Written Testimony of
Rebecca Rettig
Chief Legal & Policy Officer of Polygon Labs

“Decoding DeFi: Breaking Down the Future of Decentralized Finance”

Before the U.S. House Financial Services Committee Subcommittee on Digital Assets, Financial Technology, and Inclusion

September 10, 2024

Bio

I am the Chief Legal Officer of Polygon Labs, an international software development company building blockchain scaling infrastructure and an aggregated blockchain network. I spent the early part of my legal career at a large New York law firm litigating and defending cases relating to, among other things, traditional financial services and regulations as well as early peer-to-peer file sharing technology.

In the last seven-plus years of my legal career, I have focused on advising companies building novel applications in the blockchain space, including in decentralized finance ("DeFi"), as well as how to implement risk mitigation mechanisms that achieve regulatory goals that underlie many of our traditional systems today.

Prior to joining Polygon Labs, I was General Counsel at a UK-based software company that developed one of the most well-known DeFi protocols and created other blockchain-based user applications. As part of my work there, I began engaging with regulators and policymakers in the U.S. and abroad to meet requests for greater education about DeFi and its underlying technology, benefits, and risks as well as the ways to achieve regulatory goals within this system. I have continued that work to the present.

Recently, I co-authored a paper entitled "Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance," published in January 2024, which sets forth a three-part proposal to effectively detect, document and deter the proliferation of illicit activity in DeFi — to bring traditional financial integrity standards into the system without classifying pure technology as financial institutions — while preserving the technology as permissionless, neutral infrastructure.[1]

[1] Rebecca Rettig, Michael Mosier, and Katja Gilman, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance*, SSRN (Jan. 29, 2024), https://ssrn.com/abstract=4607332 [hereinafter Genuine DeFi as Critical Infrastructure].

Chairman Hill, Ranking Member Lynch and members of the Subcommittee, thank you for inviting me to speak today on the topic of decentralized finance.

DeFi is part of the larger web3 movement of decentralized applications built upon open networks — a movement that seeks to return the Internet to individuals and move away from the centralization and ownership of large tech companies and financial institutions. It's a movement arising from consumer demand for peer-to-peer transparent networks, for increased competition, and for control over one's own data.

DeFi is an innovative technological system that allows for novel ways of transacting (*see* Part I), brings new and different benefits from the traditional financial system (*see* Part II) and thus, has received different regulatory treatment from policymakers around the globe (*see* Part III).

I. Decentralized Finance Explained

A. Defining DeFi

The first blockchain network — Bitcoin — enabled peer to peer transfers of value; DeFi is Bitcoin's successor, allowing financial transactions through technological systems where no intermediaries are necessary.

Although there is no widely agreed-upon definition of DeFi,[2] I generally define it as a blockchain-based, software-based system that empowers users to engage in economic transactions without the need for intermediaries.

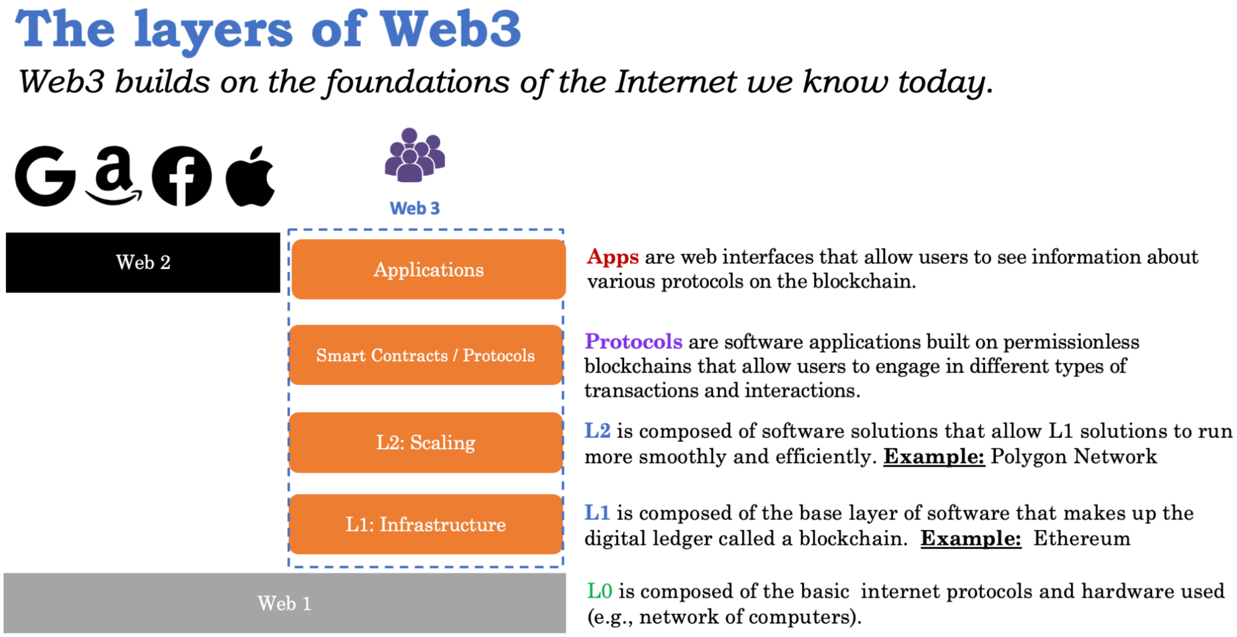
Certain hallmarks of DeFi distinguish it both from other blockchain-based software applications that allow for financial transactions and from the traditional financial system:

- it's non-custodial, *i.e.*, there is no identifiable entity or person who holds or otherwise can control cryptoassets on behalf of others: in DeFi systems, users maintain custody and control of their assets at all times;
- all transactions are user-directed and user-controlled, *i.e.*, there is no third party entity or person needed to effect any transaction; and
- the code is open source or source available, which allows users, developers and other third parties to verify functionality, and gain certainty over transactions.

[2] *See, e.g.*, Mariana de la Roche W. & Mirko Zichichi, *Bringing Clarity to the DeFi Sector: A Cross-Sector Proposal for a Unified DeFi Definition*, IOTA Foundation (Aug. 8, 2023), https://files.iota.org/comms/Bringing_clarity_to_the_DeFi_sector.pdf; Katrin Schuler, Ann Sophie Cloots & Fabian Schar, On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance, 2 (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4422473; U.S. Dep't of the Treas., Illicit Finance Risk Assessment of Decentralized Finance, 1 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf; The Bd. of the Int'l Org. of Sec. Comm'ns, *Consultation Report: Policy Recommendations for Decentralized Finance (DeFi)*, 1 n.3 (2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf.

“Smart contracts” — automated software that executes particular logic and functions in a conditional manner — comprise DeFi protocols. With this software, if a certain condition occurs under particular circumstances, then a specific action will automatically follow. A “smart contract” is not an actual legal contract between parties: “smart” refers to the fact that the code is autonomous and self-executing; “contract” refers to the fact that a transaction occurs automatically when predetermined conditions are met.

DeFi protocols are built on public infrastructure — namely blockchain networks. Like the Internet itself, this infrastructure can be accessed and operated by anyone with an Internet connection. The graphic below shows the technology stack upon which these protocols are built and the ways in which they can be accessed, including through user interfaces (discussed in Part I.B below). Leveraging public infrastructure means that information about DeFi transactions is recorded in real time and is viewable by anyone with an Internet connection.



The layers of Web3

Web3 builds on the foundations of the Internet we know today.

Apps are web interfaces that allow users to see information about various protocols on the blockchain.

Protocols are software applications built on permissionless blockchains that allow users to engage in different types of transactions and interactions.

L2 is composed of software solutions that allow L1 solutions to run more smoothly and efficiently. **Example:** Polygon Network

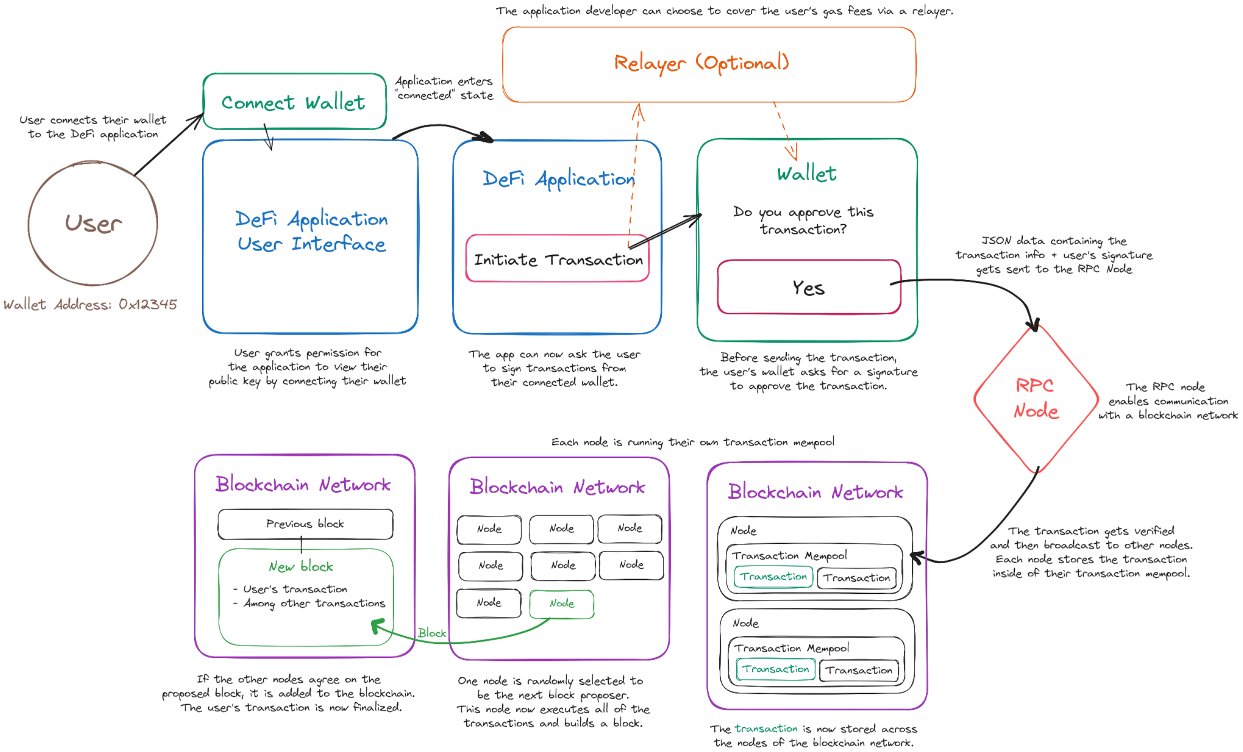
L1 is composed of the base layer of software that makes up the digital ledger called a blockchain. **Example:** Ethereum

L0 is composed of the basic internet protocols and hardware used (e.g., network of computers).

B. DeFi Software

DeFi allows users to communicate and execute financial transactions that are settled on permissionless blockchains. The below graphic shows the progression of DeFi transactions through the various software components comprising DeFi systems. The top half of the graphic depicts the DeFi software system; the bottom, the way in which base layer blockchain networks settle those transactions and record them on a blockchain.

Notably, this transaction flow is the same as for non-financial, blockchain-based applications, as well, such as blockchain-based social media applications, gaming, consumer loyalty programs and the like.


The application developer can choose to cover the user's gas fees via a relayer.
Relayer (Optional)
User connects their wallet to the DeFi application
Connect Wallet
Application enters "connected" state
User
Wallet Address: 0x12345
DeFi Application User Interface
User grants permission for the application to view their public key by connecting their wallet
DeFi Application
Initiate Transaction
The app can now ask the user to sign transactions from their connected wallet.
Wallet
Do you approve this transaction?
Yes
Before sending the transaction, the user's wallet asks for a signature to approve the transaction.
JSON data containing the transaction info + user's signature gets sent to the RPC Node
RPC Node
The RPC node enables communication with a blockchain network
The transaction gets verified and then broadcast to other nodes. Each node stores the transaction inside of their transaction mempool.
Each node is running their own transaction mempool
Blockchain Network
Node
Transaction Mempool
Transaction
Transaction
Node
Transaction Mempool
Transaction
Transaction
The transaction is now stored across the nodes of the blockchain network.
Blockchain Network
Node
Node
Node
Node
Node
Node
Node
Node
One node is randomly selected to be the next block proposer. This node now executes all of the transactions and builds a block.
Block
Blockchain Network
Previous block
New block
- User's transaction
- Among other transactions
If the other nodes agree on the proposed block, it is added to the blockchain. The user's transaction is now finalized.

The following are descriptions of the software involved in communicating a DeFi transaction:

- **Wallets:** A wallet is software comprising two unique numbers, each called keys: one public key, which is an identifier that lets users receive cryptocurrencies — similar to an email address; and one private key, which allows the user to access and send the cryptocurrencies associated with the paired public key — similar to a password.[3] Together, these keys allow individuals to utilize their wallet to interact or communicate with a blockchain network. Wallets — also called "externally owned accounts" — can either be downloadable software stored locally on a user's computer or smart contract-based accounts stored directly on a blockchain network. In DeFi, wallets are typically self-hosted — that is, downloaded, owned and controlled by the user, without an external third party providing custody. As a general rule, wallet software developers who create and make them available for download do not have any ongoing involvement with the wallet software's operation

[3] *See* Brief for DeFi Education Fund as Amici Curiae Supporting Respondents, Coinbase Inc. and Coinbase Global Inc.'s Motion for Judgment on the Pleadings, SEC v. Coinbase, Inc. et al., No. 23 Civ. 4738 (S.D.N.Y. 2023), 4; *see also* Fin. Crimes Enforcement Network, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, 16 (2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf ("Unhosted wallets are software hosted on a person's computer, phone, or other device that allow the person to store and conduct transactions in CVC. Unhosted wallets do not require an additional third party to conduct transactions. In the case of unhosted, single-signature wallets, (a) the value (by definition) is the property of the owner and is stored in a wallet, while (b) the owner interacts with the payment system directly and has total independent control over the value.").

by users. When users engage in transactions with their self-hosted wallets, they maintain independent control over their cryptocurrency.

- **User Interfaces / Front Ends:** User interfaces — sometimes referred to as front ends — are websites or applications that run on a person's full service computer, phone, or other mobile device.

  All Internet interactive sites or applications require front ends and back ends. The front end is a visual interface of a software system with which a user interacts. They are the part of a computer system or application that a user can see and with which a user interacts — usually to more easily access information and services available on the Internet. Back ends are the structure, system, data and logic underlying the user-facing application — that is, the aspects of a system or software program that a user does not see or interact with directly.

  A user provides inputs through a front end, and the back end of the system processes the inputs. The back end may read, analyze and write data that it then provides as an output to the user, through the front-end user interface. For example, www.x.com is a front end that allows a user to access X's social media software algorithm and data, with the algorithm and data being the back end.

  User interfaces relating to DeFi Systems can take a number of forms: (1) some only provide information about one or more DeFi protocols, such as potential transactions available through those protocols and related pricing and terms, without taking a fee; (2) others provide information and functionality to allow a user to connect their self-hosted wallet and then provide information about a transaction through their wallet directly to a protocol independent of the front end, with some of the providers of these interfaces taking a fee; and (3) a third type that provides some off-chain configuration (*e.g.*, a matching engine or order book hosted on a private server) where a user's transaction is reliant on the host of the off-chain server or service provider to match orders or otherwise to take steps towards completion of transactions, regardless of whether they take a fee. Although many users employ user interfaces, they are *not a necessary prerequisite* for either initiation or completion of a genuine DeFi transaction; users are able to engage in transactions on genuine DeFi protocols by accessing the smart contracts directly on a blockchain network. User interfaces, however, make these interactions less technically demanding.

  When users view interfaces to DeFi protocols, they have the same visual experience as when they interact with more traditional, web2 user interfaces. The most notable difference is that users interact with the Internet protocols in DeFi via software that allows them to retain control over their data and their assets, while in web2, all user information and assets are handled via intermediaries – whether it be large tech companies or big financial firms.

- **Protocol:** "Protocol" refers to a set of smart contracts that work together to allow users to communicate transaction instructions through a series of communications providers to a blockchain network for processing and execution. "Protocol" generally refers to a set of rules or procedures for a certain system; in DeFi protocols, the interaction among smart contracts sets the rules. These protocols may also be referred to as "dApps" — decentralized applications. As neutral technological infrastructure, DeFi protocols are akin to early Internet protocols such as HTTP, which allows for websites to exchange data and information, and SMTP, the underlying infrastructure for email.

- **Relayers:** Relayers are software that sends a user's transaction instruction to a protocol[4] by accepting a user's communication from a DeFi protocol and sending it to the next step in the transaction flow, such as a node for remote procedure calls ("RPCs") or a blockchain network node. Relayers do not take custody of or exercise independent control over user assets at any time — they relay communications, often about transactions. Users or application developers may compensate parties who run relayers, or the developer of a software application may subsidize third party relayers' gas fees.[5] Relayers are optional, at the discretion of each individual user for any transaction and for any protocol. Transactions can be fully accomplished and completed without relayers.

- **Nodes for Remote Procedure Calls:** Remote Procedure Call ("RPC") is a widely used software communication protocol that one software program can use to request a service from another software program that is running on a separate computer or network.[6] RPC is not specific to blockchains but rather relates to technology network systems more generally and has been employed for decades. In the blockchain context, RPC nodes are computers that run blockchain client software (*e.g.*, an Ethereum node). RPC nodes receive communications from wallets about users' transactions and then transmit those communications to be included in a block that will ultimately be validated and finalized on a blockchain network.[7]

  Individuals can maintain their own RPC node to communicate their own transactions. Some companies also provide RPC-node-as-a-service offerings, through which they host RPC nodes that individuals can use instead of running or hosting their own node. RPC-node-as-a-service providers generally charge fees for their services, usually paid by the developers of a DeFi application or by other third parties (*e.g.*, foundations) but typically *not* paid by users. Many RPC-node-as-a-service providers conduct some form of due

[4] *See* Antier Solutions, *The Role of Blockchain Relayer in Transforming Financial Systems*, Medium (Jul. 19, 2023), https://antiersolutions.medium.com/the-role-of-blockchain-relayer-in-transforming-financial-systems-ca2776dd761f [hereinafter Role of Relayers] ("Blockchain relayers are third-party services that facilitate the communication and transaction of data between different blockchain networks."); *see also* Benjamin Gruenstein, Evan Norris & Daniel Barabander, *Secret Notes And Anonymous Coins: Examining FinCEN's 2019 Guidance On Money Transmitters In The Context Of The Tornado Cash Indictment*, Int. Acad. Fin. Crime Litig., 10 (2023), https://edit.financialcrimelitigators.org/api/assets/b9fa10a1-5e91-4473-96f6-c240ff0761eb.pdf.

[5] *See* Role of Relayers, *supra* note 4.

[6] John Barkley, U.S. Dep't of Com., NISTIR 5277, Comparing Remote Procedure Calls, (1993), https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir5277.pdf ("The Remote Procedure Call (RPC) concept is a simple and useful technique for developing applications where communication between cooperating processes on networked systems is required").

[7] Relayers can also be — and frequently are — RPC node providers, whether as individuals or as RPC-node-as-a-service providers.

diligence and/or sanctions screening on their direct customers (those that pay fees), akin to the type of due diligence and screening Amazon Web Services ("AWS") conducts when a customer seeks to open a new server. It is important to note that AWS does not conduct the same due diligence or screening on users of a website hosted on an AWS server.

C. DeFi Use Cases

DeFi remains nascent: the oldest DeFi protocol is approximately seven years old, and DeFi did not gain meaningful traction until the summer of 2020. As of the end of August 2024,[8] DeFi protocols held approximately $82.68 billion of cryptoasset value locked. This is only 3.9% of the global cryptocurrency market cap and 0.08% of global GDP.[9] Compare this to the $17.6 trillion in commercial bank deposits accumulating over the past five decades[10]

DeFi applications have grown from simple exchanging, liquidity and borrowing protocols to robust software systems allowing for more complex transactions. Foundational use cases such as swapping through decentralized exchanges ("DEXs") as well as providing and borrowing liquidity comprise almost 60% of the TVL across all DeFi protocols.[11] Developers have expanded the scope of DeFi to include novel applications such as investing through tokenized real world assets, a use case that has gained traction via large institutions like BlackRock and Franklin Templeton. These use cases – and numerous non-financial use cases – are chronicled in The Value Prop, an open database compiling blockchain-based applications.[12]

One of the first and now most well-established DeFi use cases are decentralized exchanges, which allow users to exchange one cryptoasset for another. In the most well-known type of DEX — the automated market maker — users create pools of cryptoasset pairs ("liquidity pools"), which then allows users to exchange one cryptoasset for another in the pool. In this way, exchanging is peer-to-protocol rather than peer-to-peer. In contrast to traditional trading venues, DEXs operate 24/7/365, run autonomously (no intermediary), and eliminate counterparty risk (peer-to-software).

DEXs have gained such popularity that they rival centralized exchanges ("CEXs"). The Uniswap protocol, the most prominent DEX holding $4.6 billion of total cryptoasset value,[13] has surpassed volume on Coinbase, one of the most prominent U.S.-based CEXs, in daily and quarterly

[8] "Overview," DeFiLlama, https://defillama.com/ (last visited July 19, 2024) (estimating $97.589B in total value locked in DeFi protocols).

[9] "Total Crypto Market Cap Chart," CoinGecko, https://www.coingecko.com/en/global-charts (last visited Sep. 5, 2024) (estimating 2.124T for global cryptocurrency market cap); "Global gross domestic product (GDP) at current prices from 1985 to 2029," Statista, https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/ (last visited Sep. 5, 2024) (estimating $109,529.22B for global GDP in 2024).

[10] "Deposits, All Commercial Banks," FRED, https://fred.stlouisfed.org/series/DPSACBW027SBOG (last visited Aug. 20, 2024).

[11] "Dexes TVL Rankings," DefiLlama, https://defillama.com/protocols/Dexes (last visited Aug. 20, 2024) ($17.101B TVL for DEXs); "Lending TVL Rankings," DefiLlama, https://defillama.com/protocols/Lending (last visited Aug. 20, 2024) ($31.411B TVL for lending protocols).

[12] https://thevalueprop.io/.

[13] "Uniswap," DefiLlama, https://defillama.com/protocol/uniswap#information (last visited Aug. 20, 2024).

spot volume on a number of occasions.[14] Today, DEXs hold $17.1 billion in TVL, with more than 1,300 DEX protocols deployed.[15]

This popularity has spurred another use case – the DEX aggregator, which are protocols and interfaces that pull data from multiple sources to allow users to access the best liquidity and price for a particular trade through a single transaction.

Liquidity protocols — which allow users to supply and borrow cryptoassets — also provide core DeFi functionality.[16] Protocols such as MakerDAO, Aave and Compound, among others, allow users to supply and borrow crypto-assets in an over-collateralized manner. Like DEXs, users create liquidity pools through the supply function and can borrow against assets supplied, according to an algorithmically set collateralization ratio. Users earn fees — also through algorithmic code — where the amount earned is proportional to the amount of assets borrowed. The over-collateralization acts as a proxy for creditworthiness, ensuring that users return borrowed cryptoassets to access the greater value of their supplied cryptoassets.

Beyond exchanging and liquidity provision, users also engage in DeFi to participate in Ethereum staking and validation through a collective liquidity pool, which allows them to earn proportional validator rewards.

Developers have also created decentralized, autonomous protocols that allow for trading of crypto-derivatives (outside of the U.S.), as well as automated asset allocation and management, protocols that provide for "backstops" or "insurance" in the case of unanticipated events and even decentralized prediction markets (also outside the U.S.).

Although much of the types of activities described above harken to traditional regulated financial activity, the manner in which they occur is fundamentally different and thus, require different regulatory guardrails, as discussed in Section III below.

II. The Benefits of DeFi

DeFi offers unique benefits to users and participants in the system.

First, DeFi offers increased transparency. With open source licensing for DeFi protocols and related software, the rules of the code are open for all to see, audit and verify at all times such that users can know what will occur prior to engaging in any transaction. With protocols deployed on permissionless blockchains, all DeFi transactions are recorded publicly on blockchain ledgers in real time. The visibility of all transactions reduces information asymmetries and allows for

[14] Samuel Haig, *Uniswap Spot Volume Surpassed Coinbase In 2023*, The Defiant (Aug. 25, 2024), https://thedefiant.io/news/defi/uniswap-spot-volume-surpassed-coinbase-in-2023.

[15] "Protocol Categories," DefiLlama, https://defillama.com/categories (last visited Aug. 20, 2024).

[16] DeFi liquidity protocols hold approximately $31.4 billion in TVL. *See* Lending TVL Rankings, *supra* note 11.

verification of financial and economic data for users and protocols alike. This transparency can also allow for enhanced or new types of risk mitigation mechanisms.

Second, DeFi will improve the operational resiliency of the financial system (assuming the risks associated with DeFi are addressed appropriately). Notwithstanding certain seismic events from centralized players in the digital asset ecosystem in the last half of 2022, DeFi protocols withstood significant volatility, functioning as anticipated whereas the centralized crypto system experienced seismic shifts that caused user harm.[17] By further understanding why and how decentralized, software-based financial systems can withstand market volatility, we may be able to provide more robust underpinnings for our financial system that are not subject to failures or extreme volatility from large players in the system (*e.g.*, the 2008 financial crisis).

Third, DeFi can provide for expanded access to financial services by lowering barriers to entry, reducing prohibitive fees, and eliminating the types of discriminatory practices that can afflict the traditional financial system. While DeFi has not accomplished this feat at scale yet, given its innate characteristics of transparency and permissionlessness, it has the promise to do so. The permissionless nature allows anyone to build new applications at any time, and eliminates unknown or unaccounted for counterparty risk.

Fourth, DeFi brings increased efficiency to financial services in a number of ways:[18] whereas opening bank accounts can take days or weeks, a user can download a wallet and engage in a DeFi transaction within hours; capital is aggregated within and among DeFi protocols allowing for enhanced liquidity, which allows users to engage in all manners of financial transactions at their election; DeFi protocols operate 24/7/365, allowing for instantaneous settlement and immediate access to liquidity. "Inherently international markets have access to a larger pool of liquidity, significantly reducing transaction costs for all market participants."[19]

This does not mean that DeFi is without its own risks; however, the sources of those risks differ significantly from those in the traditional financial system. In fully decentralized systems, risk to users and to market integrity is borne primarily from technology risk and cyber risk, or from integration with centralized systems. By contrast, risk in the traditional financial system is borne primarily from concentration of data or information, centralized sources of failure (as witnessed with the Crowdstrike failure this past July), or errors in human or subjective judgment.

These benefits and the fundamental differences between DeFi and traditional financial services necessitates careful analysis when it comes to creating evergreen regulatory guardrails.

[17] *See e.g.*, *Gino Matos, DeFi protocols show resilience despite this week's macro crash: IntoTheBlock*, Crypto Briefing (Aug. 9, 2024) https://cryptobriefing.com/defi-market-resilience-tested/.

[18] Hilary Schmidt, *DeFi: A Cutting Edge Technology That Continues to Upend Traditional Financial Models*, Int'l Banker (Apr. 22, 2024), https://internationalbanker.com/finance/defi-a-cutting-edge-technology-that-continues-to-upend-traditional-finance-models/.

[19] Marvin Ammori, *Decentralized Finance: What It Is, Why It Matters* (Jun. 15, 2021) https://a16zcrypto.com/posts/article/what-is-decentralized-finance/.

III. Global Regulatory Approaches to DeFi

Global regulators have recognized the challenge in considering regulation of DeFi: the U.K.'s HM Treasury stated that "DeFi presents complex and unique challenges for policy makers and regulators".[20] This is consistent with the statement from the International Monetary Fund ("IMF") that "DeFi calls for creative risk mitigation" in any regulatory response,[21] and the Bank for International Settlements ("BIS") stating that "traditional regulatory approaches and tools may not be effective, implementable or enforceable for DeFi."[22]

Traditional laws attach to intermediaries: most financial laws in the U.S. are directed to "persons," which are defined as entities or natural persons who act affirmatively or must be regulated to do so in a way that brings integrity, fairness and transparency to the system. These current laws are not amenable to intermediary-less systems like DeFi. Global regulators have recognized the need for regulatory equivalence rather than imposing a "same risk, same regulation" framework.

To that end, DeFi has been excluded from any crypto-specific regulation to date. Recital 22 in the EU's Markets in Cryptoasset regulation ("MiCA") excludes financial services performed in a "fully decentralized manner without any intermediary," and the UK's HM Treasury stated that it would consider any regulation of DeFi at a much latter stage of any regulatory process. Japan — which enacted strict laws relating to crypto-asset exchanges and stablecoins – has not imposed any regulation of Defi nor have Singapore, Hong Kong, or the UAE, all of which have licensing regimes relating to centralized cryptoasset activity.

The most critical challenge in regulating DeFi is to ensure that any regulation does *not* force centralization into the system where it otherwise does not exist, as certain global regulators have suggested. There are ways to ensure the regulatory goals of protecting users, enhancing market integrity and combating illicit finance in DeFi systems that differ from regulation of the traditional financial system today.

Framing DeFi as purely financial services overlooks the realities of DeFi and critical tools that the government already has in ensuring the safety and security of the technological infrastructure underlying our current financial system. Grounding DeFi in its technological reality as a communications protocol, opens up new ways of thinking about achieving policy goals such as by classifying DeFi as "critical infrastructure,"[23] a concept that dates back to 1998 and that would put DeFi under the oversight of Cybersecurity and Infrastructure Security Agency, a standalone federal agency that is part of the Department of Homeland Security, which ensures that

[20] HM Treasury, *Future financial services regulatory regime for cryptoassets* (2023) https://www.gov.uk/government/consultations/future-financial-services-regulatory-regime-for-cryptoassets, at 66.

[21] IMF, *Elements of Effective Policies for Cryptoassets*, Policy Paper (Feb. 2023), at ¶ 59.

[22] Bank for Int'l Settlements, *Crypto, tokens and DeFi: navigating the regulatory Landscape* (2023), https://www.bis.org/fsi/publ/insights49.pdf, at 36.

[23] *See* Genuine DeFi as Critical Infrastructure, *supra* note 1.

the regulators are able to bring about appropriate rules and regulations in compliance with best practices for the protection of cyber systems. This is the topic of a recent paper I co-authored that describes when, why and how different parts of DeFi systems should be viewed as critical infrastructure and *not* financial services — and how doing so can achieve favorable policies that protect users.

IV. Conclusion

I appreciate the Committee's continued interest in the digital asset space generally and the efforts to understand this technology specifically. I look forward to your questions.