NOVEMBER 2022

DECENTRALIZED FINANCE:

USE CASES, CHALLENGES AND OPPORTUNITIES

IIF

INSTITUTE OF INTERNATIONAL FINANCE

Acknowledgements

The IIF would like to thank those IIF member financial institutions, academics, ecosystem actors and official sector representatives whose insights and input, particularly through interviews, have contributed to this report.

IIF acknowledges the support of Amazon Web Services, Inc. in sponsoring the production of this report and in making their staff available to the IIF for discussion.

FOREWORD

Decentralized finance (DeFi) and Web 3.0 have generated excitement and hype. Some say they are the future of finance, others focus more on the risks, challenges, and possible consumer harms, many of which have become prominent during the crypto market events of 2022. What is clear is that DeFi and efforts to develop Web 3.0 are bringing new technology and innovation to how people connect, interact, create value from content, and trade assets. This creativity is driving fresh ideas about how the broad spectrum of financial services and intermediation might be re-imagined in an increasingly digital economy.

Tokenization can bring assets of all kinds into an integrated ecosystem for the trade and transfer of value. This can range from tokenized deposits and equities to new digitally native tokens from gaming and other digital content-creating environments – in turn, this could open new ways to connect ventures and small businesses to capital and markets. Opportunity for new products and services, as well as transformative efficiency in streamlined operations for trading, settlement, and record keeping, could be realized in institutional financial service offerings – such as foreign exchange (**FX**), equities, bonds, and mortgages – by leveraging various degrees of DeFi solutions.

Cloud computing and the development of Web 3.0 help open up these opportunities for large legacy institutions and entrepreneurs alike. Many DeFi projects and nodes are hosted in public cloud environments where they can be supported by scalable, secure, and resilient infrastructure. Cloud platforms and service providers could also become a vector for traditional financial services and financial activities operating in a less centralized manner to interface and better integrate with each other.

Against this backdrop of opportunity, the core decentralized architecture and attributes of DeFi present some fundamental challenges for integration into today's operational and regulatory framework for financial services. Regulators and supervisors have invested in building capacity to study and understand the technologies and their application; however, beyond technological questions, more attention must be paid to the business model aspects before them. DeFi protocols and the new business models they support introduce tensions and challenges for integration, adoption, and compliance in traditional financial service frameworks where they disrupt current models and streams of revenue in ways that may or may not be appropriate. For all these reasons, now is the time to consider DeFi and the future of finance more closely.

This work outlines where we see challenges and solutions for the broader development and use of DeFi. In particular, we have shared where we see disconnects between current frameworks for finance and the fundamentals of DeFi. Three components of the paper explore DeFi with varying focal points and objectives.

- **Primer**: highlights the essentials of the DeFi stack, tokenization, connections with Web3.0, and the role of cloud.
- **DeFi Use Cases, Adoption, and Regulatory Considerations**: lays out challenges for DeFi adoption in the context of existing dominant structures in finance and current regulatory frameworks. It also considers some principles that could guide regulatory efforts. This section further takes stock of regulatory initiatives underway and highlights development in the Asia-Pacific region.
- **Deep Dive on Decentralization**: explores some core issues in DeFi development including business model tensions, smart contract transparency and agreement, and the blockchain trilemma (trade-off between decentralization, security, and scalability).

CONTENTS

PRIMER ON DEFI AND WEB 3.0

In this paper, we adopt a **working definition of DeFi** as encompassing **forms of finance** (either fiat- or crypto-denominated) **that make use of distributed ledger technology (DLT),** and which additionally are **significantly decentralized in terms of governance, custody, or otherwise**. This concept of DeFi envisions a world where individuals conduct all financial activities on blockchain, intermediated only by software and "smart" contracts designed to run automatically.

While many definitions exist, most in the DeFi space embrace the ethos of greater individual control and a higher degree of automation than is currently available within financial services to most participants. In a fully decentralized world, individuals conduct transactions between one another without intermediating institutions, but instead through a protocol. This vision, at its extreme, would be a massive disruption to the way financial activities are currently conducted and is unlikely to develop.

Several different definitions of decentralized finance are current in recent literature, but the common threads in recent writings are an emphasis on the technologies of DLT and smart contracts. For instance:

> *DeFi commonly refers to the provision of financial products, services, arrangements and activities that use [DLT] in an effort to disintermediate and decentralize legacy ecosystems by eliminating the need for some traditional financial intermediaries and centralized institutions. Currently, there is no generally accepted definition of "DeFi," or what makes a product, service, arrangement or activity "decentralized."* [1]

> *"DeFi" broadly refers to a variety of financial products, services, activities, and arrangements supported by smart contract-enabled [DLT]. This technology can reduce the use of traditional financial intermediaries and centralized institutions to perform certain functions, although the degree of decentralization across DeFi differs widely.*[2]

> *The cryptocurrency industry views "DeFi" as a term of art that refers more specifically to derivative contracts deployed on smart contract blockchains that facilitate asset swaps, programmatic leverage, and risk transformation.*[3]

[1] IOSCO (2022), IOSCO Decentralized Finance Report, March, cited in U.S. Treasury (2022), Crypto-Assets: Implications for Consumers, Investors, and Businesses, September.
[2] President's Working Group on Financial Markets (PWGFM), Federal Deposit Insurance Corporation (**FDIC**) and Office of the Comptroller of the Currency (**OCC**) (2022), Report on Stablecoins, November
[3] Carter, N. in Jeng, L. (ed.) (2022), *Open Banking*, OUP, April 26.

It is important to note that not all DLT is used for DeFi, an important distinction within the use cases discussed later.[4]

In this sense, DeFi is often contrasted on the one hand with traditional financial services (**TradFi**) and on the other hand with other centralized institutions "CeFi" providing services primarily pertaining to crypto-assets, or where various actors are identified under these three headings providing functions such as trading, lending and investing.[5] However, given the highly fluid ecosystem and rapidly increasing links between existing financial institutions (**FIs**) and the crypto financial system and disintermediated tools, we conceptualize a spectrum of more-or-less centralized finance (both crypto- and fiat-denominated), with institutions and protocols competing or cooperating in several spaces.

The OECD has discussed DeFi in terms of copying the existing financial structure onto a platform with a greater degree of individual authorship:

> *Decentralised Finance or 'DeFi' is an effort to replicate certain functions of the traditional financial system in an open, decentralized, permissionless and autonomous way, based on blockchains.*[6]

This is certainly true, and we would additionally leave open the possibility that the degree of individual control and authorship to transactions offered may create the opportunity for new products and services, beyond those already offered within the financial services universe.

In its 2019 study of the implications of DeFi, the Financial Stability Board (**FSB**) abstracted away from DLT, identifying three different dimensions on which decentralization was discernible. These dimensions are record keeping, risk taking, and governance.[7] In that study, peer-to-peer (**P2P**) lending platforms were seen as a kind of decentralized finance that disrupted centralized forms of credit intermediation.

While the FSB study is a useful reminder that DLT and crypto-assets are not the whole of DeFi, the fact is that the majority of the activity and most interesting developments – both positive and negative – in DeFi has been in the DLT and digital assets space. This is especially so given that the P2P lending boom of the mid-2010s in China and elsewhere slackened, including through regulatory pressures.[8]

The DeFi Stack

Crypto-assets are certainly part of DeFi, but crypto and DeFi are not interchangeable concepts. The role of crypto-assets in DeFi is as the asset layer in the "DeFi stack". The stack concept, articulated by Schär, among others, places crypto-assets as an integral part of DeFi, but does not limit DeFi to crypto. Four layers encompass the foundational stack of DeFi: the settlement layer, the asset layer, the protocol layer, and the application layer. Combinations of services built from

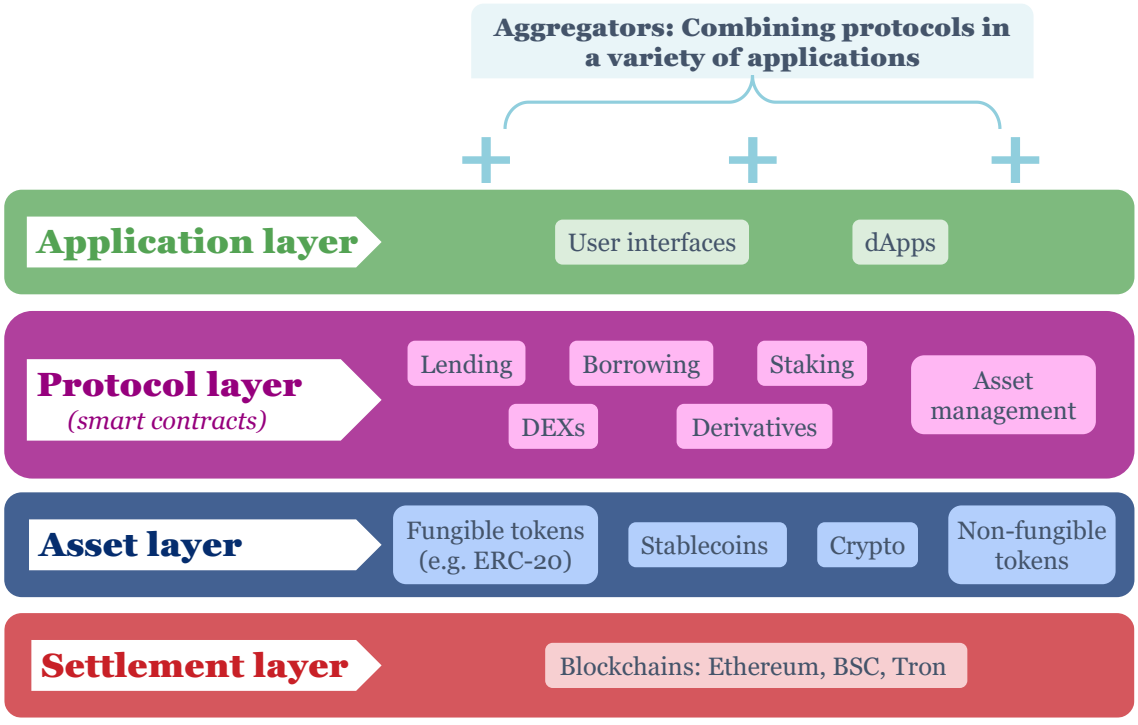
[4] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 11.
[5] E.g. Aramonte S. et al. (2021), DeFi risks and the decentralisation illusion, *BIS Quarterly Review*, December, Table 1, p. 23.
[6] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 3.
[7] FSB (2019), Decentralized Financial Technologies: Report on financial stability, regulatory and governance implications, June 6, p. 3.
[8] The global P2P lending market size was valued at US$ 83.79 billion in 2021. Source: https://www.precedenceresearch.com/peer-to-peer-lending-market, accessed November 2, 2022. See Cornelli, G. et al. (2020), Fintech and big tech credit: a new database, p. 7.

this complete stack can be combined in several ways on a fifth aggregation layer to provide a full suite of financial services owing to the composability of DeFi (see **Figure 1**).[9]

A core tool of DeFi protocols is the **smart contract**. It is the interaction of smart contracts that gives DeFi protocols their automaticity. Smart contracts could theoretically be used to encode greater Know Your Customer (**KYC**) or sanctions screening requirements into transaction logic, ensuring legal provisions are enforced. As many have pointed out, a smart contract is neither smart nor a contract at this stage.[10] Instead, it is a block of code (written in a specialized language such as Solidity) that executes transactions (including by interacting with other smart contracts, such as **oracles**, see **text box**) in predictable ways according to predetermined rules. These tools enable the automated nature of DeFi, executing transactions much faster than centralized intermediaries in some cases. Their labeling as "smart" could imply an element of sophisticated discretion, when in practice execution is binary based on whether or not a condition(s) is met.

> *Smart contracts critically depend on digital inputs that inform them whether their triggering conditions have occurred, typically provided by connected sensors that supply certified signals to the blockchain.*[11]

Figure 1: The DeFi stack



Source: IIF illustration, based on Schär 2021.

[9] Schär, F., (2021), Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, *Federal Reserve Bank of St. Louis Review*, Second Quarter, pp. 153-74.
[10] Netguru (2021), Neither Smart Nor Contracts: Smart Contracts Need a Rebrand, August 31.
[11] Bakos, Y. and Halaburda, H. (2021), Blockchains, Smart Contracts and Connected Sensors: Substitutes or Complements?, September 1, p. 1.

Oracles

The conditions that trigger certain actions in smart contracts can be signalled to these programs by "oracles". Oracles serve as data links and determine whether or not a protocol can execute a transaction. These specialized smart contracts run on a blockchain and interact with data sources or recipients in the "outside world" off the blockchain. Price feeds are one example of data source used in oracles. Another is the Chainalysis sanctions screening oracle, which verifies if a blockchain address is on a list of officially sanctioned addresses maintained by Chainalysis.[12] "Outbound" oracles can also send data to the outside world, e.g. to initiate a non-cryptocurrency payment, or to unlock a smart lock. Oracles can be compromised through so-called Sybil attacks, another source of risk to DeFi projects.

Governance tokens

DeFi protocols are often governed through governance tokens, which can be issued to promoters, core developers, VC backers or other insiders early in a project, but subsequently are also often issued to users as a reward for their participation. Depending on the protocol design, the minimum threshold in terms of ownership of tokens to have the right to propose a protocol change can be quite high and may make change challenging if needed. Once a change proposal has been voted, however, changes are normally executed automatically. Some protocols retain "admin keys" alongside governance tokens as a means for project controllers to exercise overall control over the protocol. These admin keys can be a source of cyber risk or insider fraud risk and are not generally considered consistent with the "decentralization ethos" of DeFi.

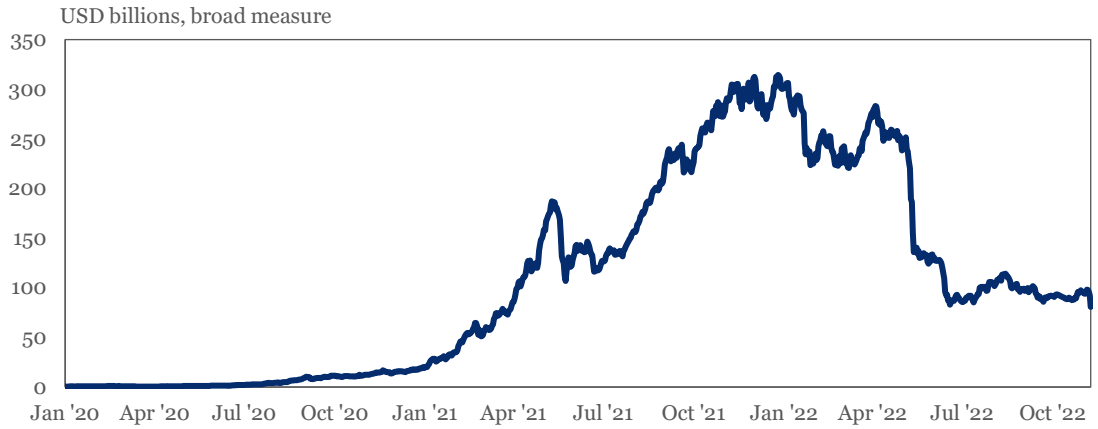
The Rise of DeFi

DeFi protocols and decentralized applications (**dApps**) grew very rapidly in 2021, before market events of 2022 chilled sentiment.

These are sizeable but volatile markets, and data sources vary considerably. Total value locked (**TVL**) is a measure of the assets deposited by users with each protocol, roughly equivalent to the liability (deposit) side of a bank's balance sheet. A broad measure of TVL across DeFi protocols, including governance tokens (see **text box**) staked in the protocol, and rewards/liquidity for staked assets, shows $80.8 billion of TVL as of November 9, down from an all-time high of $317.41 billion on December 27, 2021 and sharply down from totals at the start of November of around $95 billion (see **Chart 1**).

[12] See Chainalysis oracle for sanctions screening, accessed October 18, 2022.

Chart 1: Total Value Locked in DeFi protocols



Source: DeFi Llama, across blockchains. Data as of November 9, 2022.

How TVL is defined is important. There were on November 2, 2022 reported to be $54.67 billion in TVL on the narrowest measure, compared with $95.63 billion on the broad measure.[13] In the days after FTX's bankruptcy filing, as of November 14, these measures have declined further to $45.15 billion on the narrow measure and $75.04 billion on the broad.

TVL on the Ethereum blockchain specifically reached around $100 billion at end-2021, about four times as much as at end-2020, and much higher than the $35 billion raised by Initial Coin Offerings (ICOs) between 2016 to 2019.[14]

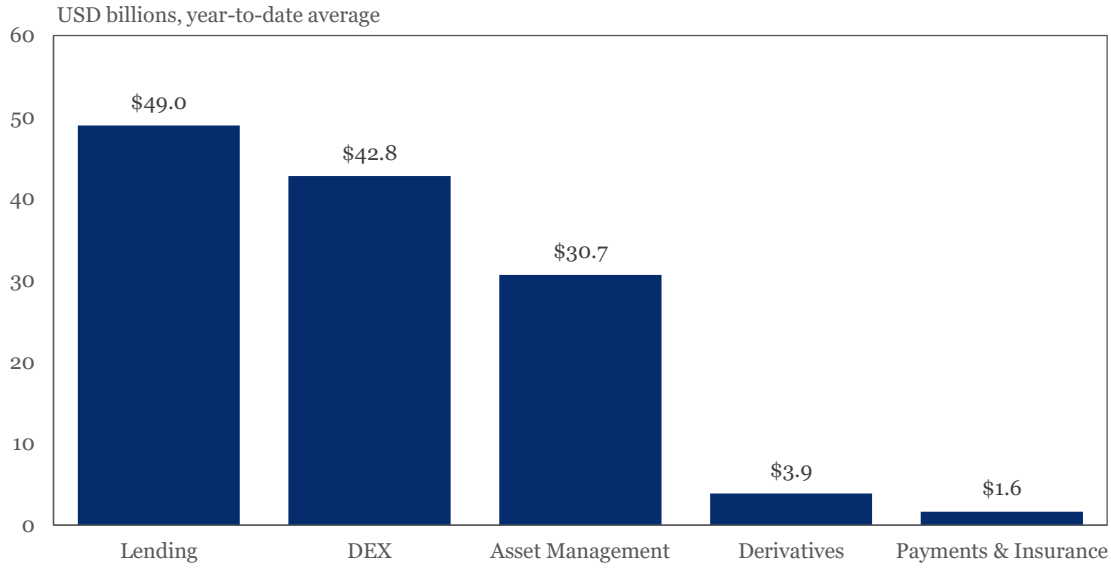
The top ten protocols by TVL as of November 9, 2022 were a broad mix of the various functions identified in **Chart 2**. They include: Aave, MakerDAO (associated with the Dai decentralized stablecoin), Lido and Hex (staking), Curve, PancakeSwap and Uniswap (automated market makers/decentralized exchanges (**DEXs**), and JustLend and Compound (DeFi lending and borrowing protocols).[15]

The data provider Defi Llama was tracking over 1950 DeFi protocols as of November 2, 2022, from over 130 different blockchains. There were 812 protocols listed that had reached $1 million in TVL, but only 17 with more than $1 billion TVL. DeFi has continued to expand in terms of the number of projects in recent months, even as total TVL has remained flat or declined.[16]

Aggregating across sectors, the dominant types of DeFi protocols are lending, DEXs and asset management, with derivatives and payments/insurance much smaller (see **Chart 2**).

[13] Source: DefiLlama - DeFi Dashboard, accessed November 15, 2022.
[14] FSB (2022a), Assessment of Risks to Financial Stability from Crypto-assets, February 16. Citing DeFi Pulse, see, "What is Total Value Locked in Decentralize Finance? | DEFIYIELD Official Blog" for an explanation of the difference between DeFi Llama and DeFi Pulse calculations of TVL.
[15] Source: DefiLlama - DeFi Dashboard. Ranking as of November 9, 2022.
[16] As of September 26, 2022, it was tracking around 1750 protocols, of which 670 had reached $1 million in TVL, and only 15 with more than $1 billion TVL.

Chart 2: Total value locked in DeFi protocols by contract type



Source: DeFi Llama; across blockchains, IIF aggregation. Data as of November 9, 2022.

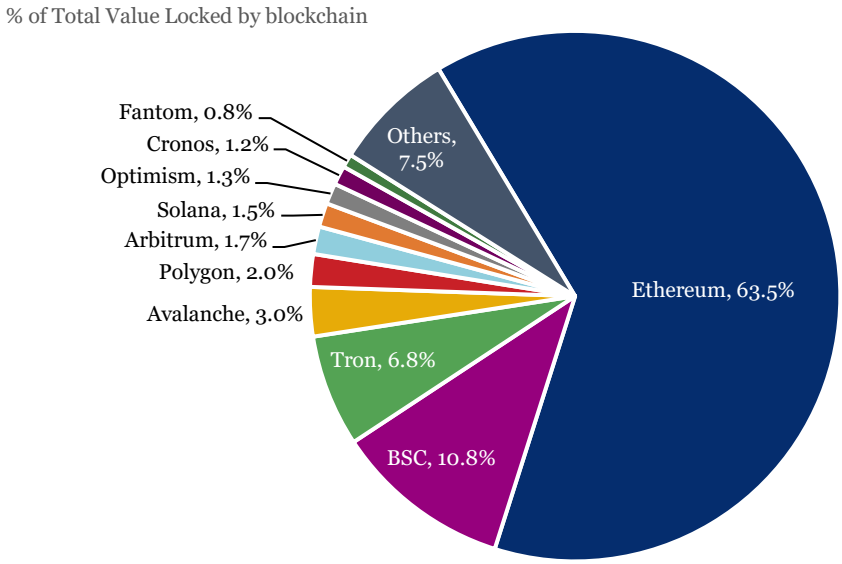
DeFi protocols and Web 3.0 protocols have become an important target of venture capital (**VC**) investment. Over $6 billion (early and seed stage) was invested in such projects over a twelve-month period up to March 31, 2022, of which just under $2 billion was invested in Q1 2022, not counting token sales. This sector was the top recipient of VC investment over this period, well ahead of sectors such as bio- and fintech.[17]

A few DeFi protocols have begun to rival, and in some cases overtake, their CeFi counterparts in measures of market size, although DeFi remains a small part of the overall digital assets market. For example, trading volumes on the DEX Uniswap have at times exceeded or rivalled those of leading centralized exchanges Binance and Coinbase,[18] while the decentralized Dai is the fourth-largest stablecoin by market capitalization and by trading volume, after the centralized stablecoins Tether (USDT), USD Coin (USDC), and Binance USD (BUSD).[19] For context, the New York Stock Exchange recorded total annual spot trading volume around 4.3 times that of Binance, for the year ended July 2022,[20] and the total trading volume in DeFi tokens is around 5% of the total crypto market 24-hour volume.[21] By some reports, Dai has achieved a fidelity to its USD soft peg target in recent months that is comparable to USDT, but lower than USDC.[22]

The Ethereum blockchain is by no means the only blockchain hosting DeFi projects, but it remains the dominant one, and thus the dominant settlement layer (see **Chart 3**). It recently underwent an important change in consensus mechanism (see **text box** on The Merge).

[17] PitchBook (2022), Emerging Tech Indicator, cited in: TaylorWessing (2022), Venture Capital Trends: Web 3.0, DeFi, Metaverse and Tokens, July 18.
[18] Aramonte, S. et al. (2021), DeFi risks and the decentralisation illusion, *BIS Quarterly Review*, December, p. 26, citing Graph 2, left-hand panel.
[19] Coinmarketcap.com, accessed on November 2, 2022.
[20] European Securities Markets Authority (ESMA) (2022), Crypto-assets and their risks for financial stability, October 4, p. 5.
[21] Coinmarketcap.com, accessed on November 2, 2022.
[22] In May and June 2022, DAI was within 0.005 cents of its $1 soft peg 99.80% of hours. This figure is the same as that cited for USDT for the longer period January 2021 – June 2022, and lower than the 99.86% figure cited for USDC for the same longer period. See Coinbase Institute (2022), Stablecoins: Coinbase White Paper, July, p. 12, 14.

Chart 3: Ethereum is the dominant settlement layer



Source: DeFi Llama. Data as of November 9, 2022.

Indicators of interconnectedness between DeFi and existing financial intermediaries have increased over time. Quantitative evidence suggests that large institutional investors have been active in the DeFi market; large-sized transactions, used as a proxy for institutional investor participation, represented the largest share of DeFi activity during most of 2021.[23] Despite these indicators of growth, it is again important to note that DeFi activity remains small relative to the much bigger crypto-assets market, which in turn is dwarfed by the size of the overall financial system.[24]

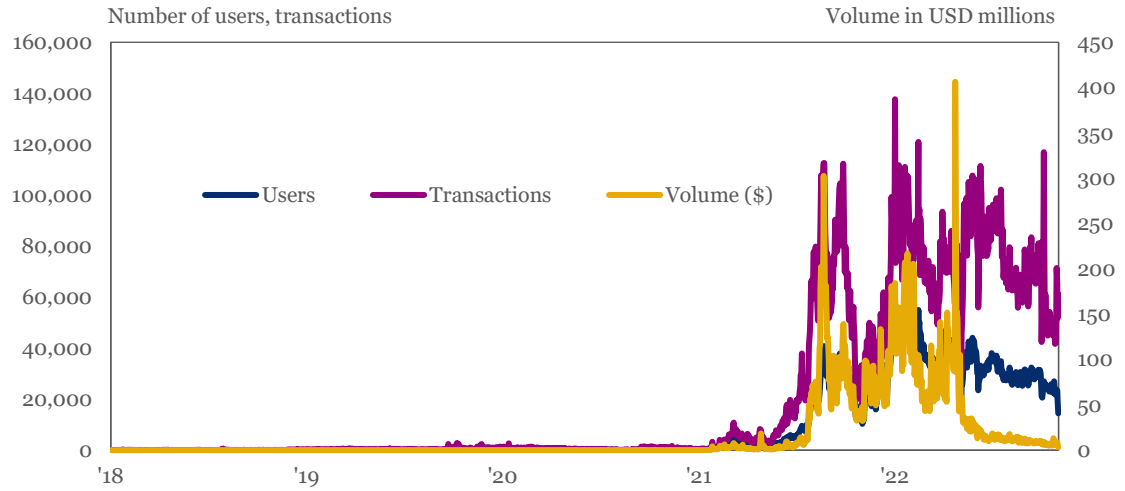
Tokenization and NFTs

Tokenized assets are a virtual representation of the store of and transacting unit of value in a digital system. These can represent any asset ranging from cryptocurrency to tokenized bank deposits. In a DeFi system, once assets are tokenized and secured, the tokens can then be traded and transacted on-chain by the automated protocols. Currently, most DeFi systems focus on crypto-assets, but tokenized bonds, derivatives, real estate, vehicles, and receivables could be traded and transacted in DeFi systems as well.

Non-fungible tokens (**NFTs**) are one phenomenon connected with DeFi that experienced explosive growth in 2021 and garnered much of the popular perception of tokenization. NFTs remain active, albeit with much lower volumes than in 2021 (see **Chart 4**).

[23] OECD (2022b), Institutionalisation of crypto-assets and DeFi - TradFi Interconnectedness, May 19, p. 17, citing figure 1.6.
[24] Bank of England (2022), Financial stability in focus - Cryptoassets and decentralised finance, March 26, p. 7, citing Chart 2. As at 2 March 2022, the crypto-assets universe comprised 0.4% the total size of the global financial system.

Chart 4: NFT Users, Volumes, and Transactions



Source: OpenSea. Data as of November 10, 2022.

A feature of NFTs is their ability to engineer theoretically unlimited and transferable fractional ownership of securities, derivatives, and real-world assets such as land, vehicles, and collectibles through a process known as "tokenization". Fractionalization does not require tokenization, however, and is frequently incorrectly used in discussion interchangeably.

Beyond digital art and collectibles such as the well-known Bored Ape Yacht Club and CryptoPunks series, NFTs are also increasingly integrated into gaming platforms. Recently, a new generation of gaming platforms has sought to adopt a "play-to-earn" business model. The blockchain-based game Axie Infinity, a Pokémon-like gaming universe, requires an up-front investment of ~$1,000, but rewards players with an Ethereum-based in-game token that can be spent on NFTs of virtual assets, or exchanged for fiat currency. Other examples of play-to-earn gaming platforms include The Sandbox, Gods Unchained, Splinterlands, and Pegaxy.[25]

Cloud and DeFi

Cloud As an Enabler of Web 3.0 and Defi Projects

In previous publications, we have emphasized the role of cloud computing as a vital enabler of digital transformation for financial services, as well as a key source of operational resilience, including during the pandemic.[26] In line with this, public cloud is an enabler of DeFi and Web 3.0 in a number of ways.

Most if not all sizeable DeFi projects are powered by cloud, due to cloud being in many cases a cheaper and/or more capable option for enterprise data storage and compute relative to alternatives such as private cloud and on-premises data centers. Cloud can help FIs and fintechs,

[25] Pay to Earn, https://www.playtoearn.online/games/, accessed September 26, 2022.
[26] See e.g. IIF (2018), Cloud Computing in the Financial Sector Part 1: An Essential Enabler, August; IIF (2020), Cloud Computing: A Vital Enabler in Times of Disruption, June; and IIF – Deloitte (2021), Realizing the Digital Promise: Call to Action, October.

including DeFi projects, address cybersecurity, single point of failure, load management, and data engineering challenges that may be beyond the capacity of any one institution.

Additionally, the cross-border nature of cloud means it is a natural fit for DeFi protocols and applications with global reach. For example, the Truffle suite of products (Truffle, Ganache and Drizzle), are made available to clients through means including AWS Cloud9.[27] As another example, Kaleido is an enterprise-grade platform for deploying blockchain and digital asset solutions, and is capable of running on AWS, Azure and hybrid private cloud solutions.[28]

The vulnerability of open-source code to bugs and also to deliberate exploitation by bad actors (e.g. through insertion of malign code in the codebase) has become a focus for DeFi project developers to ensure that risks of fraud and other 'exploits' with regard to client assets is minimized. The market is starting to provide a range of tools to manage or minimize this risk, including automated code auditing and review tools. Consensys, for example, provides tools such as MythX API, which scans for security vulnerabilities in Ethereum and other EVM-based blockchain smart contracts.[29] Such tools are often deployed over cloud infrastructure.

As well as powering DeFi projects, most of which are cloud-native, many nodes in decentralized protocols are also powered by cloud, including in Proof of Stake (**POS**) protocols such as Tron, Avalanche, Solana and, since The Merge, Ethereum.

According to the data provider ethernodes.org, 67.5% of Ethereum nodes by Network Type are Hosted, versus 30.6% Residential and 1.4% Business. Of Hosted nodes, around 63% are hosted by Amazon.com and 9.3% by Google Cloud (see **Chart 5**).[30]

Decentralization of Cloud

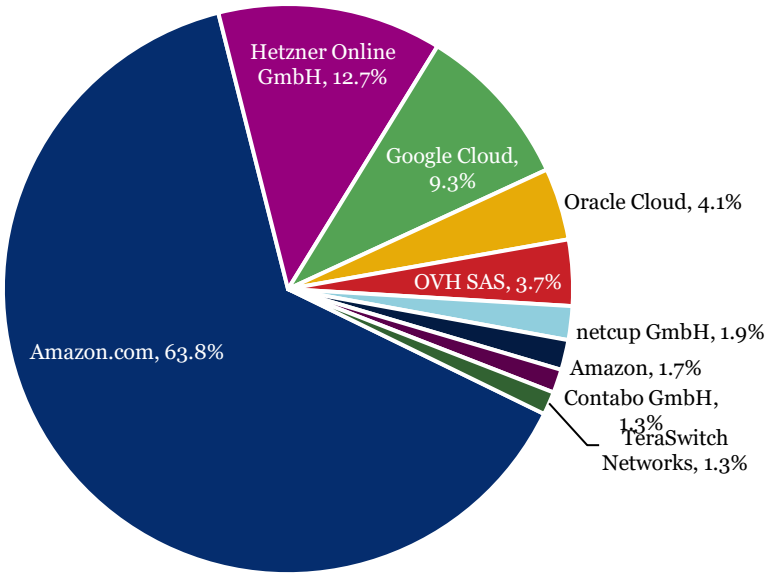
On the other side of the coin, decentralized cloud providers such as Akash Network and InterPlanetary File System are seeking to disrupt utility cloud providers, by allowing users to sell their unused computing capacity and bandwidth and to deploy their apps (including dApps) on this distributed cloud infrastructure.

Overall, however, while decentralized cloud computing may seek to disrupt public cloud utilities, DeFi appears to be a large demand driver for public cloud services. It seems unlikely that FIs would be willing to entrust their, and their customers', business-critical data to permissionless cloud networks operated by pseudonymous actors, even if encrypted while in storage or transmission and obfuscated for processing.

In some jurisdictions, such as the EU and the UK, there are moves toward direct regulation of critical service providers to FIs, including some cloud providers. Any move at scale towards reliance on decentralized cloud providers by FIs might present supervisors with the same family of challenges as are presented to them directly by DeFi actors.

[27] AWS (2020), Truffle: Build and Deploy Ethereum Smart Contracts with Truffle and AWS Cloud9 (video), March 21.
[28] Kaleido: Enterprise-Grade Blockchain & Digital Asset Platform, accessed September 28, 2022.
[29] Smart Contract Audits | ConsenSys Diligence, accessed September 28, 2022.
[30] Data as at September 27, 2022.

Chart 5: Providers of hosted Ethereum nodes



Source: ethernodes.org. Data as of November 8, 2022.

DeFi – Crypto Interdependence and the Impact of Market Conditions

The broader context for DeFi activity remains the market for crypto-assets more generally. Crypto-assets (especially stablecoins pegged to fiat currencies) provide the collateral that typically powers DeFi protocols, which users stake or deploy to earn yield or trade for other crypto-assets through dApps, although some uncollateralized lending takes place. The recent **"Crypto Winter"** saw the overall market capitalization for all crypto-assets peak at $2.937 trillion on November 9, 2021, and plunge to around $1 trillion in May, where it remained until early November before dropping to under $900 billion.[31] High-profile collapses among CeFi crypto projects, most notably the stablecoin Terra, the crypto-lenders Celsius Networks and Voyager Digital, and the crypto investment fund Three Arrows Capital, as well as factors external to crypto-assets such as macroeconomic conditions and monetary policy, combined to severely affect valuations in the space in mid-2022, while the bankruptcy of FTX in early November has contributed to a further drop of asset values across the sector. That the DeFi and broader crypto ecosystem is highly interconnected has been shown upon examination of these collapses.

The return to more normal interest rate settings has increased the cost of capital across the economy. The search for yield during the time of low interest rates led many investors to seek returns that were "too good to be true". Returns were financed by new entrants – less informed investors were buying while insiders were selling.[32] Liability and maturity mismatches

[31] Coinmarketcap.com, accessed November 2, 2022.
[32] See Auer, R. et al., Crypto trading and Bitcoin prices: evidence from a new database of retail adoption, *BIS Working Papers No.* 1049, November.

characterize some of these failures, including failing to mark exposures denominated in ETH to market.[33]

However, while there are implications for the DeFi landscape from forthcoming stablecoin regulation, it is notable that Terra itself was not a decentralized protocol in the strict sense.[34] The failed projects were all quite centralized, though they also had exposure to DeFi protocols. Thus, DeFi projects may be closely affected by regulation driven by the failures of more centralized crypto projects.

Many of the reasons we have seen recent projects fail are owed to mismanagement of well-known risks that are familiar to regulators and traditional financial institutions – credit risk, liquidity risk, maturity mismatches, excessive leverage, large exposures, and the prohibition of comingling of certain funds. These are not novel risks. The crypto-asset industry today, as well as investment in DeFi projects, generally lacks sufficient familiarity and expertise in managing these kinds of well-trodden risks in financial services, starting with the requisite understanding that these fundamentals are quite critical. Technology does not negate basic market economics, though it can allow known risks to present in new ways. Over time, for these projects to be successful, a risk management culture more akin to that of the broader financial services industry must be integrated into the entrepreneurial culture laid by technical developers that has driven advances in this space to-date.

Web 3.0

Defining a Developing Concept: What Is Web 3.0?

Web 3.0 is often contrasted to Web 1.0, the early form of the World Wide Web, where most users were passive consumers of content, and Web 2.0, where most users are also content creators in an ecosystem dominated by social media and other platforms employing a data monetization or advertising-driven model. According to its proponents, in Web 3.0, users will have more control over the content they create and be rewarded, not just through free access to social media services, but more directly through tokens and other services that are more-or-less financial in nature.

For some, Web 3.0 denotes the enablement of a set of technologies that include virtual reality and augmented reality (**VR/AR**). For many others, the key points are the idea of persistent identity in logical spaces, and the idea of portability of identities and attributes (including but not limited to digital goods such as virtual clothing or avatar "skins").

There are links between DeFi and Web 3.0. One link is to be found in the idea of NFTs as rivalrous digital goods, instantiated on one or more blockchains. NFTs that would represent verifiable identities or credentials would be one example of a Web 3.0 enabler; those that represent virtual or digital goods such as skins for virtual selves or avatars might be another. Web 3.0 can even be thought of as a hypothetical future interface between the internet and people, built on DLT with support from cloud services. This space is in very early stages of development.

---

[33] See Summons in the lawsuit *KeyFi, Inc. v. Celsius Network Limited And Celsius Keyfi LLC*, at paragraph 82. These are untested allegations only.

[34] It was heavily dependent on its founder, Do Kwon, and the Luna Foundation Guard, a non-profit foundation intended to act as a backstop to the peg: see Analytic Insight (2022), Terra was Never a Decentralized Platform, Thanks to Do Kwon's Luna Wealth, June 17.

Web 3.0 and the Metaverse – Not one and the same

The idea of Web 3.0 is also linked to the idea of the so-called "Metaverse". The term Metaverse refers to the open, persistent, real-time, interoperable, virtual world that could be built using Web 3.0 technologies, including blockchain technology, smart contracts, cryptocurrencies and NFTs, that could in turn provide the payments and legal infrastructure needed to complement VR/AR.[35]

Research by Citi discusses the possibility that the Metaverse is moving towards becoming the next iteration of the internet. This "Open Metaverse" would be community-owned, community-governed, and a freely interoperable version that ensures privacy by design. Users would increasingly be able to access a host of use cases, including commerce, art, media, advertising, healthcare, and social collaboration. According to Citi,

> *A device-agnostic Metaverse would be accessible via personal computers, game consoles, and smartphones, resulting in a large ecosystem. Using this broad definition, the total addressable market for the Metaverse could be between $8 trillion and $13 trillion by 2030, with total Metaverse users numbering around five billion.*[36]

In a similar vein, a preliminary estimate by McKinsey & Co. is that,

> *…[w]hile estimates of the potential economic value of the Metaverse vary widely, our bottom-up view of consumer and enterprise use cases suggests it may generate up to $5 trillion in impact by 2030.*[37]

McKinsey & Co. also reported that corporations, venture capital, and private equity had invested more than $120 billion in the Metaverse in the first five months of 2022, more than double the $57 billion invested in all of 2021, a large part of it driven by Microsoft's planned acquisition of Activision Blizzard Inc. for $69 billion.

To the extent the Metaverse invokes use cases beyond finance, it is out of scope of this report.

Smart Web 2.5?

Views on the relationship between DeFi and Web 3.0 among DeFi enthusiasts tend to fall into three categories: 1) DeFi must be achieved before we can move to Web 3.0; 2) DeFi and Web 3.0 are nearly interchangeable terms for an idealized future model of interactions between people and online existence; 3) DeFi represents the financial system of Web 3.0, and both will evolve simultaneously. These enthusiasts agree that DeFi tools will play an important role in moving the world forward into the next stage of the internet.

All of these views proceed on the assumption that Web 3.0 and DLT are necessarily linked. If DLT represents the financial system layer of the world that Web 3.0 aims to create, the infrastructure of DeFi – blockchains, distributed computing power and record keeping, and instantaneous settlement – will become increasingly integrated into every transaction conducted within Web

[35] Gilbert, S. (2022), Crypto, web3, and the Metaverse, University of Cambridge Bennet Institute for Public Policy, March, p. 5.
[36] Citibank (2022), Metaverse and Money - CitiGPS (citivelocity.com), March, p. 3.
[37] McKinsey & Company (2022), Value creation in the Metaverse, June, p. 6.

3.0. However, it remains an open question whether Web 3.0 is necessarily linked with DLT, as other computing paradigms are possible that may have the same or similar economics.

While both DeFi and Web 3.0 promote decentralization, Web 3.0 aims broadly at every facet of interaction, not simply financial transactions. DeFi may moreover gain prominence without the world moving to Web 3.0, but the reverse may not be true. Within this ecosystem, developments that promote DeFi adoption will positively affect Web 3.0 development and vice versa. The future of the financial system will undoubtedly maintain significant degrees of centralization even with the integration of DeFi protocols, and thus a proverbial Web 2.5 may be a more likely outcome.

Financial Services in the Next Stage of the Internet

As we consider the ways automation will shape finance, we will continue to investigate the development of Web 3.0. We see cloud and DeFi as enablers for a future transition to the next phase of the internet, however the construct. Financial institutions will no doubt play an important role in the success of any such transition, including via the provision of capital or liquidity, the processing of transactions at some point in a value chain, and by designing and developing financial services to suit the new environment. This will require regulatory acceptance and technical capabilities, or partnerships with those who have them. It is also worth noting that while automated transactions are a key element of DeFi, the smart contract system that enables them today lacks the nuance and complexity of the real world, prompting further questions.

Data Sovereignty, Sharing, and the Limits of Openness

DeFi and Web 3.0 integration raises the question of limits on self-sovereign and self-managed digital identity. In a purist version of Web 3.0, a high degree of individual control over data would enable data to flow across borders seamlessly if the data subject so desired. Increasingly, nation states, including in the Asia-Pacific region, have adopted restrictions on the free movement of data (including payments data) offshore, and/or have insisted on a local copy being stored onshore, often in the name of data sovereignty, but also for other cited reasons. The IIF has tackled this issue in a number of publications, arguing that such restrictions can limit the value of data and reduce the effectiveness of risk management and anti-fraud systems.[38]

In the theoretical world of Web 3.0, where individuals have full control and ownership over their data, one would naturally see data flow across borders seamlessly with consent. If governments are unwilling to remove restrictions on sharing of data regardless of consumer consent, this will lead to a fragmented vision of Web 3.0, just as Web 2.0 is challenged by data localization requirements in several distinct jurisdictions today. Relatedly, self-sovereign identity in extreme forms may be inconsistent with a government's prerogative to be the granter of sovereign forms of identity. The answer here appears to lie in acceptance by governments and data subjects of both the sovereign's right to issue sovereign identity, and the data subject's right to tokenize that identity claim on blockchains for re-use in the Web 3.0 environment, at least assuming governments do not natively issue tokenized verifiable credentials in their own right. There is an interesting parallel with the debate on the proper role of CBDCs and tokenized deposits in the digital assets realm.

[38] See IIF (2022), Strategic Framework for Digital Economic Cooperation - A Path for Progress, April 19 and related content available through that landing page.

DEFI USE CASES, ADOPTION, AND REGULATORY CONSIDERATIONS

The DeFi and Web 3.0 landscape is taking shape, and now is an opportune moment to explore how these technologies could generate value for financial clients and for the institutions that serve or interact with them. Use cases provide a lens to consider that question as well as a framework to identify challenges for DeFi, including around identity and the user experience, as well as some persistent questions around the stability, security, and scalability of DeFi.

In examining these areas, we take stock of the regulatory initiatives globally that seek to identify and tackle the risks and challenges arising from broader crypto-asset developments. Many of the regulatory principles discussed will also apply to the emerging DeFi and Web 3.0 space, to which regulators have yet to devote significant attention, although this is changing.

Our investigation of DeFi reveals potential for genuine long-term added value to consumers and investors through faster and more automated transactions. However, these services in many respects complement or augment – rather than replace – financial intermediaries, or reintroduce centralization in other ways. Indeed, the degree of disintermediation remains a judgement call at the protocol level across the use cases and in response to the challenges discussed in this section.

It is insufficient to simply attribute value to a DeFi protocol because it executes a financial service on a blockchain rather than using another technology. Choice of technology alone is not enough to deliver value. In many cases, engineers are attempting to address problems traditional finance solved decades, or centuries ago. A nuanced consideration of why certain use cases have gained traction and what challenges DeFi presents is needed, along with consideration of possible solutions for those challenges.

The role of public cloud as an enabler of DeFi and Web 3.0 technologies is an important consideration as it may help to address some technical, data, and security challenges raised, and may drive some standards and convergence.

Use Cases

The term "DeFi" has been applied to the provision of a variety of services and products. Offerings claiming to be DeFi span multiple categories of services, such as: payments, infrastructure, custodial services, exchanges and liquidity, investing, KYC and identity, derivatives, marketplaces, stablecoins, prediction markets, insurance, credit and liquidity.[39] To understand this space, it is key to separate genuine use cases from marketing hype, and even more important to understand that DeFi is not defined by any one use case or execution of activities. It is the execution of any number of financial services in a more decentralized manner, facilitated by technology, than those activities are otherwise currently being executed – so the question is, when is this helpful?

Protocols currently available to users cover a variety of traditional financial services that have been made more transparent or faster than their centralized counterparts, automated through the

[39] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 16, figure 2.1.

use of smart contracts, or distributed across a wider set of participants through tokenization. Within each of these categories, discussed in further detail by type of service below, the most active DeFi projects are focused on crypto-assets trading, lending, and staking.[40]

Payments represents a broad category of active DeFi protocols. The speed, verifiability, and instantaneous and **atomic** settlement make DeFi protocols good candidates for more efficient payments in a person-to-person setting, for example in cross-border transactions and remittances. Permissionless ledgers and the speed at which money can be transferred, plus the peer-to-peer ethos of decentralized payments, are attractive to consumers, although high and unpredictable fees (such as "gas fees" for transactions written on the Ethereum blockchain) can limit the appeal of this use case, particularly for smaller payments. In addition, mitigation of certain risks likely require some degree of centralized intermediary, particularly anti-money laundering, or more advanced technologies than have been brought to bear as of yet.

It is notable that the 4th-largest **stablecoin** by market capitalization is the Dai, a decentralized, crypto-collateralized token pegged to the U.S. dollar and issued by Maker DAO.[41] Stablecoins can be a payment instrument but can also facilitate crypto-asset staking and lending. DeFi actors have pioneered several types of **lending and staking products** within the cryptocurrency ecosystem. Protocols that combine the transparency of on-chain transactions with speed and execution of smart contracts have rapidly gained popularity, especially around staking or short-term lending. So far, these have been limited to crypto lending. The very high yields offered in the recent past may have been largely financed by new entrants to the market and hence be unsustainable. The popularity of these protocols may rise further as access is widened through the development of fiat-backed digitally native tokens, such as stablecoins. For these tokens to support more mature DeFi operations, a high degree of confidence in stablecoin regulation, as well as interoperability and acceptance across borders, will be required.

Further into quasi-financial services, the verifiability and speed of blockchain protocols open several further Web 3 application possibilities. While at present DeFi **trading** platforms or DEXs predominantly offer trading in crypto-asset pairs, the most active DeFi wallet providers are also able to connect to Metaverse properties and/or NFT collections. Such collections can represent financial assets such as securities, bonds and derivatives, and quasi-financial assets such as ESG credits or usage rights such as fishing quotas, mining leases, and carbon credits. As such, DeFi exchanges may go beyond trading of crypto-assets to replicate trading of securities, derivatives and similar tradable assets if appropriate regulation can be determined.

Tokenization of assets not traditionally present in liquid and tradeable formats is a promising, but still emerging area, of DeFi.[42] Perhaps the most compelling use case for DeFi would be the "**smart mortgage**" or "smart secured loan", where a tokenized form of real estate or motor vehicle (or a SME's business assets, including receivables) could be pledged in exchange for an automatically approved loan – denominated in crypto or in fiat currency via a stablecoin. Protocols promising fractional ownership of real assets, such as real estate with RealT, or mining rights as proposed by the Central African Republic, which could be traded on a liquid market or held in an individual's pension account, have also been discussed in recent years.[43]

---

[40] See Chart 1: Total Value Locked - All Chains.
[41] Top Stablecoin Tokens by Market Capitalization | CoinMarketCap, accessed November 1, 2022.
[42] OECD (2020), The Tokenisation of Assets and Potential Implications for Financial Markets, January 17, p. 33.
[43] Dentons (2022), The Tokenization of Real Estate: An introduction to fractional real estate investment, September 26; Cointelegraph (2022), How Does Tokenization Help Transform Illiquid Real Estate Ownership into a Liquid One, September 15; Ledger Insights (2022), Central African Republic Wants to Tokenize Mineral Resources, June 3.

It should be noted that tokens do not automatically confer ownership rights.[44] Ownership of real assets, particularly real estate, is legally complex; most land registries (many of which have "golden copy" status) do not currently support transfers of ownership rights via DLT-based settlement systems, nor does tokenization of a share of the underlying real asset in general entitle fractional ownership to be registered.[45] Tokenizing real world assets also seems likely to involve some degree of centralization, as a bridge between the offline physical world and the digital trading platform on which these tokens are traded will likely be needed so that there is some verification that the assets being tokenized have the attributes the tokenizer purports. While this hurdle does not seem insurmountable in countries with established property assessing and land title frameworks, many countries do not maintain robust and enforced land titles due to limits on state capacity or political issues around land ownership.[46]

Challenges to moving real assets such as land and motor vehicles into tokenized form present a high bar, given that in many markets real asset ownership record-keeping is still predominantly on paper and ownership recorded in DeFi protocols may not be recognized in law, or be recognized only indirectly (such as through corporate share ownership). Value-added services to these markets from within the DeFi space could be developed with more transparent ownership records, official sector participation, and clarity on roles of verifiers and record-keepers. We explore this further in the Enablers section.

It is as yet unclear which of the use cases discussed above will be truly net additive for customers, but interest and adoption have been growing and the occurrence of a "crypto winter" has not halted this exploration.

The technology that underpins DeFi – automated settlement and blockchains – has high utility beyond the investment vehicles discussed above. Several areas of finance have been applying these tools to aspects of their centralized businesses now for years and have already invested in automating their processes in a way that is compliant with local legal requirements. Yet, many are still investigating whether DeFi protocols can offer even greater efficiencies and cost savings. For example, **clearing and settlement** of securities and derivatives is an area of active and promising experimentation (see the examples in the **text box** on page 30).[47] However, the cost of switching to a DeFi-style protocol over an already largely automated process may outweigh potential savings. Additionally, the amortizing period may be long, particularly where firms have high local compliance obligations. Applying DeFi tools to routine or simple transactions that are not presently automated promises to quickly unlock efficiency gains, and thus cost savings. Applications of this type include private equity and SME financing, where current processes are highly manual.[48]

The possibility of using DeFi protocols to underpin central bank digital currencies (**CBDCs**) and their transactions is starting to be investigated by the official sector. The Bank for International Settlements Innovation Hub (**BIS-IH**) recently announced Project Mariana, which explores automated market makers (AMM) for the cross-border exchange of hypothetical Swiss franc, euro and Singapore dollar wholesale CBDCs. Project Mariana uses DeFi protocols to automate FX markets and settlement, potentially improving cross-border payments (a G-20 priority). The aim

[44] OECD (2020), The Tokenisation of Assets and Potential Implications for Financial Markets, January 17, p. 51.
[45] OECD (2020), The Tokenisation of Assets and Potential Implications for Financial Markets, January 17, p. 51.
[46] Tuck, L. and Zakout, W. (2019), "7 reasons for land and property rights to be at the top of the global agenda," World Bank, March 25.
[47] See also the Australian Stock Exchange (ASX) project to replace the existing Clearing House Electronic Subregister System (CHESS) with a DLT-enabled solution.
[48] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 43.

is to deliver a proof of concept by mid-2023.[49] Separately, the Federal Reserve Bank of Boston and the Massachusetts Institute of Technology's Digital Currency Initiative is collaborating on exploratory research known as Project Hamilton, a multiyear research project to explore the CBDC design space and gain a hands-on understanding of a CBDC's technical challenges and opportunities. Phase 2 of Project Hamilton will explore new functionality and alternative technical designs. Research topics may include programmability and smart contracts, among other topics. [50]

DeFi in Context – Asia-Pacific

APAC is the world's rapidly growing wealth management region. Assets under management in the region are estimated to outgrow any other region globally, and almost double from $15.1 trillion in 2017 to $29.6 trillion in 2025.[51] The region is also home to several large and relatively youthful populations such as India, Indonesia, Philippines and Myanmar, as well as of course to the demographic giant of China and the world's 3rd-largest economy of Japan and hosts many digital-first and mobile-enabled platforms including Ant Financial, Tencent, and Gojek.

Some Asian investors appear more crypto-assets positive than others and may be more inclined to experiment in DeFi protocols. In Asia, fully 100% of financial advisers answering a 2021 survey reported investing in digital assets, compared with 41% in the U.S. In Asia and Europe, well over 80% of high-net-worth individuals invested in digital assets, while the comparable figure in the U.S. was 15%.[52] Whether these differences arise from differences in overall risk appetite or from availability of better yields in more traditional markets is not revealed (see **Chart 6**).

Some prominent DeFi projects are housed in the APAC region, including: Synthetix, a derivatives DEX based in Sydney; Algorand Foundation, a blockchain organization based in Singapore; and Vietnamese game studio Sky Mavis, developer of Axie Infinity, an NFT-based gaming platform, and of Ronin Network, an Ethereum-lined sidechain. An estimated 25% of Filipinos and 23% of Vietnamese citizens have played a play-to-earn game, and at one point, players based in The Philippines made up 40% of Axie Infinity's player base,[53] where some rely on it as their main source of income.[54]

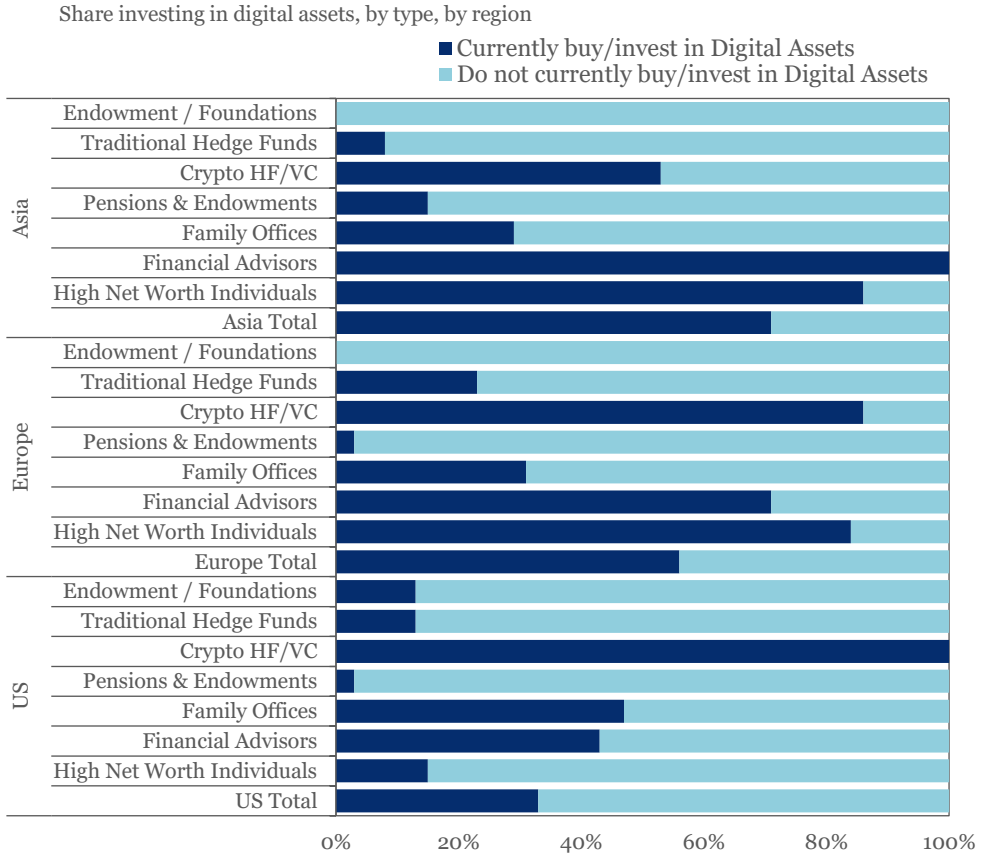
Regulators in region have taken a range of approaches to crypto-assets regulation and DeFi, though few have made bold regulatory moves (other than **China** which has banned cryptocurrency activities including mining, most recently in May and September 2021).[55] There has been an increasing intensity of activity, informed by, but not waiting upon, global standard-setting bodies' (**SSBs'**) policy work. The emphasis has been on protecting retail customers; typically, this activity has prioritized stablecoins as a key issue, perhaps in light of the $40 billion

[49] BIS-IH (2022), BIS and central banks of France, Singapore and Switzerland to explore cross-border CBDC trading and settlement using DeFi protocols, Press release, November 2.
[50] Boston Fed and MIT DCI (2022), Project Hamilton Phase 1: A High Performance Payment Processing System Designed for Central Bank Digital Currencies, February 3.
[51] PwC (2019), Asset & Wealth Management 2025: The Asian Awakening, January.
[52] OECD (2022b), Institutionalisation of crypto-assets and DeFi - TradFi Interconnectedness, May 19, p. 15, figure 1.3. Based on a survey of 1,100 respondents by Fidelity conducted in 2021.
[53] Chainalysis (2022), Geography of Cryptocurrency, October, p. 60.
[54] Gilbert, S. (2022), Crypto, web3, and the Metaverse, University of Cambridge Bennet Institute for Public Policy, March, p. 9.
[55] Chainalysis recently reported that, while the Chinese government started by banning mining in May 2021, and by September 2021 moved further to ban all cryptocurrency transaction activity, China remains the biggest cryptocurrency market in the region. See Chainalysis (2022), Geography of Cryptocurrency, October, p. 61.

collapse of the Terra stablecoin in May 2022. There has also been a focus on gatekeepers such as exchanges and custodians.

In **Japan,** the Diet was among the first parliaments globally to pass a specific law regulating stablecoin issuance following its early work on regulation of crypto-asset exchanges. The law will define stablecoins as digital currencies, impose a mandatory link with the yen and enshrine the right to redeem them at face value. The Monetary Authority of **Singapore** (**MAS**) released detailed regulatory proposals on stablecoins and crypto-assets in October, including detailed asset reserve and custody requirements for stablecoins that would be identified as "MAS-regulated".[56] In **Hong Kong SAR**, the authorities have signalled the introduction of a new regime around crypto-assets and stablecoins by "no later than 2023/24" in their January discussion paper, and announced a further series of broadly liberalizing regulatory moves in November.[57] As yet, regional regulators, in line with their peers internationally, have not specifically legislated on the topic of DeFi.

Chart 6: Global investor interest in digital assets



Source: OECD (2022b), based on a survey of 1,100 respondents by Fidelity. Data as of 2021.

[56] MAS (2022), Consultation Paper on Proposed Regulatory Approach for Stablecoin-Related Activities and Consultation Paper on Proposed Regulatory Measures for Digital Payment Token Services, October.
[57] Herbert Smith Freehills (2022), Retail access for virtual assets – risky business or radical open-mindedness?, November.

Challenges to Broader Adoption of DeFi for Consumer and Wholesale Finance

There are some fundamental architectural challenges to broader adoption of DeFi for consumer and wholesale finance that need to be squarely faced and resolved before the "DeFi promise" of more efficient transactions and more empowered financial consumers can hope to be realized. The key challenges involve the following: identity, anonymity, and pseudonymity; consensus mechanisms; user experience; and energy footprint. While these challenges may not be insurmountable, they call into question whether DeFi can be fit for purpose for adoption by mainstream consumers and investors.

The Challenge of Identity: Is Pseudonymous Finance Fit for Purpose?

Traditional financial institutions are unlikely to tolerate the kind of compliance, financial crime, AML/CFT and sanctions risk that direct participation in pseudonymous DeFi protocols would entail. Governments are similarly likely to show increasingly limited tolerance for DeFi protocols that enable sanctions evasion to occur. By the same token, customers expect financial privacy, and pseudonymous DeFi protocols are vulnerable to attribution of wallet addresses to individuals in a way that likely would not meet that expectation.

One of the most canonical characteristics of DeFi projects is **pseudonymity**, in other words the ability of users to remain anonymous and be known to other network participants only by a pseudonym, either a "handle" or merely a blockchain wallet address used to hold crypto-assets. The other canonical, and to some extent conflicting, characteristic is the **transparency** of the blockchain recording transactions among the pseudonymous wallets, which can be inspected by anyone operating a validator node, and through transparency services such as Etherscan. It could be said that pseudonymity is the way DeFi delivers privacy to users in the presence of the radical transparency of the blockchain.

The question that arises is whether DeFi (as presently architected) is fit for purpose for broadscale consumer or institutional finance. It may deliver both insufficient transparency and insufficient privacy to satisfy the legitimate demands of consumers and institutions, including governments.

Most current financial services provided by centralized intermediaries, by contrast, are **onymous**, i.e., they require the user to disclose their name and other identifying details to a financial intermediary, or to their counterparty in an unmediated transaction, before opening an account or entering a transaction. The user may also disclose (to their counterparties, or to the world at large) their "wallet" address in the form of bank account details or payment address to facilitate payments into the account or address, while keeping control over logon credentials or tokens required to pay out of the account.

However, most of these transactions are not transparent to the world but are instead made available only on a **need-to-know basis**. Access to the history of a user's transactions and their wallet balance is not available to other users, but rather entrusted to the financial intermediary (or in some cases a counterparty). That person may be required to disclose the transaction history to public authorities e.g., in response to a warrant or mandatory notice. In addition, certain transactions may be required to be disclosed to the public, e.g. under capital markets rules applicable to organized markets or trading platforms.

DeFi protocols do not normally require the user to disclose their true identity to anyone – a simple

wallet address is usually sufficient to interact with a DeFi application. However, to the extent that the dApp is powered by a public permissionless blockchain, anyone is free to inspect any block and can trace the history of transactions for each wallet.

The transparency of the blockchain renders the transaction record of individual users vulnerable to being made public against the wishes of the user, either through leaks of that person's wallet address (for example, by a counterparty to whom the address is provided), or through advanced data analytics that can resolve the ownership of wallets. Analytics firms are able to resolve wallet addresses and tag them, either with the true owner or with various profile attributes.[58]

This high level of transparency (with pseudonymity) is often touted as a benefit by DeFi proponents. Firms such as Chainalysis are able to publish analyses of incidents such as the collapse of Terra, showing individual transactions in minute detail.[59] This offers positive potential in the development of credit reporting, KYC, and market surveillance, where some actors can associate wallet addresses with real identities. However, a public immutable record of all transactions, which is vulnerable at any moment to being publicly attributed to an individual actor, does not appear compatible with legitimate expectations of DeFi users to financial privacy and commercial confidentiality.

For individuals, some payments information may be highly sensitive (for example, payments for medical procedures). For corporations, particularly for capital market participants, including over-the-counter (OTC) derivatives markets, where individual trader positions are typically known only to the trader's counterparty and often highly tradeable (and thus confidential) in their own right, the ability of competing firms to "resolve" pseudonymous wallet addresses to identify the institution controlling the wallet may be a significant disincentive to use DeFi protocols that depend on public blockchains.

Such permanent transparency of user transactions may also directly contradict the "right to be forgotten" principle embodied in some data regulations, such as the EU's General Data Protection Regulation (GDPR).[60]

Pseudonymity may make it more difficult in some cases for AML/CFT and sanctions screening checks (which typically require customer due diligence (**CDD**) or KYC information to be collected and submitted to risk assessment engines) to be undertaken. Those DeFi projects that adopt pseudonymity may find themselves operating outside the law, unless they are very carefully set up to ensure that they remain within exemptions from applicable regulations (for example, for transactions among self-hosted wallets in certain jurisdictions).

The recent controversy about Tornado Cash, in which the U.S. Department of the Treasury's Office of Foreign Assets Control (**OFAC**) sanctioned numerous individuals associated with the Tornado Cash mixer project, shows the risks that DeFi projects and those associated with them may run with regard to AML/CFT or sanctions compliance, as well as the challenges associated with enforcing such sanctions.[61]

---

[58] For example, Nansen claims to be a "blockchain analytics platform, which combines on-chain data with a massive and constantly growing database containing millions of wallet labels." See About Us | Who are we? | Nansen, accessed September 28, 2022.
[59] Chainalysis (2022), UST's Collapse & The Trades That Triggered It, June 9.
[60] Bloomberg (2022), Blockchain's Forever Memory Confounds EU 'Right to Be Forgotten', August 3.
[61] U.S. Treasury (2022), U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, Press Release, August 8; Cointelegraph (2022), GitHub unbans Tornado Cash repositories following OFAC guidance, September 23.

The Challenge of Validation and Enforcement: Can Blockchain Systems Support All Types of Financial Transactions?

DeFi presents additional challenges owing to the structure of blockchains and the nature of protocols, particularly around consensus mechanisms.

On-chain transactions require validation from other nodes to be added to the permanent distributed record. In order to ensure these are completed, most smart contract systems have an enforcement mechanism of some sort to ensure transactions are processed. Such a mechanism can be as simple as verification that the wallet address initiating a transfer of tokens does indeed contain those tokens. It can also be as complex as placing several successive processing orders across different tokens with unlimited leverage between several layers of protocols, requiring independent validators to process each stage, collecting gas fees along the way, and appropriately adding the transactions to the main ledger. Reserve pools and capitalization requirements for protocols attempt to ensure those participating in protocols have the money to meet their obligations. However, anonymity can present challenges to tracking down the funds or to calling in a claim. Even though many transactions in DeFi protocols are processed instantaneously, enforcement issues remain.[62] Unanticipated results of smart contract execution in these systems, identification of a counterparty, or protection from creditors, each present potential challenges to ensuring smooth functioning of smart contracts.[63]

Validation and enforcement in DeFi both represent basic operating questions that are essential to answer for these networks to continue to function. Without a centralized owner offering payment for keeping the system going, validators are subject to market-set rates for their services. Users want fees to be low, given they are the ones who bear them, but fees must rise high enough to incentivize enough validators to fulfil this role. This tension creates economic challenges and potentially creates an incentive for validators to collude and keep their fees high.[64] These markets are a good illustration of how cooperation is difficult to sustain without legal penalties and regular monitoring, as these scenarios create even greater rewards for deviating from cooperation than in usual financial transactions.[65] Validators need to speedily process transactions at a fair price without taking advantage of the information they see before the rest of the chain. The longer validators cooperate in maintaining an orderly and honorable transaction validation environment, the bigger the incentive to deviate and "cheat" becomes. The tension between the need for cooperative and trustworthy validators and the potential gains from noncooperation must be balanced within the DeFi ecosystem for it to continue to function. Full transparency of transactions (even pseudonymous) allows for the extraction of rents through front-running by miners of transactions they see in the pool awaiting incorporation in the blockchain – a phenomenon known as miner extractable value or maximal extractable value (MEV).[66]

One method of investing validators in the ecosystem is to put them on the payroll of protocols through structured returns on staking and importantly, delegation systems for tokens.[67] However, this centralizes the process of recording transactions. Several observers of this space have also

---

[62] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 12.
[63] Carlton Fields (2020), The Coming Storm: DeFi and Bankruptcy Courts, June 24; National Law Review (2022), The Limits of Smart Contract Enforcement, September 8.
[64] Daian, P. et al. (2019), Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges, April 10, p. 12.
[65] Carter, N. and Jeng, L. (2021), DeFi Protocol Risks: The Paradox of DeFi in Coen, B. and Maurice, D.R. (2021), *Regtech, Suptech and Beyond: Innovation and Technology in Financial Services* (Risk Books), August 6, p. 14.
[66] Schär, F. (2022), DeFi's Promise and Pitfalls, *Finance and Development*, September; Auer, R. *et al.* (2022), Miners as intermediaries: extractable value and market manipulation in crypto and DeFi, *BIS Bulletin,* No 58, June 16.
[67] See Onomy Protocol: Proof of Stake Validators, An Overview, accessed October 19, 2022.

noted that while DeFi has presented alternate and potentially more efficient recording and processing methods, it has not rewritten the laws or markets or human tendency to take the cheapest option. As Commissioner Crenshaw of the U.S. Securities and Exchange Commission notes, "Unless required, there will be projects that do not invest in compliance or adequate internal controls," and that with enough rewards available there will always be those who try to exploit a system through fraud or other malicious actions.[68] Under such conditions, "buyer beware" is not a sufficient foundation for a financial system.

Arbitrage opportunities exist at the validator stage and users have deployed bots to exploit these opportunities within validator pools. The same issues around market manipulation seen in traditional markets – frontrunning, latency optimization – happen in protocol spaces too, with more sophisticated programs and potentially at a higher speed. Academic work validates these concerns, posing that this fee-based prioritization of orders poses a system-level risk to the security of consensus layers.[69]

The Challenge of User Experience: Can Ease of Use Be Improved Enough to Support Broad Adoption?

We have just discussed operational challenges within the DeFi space, and now turn to a range of other concerns, particularly from consumers, that may hold back wider adoption unless addressed.

The user experience (**UX**) associated with participating in crypto-asset markets and DeFi protocols can be understandably daunting for some, particularly those who are not digitally literate. Part of this challenge is due to risk associated with **self-custody of private keys** to blockchain addresses; for example, keys may be stored on physical devices such as hard drives and USB sticks that are vulnerable to theft, loss, or corruption. The need to keep private keys to crypto-asset storage secret, without losing those keys, can be a constant challenge and source of anxiety for crypto-asset holders. There are stories of large fortunes being lost through inadvertent disposal of, or forgetting of the passwords to, physical devices.[70] Anxiety about self-custody is not confined to individuals or unsophisticated consumers; for example, asset managers are expected to prefer the assurance of a third-party custodian to manage their holdings, in line with existing practices in traditional finance.[71]

More broadly, **fraud** remains a persistent issue within DeFi. Pump-and-dump scams, 51% attacks, governance exploits, fake coin scams, and spoofing abound. Some estimates suggest over $10 billion was lost in DeFi scams in 2021 alone, with 2022 on track to exceed that number.[72] Several blogs have emerged dedicated to specifically tracking fraud in this space. Financial crime is nothing new, but the lack of identity verification and governance failings do seem to have allowed a remarkable level of fraud to flourish. Importantly for the discussion later, 65% of the major exploited protocols in 2022 did not conduct a third-party audit of their code.[73]

There may be serious drawbacks to completely automated execution, especially in consumer

---

[68] Crenshaw (2021), "Statement on DeFi Risks, Regulations, and Opportunities," The International Journal of Blockchain Law, Vol. 1, Speech, November 9.
[69] Daian, P. et al. (2019), Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges, April 10, p. 6.
[70] The Guardian (2022), Man who threw away £150m in bitcoin hopes AI and robot dogs will get it back, August 2; Insider (2021), Bitcoin Owner Who Lost Password Made Peace With Potential $220 Million Loss, January 17.
[71] OMFIF (2022), Digital Assets: Regulation and Infrastructure for an Evolving Economy, October 27, p. 15.
[72] EuroNews (2021), Crypto crime is booming on DeFi platforms and has caused over €9 billion in losses this year, November 19.
[73] European Securities Markets Authority (ESMA) (2022), Crypto-assets and their risks for financial stability, October 4, p. 5.

transactions where customers have come to rely on being able to **charge-back** payments where delivery has not been made, to reverse payments that have been procured by fraud, and in more complex areas of finance, where renegotiation of contracts may be commonplace and beneficial. In other types of consumer finance, such as mortgage lending, a waiting or cooling-off period before initiating the transaction and completing it may be needed to comply with consumer protection laws, or to allow time for necessary inspections and the like to be completed during the settlement period. In the realm of smart contracts, while many financial transactions can no doubt be automated, there may be a need to introduce a "human in the loop" or "human over the loop" in DeFi applications where reversibility of transactions is an expected feature. Similarly, regulators may demand human oversight and governance of DeFi protocols, not least the ability to step in during a crisis and use human judgment and ingenuity to resolve it.[74]

The Challenge of Energy Consumption: Can DeFi's Energy Footprint Be Sustainable?

Energy usage by DeFi protocols and the blockchains they run on present another concern. Currently, a blockchain-based financial system would consume an enormous amount of electricity, precisely when many societies are vowing to reduce consumption. Permissionless blockchains typically adopt a consensus mechanism that is either Proof of Work (**POW**) or POS, although others are possible such as Proof of History. The most well-known POW-based blockchain is the Bitcoin blockchain. The current estimate of the annualized total energy consumption of the Bitcoin blockchain is 117 TWh, comparable to the power consumption of The Netherlands.[75]

Possible Solutions to Open Up Broader Adoption in Financial Services

Identity and Pseudonymity Solutions

Many of the challenges around DeFi arise from technical aspects of and limitations with using public permissionless blockchains to deliver financial services. Much of the innovation in DeFi promises to focus on engineering solutions to address some of these challenges. At the same time, addressing some of these challenges also will likely lead to elements of centralization. One possible way to resolve some of these dilemmas is utilizing DeFi protocols that are both less transparent to other users, and more transparent to intermediaries and regulators, than at present.

One possible implementation of this approach is the **whitelisted liquidity pool**, a protocol where only users who have undergone CDD and KYC processes (either by the protocol operator or by a third party) are permitted to trade. Our discussions with IIF members and ecosystem actors suggest that this business model may become dominant in "institutional DeFi". Such liquidity pools typically run on private and/or permissioned blockchains, such that the history of transactions among wallets is known only to a trusted pool of verifiers, and subject to rigorous confidentiality constraints, and thus an element of re-centralization is introduced.

However, the KYC whitelisting aspect could also be implemented through private or public

[74] For example, see FSB (2022g), Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Consultative report, October 11, p. 15. Recommendation 4 (as consulted on) states in part, "The governance structure should allow for timely human intervention, as and when needed or appropriate."
[75] Bitcoin Energy Consumption Index - Digiconomist, accessed November 11, 2022.

blockchains that incorporate technologies such as **zero-knowledge proofs** or other privacy-enhanced technologies, such that users are certified (for example) to be not sanctioned individuals and otherwise low-risk, and issued with tokens representing that verification, which they surrender to the protocol along with a transaction without having to disclose their identity to other users or the system operator.[76] Other solutions may involve "Layer 2" or parallel networks where sensitive information about users – including their identity – is shared only with those who "need to know".

Such solutions may of course be resisted by those who, influenced by crypto-anarchism or cypher-punk philosophies, may claim that they are not in the "spirit" of DeFi. There is indeed likely to remain a "DeFi native" space outside the practical or legal purview of regulation, and where users run the risk of the loss of privacy (and of front-running by miners) that full blockchain transparency entails. However, that space is likely to be reduced progressively over time, and so those DeFi protocols that wish to grow will need to adapt.

Consensus Mechanisms

POW-based consensus mechanisms award the right to write new blocks of the blockchain (containing the definitive history of transactions recorded) to those miners that are able to solve cryptographic puzzles most quickly. The purpose of the POW mechanism is to ensure that it is very difficult to compromise the consensus mechanism, as one would need to control 51% of the processing power of all the miners on the network. While such as a "51% attack" is possible, and there have been examples, so far the Bitcoin blockchain has not succumbed, and nor did the Ethereum blockchain while it retained a POW consensus mechanism.

POS-based protocols, on the other hand, allocate the right to write the next block in the blockchain probabilistically according to the amount of crypto-assets staked by the various actors, called "staking pools". A 51% attack is also possible, through bad actors amassing control of 51% of the assets and then being able to add a block of transactions that benefits themselves to the blockchain. Doing so would mean controlling a huge amount of crypto-assets but is feasible if the protocol is small enough or maintains a limited enough pool of staked assets. Prominent blockchains such as Ethereum, which recently adopted the POS consensus mechanism through "the Merge" (see **text box**), also incorporate a mechanism (known as "slashing") designed to deter malicious actors from participating in the consensus mechanism.[77]

The Merge

On September 15, 2022, the Ethereum protocol that underlies a great many smart contracts, dApps and DeFi protocols, announced the completion of "The Merge", aka Ethereum 2.0. With The Merge, the Ethereum protocol moved to a POS consensus mechanism away from a POW mechanism, a move that was expected to reap significant savings in terms of the energy footprint of the protocol, in the order of 99.95%.[78] On September 15, 2022 06:42:42 UTC, at block 15537393, The Merge was completed.[79]

[76] The IIF has previously published principles for digital trust networks, including a suggested liability scheme model. These principles may be of assistance in the design and delivery of engineered solutions dependent on verifiable credentials. See IIF (2022), Principles for Digital Trust Networks, February 15.
[77] In many cases, a predefined percentage or a fixed amount of a validator's stake is lost if it doesn't behave as expected. Some protocols even apply a complete slashing of the stake or remove the validator from the group either for the current epoch or permanently. See What Is Slashing? - Cryptorobin.com, accessed November 1.
[78] See Explore the Merge with Consensys, accessed September 27, 2022.
[79] Binance (2022), Notice Regarding the Completion of Ethereum Merge & Information on ETHW Distribution, September 15.

User Experience

More modern interfaces have emerged that claim to address many of the UX challenges for users. Browser extensions or other "in the background" tools offer management of self-custodied private keys, secure login, token wallet, and token exchange in a user-friendly format. Yet, reducing user frictions comes with its own security overhead; for example, browser extension tools may create additional points of exposure to this private information from sites a customer visits if there is a bug in the tool or in the browser.[80]

Digital identity is one of the key enablers of secure DeFi, and one which is crucial to tackling fraud. While not strictly a financial service, **digital identity** and verifiable credentials issuance and validation are important enablers of greater trust achieved at lower cost. We have already mentioned possible issuance of verifiable credentials in the previous section. The behavior and programmability of on-chain activities present an opportunity for digital identity storage and management, whether fully self-managed or through government or institutional issuance.

One means of introducing a degree of flexibility similar to charge-backs familiar in credit card payment systems, without necessarily departing from DeFi principles, could be to introduce smart contract dependency on **dispute resolution oracles** – human-powered or algorithmic – set up to adjudicate on disputes arising from DeFi transactions, and even empowered to reverse transactions in appropriate circumstances.[81] Those oracles might be rewarded with a percentage of the value at stake, or earn rewards in other ways as determined by the DeFi project.

Of course, to the extent that DeFi applications include a "human in the loop" feature on smart contracts, they may not be able to reap the full economic benefits of automation. There may also be a sense that, by introducing an element of human judgment, they are departing from a "true DeFi" ethos.

It is worth mentioning that at present, most DeFi projects have a degree of flexibility built in where certain fundamental parameters are under the control of the governance token holders voting as a body. Other DeFi projects also retain special privileges for "admin key" holders, who are key developers or project backers, but these privileges are not considered compatible with DeFi principles by some and in addition can create insider risks.

Energy Footprint

POS-based blockchains consume far less electricity than POW, because control is not decided by computing power, rather by asset ownership (see **text box** on The Merge). In addition to the environmental impact, the switch to POS may reduce the risk of over-centralization by opening up the validator role to anyone with Ether to stake, not just miners.[82]

The significant energy cost savings associated with POS consensus mechanism means that POS-based DeFi could address smaller transactions where a POW-based consensus mechanism would be uneconomic, if transaction fees declined in line with energy consumption, something that is not guaranteed.[83] This may have benefits for financial inclusion, especially if combined with a

[80] See ether - Does metamask store private key on server or anywhere else? - Ethereum Stack Exchange, accessed September 29, 2022.
[81] See for example How does UMA's Oracle work? - UMA Protocol (umaproject.org), describing how human voters determine certain disputes submitted to the UMA Protocol's Data Verification Mechanism.
[82] Chainalysis (2022), How The Ethereum Merge May Impact the Crypto Ecosystem: On-chain Indicators to Watch, September 7.
[83] The Merge was not expected to lead to a reduction in gas fees: see Cointelegraph (2022), Ethereum Foundation clarifies that the upcoming Merge upgrade will not reduce gas fees, August 17. Presumably, this is because the validators are able to extract rents from transactions, by demanding a return on their staked assets for validating.

move away from pseudonymity, and towards use of client attributes to make lending and other decisions.[84]

Of course, many POW blockchain protocols still exist, notably the Bitcoin blockchain. While it does not support smart contracts, and therefore is not strictly a DeFi protocol, Bitcoins can be "wrapped" or tokenized on the Ethereum or other blockchains and thus deployed in DeFi protocols, for example as collateral.

Nodes in POW blockchains can run on specialized cryptocurrency mining equipment operating in private data centers or can be operated on public cloud installations. The environmental footprint of public cloud may be materially better than that of self-hosted installations, given public cloud providers' scale and their expertise with optimization of heating and cooling, data center location, power sourcing policies, etc.

Lastly, so-called "Layer 2" solutions involve taking a pool of transactions and netting it off-chain, and only writing to the blockchain the netted transactions on a periodic basis. Such solutions may involve less energy consumption, though they also depart from the decentralized nature of DeFi (given a single intermediary or group of intermediaries typically operates the Layer 2 ledger) and may introduce further cyber and fraud risk.

Towards a DeFi – TradFi Middle Ground

A variety of levels of decentralization are likely. The trade-offs struck between decentralization, scalability, and security are likely to fall along a continuum ranging from centralized actors managing interactions much like traditional banking, and largely decentralized protocols characterized by sophisticated users' comfort with managing their own wallets and interfaces. Along this decentralization spectrum the trade-offs between security and scalability will likely take a different shape at each point, leading to a variety of business models ranging from the fee-based structure of traditional banking at the more centralized end, to a business model more closely resembling social media platforms on the other end, deriving revenue from a combination of activities tailored to the individual.

Existing FIs will not be fundamentally displaced, especially as certain benefits do come with being heavily regulated: for example, government-backed insurance for depositors and established risk management procedures generate confidence in these firms as actors. Governments need to be able to rely on identifiable responsible entities to facilitate economic activity while preventing fraud and sanctions evasion. FIs are also extremely innovative and will adapt where they believe adaptation is beneficial, including by integrating degrees of decentralization.

Further adoption of DeFi tools and integration with DeFi protocols by FIs does present challenges, such as interconnectedness with the traditional financial system, operational risks stemming from underlying blockchains, smart contract-based vulnerabilities, other governance and regulatory risks, and scalability challenges.[85] A variety of approaches to overcome or mitigate these challenges exist, but their existence should be carefully considered by those looking to manage the degree of decentralization in their businesses.

"Institutional DeFi" (see **text box** for some recent examples) is evolving as a middle space, built on DLT and smart contracts, where concerns around anonymity are handled at the

[84] Aramonte, S. et al. (2022), DeFi lending: intermediation without information?, BIS Bulletin No 57, June 14.
[85] Carter, N. and Jeng, L. (2021), DeFi Protocol Risks: The Paradox of DeFi in Coen, B. and Maurice, D.R. (2021), *Regtech, Suptech and Beyond: Innovation and Technology in Financial Services* (Risk Books), August 6, p. 1.

onboarding stage of admission into a whitelisted liquidity pool, giving participants free rein within a walled system. Any blockchain solution that will be useful for wholesale finance (for example, in clearing and settlement) will need to be engineered to resolve the need of institutional investors for both transparency to regulators and commercial secrecy. That indeed may be the key use case for permissioned blockchains, though public permissionless blockchains which make use of verifiable credentials may be another fruitful approach.

In the retail space, reliance on pseudonymous wallets may persist, though regulators will likely continue to reduce the degrees of freedom here through standard-setting and enforcement. DeFi protocols without any sort of regulatory barriers to entry for users – such as KYC and AML controls – are likely to persist, but become increasingly marginal, ending up at the outer edges of the financial system.

Selected recent developments in Institutional DeFi

Project Guardian is a MAS initiative to "explore the economic potential and value-adding use cases of asset tokenisation."[86] The project is about integrating TradFi with DeFi in the wholesale funding markets via the creation of "permissioned liquidity pools" and trust anchors. DBS, Onyx by J.P. Morgan and SBI Digital Asset Holdings launched the first industry pilots under Project Guardian in two workstreams, exploring potential DeFi applications in wholesale funding markets. The banks conducted FX and government bond transactions against liquidity pools comprising of tokenized SGD and JPY assets including government bonds and tokenized deposits.[87] The pilot found that DeFi protocols have potential to be adapted and tailored for FX and government bond markets activities on a public blockchain.[88] Pilot One participants engaged with third-party auditing services to conduct complete smart contract audits prior to deployment.[89] Drawing on lessons learned, the FIs involved believe the industry should focus its collaborative efforts in three areas: a) addressing legal and regulatory uncertainties, b) establishing shared standards, and c) envisioning a target market structure.[90]

Separately from Project Guardian, UBS on November 3 launched a 3-year Swiss-franc denominated senior unsecured bond with a total issuance of CHF 375 million and a maturity in 2025. This bond was issued on the DLT-based central securities depository of **SIX Digital Exchange** and is the first of its kind that can also be held conventionally. In addition, this bond is intended to be listed and tradeable at both SIX Digital Exchange and SIX Swiss Exchange. Due to a single international securities identification number (ISIN) for the digital bond ("single-ISIN solution"), the handling of digital bonds is intended to be greatly simplified as there is no longer a need for a "twin bond" in the traditional world.[91]

In July, **BNP Paribas** Securities Services announced it was working with two fintechs, Fireblocks and METACO, to develop its digital custody offering. Also in July, **BNY Mellon** and **Goldman Sachs** settled the first securities lending transaction using a DLT platform provided by the fintech firm HQLA.[92]

[86] MAS (2022), Project Guardian, October 19.
[87] Finextra (2022), Singapore Fintech Festival 2022: Inside Project Guardian, November 2.
[88] Oliver Wyman *et al.* (2022), Institutional DeFi: The Next Generation of Finance, November 6, p. 29.
[89] *Ibid*, p. 35.
[90] *Ibid*, p. 36.
[91] SIX Digital Exchange (2022), UBS launches world's first native digital bond with intended dual listing and trading on SIX Digital Exchange and SIX Swiss Exchange, Press Release, November 3.
[92] OMFIF (2022), Digital Assets: Regulation and Infrastructure for an Evolving Economy, October 27, p. 13.

Middle grounds between a fully anonymous system, purely self-custodied financial transactions, and a gated community of automated financial tools exist. Participants have tended to talk about one or the other, but some midpoint in what information is stored where and how well it is masked is possible. Additionally, decentralization is a nuanced concept that encompasses multiple elements of what can be decentralized. Those existing institutions that remain open to new approaches and that pursue active experimentation will likely be able to benefit from innovation pioneered by DeFi projects, particularly those running an open-source code model. To take advantage of the opportunities, existing regulated institutions need to be open to partnering with the right DeFi protocols, where those protocols are capable of delivering "institutional-grade" security, privacy and stability.

The most likely scenario is therefore that DeFi begins to resemble traditional FIs more and more, while FIs adopt those DeFi technologies that add value. Competition and collaboration will create the financial system of the future, rather than one type of finance replacing another. Finance is likely to settle somewhere between the current system and one that relies on technology, particularly smart contracts and decentralized protocols, significantly more.

Improved Risk Management

All firms adopting, or experimenting or interacting with, more decentralized systems would benefit from updating their risk management tools and plans. They will need to invest in understanding the technologies, there should be a greater exploration of third-party relationships, and a better understanding of the smart contracts and automation code involved, and they will need to update KYC and know your customer's customer (KYCC) procedures for a world of protocols and autonomous actors.

Regulatory Considerations and Principles

Regulatory clarity and modernization could address some of the challenges to DeFi adoption. Many have called for government action to protect consumers from harm, protect market integrity (including market cleanliness and transparency), establish fair competition between existing FIs and new entrants, and allow for responsible innovation, including by giving intermediaries the confidence to invest in these technologies. As many have noted, collaboration between regulators and the private sector can support innovation and help it develop in an appropriate manner.[93] Calibrating regulation and operational risk management appropriately could help these technologies and the functions they are capable of carrying out mature in a sustainable way that could advance the tokenization of assets more broadly, including not only securities and bonds but also non-financial assets such as real estate.

Regulation in this case must ask: 1) what functions are being performed, 2) to what extent we can be comfortable with what those functions are, and 3) whether the combination of certain of those functions changes that answer. Existing FIs may feel hamstrung by existing banking rules, or even their own internal operational risk management teams, prohibiting them from employing more decentralized processes or technologies where they might enable a decrease in overhead or other operating costs. At the same time, potential risks to financial stability presented by DeFi are a legitimate concern for regulators and need to be better understood – including, for example, the exponential rate at which an error could be quickly replicated in a fully automated process affecting vast sums of assets before the error would be caught.

[93] Menon, R. (2021), The future of money, finance and the internet Speech, November 9.

This is the core question for most participants and regulators – how should this space be regulated? Some participants assert that DeFi needs "rules of the road", so long as they are flexible and well-designed. The challenge of appropriate regulation and supervision, however, is broader than an exercise in identifying gaps to cover with new rules.

Key Principles in Regulation Modernization: Risk and Outcome-Focused Regulation

As regulatory updates and clarity are considered, some principles may guide these efforts:

- broadly, the "same activity, same risks, same regulation" principle, when understood as focused on achieving the same regulatory outcome, understanding that an activity executed using a different technology may present different operational risks;
- the principle of technology neutrality; and
- the desirability of globally consistent and interoperable rules governing global finance.

First person quotes from some leading regulators gives the most direct view of activity and outcome-based regulation in context.

The U.S. Federal Reserve's Vice Chair for Supervision Michael S Barr stated recently,[94]

> *We plan to work with other bank regulatory agencies to ensure that crypto activity inside banks is well regulated, based on the principle of* ***same risk, same activity, same regulation****, regardless of the technology used for the activity.*

The FSB has also used this formula in its recent consultation paper on crypto-assets regulation, where it proposes to recommend, **[95]**

> *Authorities should apply effective regulation, supervision, and oversight to crypto-asset activities and markets – including crypto-asset issuers and service providers – proportionate to the financial stability risk they pose, or potentially pose, in line with the principle* ***"same activity, same risk, same regulation."***

To similar effect is Recital (6) in the European Union's recently completed Markets in Crypto-Assets Regulation (**MiCA**), which states,[96]

> *Union legislation on financial services should be guided by the principles of* ***'same activities, same risks, same rules'*** *and of technology neutrality.*

The BCBS has also used a variant of this formula in the context of bank exposures to crypto-assets, saying,[97]

---

[94] U.S. Federal Reserve Board of Governors (2022), Speech by Vice Chair for Supervision Barr on making the financial system safer and fairer, Speech, September 7.
[95] FSB (2022f), Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative document, Recommendation 2 (as proposed), October 11.
[96] Citing the "final compromise text" dated October 5, 2022. The final text of MiCA is expected to be published in the Official Journal in spring 2023 and will enter into application between 12 and 18 months thereafter (see European Securities Markets Authority (ESMA) (2022), Crypto-assets and their risks for financial stability, October 4, p. 14).
[97] BCBS (2021), Prudential treatment of cryptoasset exposures, June, p. 2.

> ***"same risk, same activity, same treatment"****: a cryptoasset that provides equivalent economic functions and poses the same risks as a "traditional asset" should be subject to the same capital, liquidity and other requirements as the traditional asset.*

While many if not most SSBs and regulators espouse some variant of this principle, U.K. authorities have more recently adopted a differently worded principle in their work on crypto-assets and stablecoins of "**same risk, same regulatory outcome.**"[98] Bank of England Deputy Governor (and Chair of CPMI) Jon Cunliffe expanded on this in a speech in July:

> *[T]he extension of the regulatory framework to encompass the use of crypto technologies must be grounded in the iron principle of* ***'same risk, same regulatory outcome'****. … The starting point for regulators should be to apply the same regulation to the risks inherent in the provision of a financial service no matter how it is provided. …* ***But differences in technology may mean that existing regulation may not work in this new context or, indeed, may not effectively manage the risk.*** *Implicit in our regulatory standards and frameworks are the levels of risk mitigation we have judged necessary.* ***Where we cannot apply regulation in exactly the same way, we must ensure we achieve the same level of risk mitigation – in other words, the "same regulatory outcome".***[99]

This variant of the maxim usefully foregrounds a couple of points: different activities may present the same risks and therefore should be treated similarly; different activities that present the same risks should be afforded equivalent treatment, but not necessarily identical; and equivalence can be usefully defined in terms of the level of risk mitigation.

Technology neutral regulation – Meaning and limits

The principle of technology neutrality is often espoused by SSBs and regulators, as seen above. That said, it is also worth considering for a moment what it means. The principle of technological neutrality dictates that policymakers should not "pick winners" in the competition between alternative technologies; rather, market mechanisms should determine which technologies achieve broad adoption, for this will ensure the most cost-effective solutions.[100]

However, it is possible to criticize this principle as failing to provide adequate incentives to develop or uptake innovative products or services where there is some overriding policy principle that necessitates innovation be accelerated. For example, a quite stringent adherence to technological neutrality could pose the risk of delaying the adoption of clean technologies that are compatible with the goals of climate protection.[101] Some DeFi voices occasionally criticize the principle of technological neutrality on the same basis, claiming that more should be done to favor financial innovation. By the same token, one lesson of the Financial Crisis was certainly that unbridled financial innovation, fueled by cheap money and without adequate guardrails, can lead

---

[98] HM Treasury (2022), UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: Response to the consultation and call for evidence, April, para 2.42 and 3.41.
[99] Bank of England (2022), Some lessons from the Crypto Winter – speech by Sir Jon Cunliffe, July 12.
[100] See, e.g. Lehmann, P. (2020), Technological Neutrality: A Critical Assessment, January (English translation).
[101] *Id.*

to systemic risks that can endanger the entire financial system, and with it, the real economy.

There is of course a need for clarity around regulatory boundaries and supervisory responsibilities. This may require the official sector to give guidance to financial innovators – including DeFi projects and their promoters – about how the regulatory "perimeter" or boundary may encompass them.[102] Given that in many cases the regulatory perimeter will have been designed with centralized financial services in mind, this should not be seen as a violation of the technology neutrality principle. Also, a regulatory framework that facilitates bringing these financial activities within the regulatory perimeter where associated risks will be subject to robust capital and liquidity regulation, sound risk management and ongoing supervisory oversight, will be a net positive for the DeFi activities and, most importantly, its users.[103]

Regulatory and Supervisory Challenges, Responses, and Other Enablers

The level of **decentralization** may complicate regulation and enforcement. DeFi protocols, by definition, act by means of smart contracts and in many cases are operated by "decentralized autonomous organizations" (**DAOs**) where decision-making responsibility may be diffused among governance token holders. As a result, determining responsible entities for regulators to hold accountable may be difficult. However, responsibilities in many protocols may not be as widely dispersed as their names imply. A number of official sector papers have referred to the "decentralization illusion", pointing out that in many cases governance tokens are highly concentrated or that a small group of participants hold the admin keys and other tools of power.

Regulators have begun to formulate strategies for holding decentralized organizations responsible for bad behavior. The Commodity Futures Trading Commission's complaint against Ooki DAO identifies the defendant as "an unincorporated association comprised of holders of Ooki Tokens … who have voted those tokens to govern (e.g., to modify, operate, market, and take other actions with respect to) the Ooki Protocol." In this case, the responsible entity to be regulated takes the form of anyone who voted on the protocol's operations. The OFAC recently sanctioned numerous individuals associated with the Tornado Cash mixer project, including developers.[104]

The **cross-sectoral** nature of DeFi protocols is a challenge as they may combine elements of banking, credit provision, payments, funds management and insurance. Consequently, it may be hard to classify regulatory responsibilities correctly or consistently, particularly for sector-specific regulators, and for regulators to coordinate effectively among themselves. Greater cooperation between regulators and across sectors, including with privacy regulators, can address the issue.

The **cross-border** and distributed nature of DeFi protocols creates situations where any user who is able to run a client node of a protocol can participate from wherever they are. More geographically dispersed actors complicates regulation as these protocols then involve multiple jurisdictions. In response, regulators that are used to overseeing large cross-border entities, such as banking groups and financial market infrastructures, may further develop their collaborative oversight models to address the particular challenges of DeFi.[105]

---

[102] Of course, each regulator administers one or more regulatory perimeters according to the types of licenses or registration (or activity-based regulation) it administers.
[103] C.f. IIF et al. (2022), Comments in Response to the Second Consultation on the Prudential Treatment of Cryptoasset Exposures, September 30.
[104] CFTC (2022), Complaint accessible via Media Release, September 22; U.S. Treasury (2022), U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, Press Release, August 8.
[105] See IIF (2020), Submission to FSB on global stablecoins, July 15.

The **pseudonymous nature** of public permissionless blockchains means that in many cases DeFi apps are said to be operating in a non-compliant manner, including by failing to conduct CDD or other KYC information normally obtained for AML/CFT purposes. As mentioned above, institutional DeFi may become increasingly permissioned and compliant, while permissionless DeFi may remain pseudonymous and largely non-compliant. In such a scenario, permissionless DeFi may become increasingly marginal. The possible development of tokenized verifiable credentials assisting with compliance issues could alter this dynamic, permitting greater participation in permissionless DeFi while also supporting compliance obligations.[106]

A lack of client classification or suitability checks stems from the practice of many DeFi protocols that make no distinction in terms of accessible functionality between retail and professional clients, and/or make no effort to determine product suitability, so may expose particularly retail or unsophisticated clients to levels of risk or to products that are not suitable for them.

DeFi protocols may fail to manage **conflicts of interest**, particularly between governance token-holders or other insiders and end users. **Market cleanliness** can be an issue, as DeFi protocols may not operate market integrity functions designed to avoid insider dealing, order front-running, wash trading, or other abusive practices. Public permissionless blockchains lack privacy, since identifying an address (including through a data breach or through data analytics) can also allow users to see all transactions for that address. Similar to AML/CFT challenges, the pseudonymous nature of DeFi protocols complicates **tax or sanctions compliance** for protocol operators, and tax and sanctions authorities may be unable to effectively fulfill their mandates.

Implications for Supervisors

DeFi presents challenges to supervisors as well as to regulators. Most of these challenges (particularly the cross-border and cross-sectoral nature of DeFi) are aligned to those already described above; however, the vast amount of data generated by DeFi services, along with its automated nature, pose different challenges by way of ongoing monitoring and identification of emerging risks. Some of these challenges to supervision include:

- **Lack of supervisory powers:** supervisors may lack powers or up to date enforcement tools to supervise DeFi activities, if the legislature has not acted to extend the regulatory perimeter where appropriate and consistent with the principle of "same risks, same regulatory outcome."
- **Expertise and data analytics:** supervisors may lack the expertise to understand the DeFi protocols they are responsible for or may lack access to sufficient data analytics to make sense of the activity in these protocols. As a result, supervisors may be ill-equipped to understand risks emerging in these markets.
- Supervisors may have invested in building technological capacity, but more attention must be paid to sufficiently understanding **business models**. The economic implications of service offerings that exemplify the challenges set out above are still being evaluated. As understanding grows, supervisory coordination and collaboration across different types of regulators, such as financial, consumer protection and privacy watchdogs, can ensure thoughtful and consistent application of regulation.
- **Ring-fencing of assets:** Big DeFi projects based in one jurisdiction that house client assets belonging to other jurisdictions may present issues, particularly if assets pledged or lent by clients have been mixed in omnibus accounts or used as working capital by the project.

[106] See Possible Solutions to Open Up Broader Adoption in Financial Services section at page 26.

- Some authors have suggested **"embedded supervision"** as a means for supervision to adapt to a DeFi world. One definition of this term is "a regulatory framework that provides for compliance in decentralized markets to be automatically monitored by reading the market's ledger," reducing the need for firms to actively collect, verify and deliver data.[107] Some supervisors may prefer, however, to gather their own data and leverage blockchain analytics firms to enhance their supervision.

Legal Enablers

Various legal structures may be considered or require clarity as well, to include the following:

- **E-signatures and e-transactions:** those jurisdictions that still require paper records or 'wet-ink' signatures could modernize by adopting the United National Commission on International Trade Law (**UNCITRAL**) Model Law on Electronic Commerce or similar enabling laws. [108]
- **Legal status of crypto-assets:** in many jurisdictions, the legal status of crypto-assets is still somewhat uncertain, although in many common law jurisdictions it is reasonably clear that they are a form of intangible property, over which freezing orders and other proprietary remedies are available. The U.K. Law Commission has proposed clarifying the legal status of digital assets as a third form of personal property alongside tangible property and choses in action such as securities. Such clarification would provide a strong legal foundation for the digital assets industry and for users.[109]
- **Transfer and taking security:** In the U.S., proposed amendments to the Uniform Commercial Code (**UCC**) to take account of digital assets include changes to Article 9 (concerning the creation and perfection of security interests) and the insertion of a new Article 12 (concerning the transfer of property rights in intangible digital assets).[110]
- In some jurisdictions, the legal status of, or liability regimes around, **smart contracts** and **autonomous execution** may be unclear. In those jurisdictions, legal changes may be desirable to give all stakeholders clarity.
- Legal changes to facilitate **tokenization of real-world assets,** such as real estate, vehicles, and receivables that one could leverage in secured lending transactions, is a complex challenge and one that may take many years to realize in some jurisdictions.
- Lastly, **digital trust and identity networks** will be essential to the issuance and recognition of verifiable credentials in the future trust ecosystem. Clarifying governance and liability arrangements around those networks will be paramount.[111]

Regulatory Work Underway or in Prospect

Regulators to-date have largely focused on building expertise rather than taking prescribed actions, given the limited size and scale of the DeFi universe relative to activity in digital asset

---

[107] See, e.g. Auer, R., (2019), Embedded supervision: how to build regulation into blockchain finance, *BIS Working Papers* No 811, September (revised May 2022).
[108] United National Commission on International Trade Law (UNCITRAL), UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998.
[109] See Law Commission (2022), *Digital Assets: Consultation Paper* and *Digital Assets: Summary*, July 28, both available through Digital assets | Law Commission.
[110] Uniform Law Commission (2022), UCC, 2022 Amendments to | uniformlaws.org, July 26 and September 29.
[111] See IIF and Open ID Foundation (2022), Principles for Digital Trust Networks, February 15. Those principles set out suggested governance arrangements, including a guideline liability scheme, which could guide the members of trust networks as they work out their governance arrangements at the network or federation level. The principles are designed to be compatible with centralized, decentralized (SSI) and federated trust models.

(including both stablecoins and crypto-assets) markets and the need to better understand associated risks. Most regulators appear to be addressing digital assets more broadly as a precursor to addressing DeFi platforms and services, which rely heavily on stablecoins and crypto-assets to facilitate the asset layer. Partly as a result of growth in these markets, and partly due to their increasing interconnectedness with the existing financial system, digital assets are intense areas of focus and work for regulators globally.

Table 1: Selective overview of global policy workstreams on digital assets

Financial Stability Board
• Vulnerabilities assessment arising from crypto-assets, Feb 2022
• Statement on International Regulation and Supervision of Crypto-Asset Activities, Jul 2022
• Global stablecoins: Oct 2022 consultation report; final recommendations expected mid-2023
• Unbacked crypto-assets: Oct 2022 consultation report; final recommendations expected mid-2023
• Monitoring and possible additional policy work on DeFi in 2023
Basel Committee for Banking Supervision
• Prudential treatment of cryptoasset exposures: second consultation mid-2022; final standards expected end-2022
International Organization of Securities Commissions / Committee on Payments and Market Infrastructures
• Systemic stablecoins: CPMI and IOSCO final guidance on application of principles for financial market infrastructures, Jul 2022
• DeFi:
• IOSCO report on DeFi, Mar 2022
• Crypto and Digital Assets (CADWG) and DeFi workstreams set up by IOSCO Fintech Task Force, July 2022
Organisation for Economic Cooperation and Development
• OECD report on DeFi and policy implications, Jan 2022
• OECD report on Crypto and DeFi - TradFi interconnectedness, May 2022
• Ongoing work on DeFi
Financial Action Task Force
• Updated FATF Guidance for a Risk-Based Approach to Virtual Assets and VA Service Providers Oct 2021

Source: Authors' elaboration.

Global Standard-Setting Bodies' Activities

The global financial regulation SSBs have divided their work on digital assets into four broad buckets, namely global stablecoins; unbacked crypto-assets; DeFi; and CBDCs. The major global workstreams are shown in **Table 1** and discussed in further detail below.

On **global stablecoins**, on July 13, shortly after the Terra/Luna collapse, the FSB published a statement on crypto-assets and stablecoins, saying:

> *Stablecoins should be captured by robust regulations and supervision of relevant authorities if they are to be adopted as a widely used means of payment or otherwise play an important role in the financial system.*[112]

In October the FSB delivered a consultative report on its review of its 2020 high-level

[112] FSB (2022b), FSB issues statement on the international regulation and supervision of crypto-asset activities, July 13.

recommendations, and how any gaps identified can be addressed by existing frameworks,[113] which is expected to lead to final recommendations in mid-2023.[114]

The Committee on Payments and Market Infrastructures (**CPMI**) and International Organization of Securities Commissions (**IOSCO**) also finalized guidance on the application of the Principles for Financial Market Infrastructures (PFMIs) to systemically important stablecoins in July 2022, in the wake of their October 2021 consultation report.[115] In association with the CPMI and IOSCO, the IIF also convened a roundtable workshop in November 2021 on this topic.[116]

On February 16, 2022, the FSB released a report on vulnerabilities from **crypto-assets**, focusing on private sector developments including DeFi, and building on previous work published in 2019.[117] While the report noted the limited direct connections between crypto-assets and systemically important institutions and core financial markets at present, the report noted that financial stability risks could escalate rapidly and called for timely and pre-emptive evaluation of possible policy responses. The report contains an in-depth discussion of DeFi, noting many of the challenges mentioned in this paper.

The FSB subsequently published a consultative report on **crypto-assets** in October 2022, which is also expected to lead to final recommendations in mid-2023.[118] The recommendations are closely aligned with those for global stablecoins for the most part, and the FSB also published a short narrative paper at the same time providing a description of the overall work program. Importantly, the FSB pointed to possible further policy work around DeFi in that paper, saying:

> *The FSB is analysing developments and potential risks to financial stability stemming from [DeFi] and will consider in 2023 whether additional policy work is warranted based on the findings from this work.* [119]

The IIF convened a round table with the FSB on stablecoins and crypto-assets on August 23, 2022, and intends to submit a response to the FSB's consultation papers, as it did to the FSB's consultation on global stablecoins in 2020. [120]

At end-June 2022, the Basel Committee on Banking Supervision's (**BCBS**) issued a public consultation on the prudential treatment of banks' crypto-asset exposures, following its 2021 preliminary consultation. A further BCBS consultation paper was published in mid-2022 and the final standards are expected by the end of 2022 or early 2023. [121] On September 20, 2021, the IIF and a group of trade associations submitted a joint industry comment letter in response to the BCBS's 2021 consultation report.[122]

---

[113] FSB (2022c), Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Consultative report, October 11.
[114] FSB (2021), Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Progress Report on the implementation of the FSB High-Level Recommendations, October 7.
[115] CPMI and IOSCO (2022), Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, July. CPMI and IOSCO (2021), Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, October 6.
[116] See IIF (2022), Briefing Note on Stablecoins, January 5.
[117] FSB (2022a); see also FSB (2018), Crypto-asset markets: Potential channels for future financial stability implications, October 10.
[118] FSB (2022d), Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative report, October 11.
[119] FSB (2022e), International Regulation of Crypto-asset Activities: A proposed framework – questions for consultation, October 11, p. 6-7.
[120] IIF (2020), Response to FSB on global stablecoin arrangements, July 15.
[121] BCBS (2022), Prudential treatment of cryptoasset exposures - second consultation, June.
[122] IIF (2022f), Comments in Response to the Second Consultation on the Prudential Treatment of Cryptoasset Exposures, September 30.

IOSCO published an important paper on DeFi in March, which did not contain policy recommendations or proposals but surveyed the landscape and identified key risks and vulnerabilities around DeFi protocols. In July, IOSCO published its Crypto-Asset Roadmap for 2022-23. The IOSCO Fintech Task Force (**FTF**) will prioritize policy-focused work on crypto-asset markets and activities in its initial 12 to 24 months of operation, while continuing to monitor broader fintech-related trends. The FTF has set up two workstreams focusing on Crypto and Digital Assets, led by the U.K. Financial Conduct Authority and Decentralised Finance, led by the U.S. Securities Exchange Commission. Each workstream is aiming to publish a report with policy recommendations by the end of 2023.[123]

The Organisation for Economic Co-operation and Development (**OECD**) released two major analytical reports on DeFi in January and May. The first report explained DeFi and its applications and described the evolution of DeFi markets to date. It explored the benefits and risks of DeFi and the DeFi/CeFi intersection and put forward policy considerations. The second report followed in May, focusing on the increasing institutional involvement in crypto-asset markets and the growing TradFi-DeFi interconnectedness.[124] The OECD is understood to be continuing to work on publications around DeFi.

The Financial Action Task Force (**FATF**) released updated guidance on a risk-based approach to virtual assets and virtual asset service providers in October 2021.[125]

Clarity on Regulatory Responsibility for DeFi Protocols

Swiss National Bank Deputy Head Thomas Moser recently gave an interview where he made some interesting observations about DeFi regulation:[126]

> *"If you just take the existing regulation and put it on crypto, then DeFi will disappear because you will only have centralized entities that you can regulate with the current regulation. For DeFi, where there is no single entity to be held accountable for, which is really just smart contracts interacting, you need a different type of regulation."*

The MiCA text addresses DeFi in its Recital (12a) by excluding fully decentralized services, saying in part,[127]

> *… Where crypto-asset services … are provided in a fully decentralised manner without any intermediary they do not fall within the scope of this Regulation. … Where crypto-assets have no identifiable issuer, they do not fall within Title II, III or IV of this Regulation. Crypto-asset service providers providing services to such crypto-assets are, however, fully covered by this Regulation.*

---

[123] IOSCO (2022), Crypto-Asset Roadmap for 2022-2023, July 7.
[124] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19 and OECD (2022b), Institutionalisation of crypto-assets and DeFi–TradFi interconnectedness, May 19.
[125] FATF (2021), Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers, October 28.
[126] Cointelegraph (2022), Swiss National Bank exec: Regulators may favor centralized stablecoins after Terra crisis, June 27.
[127] Final compromise text dated 5 October 2022. The final text of MiCA is expected to be published in the Official Journal in spring 2023 and will enter into application between 12 and 18 months thereafter: see European Securities Markets Authority (ESMA) (2022), Crypto-assets and their risks for financial stability, p. 14.

By contrast, the U.S. Commodity Futures Trading Commission (**CFTC**) has taken enforcement action against **Ooki DAO** for failure to register as a futures commission merchant and derivatives contract market for activities that included offering leveraged and margined retail commodity transactions in digital assets. In its complaint, the CFTC described the Defendant (Ooki DAO) as

> *"an unincorporated association comprised of holders of Ooki Tokens … who have voted those tokens to govern (e.g., to modify, operate, market, and take other actions with respect to) the Ooki Protocol" during a particular period.*

Non-voting token holders appear to be excluded by the CFTC's definition of the defendant unincorporated association, but those token-holders who voted against propositions that were carried are not excluded.[128]

Also as mentioned earlier, the OFAC recently sanctioned numerous individuals associated with the Tornado Cash mixer project, including developers. U.S. Congressman Tom Emmer expressed concern that the sanctions "were not levied against a person or an entity, but against 'privacy-enabling code," and that, as a result, the sanctioned Ethereum addresses will have no ability to appeal the sanction to OFAC as they are smart contracts with no agency.[129] The issues raised by Congressman Emmer were also raised in a lawsuit brought in a 20-page complaint in Federal Court in Texas on September 8, 2022. Plaintiffs claim the decision to sanction Tornado Cash exceeded the government's powers under the International Emergency Economic Powers Act (**IEEPA**) because Tornado Cash is not a "property," a "foreign country or a national thereof," or a "person" of any kind under the IEEPA.[130]

This litigation illustrates that some possible objects of regulation associated with DeFi projects include:

- the business entity associated with the project and its directors;
- other holders of equity in the business entity associated with the project;
- an incorporated DAO (such as may be registered under the Wyoming DAO statute);
- holders of governance tokens controlling a DeFi app (or at least, voting holders);
- developers writing the code;
- the smart contract code itself.

The last two possibilities are likely to be very controversial. Where code is developed which has both legitimate and illegitimate users, it is not clear why developers – as opposed to those who use the code – should be responsible. On the other hand, where code can only be used in an illegitimate way, there may be a good case to sanction developers, particularly where they can be identified more easily than other actors and where there are reasons to be believe they may have substantial assets. That said, in jurisdictions (such as the U.S.) with constitutionally protected free speech, regulators will always have difficulty frontally sanctioning the expressive activity of publishing code (for example, on GitHub).

Sanctioning code itself has an element of science fiction about it. However, as smart contracts will increasingly come to control large amounts of assets, it may make sense to allow for those assets to be confiscated, where it is not possible to identify any human actors or legal persons in control,

---

[128] See complaint cited at footnote 103.
[129] Emmer, T. (2022), letter dated August 23, 2022 to U.S. Treasury Secretary Yellen.
[130] See FINAL - Tornado Cash Complaint | PDF | Cryptocurrency | Office Of Foreign Assets Control (scribd.com), accessed November 1, 2022.

at least where it cannot be shown those assets belong to innocent users.

The Role of Technical Standards

DeFi is built on certain technical standards, such as the ERC-20 (fungible tokens), ERC-721 (non-fungible tokens) and ERC-1155 (fungible and non-fungible tokens) standards of the Ethereum Foundation, upon which so many DeFi projects and NFT collections are built.[131]

One of the key vulnerabilities of DeFi has been its susceptibility to cybercrime, whether through "exploits" of code bugs and loopholes, insider fraud, or brute-force keyword or private key attacks. The result is that client assets are in many cases highly vulnerable to theft or loss.

Inter-protocol "bridges" have been a particular source of loss, with the bridge hack share of total stolen funds running well over 50% in 2022.[132] As we have seen, the Metaverse is a notional logical space that links or binds numerous private virtual environments or "walled gardens", implying that one could port one's identity, and perhaps virtual goods (including NFTs) from one private space to another. To that extent, bridges among protocols underpinning individual private spaces are likely to be crucial to the Metaverse, and present particular points of cyber vulnerability.

The history of DLT and DeFi has to a large extent been intertwined with the open-source code movement. To the extent that the codebase of many DeFi protocols and projects builds on or consists entirely in open-source code, they display cyber vulnerabilities that are particularly to open-source projects. As open-source code by definition is public to any developer, bad actors can deliberately plant or ignore "trap doors" in the code, which they can exploit later. Other DeFi services such as "vanity address" generators can also embody code vulnerabilities that can have devastating consequences.[133]

Beyond technical standards that are tailored to each DeFi protocol or application, there may also be a role for technical standards to address **code security**, a key vulnerability around DeFi. Such technical standards could continue to be developed by individual protocols, or could be taken forward by standardization bodies such as the International Organization for Standardization (ISO), National Institute of Standards and Technology, or similar bodies.

Another possible subject for standardization is the field of **code audits,** given a lack of audit's role in code exploits.[134] While at present many firms, including big DeFi firms such as Consensys, offer code auditing as a human- or AI-powered service, the field of DeFi code auditing and what is required is yet to be standardized. As TradFi seeks to do more business with DeFi and with DeFi tools, pressure can be expected to increase to ensure that "institutional DeFi" has its code base audited to a certain standard, and in line with standards that have been laid down independently of the particular project in question.

Beyond technical standardization, there may also be a role for financial regulators to lay down supervisory or regulatory expectations around code audits and cybersecurity that better protect DeFi activities.

---

[131] ERC-20 Token Standard, ERC-721 Non-Fungible Token Standard and ERC-1155 Multi-Token Standard.
[132] Chainalysis (2022), Cross-Chain Bridge Hacks Emerge as Top Security Risk, August 2.
[133] See, for example, 1Inch Network (2022), A vulnerability disclosed in Profanity, an Ethereum vanity address tool, September 15.
[134] See footnote 72.

DEEP DIVE ON DECENTRALIZATION

DeFi Design, Tokenization, and Smart Contracts

Decentralized finance envisions a world where individuals conduct all financial activities "on chain" intermediated only by "smart contracts" designed to run automatically and mostly without adjustment. In reality, finance is likely to settle somewhere between the current system and one that relies on execution via technology, absent any form of intermediation or human intervention.

DeFi business models can be challenging to categorize, particularly with respect to just what is decentralized and how decentralization actually occurs. These models vary protocol to protocol depending on which services are combined. Types of activities approximate many existing financial instruments, even if the behavior and technology are different. Largely, DeFi mirrors existing lending activities from market-based providers, rather than replicating retail banking services.[135] Instead of traditional intermediaries, smart contracts aim to replace trusted third parties in custody and execution.

It is important to understand the structure of DeFi to reach a view on which parts of the existing financial system may be disrupted or complemented by the rise of such protocols, or perhaps where integration of these tools into existing services may be the natural path forward. In our exploration of these dynamics, we envision a future for the financial system where existing institutions adopt some tools of DeFi without absorbing the DeFi universe. At the same time, DeFi protocols continue to proliferate into increasingly sophisticated services, and take on many of the characteristics of centralized financial services, particularly in the institutional space.

Understanding the DeFi Business Model

Decentralized finance is an all-encompassing term for a variety of business structures. DeFi products frequently involve financial services provided on an electronic platform that are theoretically decentralized in control of the protocol (e.g. DAOs), ownership of the capital used (e.g. staking protocols), or custody of assets (e.g. DEXs). Each of these types of businesses involve replication of core financial services – lending, borrowing, trading, etc. – in a way that offers speed or transparency advantages, or enables a new combination of such.[136] Use cases and their challenges are discussed in section 2. In considering how decentralized products might interact with a future financial system, observers should consider the business model of these offerings. DeFi's relationship to centralized service offerings in the future – whether DeFi aims to provide an alternative to or integrate into the financial system – will be determined by the feasibility of these models.

It should be acknowledged that revenue generation for DeFi firms is difficult. Many DeFi firms may have trouble covering operating expenses, although transparency of project financing is rare.[137] It is tough to charge users of an open system, especially one with few barriers to entry, a fee for use, making profit generation from user fees difficult. Being able to charge fees or levies

[135] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 11.
[136] Carapella. F. et. al. (2022), Decentralized Finance (DeFi): Transformative Potential & Associated Risks, August, p. 5-6.
[137] ZeroCap (2022), How do DeFi Protocols Make Money? Revenue examples with leading projects, October 5.

more than sufficient to meet expenses requires a level of market power fundamentally incompatible with a free-to-use system. The more successful protocols from a profitability standpoint generate their money from participating in the protocols and maintaining either a controlling stake in governance or assets within the program.

It is important to understand how protocols operate and therefore, how businesses in this space are structured. What many participants refer to as the "DeFi stack" consists of the settlement layer, made up of a blockchain or a Layer 2 solution.[138] On top of this layer sits the asset layer made up of crypto-assets or other tokens, which are the medium of transaction. DeFi most properly refers to the contracting layer, which sits upon these two, and is where protocols are designed to move assets around the layer and offer financial services. Access to these smart contracts is granted via the top layer, the application layer, which is made up of user interfaces and apps.[139] Crucially, most investors interact with protocols through this application layer. These entry points are designed by builders as user-friendly APIs to connect applications and protocols, which enables connection between several protocols and the increasing ability to build leverage.[140] Further combinations of these layers can be achieved through aggregation of several of these products.

Interoperability within the ecosystem is inherent in the design. Broadly speaking, DeFi is distinguished by the layers of financial instruments built upon a digital ledger. Without the ability for contracts to interact at the digital level, protocols cannot be considered part of the ecosystem. Both interoperability and composability are key features of DeFi; different protocols exchange information while the financial transactions occurring are consistently represented within a composable stack of services.[141] In this model, interoperability is needed to ensure information transfers frictionlessly across chains and protocols, while composability enables each new protocol to interact with existing services in a way that grows the ecosystem.[142] However, pure interoperability is not achievable in practice: as chains feature different validation mechanisms, they cannot reach the same consensus about the validity of transactions on the other blockchain.[143] Cross-protocol "bridges" are one solution, but they create their own vulnerabilities to cyber-attack.[144]

The components of the stack combine to create five features of DeFi that distinguish it from traditional finance. These features are: its non-custodial nature, community-driven governance, composability, mirroring of market-based financial services (as opposed to bank-based deposits and lending), and transparency of transactions removing the need for trusted intermediaries. [145] Because DeFi protocols are non-custodial and route crypto-assets between private wallets, all DeFi transactions are recorded on-chain.[146]

Firstly, many DeFi protocols are or are stated to be non-custodial in nature (i.e. no intermediary has control over a participant's assets at any point along the chain). Within the DeFi world, there is a direct link between the seller and buyer of an asset and no intermediary holding that asset

---

[138] See further: Primer on DeFi and Web 3.0: The DeFi Stack.
[139] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 19.
[140] *Id.*
[141] MGStaking (2021), Standards, Composability, Interoperability – the key points of DeFi, Sep 7.
[142] On the other hand, protocols with different consensus mechanisms can be seen as formally incompatible, leading to the need for "bridges" between protocols (Buterin, V. 2016). Bridges immobilise crypto-assets held on one blockchain and issue tokens on another that represent that holding.
[143] Boissay, F. *et al.* (2022), Blockchain scalability and the fragmentation of crypto, *BIS Bulletin*, No 56, June 7, citing Buterin, V. (2016).
[144] See Buterin, V. (2021), Reddit post, January 8.
[145] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 10-12.
[146] Chainalysis (2022), Geography of Cryptocurrency, October, p. 6.

midway through the transaction until payment is received and the transaction is completed. Such a principle is one of the biggest differences between DeFi and current centralized services, as custody arrangements are an integral part of today's financial system, be it market- or bank-based activity.

Secondly, community-driven governance is a hallmark of DeFi. Most protocols issue governance tokens in which every holder gets a vote on changes to the protocol. While this distributes power across users of the financial tools, this structure can leave the protocol vulnerable to exploitation by insiders and well-capitalized participants (who can purchase control over the bulk of the governance tokens in some set ups) or alternatively, paralyzed by an inability to reach consensus on needed changes quickly enough.

Third, composability is a key feature. As discussed earlier, the DeFi stack entails layering of different protocols and services to create new features. Composable features have led to a myriad of new products and also potentially, new risks as these pieces interact with one another.

Fourth, DeFi activities largely mirror market-based mechanisms. Instead of exclusively mimicking traditional depository institution activities like taking deposits and making fixed-term loans, protocols layer market-based services to create newly branded products, albeit ones that in many cases are marketed similarly to banking products. Many, but not all, of these are utilizing collateralized lending as the point of entry. These products include yield farming, decentralised exchanges, derivatives and synthetics, asset management, insurance, payments, prediction markets. Additional products that do not involve collateral as the entry point – tools like noncollateralized flash loans – make up a significant part of the ecosystem. Both collateralized and uncollateralized tools share similarities with the risks of market-based financial services, particularly fire sales and lack of formal backstops.[147]

Lastly, DeFi is constructed on the premise that the instantaneous recording on a distributed ledger of financial transactions removes some of the need for intermediaries. Essentially, the transparency is meant to eliminate the need to trust another party. Academic work on networks and DeFi shows that when networks are built on transparency as a way of establishing trust, such as DLT-based systems, try to scale, they tend to break down easier and at a higher cost than intermediated systems.[148] As a result, achieving disintermediation of the financial system at scale may introduce new risks and entail higher costs from a crisis than the present intermediary-based system. This finding suggests one example of why a broad migration to an entirely decentralized system is unlikely.

Financial systems have adopted a variety of risk sharing, intermediation, and collateralized arrangements over their evolution. As an example of coexistence, the Bank of Canada demonstrated that there are conditions under which centralized lending may be optimal and conditions under which decentralized lending may be. Centralized tends to be the better option, from a capital efficiency and cost to user standpoint when "…the costs of default are large relative to the costs of using a trusted third party."[149] Which can be measured by comparing the loan size to the ex-ante value of its collateral. The valuation of collateral might be unstable in some DeFi spaces, owing to the volatility of crypto-asset prices, and therefore difficult to make this

[147] Adrian, T. (2017), Shadow Banking and Market Based Finance, International Monetary Fund, Speech, September 14.
[148] **Easier:** Lehar, A. and Parlour, C.A. (2022), Systemic Fragility in Decentralized Markets, July 25, p. 11.; Reiersen, J. (2019), Exchange networks, markets and trust, October 22, p. 5; **Cost:** Daian, P. et. al. (2019), Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges, April 10, p. 17; Lehar, A. and Parlour, C.A. (2022), Systemic Fragility in Decentralized Markets, July 25, p. 9.
[149] Chiu, J. *et al.* (2022), Grasping De(centralized) Fi(nance) Through the Lens of Economic Theory, Bank of Canada, October, p. 20.

comparative cost determination. DeFi becomes the more attractive lender when the haircut on the loan to collateral ratio is smaller. Generally, the higher the volatility of collateral assets, the less attractive DeFi lending becomes. Making this judgement call about the quality of collateral can be difficult in DeFi spaces, where rationing or selectivity in extending a loan is hampered by anonymous borrowers.

Tokenization

Presently, the asset layer of the DeFi stack is composed of an ever-expanding universe of tokens, which are generally highly volatile. Tokenized assets represent the store of and transacting unit for value in the DeFi space. In order for offered services to proliferate further, participants must be able to have confidence that their tokens will hold value. One of the most promising ways to do so is to link tokens to real-world assets. In addition to this process opening up an entirely new class of on-chain financial services related to real-world asset tokenization, tangible assets backing a virtual representation of value may exert a stabilizing effect on prices.[150] Investors typically want to be confident their assets will not suffer dramatic changes in value, and greater stability in token prices would add to their confidence.

As several authors from the BIS have pointed out, the reliance of DeFi on crypto-assets as collateral negates the touted financial inclusion benefits of DeFi, since crypto-asset collateralized loans are heavily overcollateralized, in light of the extreme volatility of them relative to more traditional assets. The borrower in such a loan is required to stake as security assets more valuable than those they borrow, and is moreover required to "top up" the collateral for fear of automatic liquidation if the minimum overcollateralization ratio is breached.[151] The ability therefore of borrowers who may own some assets – such as real estate, a motor vehicle or tools – to pledge them in exchange for a loan that is mediated automatically by smart contracts, would be a socially useful extension of DeFi from a financial inclusion perspective. As the authors put it,

> *DeFi lending must engage in large-scale tokenisation of real-world assets, unless it wants to remain a self-referential system fuelled by speculation. Representing assets such as buildings or capital equipment on the blockchain, so that it can serve as collateral underpinning loans, would be particularly beneficial for SMEs, which have more limited access to finance.*[152]

Further, incorporating digital representations of all assets is an important step toward realizing Web 3. We discuss how to enable tokenization further in Section 1 Primer on DeFi and Web 3.0: Tokenization and NFTs. Clearing that hurdle could unlock significant development in the DeFi space, particularly as tokenization could create liquidity in formerly illiquid markets, such as real estate. Tokenizing real world assets could be an enabler of greater product offerings in DeFi at the same time as growing the user base of DeFi.

Smart Contracts, Transparency, and Getting Agreement

Contracting, or the lack of, in DeFi presents a management and resolution challenge to participants and to regulators. Contracts are never perfect and cannot be written to cover all possible events or outcomes.[153] This well-known fact is one of the driving forces toward

[150] OECD (2020), The Tokenisation of Assets and Potential Implications for Financial Markets, January 17, p. 16.
[151] Aramonte, S. et al (2022), *op. cit.*
[152] Aramonte, S. *et al.* (2022), DeFi lending: intermediation without information?, *BIS Bulletin*, no 57, June, p. 6.
[153] Coase, R.H. (1937), The Nature of the Firm, November, p. 6.

centralization; centralization allows firms to deal with this "contract incompleteness".[154]

When contracts are raised in DeFi conversations, many immediately think of smart contracts, the executing instrument of transactions within the ecosystem. Of course, smart contracts are neither smart nor contracts. Their widespread use raises concerns about stability in the system as a whole arising from complex interdependencies of what are simply packages of code. Code auditing is not a regular feature of current financial market conduct, and many participants are unlikely to want to take on the burden of examining code packages themselves, raising an investor information challenge.

As the transparent and open-source nature of most DeFi projects promises that this code will be available to all, imperfections in code will leave protocols open to exploitation. Massive returns may accrue to a niche sub-industry of code exploiters as more products offer greater number of places for errors to occur. As such situations materialize, the distributed nature of governance over these protocols may make fixes impossible or too slow. Public code will mean that everyone can see an error or exploit opportunity, but distributed governance means that the protocol must agree to fixes to the code, potentially a high hurdle depending on the number and distribution of governance token-holders.

While frequently lower-cost to execute than a traditional intermediated arrangement, smart contracts suffer from volatile costs as token value fluctuates, therefore rendering processing times and collateral valuations uncertain. As we have seen over the history of centralized financial markets, people will pay a high premium for stability in valuations, perhaps limiting the reach of smart contract adoption, at least apart from stablecoin-based protocols. Even so, ecosystem actors are trying to resolve these issues through adding flexibility clauses in updates to smart contracts.[155] Yet, as DeFi develops in complexity of operations, demand for discretion in the application of contract terms will likely also rise.[156]

Additionally, researchers like Lehar and Parlour document high inherent systemic fragility within DeFi systems, related particularly to liquidation protocols, akin to block trades at scale in the system.[157] They find market prices to be permanently affected by liquidation of collateral in DeFi protocols, suggesting instability is unlikely to reduce so long as the automatic execution of trades element remains. In theory, this fragility is mitigated by the transparent nature of operations on chain, which are observable to all. Any participant has the ability to call for liquidation of undercollateralized positions. However, this collectively transfers all risk on the individual borrowers, inconsistently with the approach to credit taken by regulators in much of the world.

The Decentralization Trilemma

Ethereum co-founder Vitalik Buterin declared that developers of blockchains face an inherent trade-off between decentralization, security, and scalability when creating a protocol.[158] In this framework, developers must choose between a fully decentralized and highly scalable system (defined as one able to handle an indefinitely growing number of transactions at relatively similar speeds regardless of volume), while also choosing between decentralized and secure, and between scalable and secure. Most systems end up compromising along each of these vectors and the result

[154] Grossman, S.J. and Hart, O.D. (1986), The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration, p. 27.
[155] Chiu, J. et. al. (2022), On the Inherent Fragility of DeFi Lending, May, p. 26.
[156] Posner, E.A. et al. (2000), The Design and Interpretation of Contracts: Why Complexity Matters, p. 4.
[157] Lehar and Parlour (2022), Systemic Fragility in Decentralized Markets, July 25, p. 3.
[158] Medium (2019), The Blockchain Trilemma: Decentralized, Scalable, and Secure?, October 4, accessed October 3, 2022.

is a more stable system. For blockchain developers, compromises between these points have resulted in rapid growth of blockchain adoption. In the future, we expect that most blockchain-based finance will likely exist on a spectrum of decentralization.[159] These protocols will range from closed institutional systems, to purely self-sovereign protocols on the far reaches of the web – with individual protocols making their own determination of scalability versus security at each of these points on the spectrum. Additionally, protocols can shift across a decentralization spectrum throughout their lifecycle, a phenomenon noted by much of the academic work on this space; decentralization is rarely static.[160] These trade-offs will likely depend on regulatory decisions, with organizations like the OECD pushing the concept of recentralization for regulatory comfort.[161]

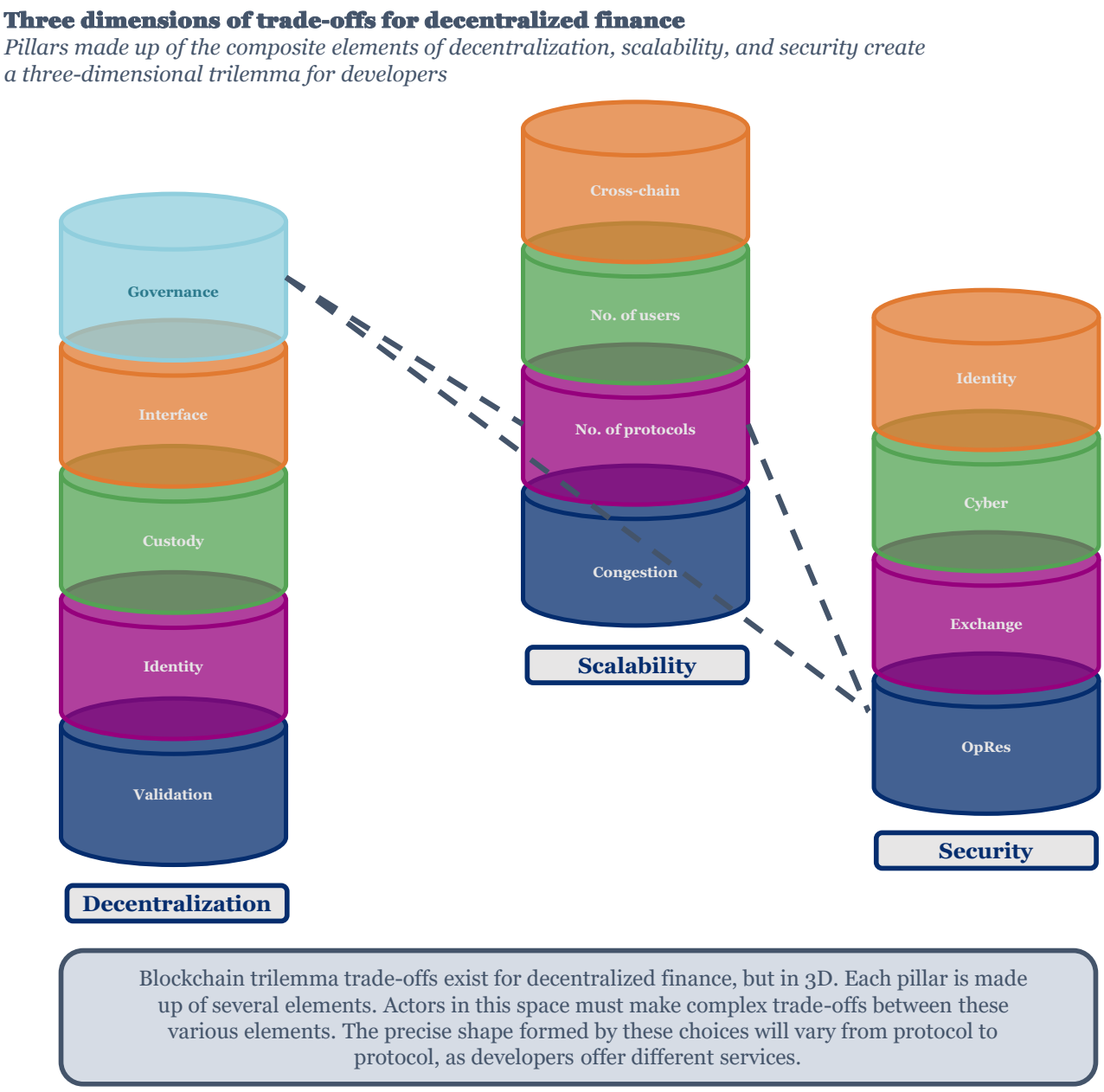
We posit decentralized finance faces a similar trilemma, but in three dimensions. For when it comes to DeFi, each vertex actually is a multilayered stack or "pillar" of different elements. For example, what is a DeFi protocol trying to decentralize: custody, identity, validation (transaction processing), infrastructure (computing power via the cloud or record storage), governance or some other element? The above list represents the key elements of the decentralization pillar, where actors in the space may be trying to develop protocols to decentralize one or all. As actors consider the trade-offs between decentralization and other pillars, the trilateral relationship will likely take a different form based on which element a protocol aims to decentralize. Decentralizing infrastructure, through distributed cloud for example, entails different security and scalability concerns than does decentralizing governance. In fact, many actors seem content to keep certain infrastructure services centralized because the added security and scalability challenges from decentralizing this element are too large. This example illustrates the multi-dimensional nature of what decentralization could actually mean in practice.[162] For a fully decentralized financial system, we much be careful to look beyond traditional banking when considering which actors hold power in this environment. In fact, many protocols will continue to make use of banks for asset custody, among other services.

At the next vertex of the trilemma, scalability elements entail network capacity, user characteristics, congestion, spectrum of services offered by protocols, and cross-chain functionality. Security elements are: privacy, cyber security, exchange resilience. These lists of elements are not exhaustive, but represent the multifaceted nature of the considerations facing developers, business leaders, and regulators.

The precise position along each vector and element(s) of focus within each pillar is likely to be different for each enterprise in the DeFi ecosystem. Each protocol will likely construct its pillar from different elements, creating new logical "shapes" each time (see **Figure 2**). For example, each of two enterprises seeking to disintermediate the custody business may rely on a centralized cloud service provider for its compute power and also require identify verification from a wallet hosting service. Each firm then could make different scalability decisions based on their desire to work cross-chain and different security calls based on their sensitivity to user privacy. The prism of decentralization trade-offs is illustrated below to highlight the potential difference in construction of each protocol-level trilemma.

[159] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 20.
[160] Ushida, R. and Angel, J. (2021) in OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 20.
[161] OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19, p. 14.
[162] This analysis bears some similarity to that presented in FSB (2019), where various elements of decentralization were identified.

Figure 2: A prism of decentralization trade-offs



Source: Authors' elaboration.

The complexity of trade-offs between the elements in each of these three pillars is likely to contribute to the continued proliferation of enterprises in this space, each catering to a specific combination of trade-offs. Additionally, this framework highlights the need for collaboration between different types of regulators to set appropriates standards and guardrails for these types of activities.

Decentralization as a Process: Considerations for the Future of Finance

As discussed in section 2, the programmability and automation offered by DeFi protocols in theory is not an unambiguous benefit. In some areas, such as payments, some frictions can be desirable. DeFi protocols that support chargebacks and/or on-chain dispute resolution will presumably gain a competitive advantage over those protocols that stick more strongly to the "your keys, your assets" ethos of DeFi historically. [163]

There may also be more interesting scenarios emerge as oracles and other on-chain actors gain more and more human-like levels of AI. Such actors may be able to perform dispute resolution or embedded supervision functions. In this case, some of the aforementioned frictions may resolve as automatic processors gain the ability to execute discretion at far faster speeds than humans could. Some in the space we have spoken with believe the trade-offs within this prism are lessening over time and, while they are unlikely to disappear, the challenge they present to enterprises will decline with the rise of new dedicated tools to manage these elements.

DeFi promises a decentralized future where no centralized intermediary holds market power. But the market so far suggests decentralization may be an illusion for many protocols, as many decentralized protocols rest decision-making power in the hands of few governance token owners or even fewer admin key holders.[164] Some element of centralization may be necessary to maintain a functional financial system.

To a large extent, regulatory guardrails will shape the development of this space. If those guardrails are too high, traditional actors may find themselves less able to experiment, particularly in the presence of a lighter-touch regime for DeFi. Regulation that prevents TradFi from participating in, or influencing, DeFi markets cannot fit TradFi institutions for the new competitive landscape, and cannot bring the benefits of established and tested risk management and supervision to the DeFi landscape.

The Path Forward

Decentralized finance has built systems where individuals conduct their financial activities "on chain" intermediated only by "smart contracts" designed to run automatically and mostly without adjustment. The path forward is more likely to find a positive point of arrival somewhere between the current system, with risk and compliance tools that are well tested and understood, and the DeFi vision of execution via technology without human intervention.

Decentralized finance tools and operations offer innovations that are likely to continue to gain attention and adoption for some functions by centralized institutions. At the same time, DeFi will continue to evolve as developers build tools to fit different purposes. The future of finance is likely to contain degrees of decentralization across the industry and make greater use of the underpinning technologies of DeFi where they offer advantages.

To achieve this evolution, DeFi will need to build new controls and ensure compliant outcomes for the activities it undertakes and services it provides. Equally, the public sector will need to

---

[163] See further: DeFi Use Cases, Adoption, and Regulatory Considerations: Architecture

[164] Learner, R. (2019), Blockchain Voter Apathy, Medium, March 30, Accessed November 2, 2022; Chiu, J. *et al.* (2022), Grasping De(centralized) Fi(nance) Through the Lens of Economic Theory, Bank of Canada, October, p. 13.

rethink how regulatory and supervisory objectives and consistent outcomes could be achieved with new models and through new technology-enabled approaches.

Investing time and effort in this work would help improve new frontiers of finance. As gamers, digital content creators, and other growing cohorts of the Web 3.0 economy become more significant parts of the overall economy, there is increasing pressure to find new solutions that are less reliant exclusively on centralized points of trust. Distributed systems and tokenization could extend compliant solutions with trading, settlement, and record keeping reimagined for digitally native participants of all sizes. At the same time, these DeFi innovations could potentially improve FX), equities, bonds, and mortgages by better integrating them into next generation automated systems and architectures.

Annex 1: Glossary

51% attack: An exploit where bad actors amass control of 51% of a protocol's assets and then can arrange the protocol operations to benefit themselves.

Atomic settlement: An instantaneous and interdependent exchange of assets, such that the transfer of one occurs only upon transfer of the other.

AML: Anti-money laundering

BCBS: Basel Committee on Banking Supervision

BIS: Bank for International Settlements

Blockchain Trilemma: The concept that a blockchain cannot simultaneously be decentralized, scalable, and secure. Theoretically, developers must balance trade-offs among these three.

Bridge: A protocol built specifically to connect blockchains.

CBDC: Central bank digital currency

CDD: Customer due diligence

CFT: Countering the financing of terrorism

CFTC: U.S. Commodity Futures Trading Commission

Cloud: provision of information technology services by third-party service providers or outsourced service providers, typically under a contract with the client and typically involving remote data storage and processing of the client's data.

Cloud-native: an application that is designed to reside on and function with the cloud from the inception stage.

Consensus mechanism: The way in which participants in a blockchain protocol reach agreement on the writing of successive blocks of the blockchain. POS or POW are popular examples.

CPMI: the BIS Committee on Payments and Market Infrastructures

Crypto-assets: A digital asset (issued by the private sector) that depends primarily on cryptography and distributed ledger or similar technology. Crypto-assets include, but are not limited to, a cryptoasset that is classified as a payment instrument in a jurisdiction and a crypto-asset that is classified as a security in a jurisdiction.

dApps: Decentralized applications. Applications that operate automatically and usually without human intervention on a distributed ledger system or blockchain.

DAO: decentralized autonomous organization

Decentralized cloud: cloud services provided through a peer-to-peer network of individuals'

excess capacity on self-managed data centers, rather than from an incorporated service provider.

DeFi: Decentralized Finance, or forms of finance (either fiat- or crypto-denominated) that make use of distributed ledger technology (DLT), and which additionally are significantly decentralized in terms of governance, custody, or otherwise.

DEX: Decentralized exchange. A DeFi platform on which participants trade assets peer-to-peer and where the exchange does not have custody of users' crypto-assets.

DLT: Distributed ledger technology

Embedded supervision: A way for regulators to continuously monitor a digital financial environment, largely automatically, by using tools within a decentralized service to monitor compliance by reading its ledger.

ESMA: European Securities Markets Authority

Fintechs: Financially-focused technology firms, providing services on a business-to-business (B2B) basis to financial institutions and/or on a business-to-client (B2C) basis.

FI: Financial institution

FSB: Financial Stability Board

FX: Foreign exchange

Governance token: A token issued to participants or investors in a DeFi protocol which grants the holder voting rights over how the protocol is run.

ICO: Initial coin offering

IOSCO: International Organization of Securities Commissions

KYC: Know your customer

Layer 1: A blockchain in which transactions are settled, e.g. bitcoin.

Layer 2: A framework on top of the blockchain that encompasses transactions which will be encoded into the blockchain at a later time.

The Merge: The Ethereum protocol move from a POW consensus mechanism to a POS one.

Metaverse: The open, persistent, real-time, interoperable, virtual world that could be built using Web 3.0 technologies, including blockchain technology, smart contracts, cryptocurrencies and NFTs that could provide the payments and legal infrastructure needed to complement VR/AR capabilities.

NFTs: Non-fungible tokens. Unique, digital identifiers that are used to verify ownership.

OFAC: U.S. Treasury Office of Foreign Assets Control

Onymous: named or identified, e.g. onymous finance requires the user to disclose their name and other identifying details to a financial intermediary, or to their counterparty in an unmediated transaction, before opening an account or entering a transaction.

Operational resilience: The ability of a system (technology or business) to be able to continue operating during adverse events or after a negative shock.

Oracles: Specialized smart contracts which serve as the data link between the on and off blockchain world which provide the information to smart contracts to determine whether or not to perform an operation, or send information outbound to data recipients or devices.

Permissioned ledgers: Record-keeping systems, such as DLT, where changes can only be made by approved participants.

Permissionless ledgers: Record-keeping systems, such as DLT, to which anyone can make updates.

P2P: Peer-to-peer

PFMI: Principles for Financial Market Infrastructures issued by CPMI and IOSCO

POS: Proof of Stake. A consensus mechanism where validators are selected based on their stake (size of holdings) of the assets in the protocol.

POW: Proof of Work. A consensus mechanism where transactions are added to the blockchain based on proof that a certain amount of work has been done through solving mathematical puzzles.

Private cloud: services in which computing resources are used solely by one single organization, either physically in the company's on-site data center(s) or externally with the third-party provider.

Protocol: The set of rules that define the operation of a blockchain or other distributed ledger, or the parameters of a DeFi platform more broadly. Sometimes is used interchangeably with DeFi project or platform.

Pseudonymity: The ability of users to be known by their handle or address alone, rather than providing their whole identity.

Public cloud: services, including general computing and/or software resources, offered by a third-party provider over the public internet. Whilst these services are generally available to any entity willing to subscribe to them, access control functions ensure the proper usage of the services by the legitimate entity under a contractual agreement with the third-party provider.

Smart contract: A block of code, written in a specialized language, that executes transactions and encodes behaviors for digital assets based on predefined conditions.

SSB: Standard-setting body.

Stablecoin: Crypto-assets where the value is pegged to a real-world asset, like a major fiat currency.

Staking: A financial instrument where investors can lock their crypto-assets in a smart contract in exchange for a reward, typically a percentage yield.

Tokenization: The process of creating digital representations of assets such as securities, bonds, land, vehicles, currency or crypto-assets, in many cases creating a more tradable and digitally native asset.

TradFi: Traditional finance

TVL: Total value locked. A measure of the assets deposited by users in a DeFi protocol

UX: User experience

Validators: Those who verify transactions and add them to a blockchain.

VC: Venture capital

VR/AR: virtual reality and augmented reality

Web 3.0: A hypothesized future form for the internet characterized by greater individual control over self-generated data and content, lower barriers to service access, persistent identity in logical spaces, the ideal of portability of identities and attributes, and greater use of VR/AR.

Whitelisted liquidity pool: A protocol where only users who have undergone CDD and KYC processes (either by the protocol operator or by a third party) are permitted to trade.

Wrapping: The process of creating compatibility between digital assets native to separate blockchains by tokenizing or "wrapping" one of the assets in a token that allows users to trade it on another blockchain.

Zero-knowledge proof: A method of verifying a particular claim (e.g. that a person is 18 years old or over) without having to share or obtain more information than needed (e.g. the person's date of birth). Typically relies on verifiable credentials, which may be tokenized, issued by a verification service provider.

Annex 2: References

1Inch Network (2022), A vulnerability disclosed in Profanity, an Ethereum vanity address tool, September 15

Adrian, T. (2017), Shadow Banking and Market Based Finance, Speech, September 14

Analytic Insight (2022), Terra was Never a Decentralized Platform, Thanks to Do Kwon's Luna Wealth, June 17

Aramonte et al. (2021), DeFi risks and the decentralisation illusion, *BIS Quarterly Review*, December

Aramonte et al. (2022), DeFi lending: intermediation without information?, BIS Bulletin No 57, June 14

Auer, R., (2019), Embedded supervision: how to build regulation into blockchain finance (bis.org), *BIS Working Papers* No 811, September (revised May 2022)

Auer, R. *et al.* (2022), Miners as intermediaries: extractable value and market manipulation in crypto and DeFi, *BIS Bulletin,* No 58, June 16

Auer, R. *et al.*, Crypto trading and Bitcoin prices: evidence from a new database of retail adoption, *BIS Working Papers No.* 1049, November.

AWS (2020), Truffle: Build and Deploy Ethereum Smart Contracts with Truffle and AWS Cloud9 (video), March 21

Bakos, Y. and Halaburda, H. (2021), Blockchains, Smart Contracts and Connected Sensors: Substitutes or Complements? , September 1

Bank of England (2022), Financial stability in focus - Cryptoassets and decentralised finance, March 26

BCBS (2021), Prudential treatment of cryptoasset exposures, June

BCBS (2022), Prudential treatment of cryptoasset exposures - second consultation, June

Binance (2022), Notice Regarding the Completion of Ethereum Merge & Information on ETHW Distribution, September 15

BIS-IH (2022), BIS and central banks of France, Singapore and Switzerland to explore cross-border CBDC trading and settlement using DeFi protocols, Press release, November 2

Bloomberg (2022), Blockchain's Forever Memory Confounds EU 'Right to Be Forgotten', August 3

Boissay, F. *et al.* (2022), Blockchain scalability and the fragmentation of crypto, *BIS Bulletin*, No 56, June 7

Boston Fed and MIT DCI (2022), Project Hamilton Phase 1: A High Performance Payment Processing System Designed for Central Bank Digital Currencies, February 3

Buterin, V. (2021), Reddit post, January 8

Carapella. F. et. al. (2022), Decentralized Finance (DeFi): Transformative Potential & Associated Risks, August

Carlton Fields (2020), The Coming Storm: DeFi and Bankruptcy Courts, June 24

Carter, N. and Jeng, L. (2021), DeFi Protocol Risks: The Paradox of DeFi in Coen, B. and Maurice, D.R. (2021), *Regtech, Suptech and Beyond: Innovation and Technology in Financial Services* (Risk Books), August 6

Carter, N. in Jeng, L. (ed.) (2022), *Open Banking*, OUP

CFTC (2022), Complaint accessible via Media Release, September 22

Chainalysis (2022), Cross-Chain Bridge Hacks Emerge as Top Security Risk, August 2

Chainalysis (2022), Geography of Cryptocurrency, October

Chainalysis (2022), How The Ethereum Merge May Impact the Crypto Ecosystem: On-chain Indicators to Watch, September 7

Chainalysis (2022), UST's Collapse & The Trades That Triggered It, June 9

Chiu, J. *et al.* (2022), On the Inherent Fragility of DeFi Lending, May

Chiu, J. *et al.* (2022), Grasping De(centralized) Fi(nance) Through the Lens of Economic Theory, Bank of Canada, October

Citibank (2022), Metaverse and Money - CitiGPS (citivelocity.com), March

Coase, R.H. (1937), The Nature of the Firm, November

Coinbase Institute (2022), Stablecoins: Coinbase White Paper, July

Cointelegraph (2022), Ethereum Foundation clarifies that the upcoming Merge upgrade will not reduce gas fees, August 17

Cointelegraph (2022), GitHub unbans Tornado Cash repositories following OFAC guidance, September 23

Cointelegraph (2022), How Does Tokenization Help Transform Illiquid Real Estate Ownership into a Liquid One, September 15

Cointelegraph (2022), Swiss National Bank exec: Regulators may favor centralized stablecoins after Terra crisis, June 27

Cornelli, G. et al. (2020), Fintech and big tech credit: a new database, September

CPMI and IOSCO (2021), Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, October

CPMI and IOSCO (2022), Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, July

Crenshaw (2021), "Statement on DeFi Risks, Regulations, and Opportunities," *The International Journal of Blockchain Law*, Vol. 1, Speech, November 9

Daian, P. et al. (2019), Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges, April 10

Dentons (2022), The Tokenization of Real Estate: An introduction to fractional real estate investment, September 26

Emmer, T. (2022), letter dated August 23, 2022 to U.S. Treasury Secretary Yellen

EuroNews (2021), Crypto crime is booming on DeFi platforms and has caused over €9 billion in losses this year, November 19

European Securities Markets Authority ESMA (2022), Crypto-assets and their risks for financial stability, October 4

FATF (2021), Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers, October 28

Finextra (2022), Singapore Fintech Festival 2022: Inside Project Guardian, November 2

FSB (2018), Crypto-asset markets: Potential channels for future financial stability implications, October 10

FSB (2019), Decentralized Financial Technologies: Report on financial stability, regulatory and governance implications, June 6

FSB (2021), Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Progress Report on the implementation of the FSB High-Level Recommendations, October 7

FSB (2022a), Assessment of Risks to Financial Stability from Crypto-assets, February 16

FSB (2022b), FSB issues statement on the international regulation and supervision of crypto-asset activities, July 13

FSB (2022c), Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Consultative report, October 11

FSB (2022d), Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative report, October 11

FSB (2022e), International Regulation of Crypto-asset Activities: A proposed framework – questions for consultation, October 11

FSB (2022f), Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative document, October 11

FSB (2022g), Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Consultative report, October 11

Gilbert, S. (2022), Crypto, web3, and the Metaverse, University of Cambridge Bennet Institute for Public Policy, March

Grossman, S.J. and Hart, O.D. (1986), The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration

Herbert Smith Freehills (2022), Retail access for virtual assets – risky business or radical open-mindedness?, November

HM Treasury (2022), UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: Response to the consultation and call for evidence, April

IIF – Deloitte (2021), Realizing the Digital Promise: Call to Action, October

IIF (2018), Cloud Computing in the Financial Sector Part 1: An Essential Enabler, August

IIF (2020), Cloud Computing: A Vital Enabler in Times of Disruption, June

IIF (2020), Response to FSB on global stablecoin arrangements, July 15

IIF (2020), Submission to FSB on global stablecoins, July 15

IIF (2022), Briefing Note on Stablecoins, January 5

IIF (2022), Principles for Digital Trust Networks, February 15

IIF (2022), Strategic Framework for Digital Economic Cooperation - A Path for Progress, April 19

IIF and Open ID Foundation (2022), Principles for Digital Trust Networks, February 15

IIF *et al.* (2022), Comments in Response to the Second Consultation on the Prudential Treatment of Cryptoasset Exposures, September 30

Insider (2021), Bitcoin Owner Who Lost Password Made Peace With Potential $220 Million Loss, January 17

IOSCO (2022), Crypto-Asset Roadmap for 2022-2023, July 7

IOSCO (2022), IOSCO Decentralized Finance Report, March

Law Commission (2022), *Digital Assets: Consultation Paper* and *Digital Assets: Summary*, July 28, both available through Digital assets | Law Commission

Learner, R. (2019), Blockchain Voter Apathy, Medium, March 30

Ledger Insights (2022), Central African Republic Wants to Tokenize Mineral Resources, June 3

Lehar, A. and Parlour, C.A. (2022), Systemic Fragility in Decentralized Markets, July 25

Lehmann, P. (2020), Technological Neutrality: A Critical Assessment, January (English translation)

MAS (2022), Consultation Paper on Proposed Regulatory Approach for Stablecoin-Related Activities, October

MAS (2022), Consultation Paper on Proposed Regulatory Measures for Digital Payment Token Services, October

MAS (2022), Project Guardian, October 19

McKinsey & Company (2022), Value creation in the Metaverse, June

Medium (2019), The Blockchain Trilemma: Decentralized, Scalable, and Secure?, October 4

MGStaking (2021), Standards, Composability, Interoperability – the key points of DeFi, Sep 7

Menon, R. (2022), The future of money, finance and the internet, Speech, February 10

National Law Review (2022), The Limits of Smart Contract Enforcement, September 8

Netguru (2021), Neither Smart Nor Contracts: Smart Contracts Need a Rebrand, August 31

OECD (2020), The Tokenisation of Assets and Potential Implications for Financial Markets, January 17

OECD (2022a), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19

OECD (2022b), Institutionalisation of crypto-assets and DeFi – TradFi interconnectedness, May 19

OFAC (2022), FINAL - Tornado Cash Complaint | PDF | Cryptocurrency

Oliver Wyman *et al.* (2022), Institutional DeFi: The Next Generation of Finance, November 6

OMFIF (2022), Digital Assets: Regulation and Infrastructure for an Evolving Economy, October 27

Posner, E.A. *et al.* (2000), The Design and Interpretation of Contracts: Why Complexity Matters, p. 4

PwC (2019), Asset & Wealth Management 2025: The Asian Awakening, January

PWGFM, FDIC and OCC (2022), Report on Stablecoins, November

Reiersen, J. (2019), Exchange networks, markets and trust, October 22

Schär, F. (2021), Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, *Federal Reserve Bank of St. Louis Review*, Second Quarter, pp. 153-74

Schär, F. (2022), DeFi's Promise and Pitfalls, *Finance and Development*, September

SIX Digital Exchange (2022), UBS launches world's first native digital bond with intended dual listing and trading on SIX Digital Exchange and SIX Swiss Exchange, Press Release, November 3

TaylorWessing (2022), Venture Capital Trends: Web 3.0, DeFi, Metaverse and Tokens, July 18

The Guardian (2022), Man who threw away £150m in bitcoin hopes AI and robot dogs will get it back, August 2

Tuck, L. and Zakout, W. (2019), "7 reasons for land and property rights to be at the top of the global agenda," World Bank, March 25

U.S. Federal Reserve Board of Governors (2022), Speech by Vice Chair for Supervision Barr on making the financial system safer and fairer, Speech, September 7

U.S. Treasury (2022), Crypto-Assets: Implications for Consumers, Investors, and Businesses, September

U.S. Treasury (2022), U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, Press Release, August 8

UNCITRAL, UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998

Uniform Law Commission (2022), UCC, 2022 Amendments to | uniformlaws.org, July 26 and September 29

Ushida, R. and Angel, J. (2021) in OECD (2022), Why Decentralised Finance (DeFi) Matters and the Policy Implications, January 19

ZeroCap (2022), How do DeFi Protocols Make Money? Revenue examples with leading projects, October 5

Lead Authors

Hannah Anderson
Policy Advisor, Digital Finance
handerson@iif.com

Laurence White
Consultant Senior Advisor, Digital Finance /Asia Pacific
lwhite@iif.com

Contributors

Conan French
Director, Digital Finance
cfrench@iif.com

Jessica Renier
Managing Director, Digital Finance
jrenier@iif.com