DeFi Primer

An overview of DeFi funding activity, concepts, and select protocols

PitchBook is a Morningstar company. Comprehensive, accurate, and hard-to-find data for professionals doing business in the private markets.

Credits & Contact

PitchBook Data, Inc.

John Gabbert Founder, CEO
Nizar Tarhuni Senior Director, Institutional Research & Editorial

Institutional Research Group

Analysis
Robert Le Senior Analyst, Emerging Tech Research
robert.le@pitchbook.com

Data
Bailey York Data Analyst

pbinstitutionalresearch@pitchbook.com

Publishing

Designed by **Kelilah King**

Published on August 27, 2021

Contents

Introduction

Decentralized finance (DeFi) refers to a new system of financial services and products that runs on public, open-sourced, and permissionless blockchains. Unlike traditional financial services, which rely on intermediaries such as banks, exchanges, or brokerages to manage and process transactions, DeFi services eliminate intermediaries, are peer-to-peer, and are typically encoded within smart contracts and protocols. DeFi services are built on blockchain platforms such as Ethereum and are accessed via decentralized applications (dApps) that connect the user to myriad financial services including paying, lending, borrowing, trading, and insuring. Unlike the digital services offered by traditional banks, dApps are built using public, open-source code, with development often occurring in the open and transactions ledgers viewable and verifiable by anyone.

DeFi's core principle is that disintermediation of legacy financial infrastructure is the key to democratizing financial access in ways that will reduce the fees and costs of financial products, increase the speed and settlement times of payments and transactions, improve the stability of financial systems, and increase transparency via open blockchains. DeFi also offers the potential for innovation and creation of new services not possible with traditional financial systems. These include low (or zero) cost payments, liquidity pools, synthetic tokens, and increased access to a wider range of non-traditional return-generating assets. As the DeFi ecosystem matures, we expect it will increasingly become interconnected with traditional centralized finance (CeFi). In the same way Bitcoin has become highly integrated with CeFi services such as payments (PayPal, for example), exchanges (such as Coinbase) and custodians (Fidelity, for example), we foresee a proliferation of "CeFi-to-DeFi" on- and off-ramps driving industry expansion. Still, while we have seen considerable development within DeFi during the past few years, many projects and digital assets are highly speculative and have yet to progress past the concept phase.

Limitations of traditional finance create opening for DeFi

Historically, centralized intermediaries including banks, brokers, exchanges, and insurers, have supplied traditional financial services that—in addition to their core products—ensure trust, safety, risk diversification, and liquidity. While centralized systems have helped power capitalist economies for generations, they nevertheless have shortcomings that have resulted in systemic failures. For example, the global financial crisis of 2007 underscored how single failures within CeFi can lead to systemic ripple effects across an entire economy. Traditional financial systems are also characterized by unequal access and have a poor track record of meeting the needs of everyone—particularly in less-developed regions of the world. Even in the US, nearly a quarter of adults remain underbanked or unbanked as of 2019, according to the Federal Reserve.[1] These failures come even as the industry continues to derive significant revenue in the form of fees for highly commoditized services that are often exacerbated during times of market volatility. For example, Americans paid $11.6 billion in bank non-sufficient funds, overdraft, and account maintenance fees during the first three months of the COVID-19 pandemic in 2020.[2] US banks also collected a record $10.6 billion in corporate bond issuance fees during this timeframe.[3] While insurance companies returned $14.0 billion to automobile customers as a sign of goodwill due to a sharp decline in driving, the refund program has been viewed as significantly less than what insurance companies saved in terms of reduced claims.[4]

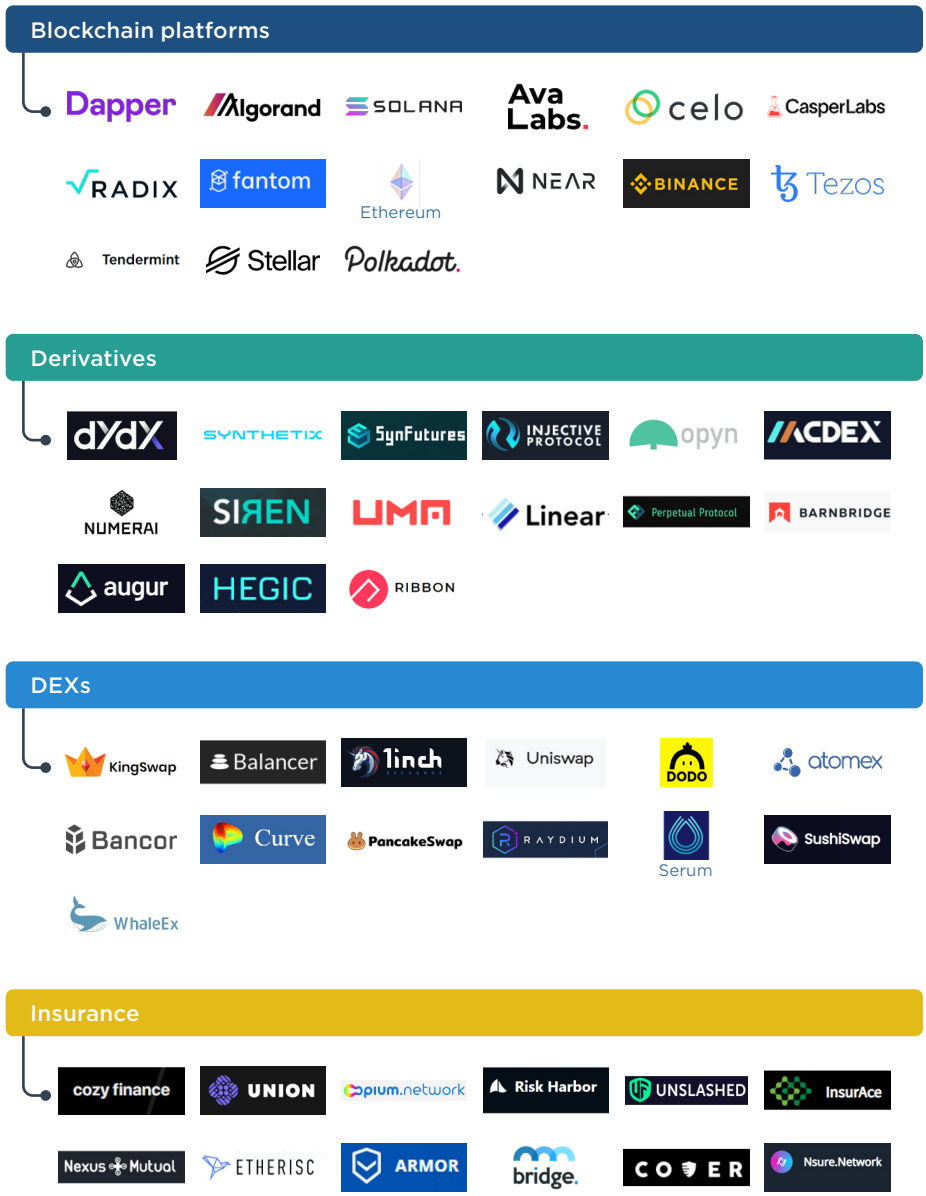
Over the past decade, many fintech startups have sought ways to disrupt the financial industry and have slowly taken market share from incumbents primarily by using technology to provide a better customer experience and by introducing new products, often at lower prices. Yet these companies are not as disruptive as they may appear because they still rely heavily on traditional bank-owned financial infrastructures to power underlying systems. DeFi, on the other hand, poses a more systemic threat as it provides an entirely new and distinct technology platform for the creation and delivery of financial services.

1: "Report on the Economic Well-Being of U.S. Households in 2019–May 2020: Banking and Credit," Board of Governors of the Federal Reserve System," May 21, 2020.
2: "Study: Big Banks Still Earning Billions from Fees During Pandemic," Stilt, Frank Gogol, August 2020.
3: "Global Banks Rake in Record Corporate Bond Fees Amid Pandemic," Reuters, Abhinav Ramnarayan, May 1, 2020.
4: "California Says Car Insurers Overcharged During the Pandemic," The Wall Street Journal, Leslie Scism, March 11, 2021.

DeFi ecosystem market map

Click to view interactive market map on the PitchBook platform

Market map is a representative overview of venture-backed or growth-stage providers in each segment. Companies listed have received venture capital or other notable private investments.



Source: PitchBook | Geography: Global
*As of July 12, 2021

DeFi ecosystem market map, continued

Lending, borrowing, and yield farming

OXYGEN, Compound, AAVE, 0x, MAKER, trusttoken, trusttoken, Goldfinch, notional, Centrifuge, YIELD, GRO, Euler, Reflexer, APY.Finance, maple, LIDO, Kava, Bunny, DeFiner, ALPHA FINANCE LAB, Anchor protocol, Badger, bZx, C.R.E.A.M., Harvest, YAM Finance, yearn.finance

Payments

Terraform, wyre, flexa, LIGHTNING LABS, CARDSTACK, DePay, fuse, MoonPay, Request, Sablier, StablePay

Scaling solutions

STARKWARE, Optimism, connext, CUDOS, rsk, OFFCHAIN LABS, SKALE, MatterLabs, polygon (Previously Matic Network), POA, Celer, LOOPRING, OMG NETWORK, Raiden network

Wallets and dashboards

METAMASK, Magic, Zapper, argent, Dharma Labs, INSTADAPP, ZERION, Authereum, Step, FRONTIER, eidoo, MEET ONE, MyDeFi

Source: PitchBook | **Geography:** Global
*As of July 12, 2021

DeFi blockchain platforms

The first use case of DeFi was Bitcoin, a peer-to-peer (P2P) electronic cash system launched in 2009 that did not require payments to flow through any financial institution. In 2015, Ethereum was launched with the goal of building decentralized applications. Most DeFi development occurs on the Ethereum blockchain. The platform has enormous first-mover advantages as it was the first to develop and enable the use of advanced smart contracts using the Solidity programing language. Smart contracts are lines of code running on a blockchain that will self-execute based on pre-defined terms. While Ethereum remains the dominant smart-contract platform, new platforms have proliferated in recent years to challenge Ethereum. Two separate platforms, Polkadot and Cardano, were started by the cofounders of Ethereum. Binance, one of the largest centralized crypto exchanges, has developed Binance Smart Chain. There are currently more than 20 smart-contract platforms that are seeking to displace Ethereum as the primary platform. Each has different technical specifications, security, and governance. The platforms are also competing to acquire developers to build dApps for them. For instance, Binance announced a program that will offer up to $5 million for developers to build dApps on its platform. Cardano developer IOHK, in collaboration with Wavemaker Genesis, launched cFund, a $20.0 million VC fund to seed projects building on Cardano with $250,000–$500,000.

Ethereum technical summary

Ethereum is currently the most widely used blockchain platform with more than 2,800 active dApps as of this writing.[5] Ethereum consists of two primary components, its blockchain architecture and Ether, or ETH, the native token required to conduct transactions and execute smart contracts on the platform. The Ethereum blockchain is a shared historical record of all transactions. Thousands of copies of the blockchain are stored on computers distributed globally, with each copy acting as a "node" to verify transactions and execute smart contracts based on a shared set of rules. This network of nodes confirms actions on Ethereum via a consensus mechanism known as proof of work (PoW). This is the same mechanism used by Bitcoin. PoW uses computational power as its primary resource for miners (who act as auditors) to validate transactions and be rewarded for doing so. PoW networks require all nodes in the network to be involved in transaction validation, which negatively impacts transaction throughput, speed, and scalability.

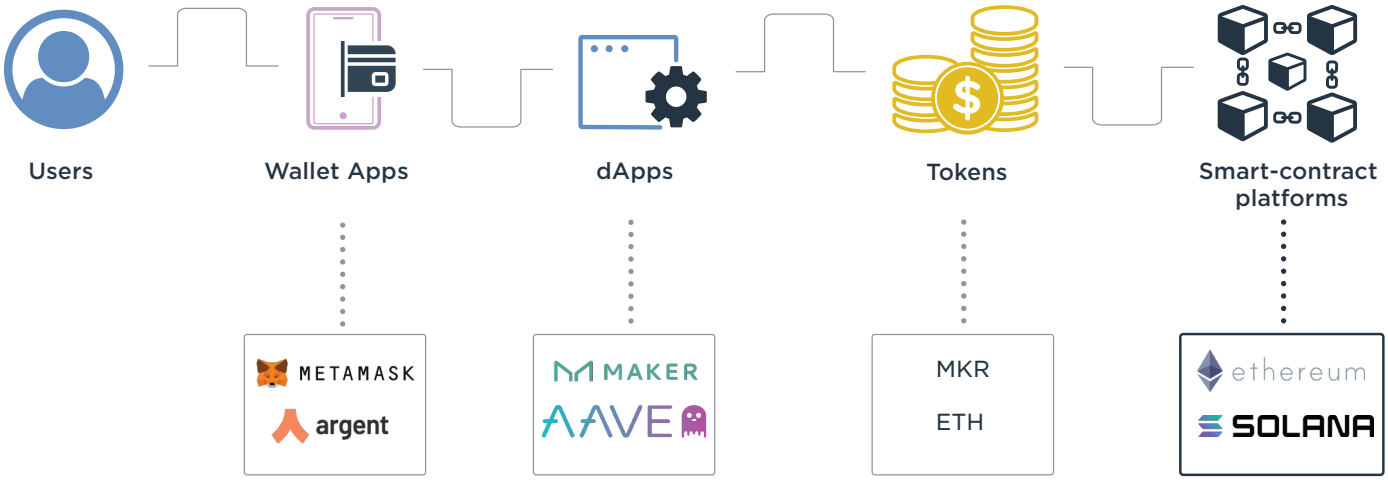
5: "State of the dApps: Ethereum," State of the dApps.com, 2021.

Smart-contracts platform comparison summary

	Ethereum	Ethereum 2.0	Solana (Solana Labs)	Avalanche (Ava Labs)	Cosmos (Tendermint)	Polkadot	Binance Smart Chain	Cardano	Tezos	Stellar
Transaction throughput (TPS)	15	100,000	56,000	5,000	10,000	400	100	250	40	1,000
Transaction fee	$5–$50	N/A	$0.00001	$0.03	$0.03	$1.78	$0.01	$0.02	$0.00232	$0.000001
Transaction finality (Average Time)	6 minutes	1–2 minutes	1–5 seconds	1–5 seconds	1–5 seconds	1–2 minutes	1–2 minutes	10 minutes	30 minutes	4 seconds
Type	Layer 1	Sharding	Layer 1	Layer 1	Layer 1	Sharding	Layer 1	Layer 1	Layer 1	Layer 1
Founder	Vitalik Buterin	Vitalik Buterin	Anatoly Yakovenko	Emin Gün Sirer	Jae Kwon	Dr. Gavin Wood	Changpeng Zhao	Charles Hoskinson	Arthur and Kathleen Breitman	Jed McCaleb
Primary office location	Zug, Switzerland	N/A	San Francisco, US	New York, US		Zug, Switzerland	Ta' Xbiex, Malta	Zug, Switzerland	Lewes, US	San Francisco, US
Year founded	2014	TBD	2017	2018	2014	2016	2017	2017	2014	2014
Token	ETH	N/A	SOL	AVAX	ATOM	DOT	BNB	ADA	XTZ	XLM
Market capitalization ($B)	$293.4	N/A	$10.5	$2.5	$3.2	$23.0	$26.1	$51.2	$2.5	$8.3
Fully diluted market capital ($B)	$293.4	N/A	$20.3	$10.9	$3.7	$26.1	$63.1	$72.1	$3.1	$18.0
VC raised to date ($M)*	$15.00	N/A	$60.0	$6.0	$29.8	$0.05	$11.8	N/A	$10.05	$3.0
VC deal count	3	N/A	4	1	3	3	3	N/A	1	2
Description	Open-source platform for decentralized applications	Upgrade to the Ethereum network that aims to improve the network's security and scalability.	Developer of protocol blockchain built to deliver layer 2 performance with layer 1 security and simplicity.	Open-source blockchain that bridges needs of developers and users with smart contracts and dApps	Cosmos is a dual-layer network that enables token, data, and asset exchanges between blockchains.	A network protocol that allows arbitrary data to be transferred across blockchains	Open-source peer-to-peer distributed system	Decentralized public blockchain	Open-source platform for assets and applications	Open network for storing and moving money
Consensus mechanism	Proof of work	Proof of work, Proof of stake	Proof of stake	Avalanche (proof of stake)	Byzatine fault tolerant	Hybrid consensus	Proof of stake authority	Proof of stake	Proof of stake	Stellar consensus protocol

Source: PitchBook | **Geography:** Global
*As of July 12, 2021

Mechanism for interacting with DeFi



Source: PitchBook | **Geography:** Global
*As of July 12, 2021

Most of the other smart-contracts platforms, such as Polkadot and Solana, use a different consensus mechanism known as proof of stake (PoS). PoS consensus mechanisms require "stakers" to validate transactions based on how many tokens they have staked (locked onto the platform) and for how long. The more tokens a validator has, the more "mining" power. PoS does not require all nodes to participate in transaction validation; hence, it has generally been viewed as the more favorable consensus mechanism as it has higher transaction throughput and speed. Ethereum is in the process of converting from PoW to PoS to solve its current scale and speed problems. The newly upgraded platform, Ethereum 2.0, promises to facilitate more efficient, speedier, and cost-effective transactions. However, the upgrade has been under development for years, including several launch delays.

Besides making upgrades to the primary Ethereum architecture (Layer 1), third-party developers have been building Layer 2 solutions—networks that are built on top of Layer 1. Layer 2 solutions have played an important role in the scaling of blockchain platforms, especially those reliant on PoW. These off-chain scaling solutions move the computations required to process transactions off the main blockchain and then later add the transactions based on them to a block on Layer 1 once the computations have been completed. While we view Layer 2 as a mid-term, band-aid solution, it is nonetheless critical in accelerating the growth of the DeFi ecosystem.

Ethereum Layer 2 scaling solutions

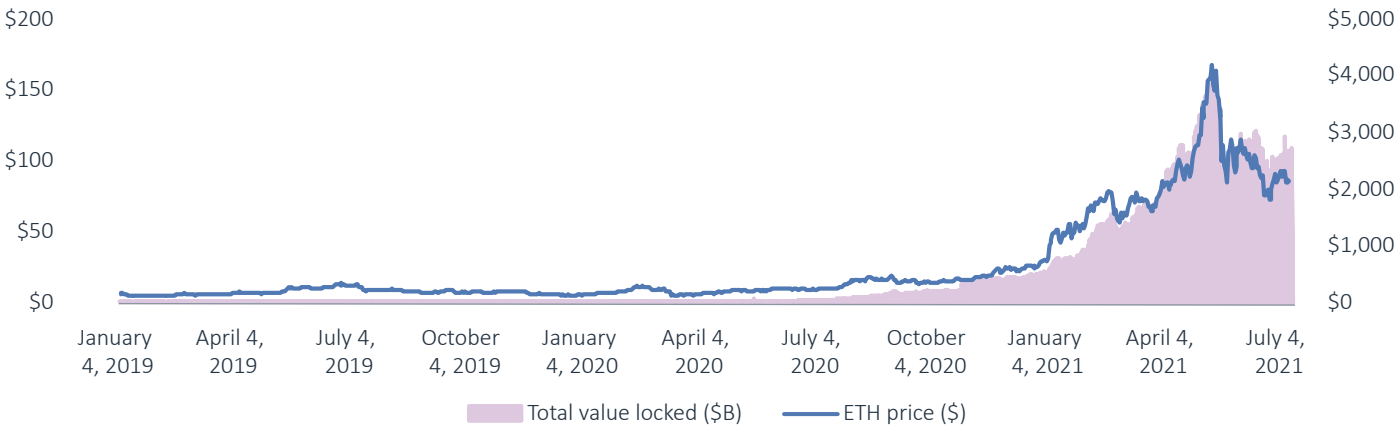
Layer 2 solution	Sidechains	State channels	Plasma	ZK rollups	Optimistic rollups
Description	Independent blockchains that run parallel to Ethereum and communicate with Layer 1 via two-way bridges. Sidechains have their own security properties and mechanisms of consensus.	Two-way channels that allow users to interact with each other, with only the net transaction published to Layer 1 once the users close the channel.	Separate smaller chains (child chains) anchored to Layer 1 that only broadcast transactions to the primary chain during low congestion times.	Zero knowledge rollups bundle hundreds of transfers into a single transaction on-chain. ZK rollups use cryptographic proofs to show that transactions are valid. Data is secured by Layer 1.	Optimistic rollups bundle hundreds of transfers into a single transaction on chain. Optimistic rollups only provide proof of validated transactions when fraud is suspected. Data is secured by Layer 1.
Protocols	Polygon, xDAI, RSK, SKALE	The Graph, Connext, State Channels, Raiden	OMG Plasma, LeapDAO, Gazelle	Loopring, zkSync	OMG Optimistic Rollup, Arbitrum

Source: PitchBook | **Geography:** Global
*As of July 12, 2021

Fast growing market opportunity

While DeFi has seen explosive growth in the past 18 months, the market for specific DeFi apps is still a small fraction of the total crypto market. One common metric used for DeFi is total value locked (TVL), which measures the amount of crypto committed to DeFi smart contracts. Users lock in crypto for staking, to conduct financial services, or to interact with a DeFi product. We view TVL as a proxy for how much demand there is for DeFi services. In the past 12 months, TVL grew to $108.0 billion from $2.0 billion and peaked at over $150 billion in May 2021. The total market cap of all crypto peaked at over $2.4 trillion around the same time.[6] We forecast that TVL could surpass $500 billion by 2026 with derivative protocols likely locking up the most value.

Total value locked and the price of ETH

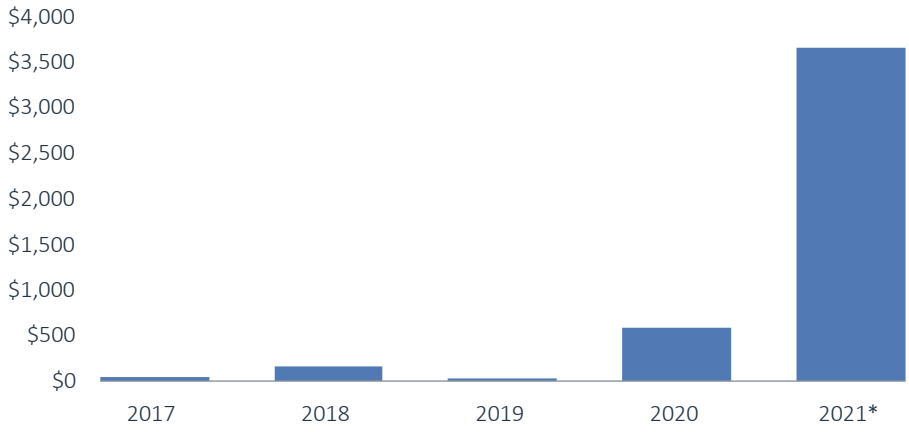


Source: DeFi Llama | **Geography:** Global
*As of July 12, 2021

6: "Crypto Total Market Cap, $," TradingView, August 11, 2021.

We also view gas fees (transaction fees) as a proxy for DeFi revenues. Ethereum gas fees jumped to $3.6 billion during the first six months of 2021 from $596.0 million in all of 2020.[7] A large portion of the fees were generated during high market volatility and network congestion in May 2021, leading to gas fees that climbed as high as $68 per transaction. While miners have earned significant revenues from gas fees in recent years, ongoing changes (such as a fee-burning mechanism and Ethereum 2.0) to Ethereum's network will substantially change the economics for miners.

Annual transaction fees ($M) paid on Ethereum



Source: PitchBook | **Geography:** Global
*As of July 12, 2021

We estimate that the total staking industry currently stands close to $100 billion and will likely double by 2024 given a successful rollout of Ethereum 2.0.

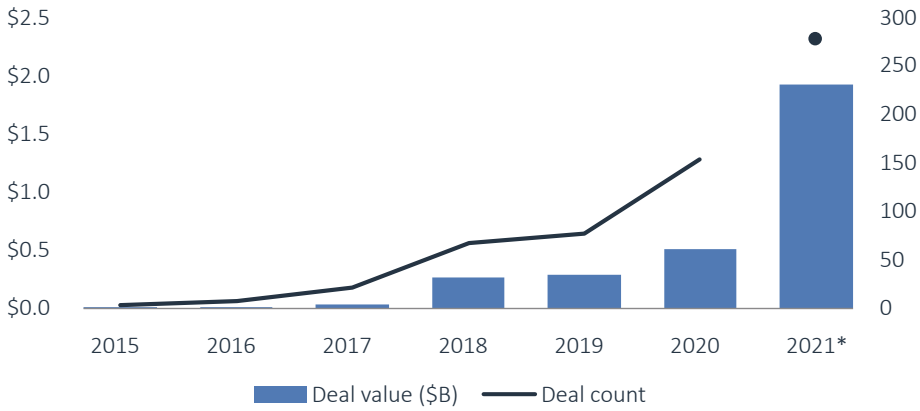
On Ethereum 2.0, transaction validation will shift from mining to staking, where stakers can earn fees of approximately 6%–7% annual percentage rate (APR) (on staked ETH), which is much lower than fees miners earn now.[8] However, we believe that with considerably higher throughputs expected on the new Ethereum blockchain, the lower per-transaction fee will be offset by a higher number of transactions. The Ethereum community also appears to generally support this view, with more than $12 billion staked to the unreleased Ethereum 2.0 network, which ranks only second behind Cardano ($29.3 billion) in assets staked among PoS blockchain platforms.[9]

Investments in DeFi on the rise

Through July 12 of this year, investors have put $1.9 billion across 278 deals into DeFi companies, which is more capital than all the previous years combined. While PitchBook tracks token deals that include venture funds (such as the $314.0 million token sale from smart-contracts platform Solana), token deals are not included in the dataset as they are often anonymous, suggesting the actual amount of capital being raised is likely larger. DeFi developers have also become more comfortable raising outside capital, with the median time for a first-time DeFi VC fundraise decreasing to 9.8 months in 2021 from 15.5 months in 2019. We believe the volume and velocity of capital flowing into DeFi has reached an inflection point, and increased institutional acceptance could accelerate investment.

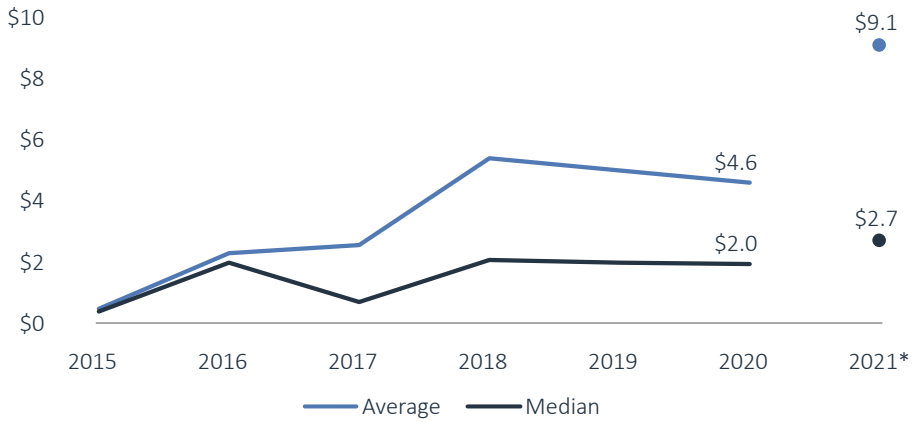
7: "The Ethereum Blockchain Explorer," Etherscan, August 11, 2021, and PitchBook estimates.
8: "The Fate of Ethereum Miners When There's Nothing Left to Mine," CoinDesk, Christine Kim, July 7, 2021.
9: Staking Rewards, August 11, 2021.

DeFi VC deal activity



Source: PitchBook | **Geography:** Global
*As of July 12, 2021

DeFi average and median deal value



Source: PitchBook | **Geography:** Global
*As of July 12, 2021

Top DeFi VC investors 2015–2021

Investor Name	Deal Count
AU21 Capital	57
Genesis Block Ventures	46
NGC Ventures	42
Genblock Capital	39
Spark Digital Capital	37
Alameda Research	35
Polychain Capital	34
Pantera Capital	29
LD Capital	29
Coinbase Ventures	29

Source: PitchBook | **Geography:** Global
*As of July 12, 2021

DeFi products and projects

Lending, savings, and yield farming

Financial service dApps seek to make it easy to borrow money (similar to secured credit), save, and earn interest. "Yield farming" is where users lock up their crypto to earn rewards (in the form of crypto) as their assets are used for various purposes such as providing market liquidity. While this practice is similar to providing liquidity in traditional finance, DeFi automates the process and opens it up to individual consumers (We will look at liquidity providers in greater depth in the decentralized exchanges (DEXs) section).

Notable projects

MakerDAO is an automated crypto lending protocol that allows users to borrow funds that are denominated in its native stablecoin, Dai. The Dai is collaterally backed by a digital currency (that is, Ether) with its value "soft-pegged" to the US dollar. Dai is different from many other stablecoins in that it is not backed by fiat currency held off-chain, but rather by a digital currency on-chain.

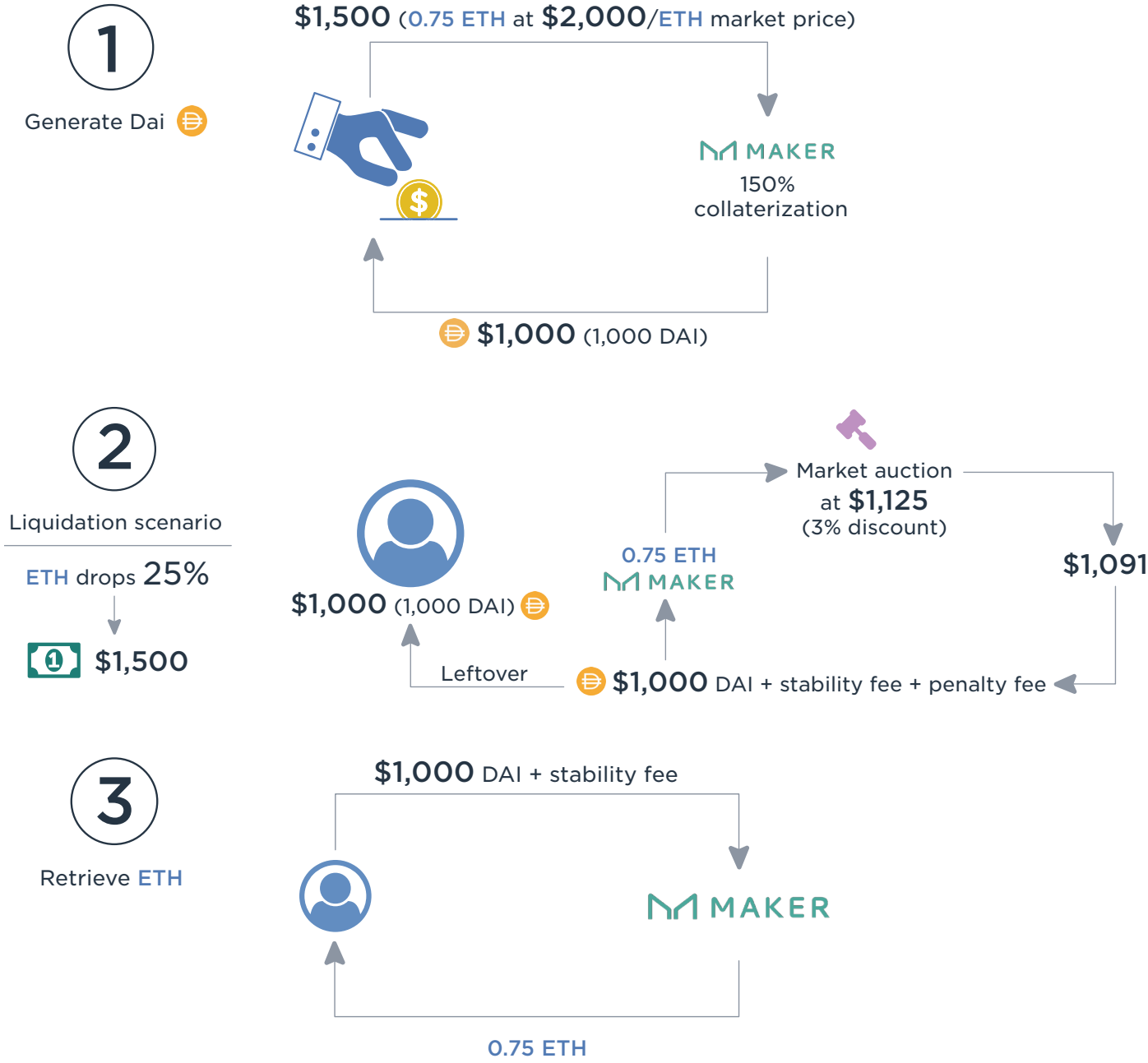
There are a variety of use cases for Dai, including providing liquidity, earning DSR (Dai Savings Rate) interest, hedging, and facilitating P2P payments. Dai can be borrowed for an interest fee by committing to lock up an asset such as Ether into the Maker platform in return for stablecoin. Borrowers run the risk that Ether could fall below a predefined threshold, triggering an automatic sell—akin to margin calls in derivatives markets.

MakerDAO is managed by holders of the platform's native MKR token, who vote on the collateralization ratio, DSR, types of collateral admitted, and other risk management rules for the Maker platform. Given that the recapitalization mechanism dilutes MKR and decreases its value, MKR holders are incentivized to set risk parameters that will maintain the stability of the system. Andreessen Horowitz became one of the early backers of MakerDAO when it purchased 6% of the total available MKR supply at the time for $15.0 million through its first crypto fund in 2018. The MakerDAO is currently one of the largest DeFi projects and has more than $5.0 billion collateralized.[10]

Compound is an automated money market protocol that allows users to earn yield on their crypto holdings or borrow crypto with interest. Whereas traditional banks seek to optimize net interest margin (that is, the spread over what they charge for loans versus what they pay in interest), Compound aspires to be a marketplace that connects borrowers and lenders directly through automated smart contracts. Compound supports multiple types of crypto, including ETH, Wrapped Bitcoin (WBTC),[11] USDC, and DAI. The borrowing and lending rates for each type of asset are adjusted algorithmically based on supply and demand.

10: "Dai," CoinMarketCap, August 12, 2021.
11: Wrapped Bitcoin is a tokenized version of Bitcoin, essentially enabling Bitcoin to be used on the Ethereum network.

Three primary Maker scenarios: 1) Generate Dai, 2) liquidation, 3) retrieve ETH



Source: PitchBook | **Geography:** Global
*As of July 12, 2021

Compound has experienced fast user adoption because of its simplified user experience (UX) and intuitive dashboard, which only requires users to connect existing crypto wallets without having to understand the underlying mechanics of the protocol. The protocol is administered by a decentralized network of holders of the governance token, COMP, who vote (or delegate their votes to any address) on proposals. As of this writing, three of the top five holders of COMP are VC funds: Andreessen Horowitz (13.2%), Bain Capital Ventures (9.8%), and Paradigm (4.3%).

Outlook

While traditional banks are still in the process of migrating their core banking systems from mainframe computers to the cloud, we believe DeFi could be the next generation of core banking systems. Blockchains fundamentally function like core banking in that transactions are tracked on a ledger and tied to account information (wallets). Further, lending and savings protocols can "onboard" users through smart contracts to participate in banking-like services. When users can easily convert DeFi holdings to fiat currency or spend stablecoins in the real-world, we believe lending and savings protocols can replace some traditional banking loans and deposit products.

Wallets and dashboards

Defi wallets and dashboards are mobile and web applications that allow users to interact with dApps, store private keys, and view balances and holdings. These wallets are primarily non-custodial in that users are responsible for the storage of funds and assets without having to rely on a third-party financial service provider (private keys are stored locally on the device). Wallets are typically the first DeFi touchpoint for users, so a simple, clean UX and user interface (UI) are critical for widespread adoption. Dashboards are consolidated interfaces that allow users to calculate net worth, track protocols and portfolios, and monitor staking and yield farming. Some dashboards provide analytics and other tools similar to those provided by traditional retail brokerages.

Notable projects

Metamask is one of the most popular DeFi wallets with more than five million monthly active users.[12] The wallet is primarily accessed through a browser extension that allows users to run dApps directly in the browser. Metamask was developed under the ConsenSys framework.

Zapper is a hub that connects to wallets to let users visualize and manage their DeFi assets and liabilities. Zapper provides a rich set of information that lets users understand their asset allocation, collateralized holdings, and liquidity opportunities. The company has raised seed and Series A rounds that combined for more than $16 million from investors such as Framework Ventures, Mark Cuban, and Ashton Kutcher.

Outlook

The adoption of non-custodial wallets has recently accelerated, largely in part to the simple UIs and UXs of wallets such as Metamask and Argent. However, we believe the recovery process (if you lose your device and/or password) is still too complex and cumbersome. The fear of losing access to a wallet and all its associated assets is high among DeFi participants. We expect easier, more intuitive recovery processes must be developed before DeFi wallets can gain mainstream adoption.

12: "MetaMask," April 27, 2021.

Payments

DeFi promises to deliver payment solutions that cost less and settle more quickly than those offered by traditional fiat payment apps.

Notable projects

Fuse is an Ethereum sidechain payment network designed to provide a very-low-cost alternative to traditional payments. The protocol consists of three layers: Fuse Chain, Fuse Studio, and Fuse Wallet. Fuse Chain is maintained by validators that have staked the FUSE network token, which is used to pay transaction fees on the network (currently $0.000003 per transaction regardless of amount). Validators verify transactions, earn transaction fees, and control the governance of the protocol. Fuse Studio is a white-label payments application that allows companies to launch payment services backed by the Fuse payment network. Fuse Wallet is a consumer-facing mobile application that can be linked to external accounts to deposit funds.

Request is an open-network payments system that allows users to share payment requests. Although there are DeFi payment applications targeted at improving traditional payment systems, even within DeFi, payments can be inefficient and complicated. In many dApps, before sending a payment, users need to verify obscure wallet addresses, tokens typically must be traded on exchanges, and gas fees need to be specified. A DeFi payment protocol such as Request could gain traction by simplifying the DeFi payments process.

Outlook:

We believe DeFi payments will become more directly integrated with wallets as opposed to standalone dApps. We expect these wallets will be similar to traditional mobile payment wallets, where users can send and request payments, transact, and even earn rewards. Also, the next generation of DeFi payments will converge with CeFi, further blurring the lines between the centralized and decentralized payment systems.

Decentralized exchanges

Decentralized exchanges (DEXs) enable the permissionless, non-custodial trading of cryptocurrencies and tokens. Unlike a centralized exchange such as Coinbase, users exchanging on DEXs do not have to provide personal information, relinquish their private keys, or give over control of their funds to participate. While centralized exchanges use traditional order books (based on the bid-ask spread) to price trades, DEXs use an automated market maker that prices trades based on an algorithm.

Notable projects

Uniswap is a DEX that has grown to become one of the largest crypto spot exchanges, with more than $135 billion in trading volume in the first nine months on its version 2 protocol, which launched in May 2020. For comparison, Coinbase had $193.0 billion in trading volume in 2020.

Uniswap's automated market maker relies on users as liquidity providers to create a market via a liquidity pool. Each liquidity pool is made up of a reserve of token pairs, such as ETH and USD Coin (USDC).[13] To create a pair market on Uniswap, liquidity providers deposit an equivalent value of ETH and USDC in return for liquidity tokens. An arbitrage opportunity exists if users do not deposit an equivalent value of a token pair. Liquidity tokens can be redeemed for a share of the trading fees. On Uniswap, a 0.3% "swapping fee" is charged for each transaction, which is then allocated to a reserve for liquidity providers. Users are charged a 0.5% trading fee in addition to a flat fee ranging from $0.99 to $2.99 based on the transaction size—much lower than fees charged by centralized exchanges such as Coinbase.

After launching with a $100,000 grant from the Ethereum Foundation, Uniswap went on to raise a $1.8 million seed round from Paradigm and a $10.9 million Series A led by Andreessen Horowitz.

Curve is a type of DEX that focuses on the swapping of comparably priced assets such as stablecoins or tokenized Bitcoin. Automated market makers such as Uniswap and Balancer that swap volatile assets with different prices are prone to arbitrage opportunities, which can hurt liquidity providers through impermanent loss—a temporary asset depreciation that may or may not recover depending on the market value of the asset. For example, if the market price of ETH jumps by 15%, an arbitrageur can obtain ETH at a cheaper price in an ETH/USDC liquidity pool and sell it on the open market. Curve minimizes impermanent loss by offering token pairs with prices that move in lockstep with market prices. The tradeoff for liquidity providers is that earning fees are much lower since Curve only charges four basis points per trade. Curve currently has almost $10 billion of liquidity in all pools and about $250 million in daily trading volume. The protocol received undisclosed VC from Codex Venture Partners in Q1 2021.

Outlook

While DEXs have gained strong traction in the past year, we believe that multichain DEXs such as Zeroswap and SnowSwap will be the next iteration that will allow users across any blockchain platform to trade. Multichain DEXs will make it easier to conduct trades across the DeFi ecosystem. Further, multichain DEXs typically have much lower trading fees than single-chain DEXs (Zeroswap and SnowSwap fees are 0% and 0.04%, respectively, while Uniswap is 0.3%), and their proliferation will create downward pressure on trading fees.

Derivatives

Derivatives are assets whose value is based on another underlying asset. Similarly, decentralized derivatives (also known as synthetic assets) allow for on-chain exposure to various on- and off-chain assets including stocks, cryptocurrencies, fiat currencies, and commodities.

13: USD Coin (USDC) is a stablecoin. One USD Coin can always be redeemed for one US dollar, giving it a stable price.

Notable projects

Synthetix is a protocol that allows users to issue and trade synthetic assets. Known as "Synths" on the platform, these derivatives track the value of other assets through oracles (data feeds that deliver off-chain data on-chain). Synths are generated when users stake the native Synthetix Network Token (SNX) at a 750% collateralization ratio. For example, a user can generate one Tesla (NASDAQ: TSLA) Synth (sTSLA) by staking $4,457.1 worth of SNX (750% of Tesla's current share price of $685.7). Users are incentivized to stake SNX to earn more SNX as rewards and share in the fees generated by Synth trades. Users can also purchase Synths without staking by purchasing Synths that have already been generated by stakers. Users typically purchase Synths because they are unable to purchase the underlying asset itself for geographical reasons such as non-US citizens seeking to purchase US equities), they lack identification, or they do not want to open multiple accounts to own different assets. Synthetix raised a $12.0 million venture round in February 2021 in a deal led by Coinbase Ventures, Paradigm, Synapse Capital, and IOSG.

UMA, short for Universal Market Access, is a protocol that seeks to democratize derivatives by enabling anyone to enter a derivative contract. In traditional derivatives, counterparties enter a legally binding agreement and post an initial margin. If one party fails to pay at the end of the contract term, the margin is forfeited, and the nonpaying party may be sued. Entering derivatives contracts with legal recourse makes sense for large financial institutions due to their large positions. For much smaller derivatives, UMA can replace the legal recourse mechanism with on-chain binding agreements. Like traditional derivatives, UMA allows any two counterparties to enter into a financial agreement on the price movement of a referenced asset by posting margin—typically 10% of the contract price—that is locked into a smart contract. For example, two parties can enter a contract that tracks the price of Tesla stock over the course of three months. One side is betting that Tesla will be below a pre-determined reference price while the other side is betting that it will be above that price. As the price of Tesla moves, the party on the losing side of the trade will have to post more margin (to maintain at 10%); otherwise, they risk a penalty through liquidation. At the end of three months, the party that correctly selected Tesla's stock price relative to the reference point is automatically paid. UMA has raised more than $4 million in VC from investors including Bain Capital Ventures, BoxGroup, and FinTech Collective.

Outlook

The derivatives asset class is the largest by far within traditional finance. We believe that decentralized derivatives and synthetic assets will likely become the largest asset class in the DeFi space—and possibly the entire crypto space in the long term. Due to the programable nature of synthetic assets, we expect novel derivative products to proliferate at a faster rate than traditional derivatives.

Insurance

DeFi insurance offers protection policies that act as safety nets for crypto and assets held in wallets, exchanges, or liquidity pools. Due to the high number of hacks, scams, theft, and smart-contract failures occurring in DeFi, users are increasingly seeking backstop measures to protect their capital.

Notable projects

Nexus Mutual is a DeFi insurance platform based on the mutual insurance model in which policyholders own the protocol and share in the risk and profits of premiums. The types of coverages the protocol provides are:

- Protocol: Provides protection to funds deposited into protocols and covers when protocols suffer from material financial losses related to governance attacks, protocol code errors, or severe oracle failures.
- Yield tokens: Yield tokens are usually held 1:1 in a liquidity pool (for example, 1:1 DAI to yDAI on Yearn Finance). However, if bad investments trigger significant ratio changes that cause the value of the yield token (yDAI) to fall by more than 10%, Nexus will cover up to 90% of that loss.
- Custody: Provides coverage if a custodian is hacked or fund withdrawals are halted for more than 90 days from a centralized custodian such as Coinbase).

Nexus Mutual members are holders of the NXM token, which can be used to purchase coverage, but also for governance, risk assessment, and claims assessment. When a claim occurs, NXM token holders can vote to approve or deny claims through a community discussion and review of on-chain and off-chain submitted data. NXM rewards are given out to those providing honest contributions to the claim assessment process. Nexus Mutual, one of the most prominent DeFi insurance protocols, also has plans to provide earthquake insurance in the future.

Risk Harbor is a DeFi insurance platform similar to Nexus Mutual, except the protocol replaces the decentralized governance process with a claims process that is fully automated through smart contracts based on pre-determined criteria, a model similar to parametric insurance.[14] Risk Harbor's rules for a claim are completely on-chain, thus having claims approved or denied open and transparent to everyone. The protocol provides coverage related for the loss of capital in some of the largest protocols such as Curve, Yearn, Aave, and Compound. Risk Harbor functions under a marketplace model, where on one side, users are seeking to purchase protection, while on the other, users underwrite by providing capital. The protocol uses "protection pools," where underwriters deposit capital and users seeking protection deposit the total premium (for a set coverage period). At every block, a proportional

14: Parametric insurance offers pre-specified payouts should a trigger event occur.

amount of capital is paid out to underwriters as a fee for providing protection. If a hack occurs and a claim is initiated, funds are paid out to insured from the protection pool if it meets preset parameters. Risk Harbor raised a $3.3 million seed round led by Framework Ventures and Pantera Capital in June 2021.

Outlook

While most DeFi insurance provides coverage for crypto and protections of capital related to DeFi projects, we believe some areas of property & casualty insurance have natural synergies with DeFi. For instance, oracles that collect weather related data off-chain can be used to pair with on-chain parametric insurance policies. Insurance within DeFi is still very nascent but we believe that coverage types will expand over time and will have the potential to disrupt traditional insurance models.

DeFi considerations

While we have seen considerable development within defi during the past few years, many projects and digital assets are highly speculative and have yet to progress past the concept phase. Further, as with any new, fast-growing technology, numerous risks and considerations exist.

Blockchain technical risks

The lack of scalability remains a key obstacle to the growth of blockchain tech, specifically for Ethereum and other PoW protocols. High network congestion can lead to failed transactions and exorbitant transaction fees. For example, Ethereum can currently process about 15–30 transactions per second, a dismal figure compared to Visa's 1,500–2,000 transactions per second with a theoretical limit of more than 24,000 transactions per second. These bottleneck risks manifested themselves in March 2020 when MakerDAO had to liquidate ETH to meet collateralization thresholds. Lack of scaling drove extremely high gas fees, effectively closing the market to only those bidders who could afford the fees, allowing them to corner the auction.

Technical vulnerabilities pose additional risks. Anyone can develop a dApp to run on Ethereum, Solana, or other smart-contracts platforms. A poorly coded protocol can be vulnerable to attacks. This occurred when the Ethereum protocol The Dao (an organization also known as Genesis DAO and not to be confused with the general term "DAO" for decentralized autonomous organization) was effectively hacked, resulting in the theft of $60.0 million worth of ETH after an initial $150.0 million token sale. The Ethereum community was forced to conduct a "hard fork" of the platform (effectively a split off the original blockchain, resulting in Ethereum and Ethereum Classic). Further complicating matters, buggy protocols can't simply be fixed by the lead developer team but require consensus votes among the many decentralized nodes before fixes can be implemented, extending the time frame during which security flaws can be exploited.

Open-sourced code allows anyone to clone an established dApp and create a duplicate application, a process known as "forking." Forking draws users, liquidity, and capital away from the original application. In one example, SushiSwap was launched in August 2020 as a fork of Uniswap. Within a week, SushiSwap saw its total value locked (TVL) jump by about $1 billion while Uniswap's TVL decreased by about the same amount. Although most forks fail, SushiSwap shows how forks remain a risk for successful DeFi protocols. As of this writing, Uniswap and SushiSwap are ranked number two and number three, respectively, based on TVL among DEXs. Other successful forks include C.R.E.A.M. Finance (a fork of Compound) and Swerve Finance (a fork of Curve Finance).

There are numerous other technical risks that stem from the vulnerabilities inherent to smart contracts. These include front-running (using knowledge such as proposed gas fees of pending trades to place a trade order that is more likely to be processed first), re-entrancy (repeatedly requesting and receiving ETH from a smart contract before it updates its internal state), and timestamp dependency (where miners can manipulate the timestamp of a block for nefarious purposes). These vulnerabilities create additional attack vectors for hackers and scammers to drain funds or manipulate smart contracts.

Fraud, hacks, scams, and exploits

The irreversibility of blockchain transactions and the fact that most DeFi applications and smart contracts do not have fail-safe measures, increases exploitive opportunities for scammers. It is estimated that DeFi hackers have netted $156.0 million in stolen funds through the first four months of 2021, more than the $129 million in all of 2020.[15] This does not include $83.4 million worth of "rug pulls," where a majority of token holders (usually the developers) cash out at once leaving everyone else with valueless tokens.

Fragmentation and limited clarity of regulations

Financial regulations are designed to protect the financial services industry and uphold stability and integrity of financial systems, market confidence, consumer protection, and financial crime prevention. DeFi, however, does not fit into the traditional framework of financial regulations. For the most part, financial regulations are designed to target financial intermediaries as a means of regulating markets and keeping them safe. DeFi—which eschews intermediaries in favor of algorithms—does not fit well within this framework and requires a new approach to financial regulation. For example, review processes associated with the Bank Secrecy Act (BSA)—such as anti-money laundering and know-your-customer—or Financial Crimes Enforcement Network (FinCEN) rules are difficult to apply to unhosted DeFi wallets since personal information is typically not collected.

15: "Cryptocurrency Crime and Anti-Money Laundering Report," CipherTrace, February 2021.

The borderless nature of DeFi with its inherent distributed, non-centralized, and often open-source construct also creates complications when it comes to determining accountability and responsibility. DeFi products typically do not have clear risk disclosures, nor do they have internal risk-management procedures or support functions for confused customers or those wishing to correct mistakes. There is also no clear way to undo transactions, which are usually irreversible by design. Lack of clear regulations is likely to hamper development and slow the rate of adoption among consumers.

Centralization risk

While DeFi and DAO projects seek to create fully decentralized and distributed governance systems, centralization risk can occur when "whales" (large holders of a specific token or cryptocurrency) control the voting power of a protocol. For example, in late-2019, a whale holding more than 90% of the voting power on Maker (based on the amount of MKR held) was able to implement a change that reduced the stability fee to 5.5% from 9.5%. While many projects such as Maker and Compound started out with centralized governance structures, these projects have over time converted to DAO governance models. However, the economic incentives to obtain and hold governance tokens have resulted in the gradual concentration of tokens for some projects.

Complicated UX and high learning curve

Most dApps are still too complex for ordinary consumers, who are not only required to develop an esoteric set of knowledge related to private-key security and DeFi-specific terminologies (gas fees, staking, and slippage, for instance), but must also navigate a complicated and ever-expanding landscape of similar applications with unclear value propositions. Opaque messaging related to financial risks along with deceptive promises of high annual percentage rates can severely diminish the user experience. For instance, Harvest's advertised 119.7% annual percentage rate is disbursed via its native iFARM reward token, which involves a complicated vesting schedule and rewards claiming process.

It is also complicated to use certain platforms. Transacting in dApps on the Ethereum blockchain requires the payment of gas fees, which can result in a failed transaction if the fees aren't high enough—something a user wouldn't know until after the fact. For all of these reasons, user literacy remains low, and many consumers participate in DeFi only for speculative purposes or to earn yield on staking tokens.

DeFi outlook

Although the industry's north star is a fully decentralized financial system, we believe DeFi will increasingly become interconnected with CeFi—similar to how Bitcoin was launched as a decentralized payments network yet has become highly integrated with CeFi services such as payments (PayPal, for example), exchanges (such as Coinbase) and custodians

(Fidelity, for example). To that end, we expect DeFi on- and off-ramps to proliferate in the coming years to enable CeFi participation. For example, in June 2021, Compound announced Treasury, a platform that gives non-crypto businesses and financial institutions the ability to deposit their cash, which is then converted to USDC, into a Compound Treasury account to earn a guaranteed 4% interest rate with 24-hour withdrawals. Similarly, Metamask Institutional gives financial institutions, family offices, and crypto funds the ability to access DeFi dApps. The application connects directly to crypto custodians and lets wealth and investment managers give clients access to DeFi assets and services. As the bridges connecting DeFi and CeFi become more reliable and secure, we expect institutional adoption of DeFi to accelerate.

Institutional adoption will take shape in multiple ways. We believe institutions will begin to purchase and hold DeFi tokens for some of the most prominent DeFi protocols. Improved knowledge and risk management will lead to larger token investments. Institutions will likely become nodes and stakers of DeFi protocols, enabling them to share in the economics. It is possible that financial institutions will become the primary stakers for most DeFi protocols as the cost to stake increases along with growth of the ecosystem. For instance, the minimum staking requirement for Ethereum 2.0 is 32 ETH, which currently adds up to more than $64,000. Increased institutional demand for DeFi will create long-term tailwinds for custodial services such as those from Anchorage and Coinbase. Traditional financial institutions such as Goldman Sachs will also likely continue to explore and develop DeFi custodial capabilities.

As new smart-contracts platforms continue to crop up, interoperability among the various platforms will be vital to growing the DeFi space. This will occur by enabling front-end wallet applications to exchange tokens, as well as by building back-end infrastructure such as cross-chain bridges that allow tokens to move seamlessly across blockchain platforms. Multichain capabilities are likely to be the next progression for DeFi wallets and dashboards. For example, Phantom, which provides a wallet that allows consumers to access dApps on the Solana blockchain, is working to expand connectivity to other smart-contract platforms, starting with Ethereum. In July 2021, the company raised a $9.0 million Series A from Andreessen Horowitz, Jump Capital, and other investors. At the same time, platform developers are building cross-chain bridges that allow data and tokens to flow across different blockchains. Polkadot and Cosmos are currently building bridges to connect with other blockchain platforms. We expect similar development to occur among other smart-contract platforms.