NO. 14–2022 OCTOBER 2022
FEDERAL RESERVE BANK OF ATLANTA'S *POLICY HUB*

Decentralized Finance (DeFi): Transformative Potential and Associated Risks

Francesca Carapella, Federal Reserve Board

Edward Dumas, Federal Reserve Bank of Boston

Jacob Gerszten, Federal Reserve Board

Nathan Swem, Federal Reserve Board

Larry D. Wall, Federal Reserve Bank of Atlanta

Summary:

Financial services in the crypto finance world are provided by a combination of centralized finance (CeFi) organizations and decentralized finance (DeFi). CeFi's are roughly similar to traditional financial intermediaries, but DeFi seeks to provide services using smart contracts (computer code) rather than an intermediary. DeFi's unusual structure creates some interesting potential but also raises new risks in addition to those already inherent in blockchains and crypto finance. This paper reviews some of the opportunities and risks.

Key findings:

1. Products offered by DeFis include lending, cryptocurrency exchanges, derivatives, payments, and asset management.
2. The use of DeFi's could mitigate some risks relative to the provision of services through traditional intermediaries.
3. However, DeFi's also create operational risks, some of which would arise in a "trustless" environment but others of which arise because the DeFi environment cannot be truly trustless.
4. Additional risks may arise from the interface of traditional and crypto finance.

Center Affiliation: Center for Financial Innovation and Stability

JEL Classification: G19, G23, G28, D23, D26, L14, L23, L86

Key words: Decentralized finance, blockchain, cryptocurrency, financial services, financial stability

https://doi.org/10.29338/ph2022-14

CENTER FOR QUANTITATIVE ECONOMIC RESEARCH

CENTER FOR HUMAN CAPITAL STUDIES

CENTER FOR FINANCIAL INNOVATION AND STABILITY

CENTER FOR HOUSING AND POLICY

ECONOMIC SURVEY RESEARCH CENTER

AMERICAS CENTER

Federal Reserve Bank *of* Atlanta

The Federal Reserve Bank of Atlanta's *Policy Hub* leverages the expertise of Atlanta Fed economists and researchers to address issues of broad policy interest. Our research centers coordinate this work and seek to influence policy discussions. Areas of interest include: forecasting, fiscal policy, and macroeconomics (Center for Quantitative Economic Research); financial stability, innovation, and regulation (Center for Financial Innovation and Stability); human capital, labor markets, health, and education (Center for Human Capital Studies); and government-sponsored entity reform, mortgage markets, and affordable housing (Center for Housing and Policy). Sign up for email updates at **frbatlanta.org/research/publications/policy-hub**.

Decentralized Finance (DeFi): Transformative Potential and Associated Risks

Summary:

Financial services in the crypto finance world are provided by a combination of centralized finance (CeFi) organizations and decentralized finance (DeFi). CeFis are roughly like traditional financial intermediaries, but DeFi seeks to provide services using smart contracts (computer code) rather than an intermediary. DeFi's unusual structure creates some interesting potential but also raises new operational risks in addition to those already inherent in blockchains and crypto finance. This article reviews some of the opportunities and risks.

About the Authors:

Francesca Carapella is a principal economist at the Board of Governors of the Federal Reserve System.

Edward Dumas is a lead market specialist at the Federal Reserve Bank of Boston.

Jacob Gerszten is a senior research assistant at the Board of Governors of the Federal Reserve System.

Nathan Swem is a senior economist at the Board of Governors of the Federal Reserve System.

Larry D. Wall is the executive director of the Center for Financial Innovation and Stability at the Federal Reserve Bank of Atlanta.

Acknowledgments: The authors would like to thank Toni Braun, Fang Cai, Peter Lone, Jillian Mascelli, Will Roberds, and Chiara Scotti for helpful comments. Staff working papers in the Finance and Economics Discussion Series (FEDS) are preliminary materials circulated to stimulate discussion and critical comment. The analysis and conclusions set forth are those of the authors and do not indicate concurrence by other members of the research staff or the Board of Governors, or the Federal Reserve Banks of Atlanta and Boston. A version of this article also appears on the website of the Federal Reserve Board of Governors and the Federal Reserve Bank of Boston.

Comments to the authors are welcome at larry.wall@atl.frb.org.

1 Overview

Decentralized finance (DeFi) refers to a set of newly emerging financial products and services that operate on decentralized platforms using blockchains to record and share data. DeFi products and services are conducted without a trusted central intermediary such as a bank, and they include payments, lending and borrowing, trading and investments, capital raising (crowdfunding), and insurance.

DeFi is a natural historical progression of financial services offered on blockchains. Nakamoto (2008) showed the potential for payment services to be provided without the involvement of traditional financial intermediaries in the white paper that originated Bitcoin and its blockchain.[1] Since the creation of Bitcoin, a variety of projects have been undertaken to expand the set of financial services provided on blockchains, with the potential of ultimately providing most, if not all, traditional financial services on blockchains. These services could be provided through firms that operate on blockchain(s) but otherwise look a lot like traditional financial intermediaries, an approach called centralized finance (CeFi) as opposed to DeFi.[2]

An important innovation that allowed for the development of DeFi was the growth of programming capability on blockchains. This innovation allows for the creation of computer code called smart contracts that can be invoked by users without going through a centralized intermediary. Smart contracts are used to create decentralized applications (dapps) that provide financial products and services. As we show in figure 1 the Ethereum blockchain is currently the most widely used dapp blockchain and hosts more than 470 dapps that represent 31 percent of the more than 1,400 currently operating dapps we have identified.[3] Many other blockchain platforms, including Avalanche and Solana, are emerging as popular dapp platforms as well. In addition, many dapps run on more than one blockchain.

Estimates of the cumulative gross value deployed in DeFi products and services range from $75 billion to more than $264 billion.[4] While this number represents a very small share of the global financial system, as we show in figures 1 and 3, the number of dapps is growing rapidly, as is the gross value deployed across various DeFi services. Nevertheless, the processing limitations of the early blockchains constrained DeFi's prospects. These limitations include the speed with which blocks are validated and added to the blockchain, the need for every transaction to be processed on the main blockchain and the rapidly increasing storage requirements for the cumulative transaction history on blockchains. However, a variety of

[1] Satoshi Nakamoto is possibly the pseudonymous author of the 2008 paper.
[2] For a comparison of CeFi and DeFi along with a discussion of their interaction, see Qin, Zhou, Afonin, Lazzaretti, and Gervais (2021).
[3] We use DeFi Llama to identify which protocols run on each blockchain. We exclude protocols that are running on Ethereum-based blockchains, such as Layer 2 chains, but that are not operating on the actual Ethereum blockchain.
[4] Sources such as DeFi Pulse define DeFi more narrowly and produce a lower range of estimates, while sources such as DeFi Llama define DeFi more broadly to arrive at the higher range of estimates.

changes that would substantially relax these constraints have been, or are in, the process of being implemented, such as the switch to "proof of stake" and the use of "sharding" (or breaking a blockchain into pieces or shards, and storing them in separate places) rollups, side chains, and Layer 2 scaling solutions.

Broadly speaking, there are two conceptual scenarios (not necessarily mutually exclusive) that could lead to a breakthrough in which blockchain finance may become an important provider of the services currently provided by off-chain financial markets and institutions. In one scenario, these blockchain services gain greater interoperability with the existing payments and financial system (for example, evolving to link real assets to public blockchains).[5] A second scenario may see crypto assets evolving to become a separate, parallel financial system that provides services for the real economy.[6] In either scenario, both CeFi and DeFi may pose financial stability risks that are exacerbated by the fact that both are currently largely outside the prudential regulatory perimeter.

Remedying many of these potential weaknesses is conceptually relatively easy for a large class of CeFi providers but could prove more challenging for DeFi providers. The existence of a centralized intermediary in the case of CeFi provides an entity that is potentially subject to regulation and with which the supervisors may be able to discuss their concerns (this notion may not apply to intermediaries located in countries lacking appropriate legal systems). However, DeFi products and services may not be so easily brought into the current supervisory and regulatory perimeter. As we discuss below, the way dapps are governed varies considerably, with some dapps not having any central authority that could be subject to prudential supervision and regulation.

In section 2 (Blockchain Basics), we review some basic aspects of blockchain platforms to provide context. In Section 3 (DeFi Products and Services), we describe the largest currently operating DeFi protocols and product offerings. In section 4 (Risk Implications of DeFi), we conclude by describing potential risks associated with these emerging technologies and use cases.

2 Blockchain Basics

This section provides a brief overview of key features of blockchain technology. Broadly speaking, blockchain platforms allow combining data blocks with innovative uses of technologies for the distribution and update of data onto a ledger shared by a network of

[5] See Carter and Jeng (2021) for a discussion of the many risks that arise from linking the existing financial system to the blockchain finance system, especially with regard to the linkages arising from stablecoins.

[6] The second scenario we outline, in which public blockchains evolve into a separate system, may manifest in a manner similar to the "dollarization" of some developing countries' financial systems. Should crypto markets develop along these lines, it would likely affect the Federal Reserve's ability to execute monetary policy.

computers. With blockchains, two points should be noted: only the last data block is needed to update the ledger, and consensus protocols regulate the way in which updates to the data set are proposed, reconciled, and recorded, while ensuring that no other previously validated data have been altered.

Blockchains can handle a wide variety of data, such as records, computer programs, or scripts. Thus, blockchains allow an extremely wide range of uses, which we describe in the subsequent sections of this paper.

2.1 Network of Computers

Blockchains record information in consecutive blocks and are maintained across potentially a large number of computers linked in a peer-to-peer network.[7] Such computers are referred to as "nodes" and are connected using ordinary internet protocols.[8] Each block contains batches of valid transactions and includes the cryptographic hash of the previous block in the blockchain, linking two successive blocks.[9] Transaction records are then replicated and available for all participants to access.

The first blockchain was implemented in 2009 and provided the distributed ledger for the cryptocurrency Bitcoin. This blockchain utilizes Proof of Work (PoW) as its consensus protocol to add a new block. [10] Under PoW, miners compete using computational power to find a solution to mathematical problems, and the solution generates an accepted hash for each block.[11] The system rewards successful miners by paying out new Bitcoin as well as fees paid for transactions included in the new block. As the number of transactions on the network increases, the amount of work required to generate a block also increases.

---

[7] While blockchain technology may be used on a network controlled by a central authority, all discussion herein pertains to blockchains deployed on a decentralized network that does not allow a single authority to control the network.

[8] As some computational and data storage requirements of the blockchain's functionality may be infeasible for some computers on the blockchain, some nodes may have limited functionality. For example, Bitcoin wallets running on smartphones may be used to transfer Bitcoin to another Bitcoin user (basically making a payment). However, they may not retain the entire Bitcoin blockchain. Moreover, some nodes may be granted special permissions that are not provided to other nodes. For example, only a subset of nodes may have capabilities and permissions to validate transactions.

[9] The essential property of a hash algorithm is that the chances of two files hashing to the same value are impossibly small. Therefore, it isn't possible for an attacker to produce a different file that hashes to the same value, resulting in a unique link between two blocks on the chain.

[10] A consensus protocol is a set of rules that provide a method to review and confirm what data should be added to a blockchain's record. Because blockchain networks typically don't have a centralized authority dictating who is right or wrong, nodes on a blockchain all must agree on the state of the network following the predefined rules, or protocol.

[11] See Centieiro (2021) for a discussion of the workings of PoW. A wide variety of alternative consensus mechanisms have been developed, and new ones are still being introduced. For a review of some of the most important consensus mechanisms, see Zhang and Lee (2020) and Cryptopedia Staff (2021).

2.2 Smart Contracts

Smart contracts are simple programs stored on a blockchain that run when invoked by a user.[12] They typically are used to automate the execution of an agreement without any involvement by an intermediary. Ongoing updates to the computing languages on blockchains as well as greater computing power are allowing for smart contracts that can be tailored to more specific needs. Similarly, the design of smart contracts to be caller agnostic (known as *composability*) allows for new smart contracts to build upon the functionalities of others into more complex protocols.[13] These protocols allow for more advanced financial use cases such as credit provisioning, insurance, and asset management.

The Ethereum blockchain (released in July 2015) popularized smart contract functionality on a blockchain network. Smart contract protocols enable lending, trading, encoding property rights, and gaming, among other uses. Anyone can deploy permanent, decentralized applications on the Ethereum blockchain. On the Ethereum blockchain, developers have created smart contract standards that provide simple templates for creating fungible tokens or non-fungible tokens (NFTs) that allow for a high level of interoperability.[14] Smart contracts can integrate real-world data in DeFi services via oracles, which are data feeds for specific information from sources off the blockchain.

3 DeFi Products and Services

As blockchains become more scalable and malleable through iterative technological innovation, they become better able to support the provision of a wide variety of financial services. Such innovations have helped the number of DeFi applications grow dramatically in terms of the number and scope of financial products and services offered. As noted earlier, we have identified more than 470 dapps operating on the Ethereum blockchain, representing roughly over half of the total value locked (TVL) in dapps, and each of these dapps offers users some kind of financial product or service. [15] Other blockchain platforms such as Terra, the Binance Smart Chain, Solana, and Cardano are emerging as popular blockchains for DeFi protocols as well. Many dapps provide discrete services rather than complex bundles of products such as we see from contemporary banks. However, new protocols are beginning to

[12] Interestingly, the concept of a "smart contract" was developed by Szabo (1997), before Nakamoto's (2008) Bitcoin blockchain paper.

[13] For more on composability in DeFi, see Schar (2021).

[14] Fungible tokens are interchangeable with each other, just as, for example, one genuine $5 bill is interchangeable with any other genuine $5 bill. In contrast, nonfungible tokens (NFTs) are not interchangeable with each other. NFTs may be used to represent claims on other digital or physical assets. NFTs representing claims on digital art, music, and sports collectibles have recently received considerable media attention (for example, see Zimmer 2021). However, NFTs could also represent claims on physical assets such as equipment or real estate.

[15] TVL is the standard measure of the resources committed to a dapp. However, as Fadilpašić (2021) observes, it is an imperfect measure for a variety of reasons, including the use of rehypothecation within DeFi.

offer a combination of several products in an attempt to become a "one stop shop" for financial services.

The key features of DeFi as currently practiced follow from its reliance on blockchains and the assets that currently exist on blockchains. Some of these features are inherent in DeFi, such as its use of smart contracts for execution and blockchains for clearing and settlement, and are summarized and compared with traditional finance in table 1.

Other features, such as governance, are evolving endogenously within the DeFi community. For example, instead of having a centralized decision-making process, some dapps utilize community governance, where governance token holders vote on proposals that determine the dapps' operation. Governance tokens represent voting power on a blockchain project and are unique to each project. For instance, the Maker lending protocol utilizes MKR tokens.[16] Any token holder can propose and discuss new policies in public forms, although most proposals originate from core groups of developers. For many DeFi protocols, one token equals one vote, and a simple majority of more than 50 percent is enough to execute a new proposal.[17] New proposals could include changes to collateralization levels, fees, and code updates.

However, if DeFi is to reach its imagined potential, some other changes will need to be made in the environment in which dapps operate. One such change that could significantly expand the scope of DeFi would be the development of mechanisms that grant on-chain tokens with legally enforceable claims on "real world" financial assets (such as corporate and consumer debt) as well as physical assets (such as ownership rights to buildings and other property).[18] Currently, most assets and liabilities for DeFi are *native tokens* and digital assets.[19]

Another generally important determinant of the rate of growth of DeFi generally is likely to be the development and adoption of a widely accepted and relatively stable cryptocurrency (or cryptocurrencies). At present, most cryptocurrencies (including the two biggest, Bitcoin and

[16] This documentation provides an explanation of the Maker protocol mechanism.
[17] Emerging alternative forms of governance votes include quadratic voting, where votes can be weighted by the number of voters and not simply based on the number of tokens. For an example of a protocol that uses quadratic voting, see Gitcoin. See Lalley and Weyl (2019) for more information on quadratic voting.
[18] DeFi protocols have faced obstacles to clarifying their legal rights regarding real-world assets. For example, liquidating off-chain assets in the event of a default could prove difficult for an on-chain protocol with no defined legal structure. Some protocols, such as MakerDAO, have begun creating or partnering with off-chain institutions to facilitate off-chain finance to overcome these challenges.
[19] Native tokens are integral parts of the operation of the network protocol they are issued on. They are often used to pay transaction fees or stakes in proof of stake systems. See Tasca (2019) for more on native tokens and their associated business models.

Ethereum) are highly volatile relative to sovereign currencies (such as the U.S. dollar).[20] One way to address the volatility problem may be through so-called *stablecoins*, in which the value of the coin is linked to a sovereign currency (or currencies). Many stablecoins exist, but concerns have been raised about the resiliency of stablecoins during periods of financial stress.[21]

An additional way to reduce the volatility of cryptocurrency prices might be for various aspects of DeFi to be more closely integrated to the existing financial system. This approach could take the form of the President's Working Group: Report on Stablecoins (2021) proposal that stablecoins should only be issued by insured depositories backed by deposit insurance and central bank liquidity facilities (such as the Federal Reserve's discount window). Finally, the creation of a central bank digital currency (CBDC) that becomes available on public, permissionless blockchains such as Ethereum may also serve to reduce volatility.[22]

In what follows we discuss the most prominent categories of DeFi products and services categories that have emerged so far, which include lending, exchanges, derivatives, payments, and asset management. We illustrate the growth of assets deployed in each of these categories in figure 1, and we list the 50 largest dapps in table 2. To date, whether DeFi products and services are primarily accessed by retail or wholesale investors isn't clear, due to the pseudonymity characterizing DeFi activity.[23] However, the recent emergence of start-ups aimed at bringing DeFi to the masses and of asset management platforms suggests that wholesale investors might be behind the lion's share of DeFi's growth so far.[24] The direct implication of a fast growth in DeFi predominantly driven by wholesale and possibly institutional investors would be the relevance of financial stability considerations even with a

[20] Graphs of the value of select cryptocurrencies, including Bitcoin and Ethereum, relative to the US dollar are available through FRED at the Federal Reserve Bank of St. Louis: https://fred.stlouisfed.org/categories/33913.

[21] See the President's Working Group: Report on Stablecoins (2021) for a review of the various concerns with existing stablecoins.

[22] Virtually all the central banks in the developed world are at least studying CBDC, if not moving toward implementing a CBDC. See Federal Reserve Board (2022) for a discussion of the issue from a US dollar perspective.

[23] Retail payments typically relate to the purchase of goods and services by consumers and businesses. Each of these payments tends to be for relatively low value, but volumes are large. In contrast, wholesale payments are between financial institutions. These are typically large-value payments that often need to settle on a particular day and sometimes by a particular time. While there are significantly fewer wholesale payments compared with retail payments, their value—both individually and in aggregate—is much larger. Given their systemic importance, wholesale payment systems are generally owned and operated by central banks.

[24] For the former, see Eyers, James (2022), "Tiiik preparing to bring crypto saving to the masses," February 18, 2022. For the latter, see Ribbon Finance or StakeDao.

volume of trades in the DeFi ecosystem far from the orders of magnitude seen in the traditional financial system.[25]

3.1 Lending

Decentralized lending platforms allow users to deposit collateral in the form of cryptocurrency assets and receive assets, typically dollar-denominated stablecoins, in return.[26, 27] Approximately one-fifth of all crypto assets locked in DeFi protocols, worth more than $50 billion, are associated with lending platforms, as figure 2 shows. Debt obtained on lending dapps incurs fees (continuously accruing interest), which are paid upon repayment of borrowed stablecoins or other currency.

Fees are often denominated in a platform's *governance token*.[28] Holders of these governance tokens can vote on the platform's risk parameters, such as collateral ratios and fee levels. Governance token holders also act as the last line of defense in case of a "black swan" event for certain protocols. For example, if system-wide collateral value rapidly falls, additional governance tokens can be minted and sold on the open market to raise funds to cover any outflows or shortfalls in collateral. Holders of governance tokens assume the risk that their holdings may be diluted to support the platform's stability.[29] The possibility of token supply dilution provides an incentive for token holders to govern the system well.

Borrowers often take out DeFi loans to retain exposure to price movements in the collateral they post, while using the loan to purchase other assets or to finance consumption (similar to taking out a margin loan against a stock portfolio). Lenders may earn an interest rate that exceeds rates offered by banks on sovereign currency denominated deposits (such as

---

[25] Traditional market players' initiatives in the DeFi space abound. Examples, among many, are JPM coin, RLS, Partior, and USDF (see Giulia Secco's March 9,2022, article, "The future is tokenised, collaboration between market players is key."

[26] The normal requirement that DeFi loans be secured by cryptocurrency impose significant limits on the uses of these loans relative to bank intermediated loans. DeFi lenders typically cannot rely on physical collateral (such as a house or the inventory of a firm) because they lack the ability to obtain a perfected security interest in the collateral. DeFi lenders cannot make unsecured loans (such as credit card loans) because the borrower is typically anonymous, thus limiting both the ability to trade on the borrower's reputation and the ability to pursue claims against the borrower through the judicial system.

[27] See Xu and Vadgama (2022) for a discussion of the relationship of traditional lending to CeFi and DeFi lending.

[28] Governance tokens are tokens that provide holders with governance (or voting) rights within a particular protocol, game, or dapp. Token holders have the power to influence decisions concerning the core protocol, product, or feature roadmap; hiring and staffing; and changes to governance materials. See Governance Tokens - Glossary | Smith + Crown (smithandcrown.com).

[29] In addition to the risks assumed by borrowers and lenders, holders of governance tokens also assume some degree of risk because many governance tokens embed mechanisms to raise funds to limit platform disruptions.

standard US dollar–denominated savings deposits).[30] Although the loans are overcollateralized, lending protocols still face exposures to fluctuations in the price of the underlying collateral asset.

Similar to more traditional (non-DeFi) securities lending practices, DeFi lending platforms generally allow users to borrow up to a limit determined by the quantity and type of collateral provided, typically significantly less than 100 percent of the collateral value. For instance, Maker, one of the largest DeFi lending platforms, caps borrowing at 66 percent of the collateral value. If the value of the loaned funds drops below this limit, users are forced to pay additional fees and could lose their collateral. A smart contract allows a third party to liquidate the collateral by converting it into the cryptoasset in which the debt was denominated.[31] Different lending platforms adopt different mechanisms to redistribute the liquidated collateral assets. The current overcollateralization requirements for DeFi loans could be relaxed by token holders through a dapp's governance mechanism (as we discuss below) if a successful system for establishing reputation on a blockchain were implemented.[32]

Along with collateralized loans, *flash loans* are a new type of uncollateralized lending product in which the funds are borrowed and repaid in the same block of transactions (an "all or nothing" execution). Legitimate uses of flash loans include arbitrage and collateral swaps (see Wang et al., 2021).[33] Despite the fact that flash loans are free of credit risk (from the perspective of the lender), they might introduce risks of different kinds. One such risk results from price impacts that may result from outsized trades (not otherwise constrained by collateral requirements) made using flash loans. Additional risks might stem from price and market manipulations, which have yet to be regulated in DeFi like they are in traditional financial systems. Across all these scenarios, a likely consequence of a sudden decrease in the price of certain assets is the forced liquidation of debt positions used by those assets as collateral. This outcome, in turn, might trigger further declines in the prices of other assets, thus resulting in a cascade of liquidations.

[30] Currently, rates on DeFi platforms typically exceed those offered by banks on retail deposits because the lender is taking more risk, and the borrower expects to make higher rates of return on speculative cryptoasset investments.
[31] A fully developed legal framework for the resolution of losses or other disputes relating to smart contracts has not been established.
[32] See Clear Chain Capital (2021) for a discussion of the current alternative approaches to undercollateralized DeFi lending. This survey notes that many approaches are vulnerable to borrowers' ability to adopt a new virtual identity after defaulting on an obligation. The survey suggests that some link to borrowers' real-world identity may be needed to overcome this problem.
[33] See Qin, Zhou, Livshits, and Gervais (2021) for a discussion of how flash loans can also be used to profitably attack DeFi ecosystems.

Largest Current Lending DeFi Protocols by Total Value Locked[34]

Name	Chain	Total Value Locked (USD $B)
MakerDAO	Ethereum	8.67
AAVE	Ethereum, Avalanche, Polygon	7.52
Compound	Ethereum	3.81
JustLend	Ethereum	2.94
AAVE V3	Multi	1.39

Source: DeFi Llama

3.2 Decentralized Exchanges

Decentralized exchanges (DEXs) facilitate trading of cryptoassets without the use of centralized market making or centralized order books. Exchanges represent the largest category of decentralized financial activity with more than $65 billion locked (as figure 2 shows). Whereas central limit order books match up individual buyers and sellers to execute a trade, DEXs link buyers and sellers to funds held in smart contracts.

DEXs typically operate by maintaining crowdsourced collections of cryptocurrencies, called liquidity pools (LPs), which are locked into smart contracts. Each available trading pair on most DEXs requires a unique liquidity pool.[35] Investors, referred to as liquidity providers, deposit equal amounts of two tokens into these liquidity pools to create a market for a given trading pair. Liquidity providers earn "fees" (interest) on their deposits based on the fee rate for the pool and the relative percentage of crypto assets provided to the pool by the liquidity provider. Users exchange tokens by swapping one asset for another in and out of the liquidity pools. Unlike centralized exchanges, DEXs never take custody of user funds, which is important because some centralized exchanges have been hacked which resulted in a loss of customers' cryptocurrency lost.[36]

DEXs are powered by automated market maker (AMM) protocols that use algorithms to define the price of digital assets in the pools.[37] The most basic and commonly used equation to determine token prices is to have the product of the values of each token in a liquidity pool equal a constant. If users have high demand for one asset and begin to withdraw it, the price of that asset will increase, while the price for the other asset decreases, thus creating an

[34] See table 1 for more information on rankings.
[35] Some protocols (such as Balancer or Curve) allow for liquidity pools with more than two tokens, with each token having an independent weight corresponding to its proportion of the total pool value.
[36] For example, see the list of crypto exchange hacks through February 2020 is available at https://selfkey.org/list-of-cryptocurrency-exchange-hacks/. Decentralized exchanges are also subject to certain risks, including that of getting hacked. For more information, see https://www.coolwallet.io/decentralized-exchange-dex-security-guide/. In addition, the SEC has issued guidance relating to crypto assets, which is available at SEC.gov | Staff Accounting Bulletin No. 121.
[37] For a more comprehensive explanation of decentralized exchange mechanisms and automated market makers, see Mohan (2021) and Xu et al. (2022).

arbitrage opportunity for liquidity providers, and the prices of both assets come back in line with their market prices.

Largest Current DeFi Exchange Protocols by Total Value Locked

Name	Chain	Total Value Locked (USD $B)
Curve Finance	Multichain	7.49
Uniswap	Multichain	5.43
PancakeSwap	Binance Smart Chain	3.78
Balancer	Multichain	1.79
SUNSwap	TRON	0.94

Source: DeFi Llama

3.3 Derivatives

Various dapps allow users to create synthetic assets on blockchain platforms that track the value of off-chain/"real-world" assets, as well as other on-chain assets.[38] Through these dapps, users can get price exposure to other digital assets, currencies, commodities, stocks, and indices. Derivatives remain a relatively small segment within DeFi with only $3.6 billion locked in synthetic assets. Much like DEXs discussed earlier, DeFi derivatives services connect buyers and sellers directly, using collateral pools. Derivatives contracts are codified in smart contracts in a way that provides incentives for people or off-chain bots called keepers to trigger a transaction that executes margins.[39] Some derivatives dapps allow users to buy and sell synthetic exposure to digital assets without actually holding the underlying asset. These derivatives can be associated with leverage, magnifying gains and losses, or inversely connected with the asset price, providing the equivalent of short exposure. Indeed, Aramonte, Huang, and Schrimpf (2021) document that two decentralized derivatives exchanges allow 25x leverage.[40] Other applications of derivatives involve prediction markets, where users can bet on the outcome of future events.

Largest Current DeFi Derivatives Protocols by Total Value Locked

Name	Chain	Total Value Locked (USD $B)
dYdX	Ethereum	.97
Keep3r Network	Ethereum	.57
Synthetix	Ethereum	.38
GMX	Avalanche, Arbitrum	.34
Perpetual Protocol	Ethereum, Optimism	.519

Source: DeFi Llama

[38] For "a hopefully comprehensive guide to the defi derivative landscape," see here.
[39] See Harvey, Ramachandran, and Santoro (2021) and Werner et al. (2021) for a discussion of the role of keepers.
[40] That said, Aramonte et al. (2021) also find that two CeFi exchanges allow 100x or more leverage.

3.4 Payments

Decentralized payment networks refer to a wide variety of dapps that allow users to privately hold and transact using cryptocurrencies, stablecoins, and reward points. Each dapp aims to overcome one or more obstacles posed by decentralized technology, including issues with efficiency, interoperability, and privacy, to provide a user experience that mimics payments in traditional finance. Some payment platforms give users the ability to spend their assets to purchase off-chain "real world" goods and services either in person or online. We describe the most prominent forms of payment dapps below.

To achieve instant and secure transactions, one method dapps use is running payment transactions on proprietary networks while still authenticating the transactions on a blockchain. For example, the Flexa app operates its own payment system that takes a user's crypto assets and immediately sends them to another user, often a merchant.[41] To protect the recipients from the risk of not receiving a payment while the transaction is being processed on a blockchain, each transaction is collateralized. Flexa rewards investors who provide collateral by paying them a small reward for each successful transaction.

Other payment networks, such as Tornado Cash, allow users to transact with enhanced privacy. In a typical transaction on a blockchain network, the addresses of both the sender and receiver are publicly visible. To achieve additional privacy, Tornado Cash uses a smart contract that accepts deposits from one address and allows withdrawals of those deposits from a new address. The new address must prove that it is authorized to withdraw the funds, but there is no on-chain link between the two addresses, allowing for increased privacy of the transaction. These protocols are sometimes referred to as "mixers" or "tumblers."

Although newer blockchain designs provide for greatly increased throughput, the quantity and timeliness of on-chain payments on Bitcoin remain severely limited by the blockchain's protocol. The Lightning Network was created as an off-chain way of relaxing the limitations of Bitcoin by processing transactions off the main blockchain.[42]

Largest Current DeFi Payment Protocols by Total Value Locked

Name	Chain	Total Value Locked (USD $B)
Tornado Cash	Ethereum	0.31
Flexa	Ethereum	0.24
Sablier	Ethereum	0.07
Lightning Network	Bitcoin	0.08
Superfluid	Polygon, Gnosis	0.02

Source: DeFi Llama

[41] See Spalding (2021) for a discussion of how Flexa is intended to work and its potential applications.
[42] The Lightning Network was conceived in a paper by Poon and Dryja (2016).

3.5 Asset Management[43]

DeFi asset management protocols assist investors by combining their tokens into pools using smart contracts, often for use on other dapps. These pools capture traditional exposure, synthetic structured tokens, or interest-bearing accounts. The pools function as a diversified portfolio of digital assets, which can then be tokenized and sold to investors. One example of an asset based on these pools are capitalization-weighted indices, which track the value of various underlying cryptocurrencies. The tokens that represent these indices give investors the opportunity to gain low-cost exposure to a basket of assets that are rebalanced at regular intervals using smart contracts. As we show in figure 1, the total amount of assets locked in asset management platforms has grown to $30 billion.

Another DeFi business model related to asset management are *aggregators* that interact with other lending protocols. Aggregators take investors' digital assets and convert them to the protocol's native token, which then is deposited into the most profitable lending service. As the rewards for the lending protocols change over time, the aggregators rebalance the native token to optimize payouts for investors.[44]

Largest Current DeFi Asset Management Protocols by Total Value Locked

Name	Chain	Total Value Locked (USD $B)
Lido	Ethereum	6.56
Convex Finance	Multichain	4.57
Arrakis	Ethereum	1.13
Yearn Finance	Ethereum	1.03
Beefy Finance	Multi	0.36

Source: DeFi Llama

4 Risk Implications of DeFi

The rapid growth in the number of DeFi apps, the growing scope of financial products that DeFi apps offer, and their growing use represent interesting opportunities for lowering costs, expanding access, and increasing transparency. The DeFi ecosystem is currently somewhat small relative to the overall financial system. Therefore, even relatively large disruptions in DeFi would pose minimal implications for the financial stability of the overall financial system. However, if current trends continue, many of the risks we discuss in this section will likely have financial stability implications for the broader non-DeFi financial system. In addition, the current developments in DeFi have the potential to trigger a DeFi version of a financial crisis, possibly with spillovers to the traditional financial system. The ability to build large leveraged positions and to conceal trades to some extent, combined with the novelty of the financial

[43] We base the categories of DeFi financial services in this section (lending, decentralized exchanges, derivatives, payments, and asset management) on those at DeFi Pulse, and these categorizations evolve over time. Currently, we define "asset management" as comprising the yield, yield aggregator, and indexes subcategories.

[44] See also Schär (2021) for a discussion of on-chain asset management protocols.

products allowing such leverage, have been common elements in the history of financial crises of the past century. If DeFi products become sufficiently widespread, a sparking event that undermines confidence in the levered positions might generate a financial crisis.[45]

Some of the types of activities that participants in finance conduct through DeFi pose risks similar to those in traditional finance—such as excessive leverage, maturity and liquidity transformation, etc., and there are similar sets of tools for managing those risks as manifested in traditional finance. However, important operational differences between DeFi and traditional finance as it is currently conducted exist that may have important risk implications.

The extent to which these operational risks have the potential to destabilize the financial system depends to a large extent on the magnitude of the potential losses, especially in the upper tail of the distribution of potential losses. Operational risks (op-risks) exist throughout the traditional financial system. The overwhelming majority of the losses, in the traditional financial system, associated with op-risk are merely a cost of doing business and are not material (individually or in aggregate) to the participant's financial conditions. These potential operational losses raise the cost of providing and using some services but do not raise financial stability concerns. However, operational losses can be so large that they impair the ability of a market or institution to provide services and/or impair users' willingness to rely on the institutions and markets suffering the operational losses.[46]

DeFi can reduce some operational risks inherent in traditional finance, particularly those associated with reliance on centralization of financial intermediation activities. However, DeFi also poses new types of operational risks, which we discuss below.

The following subsections discuss some of the benefits and risks of DeFi. The first subsection considers some operational benefits DeFi may have in reducing risks. The next section considers DeFi op-risks in a trustless environment and then in environments involving a trusted third party. The last subsection focuses on risks involving the interaction of DeFi with traditional finance as well as other aspects of crytpo finance.

4.1 Blockchain and DeFi Risk Mitigation

The operation of traditional finance creates various risks that may be reduced or eliminated by blockchains. One such set of risks arises because many clearing and settlement processes in traditional finance do not settle in real-time. For example, most checks take two days to clear, and most stock transactions take two days to settle. In part, these delays are a legacy of paper-based systems, which needed extra time for processing. However, in some cases the

[45] The past two centuries offered plentiful experience with these types of events, which showed that loss of confidence in some financial products, or the providers or those products, can have effects that reverberate through the financial system.

[46] For example, Roberds (2022) discusses how counterfeiting problems in the early 1800s led the Bank of England to withdraw £1 and £2 notes from circulation.

delay still has compensating benefits. For example, the delay in stock settlement gives buyers time to move funds into their settlement account and gives short sellers time to source the stock. In either case, these delays create the risk that one's counterparty will default on their obligation when it comes time to settle the transaction. Traditional financial intermediaries mitigate this risk in various ways, such as by placing holds on check deposits and requiring margin from stockbrokers. The clearing and settlement of blockchains, on the other hand, are done nearly in real time, with transactions cleared and settled as the block recording the transaction is added to the blockchain.[47]

A second concern that arises with traditional finance is that of identifying and aggregating the risk exposure of market participants. Traditional finance provides a number of ways to become exposed to various financial risks. Some venues, such as organized exchanges, require participants to provide information about their exposure. However, other ways of obtaining risk exposure, such as through the use of multiple dealers or over-the-counter derivatives, are not reported to a central authority and for which only the participant is in a position to calculate the aggregate risk exposure.

The details of all exposures arising from a DeFi transaction are recorded in a pseudonymous address on a blockchain. Prudential supervisors could easily aggregate exposures in real time if the entities subject to such regulation provide their blockchain address(es) to the supervisor. Moreover, even if a regulated entity sought to hide some of its exposures, pseudonymity does not necessarily guarantee true anonymity in practice. Blockchain analysts have found that it is often possible to associate an address with a specific person or institution by observing transaction counterparties and amounts associated with addresses. Thus, regulated entities that try to hide their blockchain transactions would risk exposing themselves to substantial penalties if supervisors discovered their undisclosed addresses.

A related benefit of DeFi over traditional finance is the simplification of audits. Auditors in traditional finance often need to contact counterparties and custodians to verify the accuracy of an institution's financial statements. This process is simplified with DeFi, where a public blockchain contains all transactions and balances.

The increased transparency of DeFi relative to traditional finance, however, comes at a price. Financial institutions do not want to make their transactions and exposures available to other traders in financial markets for competitive reasons. For example, revealing an institution's trades and positions would expose an institution to front-running, and possibly short squeezes, by other market participants.

[47] The only delay arises from the fact that the parties should wait for several blocks to be added before their transaction is considered final on blockchains using PoW consensus. At worst, this delay is typically far shorter than that arising in many areas of traditional finance.

A third feature of traditional finance is its reliance on trusted third parties. In some cases, trusted third parties could censor (or prevent) account holders from transacting and/or maliciously change transactions and account balances. Indeed, such censorship is the goal of laws designed to prevent money laundering and the financing of terrorism, as well as laws that impose financial sanctions on individuals and institutions.[48]

Blockchains are designed to be censor resistant, in that they contain no mechanism for blocking transactions that are otherwise in compliance. Whether a given dapp censors transactions will depend on its authors. In principle, it would be possible for a dapp to contain code to block transactions from certain addresses (likely via consultation with an external oracle). In any case, the benefit of censorship resistance seems to be limited by the ability of the authorities to impose limits the physical transactions of individuals and institutions. For example, a government could limit a firm's ability to use DeFi to avoid sanctions by ordering the firm's suppliers to accept only payments coming from approved blockchain addresses.

We believe that the concern that trusted third parties might maliciously rewrite history is overstated. Part of any rents that traditional financial intermediaries earn arises from their reputation as trustworthy keepers of financial records.[49] Any intermediary that violates this trust would risk losing that reputation and the associated rents. Moreover, any such malicious activity by an intermediary would expose the intermediary to civil suits seeking recovery of the lost sums and the perpetrators to potential criminal prosecution.

Moreover, the claim that blockchains are immutable and therefore immune to the risk of malicious change is somewhat overstated. As discussed above, no successful attacks have been launched on the two most important blockchains (currently Bitcoin and Ethereum). However, successful for-profit attacks have occurred against other blockchains in which supposedly immutable records have been maliciously rewritten. Additionally, changes to the blockchain protocol that erase previously accepted transactions can and do occur. Moreover, immutability is not necessarily a benefit in all cases as blockchain transactions that involve fraud or theft might not be reversed as quickly or easily as they would in traditional finance.

4.2 Operational Risk in a Trustless Environment

In principle, DeFi and the blockchains on which it operates are intended to create a trustless environment. All transactions take place in the open where any party has the ability to verify the validity of any or all transactions. Additionally, many dapps are on a public blockchain and so anyone can verify transactions. In principle, this openness aims to eliminate the need for

[48] Recent examples of such censorship include the Canadian government freezing the bank accounts of truckers protesting vaccine mandates and the sanctions imposed on various Russian interests after that country's invasion of Ukraine.

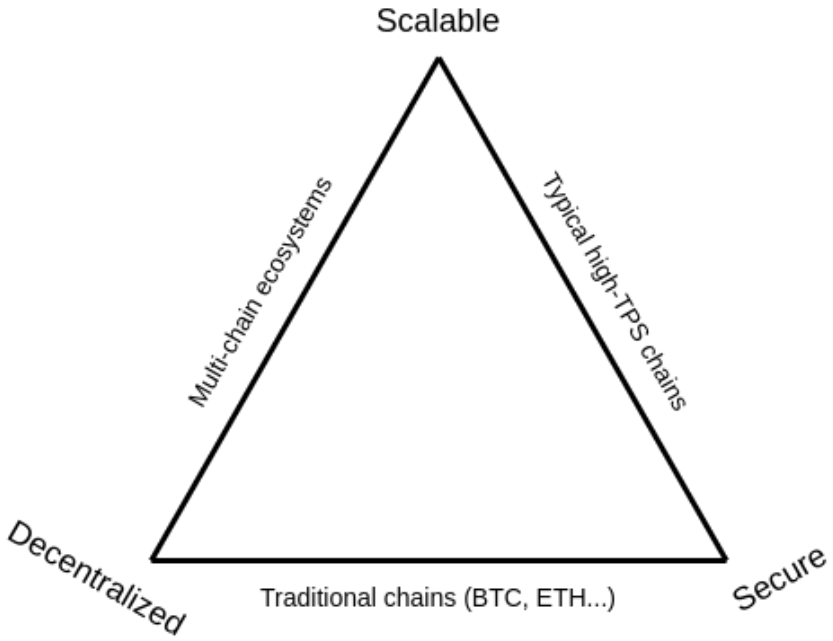
[49] See Fang (2005) for a discussion of how reputation relates to the behaviors and performance of financial institutions.

participants to trust each other. Rather, they can trust their own verification of the blockchain and the dapp.

In the following section, we will address whether a truly trustless environment is feasible. The purpose of this section is to address some of the potential operating risks that would exist even in a trustless environment.

The Blockchain Trilemma: Blockchain protocols are subject to the so-called "Blockchain Trilemma," so called because blockchain technologies can provide decentralization, scalability, and security.[50] The trilemma holds that the tradeoff among these three desirable features makes it possible to obtain any two but not all three at the same time. As an illustration of these tradeoffs, Ethereum is planning to switch its consensus protocol from Proof of Work (PoW) to Proof of Stake (PoS). This switch is intended to improve scalability through improved processing speeds.

The Blockchain Trilemma



Source: https://vitalik.ca/general/2021/04/07/sharding.html

Both PoW and PoS enhance security regarding potential fraudulent validations by randomizing which validator validates a specific block. In the case of PoW, that randomness results from the likelihood of successfully solving a difficult guessing game, whereas PoS applies a random selection algorithm. In both cases, the probability of being able to add a

[50] The blockchain trilemma is widely attributed to Vitalik Buterin. See Buterin (2021a) for a discussion of the trilemma and why he thinks that "sharding" will solve the problem.

block increases with the amount of resources devoted to being selected. However, as the resources devoted by one agent (or group of agents) exceeds 50 percent, the agent gains the ability to engage in what is called a *51 percent attack*. Successful 51 percent attacks allow the attacker to substitute new blocks for blocks that had previously been considered final. Among the problems created by this ability to substitute in new blocks is that the attacker is able to recover cryptocurrency that had previously been "spent" and spend it a second time—which is called *double spending*.[51] However, some would argue that the switch to PoS might reduce security even further.[52]

A further concern with consensus protocols is that they are typically validated in a game theoretic framework in which the object is to show that no one can earn an economic profit from attacking a blockchain. However, even to the extent a successful attack would result in economic losses, it is possible that an agent might attack a blockchain for reasons other than economic profit. For example, a state-sponsored entity could attack a blockchain to damage its enemies.

Smart contracts: Dapps are a type of smart contract, but smart contracts are merely computer programs written to run on a blockchain. A common problem with computer programs is that they contain mistakes, or bugs. Careful review of the code readily finds some of these bugs, but many others are subtle and arise only in particular circumstances. In many instances, smart contracts had design weaknesses that allowed hackers to obtain funds inappropriately.

The decentralized autonomous organization (DAO) hack on the Ethereum blockchain in June 2016 is one of the more famous examples. After the DAO raised approximately $150 million, a hacker exploited vulnerabilities (including recursive calls) that resulted in the transfer of Ether valued at the time at least $40 million.[53] The development of best practices should decrease the risk of many types of coding errors, and code reviews and external audits might reduce these risks further. However, even audits are no guarantee to solve the problem, as Werner et al. (2021) find that successful security exploits can occur on audited as well as unaudited protocols.

A second issue with smart contracts is that computer code specifies what is to happen in every state of the world, including those states where one party defaults on their smart

[51] Neither the main Bitcoin nor Ethereum blockchains have yet been the subject of a successful 51 percent attack, but many other smaller blockchains have been successfully attacked. For an example of how such an attack was conducted on an Ethereum clone called CheapETH see Copeland (2021). See also Budish (2018) for analysis suggesting that Bitcoin may become more vulnerable to a 51 percent attack as the value of individual transactions increases.

[52] See here for a high-level discussion of how PoW and PoS work, and Makarov and Schoar (2022) for a discussion of some of their vulnerabilities.

[53] In response to this hack, a hard fork was executed on the Ethereum blockchain to return the funds to their original investors (see here and here).

contract obligations. Advocates for smart contracts consider this design one of their advantages. However, Wall (2016) notes that economists and lawyers have long recognized that most non-smart contracts (for example, paper contracts) are intentionally left incomplete in important ways for a variety of good reasons. One such reason is that the cost of specifying and negotiating terms for the full, complete set of relevant scenarios would far outweigh the benefits. Create an opening for the parties to renegotiate the contract is often more cost effective.

In principle, it would be possible to design a dapp that automatically halts execution under certain conditions to allow the parties to renegotiate their contract. However, the anonymity of blockchain participants could complicate the two sides' ability to determine with whom they should negotiate.

A related problem is that smart contracts are designed to incentivize *keepers* to trigger transactions whenever certain conditions specified in the contract are met.[54] This design can be problematic in situations where the two parties to the contract would prefer negotiations.

Automatic execution can also exacerbate tensions in a financial market. For example, automatic contract execution might be problematic: without trading halts, DEXs could facilitate extreme price moves in response to smart contract executions in certain circumstances.

Custodial Risk: To execute transactions using their tokens, users must either supply the private key or delegate custody to a third party. The loss or theft of private keys can result in the loss of access to and/or ability to retrieve records, and the losses are substantial. For example, Popper (2021) reports that an estimated 20 percent of outstanding Bitcoin have been lost.

Ordering of Transactions: As noted above, the typical block contains multiple transactions. The order in which these transactions are added to a block is under the control of the winning miner (or staker in PoS), thus creating the potential for the miner to order transactions in a way that is profitable to the miner.[55] It also creates potential for users to partially control the timing of their transaction by setting a high fee for early execution or a low fee for later execution. An advantage of going early is the ability to front-run other transactions, obtaining a better price. Conversely, a back-running strategy is one where the transaction is executed after some other transaction. An attack that uses both front-running and back-running is called a *sandwich attack*. One example of a sandwich attack is that of front-running to create an imbalance on an AMM prior to the execution of another transaction on that AMM. After front-running, the attacker then back-runs to close out their position and earn a profit.

[54] See Werner et al. (2021) for a discussion of how keepers are motivated and their role in dapps.
[55] See Werner et al. (2021) for a discussion of transaction ordering attacks.

The term for a miner's ability to use their control over the ordering of transactions is called *maximal extractable value,* or MEV.[56] Carter and Jeng (2021) observe that "Most researchers consider MEV endemic to blockchains … where transactions on decentralized exchanges … are transparent."[57] They note that some Ethereum developers have proposed allowing miners to auction off the rights to reorder transactions, making MEV a form of compensation to miners (validators).

Oracle Risk: depend on data from off-chain data providers called *oracles*. An example of an oracle is a cryptocurrency exchange that provides prices that are used to trigger margin calls or liquidation. The dapp cannot perform as intended if the oracle fails to provide information in a timely manner or if the information has been tampered with. An example of tampering is when an attacker undertakes large trades in an exchange in order to alter the market price. Harvey, Ramachandran, and Santoro (2021) note that the attacker could even suffer losses from an attack on the oracle provided the profit from corrupting the price exceeds the cost of corrupting it.

Maintaining Liquidity: Transaction validation and other essential operational aspects of DeFi protocols require effort and resources on the part of participants. Most blockchains issue new native tokens as compensation for performing those activities. Many DeFi participants hope that widespread adoption of the blockchain will attract additional liquidity to enable its long-term viability. However, developers are constantly working on new protocols to address the limitations of existing protocols and create new functionality. In this event, some of these new protocols might be so successful that they could displace some current blockchains. Should this happen, liquidity might dry up in the obsolete blockchain leaving no one left to perform the tasks necessary to ensure ongoing operation of the blockchain protocol. In such cases, some assets could become trapped and no longer useable.

Regulatory Risk: Financial regulation often follows as a result of abusive behavior, fraud, and bouts of financial instability. It is no surprise that financial regulators are increasingly investigating blockchain financial activities, using their existing authority to restrict activity, and seeking new authority over blockchain based finance. Such regulation may facilitate the growth of financial activities by providing increased confidence to potential users of the

[56] See here for a longer definition. In addition, Carter and Jeng (2021) argue that MEV is analogous to a hedge fund paying for order flow to transact against uninformed traders. However, MEV seems closer to what has long been called front-running in financial markets, which occurs when those with advance knowledge of large transactions use that knowledge to draw down available liquidity at a lower price and then sell into the large transaction at a higher price.

[57] Qin, Zhou, and Gervais (2021) provide an estimate of the gains from sandwich attacks on seven decentralized exchanges and liquidations on three lending platforms. They also argue that such attacks not only affect those directly involved but could potentially endanger a blockchain's security.

services, but it can also have unintended adverse consequences for existing DeFi and its future development.

4.3 Operations Risk in an Environment with a Trusted Third Party

The goal of achieving a truly trustless financial system is unlikely to ever be fully realized. The cost of verifying every block of the blockchain and every dapp code used (and the interactions among the different computer codes) would impose a very heavy burden on every user, even users who are skilled in both computer and economics. Moreover, if crypto is to become a mainstream product, then it is going to be widely used by people who lack the ability to adequately assess the programming and economic risks associated with their crypto transactions. These people are necessarily going to need some level of trust in third parties, yet this very reliance creates some additional risks.

Blockchain Governance: The blocks in a blockchain are often claimed to be "immutable," but the computer code underlying the operation of a blockchain cannot be immutable.[58] A blockchain's protocol may contain errors (or bugs), as is the case with almost all code. Additionally, opportunities may arise to improve the functioning to increase its efficiency or add new features. This ability to change the protocol, however, raises a governance question: what process does someone follow to make changes to the protocol? This question includes not only who makes the final decision on changes, but who is authorized to draft changes to the protocol and who decides which draft changes are considered for adoption.[59]

In practice, the extent to which the governance of a blockchain is decentralized is better thought of as a spectrum rather than a discrete choice between two opposites.[60] For example, even when the final control over changes to a blockchain's protocol resides with a decentralized group of stakeholders, the group that founded the blockchain often still exercises substantial influence over its evolution.[61] From a stability perspective, the advantage of more centralized approaches someone can be expected to respond promptly to any errors that are discovered in the protocol and someone to contact to discuss supervisory concerns.

[58] The fact that the protocol is not immutable also implies that the blockchain ledger is also not immutable. Bitcoin has effectively unwound valid additions to the blockchain both in responding to a flaw in the protocol resulting in a hard fork in 2010 (Worah, 2019) and in the deliberate decision to fix an upgrade related problem by allowing a shorter blockchain to overtake a larger blockchain (Andresen, 2013).
[59] See Kiayias and Lazos (2022) for a discussion of many dimensions of blockchain governance and an analysis of how some of the more important blockchains compare along these dimensions.
[60] For a high-level overview of some of the issues associated with blockchain governance issues, see Wall (2018). For a recent critique of the issues by one of the founders of Ethereum, see Buterin (2021b).
[61] Specifically, regarding a final vote, attempts are being made to provide more clarity over blockchain governance through the use of governance tokens for some blockchains.

However, such centralized control goes against the idea of a trustless blockchain in which participants rely on the blockchain's protocol and its decentralized control.

Nevertheless, as the blockchain grows in importance, even partial decentralization has increasing potential to create governance issues. Arguably, the various stakeholders early in a blockchain's lifespan are vested in the blockchain's success and growth. However, as a blockchain grows in size and importance, it is likely to attract new stakeholders, creating the potential for the incentives of a community of users to diverge, which would make resolving complex problems more complicated. These problems could include operational issues (such as the need to resolve an exogenous disruption) and the need to resolve "economic" issues such as the distribution of financial gains.

Along with direct control over changes to the protocol, a blockchain's users may also exert indirect control by threatening to *fork* the blockchain, which occurs when a group of users reject (or adopt) a change approved (or rejected) by the blockchain's normal governance. In this case, the blockchain may be forked or split into two (or more) blockchains governed by different protocols for adding new blocks. On the one hand, forking provides a mechanism for those lacking formal governance power to exercise influence over changes. On the other hand, such forking could create an issue over which blockchain ledger represents valid claims, especially regarding claims on off-chain assets.

Dapp Governance: The unusual governance structure over dapp protocols raises a variety of concerns. If governance is concentrated in a small group of people, the risks are similar to those that exist for centralized finance projects: that the protocol will get changed in ways that benefit insiders at the expense of users of the protocol. This risk suggests that, should financial regulators gain authority over finance conducted on blockchains, they should have similar authority over on-chain protocols controlled by centralized groups (such as a DeFi protocol controlled by its original developers) as they would have over CeFi groups.

As control over a DeFi app becomes dispersed, the potential may arise for the protocol to become subject to governance attacks. This situation can arise if an outside attacker gains control of the protocol and changes it in ways that are favorable to the attacker at the expense of others in the dapp's community.[62] Moreover, the attacker may be able to obtain the keys by buying or borrowing them on the open market (Carter and Jeng, 2021) or even potentially by stealing them from the developers (Schär, 2021). A related risk raised by Werner et al. (2021) is that the majority could take actions that violate minority rights. Successful attacks on the protocol or on the rights of a minority of its users could weaken confidence in a dapp.

The dispersal of effective control over DeFi protocols also raises concerns about who the supervisors could talk with and, if necessary, act against if they have prudential concerns

[62] See Dalton (2022) for a discussion of a recent governance takeover attack on Build Finance DAO.

about the dapp. If control is widely dispersed, the supervisors may not find anyone who they feel can remedy regulatory concerns.

Censorship Resistance: An important feature of decentralized blockchains is that they are typically resistant to censorship.[63] That is, to be included on the blockchain, a proposed transaction merely must comply with the blockchain protocol. The rationale for censorship resistance is straightforward and, in some respects, appealing. This property prevents those operating the blockchain from censoring transactions from disfavored originators.

However, governments may have legitimate reasons for censorship. Censorship resistance means that a blockchain is open to every bad actor no matter where they are in the world.[64] Blockchains are already being used to facilitate scams, theft, money laundering, and a variety of other criminal activity. Additionally, blockchains could facilitate activities that, despite being legal, may increase the risk of financial instability, such as fractional reserve cryptocurrency banks.[65] The potential risks from blockchain-based finance can be somewhat reduced, especially for CeFi, to the extent that regulation can restrict financial services providers from supporting illicit activity. However, some blockchain finance operations (CeFi and DeFi) are likely to be based in jurisdictions with varied interests in supporting US regulatory goals.

DeFi Interconnections: A strength, and conversely a potential weakness, of dapps is their interoperability.[66] This ability is a strength in that smart contract *composability* allows for dapps to interoperate to provide services and products that are not available from any single dapp.[67] A weakness is that if a financial or operational issue arises with one dapp, the problem could spread across the DeFi ecosystem.[68]

The financial risk is that a shock to one market may spread through DeFi connections to other markets. For example, many DeFi services provide payments to liquidity providers to

---

[63] Censorship restraint can be thought of as part of a broader category called *credible neutrality*; see Buterin (2020).

[64] See Nicolle (2022) for a recent example of someone previously convicted of financial crimes playing an important role in DeFi application.

[65] See Wall (2019).

[66] For example, on February 2, 2022, a hacker exploited a weakness in a cross-chain bridging protocol between the Solana and Ethereum blockchains that resulted in theft of roughly 120,000 Wormhole Ethereum (WeETH) worth more than $320 million at the time. See Lessons from the Wormhole Exploit: Smart Contract Vulnerabilities Introduce Risk; Blockchains' Transparency Makes It Hard for Bad Actors to Cash Out.

[67] Werner et al. (2021) provides an example where attackers gain temporary control over governance tokens by using a flash loan. Another example is the recent governance attack discussed here: Attacker Drains $182M From Beanstalk Stablecoin Protocol (coindesk.com)

[68] For example, starting May 8, 2022, a series of event resulting in the rapid collapse of TerraUSD illustrated previously unforeseen correlations across multiple crypto assets. See the following for further details: A Data-Driven Exploration of UST's Collapse | by Riyad Carey | May, 2022 | Kaiko.

induce them to provide services, such as interest on deposits to fund loans or payments to liquidity pools used by automated market makers. Those seeking to earn such payments (or merely speculate on cryptocurrency values) can multiply their initial contribution by taking on leverage. Usually, the protocol's overcollateralization requirements limit the amount of leverage that can be taken in any one transaction. However, tokens obtained from one loan may be used as collateral for a second (or third, or fourth, and so forth.) loan. A shock to the price of the cryptocurrency (or cryptocurrencies) used as collateral for new loans could result in the liquidation of collateral underlying one or more loans, impairing the borrower's ability to supply liquidity for lending or in automated markets. The liquidation of the collateral could also affect the price of the cryptocurrency being used as col collateral.[69]

However, Schär (2021) observes that such operational interdependencies among dapps create potential problems. For example, if a series of dapps were needed to provide a financial product, the entire chain could fail if one dapp failed to perform. Such a failure to perform could be a result of insufficient investment in security that results in the dapp being the subject of a successful attack. There may also be a more innocent source of risk. Large financial firms often require extensive testing for even small changes to their more complex systems of programs, as changes to one program in the system might have unintended consequences elsewhere. To the extent that the dapps in a chain exhibit similar interdependencies, a change in the operation of one dapp risks unintended consequences for other dapps in the chain. Along with any direct losses resulting from the attack or unintended consequences of a change, the entire chain could suffer a loss of future activity if potential users lose confidence in the chain.

Those charged with writing and maintaining dapps in a chain do have an incentive to invest in security and in minimizing unintended consequences. Those working on individual dapps are at risk of loss should their dapp suffer a successful attack or even if it is changed in a way that reduces the value of a chain of composable dapps. However, those responsible for the "broken" dapp would generally bear only part of the costs of the broken chain, with other dapp writers and the chain's users bearing additional costs. Thus, we would ordinarily expect that the writers or maintainers of individual dapps would invest less than the optimal amount in security and in making sure that any of their changes they make do not have unintended consequences for other parts of the chain.[70]

4.4 The Interface of Traditional and Crypto Finance

Traditional finance has developed considerable infrastructure that allows it to provide financial services at a larger scale than crypto finance can currently provide. Thus, even under the most

[69] For additional discussion see Saengchote (2021).

[70] See Varian (2004) for a discussion of the efforts of many individuals in providing the public good of system reliability, where his analysis of the weakest link case probably best fits the case of a chain of dapps. Naghizadeh and Liu (2016) focuses more directly on security measures.

optimistic scenarios for crypto, crypto finance will likely coexist with traditional finance for a considerable period of time, which raises issues related to the interconnections between crypto and traditional finance. One such risk relates to differences in the mindset and risk mitigation approaches taken in the two methods of providing financial services. In particular, participants in the crypto market may not fully appreciate the potential risks being taken in traditional finance, and vice versa, which could result in participants on one side of the divide taking risks that participants on the other side underestimate.

DeFi Exposure to Traditional Finance: An outstanding example is that of stablecoins, especially Tether (also called USDT). Many people on the crypto side act as if the value of Tether's portfolio, which consists of off-chain financial securities, equals at least the value of outstanding USDT. If this assumption were proven incorrect and Tether were successfully run, it could have a devastating effect on liquidity and likely on confidence in other crypto markets.

Traditional Finance Exposure to DeFi: As banks and other intermediaries get deeper into providing crypto services and loans to crypto users, these banks may not fully appreciate the risks they are incurring. If a meltdown occurs in the crypto market, banks could suffer direct losses on their services and loans, create legal exposure from customers who suffered losses in the crypto market, and risk reputational damage.

On the legal exposure side, traditional financial firms may be at especially large risk. If a user suffers losses transacting through a dapp, the user could find it challenging to determine who to sue on the DeFi side, but it may not be difficult to identify the traditional intermediaries that might bear some legal liability, possibly creating the risk that traditional intermediaries will be brought into suits in which they are relatively minor players, but the only ones that can be readily identified and that have deep pockets.

5 Conclusion

The provision of financial services on public, permissionless blockchains has come a long way since the creation of Bitcoin, but DeFi has not yet reached the point of becoming systemically important. Nevertheless, the rapid growth in the role of such blockchains suggests that policymakers should start giving serious consideration to a full range of financial stability issues that could arise should such activities become systemically important. This paper discusses a generic set of stability issues that arise from the provision of financial services on blockchains, and it also highlights some unique concerns arising from the development of DeFi, especially the governance of the code used in dapps.

As policymakers decide on which assets (for example, dollars and registered securities) to allow on public permissionless blockchains, evidence indicates that DeFi will rapidly exploit any and all profitable opportunities regardless of supervisory concerns. In addition, under the scenario in which public blockchains evolve to provide a full range of services denominated in cryptocurrencies, supervisory authorities (including the Federal Reserve) may lack the

necessary tools to ensure compliance with laws and regulations. Policies considered well in advance and thoughtfully may reduce the scope of the inevitable financial stability disruptions stemming from DeFi.

6 References

Andresen, Gavin. 2013. Chain fork post-mortem. March 20. github.com/bitcoin/bips/blob/master/bip-0050.mediawiki <accessed June 1, 2022>.

Board of Governors of the Federal Reserve System. 2022. Money and payments: The U.S. dollar in the age of digital transformation. January. federalreserve.gov/publications/files/money-and-payments-20220120.pdf <accessed June 1, 2022>.

Budish, Eric. 2018. The economic limits of bitcoin and the blockchain. National Bureau of Economic Research working paper no. w24717.

Buterin, Vitalik. 2020. Credible neutrality as a guiding principle. January 3. nakamoto.com/credible-neutrality <accessed June 1, 2022>.

——. 2021a. Why sharding is great: Demystifying the technical properties. April 7. vitalik.ca/general/2021/04/07/sharding.html <accessed June 1, 2022>.

——. 2021b. Moving beyond coin voting governance. August 16. vitalik.ca/general/2021/08/16/voting3.html <accessed June 1, 2022>. .

Carter, Nic, and Linda Jeng. 2021. DeFi protocol risks: The paradox of DeFi. In *Regtech, Suptech and Beyond: Innovation and Technology in Financial Services*, RiskBooks. papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699 <accessed June 1, 2022>.

Centieiro, Henrique. 2021. Bitcoin proof of work—The only article you will ever have to read. May 20. levelup.gitconnected.com/bitcoin-proof-of-work-the-only-article-you-will-ever-have-to-read-4a1fcd76a294 <accessed June 1, 2022>.

Chainalysis. 2022. Crypto crime trends for 2022: Illicit transaction activity reaches all-time high in value, all-time low in share of all cryptocurrency activity. January 6. blog.chainalysis.com/reports/2022-crypto-crime-report-introduction <accessed June 1, 2022>.

Clear Chain Capital. 2021. The current state of undercollateralized DeFi lending. July 2. medium.com/coinmonks/the-current-state-of-undercollateralized-defi-lending-2021-1f84e14527b5 <accessed June 1, 2022>.

Copeland, Tim. 2021. Hacker shows how he "51% attacked" Ethereum clone CheapETH for $100. May 17. theblockcrypto.com/linked/105030/hacker-shows-how-he-51-attacked-ethereum-clone-cheapeth-for-100 <accessed June 1, 2022>.

Cryptopedia Staff. 2021. Blockchain consensus mechanisms beyond PoW and PoS. December 3. gemini.com/cryptopedia/blockchain-consensus-mechanism-types-of-algorithm <accessed June 1, 2022>.

Dalton, Mike. 2022. Build finance DAO suffers governance takeover attack. February 15. cryptobriefing.com/build-finance-dao-suffers-governance-takeover-attack <accessed June 1, 2022>.

Drinhausen, Katja, and Vincent Brussee. 2021. China's social credit system in 2021. March 3. merics.org/sites/default/files/2021-

03/MERICS%20ChinaMonitor%2067%20Social%20Credit%20System%20final%20%281%29.pdf <accessed June 1, 2022>.

Fadilpašić, Sead. 2021. Total value locked in DeFi is a "deceptively complicated metric."July 28. cryptonews.com/news/total-value-locked-in-defi-is-a-deceptively-complicated-metr-11231.htm <accessed June 1, 2022>.

Fang, Lily Hua. 2005. Investment bank reputation and the price and quality of underwriting services. November 10. onlinelibrary.wiley.com/doi/10.1111/j.1540-6261.2005.00815.x <accessed June 1, 2022>.

Gogel, D. 2021. DeFi beyond the hype: The emerging world of decentralized finance. May. wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf <accessed June 1, 2022>.

Harvey, Campbell R., Ashwin Ramachandran, and Joseph Santoro. 2021. DeFi and the future of finance. April 5. ssrn.com/abstract=3711777 <accessed June 1, 2022>.

Johnson, Travis L., and Nathan Swem. 2019. Reputation and investor activism: A structural approach. August. papers.ssrn.com/sol3/papers.cfm?abstract_id=3347501 <accessed June 1, 2022>.

Kiayias, Aggelos, and Philip Lazos. 2022. SoK: Blockchain governance. arxiv.org/pdf/2201.07188.pdf <accessed June 1, 2022>.

Lalley, Steven P., and E. Glen Weyl. 2019. Nash Equilibria for Quadratic Voting. July 18. arxiv.org/pdf/1409.0264.pdf <accessed June 1, 2022>.

Makarov, Igor, and Antoinette Schoar. 2022. Cryptocurrencies and decentralized finance (DeFi). National Bureau of Economic Research working paper no. w30006. nber.org/papers/w30006 <accessed June 1, 2022>.

Mohan, Vijay. 2020. Automated market makers and decentralized exchanges: A DeFi primer. October 30. ssrn.com/abstract=3722714 or http://dx.doi.org/10.2139/ssrn.3722714 <accessed June 1, 2022>.

Naghizadeh, Parinaz, and Mingyan Liu. 2016. Opting out of incentive mechanisms: A study of security as a non-excludable public good. *IEEE Transactions on Information Forensics and Security* 11, no. 12: 2790–803 ieeexplore.ieee.org/document/7539363 <accessed June 1, 2022>.

Nakamoto, Satoshi. 2008. Bitcoin: A peer-to-peer electronic cash system. October 31. nakamotoinstitute.org/bitcoin/?msclkid=d4dd4345aaeb11ecbc83fa805b236657 <accessed June 1, 2022>.

Nicolle, Emily. 2022. Crypto secrecy makes DeFi a financial felon's wonderland. January 27. bloomberg.com/news/articles/2022-01-27/crypto-s-cloak-of-anonymity-makes-defi-a-wonderland-for-felon <accessed June 1, 2022>.

Poon, Joseph, and Thaddeus Dryja. 2016. The bitcoin lightning network: Scalable off-chain instant payments. January 14. lightning.network/lightning-network-paper.pdf <accessed June 1, 2022>.

Popper, Nathaniel. 2021. Lost passwords lock millionaires out of their bitcoin fortunes. *New York Times*, January 12. nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html <accessed June 1, 2022>.

President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. 2021. Report on stablecoins. November. home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf <accessed June 1, 2022>.

Qin, Kaihua, Liyi Zhou, and Arthur Gervais. 2021. Quantifying blockchain extractable value: How dark is the forest? December 10. arxiv.org/pdf/2101.05511.pdf <accessed June 1, 2022>.

Qin, Kaihua, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the Defi ecosystem with flash loans for fun and profit. March 20. arxiv.org/pdf/2003.03810.pdf?ref=https://githubhelp.com <accessed June 1, 2022>.

Qin, Kaihua, Liyi Zhou, Yaroslav Afonin, Ludovico Lazzaretti, and Arthur Gervais. 2021. CeFi vs. DeFi—Comparing Centralized to Decentralized Finance. June 16. arxiv.org/pdf/2106.08157.pdf <accessed June 1, 2022>.

Roberds, Will. 2022. Unstable coins: The early history of central bank analog currencies. Federal Reserve Bank of Atlanta *Policy Hub*, February. doi.org/10.29338/ph2022-2 <accessed June 1, 2022>.

Saengchote, Kanis. 2022. Decentralized lending and its users: Insights from compound. February 20. ssrn.com/abstract=3925344 <accessed June 1, 2022>.

——. 2021. Where do DeFi stablecoins go? A closer look at what DeFi composability really means. July 26. ssrn.com/abstract=3893487 <accessed June 1, 2022>.

Schär, Fabian. 2021. Decentralized finance: On blockchain-and smart contract-based financial markets. Federal Reserve Bank of St. Louis *Review*, second quarter. research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets <accessed June 1, 2022>.

Securities and Exchange Commission. 2022. Staff Accounting Bulletin no. 121, April. sec.gov/oca/staff-accounting-bulletin-121 <accessed June 1, 2022>.

Spalding, Tyler. 2021. Flexa: The pure-digital payments network. October 6. gemini.com/cryptopedia/flexa-crypto-amp-token <accessed June 1, 2022>.

Szabo, N. 1997. Formalizing and securing relationships on public networks. *First Monday* 2, vol. 9. journals.uic.edu/ojs/index.php/fm/article/view/548 <accessed June 1, 2022>.

Tasca, Paolo. 2019. Token-based business models. In *Disrupting Finance: Fintech and Strategy in the 21st Century*. Palgrave Studies in Digital Business & Enabling Technologies. library.oapen.org/bitstream/handle/20.500.12657/23126/1007030.pdf?sequence=1#page=154 <accessed June 1, 2022>.

Varian, Hal. 2004. System reliability and free riding. November 30. infosecon.net/workshop/downloads/2002/pdf/49.pdf <accessed June 1, 2022>.

Wall, Larry D. 2016. "Smart contracts" in a complex world. Federal Reserve Bank of Atlanta *Notes from the Vault*, June. atlantafed.org/cenfis/publications/notesfromthevault/1607 <accessed June 1, 2022>.

——. 2018. Blockchain challenges and governance. Federal Reserve Bank of Atlanta *Notes from the Vault*, July. atlantafed.org/cenfis/publications/notesfromthevault/07-blockchain-challenges-and-governance-2018-07-30 <accessed June 1, 2022>.

——. 2019. Fractional reserve cryptocurrency banks. Federal Reserve Bank of Atlanta *Notes from the Vault*, April. atlantafed.org/cenfis/publications/notesfromthevault/04-fractional-reserve-cryptocurrency-banks-2019-04-25 <accessed June 1, 2022>.

Wang, Dabao, Siwei Wu, Ziling Lin, Lei Wu, Xingliang Yuan, Yajin Zhou, Haoyu Wang, and Kui Ren. 2021. Towards understanding flash loan and its applications in defi ecosystem. April 21. arxiv.org/pdf/2010.12252.pdf <accessed June 1, 2022>.

Werner, Sam M., Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt. 2021. Sok: Decentralized finance (defi). arxiv.org/pdf/2101.08778.pdf <accessed June 1, 2022>.

Worah, Aditya. 2019. Bitcoin could have died in 2010—But Satoshi Nakamoto's hard fork saved it! January 14. cryptoground.com/a/bitcoin-could-have-died-2010-satoshi-nakamoto-hard-fork <accessed June 1, 2022>.

Xu, Jiahua, and Nikhil Vadgama. 2022. From banks to DeFi: The evolution of the lending market. University College London, Centre for Blockchain Technologies. arxiv.org/pdf/2104.00970.pdf <accessed June 1, 2022>.

Zhang, Shijie, and Jong-Hyouk Lee. 2020. Analysis of the main consensus protocols of blockchain. *ICT Express* 6, no. 2: 93–7. doi.org/10.1016/j.icte.2019.08.001 <accessed June 1, 2022>.

Zimmer, Ben. 2021. "Fungible": The idea in the middle of the NFT sensation. *Wall Street Journal*, April 16. wsj.com/articles/fungible-the-idea-in-the-middle-of-the-nft-sensation-11618595061 <accessed June 1, 2022>.

APPENDIX Tables and Figures

Table 1: Traditional Finance versus DeFi

	Traditional Finance	DeFi
Custody of Assets	Held by a regulated service provider or custodian on asset owners' behalf.	Held directly by users in noncustodial wallets or via smart contract-based escrow.
Units of Account	Typically denominated in fiat currency.	Denominated in digital assets or stablecoins (which may themselves be denominated in fiat money).
Execution	Intermediaries such as banks or brokers typically process transactions between parties.	Via smart contracts operating on the user's assets.
Clearing and Settlement	Processed by service providers or clearinghouses, typically after a period of time.	Writing transactions to the underlying blockchain completes the settlement process.
Governance	Specified by the rules of the service provider, marketplace, regulator and/or self-regulatory organization.	Managed by protocol developers or determined by users holding tokens granting voting rights.
Auditability	Authorized third-party audits of proprietary code or potential for open-source code that is publicly verified	Open-source code and public ledger allow auditors to verify protocols and activity.
Collateral Requirements	Transactions may involve no collateral, or collateral less than or equal to the funds provided.	Overcollateralization generally required, due to digital asset volatility and absence of credit scoring
Cross-service Interaction	Limited. Movement toward Open Finance via application programming interfaces or dedicated intermediaries.	Any service may integrate with any other service on the same blockchain, and potentially across chains.
Access and Privacy	Identity checks conducted by service providers. Personal data subject to national privacy laws.	Identity verification requirements under discussion by anti–money laundering regulators. User balances and transaction activity are generally public.
Security	Vulnerable to hacks and data breaches in software systems controlling assets.	Vulnerable to hacks and other technical and operational risks of smart contracts.

Investor Protection	Government-mandated disclosure and consumer protections, anti-fraud enforcement, exposure limits, and insurance schemes.	Users assume all risks as a default, although private redress arrangements such as DeFi insurance offer some protection against losses.
Prudential Regulation	Myriad regulators require financial institutions to maintain adequate levels of capital, undergo stress tests, disclose information, etc.	No regulatory requirements currently, but ongoing discussions among regulators to assess the best policies for specific DeFi use cases.

Note: The table is based on Gogel et al. "DeFi Beyond the Hype" May 2021, available at https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf.

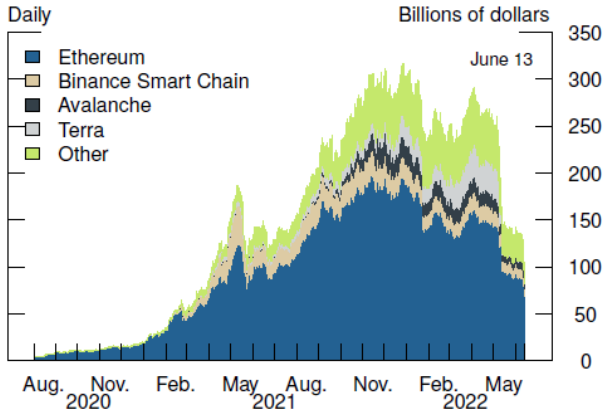
Table 2: Top 50 DeFi Applications by Total Value Locked

	Platform Name	Category	TVL ($B)		Platform Name	Category	TVL ($B)
1.	MakerDAO	CDP	$8.67	26.	Venus	Lending	$0.76
2.	WBTC	Bridge	$7.76	27.	Iron Bank	Lending	$0.74
3.	AAVE	Lending	$7.52	28.	Vires Finance	Lending	$0.67
4.	Curve	Dexes	$7.49	29.	SUN.io	Dexes	$0.66
5.	Lido	Liquid Staking	$6.56	30.	Abracadabra	CDP	$0.63
6.	Polygon Bridge & Staking	Chain	$6.11	31.	Stargate	Cross Chain	$0.60
7.	Uniswap	Dexes	$5.43	32.	Alpaca Finance	Yield	$0.59
8.	Convex Finance	Yield	$4.57	33.	Liquity	CDP	$0.59
9.	Compound	Lending	$3.81	34.	Keep3r Network	Derivatives	$0.57
10.	PancakeSwap	Dexes	$3.78	35.	DefiChain DEX	Dexes	$0.56
11.	JustLend	Lending	$2.94	36.	Bancor	Dexes	$0.50
12.	Multichain	Bridge	$2.73	37.	Parallel DeFi Super App	Lending	$0.49
13.	Instadapp	Services	$2.08	38.	Solend	Lending	$0.44
14.	Balancer	Dexes	$1.79	39.	cBridge	Bridge	$0.41
15.	AAVE V3	Lending	$1.39	40.	Tornado Cash	Privacy	$0.40
16.	Frax	Algo-Stables	$1.34	41.	Synthetix	Derivatives	$0.38
17.	JustStables	Algo-Stables	$1.31	42.	Poly Network	Bridge	$0.38
18.	Arrakis Finance	Yield	$1.13	43.	BiSwap	Dexes	$0.37
19.	hBTC	Bridge	$1.12	44.	Quickswap	Dexes	$0.37
20.	JustCryptos	Bridge	$1.07	45.	Beefy Finance	Yield Aggregator	$0.36
21.	Yearn Finance	Yield Aggregator	$1.03	46.	Serum	Dexes	$0.36

22.	dYdX	Derivatives	$0.97	47.	Rocket Pool	Liquid Staking	$0.36
23.	SUNSwap	Dexes	$0.94	48.	Olympus DAO	Reserve Currency	$0.34
24.	Portal	Bridge	$0.90	49.	Atrix	Dexes	$0.34
25.	VVS Finance	Dexes	$0.78	50.	RenVM	Bridge	$0.30

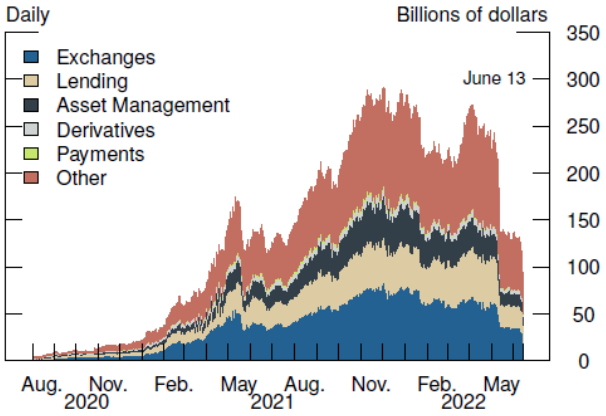
Source: DeFi Llama, DefiLlama—DeFi Dashboard

Figure 1
Total Value Locked by Blockchain



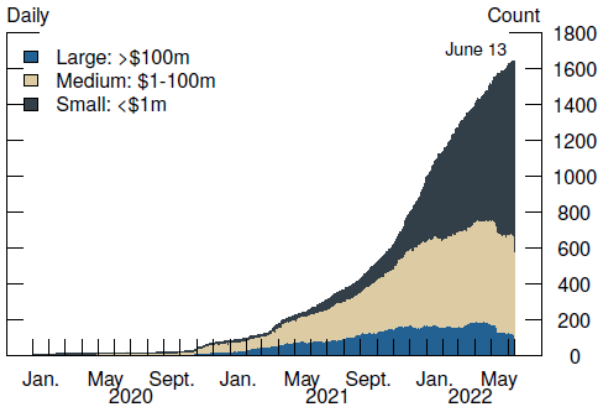
Note: Total Value Locked is the overall value of assets committed to a DeFi protocol. This metric includes governance tokens staked in the protocol, staked liquidity provider tokens where one of the coins in the pair is the governance token, and borrowed coins in lending protocols.
Source: DeFi Llama.

Figure 2
Total Value Locked by Category



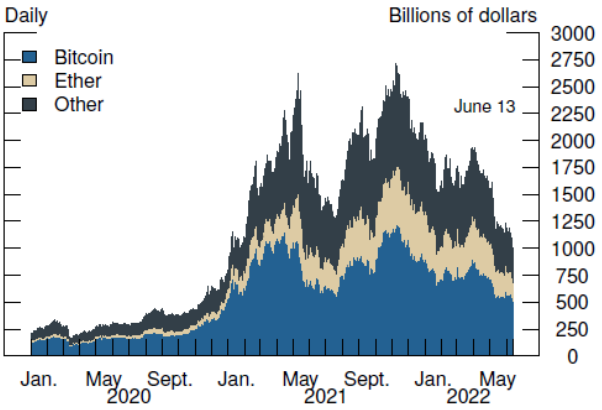
Note: Total Value Locked is the overall value of assets committed to a DeFi protocol. This metric includes governance tokens staked in the protocol, staked tokens where one of the coins in the pair is the governance token, and borrowed coins in lending protocols. Certain tokens are double counted across protocols.
Source: DeFi Llama.

Figure 3
Number of Decentralized Applications



Source: DeFi Llama. Size measured in gross total value locked.

Figure 4
Total Market Cap by Cryptocurrency



Source: CoinMetrics