DeFi Beyond the Hype

The Emerging World of Decentralized Finance

Produced by the Wharton Blockchain and Digital Asset Project,
in collaboration with the World Economic Forum

May 2021

Wharton
University of Pennsylvania

Introduction

Decentralized Finance (DeFi) is a developing area at the intersection of blockchain, digital assets, and financial services. DeFi protocols seek to disintermediate finance through both familiar and new service arrangements. The market experienced explosive growth beginning in 2020. According to tracking service DeFi Pulse, the value of digital assets[1] locked into DeFi services grew from less than $1 billion in 2019 to over $15 billion at the end of 2020, and over $80 billion in May 2021.[2] Yet DeFi is still early in its maturation.

The goal of this report is to demystify DeFi. It describes the basic attributes of DeFi services, the structure of the DeFi ecosystem, and emerging developments. A forthcoming **Decentralized Finance Policy-Maker Toolkit** will offer guidance on risks and policy approaches for governments navigating this new space.

DeFi is a general term covering a variety of activities and business relationships. We identify six major DeFi service categories—stablecoins, exchanges, credit, derivatives, insurance, and asset management—as well as auxiliary services such as wallets and oracles. While traditional finance relies on intermediaries to manage and process financial services, DeFi operates in a decentralized environment—public, permissionless blockchains. Services are generally encoded in open-source software protocols and smart contracts.

Like blockchain technology more generally, DeFi has an enthusiastic base of evangelists, who promote its potential for efficiency, transparency, innovation, and financial inclusion. It also has its critics, risks, and unknowns. There have already been significant examples of fraud, attacks, governance controversies, and other failures in the DeFi world. At this early stage, it is essential for industry and governments alike to develop a well-informed and nuanced understanding of the opportunities, risks, and challenges.

The **Blockchain and Digital Asset Project** is a program of the Wharton Initiative on Financial Policy and Regulation. It is led by Professor Kevin Werbach. Drawing on the expertise of the Wharton School and a global network of contributors, the project studies the business and regulatory implications of distributed ledger technology.

For further information, please contact werbach@upenn.edu.

What is DeFi?

THE FUNDAMENTALS

DeFi is a general term for decentralized applications (Dapps) providing financial services on a blockchain settlement layer, including payments, lending, trading, investments, insurance, and asset management. DeFi services typically operate without centralized intermediaries or institutions, and use open protocols that allow services to be programmatically combined in flexible ways.

Historically, intermediaries have played essential roles within financial markets, serving as agents and brokers of trust, liquidity, settlement, and security. The range and value of intermediaries has grown over time to meet the needs of an increasingly complex financial system. Since the 2008 Global Financial Crisis, there has been increased attention on inefficiencies, structural inequalities, and hidden risks of the intermediated financial system.[3] More recently, controversies such as the GameStop short squeeze, in which retail investors were blocked from trading during a period of volatility, cast a spotlight on other shortcomings of legacy financial infrastructure: slow settlement cycles, inefficient price discovery, liquidity challenges, and the lack of assurance around underlying assets.[4] DeFi aims to address some of these challenges—though many still apply to the DeFi ecosystem in its current state.

DeFi leverages blockchain technology to facilitate alternatives to traditional service providers and market structures. It offers the potential for innovation and creation of new services for improving efficiency of financial markets—building upon work being done in financial technology (fintech) and blockchain technology more broadly. Whether it achieves this promise remains to be seen.

DeFi Building Blocks

DeFi takes advantage of various technologies developed in the blockchain sphere. All have applications outside of DeFi, but play essential roles within the DeFi ecosystem.

Blockchains: Distributed ledgers serving as the settlement layer for transactions. Currently, most DeFi services operate on the Ethereum network, due to its capabilities and developer adoption.[5] DeFi activity is growing on and across other blockchains as well.

Digital Assets: Tokens representing value that can be traded or transferred within a blockchain network. Bitcoin and other cryptocurrencies were the first blockchain-based digital assets. Others have a range of intended functions beyond payments.

Wallets: Software interfaces for users to manage assets stored on a blockchain. With *a non-custodial wallet*, the user has exclusive control of funds through their private keys. With *custodial wallets,* private keys are managed by a service provider.

Smart Contracts: Blockchain-based software code that carries out, controls, and documents relevant events and actions according to predefined terms and rules.

Decentralized Applications (Dapps): Software applications built out of smart contracts, often integrated with user-facing interfaces using traditional web technology.

Governance Systems: Software-based mechanisms that manage changes to smart contracts or other blockchain protocols, often based on tokens that allocate voting rights to stakeholders.

Decentralized Autonomous Organizations (DAOs): Entities whose rules are defined and enforced in the form of smart contracts.

Stablecoins: Digital assets whose values are pegged to a fiat currency, a basket of fiat currencies or other stable-value assets.

Oracles: Data feeds that allow information from sources off the blockchain, such as the current price of a stock or a fiat currency, to be integrated into DeFi services.

DEFINING CHARACTERISTICS

Not every application of blockchain technology—even those involving financial transactions—is a form of DeFi. Nor is every element contributing to the DeFi ecosystem appropriately considered a DeFi service, business or software protocol. While the space is evolving, there are certain distinguishing characteristics:[6]

1. **Financial services:** DeFi directly mediates the transfer and exchange of value. Auxiliary services such as oracles, query systems, and decentralized storage may be important enablers of DeFi activity, but they should be distinguished from DeFi services themselves.
2. **Trust-minimized operation and settlement:** DeFi projects generally build on public, permissionless blockchains offering smart contract functionality, such as Ethereum. Transactions are executed and recorded according to the rules of the DeFi protocols. Trust minimization is often extended to the governance structures that establish the conditions for protocol changes.
3. **Non-custodial design:** The assets issued or managed by DeFi services cannot in theory be unilaterally expropriated or modified by third parties, even by those providing intermediation and other services.

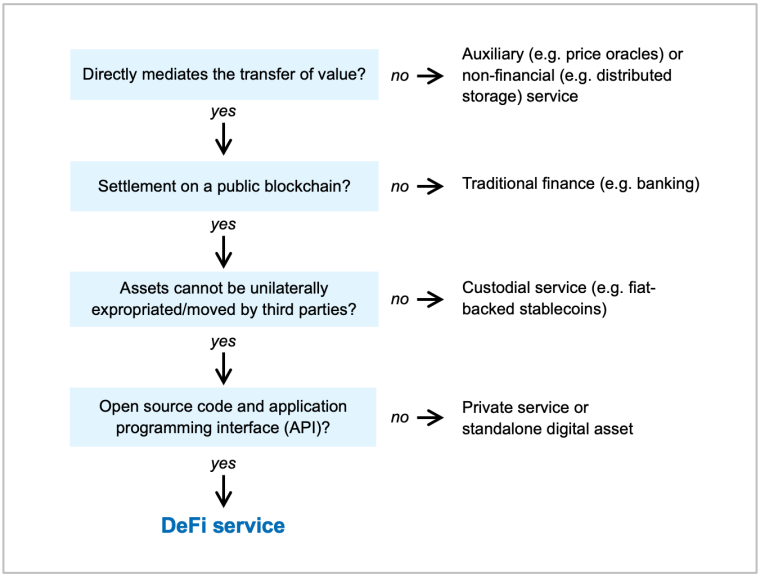

Figure 1 – DeFi classification flowchart.

Users retain full control. Thus, centralized cryptocurrency exchanges that have custody over digital assets are not DeFi businesses, though many are developing DeFi offerings.

4. **Open, programmable, and composable architecture:** There is broad availability of the underlying source code and a public application programming interface (API). Components can be composed together and programmed to create new financial instruments and services dynamically. For example, a stablecoin may be used as the foundation for a derivative which is used as collateral on a loan and subject to an insurance contract.

The **Decentralized Finance Policy-Maker Toolkit** offers a more granular description of the DeFi service architecture, and the relationship of its components.

Comparing Traditional Finance to DeFi

	Traditional Finance	**DeFi**
Custody of Assets	Held by a regulated service provider or custodian on asset owners' behalf.	Held directly by users in non-custodial 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 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.

INCENTIVE STRUCTURES AND GOVERNANCE

While strictly speaking not required, most DeFi services incorporate token-based incentive structures for important objectives such as liquidity and governance. As shown in Figure 2, these typically involve digital asset holders locking up assets in order to receive payments (similar to earning interest on a certificate of deposit) and DeFi users paying in fees (analogous to interest rates) to access assets from the resulting pool. Unlike traditional finance, this arrangement applies to virtually every category of DeFi. The assets obtained might be stablecoins, a different token than the one the user provides (in the case of an exchange), loans, or insurance contracts, for example.

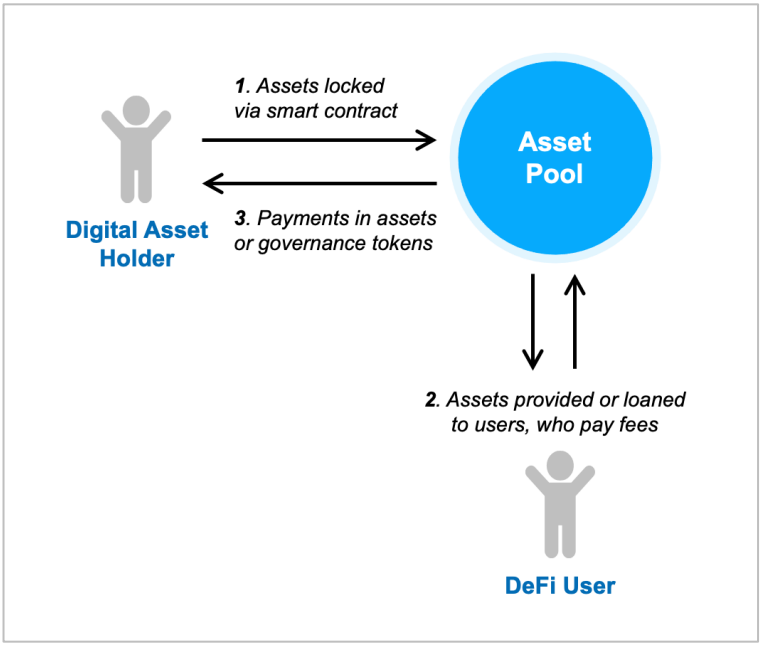

Figure 2 – DeFi incentivized asset pooling.

Common mechanisms include *lock-up yields* that pay interest for immobilizing digital assets in pools, where they serve as liquidity or collateral for a DeFi service; *liquidation fees* that pay market-makers a percentage of the value of under-collateralized, liquidated loans; and *liquidity mining* that pays the interest in the form of tokens issued by the DeFi service itself. Because of DeFi's composable, programmatic architecture, these mechanisms can be further integrated into structures such as *yield farming*, which optimizes returns from liquidity mining and lock-up yields by automatically moving funds

across DeFi services. The earnings rate may be determined in several ways, including a pro-rata share of transaction fees, parameters set through the protocol's governance process, or a bonding curve that rewards earlier participation.

The idea of using tokens to incentivize decentralized network growth is not new. It is the essential to the consensus system of Bitcoin and other cryptocurrencies. Coinbase co-founder Fred Ehrsam outlined in 2016 how tokens could be used to help solve the proverbial chicken and egg problem of bootstrapping new networks and marketplaces.[7] In the 2017 initial coin offering (ICO) bubble, however, tokens were often sold to speculators who flipped them for a quick profit, providing little functional benefit to the networks.[8] DeFi provides a new opportunity for token models that reward long-term focused participants. The provision of capital is not just a payment to fund future protocol development and reward insiders; it is a direct contribution to DeFi activities such as trading, lending, stablecoin collateralization, and insurance. More liquidity increases the value of the network, and some of that value flows back to the liquidity providers. However, well-designed incentive structures and careful attention to leverage and volatility are needed to address risks.

One of the major applications of DeFi incentive structures is governance. Tokens issued in connection with liquidity mining or related mechanisms often provide governance rights for the DeFi service. Token-holders can vote on proposed changes to protocols, or on defined parameters such as interest rates or collateralization ratios. The scope of decisions that can be made by token holders other than the developers varies. These tokens are tradeable on certain exchanges, with their value in theory tied to the activity level of the issuing DeFi service.

In addition to its role in incentivizing activity, token-based governance provides a mechanism for further decentralization of DeFi services. As developers cede more control around essential decisions to token holders, their power over the protocol decreases. In many current DeFi projects, token-holder votes can instruct designated signers to change certain protocol values. A further level of decentralization requires multiple designated private keys (an arrangement known as multisig) to make modifications. The endpoint of this process occurs when developers establish a Decentralized Autonomous Organization (DAO) which executes the governance decisions of token votes as automated smart contracts, which no one has special power to countermand. With the benefits of decentralized governance come risks as well. For example, an attacker might use the governance system to impose policies that allow it to drain funds, with no effective means of recourse.

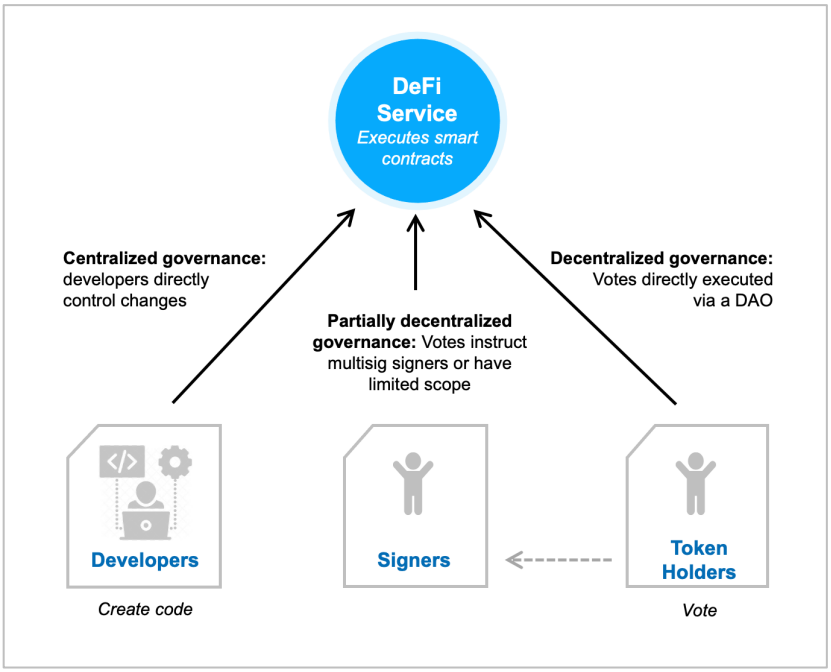

Figure 3 – DeFi governance mechanisms.

Opportunities and Challenges

Without taking a position, this table lists potential benefits that DeFi might produce, and hurdles that it faces. Further analysis of DeFi risks is provided in the **Decentralized Finance Policy-Maker Toolkit**.

Opportunities	Challenges
Reduced friction and transaction costs for creation, distribution, trading, and settlement of financial assets.	**Scalability, throughput, and transaction fees** for blockchain settlement platforms are significant limiting factors. Energy usage raises concerns about contributing to climate change.
Increased standardization and functional interoperability, allowing reuse and recomposition of financial primitives.	**Limited interoperability** across blockchains and with traditional financial services.
Increased auditability and transparency of transactions through blockchain-based records.	**Privacy considerations** may be in tension with transaction transparency.
Improved accountability for decisions through software-based governance systems.	**Immature governance** as high-stakes decisions are made by small, inexperienced teams. Lack of accountability when developers are anonymous.
Greater stakeholder control through non-custodial, disintermediated service provision.	**Hidden centralization of control** and low thresholds for governance rights may give certain actors disproportionate power.
Improved market access by providing global, 24/7 availability of services and removing barriers such as bank account requirements.	**Regulatory questions** and enforcement challenges in applying national legal requirements to decentralized global networks.
Faster settlement, reducing counterparty risks and freeing up capital.	**Immature technology** is being used to manage high-value assets. Poor design choices and implementations have led to significant losses.
Greater inclusivity of financial services by making automated tools available to all, with transparent and non-discriminatory execution.	**Extreme short-term returns** during DeFi's early growth stage attract unscrupulous actors and warp user expectations. Limited usability impedes large-scale adoption.
Permissionless innovation, allowing the creation of novel products and services.	**Potential for facilitation of financial crime** such as money laundering.

Despite its rapid growth and development, DeFi is at an early stage. Much of the activity to date is highly speculative and targeted at existing digital asset holders— and returns are likely to compress over time. The most common motivations for participation appear to be creation of leverage for digital asset purchases, or profiting from the various incentive mechanisms. The user experience of most services is still not optimized for mainstream retail market participants. Resilience to runs and other familiar risks in financial systems remains relatively untested at scale. Hacks and other attacks to drain funds are disconcertingly common, with over $120 million stolen in 2020 according to research firm The Block, of which less than $50 million was recovered.[9] The Ethereum blockchain, which supports the vast majority of current DeFi activity, faces major scalability challenges.[10] Further market development will require significant improvements across these and other areas.

DeFi Service Categories

DeFi embodies a variety of activities meeting the criteria of trust-minimized, non-custodial, open, composable, and programmable financial services. We identify six major DeFi categories, in addition to auxiliary services such as oracles and wallets. The lines between them are not always clear. However, this typology generally reflects participant perceptions of the DeFi market.

1. **Stablecoins** seek to maintain a constant value of a token relative to some asset, most commonly the U.S. dollar or other major fiat currency. *Non-custodial* stablecoins function as DeFi services themselves. *Custodial* stablecoins are centralized but may be incorporated into DeFi services.
2. **Exchanges** allow users to trade one digital asset for another. DeFi exchanges avoid taking custody of user assets, either through a decentralized order book or by matching orders and setting prices algorithmically.
3. **Credit**[11] involves the creation of time-limited interest-bearing instruments, which must be repaid at maturity, and the matching of lenders and borrowers to issue those instruments.
4. **Derivatives** are synthetic financial instruments whose value is based on a function of an underlying asset or group of assets. Common examples are futures and options, which reference the value of an asset at some time in the future.
5. **Insurance** provides protection against risks by trading the payment of a guaranteed small premium for the possibility of collecting a large payout in the event of a covered scenario.
6. **Asset management** seeks to maximize the value of an asset portfolio based on risk preferences, time horizons, diversification, or other conditions.

While this report includes examples throughout, it is important to keep in mind that DeFi is developing quickly. These categorizations—and the projects that fit within them—may change over time.

Because DeFi services are programmable and composable, aggregators have emerged that mediate activity across services in these base categories. Yield farming services such as Yearn Finance, which optimize returns from liquidity and collateral provision, are one example. Exchange aggregators such as 1inch and Matcha send trade orders to the exchange offering the best price. Zapper and Zerion provide integrated interfaces for order routing, yield optimization, and other DeFi activities across different protocols, reducing complexity for users. Tally

aggregates DeFi governance token activity to facilitate participation in governance decisions. Because of their potential for better usability, aggregators may originate a significant share of DeFi activity in the future.

STABLECOINS

Stablecoins are crucial to DeFi, because they separate the risk/return calculus of the DeFi services from the often-high volatility of digital assets. Financial interoperability requires stable prices for value exchange and investors expect a steady unit of account for financial services.

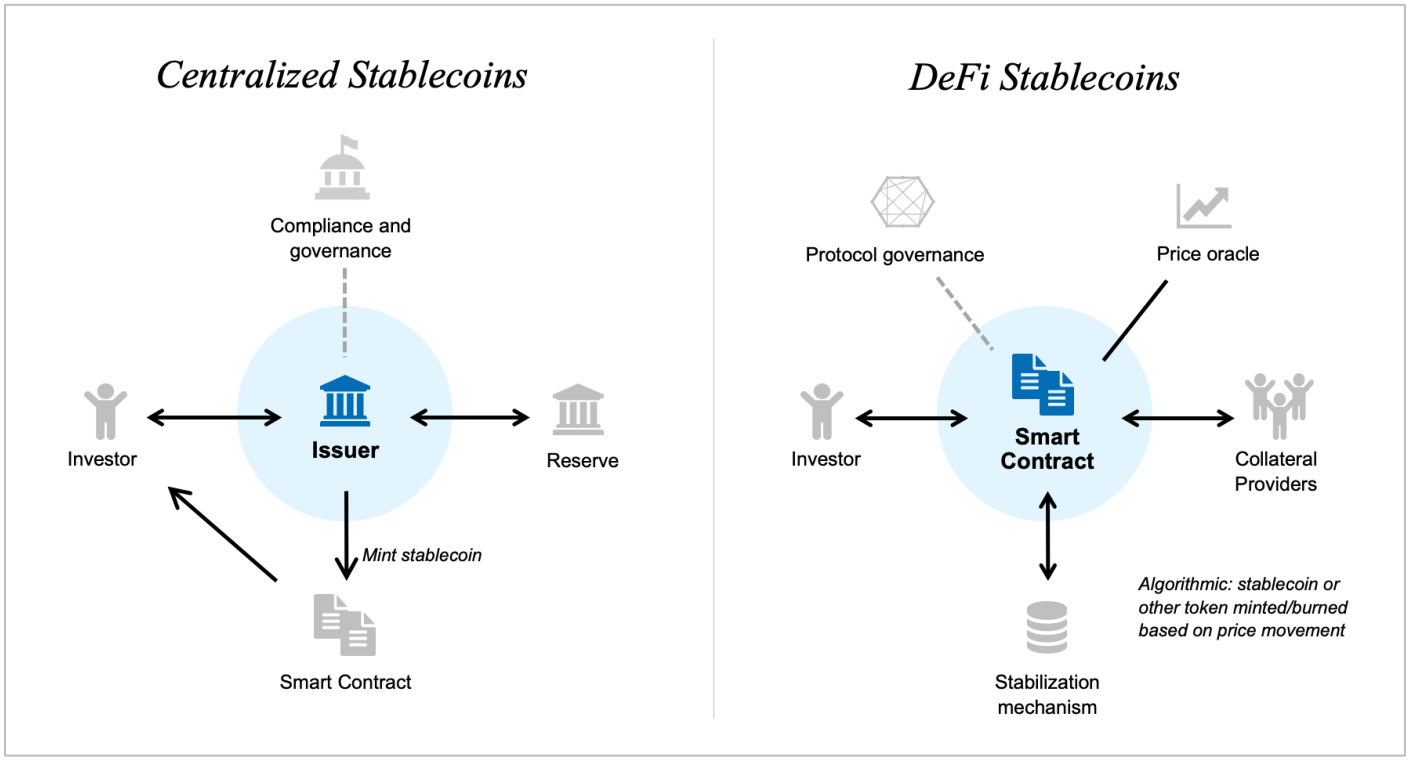

Figure 4 – Stablecoins.

Broadly, stablecoins can be organized into three categories:

1. **Custodial** or centralized stablecoins such as USDC or Facebook's proposed Diem use holdings of fiat currency or high-quality liquid assets as a reserve. Because they require trust in the custodian, they are not DeFi instruments. However, they are included here because they may be incorporated into other DeFi services.
2. **Asset-backed** stablecoins use smart contracts to assemble and liquidate collateral in the form of cryptocurrencies or other assets.
3. **Algorithmic** stablecoins attempt to maintain the peg through dynamic expansion and contraction of token supply.

Because they operate on a non-custodial, decentralized, trust-minimized basis, asset-backed and algorithmic stablecoins are DeFi services themselves. As with other areas of DeFi, projects are experimenting with different

mechanisms. How effective each will be in maintaining its peg at scale and through different market conditions remains a source of uncertainty.

MakerDAO and the DAI Stablecoin

DAI is a US dollar-denominated asset-backed stablecoin built on the Ethereum blockchain. It is based on the Maker protocol, which is governed by MakerDAO, a decentralized autonomous organization. The Maker Foundation spearheaded development of MakerDAO, but is now in process of decentralizing its functions.

The protocol allows anyone to deposit collateral into a Maker Vault, in return for a "loan" in the DAI stablecoin. Users must over-collateralize their positions to open a Maker Vault. If the value of the collateral falls below a minimum threshold, the Vault is liquidated, reducing supply to bring the DAI price back up to the peg. To retrieve collateral, the borrower must repay the DAI, along with interest. The accrued interest is used to reduce the supply of a second, non-stable token, MKR, which grants governance rights over the Maker protocol. MKR holders vote to set the interest rate, collateralization ratio, allowable collateral types, and other attributes. The system includes several other incentive mechanisms and backstops to maintain the price peg under different market conditions. Because it is decentralized and native on the Ethereum blockchain, MakerDAO is widely incorporated into other DeFi services, with over $4 billion of DAI circulating as of May 2021.

EXCHANGES

Exchanges are important to DeFi in two ways: They allow holders of various digital assets to use DeFi services, and they provide opportunities to profit from appreciation in the value of tokens. Centralized exchanges require traders to trust an operator to safeguard user funds, provide accurate price information, match buyers and sellers to process trades, settle transactions, and engage in transaction monitoring. This is true whether the exchange is purely fiat-based (such as NASDAQ), facilitates trading between fiat and digital assets (such as Coinbase), or only processes trades among digital assets (such as Uniswap). While centralized exchanges can trade digital assets used in DeFi services, they are themselves custodial and neither trust-minimized nor programmable.

DeFi exchanges, by contrast, decentralize key functions. They can be accessed programmatically with non-custodial wallets. Transactions are automatically processed by smart contracts on a peer-to-peer basis or against a pool of capital. While exchanges can operate order books either on or off the blockchain, the most prominent form of DeFi exchange, automated market makers (AMMs), does away with the traditional order book entirely. Any holder of digital assets can lock up funds as liquidity for potential trades, earning a yield paid by traders. The price of any trade is determined algorithmically, based on the ratio if available liquidity in the assets being traded. A trader is therefore dealing against liquidity pools supplied by market makers, rather than an order book of potential counterparties subject to a bid/ask spread. Different design choices for DeFi exchanges produce

tradeoffs around throughput, latency, security, scalability, and fees, and slippage (the extent to which a larger order alters the price).

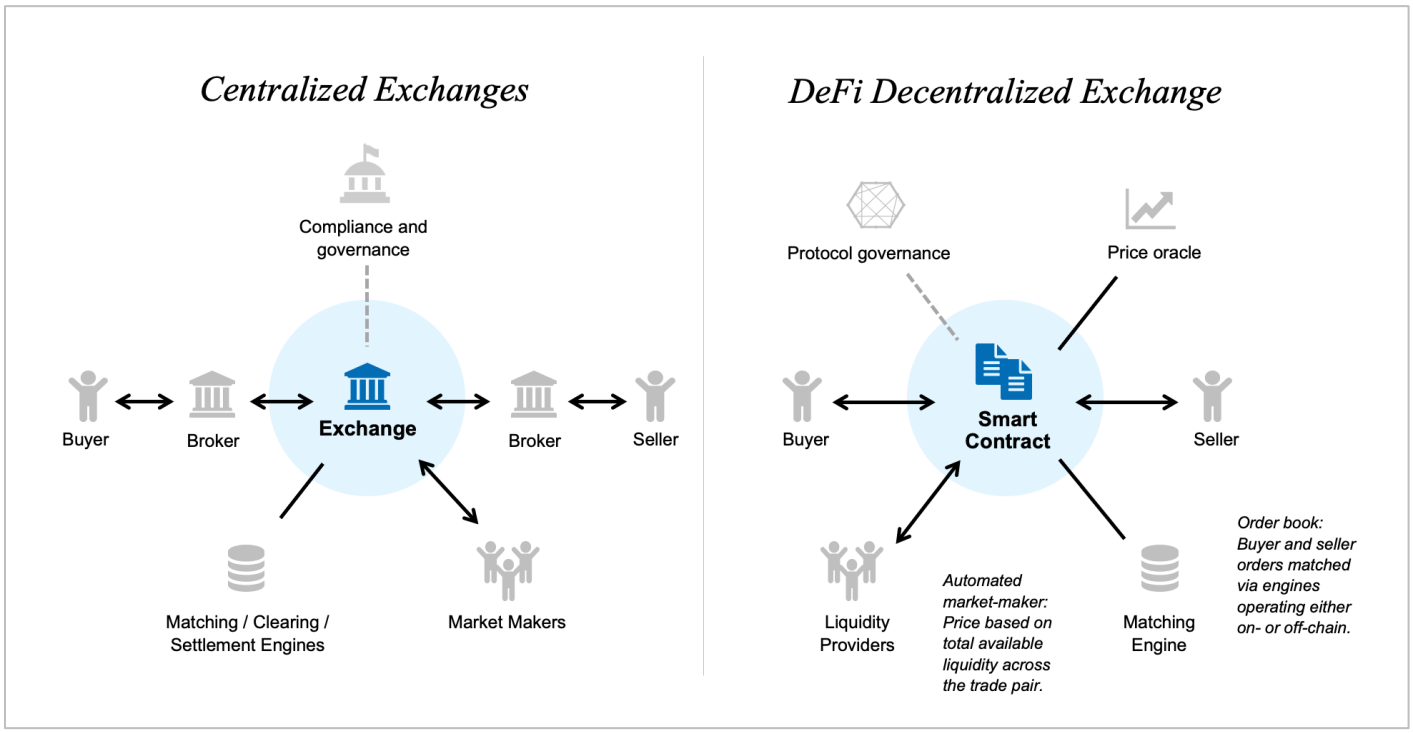

Figure 5 – Exchanges.

Uniswap and Sushiswap

Uniswap is a decentralized AMM protocol built on Ethereum. It uses an algorithm in which the product of the liquidity pool token count in the two digital assets being traded always equals a constant (x*y=k). Buying tokens removes them from the liquidity pool, causing their price to increase to maintain the constant. Uniswap also charges a trading fee, part of which is distributed to liquidity providers. Among other things, this model provides liquidity on very thinly traded assets and reduces high spreads for illiquid assets. From launch in November 2018 to the end of 2020, Uniswap facilitated over $100 billion in trading volume. As with other DeFi platforms, Uniswap is rapidly developing and adding new features.

In mid-2020, an anonymous developer forked the Uniswap software to create SushiSwap. It added a governance token, SUSHI, whereby the community votes on major changes to the protocol. A portion of trading fees across the platform are paid out to SUSHI token holders. The potential for value accrual in SUSHI tokens, in addition to liquidity provision, attracted substantial interest in SushiSwap. Uniswap subsequently created a UNI governance token. Uniswap's cash flows do not yet accrue to the UNI token holders, but Uniswap has announced plans to do so.

CREDIT

Borrowing and lending are central to finance, because they facilitate risk-taking and expand the supply of capital through leverage. The classic form of centralized credit provision is banking. The bank manages the spread between the interest rates it pays to depositors, whose assets are liquid, and the rates it receives from borrowers on longer-term loans. It must assess credit-worthiness of borrowers and set interest rates appropriately to account for defaults.

By contrast, DeFi credit protocols such as Compound and Aave pool together tokens, subject to an interest rate determined by the ratio of supply to borrowing. When lenders commit capital to DeFi credit services, they receive platform-native tokens representing their tokens plus the specified interest rate. Net of transaction fees—which accrue to service providers—lenders receive and borrowers pay the same interest rate, which is typically variable (some platforms now purport to offer fixed rates as well). Both sides maintain full custody over their assets and the ability to liquidate at any time. Credit terms can be quite complex, and these instruments can themselves be securitized and traded.

Flash Loans

Flash loans enable users to borrow instantly from decentralized credit protocols such as Aave and dYdX with no collateral required, provided that the liquidity is returned at the end of the same transaction (which may contain a series of actions). If this does not happen, the whole transaction is automatically reversed.

Flash loans can be used to swap the collateral supporting a loan, to liquidate a liquidity pool on a decentralized exchange in order to refinance a loan, or to conduct arbitrage by exploiting the priced differences of an asset across various exchanges. They can also be used to exploit protocols for market manipulation, essentially creating artificial leverage. For example, in October 2020, an attacker siphoned off $24 million of tokens through Harvest Finance, a DeFi robo-advisor, by using large flash loans repeatedly to manipulate stablecoin oracle prices.

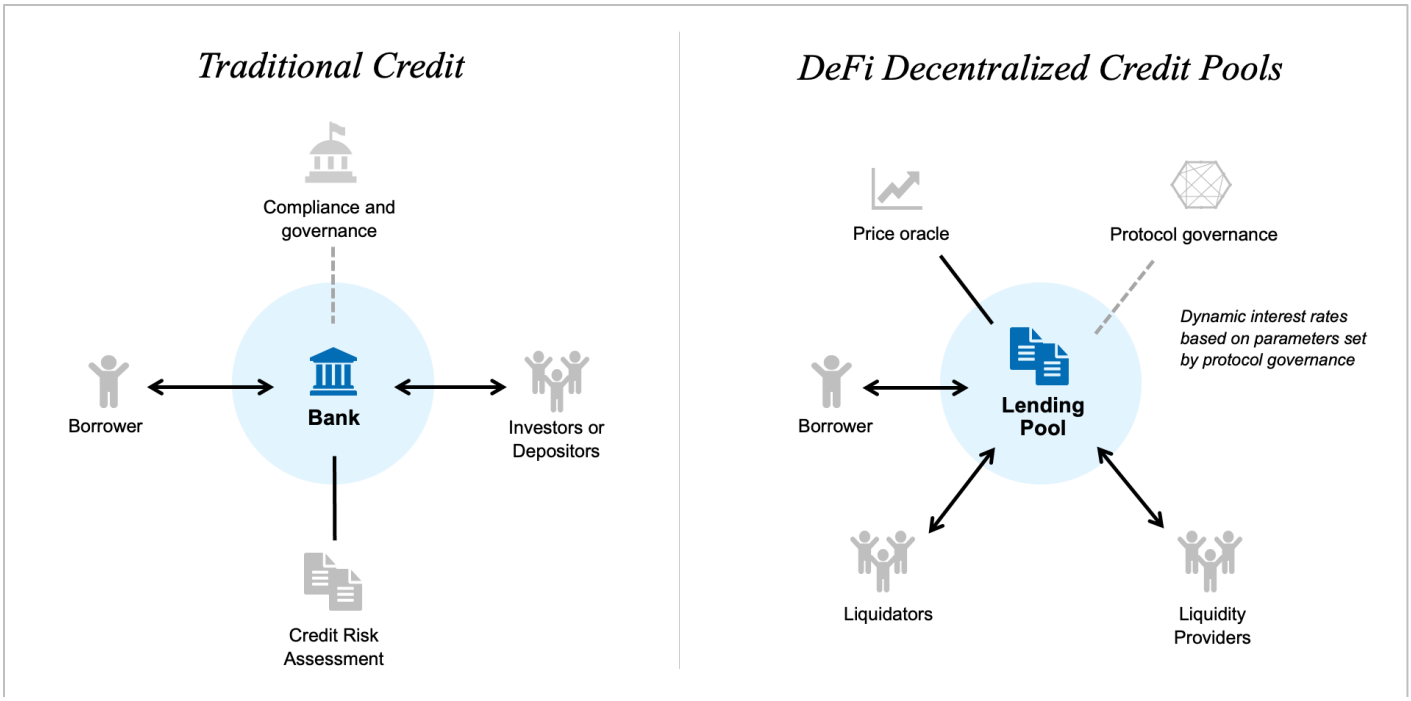

Figure 6 – Credit.

DeFi loans are generally backed by collateral in the form of digital assets. Because loans are secured with assets held in smart contracts, there is no need for credit checks or other borrower-specific evaluation prior to a loan. To buffer against price fluctuations, loans are generally overcollateralized, meaning the borrower must supply collateral greater than the value of the loan amount. As with asset-backed stablecoins, if the collateral value falls below a specified ratio of the loan value, the position is automatically liquidated to pay back the debt. A percentage of interest paid by borrowers is typically allocated to a reserve pool to repay lenders when a liquidation fails to cover the value of the loan (known as a failed liquidation). This requirement means that loans are generally used for leveraged trading or accessing new assets.

Compound

Compound is a money market protocol that lets users instantly lend to or borrow from a pool of assets in a smart contract. The interest earned is denominated in the same token that is lent. Interest rates are algorithmically derived and a function of the amount of assets available in each market based on supply and demand of each asset to reflect market conditions.

COMP governance token holders can propose and vote on all protocol changes, including interest rate models and supported collateral types. The COMP token popularized "liquidity mining," whereby a predetermined amount of COMP is distributed to all lenders and borrowers every day. While there is no cash flow attached to COMP at this stage, the value of the token reflects investor expectations about the success of the protocol. There may be a proposal in the future that allows COMP token holders to capture value directly from the platform's usage.

DERIVATIVES

Derivatives increase the sophistication of financial transactions beyond lending, creating both valuable market opportunities and new risks. A derivative could be based on the value of a stock, commodity, digital asset, at the present time of in the future; the cash flow of a business (creating a crowdfunding relationship); or a real-world event, such as the outcome of a sporting event or the weather (creating a prediction market).

In centralized finance, derivatives traders rely on a futures commission merchant and other intermediaries to accept orders to buy or sell futures or options contracts. They also accept money or other assets from customers to support such orders. Traders submit their orders to their respective clearing member firms, which then conduct the trade on the traders' behalf. The clearinghouse stands in between the two clearing firms and assumes the legal counterparty risk for the trade. It executes all the activities involved in clearing, securing, and settling the transaction.

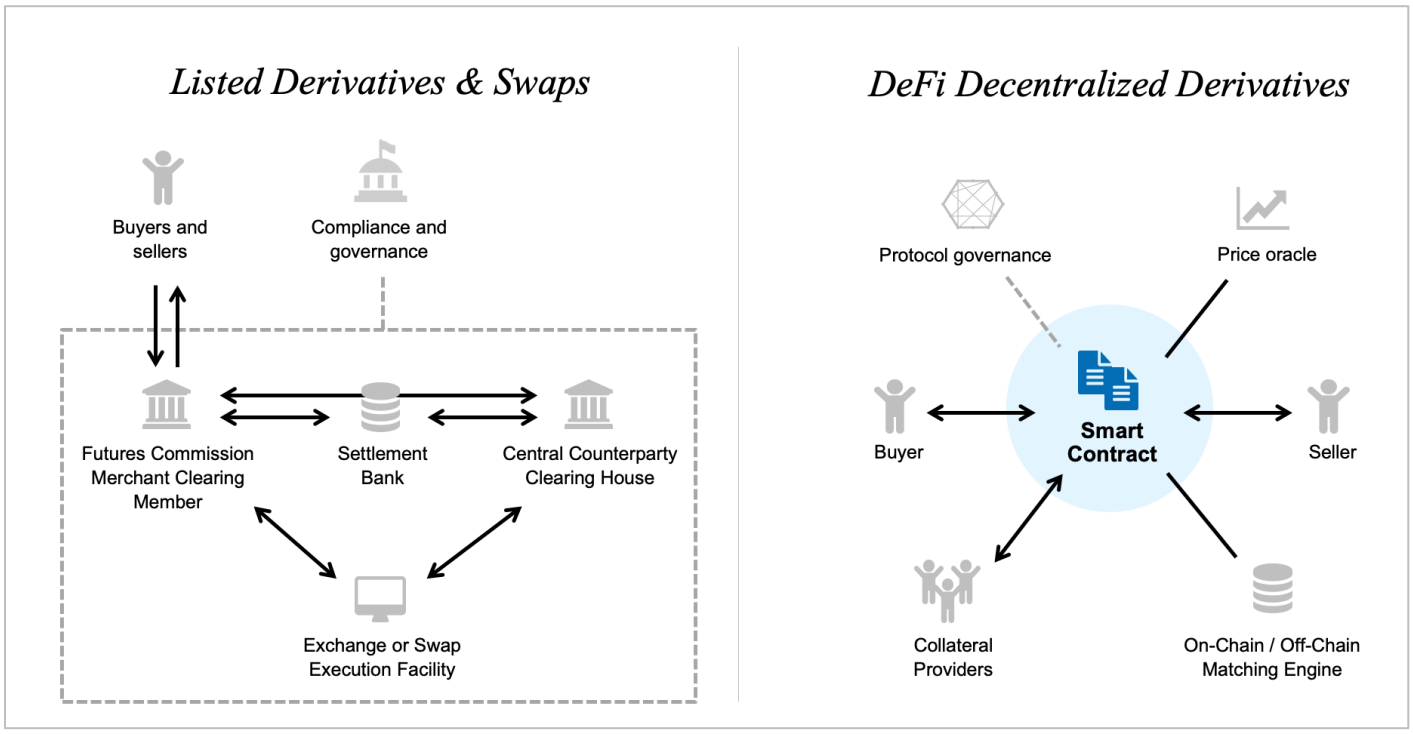

Figure 7 – Derivatives.

DeFi derivatives services connect buyers and sellers directly, backed by incentivized collateral pools as with the other major DeFi categories. Some allow users to buy and sell synthetic exposure to digital assets, without actually holding them. The derivatives can be associated with leverage, magnifying gains and losses, or inversely connected with the asset price, providing the equivalent of short exposure. Other applications involve prediction markets where users can bet on the outcome of future events, generating information collectively through the "wisdom of crowds."

Synthetix

Synthetix is a synthetic asset issuance protocol built on Ethereum. Users can get price exposure to digital assets, currencies, commodities, stocks, and indices through the creation of synthetic assets known as Synths. These Synths are overcollateralized derivatives. SNX token-holders stake and collateralize all Synths outstanding, earning trading fees in return. They can participate in the governance of the protocol through three distinct DAOs: The protocol DAO, the grantsDAO, and the SynthetixDAO. Notably, Synths may track the value of assets that users cannot purchase directly, due to jurisdictional or other regulatory requirements.

INSURANCE

Risk is essential to finance, and is correlated positively over time with returns. However, investors and others will often prefer to pay a definite but small amount to avoid the possibility of a larger loss. Others will be able to profit by taking on a portion of those risks in return for a payment. A centralized insurance carrier balances premiums received against investments made to maintain sufficient capital reserves for claims, along with associated risk assessment, underwriting, and claims management. While there are opportunities for DeFi derivatives to function as insurance against financial defaults, the primary focus of DeFi insurance services are the DeFi-specific risks posed by smart contract failures, successful hacks of DeFi protocols, game-theoretical risks of incentive systems, and similar failures.

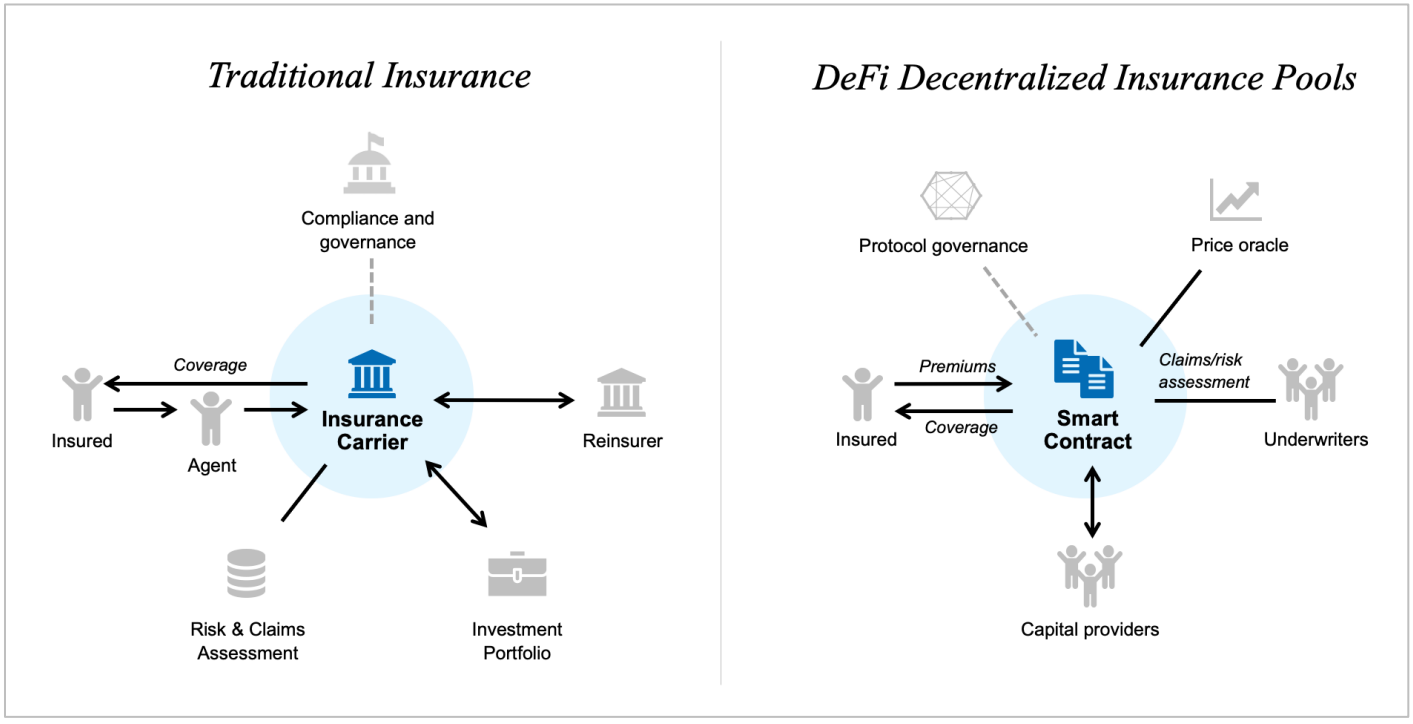

Figure 8 – Insurance.

DeFi insurance pools are collateralized with digital assets that provide capital associated with individual protocol, in return for tokens granting a share of premiums. In the event of a hack or other failure, those funds reimburse premium-paying users. Claims assessors vote on whether claims are paid out, while claim payments are typically enforced by token-driven economic incentives. Surplus and investment returns generally accrue to capital providers or governance token holders.

NexusMutual

NexusMutual offers smart contract insurance cover, which currently allows users to pay 2.6% annually for protection against a smart contract bug, and provides a payout in ETH or DAI based on claims assessment member votes. Recently, Nexus launched protection for funds deposited in centralized digital asset services, such as BlockFi and Celsius, in the event of a hack.

Nexus Mutual is established as a UK limited company regulated by the Financial Conduct Authority, similar to traditional insurers. Each user is subject to identity checks to become a part-owner of the mutual, with membership rights represented by NXM tokens. The NXM token can be used to purchase cover as well as participate in claims assessment, underwriting, and mutual governance. The value of NXM is driven by a formula including variables set by governance votes, and correlated with the size of the mutual fund pools. Over time, Nexus Mutual plans to invest its assets to earn yield on the float.

ASSET MANAGEMENT

Investors rely on asset managers to manage and allocate their portfolio. In traditional finance, an investment manager will typically assemble a regulated product such as a mutual fund, ETF, separately managed account, or private equity interest. Wealth managers package these products into asset allocations distributed through financial advisors and brokers to clients. Robo-advisors provide automated financial services with minimal to no human intervention or oversight.

In DeFi, the underlying investments can be composed of tokens, digital assets capturing traditional exposure, synthetic structured tokens, and interest-bearing accounts. DeFi asset management protocols combine them through smart contracts into “vaults” or “pools”, which function as a diversified portfolio of digital assets. The boundaries between asset classes and package types, as well as typical business models for these services, are still developing.

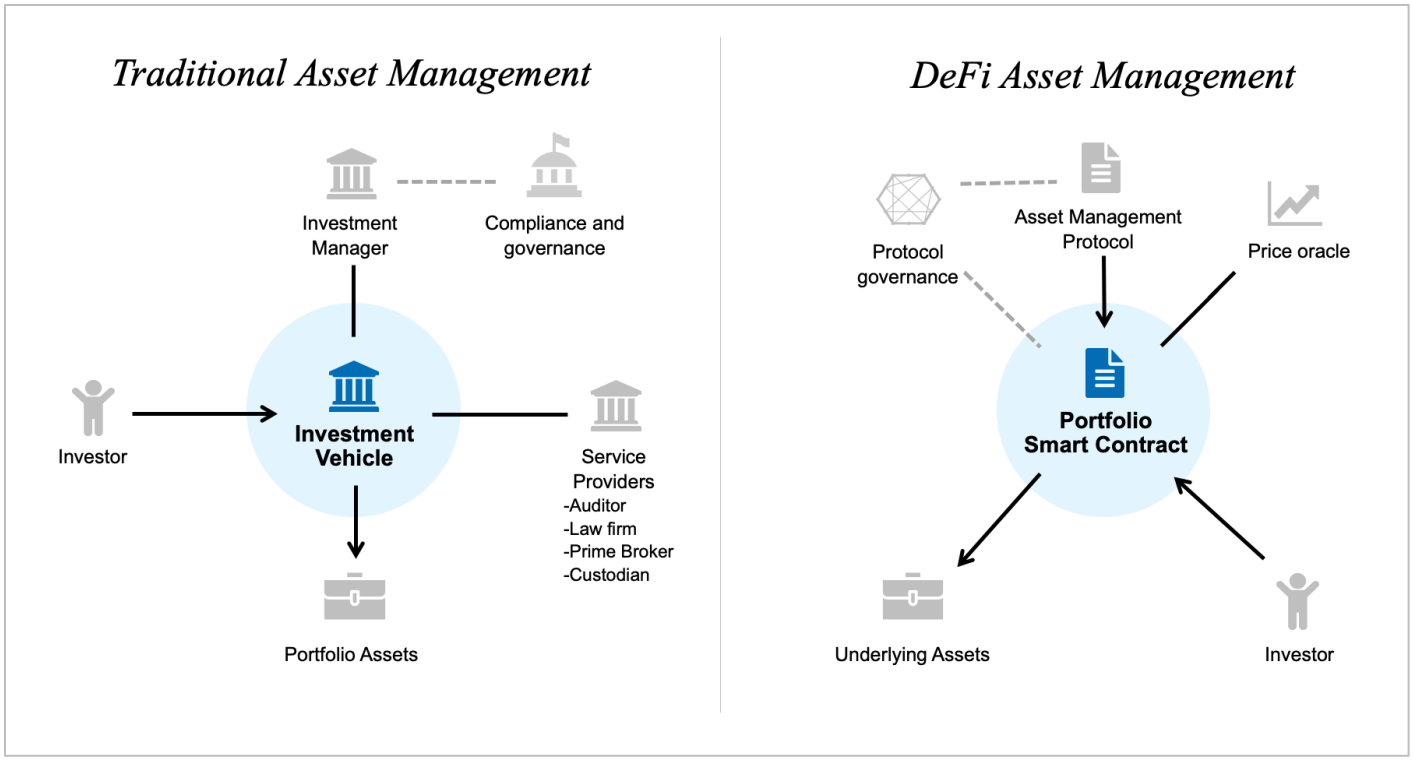

Figure 9 – Asset Management.

Set Protocol

Set is a decentralized portfolio management protocol enabling users to create a token that represents a fully collateralized portfolio of other digital assets, including Bitcoin, Ethereum, and stablecoins. The underlying collateral that backs each Set is held inside of a vault smart contract. Sets automatically rebalance with predefined logic when certain conditions are met, such as a rebalance interval or a minimum percent deviation from target, eliminating the need to trust a human counterparty and reducing trading fees, similar to robo-advisors in traditional finance.

As an example of the potential of DeFi asset management, Set Protocol and data company DeFi Pulse created a capitalization-weighted index of the top 10 DeFi tokens, called the DeFiPulse Index. By purchasing a Set representing the index, investors gain one-click, low-cost exposure to a basket of assets that rebalances monthly as prices change.

The Future of DeFi

Within and beyond the categories described here, DeFi is evolving rapidly. Developers are experimenting with new services, business models, and combinations of DeFi protocols. Technologies are maturing. Services are

moving to decentralized management and governance of protocols. Tools are emerging to simplify the user experience on and across DeFi services.

A significant aspect of ongoing DeFi development will involve composition of Dapps and financial primitives as "Money Legos." Already, aggregator services are emerging. DeFi composability might create new financial instruments and services, as well as new risks due to unanticipated interaction effects.

The investor population will also change as both less-sophisticated participants with more-limited cryptocurrency experience and more-sophisticated institutional traders enter in greater numbers. Speculative demand bubbles that produced spectacular returns over short periods will not be sustainable. Regulators will engage more actively in the DeFi area, especially as financial institutions and centralized finance providers look to become involved. While we cannot offer a crystal ball to predict the future of DeFi, we highlight some significant recent developments.

LENDING INNOVATIONS

Lending activity in traditional finance is often not secured by collateral, because identity data and credit-scoring are used to assess creditworthiness and limit defaults. Despite the absence today of analogous mechanisms, unsecured DeFi lending solutions such as flash loans are gradually emerging.

- **Fixed Rate Products** offer a stable interest rate despite fluctuations in the value of underlying assets. Yield Protocol creates tokens that may be redeemed one-for-one for a target asset after a predetermined maturity date, similar to zero-coupon bonds. The implicit yield curve is beginning to serve as the foundation for additional products.
- **Credit Delegation** allows users to deposit collateral assets into a DeFi lending service such as Aave, and then authorize trusted users to draw loans against that collateral. The two parties specify details of the loan through an arrangement called a Ricardian contract, in which a legal agreement is cryptographically linked to an associated smart contract on the blockchain. This system allows a depositor with unused borrowing power to delegate a credit line to someone whom they trust to earn additional interest. Borrowers can also refinance existing loans at much more favorable terms.
- **Institutional Corporate Credit** services such as Maple Finance allow institutions to borrow from liquidity pools managed by experienced investors. These Pool Delegates are responsible for assessing borrowers and negotiating loan terms before lending from their managed pool.

RISK MANAGEMENT INNOVATIONS

There is growing demand for better tools to repackage and redistribute risk associated with DeFi activities, allowing more efficient capital allocation and more complex derivatives.

- **Options** form the basis for a wide range of hedging strategies in finance. Opyn is a DeFi service for creating tokenized options, which can be used to hedge against risks or take speculative positions. It also supports flash mints, analogous to flash loans: options without collateral that are burned before the end of

the transaction. Ribbon Finance further supports **Structured Products** that combine options with other instruments for even more complex strategies.

- **Tranched Lending**, under development by DeFi service BarnBridge, separates debt pools into tranches of assets with different risk/reward characteristics, which investors can access separately.
- **Credit Default Swaps** allow investors to purchase insurance against default risk of credit arrangements. Saffron Finance is working on enabling this mechanism in DeFi, where users are able to trade swaps on the underlying lending platform.
- **Reinsurance** is traditionally how insurance companies themselves diversify risks. NexusMutual and other DeFi insurance players have begun extending smart contract insurance to each other, mimicking these arrangements.

SCALING INNOVATIONS

Ethereum in its current form is slow and suffers from high transaction fees, known as gas prices. Other blockchains such as Algorand, Avalanche, Binance Smart Chain, Cosmos, EOS, NEAR, Polkadot, and Solana are trying to attract DeFi-focused developers and users with promises of higher throughput and lower fees. However, better scalability at the base layer may come at a cost in the degree of decentralization or other attributes. The Ethereum Foundation promises significant scalability improvements in the upcoming Eth2, while Ethereum developers have been building a variety of Layer 2 solutions, such as sharding or "rollups," that offload computation execution, but keep some transaction data on-chain. Eth2 is also scheduled to replace proof-of-work mining, which has been criticized for intensive energy usage, with a proof-of-stake system.

Conclusion

DeFi is a new, fast-growing area. Yet it remains immature, with a variety of unresolved economic, technical, operational, and public policy issues that will be important to address. Although some protocols have attracted significant capital and the associated network effects in a short period of time, the DeFi sector remains volatile. DeFi has the potential to transform global finance, but activity to date has concentrated on speculation, leverage, and yield generation among the existing community of digital asset holders. In addition, the very flexibility, programmability, and composability that make DeFi services so novel also expose new risks, from hacks to unexpected feedback loops among protocols.

Retail investors, professional traders, institutional actors, regulators, and policy-makers will need to temper enthusiasm for the innovative potential of DeFi with a clear understanding of its challenges. Developers are actively working to address vulnerabilities and introduce new mechanisms to manage risks efficiently, but the process is ongoing. DeFi will ultimately succeed or fail based on whether it can fulfill its promise of financial services that are open, trust-minimized, and non-custodial, yet still trustworthy.

Acknowledgments

Lead Author

David Gogel (dYdX)

Project Coordinators

Sumedha Deshmukh (World Economic Forum)
André Geest (Ludwig Maximilian University)
Daniel Resas (Schnittker Möllmann Partners)
Christian Sillaber (University of Bern)
Kevin Werbach (Wharton School, UPenn)

Contributors

Teana Baker-Taylor (Crypto.com)
Ann Sofie Cloots (Cambridge University)
Brendan Forster (Dharma)
Jordan Lazaro Gustave (Aave)
Fabian Schär (University of Basel)
Lex Sokolin (ConsenSys)

Reviewers

Sebastian Banescu (Quantstamp)
Jacek Czarnecki (Maker Foundation)
Charles Dalton (PayPal)
Joyce Lai (New York Angels, NewTerritories.io)
Ashley Lannquist (World Economic Forum)
Xavier Meegan (ING)
Sheila Warren (World Economic Forum)

[1] We use the general term digital asset rather than cryptocurrency, virtual currency, or cryptoasset. Terms may have distinct legal meanings in certain jurisdictions.

[2] https://defipulse.com. Increasing digital asset prices contributed to this rise, but organic growth was also very strong. The number of DeFi wallets grew from 100,000 to 1.2 million during 2020, and new DeFi applications went from eight in 2019 to over 230 in 2020. *Exclusive: DeFi Year in Review by DappRadar*, The Defiant (December 28, 2020), https://thedefiant.substack.com/p/exclusive-defi-year-in-review-by-1f2.

[3] *See. e,g.*, Tobias Adrian, John Kiff, and Hyun Song Shin, *Liquidity, Leverage, and Regulation 10 Years After the Global Financial Crisis*, Annual Review of Financial Economics 10:1-24 (2018).

[4] *See e.g.* Laurence Fletcher, *Hedge funds rethink after GameStop pain,* Financial Times (April 14, 2021), https://www.ft.com/content/f7ddacb6-dc07-4142-adb2-f7eedf3a2272

[5] Nat Maddrey, *Ethereum's DeFi Evolution: How DeFi is Fueling Ethereum's Growth*, Coin Metrics (September 29, 2020), https://coinmetrics.io/ethereums-defi-evolution-how-defi-is-fueling-ethereums-growth/.

[6] Some efforts are underway to catalog and categorize the DeFi landscape, including the ConsenSys DeFi Score (https://defiscore.io/) and Codefi Inspect (https://inspect.codefi.network/). These use slightly different definitions of DeFi than the one presented here.

[7] Fred Ehrsam, *Blockchain Tokens and the Dawn of the Decentralized Business Model*, Coinbase Blog, August 1, 2016, https://blog.coinbase.com/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f.

[8] Olga Kharif, *Hedge Funds Flip ICOs, Leaving Other Investors Holding the Bag*, Bloomberg (October 3, 2017), https://www.bloomberg.com/news/articles/2017-10-03/hedge-funds-flip-icos-leaving-other-investors-holding-the-bag.

[9] *2021 Digital Asset Outlook Report*, The Block Research, https://www.theblockcrypto.com/post/88463/2021-digital-asset-outlook.

[10] Ethereum is in the midst of transitioning to a new version, Eth2, which promises significant scalability improvements, including replacing energy-intensive proof of work mining with proof of stake. *The Eth2 Upgrades: Upgrading Ethereum to Radical New Heights*, Ethereum Foundation, https://ethereum.org/en/eth2/.

[11] We use the term credit for borrowing and lending relationships broadly, rather than in the technical sense of money creation. In contrast to CeFi bank loans, where the borrowing process is separate from the pooling of capital to fund it, DeFi services can provide both sides simultaneously, often targeting the same users.