a centralized entity beneficial.[142] However, the team may subsequently invite community participation in product development through the establishment of a DAO when the protocol enters the growth stage. Network effects may gradually reach a point where the community through the DAO can sufficiently support and govern the protocol without the founding team. At that point, the protocol and its governing DAO may then be considered sufficiently decentralized.[143] This outcome also reflects the user empowerment and ownership sharing model of Web3.[144]

In addition to novel experimentation with progressive decentralization by developer teams, technological research and advances are helping to encourage more active user participation, reduce information asymmetries, and promote representative governance. For example, quadratic voting aims to even out the distribution of voting power by scaling up the number of tokens required to cast an additional vote quadratically rather than linearly. This design helps to reduce concentration risks when active voting members make up a smaller portion of the total number of DAO members.[145] Additional tools and innovations for reducing concentrations of power and influence during the voting process include proof of personhood,[146] Web of Trust,[147] and proof of participation (POAP).[148]

While DAOs have been around for just over five years, best practices have begun to emerge. These include constraining decision-making to parameter setting (i.e., fees, collateralization ratios), treasury management, and protocol governance.[149] So long as users retain custody of their assets, a particular DAO's characteristics, such as its degree of centralization or how long it takes for a change to be approved, will not be able to inflict significant harm to a protocol's users or affect the safety of the protocol. Likewise, because DAOs do not directly custody user assets, malicious actors simply cannot access users' funds in the event of a governance attack. On the other hand,

[141] *See id.* at 13 ("Theoretically, a truly distributed decision-making process contributes to greater decentralisation, becoming more dynamic and responsive to its community and stakeholders.").

[142] Jad Esber & Scott Duke Kominers, *Progressive Decentralization: A High-Level Framework,* a16z crypto (Jan. 12, 2023), https://a16zcrypto.com/posts/article/progressive-decentralization-a-high-level-framework/.

[143] *See generally* Miles Jennings, *Principles & Models of Web3 Decentralization,* a16z Crypto at 13-24 (Apr. 6, 2022), https://a16z.com/wp-content/uploads/2022/04/principles-and-models-of-decentralization_miles-jennings_a16zcrypto.pdf (articulating various models of progressive decentralization through the use of incentives and community governance).

[144] *See* Jad Esber & Scott Duke Kominers, Why Build in Web3, Harvard Bus. Rev. (May 16, 2022), https://hbr.org/2022/05/why-build-in-web3 (explaining the sense of psychological ownership fostered by Web3 wherein users become 'fans' of a platform, seeing it as an extension of their own values).

[145] A simple form of quadratic voting may require only one token for a single vote, but four tokens for a second vote and nine tokens for a third vote, making it significantly more difficult for individuals to acquire an outsized share of votes through amassing governance tokens. *See* Vitalik Buterin, Zoë Hitzig & E. Glen Weyl, *Liberal Radicalism: A Flexible Design for Matching Funds,* Soc. Sci. Rsch. Ctr., 1-17 (Sept. 18, 2018) (explaining quadratic voting).

[146] *See generally* Divya Siddarth et. al., Who Watches the Watchmen? *A Review of Subjective Approaches for Sybil-resistance in Proof of Personhood Protocols,* Cornell arXiv at 3-23 (Oct. 13, 2020) (providing a review of the various digital sources of authentication).

[147] *Id.* at 10-11.

[148] *Id. See also Moving Beyond Coin Voting Governance,* Vitalik Buterin (Aug. 16, 2022), https://vitalik.ca/general/2021/08/16/voting3.html.

[149] Jennings & Quintenz, *supra* note 36.

users who disagree with the decisions voted on at a DAO may express their dissatisfaction by withdrawing funds from the protocol or creating a newer version of the protocol (i.e., forking).[150]

Recent enforcement actions against DAOs have demonstrated that while these structures present novel forms of stakeholder governance, members are not necessarily shielded from liability in the same manner as in traditional corporations.[151] Due to this limitation, DAO members that engage in lawful activity may fear engaging in meaningful governance decisions, as there may be seemingly unknown risks. The use of legal structures has already aided in resolving some uncertainty among DAO members, and we are encouraged by, and urge further legislative developments recognizing DAOs as legal entities.[152]

Solving the DAO Dilemma

While Web1 protocols like HTTP and Web3 protocols are both autonomous, only the latter can accrue value. For example, the SMTP protocol does not have stakeholders, meaning no one receives fees or other forms of value from SMTP when emails are sent, and no one is incentivized to encourage use of SMTP. In contrast, Web3 protocols may have mechanisms for value accrual, and this value is often transferred to the DAOs to facilitate upgrades or changes to the protocol.[153]

However, third party apps that do not comply with a 'Regulate Businesses, Not Public Good Protocols' regulatory framework (as described in the Policy Recommendations section) can still access Public Good Protocols and, therefore, create residual risk. Namely, as DAOs of Public Good Protocols can generate revenue from transactions derived from non-compliant apps, they may be incentivized to facilitate non-compliant activity with non-compliant third-party apps. The question then becomes, how should this residual risk be minimized?

Regulation should require Public Good Protocols to have the fundamental features as outlined in prior sections: decentralized, autonomous, open source, standardized, and non-discriminatory. However, regulation of a business cannot be effective in achieving its policy objectives without proper incentives for compliance. Consequently, any Web3 regulatory framework must resolve this 'DAO Dilemma' by mitigating this residual risk of DAOs permitting non-compliant, third-party apps to use Public Good Protocols.

We propose a solution that draws on smart contract architecture first presented by Andreessen Horowitz. We note that the following Default Value Accrual (DVA) architecture abides by the principle of 'Same Activity, Different Risk, Different Regulation but Same Regulatory Outcome'[154] and targets DAOs and not protocols as the relevant sites of regulation.

For-profit DAOs, which receive fees from applications accessing a protocol, should ensure that each app accessing the protocol is doing so via separate gateway smart contracts that segregate transactions according to each respective app business. Each transaction performed via these app-specific smart contracts should be authenticated by the app's private key.

[150] This is commonly referred to as 'rage quitting' among crypto users. *See, e.g.,* Danny Nelson, ROOK Investors Aim to 'Rage Quit' Through Plan to Liquidate $25M Crypto Treasury, CoinDesk (Apr. 11, 2023), https://www.coindesk.com/business/2023/04/11/rook-investors-aim-to-rage-quit-through-plan-to-liquidate-25m-crypto-treasury/.

[151] *See* CFTC v. Ooki DAO, No. 3:22-CV-5416, 2022 WL 17822445 (Dec. 20, 2022).

[152] *See, e.g.,* Wyo. Stat. §§ 17-31-101 to 110 (West 2023); H.B. 3768, 88th Legis. (Tex. 2023); So Saito & Sergio Elias-Wilson, *Decentralized Autonomous Organization under Japanese Law,* So & Sato Innovative Lawyers (Nov. 9, 2022), https://innovationlaw.jp/en/dao-under-japanese-law/ (providing the legal background of Japan's current regulation regime related to DAOs); Taras Zharun, *Swiss Foundation as a DAO Legal Wrapper: What You Need to Know,* LegalNodes (Aug. 4, 2022), https://legalnodes.com/article/swiss-foundation-dao-legal-wrapper (explaining the legal status of DAOs in Switzerland).

[153] *See* discussion *supra* part 'Benefits of DeFi: Participatory Stakeholder Governance'.

[154] *See* discussion infra section 'Same Activity, Different Risks, Different Regulation, Same Regulatory Outcome (NOT 'Same Activity, Same Risk, Same Regulation').'

Solving the DAO Dilemma - Continued

This default, app-based segregation of transactions would allow for jurisdictional variations in regulation. For instance, hypothetical business-level regulation may require DAOs to transmit the fees accrued from an app trading unregistered securities in the US to a public service organization, such as our proposed Independent Certification Regime Organization (ICRO) (see Section V) or a government agency. This transfer arrangement of fees derived from non-compliant activities could be achieved through additional smart contracts that automatically divert funds associated with the address of a non-compliant app.

A DVA mechanism could eliminate the incentive for DAOs to encourage non-compliant activities on the protocol by siphoning off funds before reaching the DAO. This consequently reduces the universe of non-compliant apps and allows regulators to target them without jeopardizing the credible neutrality of the underlying protocol infrastructure.

This DVA mechanism solution aligns with the decentralized, open source, autonomous, standardized, and non-discriminatory characteristics of Public Good Protocols.[155] It ensures the credible neutrality of the protocol by neither motivating nor banning non-compliant apps from connecting to the protocol. Doing either of those things would threaten the permissionless nature of Public Good Protocols by introducing discriminatory behavior.

Moreover, a regulatory regime could create incentives for DAOs to implement this technical architecture. For example, if individual, identifiable members in a DAO are deliberately encouraging businesses to use the protocol for non-compliant activities, the relevant regulatory agency should have the ability to enforce against or penalize these bad actors.[156] If DAOs were subject to ex ante regulation, there would be strong incentives to implement such compliance measures in their architecture at inception.

It is crucial, however, to note that the novelty and potential complexity of determining when and how individual DAO members are subject to liability. For a fair and accessible Web3, fundamental legal principles that protect individual rights, ensure adversarial testing, and improve the prospect of an enforceable judgment are all needed.[157] Wrapping a DAO in a legal entity structure or siloing the financial activities of the DAO in a separate legal entity structure may help limit the risks to individual DAO members while encouraging a safe and compliant DeFi ecosystem.[158]

Lastly, as we articulate further in the Policy Recommendations section, relevant regulators could create other motivating forces for DAOs to implement DVA mechanisms. For example, we propose a safe harbor regime that provides a means for centralized businesses to progressively decentralize their centrally managed protocols into Public Good Protocols. ICROs or the relevant regulatory body could make this safe harbor treatment contingent upon the DAO having a DVA mechanism in the DAO's smart contract architecture.[159]

[155] Jennings & Quintenz, *supra* note 36.

[156] *Cf. Id.* (underscoring the importance of maintaining the ability to pursue legal action against individuals who perpetrate crimes via email without banning the use of SMTP altogether).

[157] *See* Brief for Ooki DAO as Amicus Curiae Regarding Plaintiff's Motion for Alternative Service, CFTC v. *Ooki DAO*, N.D. Cal. (2022) (No. 3:22-cv-05416-WHO) at 13 n.9.

[158] *See* Miles Jennings, *Regulate Web3 Apps, Not Protocols Part III: The Web3 DAO Dilemma*, A16Z CRYPTO (Jan. 1, 2023), https://a16zcrypto.com/posts/article/regulate-web3-apps-not-protocols-part-iii-the-web3-dao-dilemma/#section–4.

[159] *See* discussion *infra* 'Independent Certification Regime Organization or 'ICRO': a self-regulating entity.'

3 Protocol Risk: Cybersecurity vulnerabilities

Cybersecurity risk mitigation must be folded into the fabric of all levels of the DeFi technology stack. While discussion of DeFi cybersecurity risks typically focuses on the resiliency of the underlying blockchain, cybercriminals are more likely to exploit smart contract vulnerabilities of the DeFi protocol.[160] The Federal Bureau of Investigation (FBI) has noted that hackers target "the complexity of cross chain functionality and open source nature" of DeFi services.[161] In 2022, just over 82% of crypto assets stolen by cybercriminals came from hacks of DeFi protocols.[162] But interestingly, as much as 69% of these protocol hacks were hacks of cross-chain bridge protocols, not protocols built on top of base layer blockchains.[163] These figures show that cross-chain bridges are a significant vulnerability to the DeFi system, and many of these bridges are controlled by a single or small group of parties.

The FBI highlighted three typologies by criminals exploiting smart contracts in DeFi cyberattacks: (1) initiating a flash loan to exploit a smart contract vulnerability, allowing the attacker to drain funds within the bounds of the contract; (2) exploiting token bridge signature requirements to steal investment funds, and (3) taking advantage of a platform's reliance on a single oracle by conducting leveraged trading to manipulate pricing and exploit pricing errors.[164]

A Code auditing and bounty programs

Thorough auditing of smart contracts acts as a critical line of defense and is the prime method for preventing DeFi cybersecurity attacks.[165] A cottage-industry of smart contract auditors have emerged, and these companies utilize experienced developers, automated systems, and simulations to review smart contract code for logical and technical flaws, threat models, divergences from white papers, and other deficiencies that can cause programs to operate in ways other than intended.[166] Additionally, developers will often aim to improve smart contracts' security through the use of bounty programs, wherein community members are rewarded for identifying smart contract deficiencies.[167]

B Specific oracle risks

DeFi protocols often rely on data oracles, which are technical systems that enable the integration of off-chain data.[168] However, the potential inaccuracy of data feeds from oracles may create vulnerabilities for DeFi protocols, especially those that rely on such data to execute functions instantaneously. Vulnerabilities range from the potential

[160] A recent exploit of Curve by hacking pools related to Curve allowed hackers to steal approximately $62 million. This hack exploited bugs in the compiler that used Vyper, a programming language used to write smart contracts. This is a problem with any smart contract that uses the Vyper compiler. 12Swap, *Curve Exploit Explained*, Medium (Aug. 4, 2023), https://medium.com/@onetwoswap/curve-exploit-explained-72555ab405e9#:~:text=4-,Global%20problem%20behind%20Curve%20exploit,fell%20by%20more%20than%2020%25.

[161] *Public Service Announcement: Cyber Criminals Increasingly Exploit Vulnerabilities in Decentralized Finance Platforms to Obtain Cryptocurrency, Causing Investors to Lose Money*, Fed. Bureau of Investigation (Aug. 29, 2022), https://www.ic3.gov/Media/Y2022/PSA220829 (last visited June 22, 2023).

[162] *2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers*, Chainalysis (Feb. 1, 2023), https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/.

[163] *See Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk*, Chainalysis (Aug. 2, 2022), https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/.

[164] *See* Fed. Bureau of Investigation, *supra* note 161.

[165] *See Smart Contract Audits Are Your First Line of Defense Against DeFi Exploits: Here's Why*, HackerNoon (Dec. 10, 2022), https://hackernoon.com/smart-contract-audits-are-your-first-line-of-defense-against-defi-exploits-heres-why; *see also* Fed. Bureau of Investigation, *supra* note 161 (providing a recommendation from the FBI for DeFi investment platforms to conduct code audits).

[166] *See, e.g.*, Solidity Finance, https://solidity.finance/ (last visited June 22, 2023); OpenZeppelin, https://www.openzeppelin.com/ (last visited June 22, 2023).

[167] *See Daniel Perez & Benjamin Livshits, Smart Contract Vulnerabilities: Does Anyone Care?*, Cornell Arxiv at 2 (Feb. 2019), https://allquantor.at/blockchainbib/pdf/perez2019smart.pdf.

[168] *See, e.g., Applications of Oracles in Smart Contracts*, Ethereum Found., https://ethereum.org/en/developers/docs/oracles/#applications-of-oracles-in-smart-contracts (last visited June 23, 2023) (describing the host of existing cases demonstrating the utility of oracles in smart contract development, including retrieving financial data, generating verifiable randomness, creating prediction markets based on real world events, and automating smart contracts).

manipulation of data by centralized oracles[169] to those associated with parties seeking to profit and exploit DeFi protocols that depend on particular data feeds.[170] When a DeFi protocol relies on deprecated, manipulated, malicious, or otherwise inaccurate data, the resulting damage can be significant.[171]

To mitigate the risk of oracle manipulation and attenuate the potential for oracle-based smart contract exploits, it is advised that DeFi protocols incorporate a methodology that leverages decentralized oracles[172] and harnesses median values derived from multiple independent sources or employs time-weighted average price feeds from varied data inputs.[173] Although completely eradicating oracle risk presents a considerable challenge, these methodologies provide robust and pragmatic solutions for risk mitigation in DeFi protocols.

C **Cross-chain interoperability risks and bridging risks**

Interoperability across blockchains is typically provided by bridges, which hold a crypto asset token from one blockchain and provide a representation of it (i.e. "wrapped token") to be used in a second blockchain.[174] Bridges are an important component of the DeFi ecosystem because they allow developers to create decentralized applications that interact with and utilize the distinctive features of multiple different blockchains, ultimately providing DeFi users with more features and a smoother experience.[175] However, as a relatively new innovation, cross-chain bridges have been the targets of some of the largest crypto asset hacks in recent history.[176] Due to the high concentration of locked assets, bridges have become a common target for crypto asset theft and hacks. In addition to the loss of user assets, cybersecurity risks in bridges are problematic because of contagion effects that impact the assets across multiple blockchains.[177] While bridging risks remain an important topic in DeFi cybersecurity risks, some solutions proposed include increasing code auditing before the launch and during the operation of the bridge, increasing the number of validators, and implementing a bug bounty program to prevent future attacks.[178]

D **Other means to address these cybersecurity risks**

In addition to the solutions articulated above, we provide a few other means to mitigate cybersecurity risks. First, government agencies should support the formation of public-private information sharing and analysis centers (ISACs),[179] analyzing how standards related to traditional finance and cybersecurity risk management can be interpolated into DeFi.[180] Currently, there is an effort among crypto asset and cybersecurity experts to create a crypto asset ISAC, where the industry can coordinate responses to crypto hacks and establish industry

[169] *Centralized Oracles*, Ethereum Found., https://ethereum.org/en/developers/docs/oracles/#centralized-oracles (last visited June 23, 2023) (discussing the types of oracles and the issues associated with centralized oracles); *Oracle Manipulation Attacks*, Smart Contract Security Field Guide, https://scsfg.io/hackers/oracle-manipulation/ (last visited Sept. 20, 2023).

[170] Smart Contract Security Field Guide, *supra* note 169.

[171] *Id.*

[172] *See* Tarun Chitra & Guillermo Angeris, *Improved Price Oracles: Constant Function Market Makers* (June 21, 2020) at 2-3, (discussing the security benefits of decentralized oracles). *See also* Smart Contract Security Field Guide, *supra* note 169.

[173] Smart Contract Security Field Guide, *supra* note 169.

[174] *See* Fin. Stability Bd., *supra* note 140.

[175] *Cross-Chain Bridges and Associated Risks,* Chainlink, https://docs.chain.link/resources/bridge-risks (Last visited June 23, 2023).

[176] *See, e.g., Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk,* Chainalysis (Aug. 2, 2022), https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/; Martin Köppelmann, *Bridge Exploits Cost $2B in 2022, Here's How They Could Have Been Averted,* CoinDesk (June 2, 2023), https://www.coindesk.com/consensus-magazine/2023/06/02/bridge-exploits-cost-2b-in-2022-heres-how-they-could-have-been-averted/.

[177] *See* Fin. Stability Bd. *supra* note 140.

[178] *See* Coby Moran, *Blockchain Bridges Keep Getting Attacked: Here's How to Prevent It.*, CoinDesk (Oct. 14, 2022), https://www.coindesk.com/layer2/2022/10/14/blockchain-bridges-keep-getting-attacked-heres-how-to-prevent-it/.

[179] An Information Sharing and Analysis Center (ISAC) is a non-profit entity, which accumulates data on cyber-related threats to critical infrastructure and facilitates information exchange between the private sector and governmental agencies. *See, e.g.,* FS-ISAC, https://www.fsisac.com/ (last visited July 24, 2023).

[180] *See* Crypto Council for Innovation, Comment Letter on the Office of Science & Technology Policy's Request for Information regarding Digital Assets Research and Development (June 23, 2023), https://cryptoforinnovation.org/wp-content/uploads/2023/03/OSTP-RFI-CCI-Comment-Letter-March-2023.pdf.

cybersecurity standards and best practices.[181] Industry members have also developed online platforms where individuals and firms can report illicit activity, including hacks.[182]

Moreover, similar to how the Public Company Accounting Oversight Board (PCAOB) creates and enforces standards for auditors of public companies, the development of industry-consulted code auditing standards would assist in protecting consumers from auditing rubber stamps. Instead, an Independent Certification Regime Organization could develop these standards (described later in the Policy Recommendations section).[183] As also described in this section, a mandatory disclosure regime is critical to educating users about the dangers of using DeFi protocols that are not code audited.[184] As DeFi protocols continue to evolve and encourage further user experimentation, the attack surface area malevolent actors can target will only increase,[185] stressing the need for our aforementioned solutions.

4 Protocol Risk: Underlying blockchain risks

DeFi protocols also are exposed to risks posed by their underlying blockchains. For instance, blockchains are built and maintained by validators. Validator-related risks include MEV. Due to the high transparency of Ethereum, validators can frontrun blockchain transactions and selectively order them to their benefit.[186] One can argue that the risk is similar to information asymmetries in TradFi with high frequency traders trading at traditional exchanges.[187] But these risks involve a new category of participants—the validators—whose job it is to maintain a neutral public blockchain. Accordingly, economic incentives will need to be incorporated into the blockchain to properly incentivize validators and other participants who support blockchain maintenance. For example, private sector solutions, such as Chainlink's Fair Sequencing Service (FSS), derived from academic research on transaction order fairness and transaction data encryption, help address MEV by removing the temporary centralization in the mining process and decentralizing the transaction ordering process.[188]

In addition, the underlying blockchain may suffer network congestion during times of high use or stress. Ransomware attacks and other software exploits also may trigger network congestion and cause spikes in transaction fees.[189] Blockchain base layers (Layer 1s) that aim for greater scalability and cheaper transaction costs, roll-ups, and Layer 2 scaling solutions that overlay the Layer 1 blockchain are some forms of technological solutions in development to address this network congestion issue.[190]

[181] CryptoISAC, https://www.cryptoisac.org/ (last visited July 24, 2023).

[182] ChainAbuse, https://www.chainabuse.com/ (last visited July 24, 2023).

[183] *See* Gerard Brennan & Sheng-Feng Hsieh, *Issues, Risks, and Challenges for Auditing Crypto Transactions,* Int'l J. Acct. Info. Sys. 10-11 (Aug. 2022) ("[I]t is the 'wild west' for entities with material positions in crypto assets just trying to figure out on their own how to best report these crypto asset-related transactions and balances within existing accounting standards. It is also unclear for auditors how to identify and execute appropriate audit procedures when they are performing financial audits in which crypto assets are significantly involved. . .[L]aws to regulate crypto asset transactions and centralized service providers are 'fragmented' worldwide. This fragmentation also increases the complexity and risk of external audit compliance with related international regulations and standards.").

[184] *See* discussion *infra* part 'Independent Certification Regime Organization or 'ICRO': a self-regulating entity.'

[185] For example, in the Uniswap v4 whitepaper, the innovation of 'hooks'—customizable rules added to a liquidity pool to automatically trigger certain operations—carries potential risk. If a hook is programmed incorrectly or maliciously, it may induce unexpected behavior in the liquidity pool (i.e., higher or lower fee rates, total lack of fees, etc.). Or, if a contract deployer maintains control of the hooks, they could be easily manipulated for personal gain. Unchained, *The Chopping Block: Why Uniswap V4 Creates a Bigger Attack Surface Area,* Laura Shin (June 15, 2023), https://podcasts.apple.com/us/podcast/the-chopping-block-why-uniswap-v4-creates-a/id1123922160?i=1000617136798; *see generally* Adams et al. *supra* note 20.

[186] Carter & Jeng, *supra* note 26, at 17.

[187] *Id.; see also Philip Daian et al., Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges,* Cornell Arxiv (Apr. 10, 2019).

[188] Ari Juel, *Fair Sequencing Services: Enabling a Provably Fair DeFi Ecosystem*, Chainlink (Sept. 11, 2020), https://blog.chain.link/chainlink-fair-sequencing-services-enabling-a-provably-fair-defi-ecosystem/.

[189] *See* Konstantin Sokolov, *Ransomware Activity and Blockchain Congestion*, 141 J. of Fin. Econ. 771, 772-73 (2021) (noting that the likelihood of bitcoin block congestion increases by 15%–27% during a typical spike in ransomware activity).

[190] John Fáwolé & Bartosz Barwikowski, *Blockchain Layer 1 vs Layer 2 Scalability Solutions,* Hacken (May 11, 2023), https://hacken.io/discover/l1-l2-scalability/#Layer_1_Network.

Other operational risks related to the architecture of the blockchain can be thought of as issues relating to establishing consensus—a mechanism whereby all the nodes of a distributed blockchain network agree about the information on a set of transactions. Consensus is necessary for verifying the authenticity of transactions and ensuring the general security of the blockchain.[191] On the one hand, difficulties in reaching an agreement may lead to rare instances of network outages due to consensus failures.[192] On the other hand, concentrations of power in the validation process could lead to 51% attacks or validator cartels, leading to blockchain alterations to the benefit of those in control.[193] Depending on specific objectives, alternative consensus mechanisms to Proof of Work (PoW) or PoS,[194] such as DPoS, may alleviate the outlined risks by increasing decentralization or bolstering the objectivity of transaction ordering.[195]

5 Protocol Risk: Interconnections with the traditional financial system

As more TradFi institutions and users engage with DeFi, the interconnectedness between the two sectors grows. The consequent network effects and the resulting influx of capital lead to further innovation, increased efficiency, and gains from economies of scale. However, risks like DeFi protocol failures or stablecoin runs (i.e., an influx of conversion demands from crypto to fiat currency) may expose TradFi institutions to crypto sector risks. However, significant risks spilling over from DeFi into TradFi have yet to materialize. For example, the collapse of Terra/Luna that led to $40 billion in losses did not affect the traditional financial system, but it did expose many CeFi actors who were over-leveraged. Conversely, crises arising from TradFi have spilled over into the DeFi ecosystem.[196] For example, when Silicon Valley Bank collapsed, 8% of USDC's cash reserves were stuck at the bank leading to a temporary dollar de-peg of one of the most important payment stablecoins used in DeFi.[197]

Stablecoins are crypto assets designed to trade at par with a reference asset (such as the US dollar), typically used as a means of payment or store of value.[198] Stablecoin issuers are typically centralized, especially fiat-backed payment stablecoins. Stablecoins are vitally important in DeFi as they provide the main form of value transfer (i.e., payment) in DeFi systems.[199] The use of stablecoins enables users to move funds between various DeFi applications without having to convert their assets into fiat currencies or to use slow traditional bank payment mechanisms (e.g., ACH, wire transfers, etc.) during the process.[200]

[191] *See* Shubhani Aggarwal, Neeraj Kumar, Attacks on Blockchain, 121 Advances in Comput. 399, 399-410 (2021) (discussing consensus and ledger-based attacks, including Finney attacks and 51% attacks), https://www.sciencedirect.com/science/article/abs/pii/S0065245820300759?via%3Dihub.

[192] *See* Carter & Jeng, *supra* note 26, at 14.

[193] *Id.* at 19.

[194] Ethereum was first launched utilizing a proof-of-work protocol and later transitioned to a proof-of-stake model. *See Proof-of-Stake vs. Proof-of-Work: Security*, Ethereum Found., https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/pos-vs-pow/#security (last visited June 1, 2023)

[195] Yuanyuan Sun, Biwei Yan, Yan Yao & Jiguo Yu, DT-DPoS: *A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust*, 187 Procedia Comput. Sci. 371, 372-376 (2021) (discussing potential implementations of DPoS that would improve security of blockchains); *Delegated Proof of Stake (DPoS): Disincentives for Attacks*, BitShares, https://how.bitshares.works/en/master/technology/dpos.html#disincentives-for-attacks (last visited June 1, 2023).

[196] *See, e.g.*, Andrew O'Neill, *Stablecoin Depegging Highlights DeFi's Exposure To TradFi Risks*, S&P Global (Mar. 15, 2023), https://www.spglobal.com/ratings/en/research/articles/230315-stablecoin-depegging-highlights-defi-s-exposure-to-tradfi-risks-12669023.

[197] Krisztian Sandor, *Circle Confirms $3.3B of USDC's Cash Reserves Stuck at Failed Silicon Valley Bank*, CoinDesk (Mar. 10, 2023), https://www.coindesk.com/business/2023/03/11/circle-confirms-33b-of-usdcs-cash-reserves-stuck-at-failed-silicon-valley-bank/.

[198] Gordon Y. Liao, *Macroprudential Considerations for Tokenized Cash*, Soc. Sci. Rsch. Ctr., 2-3 (Sept. 29, 2022); *Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements*, Bank for Int'l Settlements & Int'l Org. of Sec. Comm'n., 8 (July 13, 2022), https://www.bis.org/cpmi/publ/d206.pdf.

[199] *See* Jay Speakman & Paolo Besabella, *The Role of Stablecoins in Decentralized Finance and Combating Inflation*, BeInCrypto (Jan. 1, 2023), https://beincrypto.com/the-role-of-stablecoins-in-decentralized-finance-and-combating-inflation/.

[200] Heike Mai, *Stablecoins: DeFi, Libra and Beyond, Deutsche Bank Research* (Mar. 25, 2022), 2 https://www.dbresearch.com/PROD/RPS_EN-PROD/Stablecoins%3A_DeFi%2C_Libra_and_beyond/RPS_EN_DOC_VIEW.calias?rwnode=PROD0000000000435631&ProdCollection=PROD0000000000522496.

Due to the close connection between fiat-backed stablecoin issuers and the traditional financial system, fiat-backed stablecoins are viewed as a source of spillover risk to TradFi. Some widely used stablecoin arrangements may even be considered as global, systemically important, financial market infrastructures.[201] However, fiat-backed stablecoins may also help dampen the impact of DeFi volatility on the traditional financial sector. For instance, during a decline in digital asset prices, the behavior of crypto users to rebalance well-collateralized stablecoin holdings from smart contracts to externally-owned TradFi accounts may insulate the traditional financial system from significant demands on fiat redemption, thereby providing support to financial stability and minimizing contagion risk.[202] Moreover, the unbundling of payment services and credit provision fostered by payment stablecoins and other fintech innovations may reduce the systemic risk arising from liquidity mismatches and moral hazard that currently exists in the traditional banking system.[203]

It is important to note that not all stablecoins are alike. Whereas stablecoins using off-chain collateral such as cash equivalents, bank deposits, or commodities require a centralized actor to manage the underlying assets, algorithmic stablecoins that use on-chain collateral are managed via smart contracts and DAOs.

1 Protocol Risks: Conclusion

Where the risks for Public Good Protocols cannot at times be mitigated through technical solutions, regulators should identify and locate the pain points in these protocols based on the type of protocol and DeFi services offered. These pain points may include code flaws (such as smart contract vulnerabilities) or robustness issues with the underlying blockchain during high stress or volume influx. Moreover, regulators should consider encouraging mechanisms that promote protocol longevity and resiliency.

‘Same Activity, Different Risks, Different Regulation but Same Regulatory Outcome’ (NOT ‘Same Activity, Same Risk, Same Regulation’)

Regulators worldwide generally adhere to the regulatory principle ‘Same Activity, Same Risk, Same Regulation’ when regulating traditional non-banks and banks. It is natural then for regulators to fall back on this familiar principle when considering regulation for the digital assets space.[204] However, due to DeFi’s disintermediated nature and novel technological solutions to providing financial services, as articulated in the sections above, DeFi can have fundamentally very different risks, so this long-standing regulatory principle does not apply well to DeFi in all instances.

For instance, DeFi may engage in the *same activities* (i.e., similar financial services) as those found in TradFi, but the intrinsic operational and technological differences in DeFi may result in *different risks*. As elaborated above, credit risks in TradFi broadly stem from borrowers’ creditworthiness (hence, banks’ reliance on credit scores, such as FICO), while credit risks are more minimized in DeFi lending since protocols typically rely on overcollateralization.[205] Consequently, transposing regulations written for TradFi activities to DeFi activities is not always appropriate to achieve the same regulatory outcome of financial soundness and consumer protection. Therefore, the focus is on whether the risk (not the activity) is the same. If the risk is similar, then the regulatory outcome should be similar.

[201] *See generally* Bank for Int’l Settlements & Int’l Org. of Sec. Comm’n. *supra* note 198, at 11-12 (articulating standards to determine if, and when, a stablecoin becomes systemically important).

[202] *See* Liao, *supra* note 198, at 2-3 (examining the relationship between Terra stablecoin collapse and the accompanying increases in balances in other forms of tokenized cash).

[203] *See id.* at 4-5 (highlighting that public guarantees, such as deposit insurance and bank bail-outs, incentivize excessive risk taking, and that unbundling payments from the money-bank-payments triangle can create new forms of competition that benefit consumers); *see generally* Ye Li & Yi Li, *Payment Risk and Bank Lending: The Tension between the Monetary and Financing Roles of Deposits 2-9* (Fisher Coll. of Bus. Working Paper, Paper No. 2021-03-017, Apr. 26, 2023).

[204] *See, e.g.,* Press Release, Financial Stability Board, FSB Proposes Framework for the International Regulation of Crypto-Asset Activities (Oct. 11, 2022), (“They are grounded in the principle of ‘same activity, same risk, same regulation: where crypto assets and intermediaries perform an equivalent economic function to one performed by instruments and intermediaries of the traditional financial sector, they should be subject to equivalent regulation.”).

[205] *See* discussion *supra* ‘Benefits of Decentralized Finance: Reducing Counterparty Risk.’

Relatedly, DeFi and TradFi activities that differ from each other may, in fact, share similar types of risks. For instance, endogenously-backed stablecoins—digital assets backed by collateral issued on the same protocol that the digital asset is issued—present similar information asymmetry risks also found in some TradFi trading activities (i.e., adverse selection, moral hazard, differences in sophistication between users and market makers, etc.).[206] Unlike exogenously-backed stablecoins, if the endogenous stablecoin collapses, the underlying collateral would collapse too;[207] which may justify regulation to ensure robust consumer and investor protections (e.g., applying relevant securities laws).

DeFi also poses novel risks that existing regulatory frameworks were not designed to address. To determine what regulation is appropriate, regulators should identify the relevant DeFi-associated activities, and assess if they present the same, different, or removed risks. As a result, '**Same Activity, Different Risk, Different Regulation but Same Regulatory Outcome**' should be the principle followed when crafting regulatory approaches for DeFi and for mitigating the risks highlighted above.[208]

Additionally, the transparency characteristics of DeFi address some of the information asymmetries that traditional regulations aim to address. In TradFi, users rely on businesses, vendors, intermediaries, and custodians to settle transactions. Information asymmetries are prevalent in this model, necessitating regulation to establish trust in these various parties—especially when intermediaries have little incentive to meet the informational needs of investors.[209] Conversely, DeFi allows users to engage in multiple forms of peer-to-peer activities based on publicly-available information on blockchains while reducing reliance on third-party intermediaries. This feature eliminates many of the information asymmetries and counterparty risks that plague traditional markets.

For these reasons, creating a fit-to-purpose regulatory framework is optimal. Some of the most prevalent DeFi risks have been identified in the section above. However, this list is not exhaustive, and all DeFi risks cannot be addressed by an *ex ante*, one-size-fits-all approach. Doing so would violate the core design principle of '*Same Activity, Different Risk, Different Regulation but Same Regulatory Outcome*.' Consequently, a one-size-fits-all system would risk choking off DeFi's current benefits and may stymie benefits that could arise as the technology and its use cases evolve. In contrast, an ideal regulatory framework would entail parsing through the risk profiles of specific DeFi activities in consideration of risk mitigation mechanisms while allowing the public to reap the benefits of the new technologies.

[206] *See* Stephen G. Cecchetti & Kermit L. Schoenholtz, *TradFi and DeFi: Same Problems, Different Solutions,* Money & Banking (May *30*, 2022) (discussing the challenges common to both DeFi & TradFi, including information asymmetries, market efficiency, and market integrity); *see also* Richard K. Lyons & Ganesh Viswanath-Natraj, *What Keeps Stablecoins Stable?* 42-34 (Nat'l Bureau Econ. Res. Working Paper, Paper No. 27136, May 2020) (discussing the information asymmetry present in stablecoin markets responding to speculative events); Binh N. Thanh, Thai N. Vu Hong, Huy Pham, Thanh N. Cong & Thu Pham Thi Anh, *Are the Stabilities of Stablecoins Connected?*, J. Indus. Bus. Econ. at 2 (Jan. 2022) (discussing the information asymmetry in Stablecoin markets between savvy developers and investors); Lennart Ante, Ingo Fielder & Elias Strehle, *The Impact of Transparent Money Flows: Effects of Stablecoin Transfers on the Returns and Trading Volume of Bitcoin,* 170 Tech. Forecasting Soc. Change 2-3, 7-9 (Sept. 2021) (demonstrating the degree of public information asymmetry in stablecoin transfers); Enrico Rossi, Stablecoins in *Three Dimensions: Foundations of Value in the Crypto-Economy,* UCL Cent. For Blockchain Tech. at 16-25 (June 22, 2022) (discussing the similarity of information asymmetry in TradFi and DeFi markets, detailing the function of information asymmetry in stablecoin markets in particular).

[207] *See, e.g., What Is a Stablecoin?*, Chainlink (Oct. 8, 2022), https://blog.chain.link/stablecoins-but-actually (discussing the collapse of UST and the simultaneous collapse of its supposed underlying collateral: LUNA). *See also Two Thought Experiments to Evaluate Automated Stablecoins*, Vitalik Buterin (May 25, 2022), https://vitalik.ca/general/2022/05/25/stable.html. When constructing a legal framework for regulating protocol-minted stablecoins that are fully or partially backed with on-chain collateral (DAI, for example), regulators should identify the quality of a stablecoin's collateral that provides the basis for its peg. In particular, if the stablecoin's underlying collateral is closely tied with the nexus of the same protocol that mints the stablecoin (commonly referred to as endogenous collateralization), there is a heightened risk the stablecoin can lose its peg during times of heightened market activity. In contrast, stablecoins that utilize high-quality collateral that exists outside of the same protocol that mints the stablecoin (commonly referred to as exogenously collateralized stablecoins) have empirically performed better in terms of maintaining their dollar-peg. Additionally, stablecoins are often not entirely endogenously or exogenously collateralized, and some stablecoins, such as Frax, use a combination of both endogenous and exogenous collateral. *See generally Adrien d'Avernas, Vincent Maurin & Quentin Vandeweyer, Can Stablecoins Be Stable?* (Becker Friedman Inst. Univ. Chicago Working Paper No. 2022-131, Sept. 2022).

[208] Evaluating the differences in risks underlying TradFi broker-dealers and non-custodial DeFi exchanges, is particularly illuminating here. Both parties enable users to engage in the same activity, which is providing a form of capital (traditional fiat or a crypto asset) to acquire a new asset. However, in DeFi exchanges, users never transfer custody of their assets whereas TradFi broker-dealers often take customer's assets, creating more risk for the latter. *See* Jennings, *supra* note 30.

[209] Letter from Andreessen Horowitz to HM Treasury, *supra* note 40.

5 DeFi Policy Recommendations

Source: @alvaro pinot/unsplash

As explained above, DeFi provides a number of benefits while eliminating some of the risks present in the traditional financial system. However, some risks remain, many novel due to the new technology. Because the risks presented in DeFi are fundamentally different from those in TradFi, the application of the updated principle '*Same Activity, Different Risk, Different Regulation, Same Regulatory Outcome*' would be more effective for protecting consumers, and ensuring financial safety and soundness.

The policy recommendations elaborated below were developed after carefully assessing the types of risks that DeFi poses to consumers, and how best to mitigate these risks through reducing information asymmetries, increasing network security, and implementing other consumer safeguards.

Following the regulatory approach '*Regulate Businesses, Not Public Good Protocols*' (which adheres to the principle '*Same Activity, Different Risk, Different Regulation but Same Regulatory Outcome*' by placing regulatory obligations on the app-operating businesses), we propose the following three policy recommendations. We believe this approach ensures consumer and investor protection, and mitigates financial risks without stifling the benefits of these innovative technologies:

1. **Mandatory Disclosure for App-Operating Businesses**
   A standardized disclosure regime for app-operating businesses that includes information about the underlying DeFi protocol.

2. **Independent Certification:**
   The establishment of an Independent Certification Regime Organization (ICRO), which certifies DeFi protocols that meet the ICRO's criteria, including security code audits.

3. **Regulatory Safe Harbor:**
   A safe harbor regime for nascent protocols that aim to decentralize.

We elaborate on each policy recommendation below.

1 Mandatory Disclosure Regime

To achieve a sustainable, user-centric Web3, participants must be empowered to navigate an ever-changing and complex decentralized environment. Enforcing mandatory disclosures on businesses can help to facilitate user autonomy and ecosystem resiliency.[210]

Code disclosure

The principle of transparency and disclosure have served as the bedrock of fair markets regulation today and should play a critical role for DeFi as well. While the protocols have publicly viewable code, most end users cannot read programming code.[211] Protocol disclosures should be conveyed in an easy-to-understand manner for the average user and disclosed by the app-operating business that chooses to build apps on the protocol, preferably via the website of the app-operating business.

[210] *See, e.g., Structured Disclosure at the SEC: History and Rulemaking*, U.S. Sec. & Exch. Comm'n, https://www.sec.gov/page/osdhistoryandrulemaking (last visited June 13, 2023) (explaining that disclosures have been utilized by the SEC to protect investors and maintain fair and efficient markets); *see generally* also Chris Brummer, *Disclosure, dApps and DeFi*, Stanford J. of Blockchain L. and Pol'y. (Mar. 2022) at 47 n.95 (tracing the historical role disclosures have played for investor protection since the 1930s).

[211] Brummer, *supra* note 210, at 32.

Currently, there is no standard for what a disclosure about the underlying protocol should include. At minimum, the disclosure may include how the protocol works, governance, funds and assets management, security, and other material terms. While white papers may help bridge this technical gap, they may be filled with confusing terms or overstate the protocol's abilities.[212] More specifically, the security aspect of the disclosure should include information about whether a security code audit was conducted and its results. Additionally, the app-operating business should disclose what remediation avenues, if any, are available to the end user. Disclosures should impart clear, user-friendly information and could consist of a set of simple yet essential yes or no questions. They should also offer relevant explanatory data points, such as number of outstanding tokens, etc., or a set of risk indices on the homepage of the app's website, which may be further elaborated elsewhere on the site.[213]

When consumers and investors find information difficult and costly to access or analyze, a variety of harms may result. Mandatory, comprehensible disclosures address this information gap, which in turn leads to more efficient markets and allows participants to manage risks in ways that could lead to mutually beneficial conduct.[214] This framework would also incentivize app-operating businesses to carefully assess and choose which protocols to build on. Ultimately, the disclosures themselves can be leveraged as a standard-setting mechanism that could facilitate enhanced cybersecurity and protocol robustness throughout the ecosystem.[215]

Protocol-Related Disclosures by App-Operating Businesses

DeFi businesses should disclose which underlying protocol(s) they use to provide their services and additional disclosures related to the safety of the protocol(s). Protocol disclosures can be broadly classified into four categories (as applicable):[216]

1. general software disclosures
2. tokens disclosures
3. financial disclosures
4. automation disclosures

Together, these disclosures should provide ample information to users so they can quickly understand the risks of interacting with businesses that utilize these protocols. Moreover, these disclosures are comprehensive and require businesses to utilize resources.

[212] *Id.*

[213] While a binary yes or no question may provide the most concise delivery of information, this may fail to describe all dimensions of risk, such as when the last risk took place, whether the newest version of the protocol has been audited, or if the audit results were public. Xavier Meegan, *Identifying Key Non-Financial Risks in Decentralised Finance on Ethereum Bl*ockchain (Oct. 2020) (M.A. Thesis, Polytechnic University of Milan), https://www.researchgate.net/publication/344689196_Identifying_Key_Non-Financial_Risks_in_Decentralised_Finance_on_Ethereum_Blockchain.

[214] *See* William Magnuson, *The Failure of Market Efficiency,* 48 Brigham Young Univ. L. Rev. 827, 843-45 (Apr. 30, 2022) (explaining that financial regulation, such as the Securities Act of 1933, the Investment Company Act of 1940, the Williams Act of 1968, The Sarbanes-Oxley Act of 2002, and the Dodd-Frank Act of 2010, all served to require the production of information for financial markets that enabled "more rational decisions" and "more mutually beneficial transactions").

[215] *See* Douglas W. Arner, Dirk A. Zetzsche, Ross P. Buckley & Jamieson M. Kirkwood, *The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023,* Univ. of H.K.19-20 (May 17, 2023) (emphasizing the need for standardized information disclosure requirements including auditing standards; *see also* Balázas Bodó & Primavera De Filippi, Trust in Context: The Impact of Regulation on Blockchain and DeFi, Univ. of Amsterdam Ctr. for L. & Econ. (Mar. 7, 2022); Lin William Cong, Kimberly Grauer, Daniel Rabetti & Henry Updegrave, *The Dark Side of Crypto and Web3: Crypto Related Scams* (Feb. 14, 2023) (discussing audits as a means of improving security and preventing fraud).

[216] *Crypto Asset Disclosure Study Insights on Holders and How They Analyze Their Holdings at 3*, BroadRidge (2023), https://www.broadridge.com/_assets/pdf/broadridge-crypto-asset-disclosure-study-report.pdf.

Protocol-Related Disclosures by App-Operating Businesses - Continued

Software disclosures relate to general information about the functioning of the protocol, including its purpose and features, governance, potential modifications, and official communication channels. It also includes delineating risks and any measures to mitigate them, such as emergency procedures, bug bounty programs, or processes for ongoing monitoring.

An essential component of software disclosures is the code audits of the underlying protocol, which an application provides access to. Such code audits provide disclosures that are critical for ensuring the protocol's overall security and establishing consumer trust. A best practice for code audits includes undergoing three dimensions of analysis: static, dynamic, and software composition (i.e., external dependencies).[217] Code audit approvals should be granted for a limited time and may be withdrawn if a security breach is discovered or there is a significant code change.[218]

Token disclosures relate to the protocol's native token(s). This entails descriptions of the token's purpose, utility, special features, and information regarding its launch, supply, and distribution. Other token-related disclosures include potential risk factors associated with holding or trading the native token, any governance features (including rules related to participating in the decision-making process), and sources of official communication channels for future announcements relating to updates and changes that may be made to the token. Note that not all DeFi protocols create tokens.

Financial disclosures more generally relate to any potential earnings and fees that users may incur when interacting with the protocol, including from activities such as mining, staking, and liquidity provision. These disclosures should also describe how users can independently access, search, and verify their transaction history.

Finally, automation disclosures relate to the autonomous features of a protocol's smart contracts. For instance, this may include:

- identifying aspects of the protocol that are immutable versus mutable/upgradeable,
- if mutable, what are the relevant mechanisms, in terms of both governance and signature schemes,
- how smart contracts are used to exchange crypto assets, and
- formulas used to determine the pricing and composition of native tokens, or processes through which an approved DAO governance proposal is implemented in the protocol's smart contract.

Because some decentralized protocols rely on DAOs for code updates and alterations, it is conceivable for a protocol's DAO to be responsible for providing updates and any additional information to ensure renewed ICRO certification (see following section on discussion of ICRO certification). For reporting purposes, some notifications of changes and implications of the changes could be automated.

While this list is not exhaustive, it aims to illustrate the types of disclosures related to protocols, in contrast to the activities-based disclosures described in the following section. Regulators would issue mandatory disclosure requirements for app-operating businesses, while the ICRO could provide an additional determination of relevant protocol disclosures for protocol developers.

[217] *See* Olivier Fliche et al., "Decentralised" or "Disintermediated" Finance: What Regulatory Response? 32-33 (Discussion Paper, French Prudential Supervision and Resolution Authority, 2023), https://acpr.banque-france.fr/sites/default/files/medias/documents/20230403_decentralised_disintermediated_finance_en.pdf. ("[S]tatic analysis makes it possible to detect formal errors in programming or design; dynamic analysis focuses on monitoring the execution of the program; finally, software composition analysis (sca) makes it possible to draw up an inventory of the external dependencies of the program under review to third-party libraries or open source components.").

[218] The ICRO, utilizing its expertise, should determine the period of time a code audit approval lasts as well as what constitutes a significant code change.

2 Independent Certification Regime Organization (ICRO): a self-regulating entity

As organic food production began to grow in the 1970s and 1980s, farmers, food processors and distributors wanted to communicate to consumers that their products were not produced using synthetic chemicals.[219] Independent certification organizations, which were self-regulating entities that determined criteria for organic certification, were formed to develop criteria for an organic foods label, helping consumers to understand what they were consuming.[220] This paper proposes an Independent Certification Regime Organization akin to these organic certification organizations.

We use this independent certification model as a guiding point rather than the model of traditional Self-Regulatory Organizations (SROs), such as Securities & Exchange Commission-overseen stock exchanges (e.g., New York Stock Exchange, etc.), clearing houses (e.g., Depository Trust and Clearing Corporation, etc.), and broker-dealer associations (e.g., Financial Industry Regulatory Authority),[221] or designated markets overseen by the Commodity Futures Trade Commission (e.g., Chicago Mercantile Exchange, etc.), derivatives clearing organizations (e.g., Options Clearing Corporation), or registered futures associations (e.g., National Futures Association).[222] However, it is possible that over time this ICRO could become an SRO overseen by a financial regulator—an idea that some academics have proposed.[223]

The ICRO's protocol certification program helps avoid placing excessive compliance burdens on software developers while also incentivizing them to implement best practices to gain user adoption.[224] In addition, an ICRO can set standards and best practices. If the protocol fails to meet the ICRO's criteria, the ICRO can either decertify or not renew the protocol's certification. If properly implemented, an ICRO could lead to effective industry standards, with buy-in from industry participants.

Such a certification accomplishes several goals. First, it fosters market efficiency—businesses would no longer have to expend the time necessary to answer all the relevant disclosures. Second, a certification regime produces a flywheel effect wherein protocols are heavily encouraged to provide adequate disclosures. For example, a business is more likely to use a Certified Protocol than a non-certified one since the former has already received an authoritative stamp of approval. Protocol developers, who are incentivized to attract as many users to their protocol as possible, know this and consequently would take the time to receive a certification to attract businesses. Lastly, the ICRO can help determine best practices in risk management, code audits, disclosures, etc. Best protocol practices can improve consumer safety and cybersecurity without stifling the process of technological innovation.[225]

[219] Jessica Ellsworth, The History of Organic Food Regulation (June 15, 2001) (Third Year Paper, Harvard Law School) (on file with the Harvard University Library System).

[220] *Id.*

[221] *See, e.g., Self-Regulatory Organization (SRO) Rulemaking & National Market System (NMS) Plans,* U.S. Sec. & Exch. Comm'n, https://www.sec.gov/rules/sro/sro.shtml (last visited June 23, 2023).

[222] *See, e.g., CFTC Oversight,* U.S. Gov't Accountability Off., https://www.gao.gov/products/ggd-92-28r (last visited June 23, 2023).

[223] *See* Timothy J. Massad & Howell Jackson, *How to Improve Regulation of Crypto Today—Without Congressional Action—and Make the Industry Pay for It,* at 7 (Brookings, Hutchins Center Working Paper #7, Oct. 2022) (discussing the potential for a joint SEC-CFTC Crypto SRO), https://www.brookings.edu/wp-content/uploads/2022/10/WP79-Massad-Jackson-updated-2.pdf.

[224] This is already being considered across a number of jurisdictions. *See, e.g., Response to ACPR's Discussion Paper: "'Decentralised' or 'Disintermediated' Finance: What Regulatory Response",* Polygon Labs (May 23, 2023), https://polygon.technology/blog/response-to-acprs-discussion-paper-decentralised-or-disintermediated-finance-what-regulatory-response?utm_source=acpr-response-blog&utm_medium=blog.

[225] *See* discussion *supra* 'Disclosures and Standard-Setting.'

3 Regulatory Safe Harbor for Nascent DeFi Innovations

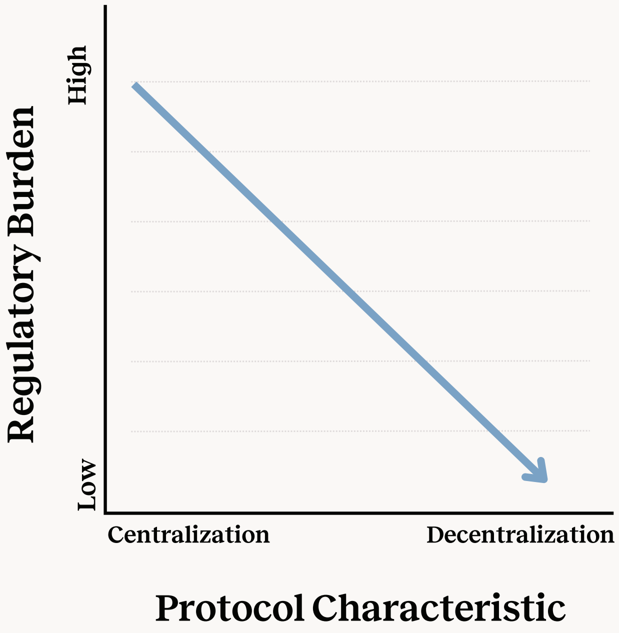
As outlined in the '*Same Activity, Different Risks, Different Regulation but Same Regulatory Outcome*' section, the risks that DeFi presents can be fundamentally different to those in TradFi, and existing entities-based regulations were not drafted to address these DeFi-specific risks. To foster innovation in a risk-calibrated manner, this paper proposes a safe harbor for progressively decentralizing protocols that can eventually become Public Good Protocols.

Many DeFi protocols, when launched, do not start off as decentralized. Such protocols develop and morph over time into protocols that are decentralized in governance and operations (i.e., progressive decentralization). This gradual process is beneficial, as greater control enables the developers of the protocol to ensure that it is not vulnerable to attack. As confidence in the protocol's safety grows, the developers gradually remove any elements of control (such as pause mechanisms) to make it fully decentralized. To allow for progressive decentralization to occur in a controlled manner that protects consumers, this paper suggests that regulators provide a safe harbor for newly released protocols that aim to decentralize.[226]

To be eligible for a regulatory safe harbor, protocol developers must first comply with the mandatory disclosure requirements articulated in the previous section. The ICRO should determine any additional general and safe harbor-specific eligibility criteria to receive the exemptions.[227] For instance, a reasonable time period for the safe harbors would be two to three years, and certain maximum TVL thresholds could be established.[228] Safe harbor participants also may be required to submit code audits and an entry/exit strategy, as well as periodic reports during the period of regulatory shelter for regulatory monitoring and analysis. The regulatory requirements decrease as the protocol progressively decentralizes. Once the protocol has transformed into a Public Good Protocol, the protocol graduates out of the safe harbor program and provides the accompanying benefits of Public Good Protocols.[229] See Figure 3 below and Figure 5 for more details about safe harbor compliance.

FIGURE 3

Safe Harbor Approach: Regulatory Burden vs. Progressive Decentralization



[226] This safe harbor approach has been put forward by SEC Commissioner Hester Peirce. Peirce, *supra* note 14.

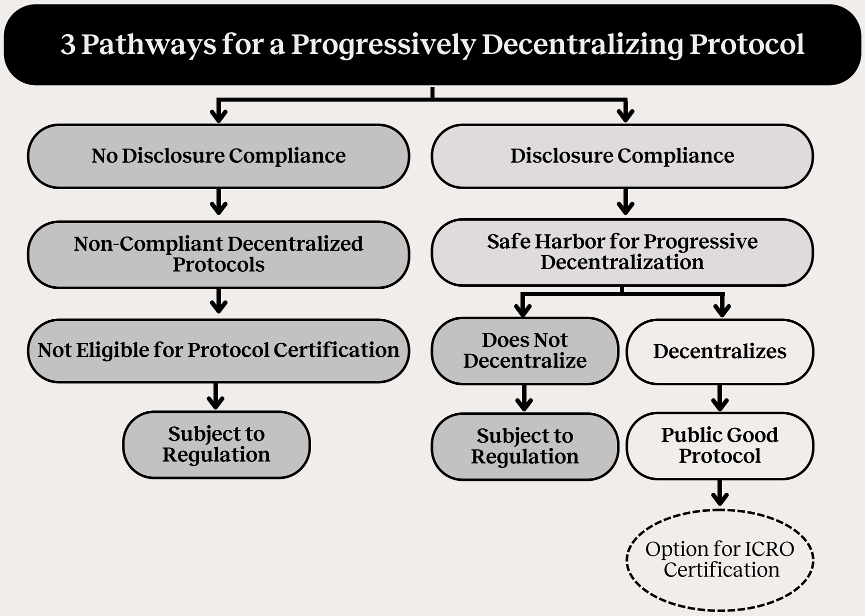
[227] *See, e.g.,* 'Box 2', which articulates how multiple safe harbors can be established via general and safe harbor-specific eligibility requirements.

[228] *See* Peirce *supra* note 14.

[229] *See* discussion *supra* 'Benefits of DeFi.'

Note that some protocols may not become Public Good Protocols during the safe harbor program because they do not reach the point of decentralization. These Non-Public Good Protocols would be subject to the existing regulations according to their activities.[230] See Figure 4 below on the different pathways a transitioning protocol can take within our proposed regulatory framework.

FIGURE 4
Potential Pathways for Progressively - Decentralizing Protocols


3 Pathways for a Progressively Decentralizing Protocol
No Disclosure Compliance
Disclosure Compliance
Non-Compliant Decentralized Protocols
Safe Harbor for Progressive Decentralization
Not Eligible for Protocol Certification
Does Not Decentralize
Decentralizes
Subject to Regulation
Subject to Regulation
Public Good Protocol
Option for ICRO Certification

As portrayed in Figure 4, there are primarily three pathways for DeFi protocols. If the DeFi protocol meets the mandatory disclosure requirements and the regulatory safe harbor eligibility requirements, then it can either (i) fail to decentralize and would therefore be subject to regulation or (ii) decentralize and become a Public Good Protocol (meaning it would not be subject to regulation) and be eligible for ICRO certification. Note that the regulatory safe harbor may require a code audit to enter the program and may additionally require code audits during the course of the program.

On the other hand, if the transforming DeFi protocol does not have features that support app-operating businesses in complying with their mandatory disclosure requirements, then it would fail to qualify for both a regulatory safe harbor and an ICRO certification. It also would be subject to regulation. While it is impossible to prevent such non-compliant protocols from existing, the lack of legitimacy due to the absence of certification would disincentivize mass usage. Additionally, the businesses operating these non-compliant protocols would be subject to regulation, minimizing the risks they present to consumers.

[230] In the case a progressively decentralizing protocol chooses not to provide the necessary materials to meet the eligibility of the safe harbor, such a protocol should be considered non-compliant and therefore is not eligible to be a certified protocol. While it may be impossible to prevent such decentralized protocols from existing, the lack of legitimacy due to the absence of certification would disincentivize mass usage of a non-compliant protocol.

Case Study: The Digital Millennium Copyright Act (DMCA) Safe Harbor

A Web2 parallel that illustrates the importance of safe harbors for innovative industries is the Digital Millennium Copyright Act (DMCA) of 1998, which provides a safe harbor for online service providers (OSP) by shielding them from liability for the content its users posted.[231] Without this safe harbor, many of the Web2 companies that have become foundational in facilitating public communication and advancing the digital economy would not have survived to this day.

"It was likely no overstatement to say that the DMCA, and in particular its safe harbor provisions, saved the web as we know it today. Without the safe harbor provisions, social networking would likely not exist, and blogging would probably be confined to those who could host their own servers rather than being readily accessible to the masses at virtually no cost. Without the safe harbor provisions, the nascent field of cloud computing would likely have been strangled in the crib, or at least stunted and twisted to carefully fit the confines of the most recent court case. Without the safe harbor provisions being codified, Google most likely would have refused to purchase YouTube due to the obvious concerns about secondary liability that such a service model provides."[232]

Under the DMCA, there are four types of safe harbor provisions based on the type of OSP activity: storage, transmission, caching, and use of information location tools.[233] Safe harbor eligibility conditions include requiring OSPs to adopt measures to address users who repeatedly infringe copyrights and to not interfere with copyright owners when they try to identify and protect their works.[234] Each safe harbor provision has additional eligibility conditions.[235] For example, to be eligible for the 'storage safe harbor,' OSPs must agree to take down the infringing material upon knowledge or awareness of a violation.[236]

Nascent startups often are unable to afford the costs of litigation, even when they are confident of winning due.[237] By removing regulatory uncertainty, small Web2 companies were empowered to innovate more freely.[238] Furthermore, the DMCA's safe harbor provisions encouraged investments in many of startups that otherwise would not have been funded without these regulatory exemptions.[239]

Outside the US, many countries also recognized the importance of safe harbors in fostering innovative technology industries during Web2. In a 2009 Australian government report on building the country's digital economy, the government highlighted the fact that safe harbors could help businesses reduce the risks arising from regulatory uncertainty, attracting greater investment into the country.[240] However, a safe harbor with overly-stringent restrictions can stifle nascent businesses. For example, under France's implementation of the 2000 Directive on Electronic Commerce (ECD)—the European parallel to the DMCA—website publishers were ineligible for the safe harbor protections that other European website publishers had. Eventually, French social news sites, such as Fuzz.fr, had to shut down. [241]

[231] Timothy Wiseman, Limiting Innovation Through Willful Blindness, 14 Univ. Nev. L.J. 210, 210-15 (2013), https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1531&context=nlj.

[232] *Id.* at 515.

[233] 17 U.S.C. 512; *see also* Mitchell Zimmerman, *Your DMCA Safe Harbor Questions Answered,* Fenwick (2017), https://assets.fenwick.com/legacy/FenwickDocuments/DMCA-QA.pdf.

[234] *Id.*

[235] 17 U.S.C. 512; Cong. Rsch. Serv., Digital Millenium Copyright Act (DMCA) Safe Harbor Provisions for Online Service Providers: A Legal Overview (2020) Copyright Act.

[236] *Id.*

[237] *Id.*

[238] *See* Wiseman *supra* note 231, at 215.

[239] *Id.*

[240] *Id.* at 229.

[241] *See* Wiseman *supra* note 231, at 229.

FIGURE 5
Compliance End State

	Disclosures	Protocol Code Audits	Protocol Certification	Progressive Decentralization Safe Harbor	Subject to Regulation (in relevant jurisdictions)
App-operating Business (including Foundations and DAOs)	🔴				🔴
Nascent Protocols (developed by the developer team)	🔴	🔴		🟢	🟡
Mature Non-Public Good Protocols (not decentralized)	🔴	🔴			🔴
Mature Public Good Protocols	🔵	🔵	🟢		

🔴 Mandatory

🟢 Eligible to receive upon meeting certain conditions

🔵 Best practice, but not mandated (needed to receive certficiation)

🟡 Required if the nascent protocol:
(a) does not fall under the Safe Harbor, or
(b) fails to decentralize within the Progressive Decentralization Safe Harbor period

6 Conclusion

Source: @micah boswell/unsplash

DeFi is a quickly growing and evolving industry, but it is still nascent. This paper's proposed 'Regulate Businesses, Not Public Good Protocols' approach to regulation provides many of the necessary economic and regulatory incentives to encourage DeFi protocols to be either (1) regulated as businesses or (2) not explicitly regulated due to their status as a Public Good Protocol, which can be facilitated by our proposed regulatory safe harbor program. Mandatory disclosure obligations would be the responsibility of the app-operating businesses, and this disclosure regime would be enhanced by a certification regime whereby the ICRO provides independent certification of Public Good Protocols. Importantly, adhering to the updated regulatory principle of '*Same Activity, Different Risk, Different Regulation but Same Regulatory Outcome*,' this framework will help foster the positive benefits supported by the open source, autonomous, standardized, and non-discriminatory features of Public Good Protocols that will serve as the public goods infrastructure for the DeFi and Web3 ecosystem of the future.

Prepared by

Linda Jeng
Head of Global Web3 Strategy,
Crypto Council for Innovation

Kristy Lam
Policy Coordinator,
Crypto Council for Innovation

Christian Lansang
Law and Policy Fellow,
Crypto Council for Innovation

Sean Lee
Senior Advisor,
Crypto Council for Innovation

Tyler Peltekci
Summer Associate,
Crypto Council for Innovation

Working Group acknowledgements

Sincere appreciation is extended to the individuals below, who in many cases spent numerous hours providing critical input and feedback to the drafts. These individuals represent the majority of CCI members, and their diverse insights are fundamental to the success of this work.

Andreessen Horowitz

Zach Gray
Associate General Counsel, a16z crypto

Bill Hinman
Advisory Partner, a16z crypto

Miles Jennings
General Counsel and Head of Decentralization, a16z crypto

Michele Korver
Head of Regulatory, a16z crypto

Brian Quintenz
Head of Policy, a16z crypto

Block

Melissa Netram
Head of Bitcoin Policy

Will Wilkinson
Head of Policy, TBD/Block

Crypto Council for Innovation

Yaya J. Fanusie
Director of Policy for AML & Cyber Risk

Sheila Warren
Chief Executive Officer

Paradigm

Brendan Malone
Policy Manager

Rodrigo Seira
Special Counsel

Ribbit Capital

Jessi Brooks
Chief Compliance Officer & Associate General Counsel

Spruce Systems, Inc.

Jonathan Rufrano
Public Sector & Institutional Lead

Reviewer acknowledgements

We wish to thank those who reviewed our paper and for their thoughtful feedback.

Ross Buckley
ARC Laureate Fellow & Scientia Professor,
University of New South Wales Sydney

Jon Frost
Head of Economics for the Americas,
Bank for International Settlements

Jason Gottlieb
Chair of Digital Assets Department, Morrison & Cohen

Josh Lipsky
Senior Director, GeoEconomics Center, Atlantic Council

Michael Mosier
Partner, Arktouros PLLC

Jennifer Schulp
Director of Financial Regulation Studies, Cato Institute

Jack Solowey
Policy Analyst, Cato Institute

Crypto
Council for
Innovation

Key Elements of an Effective DeFi Framework

Questions?
Please email us at: info@cryptoforinnovation.org

—

Source (cover image): @marek piwnicki/unsplash